October 2003

Trends in the Selection of Automatic Identification Technology in Electronic Commerce Applications

Katina Michael
University of Wollongong, katina@uow.edu.au

Trends in the Selection of Automatic Identification Technology in Electronic Commerce Applications

Abstract

Since the 1970s, automatic identification (auto-ID) technologies have been evolving to revolutionise the way people live and work. Previous research has not addressed auto-ID technological innovation as a field of study, despite its growing importance on consumer, business and government electronic commerce (EC) applications. This paper is specifically concerned with five auto-ID technologies, bar codes, magnetic-stripe card, smart card, biometrics and radiofrequency identification (RF/ID) tags and transponders. Using multiple embedded case studies and applying the fundamental concepts of the systems of innovation (SI) approach, the overall aim is to understand the selection environment of the auto-ID industry. The results show that industry competition encourages the coexistence of numerous auto-ID technologies, dispelling the idea that one superior technology will make all others obsolete. This can be seen by the trends of migration, integration and convergence that are occurring in auto-ID innovation today. The significance of the study rests in its practical contributions. Stakeholders will benefit by becoming more aware of the opportunities in the market for the recombination of one or more auto-ID techniques. Additionally, suppliers of auto-ID system components will understand the new paradigm where various auto-ID firms can share in the same trajectory successfully.

Keywords

automatic identification, selection environment, technological trajectory, convergence, coexistence, RFID, biometrics, bar code, smart card, magnetic-stripe card

Disciplines

Physical Sciences and Mathematics

Publication Details

This book chapter was originally published as: Michael, K, Trends in the selection of automatic identification technology in electronic commerce applications, in N. Cerpa & P. Bro (eds), Building society through e-commerce: e-Government, e-Business and e-Learning, University of Talca, Chile, 2003, 135-152.

Trends in the Selection of Automatic Identification Technology in Electronic Commerce Applications

Katina Michael

University of Wollongong, NSW, Australia
+61-2-42213937
katina@uow.edu.au

Abstract

Since the 1970s, automatic identification (auto-ID) technologies have been evolving to revolutionise the way people live and work. Previous research has not addressed auto-ID technological innovation as a field of study, despite its growing importance on consumer, business and government electronic commerce (EC) applications. This paper is specifically concerned with five auto-ID technologies, bar codes, magnetic-stripe card, smart card, biometrics and radio-frequency identification (RF/ID) tags and transponders. Using multiple embedded case studies and applying the fundamental concepts of the systems of innovation (SI) approach, the overall aim is to understand the selection environment of the auto-ID industry. The results show that industry competition encourages the coexistence of numerous auto-ID technologies, dispelling the idea that one superior technology will make all others obsolete. This can be seen by the trends of migration, integration and convergence that are occurring in auto-ID innovation today. The significance of the study rests in its practical contributions. Stakeholders will benefit by becoming more aware of the opportunities in the market for the recombination of one or more auto-ID techniques. Additionally, suppliers of auto-ID system components will understand the new paradigm where various auto-ID firms can share in the same trajectory successfully.

1. INTRODUCTION

This paper is concerned with automatic identification (auto-ID) technologies which first came to prominence in the early 1970s. As opposed to manual identification, auto-ID is the act of identifying a living or nonliving thing without direct human intervention. From bar codes on supermarket store items, to magnetic-stripe cards allowing the transfer of government benefits to smart cards used in place of cash to purchase goods and services. From fingerprint biometric devices used to bypass immigration officials at airports to RF/ID tags used to monitor low-risk prisoners serving their sentence from home. The traditional problem for stakeholders in the auto-ID market has been one of choice. Particularly for the auto-ID manufacturer, which path to follow has always been linked to the question of the long-term survivability of a given auto-ID device.

Yet, each stakeholder considers the selection environment from a different perspective. For instance, service providers may be interested in the implementation of an auto-ID device that will increase application usage, while consumers may demand a secure method for conducting transactions. In applying the SI concepts to the auto-ID market, the problem of choice is not considered in terms of the production function that Schumpeter and other neo-classical economists had originally helped to establish. Rather, stemming from evolutionary economics, SI considers a pattern of innovation that is evolutionary in nature. The idea that innovation occurs in the auto-ID industry continually searching for an optimal solution is thus challenged. More important is the system of innovation since firms never innovate in isolation, indicating that innovation is driven through the interaction of auto-ID stakeholders. The objective of this paper is to identify the prevalent trends in auto-ID innovation using mini case studies.

2. LITERATURE REVIEW

Almost all previous research in the field of auto-ID has focused only on a single device. Some of the more significant references are cited in table 1 below.

