RFID as the Key to the Ubiquitous Network Society

A Japanese Case Study on Identity Management

Wouter Schilpzand & Christian van 't Hof

Rathenau Institute, The Netherlands
Eindhoven University of Technology, The Netherlands
Embassy of the Kingdom of The Netherlands, Japan

February 2008

Preface

This document reports on a research project on RFID in Japan, conducted by the Rathenau Institute, the Eindhoven University of Technology and the Embassy of the Kingdom of The Netherlands in Tokyo. The project consisted of desk research, interviews, observations and an expert meeting, held in Tokyo on 24th July 2007. Most of the research was carried out by Wouter Schilpzand, Master's student at the Eindhoven University of Technology, and stationed as a research trainee at the Netherlands' Embassy in Tokyo (April-July 2007) and the Rathenau Institute (March and October 2007). During the project he was supervised at the embassy by Daan Archer, attaché for science and technology, and at the Rathenau Institute by Christian van 't Hof, senior researcher. They both joined Wouter Schilpzand during the expert meeting and many of the interviews held with RFID experts in Japan. Finally we are very grateful to Kikuo Hayakawa of the Royal Dutch Embassy and Bart Schermer of the RFID Platform Netherlands for making the fieldtrip a success. It were these four men who joined Wouter Schilpzand during the expert meeting and many of the interviews held with RFID experts in Japan.

RFID, short for Radio Frequency Identification, refers to small chips being read from short distances. This technology is seen as key in a development towards an increasingly digitised public space in which people and objects are connected through digital networks. In this project we elaborate on current research being performed by the Rathenau Institute and aim to introduce a Japanese concept into the European debate on RFID: Ubiquitous Network Society. This report is written by Wouter Schilpzand and Christian van 't Hof.

Content

1. RFID, Identity Management and the Ubiquitous Network Society

RFID systems consist of chips that communicate on radio frequency, providing an identity which unlocks information from databases within the system. One of the most common applications is smart cards for payment, access and identification. In Europe, the rapid adoption of this new technology has led to concerns and debate over privacy: who is allowed to track whom. Meanwhile in Japan, RFID is more perceived as adding value to customer service. To describe both sides of the RFID revolution from a societal point of view, we will first introduce the concept of Identity Management in this chapter. Secondly, we will describe how RFID is a key technology in a next phase in the information society, in which digital communication will converge into an omnipresent network. Here too, Japan and Europe are dealing quite different with technological developments, setting the stage for a fertile cross cultural comparison.

RFID and Identity Management

RFID systems consist of chips that communicate on radio frequency, providing an identity which unlocks information from databases within the system. Specific persons can be identified once the database can link the identity number of the chip to the person carrying it, as is the case with ID cards. Once the identity is confirmed, the system can respond for example by opening a door, providing information, performing a transaction, or any other kind of service. Meanwhile the service, as well as the combination of ID, place and time, is registered.

Until recently, RFID was mainly used for logistical purposes to identify cargo. Now it has entered the public space on a massive scale: public transport cards, the biometric passport, micro-payment systems, office ID tokens, customer loyalty cards, et cetera. What do these applications tell about their users and who profits from the information RFID systems generate? On the one hand we can see privacy advocated, urging to strengthen data protection laws, while on the other hand business consultant promise higher returns on investments from more personalised services. In order to study both the pros and cons of identifying people through RFID and analyse its societal impact, we introduce the concept Identity Management. In this context, Identity Management is understood as how a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system (Van 't Hof, 2007). It goes beyond the juridical notion of protecting personal data and emphasises the active role for users determining their identity in the digital public space.

Recent research (Van 't Hof 2007) shows that users generally perceive RFID as not more than an electronic key or wallet. To the maintainers/owners of the system however, it registers movements, spending, productivity, preferences, habits and so forth. This gives them a means of providing feedback according to these identities and thus control over their users. With public transport cards, for example, operators urge users to personalise card, providing them with opportunities for analysing travel behaviour, price differentiation and direct marketing. Other examples are loyalty cards tracking access and spending behaviour and the office access cards to register working time. Still, being tracked and registered can also provide benefits: being identified as a loyal customer and being rewarded with discounts and services accordingly, being identified in the office as working hard, or being rescued during an emergency. Identity Management is therefore not just about securing personal data, it is about balancing the trade-offs of people using information technology to identify one another.

Although the smart card can be seen as the most visible application of RFID, it will most likely be a short phase, with the next generation of RFID systems waiting to be introduced. Signs from laboratories, business developers and some successful pilots show RFID technology is bound to converge with other digital technologies currently used, most importantly mobile phones and the Internet. The data generated by users is therefore likely to converge too, stressing the importance of an active approach to Identity Management even more.

A Paradigm shift in the Information Society

Many public places around the world are increasingly equipped with digital communication devices. Mobile phones are abundant, providing users a means to send their spoken word, written text, photo's and film onto mobile networks like GSM, GPRS and CDMA. Screens flash up on every corner of the streets, while security cameras track suspicious behaviour. Cars are provided with on-board navigation and payment tools, while in public transport travellers pay with smart cards, leaving a trail of digital footprints behind. RFID readers are placed at any location and send their signals in hope to encounter chips that provide them with a code to perform transactions, give access and identify cargo and people. We are nearing a phase in the information society in which sensors and computers are everywhere, a development named "ubiquitous computing" by Xerox or "ambient intelligence" by Philips.

Meanwhile, the networks supporting the data flows of these computers are converging. Telecommunications, radio, television, navigation data all went from analog to digital, and are moving from a broad variety of protocols more and more to a single protocol: the Internet Protocol, or IP. This protocol will not only enable the compatibility of networks, but also serve to identify access points within the network. Many experts believe IPv6 will be implemented soon, providing us a practically infinitely range of identification numbers - large enough to give every grain of sand on this earth its own unique address. More and more, object and person are known and connected to the network. Considering these two developments together, ubiquity and network convergence, the question emerges: are we heading towards one ubiquitous communication network? And if so, what are the consequences for the people using - or put stronger, "living inside" - this network?

Perhaps one of the most fundamental changes in the evolution of this ubiquitous network is the perception of time and place. At the turn of the millennium, cyberspace was heralded as a free space in which anyone from anywhere could communicate at any time to anyone. Following Gibson's (1984) definition, cyberspace was perceived as a new galaxy, with fundamentally new rules of physics concerning time and place. Cyberpresence was perceived to be independent of place of access to the network, while the virtual identities (personal websites, newsgroups, etc.) people remained virtually present, even when they were logged off. Users were also enabled to participate in different corners of cyberspace at the same time, encountering people one would normally never meet. With a virtual identity, one was finally freed from any physical limitations and meanwhile feeling lost in an endless space of options. Still, this notion of timelessness in space has proved to be very temporary.

In the current phase the information society is entering, cyberspace is not a galaxy far, far away one logs onto through an Internet enabled PC. Rather, it is every bit of communication surrounding us while we move through physical space. IP addresses of personal computers turned out to be traceable in case of crime investigation. Data retention laws oblige providers to store data on who was connected to whom, while using a PC, mobile phone or bank account. Navigation devices not only direct us through the physical space, but register our whereabouts to boot. The virtual identity, once lost in cyberspace, is currently becoming a carbon copy of our physical identity. Place and time are not just accompanying data, but rather defining characters of our identity. The physical and virtual reality are increasingly becoming one.

Every new phase in society needs a name in order to be recognised. At the turn of the millennium, the society being increasingly organised trough flows of data was termed as "Information Society", "network society" or "digital age". These terms underline the

interconnectedness through flows of digital data. In fact we are talking about the Internet, but it's characteristics are so fundamentally different, that even an obvious "Internet 2.0" would be an understatement. So, how do we this new phase of convergence and ubiquity? Xerox PARC, by the person of the late Mark Weiser, was the first to explicitly name this development already in the 1980s, calling it Ubiquitous Computing (Weiser et al, 1999). Weiser envisioned a world where little computers were doing their work, integrated in the woodwork of our everyday items. A decade later, Philips coined the term "ambient intelligence" underlining the notion of an environment being smart through embedded sensors and computers (Aarts, E. & S. Marzano, 2003). Still, both terms failed to explicitly address the interconnectedness of the computers and the networks that would enable this interconnectedness. Then, "the Internet of things", a phrase promoted by the International Telecommunications Union does stress the interconnectedness, but leaves out the role of users within the network, urging the European Commission to launch the phrase "Internet of people".

Japan as a Ubiquitous Network Society

In our perception, the only society fully recognising both the ubiquity as well as the convergence of information technology, is Japan. In recent years, businesses, academia and government defined their new phase as going from an e-society towards a Ubiquitous Network Society. During the e-Japan phase, roughly from before the turn of the millennium up until 2004, people where connected through information networks, mainly through Internet connections and mobile communication devices. As a next step, "things" where hooked up to the network, mainly through RFID and Internet connections. In the Ubiquitous Network society to come, both people and things are connected through a single network, consisting of seamlessly integrated smaller networks and largely based on IP. Therefore, if we are to gain a deeper understanding of what the new phase in our information society will bring, we need to go to Japan. Not because Europe will probably go in the same direction, but rather to analyse how convergence and ubiquity can work out under the particular situation Japan is currently in.

In the following chapters, we will describe this evolution in connecting people and things towards a Ubiquitous Network Society through the application of RFID. The first application is a public transport card, which we can see as "classic RFID", a chip being read throughout a network, only for performing transactions and providing access. The second application can be analysed as a next step in RFID: combining more and more functions onto a RFID chip and being connected to the Internet through a mobile phone. The third application radically changes the relationship between user and maintainer of the network. With the ubiquitous reader, an RFID user is not just "read" by his environment, he is reading his environment himself. Finally, we go into the question what the evolution of RFID use says about the development towards a Ubiquitous Network Society and what we can learn from that in Europe. But before we explore these different applications and scenarios, we will explore some relevant differences between Japanese and Western culture.

2. RFID and Identity Management in Japan

Japan is currently in a development going from E-Japan to U-Japan, or from a digital society towards a Ubiquitous Network Society. RFID is perceived as a key technology in this development. How can Identity Management as a concept help to understand the societal aspects of this development? We then first have to understand how the Japanese perceive the use of personal data in information systems. Although we, as European researchers, within the scope of this research will never reach a full understanding of Japanese culture, we can still sketch a rough image on the basis of the expert meeting and interviews we held and some key texts available.

Wa, Rinri and personal data protection

When focusing on human centric applications of RFID, there are a few cultural aspects that need be addressed. What role do personal data protection and privacy discussion have in Japan? How do companies relate to their customers? How do consumers trust institutions in the public and private sector? How do people in Japan relate to IT? Answers to these questions may help us create a context in which to place the developments in RFID applications in Japan. Having a grasp of the context, in turn, may give us a clue as to whether and how these innovations may be regarded in Europe.

Traditionally, culture in Japan has focused more on the group than on the individual person. It is the functioning within the group that primarily defines the Japanese individual. This is closely linked to perhaps one of the most concepts in Japanese culture: the preservation of harmony, known as *wa.* (Matsumoto & De Mente, 2003). Maintaining this harmony, or *wa*, is not always easy. Guiding people in their everyday life is *rinri,* often translated as "the ethics". Still, the concept of *rinri* differs from the European idea of ethics. European ethics traditionally deals with safeguarding the individual subjectivity and autonomy. According to Kitano (2007) *rinri* rather offers methods through which harmony among members of a society is achieved. This may be changing as Japanese youngsters readily adopt a more Western lifestyle, but *wa* and *rinri* still go a long way in defining the Japanese cultural identity. The emphasis on harmony and groupism that we find in Japanese culture has their reflection in the Japanese legal system. Preservation of harmony is not served well by attributing guilt. Rather, there is an emphasis on *taking* the blame than in pointing the finger. That makes Japan less of a lawyer-oriented culture than we may be used to in Europe and North America, as one of the key points of a legal system is attributing guilt (Srinivasan, 1992).

When considering RFID applications in Europe and the US, privacy is a prominent issue. As a cultural concept, it's proved very powerful and very successful. But the notion of privacy is not that old, being a typical result of the 18th century Enlightenment period in European history. It was during this period that the idea of the human individual as the fundamental element of society was developed. Thus, as privacy is more or less a European "invention", it should be no surprise that other cultures place a different value on privacy. Or maybe attach a different meaning to it than we do. Still, as Japan was guided by the strong hand of the Allies into rigorously reforming their constitution and legal system after World War II, the Western concept of individuality was introduced in the Japanese legal system. Especially the Japanese constitution seems the spitting image to the one of the United States of America, with the same rights to "life, liberty and the pursuit of happiness". In practise, the similarities often disappear. Where the judicial system in the Western hemisphere places much importance on precedence and jurisprudence, in Japan legal technicalities are not as important as the pursuit of harmony. Two decision may well be inconsistent, as long as the goal of harmony is achieved by finding a solution acceptable to all parties.

