

## RFID Applications

To a large extent, the current notoriety of RFID is due to its rapidly increasing use in end-user applications and the unique features it they affords. To motivate our discussions of systems, software, and services in subsequent chapters, we begin our exploration of RFID technology by discussing three selected applications of special significance, namely e-passports, ticketing, and supply chain management. In all three cases, RFID has been deployed in large-scale systems supported by networked services of varying complexity and provides useful examples on which to model our discussions. We conclude this chapter by briefly outlining other applications of RFID as well as reporting on current standardization efforts, with particular reference to its role in application development.

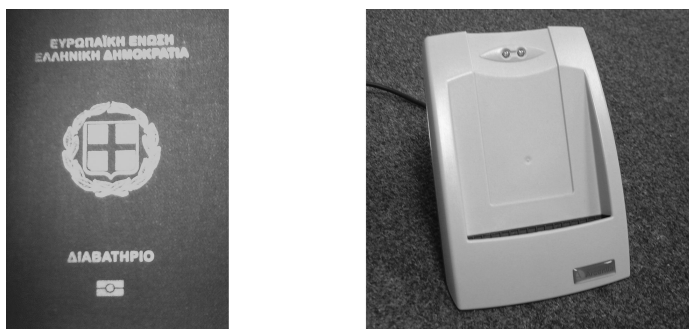
### 2.1 ICAO e-Passports

In May 2004, the International Civil Aviation Organization (ICAO) approved the specification for the so-called machine-readable travel documents (MRTDs). MRTDs use standard RFID technology to store personal and biometric information on passports, visas, and travel cards. Their development is seen by ICAO and its member countries as a significant improvement over manual inspection of travel documents at border control points in terms of efficiency and data entry precision. Nevertheless, the rapid development of MRTD specifications and their quick adoption and implementation have been driven by the desire to increase the security of air travel, as evidenced by public statements by law enforcement officials on both sides of the Atlantic. By 2007, more than a hundred countries had issued or were in the process of issuing passports that conform to the MRTD specification. A smaller number have upgraded their border controls with scanning equipment for MRTDs.

## RFID technology and MRTD

The ICAO provisions call for ISO 14443-compliant RFID tags (discussed in Section 3.2.2) embedded in travel documents to hold personal and biometric information on the traveler. RFID readers (see Figure 2.1) operated by immigration services interrogate and retrieve traveler information without the need for manual intervention. Due to the current capacity of tags, biometric data are restricted to photographs but the standard also provides specifications for iris scans and fingerprints for future use. Millions of e-passports are already in use, and thousands of MRTD-capable immigration control facilities have been deployed at disembarkation points in several countries. It is noteworthy that according to the specification MRTDs remain valid even if the embedded chip is damaged or unreadable for any reason.

To control access to the data stored in the MRTD, the standard recommends that information stored in the second line of the machine-readable zone (MRZ) of the document be used as the key for the reader to gain access to the RFID memory content. As a result, this key is made up of a combination of the passport number, its date of expiry and the date of birth of its holder, which is easily obtained. A long-term goal of ICAO seems to be the development of a supplementary public key infrastructure to allow MRTD inspecting authorities to verify the authenticity and integrity of the data stored in the document.



**Fig. 2.1.** A Greek e-passport and an associated reader. Note the mark at the bottom of the front cover of the passport indicating that it is MRTD compliant. The Greek MRTD system has been developed by Arcontia in collaboration with ACG.

The ICAO specifications also define the data that shall be stored in an MRTD:

- personal data that to a large extent duplicate what is currently displayed on the photo page of a typical passport already and

- biometric data that include a (low-resolution) photograph, textual descriptions of the characteristics of the holder, and provision for fingerprints and iris scans.

Though a lot of discussion has been devoted to the biometric information included in the e-passport, the reality is that current RFID technology employed in its implementation has insufficient capacity to hold this information. Tags available commercially in large quantities provide up to 4 Kbytes of storage which is not enough to hold even a single high-quality image that can provide adequate resolution for automatic face recognition. Fingerprints have similarly high storage requirements (even when compressed with sophisticated wavelet schemes), and this is also true for iris scans.

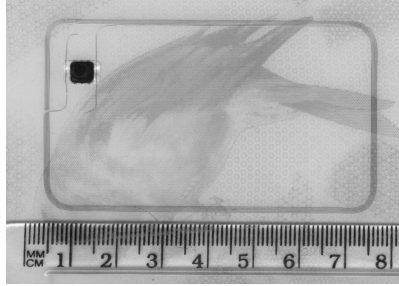
Also note that RFID in e-passports has further implications related to system maintenance. While passports are typically issued for a period of 5 to 10 years (for adults), RFID chips are under warranty for a mere 2-year period. This raises very considerable concerns for the long-term viability or indeed the value of this system and casts doubts on the prudence of the decision to invest considerable amounts on this technology.

## **MRTD security and privacy**

While MRTDs certainly facilitate faster and more accurate data entry, they have justifiably received strong criticism regarding their security and privacy performance. Furthermore, upon closer examination, any claims that their deployment may improve the safety of air travel do not stand up to scrutiny and in some cases it may in fact reduce the effectiveness of border control due to the automation of the process.