Table 1. Previous Research in Auto-ID Technologies

Auto-ID Technology	Significant Previous Research
Bar code	Grieco et al. 1989; Harmon & Adams 1989; Palmer 1989; Collins & Whipple 1990; Cohen, J. 1994; Pavlidis 1996; Brown 1997; Howlett et al. 1997; LaMoreaux 1998; Albright 1998; Proefke 1998; Moore 1998; McInerney 1998; Johnston & Yap 1998.
Magnetic-stripe cards	Colton & Kraemer 1980; de Bruyne 1990; Naujokas 1989; Harrop 1990; Egner 1991; Troy 1993; Chu 1995; Smith, D. et al. 1996; O'Mahony et al. 1997; Essinger 1999; Crossfield 2001.
Smart cards	Svigals 1987; Bright 1988; Chaum & Schaumuller-Bichl eds. 1989; Hawkes et al. eds. 1990; McCrindle 1990; Cordonnier 1991; Devargas 1992; Bussin 1993; Zoreda & Oton 1994; Conolly 1995; Kaplan 1996; Wolfgang 1996; Hendry 1997; Rankl & Effing 1997; Allen & Barr (eds) 1997; Hamann 1997; Lindley 1997; Elliot & Loebbecke 1998; Turban & McElroy 1998; Blythe & Holland, 1998; Dreifus & Monk 1998; Ferrari et al. 1998.
Biometrics	Goldstein et al. 1971; Mammone & Murley (eds) 1994; Bernier 1995; Carback 1995; Cross & Smith 1995; Cameron et al. 1996; Williams 1996; Fairhurst 1997; Wildes 1997; Jain, A. K. et al. 1997; Campbell 1997; Bigun et al (eds) 1997; Shu & Zhang 1998; Camus et al. 1998; Boves & Os 1998; Jain, A. K. et al. 1999; Gunnerson 1999; Swartz 1999; Jain, L. C. et al. (eds) 1999.
RF/ID Tags & Transponders	Kitsz 1987; Evans 1988; Hewkin 1989; Ames ed. 1990; Styles 1990; Curtis 1992; Goedseels 1992; Shepherd 1992; Haendler & McDaniel 1993; Ollivier 1993; Wouters et al. 1993; Harmelink 1993; Geers 1994; Hind 1994; Wenter 1994; Gerdeman 1995; Brodsky 1995; Geers et al. 1997; Linton 1997; Finkenzeller 1999.

What is surprising to note is that the key concept "automatic identification" has appeared in the titles of only a limited number of publications including: Moran (n.d.), Berge (1987), Sharp (1987), Schwind (1987), Gold (1988), Hewkin (1989), Smith (1990), Adams (1990), Cohen (1994), LaMoreaux (1998), O'Gorman and Pavlidis (1999), and Swartz (1999). This does not mean that the term is unfounded, for it is commonly used within the body of literature, but usually in the context of a single device only. Most recently the term, has been usurped by RF/ID suppliers trying to promote the advantages of transponders over bar codes. What the lack of clarity in the use of the concept signifies is a deficiency in understanding that the various auto-ID techniques belong collectively to a larger auto-ID technology system (TS). This is the critical gap in the literature that this paper aims to fill.

There are four primary works that attempt to cover issues related to auto-ID technologies as a field of study. The first is *Automatic Identification and Data Collection Systems* (Cohen, 1994). While it serves as an excellent overview into the field it fails in terms of its unbalanced focus on bar code technology versus other auto-ID technologies. The second work is by Hewkin (1989), "Future Automatic Identification Technologies", and the third is by Swartz (1999), "The Growing 'MAGIC' of Automatic Identification." These two works, published ten years apart, deal with the need to understand auto-ID innovation, yet neither goes into detail about prevailing trends in the industry at large. Hewkin understands the auto-ID market well and emphasises the need for industry-wide communication flows between the different auto-ID players, irrespective of their product focus. Swartz, on the other hand, who has been able to witness the changes in the industry over the last decade, analyses the most prominent auto-ID technologies and presents a framework for understanding the converging technologies. His insights are very important in that they assist to support the findings of this paper. Finally, one other important contribution, which cannot go without mention, is by Smith (1990) who stipulated the focus of the AIM (automatic identification manufacturers) activity group was more than just bar code. In the context of auto-ID techniques he wrote (p. 52): "[t]he members of AIM collectively cover all the established technologies as well as most of the emerging ones." It should also be noted, that in reviewing literature, the reader should make use of the author's PhD thesis, *The Technological Trajectory of the Automatic Identification Industry* from which this paper was extracted (Michael, 2003b, see especially ch. 7).

3. METHODOLOGY

Five mini-case studies will be presented featuring the most prominent auto-ID technologies used today. These techniques were chosen for their substantial impact on electronic commerce applications between consumers, businesses and government. Each differs in terms of its technical complexity and user requirements. Bar codes are printed labels that use symbologies, magnetic-stripes are usually featured on card technologies, smart cards incorporate integrated circuits (IC), biometrics use personal physical characteristics or traits to authenticate or verify living things, and RF/ID tags allow for contactless communication. The case studies are organised chronologically, dependent on the technology's commercial introduction, in order to highlight particular trends

occurring in the auto-ID industry as they relate to the notion of a selection environment. In each mini-case, one EC application will also be presented as an embedded study. Each technology (i.e. the unit of analysis) is tied to an application (i.e. the sub-unit of analysis). The five application areas relate to manufacturing, financial transactions, telecommunications, government services, and security and monitoring. The case study protocol is centred on three main questions: what is the technology, what is the application, and what is the selection environment for that innovation. The information gathered for the case studies is historical in nature, sourced from a variety of documents and archival records. The cases will be presented in a descriptive manner and the dominant trends and patterns will be interpreted to shed light on the auto-ID selection environment. Using the SI approach, the firm (in this case the auto-ID technology provider), will be considered as the central actor in the innovation process.