Legal protection of personal data is therefore a quite a new phenomenon in Japan. For most of history, people in Japan had quite willingly informed companies of what they wished to

know, but with the rise of computerisation and aggressive use by direct-mail companies gradually raised the issue that privacy needed to be protected. When the OECD urgently recommended legal protection of personal information in 1980, Japan started a process towards the development of a personal data protection law, albeit reluctant to protect data at the risk of hampering administrative efficiency (Srinivasan, 1992). This resulted in the *Act for Protection of Computer Processed Personal Data held by Administrative Organs*, which was promulgated in December 1988. “This law was drafted not so much because of public opinion as because of pressures of international society”, writes professor Tsuyoshi Hiramatsu in 1990 (Hiramatsu, 1990). As a law, it lacked a bit in clarity. Language was vague and no limitations to gathering data were set. Also, there was no responsibility placed on the agencies holding the data.

A new law made up for a lot of the shortcomings, though. Four years ago, in 2003, the Personal Information Protection Law has come into effect in Japan, which markedly improves on the existing legislation. In summary, this law regulates the handling of personal information by the private sector. It requires firms to notify the individuals concerned of the purpose for which the data will be used, maintain accuracy of the data and keep the data secure. Individuals are always to be allowed access to their personal information. To ensure accountability on the side of the database-owners, every firm that handles the personal data of over 5000 individuals needs to appoint a data-manager, who is *personally* responsible for the correct handling of the data. (Freshfields Bruckhaus Deringer, 2005).

Critics say that this law doesn't take things far enough, however. Practicing attorney and professor at law Takato Natsui states that unlike in Europe, there is no independent data protection authority to check on the proper enforcing of this law (Natsui, 2007). Criticism from another corner, however, state that the new law for the protection of personal data might be taking things to far. According to prof. Kimura, cultural anthropologist, the law for the protection of personal data has fed a sense of unease amongst the Japanese populace. It would seem that the very effect of this law is that many Japanese become quite edgy when their personal data are used. He notices response rates in his surveys falling, as people will not give data on their personal situation (Kimura, 2007). The concept of privacy in Japan, both he and prof. Natsui state, is limited to the use of personal data.

Concerning the protection of privacy specifically where RFID is concerned, the Japanese Ministry of Economy, Trade and Industry (METI) together with the Ministry of Internal Affairs and Communications (MIC) have jointly created the *guidelines for privacy protection on electronic tags*, which were published in 2004. These guidelines mostly address the obligation of firms to notify consumers of the use of tags and the obligation to allow for consumers to deactivate tags. The guidelines are completely aimed at the use of RFID in shops and other forms of item level tagging and make no mention of RFID applications like smart cards, though. This in itself may not that much of a surprise, as these guidelines were drafted in close cooperation with EPC Global, to which both ministries turned for advice (Natsui, 2007).

With regard to the databases on information gathered by the tags, these guidelines refer to the aforementioned law for the protection of personal information. As guidelines, they are not enforced as laws and thus have little power. However, firms tend to adhere to government guidelines quite well, says professor Ota, who teaches business culture at Hitotsubashi University. If companies would get bad publicity somehow, and it would turn out that it was not complying to government guidelines, this would tarnish the firm's good name even further. Japanese firms are quite fearful of public scandals, which is a trait following from trying to uphold societal harmony and rather take the fall than point the finger (Ota, 2007). All in all, it can safely be concluded that Western legal concepts on privacy and data protection are insufficient to understand the handling of personal information in a Japanese context.

Identity Management, *anshin* and consumerism

If the Western concept of privacy does not work, how about Identity Management? Is this a concept suitable to analyse how personal data is used in RFID systems? This question was central during a presentation on "RFID and Identity Management in Europe" at the expert meeting in Tokyo, attended by academia, businesses and government. Or put more precise: does Identity Management equal *rinri*? The first responses were low, but once Professor Kimura proposed Identity Management has more to do with *Anshin* everyone agreed. This concept proved to be leading us to a deeper understanding on why RFID has become so broadly accepted in Japan, leading to virtually no debate on privacy or personal data protection.

Prof. Kimura shows that in general, Japanese are not a trusting people. His research comparing Japan, South Korea and Finland shows that the Japanese are the least trusting of the three (Kimura, 2007). Research by Prof. Hofstede shows a similar result, stating that Japan has a culture striving strongly towards uncertainty avoidance (Hofstede, 1997). While lack of trust and risk avoidance do not correlate perfectly, they both indicate that the Japanese prefer to be in controlled environments with as few surprises as possible. This manifests itself in *anshin*, a word much used and a concept much valued in Japan. *Anshin* translates best as "peace of mind". But there's more to it. Since there is great emphasis on risk aversion, *anshin* could perhaps be understood as "inner peace through external control". Anshin plays a considerable part in the adoption of RFID in Japan, confirm several experts. Many new RFID enabled services aim at improving the *anshin* of their customers. One example, giving young children a tag to keep an eye on their whereabouts, is described in more detail in chapter 5. Another way in which RFID is used to improve *anshin* can be found in pilots for food traceability. Or, unrelated to RFID but interesting all the same, Japan's largest mobile carrier NTT DoCoMo released a mobile phone on the market especially for children, with an on board GPS tracking facility and content filter so that parents were assured of their children's' location as well as their protection from harmful content.

Paradoxically enough, to our European eyes at least, many Japanese give out their personal data to companies more easily than to the government. Consumers readily fill out registration cards for loyalty programs, but refuse to provide personal details to government. For example, recently, efforts of the Japanese government to introduce a social security number were postponed after public protests. When asked for an explanation, most Japanese we spoke, used the word *o kami*, which stands for both government as well as God and refers to a certain fear for too much state control from above. Two factors may be of help in explaining this. First of all, World War II, when millions suffered, amongst which their own population. As a result, Japanese people tend to want to keep their government in check. Another reason is that companies, traditionally, are viewed as an integral part of society.

Companies have a strong relationship with the communities around them and often play a key part in social networks. This manifests itself not only in that employees spend most of their time (including leisure) with their colleagues, but also that at certain holidays, companies organise events to thank the community for their support (Ota, 2007). With regard to the way that companies are beginning to use RFID, this attitude of serving the community becomes readily apparent. As Bart Schermer, secretary to the RFID Platform Netherlands, an industry organisation promoting RFID, noted during the RFID study tour, there is a fundamentally different rationale for introducing RFID by Japanese companies compared to their Western counterparts. Where Western firms tend to primarily want to introduce RFID to cut costs in logistic chains, Japanese firms primarily aim at employing RFID to better inform their customers about their products, thus improving the level of service. Japanese companies not seeking a way to cut personnel costs through RFID introduction has its origins in the idea lifelong employment, still quite common in Japanese firms. A common feeling during the RFID expert meeting was that in the longer term RFID may lead to less staff being hired, but it is not likely to lead to staff redundancies in the short term.

In general, it's safe to state that there is a trusting bond between consumers and businesses in Japan, more than there is in Europe. When firms introduce RFID enabled services, or indeed any service or product, they are well developed and generally very reliable. New systems are only rolled out when they are deemed reliable and better than the current one. Japanese consumers do like the consuming game, but products and services do have to live up to the expectations. Reliability is of utmost importance when introducing a product. This may well be rooted in the shame culture: if a product fails, a producer takes responsibility and does not point a blaming finger. Also, Japanese, especially urban dwellers are avid consumers. This manifests itself in a strong curiosity towards new things. Shop windows and television shows hop from hype to hype. And the Japanese consumer follows eagerly. Outer appearance is paramount amongst the urban population. Besides wearing Versace coats and Luis Vuitton bags, showing you're modern and trendy is part of everyday life. As professor Kimura put it: "we buy what fascinates us." Professor Ota sees a link with the close connection between consumers and the companies. Consuming is a way of helping Japan stay a strong economy.

Japan as a socio-technical laboratory

Aside from these socio-cultural factors, some uniquely Japanese business-led research and development add to the adoption of RFID. One such enterprise is the Ubiquitous Network Laboratory led by prof. Ken Sakamura, who is the first to have specifically design a network architecture suitable for realising the Ubiquitous Networking Society. Also, mobile carriers are not dominated by the businesses developing the phones, but by the service providers. NTT DoCoMo, being the dominant mobile communication provider with a share 54% plays a significant role in implementing new applications. In Europe, mobile services are mainly defined by the companies developing the phones (i.e. Nokia), while in Japan the service provider sets the standard.

Therefore the difference between the use of a mobile phone and the Internet is already blurring in Japan, both in the perception of the consumers as well as in the statistics. High speed mobile Internet, like I-mode, is common and often used in Japan. In fact, of nearly 88 million Internet users in Japan, almost 81 million use a personal computer to do so and 71 million use their mobile phone (MIC, 2007). The total population of Japan in 2007 is just over 127 million people. So, note that the figure on fixed and mobile Internet use should not be totalled to arrive at the total number of Internet users. Most people use both terminals to access the Internet. In urban areas, commuters heavily rely on public transportation. As it is taboo to make phone calls on-board a Japanese train (fitting the concept of *rinri* that people should not disturb their fellow passengers), people tend to while away the ride writing e-mails, surfing the web and placing on line purchases (Nikkei daily, 2007).

Still, what we have seen in Tokyo, in terms of RFID systems, is not necessarily representative for the rest of Japan. Most of the RFID ticketing and payment systems are limited to the big urban areas. The same goes for broadband accessibility and, therefore, adoption. And, while the Japanese consumer market may be called relatively homogeneous, there are different societal groups with different needs and attitudes towards IT. In contrast to what is often thought in Europe, the Japanese are not the biggest IT adopters on the block. Most recent data by the OECD shows that Japan ranks 12th of OECD countries in broadband penetration in Japan, compared to a second place for The Netherlands (OECD, 2007). Prof. Kimura warns for a digital divide that exists in Japan. A digital divide may be especially worrisome when, as we shall see in the next chapter, the Japanese government strives towards having IT play a much more prominent role in offering solutions to social issues such as care for the elderly and for the disabled (MIC website, 2007) An MIC press conference confirms a digital divide between old persons and the younger. While more and more older persons do have access to Internet either by PC or by mobile phone, a big gap remains present (MIC White Paper, 2007). The MIC spokesperson presenting the 2007 Information and Communications in Japan White Paper tells us that the MIC is not very optimistic about alleviating this digital divide. Prof. Kimura shows that an age divide is not the only kind of

digital divide present in Japan. He shows that people in urban areas have larger IT use statistics than do people in rural areas and that the higher incomes have a significantly higher use rate than do the lower incomes (Kimura, 2007).

Nevertheless, Japan has a unique position to be at the forefront of the next phase in the information society, using RFID to its full potential. Japan can therefore be viewed as a socio-technological laboratory for Europe rather than seeing developments in Japan as the logical next step for Europe. Through our desk research and the interviews we held with Japanese experts, we can discern the following social and cultural factors in Japanese society which strongly support the uptake of the concept of Ubiquitous Network Society. These are:

- A large, relatively homogeneous consumer market: 130 million people, speaking one language, with a GDP per capita equal to Western European nations
- Anshin (peace of mind) overruling privacy concerns
- A "shame culture" rather than a "blame culture", limiting the misuse of personal data and lawsuits accordingly
- A stronger trust in big businesses
- A stronger urge of consumers to take up any new application at hand
- Network convergence already part of daily practise

3. Going from e-Japan to u-Japan

In our perception, the society most fully recognising both the ubiquity and the convergence of information technology is Japan. In recent years, businesses, academia and government defined their new phase as going from an e-society towards a Ubiquitous Network Society. During the e-Japan phase, roughly from before the turn of the millennium up until 2004, people were connected through information networks, mainly through Internet connections and mobile communications devices. As a next step, "things" are hooked up to networks, mainly through RFID and Internet connections. In the Ubiquitous Network society to come, both people and things are connected through a single network, based on the Internet Protocol. It's hard to trace the origin of the term Ubiquitous Network Society, as many organisations claim it. But perhaps that's also part of it's success.