4. BAR CODE

Bar codes are the most widely used technology in the auto-ID industry today. Before the bar code, only manual identification techniques existed. Handwritten labels or carbon-copied paper were attached to 'things' needing identification. In 1932 the first study on the automation of supermarket checkout counters was conducted by Wallace Flint and by 1934 a bar code patent describing the use of parallel lines was filed (Palmer, 1995). The first universal product code (UPC) to cross the scanner of a supermarket was in 1974 (Brown, 1997). The UPC is an example of a bar code symbology, made up of a series of dark and light contiguous bars; a language with its own rules that can be translated into ASCII code for unique identification (Collins & Whipple, 1994). The main technical drawback of the bar code is that it cannot be updated once it has been printed.

4.1 Manufacturing

One prominent application of bar codes is in manufacturing, playing an integral role in a company's enterprise resource planning (ERP) system. Specific part types are identified by a bar code and tracked until they are assembled into a finished product then dispatched accordingly. This ensures that the right parts are used for the designated task. Bar code labels on individual packaging items result in goods getting to their correct destinations on time. Such automated manufacturing practices are saving large companies millions of dollars annually. Bar codes can also transmit order information and other data via electronic data interchange (EDI). This allows for international operations worldwide to be linked together. Operations managers now receive timely accurate data and have an ability to exercise a just-in-time (JIT) strategy. Highly automated systems have reduced labour costs and increased productivity. Quick response (QR) and direct store delivery (DSD) practices have also lead to better customer relations.

5. MAGNETIC-STRIPE CARD

Almost simultaneously that the retail industry underwent revolutionary changes with the introduction of bar code, the financial industry adopted magnetic-stripe

card technology. However, the magnetic-stripe card had a more direct and personal impact on the cardholder than bar code. The consumer had to carry the card, use it appropriately, and was liable legally for it in every way. Today, magnetic-stripe cards are still the most widely used card technology in the world (Kaplan, 1996). The strip itself is divided laterally into three distinct tracks, each serving a different function. It is magnetically encoded with a unique identification number that is represented in binary. When the strip is queried, the 1s and 0s are sent to the controller in their native format and converted for visual display into decimal digits. The magnetic-stripe card has several limitations, among which is durability and data capacity. Yet today, it is the problem of multi-million dollar card fraud, stemming from the fact that most magnetic-stripes are skimmable and counterfeitable, that has understandably led the media to cast the technology in a negative light.

5.1 Financial Transactions

A cursory glance at the content of one's wallet will reaffirm why financial services is the main application of magnetic stripe cards. Auto-ID has been responsible for the financial transaction card (FTC) explosion in the form of debit and credit cards that have paved the way for a cashless society. Debit cards give the cardholder access to their savings and cheque account balance, whereas credit cards give the cardholder access to a pre-established line of credit. Debit cards require the cardholder to enter a personal identification number (PIN) at an automatic teller machine (ATM), whereas credit cards only require signature verification at supervised terminals such as at electronic funds transfer at point of sale (EFTPOS). Today, phone and Internet banking practices, as well as online purchases between businesses and consumers (B2C) continue to boost the total value of EC transactions worldwide. However, the overriding sentiment among users of these services is that there must be better security.

6. SMART CARDS

The history of the smart card begins as far back as 1968. By that time magnetic-stripe cards, while not widespread, had been introduced into the market. Momentum from these developments, together with advancements in microchip technology made the smart card a logical progression. Currently, while there is a movement by the market to espouse the technology (especially in Europe), numerous countries continue to adopt magnetic-stripe cards. This phenomenon is contrary to the many advantages the smart card possesses which include multiple applications on a single device, greater storage space, and superior security using encryption algorithms. According to Rankl and Effing (1997) smart cards can be divided into two broad groups: memory cards and microprocessor cards (contact/contactless). In contact smart cards, a power supply requires to have physical contact for data transfer. The tiny gold-plated 6-8 contacts are defined in ISO 7816-2. As a rule, if a contact smart card contains a magnetic-stripe, the contacts and the stripe must never appear on the same side. Each contact plays an important role. Two of the eight contacts have been reserved (C4 and C8) for future functions but the rest serve purposes such as supply voltage (C1), reset (C2), clock (C3), mass (C5), external voltage for programming (C6), and I/O

(C7). Contactless smart cards on the other hand, work on the same technical principles that animal transponder implants do (see section 8 below). While the smart card is a sophisticated auto-ID technology it has been argued that the device is still susceptible to damage, loss and theft.

6.1 Telecommunications

Predictably, prepaid smart cards for public payphones account for the largest segment of the smart card market (Crotch-Harvey, 1996). In 1995, telecommunications-specific smart cards accounted for eighty per cent of the market. The first recognised trial of smart cards for prepaid telephone cards was by the French Post Telephone and Telegraph (PTT) in 1982-83. The French justified the move from coin operated payphones to smart card payphones by highlighting that about fifteen per cent of phone call tariffs were lost as a direct result of telephone charging fraud and coin theft (Svigals, 1987). By 1995 there were a reported 1.5 billion prepaid telephone cards sold, about a quarter of which could be accepted in one fifth of payphones in more than seventy countries (Lutz, 1997). Smart cards in the telecommunications sector are also used as SIM (subscriber identity module) cards in GSM (global system for mobiles) handsets or PDAs (personal digital assistants) to enable a plethora of mobile commerce (m-commerce) applications. NTT DoCoMo's i-Mode and c-Mode continue to push the bounds of the wireless Internet, allowing the user to do almost anything that the fixed Internet offers, such as book airline tickets, buy and sell shares on the stock market, play their favourite games, check the latest weather forecasts, shop and browse for products, play government-approved lotteries, download images and even use the company's intranet (see figure 1). Smart cards can even be inserted into cable television (CATV) set-top boxes to allow for home shopping, video-on-demand (VoD) or pay-per-view (PPV) screening.

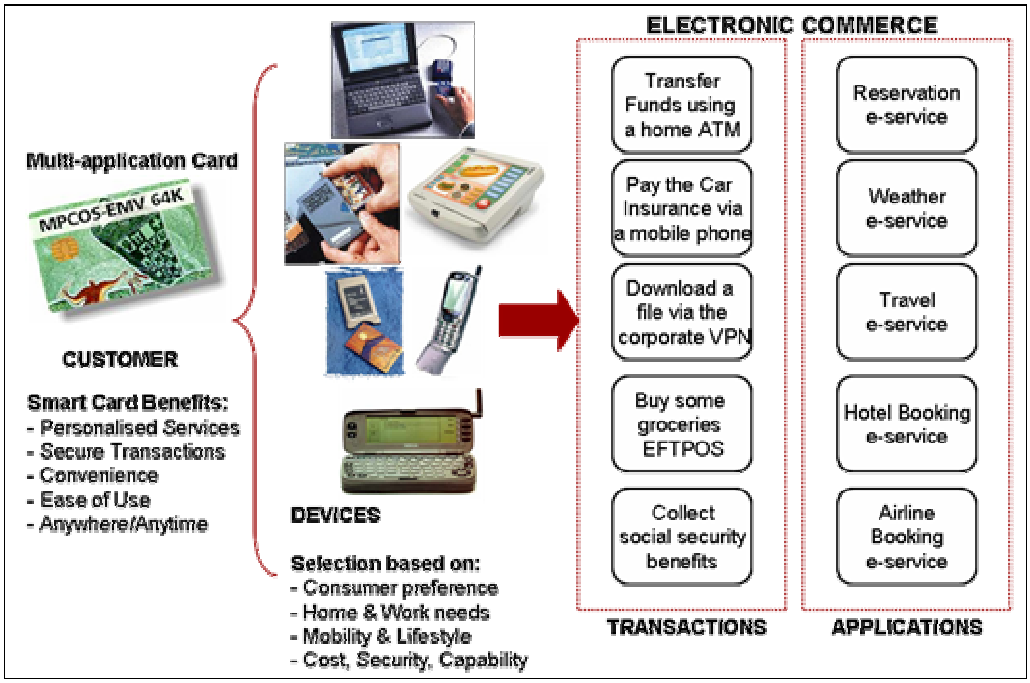


Figure 1. Multi-application Smart Cards in Telecommunications

7. BIOMETRICS

Biometrics is not only considered by many to be the most secure way to identify an individual but also a more convenient technique whereby the individual does not necessarily have to carry an additional device, such as a card. Unique identification, as Zoreda and Oton (1994) point out, is only a matter of measuring a permanent biological trait whose variability exceeds the population size where it will be applied. As a general rule however, the trait must satisfy the requirements of universality, uniqueness, permanence and collectability (Jain et al., 1997). Some of the most popular biometric techniques include: face, fingerprint, hand geometry, iris, retinal pattern, signature, voice print, and DNA. The enrollee's physical characteristic is stored in the form of a template (known as a reference value), and is compared against stored samples for verification. False accept rates (FAR) and false reject rates (FRR) determine the applicability of a particular biometric technique to a given application. There is universal agreement in the literature, that no one biometric technology has emerged as the perfect technique suitable for all applications. This has led to the idea of multimodal biometric devices, though this notion has not been welcomed by civil libertarians who believe citizens are giving away too much personal information. Other shortcomings of biometrics include: the exclusion of persons who do not possess a particular body part(s), the ability to dupe systems using disguises or static false images, user acceptance in some countries (e.g. linked to privacy-related issues), lack of standardization, and prohibitive costs for systems integration.

7.1 Government Services

Governments have long searched for a way to conduct transactions with citizens (G2C) that ensure that funds are transacted with a bona-fide individual to whom benefits are ensuing. Each year governments worldwide lose billions of dollars to individuals making fraudulent claims. Most of the problems stem from outdated identification number systems based on social security schemes which allow for the incidence of duplicate numbers (Lunde, 1980). The larger the country's population, the more difficult administration becomes, especially when one considers the multiplicity of services governments may offer, such as pension, medicare and family allowance. In the U.S. biometrics have been used for electronic benefits transfer (EBT) and other social services since 1991. In a bid to stop fraud the Los Angeles County in California introduced AFIRM (Automated Fingerprint Image Reporting and Match) for the administration of its General Relief (GR) program in the Department of Public Social Services (DPSS). Other states have since followed the example of Los Angeles County, including New Jersey and Connecticut that enroll and qualify persons for General Assistance (GA) and Aid to Families with Dependent Children (AFDC) using fingerprint identification. Most government biometric schemes are accompanied by a card technology which stores the individual's template and usually carries the cardholder's photograph, signature, and unique ID number. Beyond EBT, national cards can also be used by citizens to receive medical services, for voting, traveling interstate and for driver's license identification (see figure 2). At this stage, it is unlikely that citizen ID cards dedicated to government services will be used for commercial purposes as well.