A brief history of the Ubiquitous Network Society

One of the actors that has played a key part in developing the concept of the Ubiquitous Network Society is the Nomura Research Institute (NRI). This institute is considered to be one the most influential private sector think tanks in Japan. Primarily an IT consulting firm, this firms regularly researches trends and developments in IT. The NRI is the first to explicitly state a shift in paradigm. They do so in an article, aptly named *Ubiquitous Networking: Towards a New Paradigm,* which was published in 2000 (Murakami, 2000). This article acknowledges the concept of Ubiquitous Computing, but points at the importance of networks to realise this concept. Rather than focusing on individual ICT elements, as do the concepts of Ubiquitous Computing and Ambient Intelligence, this paradigm focuses on the pervasive character of a network that connects both people and objects. Ubiquitous Networks, according to the author, Murakami, allow the connecting of all kinds of user terminals to an all-encompassing network, or a series of interconnecting and interoperable networks.

In this early stage, Murakami doesn't refer to RFID as an enabler of the Ubiquitous Network yet. Over the years, a number of papers following up on this subject appear. The vision evolves and Murakami shifts his focus from connecting different user terminals to a model that focuses more on users and their connectivity to IT networks to interact with each other and with service providers over this network. Considering that the Nomura Research Institute is a system integrator many clients of whom are firms that offer such services, this shift might be the result of business sense. Whatever the reason, this shift from connected terminals to humans connecting to a network, opens up a new perspective of emphasising on how to use this connectivity, and not just on how to build it.

In 2004, Murakami publishes another article, called *Ubiquitous Networking: Business Opportunities and Strategic Issues* (Murakami, 2004). In this article, he discusses the uptake of the new paradigm amongst Japanese business and policy makers. From 2002 onwards, big high technology firms such as NEC, NTT DoCoMo and Hitachi, start embedding their activities related to ubiquitous networks in the structure of the company, by erecting divisions specifically tasked with developing the ubiquitous network or offer related services (Murakami, 2004). This is especially interesting when one considers that the term "ubiquitous" is by no means a Japanese one and in those years (2000-2002) not all that well known. Thus, introducing it as a division title, is more than just a fancy name. In a later article, Murakami explores the prevalence and the use of the word "ubiquitous". He quotes a survey that explores the appearance of newspaper articles on ubiquitous computing of ubiquitous networking. This is seen to take off after 2000, with 24 articles, continuously rising to 554 appeared articles in 2004 (Murakami, 2005).

The 2005 article is interesting for another reason, in that it is the first to specifically mention RFID as an enabler for the ubiquitous network. The role of RFID in the ubiquitous network is further explored by Dr. Murakami's colleague Mr. Tsuji. In his article *Next-Generation*

Ubiquitous Network Strategy, Tsuji describes how RFID tags provide a means to also include items without real networking or computing power in the ubiquitous network. In previous reports on the ubiquitous networks, the emphasis was more on connecting users though user terminals than connecting users to essentially non-smart objects. As RFIDs generally hold very little information, Tsuji explores ways to have the RFID tags refer to on line databases from in which the relevant information is stored. (Tsuji, 2006) Interestingly, when he explores a possible network architecture and infrastructure to do so, he bases himself on work by EPC Global, even though this very task was being tackled much closer to home.

The paradigm embodied in technological practice

If we may consider the Nomura Research Institute as a key player in stating the Ubiquitous Network as a new IT paradigm, special mention must be made of the work done by Prof. Ken Sakamura in developing technology and infrastructure to support it. Many experts in the field consider Prof. Sakamura to be amongst the founders of the Ubiquitous Network Society concept. In 2002, he established the Ubiquitous Networking Laboratory (UNL) in 2002 which aims at researching and developing a ubiquitous networking environment (Ubiquitous Networking Laboratory, 2005). Interestingly, the mission stated in the documentation on his laboratory is to realise the vision of Ubiquitous *Computing* rather than Networking. While creating a networking environment is the main goal, this was apparently not perceived as a reason to formulate a different paradigm than Ubiquitous Computing, even though the original vision was very unclear in the respect of networking. When he talks about it though, prof. Sakamura does speak about the Ubiquitous Network Society and acknowledges his role in outlining the paradigm (Sakamura, 2007).

The work of the UNL aims at three goals: the development of RFID chips, network infrastructure and the development and testing of applications. The applications the UNL is working on, all have in common that the relation between user and RFID technology is the exact opposite as in the "classic" applications of human centric RFID in which users carry a tag through a network of readers. The UNL puts a tag on objects and hands the RFID reader to the user. To give a few examples: a medicine verification system where medicines are equipped with a tag and users can request information on them with a handheld reader, or a guiding system for the visually impaired, where their cane is equipped with an RFID reader and tiles in the sidewalk contain a chip.

The core concept behind the technology developed and employed by the Ubiquitous Networking Laboratory is to create a system that bridges the real world, with the objects we see around us every day, and a virtual representation of it, where information about these objects and their relations are stored in databases. This concept goes by the name of *Ubiquitous ID architecture*. The most basic, and perhaps the most important, part of this architecture is the ucode. The ucode is a 128 bits code, contained on a tag. With a 128 bit code, it is possible to create 2^{128}, or roughly 34.10^{40}, different codes. In practise, this is a nearly inexhaustible number. If you would give a trillion items a different number each day for a trillion years, you still wouldn't nearly have used all the possible combinations up. The code which is broadcast by a tag, does not mean anything in itself, it is just an identifier. When it is picked up by the reader, it is then sent to the u-code Relation Database, which refers the UC to the information associated with the number is stored (Sakamura, 2007). This way, the content associated with a particular chip can easily be updated. Storing information in the chip itself would require changing the chip whenever a situation evolves. Besides, tags have only a very limited data storage capacity.

Up to a point, the ucode system is similar to the EPC Global RFID codes, which are used in the rest of the world (and also in a large part of Japan). The ucode system differs from the EPC Global system, however, in its openness. The EPC Global standard refers to standardised tags, emitting a code at a standard frequency which hase some fixed space for numbering organisations and product types and provides this information only to the the large licenced companies who maintain the RFID environment (e.g. a retail chain). The ucode system, on the other hand, includes many different tags (supporting RFID tags with different

frequencies, infrared beacons, etc.), and can include many different code standards, amongst which the EPC codes. Users of ucode have much flexibility on how they want to use both the code and the system. The basic assumption behind this concept is that many objects in the world around us will be tagged and used for many different functions by many different people. As different uses will require different tags, the ucode system is very open to include new kinds of tags. In short, the ucode system is much more flexible than the EPC Global system, making it much more suitable for use in a (semi-)open system, for example in public space.

The Ubiquitous Networking Laboratory has developed a PDA-sized handset that picks up the the codes transmitted by the tags and retrieves and displays the associated information. This device communicates with its environment in three different ways. First, it communicates with objects. Or, with their tags, to be more specific. To this end, it is equipped with a multi-frequency RFID reader, an IR receiver and a bar-code reader. Secondly, it communicates with the information databases to retrieve the information associated with the tags. For this, it is equipped with either Bluetooth or wireless LAN functions. And last, the Ubiquitous Communicator has to present the information to the user. This is done through a full colour screen and a headphone. These elements combined (the tags, the infrastructure and the user terminal) make the ucode system the first system that is completely tailored to fit the Ubiquitous Network Society paradigm.

The Ubiquitous Networking Laboratory is not the only firm in Japan which has made the Ubiquitous Network Society its business. NTT DoCoMo for example, Japan's largest mobile carrier, also strongly emphasises a vision in which a pervasive network connects us anywhere at any time. Development efforts by this firm are directed heavily into high-speed mobile broadband Internet and creating new functions for mobile handsets. A good example is the joint venture that NTT DoCoMo established together with Sony, called FeliCa Networks. FeliCa Networks develops and manages the application of RFID in the mobile phone, used mainly as an electronic wallet, for ticketing and for loyalty systems. Following the entrepreneurial turmoil on the concept of Ubiquitous Network Society, the Japanese government followed suit by putting the concept into policy.

Policy for the Ubiquitous Network

Now that we have identified two parties that helped shape and develop the Ubiquitous Network paradigm, it is interesting to explore how the Japanese government picked up on this development. In 2003, the Japanese Cabinet Office (the Ministry of the Prime Minister, that has considerable power in making policy) adopted the e-Japan II policy. This policy aimed at the promotion of IT utilisation in Japan and had the creation of a ubiquitous network as one of the goal scenarios. When this policy ended in 2005, IT stimulation policy had been taken over from the Cabinet Office by the Ministry of Internal Affairs and Communication (MIC). The new policy package then adopted was called the u-Japan policy, where the u is for ubiquitous. Creation of a ubiquitous network had shifted from being a goal in one of the scenarios in the e-Japan II policy to the focus of the new policy. The MIC has, for this purpose, adopted the Ubiquitous Network paradigm, which they call the Ubiquitous Network Society. Interestingly, when enquired after the origins of the Ubiquitous Network Society concept, the spokespersons of MIC claim to have developed this vision. The same was true with the other two organisations we mentioned before. Who the actual inventor was, is not of real importance. What this does show, is that these organisations do share a broad support of the concept. After all, one would not claim to have developed a concept one does not support.

The u-Japan policy was adopted in 2005 and aims at Japan being the "World's front runner of the IT revolution" (MIC website, 2007). How exactly this ambitious goal will be achieved is not something that we will discuss here in much length. What we are mostly interested in, is to see what the MIC envisions for RFID in attaining the Ubiquitous Network Society. The u-Japan policy has three major goals: the development and promotion of network technologies, of utilisation technologies (read: RFID) and the development and promotion of safety and security through IT (also, mainly RFID and sensor networks) (Nakazato, 2007). These goals are translated into three ambitious slogans. First is to ensure that 100% of the Japanese population to have access to broadband Internet. Secondly to ensure that 80% of the

population appreciates the role of IT in resolving social issues. And third is to ensure that 80% of the population feels comfortable with the use of IT (MIC website, 2007). Whether these goals are attainable remains to be seen. But it is interesting to note that these goals are all phrased in a way that centres on users and their attitude towards and use of IT. This fits the paradigm of the Ubiquitous Network Society, in which users can connect to everything anywhere, anytime, very well.

This user centric approach is reflected in the kind of projects sponsored and undertaken by the MIC. While the scope of this policy package is potentially huge, the actual budget is somewhat smaller. Per year, the u-Japan policy package is attributed roughly 1 billion Yen (Uchida, 2007). With current exchange rates, that equals to 60 million Euro. The level of involvement of the MIC is very much on the practical level. It aims at developing and testing RFID and network technologies in real projects, aiming for the projects to deliver services that have a societal value. Human centric RFID plays a big part in many of these projects. The goals of these pilots are not only to test and tweak the technologies used and to help resolve issues that may arise, but also to create a set of best practises that firms and organisations can use as an example if they would emulate such services and to create strategic networks amongst firms. To this end, the MIC awards the best new services that fit in the Ubiquitous Network Society vision with a prize in order raise understanding and support for IT and to set examples (MIC website, 2007). But in stimulating IT adoption and enhancing IT accessibility, the MIC does not limit itself to individual people. Increasing IT knowledge and IT adoption amongst Japanese firms, who typically do not use IT very intensively, is also a goal of the u-Japan policy (MIC website, 2007).

In the projects relating to RFID the role of MIC does not really target the chips themselves. Rather, the MIC wishes to stimulate the smooth functioning of networks that link these chips to their information. This can be illustrated well with a pilot that was carried out in 2006, concerning food traceability. This pilot employed RFID in the supply chain of Japanese beef, enabling supermarket shoppers to receive detailed information about the origins of the beef, its subsequent processing and even recommended recipes. These data do not reflect the results of one single database and network, as each part of the supply chain is likely to have it's own data gathering and storage system. The part that MIC plays in such projects is to fund the developing of technologies to ensure that these networks and databases become interoperable and to ensure that each and every actor has access to the right parts of the databases (Nakazato, 2007). Other pilots that have been carried out to attain similar goals are the use of RFID for medication support, where medication is tagged and users get information about the medicines through an RFID reader, and pilots for child safety, in which children receive a tag and readers in the environment register their arrival at school for their parent's peace of mind. This last example of RFID will be illustrated in more detail in chapter 5.

The u-Japan policy package is not the only Japanese policy in which RFID development and stimulation plays a part. The Japanese Ministry of Economy, trade and Industry (METI) has played a very active part in stimulating RFID for business to business transactions. METI has focused on three areas in paving the way for large scale use of RFID: international standardisation, price reduction and subsidising field trials to generate best practises (METI, 2006). In the field of international standardisation, METI closely collaborates with EPC Global. METI aims at helping Japanese RFID producers as well as users by cooperating with EPC Global: Japanese produced chips need to be usable not just domestically and international supply chains should be able to employ a common set of technologies. Thus, activities in the international standardisation for RFID has occurred in two categories mostly: developing an internationally supported product code and setting technical standards.