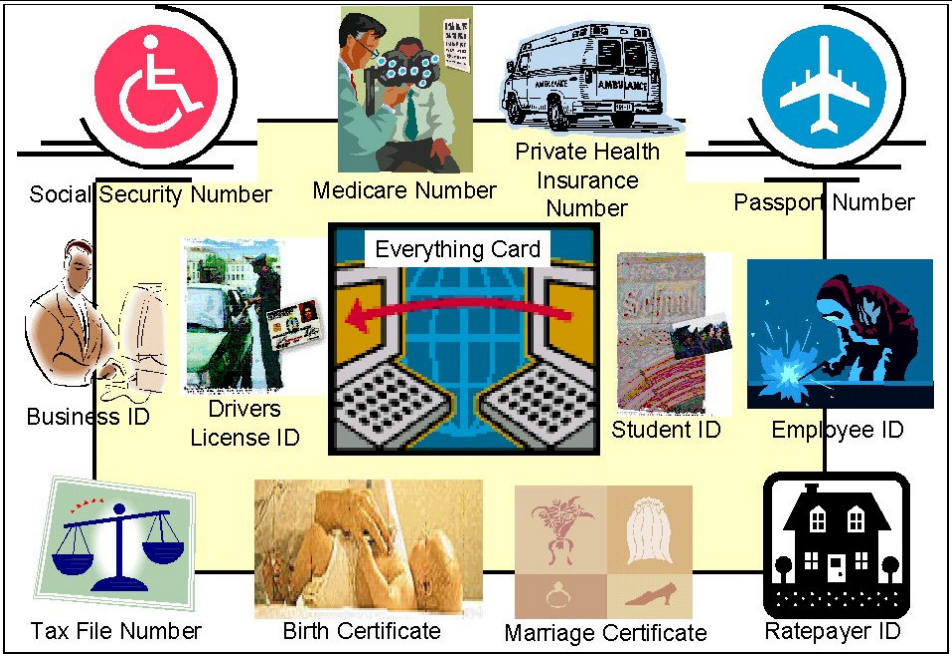


Figure 2. Government National ID Cards Using Integrated Auto-ID Solutions

8. RF/ID TAGS AND TRANSPONDERS

One of the first applications of RF/ID was in the 1940s by the US Defense Force. Transponders were used to differentiate between friendly and enemy aircraft (Ollivier, 1995). It was not until the late 1980s however, when the Dutch government voiced their requirement for a livestock tracking system that the commercial direction of RF/ID changed. It began to appeal to a broader customer audience. The main advantage of RF/ID is that the tag or transponder need only pass by a reading station for a transaction to be enacted; it does not have to make direct contact with a reader. An antenna transmits information between the tag and the reader and a computer interprets or manipulates the information accordingly. Depending on their power source, transponders can be classified as active or passive. Active transponders are usually powered by a battery (with a limited lifetime), which operates the internal electronics. A passive transponder on the other hand, is triggered by being interrogated by a reading device that emits radiofrequency (RF) power as the transponder has no internal power source of its own. Transponders, unlike tags, are not worn on the exterior of the body or part. On humans or animals they can be injected into the subcutaneous tissue.

8.1 Animal and Human Monitoring

Transponders are excellent mechanisms to identify and keep track of animals especially in closed systems (Finkenzeller, 1999). They are implanted in household pets (e.g. dogs, cats and birds), common livestock (e.g. cows, sheep and pigs), animals used for experimental research (e.g. mice and monkeys), and pests (e.g. rabbits) that need to be continually tracked to control numbers. The use of tags and transponders in livestock farm management however, has revolutionised the way farmers work. Allflex and Oxley Systems are just two of a

whole list of companies that have been promoting RF/ID tags as a management tool for agribusiness co-use. The farmer has the ability to centralise all his/her operations whether it be in the prevention of disease in herds, feed-control or in meeting production goals. The introduction of strict regulations has also meant that the mandatory identification of animals has acted to inevitably increase the adoption of RF/ID transponders (e.g. the 1992 European Union Council Directive 92/102/EC). Look (1998) believes that in the not-to-distant future the detailed history of every piece of meat will even be tracked and recorded on the package label in supermarkets. Outbreaks of BSE (bovine spongiform encephalopathy) and other viruses have seen consumers demand more information.

Animals are not the only living beings that can be implanted (Michael, 2003a). Hewkin (1989) was one of the first people to suggest that subminiature read-only tags would be injected under human skin using a syringe to reduce problems such as fraud. This was probably in response to Dr Daniel Man's 1987 patent regarding a homing device implant designed for humans called "Man's Implanted". The device is considered by some as having a plethora of potential uses including: the enhancement of 911 services, a device for locating kidnapped children or older persons who may become disoriented, for tracking and monitoring very important persons (VIPs), employees, soldiers or criminals, and many other types of location-based services (LBS). A little over a decade after Man's patent, Professor Kevin Warwick of the University of Reading became the first known individual to embed a silicon transponder (23 by 3 millimetres) into his body (his left arm), for tracking purposes (Sanchez-Klein, 1998). The ten-day trial was confined to the boundaries of his university department building. Sensors around the department were triggered every time Warwick was in range of a reader. Warwick believes the ultimate goal of the transponder technology is to connect humans more closely with computers. However, his very publicised follow-up Cyborg 2.0 experiment, which intended to prove that two persons with implants could communicate sensation, did not live up to expectations (Dobson, 2001). Yet, this has not discouraged companies like Applied Digital Solutions and Wherify from launching commercial products that use transponders together with the global positioning system (GPS) to track humans for a variety of purposes (see figure 3).