Product codes, such as the bar-code, are not necessarily shared internationally. Europe, for example, uses a different type of bar-code than does Japan. Remedying this streamlines international logistics. Activities for setting technical standards occurred for example in the domain of bandwidth use, read range and syntax and semantics of the data communication between tags, readers and host servers (METI, 2006). The last part effectively being the "language" that the RFID system speaks, with syntax meaning how the codes (compare to sentences and words we use) are formed and semantics being the meaning of these codes. METI says that most of the work in the field of standardisation has by now been completed.

The work still ahead mainly focusing on ensuring interoperability of different closed RFID systems (Kameyama, 2007).

METI's involvement with RFID lies thus mainly in the area of item level tagging. Item level tagging was also the rationale for METI to initiate and fund the Hibiki project. The goal of this project, which ran from 2004 through 2006, was to develop an RFID inlet compatible to the EPC generation 2 specifications with should not cost more than 5 Yen. METI tendered this project and Hitachi, along with four supporting companies, was selected to carry it out. The result was the mu-chip, which, at the time of release was the smallest RFID chip in the world. The low cost of the mu-chip make it a good candidate not only for item level tagging in closed supply chains, but also for use in ubiquitous network scenarios. Hitachi is closely involved with Ken Sakamura's Ubiquitous Networking Laboratory who sees a part to play for the cheap mu-chip in his vision of tagging items in the real world to provide users with a ubiquitous communicator with information on those items (Imura, 2007).

As we focus on Identity Management issues in this study, item level tagging is of less relevant in this context. Moreover, the concept of the Ubiquitous Network Society and the role that RFID plays in it, also emphasises on human centric applications of RFID. Almost by definition, as RFID for supply chain management is based in closed systems, which is a contradiction to the notion of ubiquity. Therefore, the next chapters will focus on specific applications of human centric RFID. We will interpret them in the light of the Ubiquitous Network Society and see how each application will take this vision one step further. First, in chapter 4, an application very common in Europe too: a public transport smart card. But due to its scale and manner of implementation of much interest. Then chapter 5 deals with the more advanced RFID applications: convergence of RFID with mobile phones and the Ubiquitous Communicator, placing the reading in the hands of the user who can then surf trough the public space as if it were cyberspace. Finally, in the concluding chapter we will we elaborate on the functionality of these three application, to sketch the following steps towards a Ubiquitous Network Society and the Identity Management issues at hand.

4. SUICA: building up identity along the tracks

Suica is Japan's Super Urban Intelligent CArd: an RFID smart card for using the services of the world's biggest people carrier: the East Japan Railway Company. While European RFID transport cards are still in their infancy, this system is running very successfully on a large scale. As of June 2007 over 20 million Suica cards have been sold, providing access to 1739 stations (Mizutani, 2007). Of special interest from Identity Management point of view, is the elaboration of the functionality of SUICA. In 2004 an e-money function was added, currently suitable for payment in over 12.000 stores and services in and around the stations. January 2006 saw the start of Mobile Suica, incorporating the RFID application into the mobile phone. And as off March 2007, a new card for public transport, based on Suica, was launched: Pasmo, a collective undertaking of 101 mass transit companies in the Tokyo metropolitan area, completely interoperable with Suica. This elaboration on functionality provides maintainers of this RFID environment a rich picture of the travel and consumption profiles of it's users. But as we will see, this has not (yet) led to invasive marketing. Within this, both users and maintainers appear to have stricken the right balance in Identity Management - something which could prove to be a valuable example for us Europeans.

The tracks leading to Suica

Suica is the result of a long process. The development process started back in 1987. The Research and Development department of what then still was the state-owned company Japan National Railways, had some interest in an emerging technology: proximity cards. Proximity cards were capable of storing much more data than magnetic cards and didn't need to be taken out of the wallet, which would improve user convenience. The first experiments that were carried out used write-only cards. This meant that the cards only contained a code to identify the user and that every transaction had to be settled on line through a direct link to the server. Credit information and user location would that be updated in an on line database. With 15 million users a day, it quickly became apparent that this would not be feasible. Especially considering the state of affairs in local area networks in those years. Therefore, it wasn't long before the decision was made to use a rewritable chip. This way, the account information could be stored and updated on the card, thus relieving the stress on the network. First prototypes of the chip arrived in 1988. Testing could begin. (Shiibashi, 2002)

In the meantime, Japan National Railways had been privatised and divided by region. JR East, the largest of the newly formed railway companies, had managed to claim the IC card research team and given it a place in the new organisation. In 1990, when magnetic cards were introduced in the region around Tokyo, the future for the proximity card system did not look bright. After all, the magnetic cards just introduced had required heavy investment in ticketing infrastructure and would reduce the immediate need for yet another new system. The suppliers of the different parts of the proximity card system had a feeling things would take a turn for the worse and announced that they would seize their development efforts. Within JR East the research was scaled down, but did nevertheless continue. In the years that followed, the required specifications and functions for the new system were listed. First and foremost, the proximity cards' system had to be at least as reliable as the magnetic cards. Furthermore, the new system also had to be cheaper than the current one and should be able to grow into a platform for offering new services (Shiibashi, 2002).

JR East has had to solve some problems in order to make the new system more reliable. As many people in the big urban areas rely on fast and efficient public transport in their daily commutes, the stream of passengers at the ticket gates should not be hampered. In order to prevent queues getting longer, the maximum time in which the transaction had to take place was set not to exceed 0,1 seconds. The first field tests, in 1994, were quite disappointing. The number of transactions that failed was more than twenty times as high as that of the benchmark. The two main causes found were the inconvenient shape of the "communications field" (it had the shape of a rugby ball that stood tip down on the reader-writer) and the frequency used by the system. The development team had chosen for a *quasi-*

microwave frequency. In the lab, cards and readers operating at these frequencies yielded the best results for at minimum cost. During the field test it came to light that the water in the human body readily absorbs this signal and thus diminished the communications field with its already clumsy shape (Shiibashi, 2002).

In 1995, enough progress had been made for a second field test. The communications field had been transformed and now had the size and form of a hemisphere. Furthermore, a shorter wavelength was used in the communication between the card and reader. While the margin of error still was transgressed quite heavily, it had improved considerably. Still, the amount of failed transactions was still about four times as big as with the magneto-tickets. And another problem arose. This series of tests was carried out over half a year, while the first field test took only a month. These first cards carried a battery to strengthen the broadcasted signal. The battery turned out to last only three months. Having to renew one's card four times a year was considered inadmissible, so another solution needed to be found (JR East website, 2007).

A final series of field tests in April 1997 had to reveal if the contactless ticket could live up to the expectations. The power source for the transaction had been replaced from the card to the reader, thus eliminating the need for a battery. Instead, the chip in the card was powered by electromagnetic induction, drawing energy from the interrogator signal from the reader. The real innovation to reduce the fail rates turned out not to be based on technology but on user behaviour. To ensure that users held their card long enough within the read range, the *Touch and go* principle was devised: briefly let the card touch the screen of the reader and then move onwards. Now, users no longer pulled their card through the communications area too quickly. (Shiibashi, 2002)

The chip that Suica's developers decided to use was Sony's *FeliCa.* The process of developing FeliCa started in 1988 and was carried out in conjunction with Suica's development, for a large part. It is not a coincidence that the specifications that JR East required for Suica completely match the specifications of the FeliCa chip. FeliCa has grown out to be the *de facto* standard in Japan for RFID payment and loyalty systems. Outside of Japan, there are some RFID smart cards that are based on FeliCa. Hong Kong's Octopus card, that was introduced in 1997, was the first and, with 20 million cards sold, the biggest application of FeliCa outside Japan (FeliCa Networks, 2007).

One year before Suica was to be introduced, the Japanese Ministry of Land, Infrastructure and Transport hosted meetings for all firms providing public transport that considered implementing contactless smart cards. The goal: to set a common standard so that the different systems would technically be interoperable. This resulted in the Consortium of Japanese Railway Cybernetics, launching a set of standards in 2000. When an RFID train pass is bought from a company that adheres to these standards, it can be used on the networks of all transport providers that use these standards too. We may safely assume that both JR East and Sony have had a dominant position in this process. The standards released by the consortium are completely in line with the technical specifications that JR East had set for Suica, which in 2000 was well in its implementation phase (Nakamura, 2004). And thus matched the specifications of Sony's FeliCa chip. As for international standardisation, that has not had top priority. In fact, as we briefly mentioned before, when Suica was introduced, it did not adhere to any international standards whatsoever. However, JR East has worked to have Suica acknowledged by the International Standardisation Organisation (ISO), in which it has been successful. Suica now adheres to ISO standards for communication protocols and has gained ISO accreditation for security evaluation and certification (Shiibashi, 2005).

Once the technology proved up to the task, the development team could focus on the financial side of introducing the new system. The costs for introducing it in the Tokyo metropolitan area were estimated at 46 billion Yen (the equivalent of roughly 460 million Euro, at 1998 exchange rates). Because magnetic cards had been introduced some ten years earlier, at considerable investment, just replacing this system for a new one was not an option. However, in time the ticketing gates were due for replacement. The cost of this was estimated at 33 billion Yen. Adding a Suica reader to these new machines could be done with virtually no extra cost. And, as an added advantage, Suica required much less maintenance than the

system in place, which has very many vulnerable moving parts. De maintenance costs saved were calculated to amount to 13 billion Yen over ten years. Exactly the amount needed to offset the costs of introducing Suica (Shiibashi, 2005). Based on these calculations, JR East decided to introduce Suica in Tokyo and its surrounding area. From November 11th 2001, Suica could be used at 424 of JR East's stations. Within half a year, another 40 stations were added to this number. Over the years, the network of stations has expanded and numerous functions have been added to the new ticket.

Suica becoming a full service card

One of the demands that JR East's management had with respect to Suica, was that it should grow to be a platform for multiple services. (Shiibashi, 2002) In the course of the years that followed Suica's introduction, this demand was fulfilled. Suica could be used on more and more stations. And JR East also introduced completely new functions to the card. Adding new functions to Suica, for a company like JR East, was relatively easy. JR East has a very broad portfolio, apart from mass transit by train. The company owns a great deal of real estate, especially on, under and around the stations (Tokyo's larger stations lead a successful second life as shopping malls and office buildings). JR East also issues its own credit card: View. It owns department stores, coffee shops and fast food chains. This broad base of operations expands JR East's possibilities to add other functions to Suica, without having to depend heavily on other companies. Here, we will give a brief overview of the development of Suica after its launch in November 2001.

In the first months of 2003, about a year and a half after Suica started, JR East combined Suica with View, her own credit card. From then on, Suica could be linked to your credit account to provide users with an auto-charge function. Whenever one's stored credit dropped below a predefined amount, there would be an automated transfer from one's credit account to the Suica account. At the end of the same year, Suica started operations in another area serviced by JR East: Sendai. In this town with roughly a million inhabitants, Suica can be used at more than 70 stations since October 2003. Also started in 2003, Suica could be used in some of the lines of the Shinkansen, Japan's high speed train. From March 2004, two and a half years after the kick off, Suica got a new dimension. It became usable as money in nearly 200 shops at 64 stations. A year later, this number had risen to over a 1000. Also, shops outside the direct station areas had joined the service (Mizutani, 2007). The step to e-money, as RFID enabled cash cards are referred to in Japan, was an important one for JR East. The goal to make Suica a platform for other kinds of payment than just for train fares was first made explicit in JR East's 2001 annual report (JR East, 2002). Also in 2004, JR East's sister company JR West launched ICOCA. ICOCA is technically identical to Suica and the two cards can be used on each others network.

Starting from the first quarter of 2005, Suica could be used to purchase a first class ticket. At a machine on the platform one enters a destination, touches the embedded reader briefly with the Suica card and pays the fee. This information is then loaded on the Suica. On board, upon having found a seat, the Suica is held to a reader over the seats. There, a light goes from red to green. This way, the ticket inspector knows that the seat is paid for and that the traveller needs not be disturbed. In January 2006, Mobile Suica was launched: Suica on your mobile phone. JR East had big expectations for this. The first year however, the number of people signing up was disappointing. 13 Months after introduction, 350.000 people had registered an account. That was a mere third of what JR East had expected beforehand. (Balaban, 2007). This disappointing figure had two possible reasons. First, the service was originally only available for people with a View card, JR East's own credit card. After this first year, Mobile Suica membership has been opened up to people that carry other major (international) credit cards. Another problem is that potential user have to download the required software on their mobile phone themselves. The used to be a complicated affair, taking up to an hour. JR East has reduced this to a process taking roughly ten minutes. Ever since these obstacles have been scaled down, the number of new registrations a month has doubled (Mizutani, 2007).

Perhaps the biggest milestone in the (short) history of Suica has been the introduction of

Pasmo. 101 Public transport providers in the Tokyo metropolitan area (train, subways and buses) launched their answer to Suica on March 18th, 2007. Pasmo shares the ticketing and e-money functions with Suica. The two systems are completely interoperable. The Pasmo group had worked together for some time already, under the name Passnet, so users could travel their collective network with a single ticket. The launch of Pasmo considerably enlarged the reach of Suica. And at that, not just the reach in public transport. Many shops in and around the stations of members of the Pasmo group (like JR East, these companies in general double as real estate owners) installed a Pasmo-reader to accept shop transactions. Suica can also be used here. JR East supplied the technology to the Pasmo group free of charge. But from every Pasmo transaction in a shop, a few Yen find their way to the coffers of JR East. The exact amount or percentage is a closely guarded secret (Nikkei, 2007; Mizutani, 2007). In the meantime, Suica can be used at 1739 stations and one can pay with it in 13.000 shops (Mizutani, 2007).

Still, some institutional problems occurred in extending the functionality of Suica as a micro payment system. Since the year 2000, many smart cards with perform either as an prepaid debit card or a postpaid bankcard have sprung up. With the introduction of an e-money function in 2004, Suica has become one of them. But there is no common standard for these applications. While all of these systems rely on the same chip - Sony's FeliCa - they are on the whole not compatible. The hardware in the reader-writer differs from system to system. Some, like Suica, are built for speed while others are built for optimum security. Today, some ten different FeliCa based e-money systems exist of which only a few work on other platforms than their own. As major chains of retailers discover the advantages of starting a smart card payment service, with inclusion of a loyalty card, consumer confusion may arise. A growing counter trend is the number of reader-writer developers that offer multi-platform readers. However, it remains to be seen whether retailers will allow competitor's smart cards to settle their clients' bills. While so far, the use of e-money continues to incline rapidly, newspapers are sceptical on the effect of the lack of standardisation on the adoption of e-money and similar systems (Nikkei March 28th, 2007; Nikkei, April 26th 2007; Nikkei, April 30th 2007).

Travellers embracing the penguin and robot

Suica has been very popular since it started in November 2001. After a month time, more than a million and a half cards had been sold. After half a year, that figure had risen to 4,5 million. And, as mentioned before, after 5,5 years, JR East had sold over 20 million cards (Mizutani, 2007). But what do these figures mean? At first, we will mention two cultural traits that may have helped the adoption of Suica considerably. After that, there are some traits of the Suica system that have helped its spread. Recall that the Japanese like to consume and adore gadgets. Collectibles are immensely popular. This trait became very visible during the introduction of Pasmo, in March 2007. JR East and the Pasmo group had printed 110.000 commemorative cards to celebrate the launch. This card portrayed the cute mascots of both brands: Suica's penguin and Pasmo's pink robot. All 110.000 were sold out after three hours (Kitanishi, 2007). The one-million mark, that Suica hit after roughly a month, took Pasmo only four days to reach. And what's more: acquiring a Pasmo card became a reason for travelling to Tokyo. Domestic tourists planned a trip to the capital so that they too would have a Pasmo (which wouldn't work in their home town) (Japan Times, 2007).

The other trait that many (Japanese) people we spoke to attributed themselves, is valuing convenience. When products or services are seen as convenient, companies tend to do well. The system of *convenience stores* is well established and even better spread throughout Japan, and many firms use the term "convenience" in their advertising. Suica and Pasmo have both proved to be a convenient system for their users: the need to queue up and buy tickets has been reduced, as has the need to take your ticket from your wallet and feed it through the machine. Closely connected to this high appreciation of convenience is is the value that the Japanese place in product reliability. A malfunctioning product may seriously harm the producer's image and will greatly hamper the product's adoption.

Besides answering to the needs and likes of their customers, there are some traits to the Suica (and therefore, Pasmo) system that help explain it's popularity. Compared to European

RFID public transport cards, it has proved very reliable. Big technical malfunctions have yet to occur and the extensive field testing had ensured that the system was well developed when introduced. A visit to the National Consumer Affairs Centre revealed that of 1.1 million complaints that they received in 2006, only 93 were related to IC cards (Okunishi, 2007). That equals to less than 0,01 percent of total complaints. Note that this is the number of complaints relating to IC cards in general, not only Suica. In all, less than a hundred annual complaints in a system with more than 10 million daily uses, is fairly slim. Another aspect of the Suica system that helped its adoption is the presence of railway staff at the ticket gates. Wherever you go by way of Japanese public transport, at all ticket gates there is someone present to help. Also, when using the ticket vending machines, human support is never far away when it is needed. This continued human presence reduces any fear or mistrust that potential users may have when choosing to adopt a new technology.

Acquiring Suica has a very low threshold. Contrary to Europe, where a personalised system seems to become the norm (Van 't Hof, 2007), Suica became popular as an anonymous card. One steps up to a vending machine, inserts 2500 Yen (roughly 15 Euro) and get a Suica with 2000 Yen credit. The 500 Yen serves as a deposit and is refunded when the card is handed in at any station. When using Mobile Suica or View Suica, one does have to create a personal account at JR East (as your mobile phone or credit card will be used). Furthermore, there has never been pressure to phase out the older ticketing styles. In some instances firms announce that the new system will soon be the only one. Thus, users are forced to either adopt the new system or refrain from using it altogether. This may create a sense of resentment with users, resulting in slower adoption. The Dutch public transport company RET for example, which operates the bus and subway system in Rotterdam, met a lot of resistance when they announced making the current ticket system, the *strippenkaart,* redundant as soon as the new RFID card is introduced (Verlaan, 2007). In case of Suica, no such plans are apparent. On the contrary, JR East successfully manages to get by with at least four different ticketing systems, of which Suica and the older magnetic tickets are only two.

Managing an enriched travellers ID

So how do these travellers, interacting with the SUICA system, define what is known and not known about them and how this relates to the information known or not known to the persons maintaining the system? In principle, SUICA users can remain anonymous and most of them do. Identity Management is in that sense not more than defining one self as a paying traveller. Perhaps with one issue on the side: fear of identity theft and e-pickpocketing. While no problems have occurred as of yet, data skimming is something that users do worry about (Nakanishi, December 20th 2006). Recall that prof. Kimura showed Japanese not to be a very trusting people. This may go some way in explaining the relative small number of personalised Suica account.

In theory, even the use of an anonymous cards can build up a rich identity once travel and consumption data are combined in a marketing profile. Offers and discounts can be set up on the basis of these profiles, leading to either aggressive marketing, or unfair price differentiation. Still, we did not find any proof for this kind of use. As was stated by the National Consumer Affairs Centre there were a few complaints on SUICA, but none of them involved marketing. So then, what kind of personal information do travellers disclose with using SUICA and what do the transport companies do with it?

Suica employs a layered, centralised data storage system. Every Suica card (or Mobile Suica account) sold, has a unique number, on the basis of which a portfolio with the records of the use history of the last 26 weeks is kept. This layered system has a number of levels on which the data are stored. The first step is the card itself. The data on the last twenty transactions are stored on the FeliCa chip. This data are also accessible to users. At terminals next to the ticket-vending machines in the stations, users can retrieve the information stored on the card. The ticketing gates at the station store the data on every transaction that they carry out. These data are stored for a maximum of three days. The gates are, in turn, connected to the station's local network. At the central server of the station, the data are cached for two weeks.

The station database then sends its contents to JR East's central database at regular intervals, where all data are simultaneously stored on to different servers for reliability purposes. Since March 2007, there is one layer above this still: the *mutual use centre* that JR East maintains together with the Pasmo group. The function of the mutual use centre primarily is not to store the data, but to ensure that all payments over the two systems end up where they should (Mizutani, 2007).

This layered approach to data storage has two reasons. First of all, it's a question of speed. If the transaction should be stored centrally in real time, precious time is lost. Especially during rush hour, when hundreds of thousands of transactions have to be completed every minute. The second reason is reliability. Should a link break somewhere in the chain, the system has to keep functioning to prevent chaos. A big reason for this fear are earthquakes. Japan, being located on a tectonic fault line, regularly experiences earthquakes that can be very strong. This causes many problems and disruptions, amongst which broken data cables. Thus, creating a layered system that caches the data at different places makes for a system more resilient to disruptions.

The majority of Suica users have bought an anonymous version of Suica. One buys a card from a vending machine and uses it, without ever trading in personal data. While the newer forms of Suica, like View Suica or mobile Suica do require a personal application, the majority of Suica accounts in existence are anonymous. Of the more than twenty million accounts, only three million are personalised (Mizutani, 2007). Of course, when buying an anonymous Suica card from a vending machine, no personal data are involved. However, when signing up for a View Suica card (combining Suica with JR Easts own credit card) or a mobile Suica account, one does so on a personalised basis. As one primarily applies for the credit card, this is quite normal. We have applied for both the personalised types of Suica. When signing up for the View credit card, JR East does require a lot of information. Not only does application require filling out address information, the applicant also has to state where he or she works, what his/her status is within the company, how long one has worked for this company and what one earns on a monthly basis. Besides, one has to fill out if one is in debt and if so, for how much. How JR East uses this data to reach a decision on issuing a credit card, is unknown to us.

In signing up for mobile Suica, things go somewhat differently. As this account can be linked to an existing credit card, questions on income are no longer relevant, and no longer asked. Address details are required, as are name, age and sex. What is striking to see, is the amount of explicit opt-in requests. On multiple points in the registration process, the user is requested to confirm his/her consent that JR East does have access to the personal data provided. This happened quite explicitly, so that users will have a very good idea about their relationship with JR East. During the process, there were a total of three opt-in points. The first occurred upon entering one's personal data (address, mobile e-mail, name, age and sex). The applicant is asked to consent to JR East logging these data in their administration. Second time is when entering the details of one's credit account. This is done optionally, if users want to charge their mobile Suica over the Internet, using their credit card. Users are requested to consent to JR East contacting the credit card issuing bank to confirm these details. The third opt-in is one on information feedback. Users may choose to receive information on JR East and mobile Suica through e-mail. In all, JR East is quite thorough in informing their clients on the handling and use of personal data.

The sheer wealth of data that the Suica database represented, did not go unnoticed for long at the marketing department of JR East. In 2003 and 2004, a number of articles appear in Japanese transport magazines about the possibilities for personalised marketing in the new era. JR East was riding the wave of IT-enabled innovation and used the concept of Ubiquitous Computing to think about the station of tomorrow and Suica's role in it. (Egami, 2003; Nakagawa 2004) In these articles, the authors explore the possibility for marketing tailored to the clients' personal profile. They speculate on the possibilities of personalised offers on the basis of this client's history (that can be derived from his Suica account). In practise, these plans have not amounted to much. On the contrary, JR East tells us expressly not to plan on using the Suica-databases for marketing purposes anytime soon. Partly, this can be explained by the effects of promulgating a new law on personal data protection in 2003. As

we've mentioned in the preceding chapter, this law has caused some unease in Japan with people fearing misuse of their personal data even while in practise, there does not seem an urgent need to do so. In extension to this, JR East fears a scandal if users feel that JR East is misusing their data, whether justified or not. JR East therefore denies to use Suica generated data for personal marketing anytime soon (Mizutani, 2007).

JR East's marketing division wasn't the only one to notice the rich profile that are created by Suica. So did the Tokyo Metropolitan Police Department. And apparently, they had less qualms to use the Suica database. While no data are available on Suica-data use by the Tokyo Police and other government agencies, both JR East and the Police Department acknowledge that it happens. When asked, JR East's spokesperson was reluctant to share any kind of quantification on how often the police had requested data "Yes, it happens, sometimes." "Could you be more specific?" "Well, it happens sometimes." (Mizutani, 2007) Perhaps more tellingly was the nonchalant answer by the spokesman of the Tokyo Metropolitan Police. He told us that it is just another means of collecting data in a criminal investigation. That they didn't retain the data on how often they requested JR East for their cooperation. That it would be best to pose this question to JR East...