Figure 3. The VeriChip Human Transponder Implant by Applied Digital Solutions

9. CROSS-CASE ANALYSIS

The changes brought about by auto-ID were not only widespread but propelling in nature. No sooner had one technology become established than another was seeking entry into the market. The technical drawbacks of magnetic-stripe cards for instance, meant that smart cards were more suitable in particular application scenarios. A pattern of migration from one technology to another seemed the rule rather than the exception- that was until biometric techniques increased security not only in magnetic-stripe cards but bar code cards as well. There was also the movement from contact cards to contactless cards and bar codes to RF/ID transponders but by no means were the technologies making one another obsolete but spurring on even more research and development (R&D) and an even greater number of new applications and uses. Figure 4 shows the different types of patterns that have occurred in the auto-ID industry. The three main flows that are depicted in the diagram are migration, integration and convergence. These trends are also summarized in table 2.

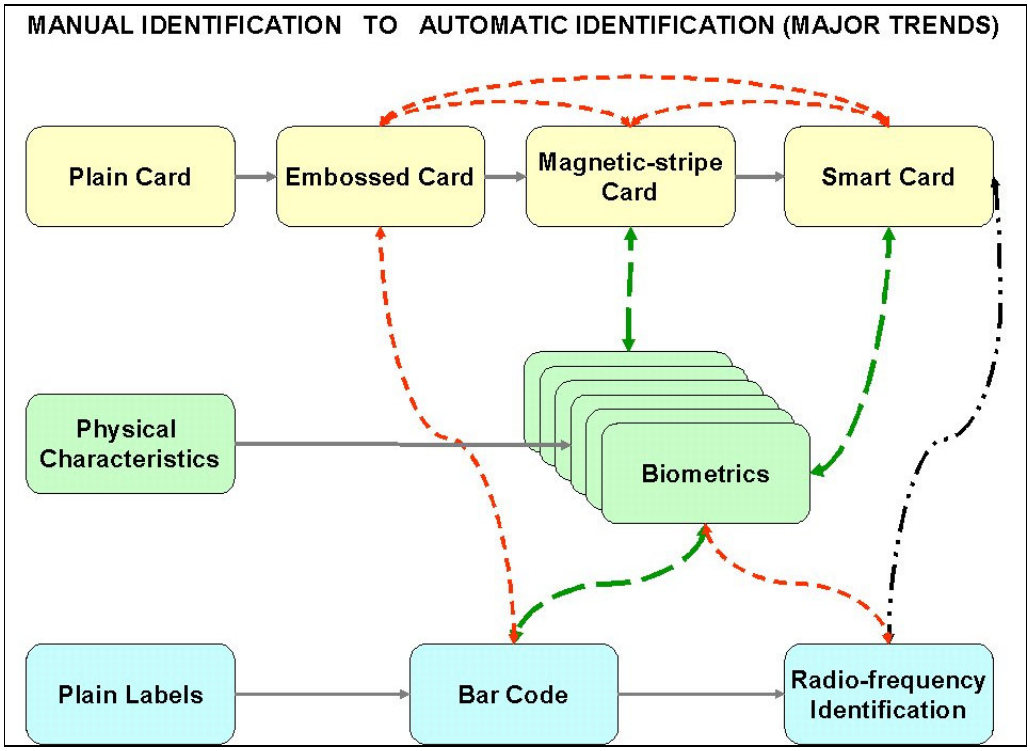
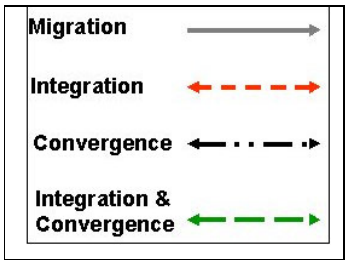


Figure 4. Trends in the Auto-ID Industry: migration, integration and convergence



The table identifies the relationship between different auto-ID techniques. The abbreviations used include 'M' for migration, 'I' for integration and 'C' for convergence. The matrix is to be read from left to right. For instance, taking the case of bar code, one can see that both migration and integration (MI) trends occurred between it and RF/ID transponders. The asterisk depicts a redundant flow.

Table 2. The Auto-ID Industry Selection Environment

Auto-ID Technology	Bar Code	Magnetic-Stripe Card	Smart Card	Biometrics	RF/ID Tag & Transponders
Bar Code	*	MI	MI	MI	MI
Magnetic-Stripe Card	I	*	MI	MI	MI
Smart Card		I	*	MI	MIC
Biometrics	IC	IC	IC	*	M
RF/ID Tag & Transponders		I	C		*

Dependent on a given application scenario, some customers and service providers may choose to migrate from one auto-ID device to another, seeking better security, more storage capacity, greater functionality, a reduction in fraud and counterfeit, even a smaller device that would be more convenient for the end-user to carry. Integration of various auto-ID techniques has also proven popular and this is particularly obvious with respect to card technologies. Service provider legacy identification systems have evolved as the techniques have become available- from embossed numbers, to bar codes, to magnetic-stripe and microprocessor functionality all on the same device. Auto-ID technologies have even converged, as can be seen from the example of the contactless smart card, a recombination innovation that brought together a RF/ID tag with an on-board IC.