The only service for which JR East uses Suica for marketing, is SuiPo. SuiPo is a conjunction of Suica Poster. In six of the bigger stations in downtown Tokyo, a poster wall can be found with Suica readers attached to it. When one touches the reader with your Suica or ones Suica enabled mobile phone, one receives an e-mail to register for this service. When one uses a Suica card, one first needs to register an account and enter a mobile e-mail address. Then, after signing up, one receives an e-mail with a coupon that gives a reduction on the price of the product advertised. But only when requested by the user, after touching the Suica reader. Furthermore, the offer has in no way been adjusted to fit the profile of the current user. Suica not being used for large scale marketing efforts can seem odd, considering the Japanese advertising practise. On every corner, billboard and neon signs come at you, screaming. In busy shopping areas, young women in miniskirts are promoting the newest models in mobile communication through a hefty sound system. In that sense, Suica based marketing is an island of calm in a sea of multi sensory impulses.

5. Next steps in convergence and ubiquity

Although impressive in scale, success and functionality, SUICA is just one among many common examples of RFID and Identity Management we can observe in Europe too. In this chapter we will go to the forefront of developments: the convergence of RFID, Internet and mobile telephony and putting the reader in the hands of the users. In these socio-technical developments, we can observe an evolution in Identity Management, Japanese style. It's not efficiency and marketing versus privacy issues that set the agenda, but rather convenience and control to achieve harmony (wa) and peace of mind (anshin). We will first describe the FeliCa system for uploading smart card applications onto an Internet enabled mobile phone. Then, with the Children Safety Service and the Ubiquitous Communicator it's not the maintainer of the RFID environment holding the reader, but the customers themselves. These two developments put Identity Management in a different perspective. The first because it goes much further in enriching user profiles, the second for reversing the relationship between reading RFID and being read.

Mobile FeliCa: adding a screen and Internet to a smart card

Mobile FeliCa in the name of an RFID chip embedded in Internet enabled mobile phone.
The FeliCa system consists of an Internet enabled phone with an incorporated RFID chip. The services used most are loyalty cards and e-money systems that were previously offered on smart cards. When considering how people manage their identity in a Ubiquitous Network Society, this is the next step. People carrying a smart card have to move between fixed nodes in the network with their card (taking your Suica from ticket gate to top-up machine) in exchange for services (train rides). So you get the services, as long as you actively approach the nodes. Incorporating the same functions in a mobile phone adds the power of Internet and a screen to these services. Take the case of Suica on your mobile phone: users still have to touch the reader-writer in the ticket gate with your phone, but adding Internet and the little screen to the equation opens new paths for information provision and added services.

The first RFID-equipped phones appeared on the market in 2004. The RFID chip that operates on Mobile Phones in Japan is a member of the FeliCa family, the same chip that Japanese proximity cards rely on. Sony started the development of its FeliCa platform back in 1988, assumingly in close conjunction with JR East. At first, it had been developed as a chip for proximity cards only: the contactless smart cards. It probably will not have taken long for Sony to realise that adapting FeliCa to fit in mobile phones might make an interesting business proposition. Work started and in 2004 Sony and NTT DoCoMo, Japan's largest mobile carrier, set up a joint venture with the name FeliCa Networks. The mission of this new firm was multifold. First of all, FeliCa Networks developed the new generations of Mobile FeliCa chips. Secondly, they created the FeliCa operating system and the middleware specifications to ensure that the FeliCa chip and the mobile handsets would understand one another. Thirdly, FeliCa Networks maintains and manages all the data traffic and data storage generated by people using their Mobile FeliCa enabled applications. In that sense, FeliCa Networks is a full-service company (Ogawa, Maruko, 2007). Firms approach it when they want to offer a service over Mobile FeliCa, develop the content and leave the infrastructure related issues like data management and storage with FeliCa Networks.

The market for mobile phones and their operation functions quite differently in Japan compared to the one in Europe. First of all, there are only three mobile carriers, for a market of nearly 130 million people. Of these three firms, NTT DoCoMo is the dominant player, with a market share of roughly 57% in 2006. KDDI and Softbank divide up the rest of this market, with a 25% share for KDDI and the remaining 18% for SoftBank (FeliCa Networks, 2007). These mobile carriers, and NTT DoCoMo in particular, are very actively involved in R&D for developing handset technology, handset content and network technology. In contrast to Europe, where handset manufacturers like Nokia and Siemens more or less dictate what services the mobile carriers can offer, Japanese carriers send the manufacturers a list of

features and specifications that the new handsets have to offer.This helps explain why NTT DoCoMo has had such an active involvement in the development of Mobile FeliCa.

NTT called the RFID enabled phone *osaifu keitai*, Japanese for *wallet phone*. This name has since then been adopted to signify that a handset is Mobile FeliCa equipped. In 2005, both the other carriers accepted the standards drawn up by FeliCa Networks and started including the chips in their handsets. At the end of 2005, the chip was included in 10 million handsets. In March 2007 this number had expanded to 30 million handsets were equipped with it. FeliCa Networks estimates that the chip is built in in roughly 80% of the new handsets. Total sales volumes for FeliCa had topped 200 million in March 2007, with 160 million chips for use in proximity cards and 40 million for use in mobile telephones (Sony, 2007).

Osaifu keitai as a knot in an accelerating currency flow

While little data is available about the actual number of people that use applications enabled by Mobile FeliCa, general manager of the Planning Department Shusaku Maruko estimates that with ten million users, there will be a critical mass for Mobile FeliCa applications to speed up adoption. If the current trend continues, this figure will be reached before the end of 2007. The most popular applications are Edy (an e-money system), iD (a credit payment system by NTT DoCoMo), and loyalty cards for Coca Cola and airline ANA (FeliCa Networks, 2007). We observed that the most popular applications are without exception services that were available already through a proximity card. Building on what consumers know facilitates the adoption of Mobile FeliCa. In the case of Edy, users tend to spend more with their *osaifu keitai* then they used to with their proximity card. Per transaction with Edy, the average amount spent rose from 500 Yen to 630 Yen (over 20%). Furthermore, the average amount by which users topped up their stored credit rose simultaneously from 2900 Yen to 4200 Yen.

This rise may have at least two explanations. First is that the early adopter of this mobile payment scheme are mainly young male adults that are well off, while the card variety of Edy is embedded much broader amongst different user groups. It is likely that these young urban adults like spending. The second reason could be complimentary to the first. Charging one's account with an e-money application on a mobile phone is mostly done via mobile Internet, with a visit to Edy's Internet site to confirm a transaction from your credit card to your Edy account. With the card variety, many people rely on wall-bound terminals in which they insert cash to add value to their account. This ability to top up one's account with the press of a few buttons, and being able to do so anywhere may well lead to a lower awareness of how much money is actually being spent. Consumer behaviour with the *osaifu keitai* thus makes starting an application on it an interesting proposition for firms. When companies enter into a business agreement with FeliCa Networks, they pay a licencing fee for making use of the Mobile FeliCa technology and infrastructure. Furthermore, they pay a percentage of every transaction that is carried out using Mobile FeliCa. FeliCa Networks has no comment on the amount of money paid for both the licence and the per-transaction fee (Ogawa, 2007).

The young generation in Japan has, already before the arrival of the *osaifu keitai*, been avid consumers over the mobile phone. According to a survey by the Ministry of Internal Affairs and Communications, quoted by Japan's leading newspaper Nikkei, the mobile phone shopping and paid download market was valued at 722,4 billion Yen in 2005. (Nikkei 2007) At the exchange rates of 140 Yen per Euro of that time, that amounts to approximately 5,2 billion Euro. Much of these purchases, which are done on line through using Internet on the mobile phone, are done during the long commutes by train that most Japanese take every day. Making a phone call on the (crowded) trains in Japan is considered taboo and therefore hardly ever occures. In general, it is safe to say that the Japanese view their mobile much more as a multi-service platform as Europeans do. Mobile Internet, at reasonable speed, is used by two thirds of phone users. New types of services, like GPS tracking for children's phones, are introduced on a regular basis. Since a lot of people in Japan are accustomed to using their mobile phone, we assume that adopting the *osaifu keitai* may not be such a big step. Just a slightly different way of using your mobile, when people are already used to interfacing with it in different ways.

Payment schemes aren't the only services that use Mobile FeliCa as a platform. In March 2007, there were approximately 70 different services offered over the *osaifu keitai*. These services can be divided into five categories: finance and payment, transportation, entertainment (mostly ticketing, for example with baseball club SoftBank Hawks), loyalty cards and retail promotion and finally access control. Although not meant a such, these applications could stimulate shadow economy through customer loyalty systems that are so common in Japan and are ever more popular when they are so conveniently offered using RFID. Most major brands of soft drinks, banks, convenience stores or public transport offer a reward to people making regular purchases. This is usually done in the following way: for every hundred Yen you spend, you receive 2 Yen of (virtual) money that you can use for the next purchase in the same store or chain. Sometimes, these schemes are interlinked. For example, many Japanese youngster start saving up for an JAL airline ticket to the States or Europe just by drinking Coke at school. These interlinkages are becoming ever easier to realise now that all these applications are loaded onto one single device (Maruko, 2007).

This development raises an interesting question. Namely: how to deal with e-money in charting and controlling money reserves? So far, the financial authorities in Japan do not monitor the flows of e-money as such. It can be reconstructed by checking the administration of the e-money issuers. To keep these flows within the sight of the financial authorities, every transaction with e-money must occur through the network of the issuer, even when that is technologically cumbersome. The Japanese authorities have indicated that so far, it does not foresee having to change its policy on e-money. However, the situation will be monitored to prevent a shadow economy from emerging (Taku Iwaki, 2007).

The *osaifu keitai* as an Identity Management tool

When moving from smart cards to the mobile phone, nearly all services become personalised by default. This is quite a difference as users now have to sign up personally, often stating name and giving either their mobile number or their mobile e-mail to the service provider. Most smart cards offer an anonymous alternative. But users get more information, too. Transaction histories are stored on the phone and often, supporting services are offered through mobile Internet. For example, topping up one's credit on a mobile application of e-money. Or reserving a first class ticket for train through Internet with mobile Suica. Meanwhile, information on ones account, offers and services can be communicated through the screen on the mobile. Compared to proximity cards, RFID enabled phones provide much opportunities for Identity Management. It builds up a much richer user-identity, which can be managed from the side of both provider and user through a wearable interface.

The *osaifu keitai* as an Identity Management tool is taken even a step further with the introduction of a second version of the Mobile FeliCa chip. The new version has 16 kB of internal memory, compared to 5 kB earlier. This enables users to install three times as many applications as the original ten. There's another new feature included in the newer chip that is of interest: Limited read/write capabilities. When two chips are with a 3 centimetre range of one another, they can exchange data at 212 kbps. Fast enough for exchanging agenda-items, pictures or ring tones from one phone to another. This new service has been introduced in spring 2007, under the name *Touch Message*. Technically, this enables users to exchange everything on their mobile, even their stored credit in their electronic purse. However, it can be used only to exchange photo's and agenda items at the moment. The inclusion of a read-write function in the Mobile FeliCa chip is an interesting development. Giving users the possibility to exchange information with other Mobile FeliCa chips diffuses the traditional boundary between RFID tags and their readers. This potentially puts users in the centre of RFID enabled communication and services, where they, and not the service providers, determine when to share what kinds of information. While at the moment it is only applied in very basic functions, placing the reader in the hands of users is already implemented with the following two applications.

Touch Message diffuses the commonly held disticntion between RFID tag and RFID reader. Instead of being just a tag to be scanned by readers in the environment, with Mobile FeliCa, phones are showing characteristics of readers themselves. Hitachi, a large Japanese

electronics manufacturer, too, has been developing an RFID reader for the mobile phone. As the mobile FeliCa tag only operates on the 13,56 MHz frequency, there is still room for readers with other frequencies to be included in the mobile phone. Hitachi has announced that it will launch a mobile phone with an RFID reader module operating at 2,45 GHz, which is the frequency of choice for many RFID applications as read range and data transfer speed are quite high (Imura, 2007).

Reading Ubiquitous Tokyo

The Tokyo-based Ubiquitous Networking Laboratory and its projects deserve special attention in this chapter. As we mentioned in chapter 3, prof. Ken Sakamura is considered to be one of the founders of the Ubiquitous Network Society concept. Since it's establishment in 2002, the Ubiquitous Networking Laboratory has aimed at creating a system of tags, communication protocols and standards and network infrastructure to create their vision of the Ubiquitous Network Society: a tagged environment with users carrying readers through it. This system has over the years been tested for a number of applications such as food traceability, as an aid in medicine distribution and to help the visually impaired navigate on the street. Remember that most of the projects that the u-code system is used in, are still in the phase of feasibility studies and pilots. However, as we will see, the first real applications are now emerging.