9.1 Migration from Bar Code to RF/ID Tags and Transponders

RF/ID manufacturers are starting to make inroads into the bar code market. While some predict RF/ID will totally replace bar codes, it is more realistic to say that RF/ID will have a market for high-cost items rather than low-cost items. The current movement is towards combining RF with EAS (electronic article surveillance). Bar codes have poor readability rates in applications that are exposed to harsh environments whether it is indoors or outdoors. RF/ID can capitalise on this and other weaknesses, particularly where material handling and tracking of components is of the utmost importance. RF tags have many advantages over bar code, including: the amount of information that can be stored, line-of-sight (LoS) is not mandatory, the level of accuracy achieved, and that tagged objects can be mobile while being processed. Proponents of RF/ID, like the Auto-ID Center (2001), believe that before too long, bar code will be replaced by RF/ID. There are however, numerous counter arguments for why bar code will not be replaced altogether by RF/ID. For the time being at least, it seems impossible that every single bar coded item in existence today will have a RF/ID tag or transponder attached to it. Sheer economics and the lack of physical infrastructure would not make this feasible, especially in less developed countries (LDCs).

9.2 Migration from Magnetic-stripe to Smart Cards

Murphy (1996, p. 80) asserts that, “smart cards are the talk of the card manufacturing industry, but the magnetic stripe will be the bread and butter of card makers for the near term.” Yet, one cannot ignore the gravitational pull that is obviously occurring from magnetic-stripe to the chip card. The magnetic-stripe card was more of an enabler, a convenience card, something that would accustom

people to a particular style of behaviour. The smart card is being heralded as the grand solution to personalisation. But already the widespread use of magnetic-stripe has ensured that the size of smart cards must maintain the same ISO standard dimensions. Hybrid cards now have a physical location for microchips, magnetic-stripes, bar codes, embossed characters, holograms and photographs. Many ATM machines have already been upgraded to accept both magnetic-stripe and smart cards. Some smart cards have even been developed to emulate magnetic-stripe or bar code cards so that very costly card readers do not have to be entirely replaced, at least in the short term. This has posed a special challenge to card issuers who are attempting a seamless migration. McCrindle (1990, p. 72) stated, "the two types of technology must coexist". Murphy (1996, p. 83) also agreed that "...cards will be issued for many years with both mag stripes and computer chips." What is of interest to note however, is that the longer the migration phase continues, the more hybrid cards are becoming a defacto standard for applications.

9.3 Integration- the Rise of Multi-Technology Cards

It is difficult to say whether integration was a consequence of an attempt at migration in some applications areas or an independent occurrence. Initially integration of auto-ID techniques on the same device was born from the idea that each technique could serve its own function for different applications (this was particularly true of closed systems). In addition, as a consequence of migration patterns, multi-technology cards served as a way to transition from auto-ID legacy systems to future modes of operation. The requirement to include more than one technique on the card was a result of roll-out phases in preparation for new technologies. New cardholders receive the latest cards while existing cardholders are transitioned prior to card expiration. Hodgson (1995) described this incidence of multi-technology cards as an evolutionary process. Multi-technology cards form a strong argument and present us with a compelling reason for why individual auto-ID techniques will continue to coexist in the future (see figure 5).

Figure 5. Integrated Devices Point to Coexistence of Auto-ID Techniques

9.4 Converging Auto-ID Technologies

The convergence of auto-ID technologies is now starting to become evident at different levels such as standards, regulations, infrastructure and applications. Application centralisation especially is prominent on the agenda of global service providers who are seeking to increase customer loyalty and decrease churn by bundling services together. True convergence however at the auto-ID device level is not as common as it is often portrayed. It all depends on the definition one uses to describe what they mean by convergence. Greenstein and Khanna (1997) describe two types that should be preferred when discussing the auto-ID industry, "convergence in substitutes" and "convergence in complements." The most authentic example in auto-ID of convergence in complements at the present is that between the contact smart card and RF/ID card. Smart cards once required direct contact with a reader, however, today the RF smart card can be utilised by either inserting it in a reader or by presenting it close to a RF field. Additionally, the ability to store biometric templates on a bar code or magnetic-stripe is another example of convergence in complements. In the case of the bar code, the biometric replaces the need for a unique ID number to be stored, with an ID derived from a fingerprint or other unique human characteristic or trait.

10. CONCLUSION

While recombinations and mutations of auto-ID technologies are continually being invented, it does not mean that existing markets for particular techniques will suddenly disappear. On the contrary meeting requirements to new business problems increases the range and depth of auto-ID innovations and should be understood as an evolutionary step in the development of the industry at large. It is through this interaction and feedback, between service providers that require EC applications and auto-ID technology providers that assist in designing solutions for them, that end-user needs are met and on-going innovation is assured. In this manner, coexistence can be put forward as a plausible model of the future for the auto-ID industry. In open systems especially, it is highly unlikely that a single auto-ID device could ever cater for the needs of a complete end-to-end application, rather auto-ID technologies usually work in concert to fulfil large-scale initiatives. This in itself increases the need for auto-ID diversity, rather than being a limiting factor. And while some have a vision that every single non-living thing will eventually be 'smart' or 'intelligent', as put forward by the development of the Electronic Product Code (EPC), consumers will probably insist that some things remain 'dumb'. In understanding the auto-ID selection environment, the paradigm has shifted from an economy that seeks the domination of one auto-ID device towards an economy that accepts (if not welcomes) the coexistence of numerous auto-ID devices. While the relative shares of production for each auto-ID device may vary over time, and some devices will address particular market needs better than others, overall several technologies will continue to co-exist. Thus it can be said that different auto-ID devices are sharing in the same trajectory. It is therefore more correct to speak of a holistic auto-ID industry in terms of one unified technology system (TS), rather than smaller separate industries that focus on the ascendancy of a single *super* auto-ID technology.