Conceptually the most interesting pilot the the UNL is involved in, is the Tokyo Ubiquitous Technology Project. This is a four year project commissioned by the the Tokyo Metropolitan Government in which the u-code system is tested in public space on quite a large scale. The Tokyo Metropolitan Government values this project as a way to promote Tokyo as candidate for the 2016 Olympics. Tokyo wishes to set itself apart from competing cities by reinforcing its high-tech image and "presenting to the world a model 21st century city" (Tokyo 2016 Olympic Games Bid Promotion Office, 2006). As part of this goal, the Promotion Office specifically mentions ubiquitous technology as one of the fields of "Japan's highly regarded science and technology" that will be important part of the promotion campaign. This was, for the UNL, a very fortunate development.

The project consists of a number of pilots in which the u-code system is tested for different urban goals. From January through March 2007 an area in Tokyo's luxurious shopping district Ginza was fitted with different kinds of passive and active RFID tags. During these three months, a total of 1500 people participated in the pilot. They received a Ubiquitous Communicator and were asked to explore the neighbourhood with it. (Foreign Press Centre Japan, 2007) While the UNL was responsible for the technical infrastructure and the operation of the database, the content was provided by the participants in the city. Shop owners could show their menu or offer a discount through the UC. The local government of Chuo-ku, the district in Tokyo that Ginza is part of, was responsible for the route information and touristic tidbits. The content was presented to users in different forms: maps, written texts, spoken word and short movies (Sakamura, 2007).

Users browse through the streets as if they were surfing the internet. Active and passive RFID tags were placed on lampposts, on the ceiling of a subway station, near sites of historical interest and in shop windows. The tags are recognisable by the bright yellow u-code logo. Approaching a tag is as if clicking on an icon of a web page and access information on routes and addresses, shop information, touristic information and timetables for public transport, depending on which tag they approached. Most information was accessible through passive tags, which requires users to hold the UC very close to it. Such was the case for accessing route information, touristic information and most info on stores. Here too, travel and spending profiles emerge which could lead to identity management issues. While in theory the user should be in control of the flow of personalised data, some stores were targeting potential customers through active tags. This means that it is picked up by the UC over a longer distance, and thus without any effort on the part of the user. Some users did complain about this unrequested information, says the Nikkei newspaper. (Nikkei, April 2nd 2007) While moving to a tag might be seen as a form of consent, information from an active tag arrives without such an act of consent. Or to elaborate on the Internet analogy: ubiquitous spam.

On the whole, the people participating in this pilot reacted positively. As might be expected, young people were more enthusiastic than older people about its functions. Japanese users were most interested in info on participating stores and other information on what could be done in the city. Foreign users were quite happy with the navigation information and the timetables for the subway. There were some technical problems, though. While the communication between tag and UC worked fine, retrieving information from the databases and downloading content sometimes went slowly. Professor Sakamura explained this was most likely the result of illegal broadcasting equipment in trucks and taxis. These illegally used the same frequency as the W-lan function of the UC relied on. (Sakamura, June 2006) Prof. Sakamura estimates that it will take less than four years to introduce the u-code system in similar project on a commercial basis. The technology is ready for it, but the infrastructure still has to be built. Also, if the u-code system, will be used on such a scale in the public domain with so many participants, an organisational model will need to be developed in which responsibilities and duties are clearly defined (Sakamura, 2007).

On a smaller scale, commercial applications of the u-code system are starting to pop up. June 2007 saw the launch of the Ubiquitous Art Tour. Throughout Tokyo Midtown, a large new shopping and leisure mall in the centre of Tokyo, there is a permanent sculpture exhibition. These works of art are part of the public space. For 700 Yen (about 4,50 Euro) one can rent a UC that will act as a tour guide. Active RFID tags and Infrared beacons have been placed along the route and will trigger the UC to show a picture of the space ahead of you on which an arrow shows the way you should go. A voice (the service is available in Japanese, English, Korean and Chinese) tells you where to go at the same time. When arriving at a piece of art, the UC is triggered to offer the user information about it, both in written text, spoken word or in video. Contrary to the Ginza pilot, the tags have been fitted very inconspicuously so that people will not be distracted when they are browsing the artworks.

The vision behind Sakamura's ucode system of which the Ubiquitous Art Tour and the Tokyo Ubiquitous Technology Project are examples, is an open system where everyone carrying a reader can get information about all things tagged: route information, information on train tables, the location of public restrooms and the sales on offer in shops. Such a vision requires people to have a reader like the Ubiquitous Communicator with them at all times. This may be asking a lot of people, realises the Ubiquitous Networking Laboratory. There have been plans to include telephony, for example through Voice over IP on the UC and thus confront the telecom operators heads on. The Ministry of Internal Affairs and Comminucations tells us, though, that the UNL have decided not to do so and find niches for the use of the UC. For even if the vision of one large, open system in public space where everything is tagged and everyone carrying a UC may not make it, there is still plenty of opportunity for it in smaller, closed systems like the Ubiquitous Art Tour.

As the mobile phone in Japan is an object much used in Japan, not only for voice communications but also for internet access, we feel that the mobile phone will play a key part in realizing this vision. The mobile phone in Japan is an object in which many applications, users and producers interact. The dominant firm in Japan in the field of mobile communications is NTT DoCoMo. They play an active part in developing network technologies that will help enabling the Ubiquitous Networking Society. I-mode, high speed internet for mobile phones was developed by this firm and is quite popular in Japan. But the development process of faster and more secure data transfer continues. And, if the current trend is anything to go on, so will adoption of these innovations.

Warabi: children as dots on a map

While in Europe one of the main Identity Management issues concerning RFID is the possibility of being tracked, Japanese users see much advantage in such an application. The last few years have seen the introduction of a markedly different application of RFID than we've seen so far: tracking children. Here we can observe the *anshin* aspect of Identity Management Japanese style. From 2004, we see a number of reports on cases where

schoolchildren are equipped with an RFID tag so that their parent know where they are (see, for example, articles by writer of the "RFID in Japan" blog, Mr. Konomi, a few links to which have been included in the sources) (Konomi 2004, 2005, 2006). Children are equipped with an active RFID tag. The tag broadcasts a signal over a distance of up to 30 metres thanks to an on board battery. This signal is picked up by RFID reader base stations placed in the environment. For example, at the gates of the school they go to, or in a neighbourhood. Parents can view their children's location on a website or receive an e-mail when their children enter school or when their signals are picked up by a specified base station. Thereby the parent gains *anshin* knowing where their child is, while the children gains *anshin* knowing their parents are watching over them.

In July 2007 we visited Warabi, a small community just to the north of Tokyo to investigate the *Kodomo Mimamori Service*, or Children Safety Service. Representatives of technology firm Mitsui Knowledge Solutions (suppliers of the technology) and the Warabi Cable Company (service provider) explained to us how the system works. This service is maintained and operated by the local cable company. Over an area of roughly five square kilometres, 150 RFID readers with a read range of 200 to 300 metres have been installed using the existing cable infrastructure suspended over the road. Participating children are equipped with a tag to hang from their schoolbag of carry in their trousers. The tag broadcasts its unique code once a second, which is picked up by one of the readers. Parents can log onto the services' website and see a map of the area with a blip on the location of their child. Also, they can see where he has been by tracing his movements back in time. Additionally, they receive an e-mail when his or her signal is picked up by up to three pre-designated readers. The service has started commercially in April 2007, as an expanded version of a successful pilot that was carried out in 2006. The original pilot received subsidies from the Ministry of Internal Affairs and Communication as part of the U-Japan policy package. Because of these subsidies, elementary school pupils can subscribe for free until the beginning of this year.

While the service was offered without much promotional efforts, it was quickly adopted: already 800 out of 3500 pupils in the municipality have signed up three months after introduction. A questionnaire among parents proved most parents are willing to pay for this service (Shingo, 2007). When asking whether parents or children regarded the system as perhaps being invasive we were presented with figures on approval. No one objected to the system, while the main motivation for using it was clear: *anshin*. Moreover, during our talks with the representatives it turned out both parents and children were discovering new Identity Management options themselves. Children would be exchanging their log in codes for their identifiers so they can check each other's whereabouts, while parents would be using the system to check if their children remain at home while they went out shopping.

Building on the need for *anshin*, a pilot in a neighbourhood in Yokohama went one step further: adding an panic button to the tag. When a child feels threatened, it presses the button and an adult will come running. These adults are professional security guards and volunteers. There was a big issue with false alarms, though. Over the four months that the pilot was running, there were 53 instances of emergency alarms. All were false. Because these false alarms we so frequent, volunteers eventually took them less serious. Still, more than half of the parents that partook in the pilot were willing to pay a monthly fee of 2000 Yen (roughly 14 Euro) for such a service (Konomi, 2005). Also with other child tracking devices malfunctions defeated the purpose of the RFID systems. According to Kimura, the e-mail function that is supposed to inform parents of their children's safe arrival at school, malfunctioned in certain pilots. This caused mild panic with the parents, who quickly came to rely on the daily e-mail. In general, professor Kimura criticises, there is not enough attention for the side-effects of the introduction of such services. (Kimura, 2007)

In our perception, the popularity of such services is not primarily due to an actual lack of security, but rather with the perception of safety in the public domain. Compared to Europe, Japan has a remarkably low crime rate, while fear for crime is higher in Japan. In the Warabi case for example, the child tracking service was an answer to feeling of insecurity as Warabi has one of the highest crime rates in the country. These rates did not involve a single case of child abduction, but were mainly based on petty crime such as bicycle theft. Our suggestion to

fit the RFID tags into the bicycles instead of being worn by children received not much more than a polite smile. Japanese will go to great length to improve their a*nshin*, a feeling of security and peace of mind, something that needs to be taken into account studying RFID and Identity Management in this Ubiquitous Network Society.

6. Lessons from u-Japan

We started this project under the titel "RFID and mobility in Japan", with the aim to analyse social, legal and ethical aspects of human centric RFID applications in Japan. We soon discovered the implementation of RFID in Japan is part of a much broader vision of a society in which everything is sensored and connected, the Ubiquitous Network Society. This became the new focus of our research and thus was incorporated into the project Public Space 2.0 of the Rathenau Institute, in which we are developing a new paradigm for the information society. In this paradigm, two technological developments - ubiquitous computing and network convergence - are taken as a starting point to analyse how our perception of time and place in cyberspace are changing. The comparability to the Japanese concept of Ubiquitous Network Society was striking. In analysing the social, legal en ethical aspects of this phase in the information society, we take Identity Management as a leading concept. Here too, we found fertile ground in Japan for further research. While in Europe the main Identify Management issues are focused on privacy and personal data protection laws, Japanese Identity Management is more about *wa* (harmony), *rinri* (the way to achieve harmony) and *anshin* (inner peace through external control). Put differently, the Japanese achieve a higher level of order without law.

During our field research in Japan we encountered many applications currently in use, which are in Europe still on the drawing board or in a pilot phase. Public transport cards can be found in some European cities, either in pilot phase or already functioning for a year or two. Main issues here are privacy concerns of travelers being tracked in their movements, low acceptance and transport operators struggling to prove their return on investments. Suica, Japan's major RFID transport card had it start up problems too, but has turned into a succes for quite some years now. Identity Management here is not just about having paid for transport and gaining access accordingly, it's more about the *wa* between a moving group of profiled customers and an omnipresent provider. Either as an anonymous smart card, or as a personalised application on the mobile phone, it provides transport companies new business opportunities on the basis of user identity, while travelers themselves gained new services on the basis of their identity without being overburdened with ubiquitous spam. The way to achieve this is not to force the system upon its users, but aim at convenience (time savings during check in), leaving many alternatives (paper, magnetic cards) open and give the system a human touch through human presence at the turnstiles and ticket machines.

Japan also proved to be a sort of socio-technological laboratory for us to analyse new RFID applications in real life settings. The RFID enabled mobile phone can be seen as a smart card with a screen and internet connection, but it's also a multi service platform which is personalised by default. Here too, we observed a tendency to achieve harmony between user and supplier needs. Suppliers seek to nurture their customers with a broad array of loyalty point schemes based and additional services on costumer profiles. Many if not all of the services provided are ruled by an opt in regime. The users perceive their *osaifu keitai* much more as an Identity Management tool than just a phone, handling their written correspondence and financial administration. We observed a tightening relation between businesses and consumers and an acceleration flow of e-money and saving points. This could lead to government interference, as this holds a potential danger of a shadow economy. Identity Managment on the basis of customer loyalty could then shift towards identifying tax evaders.

Elementary in the Ubiquitous Network Society concept is that the network connects the identity of people and things. So, not just users but the physical environment is being drawn into the Identity Management schemes too. We used the Ubiquitous Communicator which provided us information on the basis of our location and observed this really adds a virtual dimension to the physical space. Although mostly still in a pilot phase, we had some flavours of what it would be like to be surfing through a ubiquitous network as an art lover, tourist or fun shopper. Another application connecting localization to identity is the Children Safety service. Being identified through an active RFID within a network of readers through the town,

the whereabouts of children is monitored by parents and schools. From a European perspective this could be quite invasive to ones privacy, but for the Japanese it's the Anshin that counts.

Viewing these applications together, we can already have a glimpse of what this Ubiquitous Network Society will look like in practice. RFID is likely to converge with the mobile phone and internet. RFID secures the localization of people and things, the mobile phone provides a user friendly interface and transmission and the internet connect it all. The smart cards functions will be elaborated and an RFID reader will be added for reading tags from the environment, just like the Ubiquitous Communicator. Connecting the actions on the spot to the internet, the phone will provide a range of location based services, such as directions, product information, access to buildings, emergency services, identification and the like. The mobile phone thereby becomes the ultimate Identity Management tool for both users and suppliers.

Whether Europe will go in the same direction remains to be seen. Although many applications we have seen in Japan are likely to be introduced on the European market too, many specific traits of Japanese culture that pave the way to adoption. The argument can therefore also be turned around: if Japan will not succeed in becoming a Ubiquitous Network Society, perhaps no one will.

Sources

Publications

Aarts, E. & S. Marzano, 2003, “The New Everyday: Views on Ambient Intelligence” 010 Publishers, Rotterdam

Balaban, D., April 2007, Japan’s Mobile Wallets Fail To Inspire–Yet, http://www.cardtechnology.com/article.html?id=200704131WCTISI9 accessed on May 8th, 2007.

East Japan Railway Company, 2007, JR East & the Suica Project, presentation.

East Japan Railway Company, 2002, Annual Report 2001, Tokyo, Japan.

East Japan Railway Company, Following the track leading to Suica, www.jreast.co.jp/e/development/story/index.html, accessed on April 4th, 2007.

FeliCa Networks, 2007, Introduction of Mobile FeliCa in Japan, presentation.

Gibson, William, 1984 “Neuromancer”

Hayashi Shingo, Warabi Cable Company, July 26th 2007, Children Safety Service, presentation.

Hof, C. van ‘t , 2007, RFID & Identity Management in Everyday Life. Striking the Balance between Coninvience, Choice and Control. Rathenau Isntitute, The Hague

Hofstede, G, 1997, Cultures and organizations: Software of the mind, London: McGraw-Hill.

Imura, R., July 2007, Hitachi Information & Telecommunication Systems, interview.

Kallender, P., March 2005, Japan tightens personal data protection, in: Infoworld.com, http://www.infoworld.com/article/05/03/28/HNjapntightensdataprotection_1.html accessed on April 26th, 2007.

Kameyama, W., June 2007, Ministry of Economy, Trade and Industry, Commerce and Information Policy Bureau, Information Policy Division; interview.

Kitanishi, K., April 17th 2007, Pasmo Card sells out to benefit of Jr East, The Nikkei Financial daily, Tokyo Japan.

Kitano, N., 2007, Animism, Rinri, Modernization; the Base of Japanese Robotics, Tokyo: Waseda University.

Konomi, S., September 25th 2004, Another instance of tracking kids with RFID, http://ubiks.net/local/blog/jmt/archives3/002418.html accessed on June 18 2007

Konomi, S., October 5th 2005, Lessons learned: RFID Kids Tracking, ubiks.net/local/blog/jmt/archives3/004343 accessed on June 18 2007.

Konomi. S., December 17th, 2005 "RFID Watches Over School Kids in Japan", http://ubiks.net/local/blog/jmt/archives3/004559.html accessed on June 18 2007.

Konomi. S., June 26th, 2006, Saitama Schools to Use Active RFID Tags, http://ubiks.net/local/blog/jmt/archives3/005555.html accessed on June 18 2007.

Maruko, S., July 2007, General Manager Planning Department, FeliCa Networks, Interview.

Matsumoto, M. & De Mente, B. L., 2003, Japanese nuance in plain English, Tokyo: Kodansha International.

MIC website on the u-Japan policy package http://www.soumu.go.jp/menu_02/ict/u-japan_en/j_r-menu_u.html, accessed on April 19th, 2007.

Mitsui Knowledge Solution, July 26th 2007, Wink's Kids Tracking Service, presentation.

Mizutani, K., East Japan Railway Company, General Manager Suica Department, June 2007, interview.

Murakami, T., 2000, Ubiquitous Networking: Toward a New Paradigm, NRI paper no. 2, Tokyo: Nomura Research Institute.

Murakami, T., 2004, Ubiquitous Networking: Business Opportunities and Strategic Issues, NRI paper no. 79, Tokyo: Nomura Research Institute.

Murakami, T., 2005, Japan's National IT Strategy and the Ubiquitous Network, NRI paper no. 97, Tokyo: Nomura Research Institute.

Nakamura, F., May 18th 2004, Smart cards in Japan, presentation, http://www.itscanada.ca/standardscommittee/documents/FumihikoNakamura.pdf accessed on April 20th, 2007
Nakanishi, T., December 20th 2006, Spread of "cardless" e-money systems spurs fear of misuse, The Nikkei Financial daily, Tokyo Japan.

Nakazato, G, Ministry of Internal Affairs and Communication, June 2007, interview.

Natsui, T., 2005, Guidelines for Privacy Protection on Electronic Tags of Japan, in: RFID and the construction of Privacy, (eds: Garfinkel, S. & Rosenburg, B.) New York: Addison Wesley pp 507-514.

Natsui, T., May 2007, Meiji University, Faculty of Law, Japan: Tokyo, interview.
Kimura, T., May 2007, University of Tokyo: Department of Cultural Anthropology, Japan: Tokyo, interview.

Ogawa, A., June 2007, Planning Department, FeliCa Networks, Interview.

Okunishi, M., National Consumer Affair Center, July 2007, interview.

Ota, H., June 2007, Hitotsubashi University: International Affairs Department, Japan: Kunitachi, interview.

Sakamura, K., June and July 2007, Ubiquitous Networking Laboratory, interview.

Setsuko Egami, September 2003, Offering Ubiquitous Services, in: Japan Railway & Transport Review, vol 36, pp 37-41.

Setsuko Egami, 2004, For creation of new values in transportation and daily life, in: JR East Technical Review vol. 3, pp 4-8.

Shiibashi, A., September 2002, Introduction and Future Development of Suica Non-contact IC Card Ticketing System, in: Japan Railway & Transport Review vol. 32.

Shiibashi, A., 2005, Suica Technology and strategy for future development, in: JR East Technical Review vol 6, pp 40-49.

Srinivasan, S. 1992, Privacy and data protection in Japan, in: Government Information Quarterly, vol 9, no. 2 pp 121-133, JAI Press.

Srivastava, L. et al., 2005 “The Internet of Things” ITU Report, Geneva

Takeshi Nakagawa, 2004, Creation of services in "Ubiquitous Computing" era, in: JR East Technical Review vol. 3, pp 9-14.

Taku Iwaki, April 28th 2007, Firms woo customers with e-money, Daily Yomiuri, Tokyo Japan.

Tsuji, T., 2006, Next-Generation Ubiquitous Network Strategy, NRI paper no. 104, Tokyo: Nomura Research Institute.

Tsuyoshi Hiramatsu, 1990, The new Japanese act on the protection of personal information by means of computer processing, in: Archiv fur Urheber-, Film-, Funk-, und Theaterrecht, vol 112, p 164.

Uchida, A., July 2007, Ministry of Internal Affairs and Communication, International Economic Affairs Division, interview.

Verlaan, J., September 29th 2007, Ov-chipkaart kampt met tal van gebreken, NRC Handelsblad, Rotterdam, The Netherlands.

Weiser, Mark; Rich Gold and John Seely Brown, 1999. ""The origins of ubiquitous computing research at PARC in the late 1980s"". IBM systems journal 38 (4).

Anonymous publications

Anonymous, July 2005, Personal information protection law Japan, Tokyo: Freshfields Bruckhaus Deringer.

Anonymous, September 2005, Creating the future with Ubiquotous Computing, Ubiquitous Networking Laboratory, web publication, www.ubin.jp/english/yrpunl.pdf, accessed April 16th, 2007.

Anonymous, January 2006, Latest developments in Policies on RFID Tags, Tokyo: Ministry of Economy, Trade and Industry, Information Economy Division.

Anonymous, May 12th 2006, Formulation of the "Fundamental Principles for the Tokyo 2016 Olympic Games", www.metro.tokyo.jp/ENGLISH/TOPICS/2006/ftg5v100.htm, accessed June 5th, 2007.

Anonymous, 2007, 2007 White Paper Information and Communications in Japan, Tokyo: Ministry of Internal Affairs and Communications.

Anonymous, March 2007, Tokyo Ubiquitous Technology Project in Ginza, Foreign Press Center Japan, Tokyo, Japan.

Anonymous, March 1st 2007, FeliCa IC Chip cumulative shipments reach 200 million units, Sony press release.

Anonymous, March 28th 2007, E-money now 3-way contest as seven &I enters the fray, The Nikkei Financial daily, Tokyo Japan.

Anonymous, March 28th 2007, E-fray, Nikkei Weekly, Tokyo Japan.

Anonymous, April 2nd 2007, Ubiquitous technology acts as town guide, Nikkei, Tokyo Japan.

Anonymous, April 12th, 2007, Pasmo fare card selling out too fast, The Japan Times, Tokyo Japan.

Anonymous, April 26th 2007, E-money use grows, but lack of standards a pain for shoppers, The Nikkei Financial daily, Tokyo Japan.

Anonymous, April 30th 2007, E-money soars as retailers, railways climb on board, Nikkei Weekly, Tokyo Japan.

Anonymous, June 4th 2007, Easy-buy Mobile phone shopping luring young customers, Nikkei daily, Tokyo Japan.

Anonymous, June 4th 2007, Cell phones prop up consumption, Nikkei daily, Tokyo Japan.

Anonymous, July 2007, OECD Communications Outlook 2007, Paris: OECD.

Interviews and site visits

In chronological order. Interviews unless mentioned ontherwise

May 25th, 2007 Meiji University: Faculty of Law - Prof. Takato Natsui

May 31th, 2007 University of Tokyo: Faculty of Cultural Anthropology - Prof. Tadamasa Kimura

June 1st, 2007 Ubiquitous Networking Laboratory - Prof. Ken Sakamura
June 1st, 2007 Tokyo Metropolitan Government

June 4th, 2007 Ministry of Economy, Trade and Industry, Commerce and Information Policy Bureau

June 8th, 2007 FeliCa Networks: Planning Department / Business Solution Department

June 11th, 2007 Hitotsubashi University: International Affairs Department - Prof. Hiroshi Ota

June 13th, 2007 Yokosuka Research Park: NTT DoCoMo [site visit]

June 14th, 2007 East Japan Railway Corporation: Suica Department

June 21st, 2007 Ministry of Internal Affairs and Communications: Information Policy Bureau

July 23rd, 2007 Nomura Research Institute - Tadashi Tsuji

July 23rd, 2007 Ubiquitous Networking Laboratory - Prof. Ken Sakamura

July 23rd, 2007 Ubiquitous Art Tour [site visit]

July 24th, 2007 Expert meeting RFID and the Ubiquitous Network Society

July 25th, 2007 NTT DoCoMo [site visit]

July 25th, 2007 FeliCa Networks: Planning Department

July 26th, 2007 National Consumer Affair Centre

July 26th, 2007 Ministry of Internal Affairs and Communication

July 26th, 2007 Warabi Cable Company / Mitsui Knowledge Solutions

July 27th, 2007 Hitachi - Prof. Ryo Imura

July 27th, 2007 University of Tokyo: Faculty of Cultural Anthropology - Prof Tadamasa Kimura / Hitotsubashi Unversity: International Affairs Department - Prof. Hiroshi Ota