11. REFERENCES

Adams, R., (1990), Sourcebook of Automatic Identification and Data Collection, Van Nostrand Reinhold, New York.

ADS, (2002), Applied Digital Solutions, ADSX, http://www.adsx.com/, [accessed 15th October 2002].

Ames, R., (1990), Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?, Van Nostrand Reinhold, New York, p. G-1.

Auto-ID Center, (2001), Home, Auto-ID Center: identify any object anywhere automatically, http://www.autoidcenter.org/, [accessed 2nd February 2003].

Berge, P., (1987), IATA and automatic identification standards for the airlines, Bar Code Symbologies, Standards and Technology Updates, AIM, London.

Bright, R., (1988), Smart cards: principles, practice, applications, John Wiley & Sons, New York, p. 13.

Brown, S. A., (1997), Revolution at the Checkout Counter: the explosion of the bar code, Harvard University Press, London.

Cohen, J., (1994), Automatic Identification and Data Collection Systems, McGraw-Hill Book Company, London.

Collins, D. J. & Whipple, N. N., (1994), Using Bar Code- why it's taking over, Data Capture Institute, Massachusetts.

Crotch-Harvey, T., (1996), Smart cards in telecoms, Smart Card News, http://www.smartcard.co.uk/telecoms.htm, [accessed 22nd March 1997].

Dobson, R., (2001), Professor to try to 'control' wife via chip implant, Rense.com, http://www.rense.com/general10/professortotry.htm, [5th June, accessed 15th October 2002].

Finkenzeller, K., (1999), RFID Handbook: radio-frequency identification fundamentals and applications, John Wiley & Son, New York.

Geers, R., et al. (1997), Electronic Identification, Monitoring and Tracking of Animals, CAN International, New York.

Greenstein, S. & Khanna, T., (1997), What does industry convergence mean?, in "Competing in the Age of Digital Convergence" by (ed.) Yoffie, Harvard Business School, Massachusetts, pp. 201-226.

Hewkin, P. F., (1989), Future automatic identification technologies, Colloquium on the Use of Electronic Transponders in Automation, pp. 6/1-6/10.

Hodgson, K., (1995), Multi-tech cards: just the beginning, Security, 32(10), pp. 19-20.

Jain, A. K. et al., (1997), An identity-authentication system using fingerprints, Proceedings of the IEEE, 85(9), pp. 1365-1387.

Kaplan, J. M., (1996), Smart Cards: the global information passport, International Thomson Computer Press, London, p. 68.

LaMoreaux, R. D., (1998), Barcodes and Other Automatic Identification Systems, Pira International, New York.

Look, G., (1998), Auto ID makes tracks in livestock traceability, ID Systems- the European source for auto ID, http://www.idsyseuro.com/cow0498.htm. [accessed 25th April 1998].

Lunde, A. S. et al., (eds) (1980), The Person-Number Systems of Sweden, Norway, Denmark, and Israel, U.S. Department of Health and Human Services: National Centre for Health Statistics, Maryland.

Lutz, K., (1997), Telecommunications and information services, in "Smart Cards: seizing strategic business opportunities", by (eds) Allen & Barr, McGraw-Hill, New York, pp. 128-150.

McCrindle, J., (1990), Smart Cards, Springer-Verlag, London.

Michael, K., (2003a), The automatic identification trajectory, in "Internet Commerce: digital models for business", by Lawrence et al., John Wiley & Sons, Australia, pp. 131-134, 136.

Michael, K., (2003b), *The Technological Trajectory of the Automatic Identification Industry*, University of Wollongong, Australia, PhD Thesis.

Moran, R., (n.d.), Automatic Identification Systems: growth markets- a major enabling technology for the 90s, Business Communications Co., New York.

Murphy, P. A., (1996), Does plastic still have a great future?, Credit Card Management, 9(3), pp. 80-90.

O'Gorman, L. & Pavlidis, T., (1999), Auto ID technology: from barcodes to biometrics, IEEE Robotics & Automation Magazine, 6(1), pp. 4-6.

Ollivier, M. M., (1995), RFID- a new solution technology for security problems, European Convention on Security and Detection, 408, pp. 234-238.

Palmer, R. C., (1995), The Bar Code Book- reading, printing and specification of bar code symbols, Helmers Publishing Inc., New Hampshire.

Rankl, W. & Effing, W., (1997), Smart Card Handbook, John Wiley and Sons, New York.

Sanchez-Klein, J., (1998), And now for something completely different, PCWorld.com, http://www.pcworld.com/news/article.asp?aid=7954, [27th August, accessed 22nd November 2001].

Smith, I. G., (1990), AIM- an industry activity group for automatic identification, Computing & Control Engineering Journal, 11, pp. 49-52.

Svigals, J., (1987), Smart Cards: the new bank cards, Macmillan Publishing Company, New York, p. 29.

Swartz, J., (1999), The growing 'MAGIC' of automatic identification, IEEE Robotics & Automation Magazine, 6(1), pp. 20-22, 56.

Wherify, (2003), GPS Locator for children: Peace of mind for parents, cool for kids, Wherify Wireless Location Services, http://www.wherifywireless.com/, [accessed 5th January 2003].

Zoreda, J. L. & Oton, J. M., (1994), Smart Cards, Artech House, Boston, p. 16.