Duplicating the RFID component of an MRTD (see Figure 2.2), including all the data held, is a fairly straightforward process that can be achieved at relatively low cost with commodity equipment. This was demonstrated at the Black Hat conference by Lukas Grunwald soon after e-passports became available, and today the passports of several countries have been attacked in this way. The simplicity of the duplication process is such that it makes copying the electronic component of an e-passport far easier than reproducing the printed elements, though modification of the passport data has not been demonstrated yet and it is certainly much harder, as their integrity is protected by the digital signature of the issuing authority.

Access to personal data stored in the chip is facilitated rather than hindered compared with paper only travel documents. Since MRTDs provide access to their data via a wireless channel, it can be easier to access such data as it is not necessary to gain physical access to the document itself and certainly not necessary to open it as required for visual inspection. It has been demonstrated that with specialized equipment it is possible to communicate with an e-passport over a distance of several meters and probe for access to the data. Even in cases where additional external shielding is used to protect



**Fig. 2.2.** RFID tag embedded in the UK e-passport.

against unauthorized remote access for example as implemented in the latest version of the USA e-passport, it has been shown that it is still possible to interrogate the RFID chip if the document is not firmly folded.

Finally, the ICAO specifications permit e-passports to only support what is referred to as passive authentication, which provides no access control mechanism to the RFID chip. Fortunately, most countries have opted for stronger protection under the provisions of the so-called basic access control (BAC) and active authentication mechanisms, although the implementation of either or both schemes is optional. Basic access control operates by establishing a secure channel between the reader that carries out the inspection and the e-passport and protects both the confidentiality and integrity of the transmission. To achieve this, BAC requires symmetric cryptography provisions, including the generation of encryption and authentication keys from passport information that is printed on the actual document (specifically passport code, expiration date, and birth date of the holder).

At border control points, inspecting officers would pass the MRTD presented by the traveler through an optical character recognition (OCR) system to retrieve the information used for the generation of the cryptographic keys. These are printed on the machine-readable strip according to a previous ICAO regulation. The actual cryptographic keys would be computed on the fly by an attached computer, which would subsequently communicate with the e-passport and retrieve the data, store it, and possibly display it on the operator screen. The whole process would last only a few seconds.

Yet recent work has highlighted the fact that due to regularities and practical constraints on the range of seed data, many if not all MRTD implementations would employ keys with low entropy and thus be relatively easy to break. In fact, practical attacks on e-passports on the general public, either via brute force or through eavesdropping in the exchanges directed by the inspection system, have been demonstrated using relatively inexpensive hardware in [17]. In addition to the obvious dangers associated with harvesting personal data in this manner, it is also feasible that the unique identifier established by the passport code could be used as the key for tracing applications, where

individuals could be followed from location to location and their movements recorded in some detail.

## **MRTDs and network infrastructure**

E-passport applications have simple requirements both in terms of RFID tag access and supporting network services. At any one time, only a single tag is within the range of the reader and there is ample time to carry out the required data retrieval. Furthermore, the volume of collected data is relatively low since even at peak periods and for the largest operators of e-passport inspection systems, over a single day only a few hundred thousand recordings are made at most and normally data rates would be well below that. In any case, such inspection systems raise very restrictive interoperability requirements since they operate within a national scope and are commonly supported by proprietary database applications over secured private networks.

One area that could require some networking support is the implementation of active authentication and extended access control, although this is something to be considered in the future as far as the ICAO is concerned. Under these proposals, individual tags have unique keys that certify their authenticity and that can be checked against databases maintained by the issuing authorities. Moreover, rather than a cached copy of the public keys of all known issuers replicated at each station, a complete public key infrastructure (PKI) with key revocation provisions can be supported. Such a system would considerably improve security of the e-passport and privacy protection but at the same time would raise considerable additional issues related to its trusted operation.

Nevertheless, MRTDs cannot deliver their potential benefits—outside the narrow scope of data entry—unless they are supported by networked control points interlinked with law enforcement systems, as outlined by a recent report by the UK National Audit Office. In this report, NAO severely criticizes the decision to proceed with deployment of e-passports without provisions for enabling full network support, which they consider necessary to justify the investment in this technology.

## **2.2 Ticketing**

One of the earliest and still fast growing applications of RFID has been in metropolitan public transport ticketing. RFID-based ticketing systems were operational as early as a decade ago and today have been deployed in numerous cities across the globe. In such applications, RFID tags would be embedded in credit-card-sized reusable tickets that store either a seasonal pass or credit that can be used against travel. Readers, positioned primarily at the entrance gates, validate the tickets or deduct fares for travel as appropriate (see Figure 2.3). Unlike older ticketing technologies, notably those employing a magnetic

strip to encode data, RFID-based tickets are capable of holding a code that uniquely identifies the passenger and the ticket and in some cases also store personal information about their holder and a record of the most recent trips.

RFID offers distinct advantages due to the superior durability of tickets, which are placed in a hard plastic enclosure and as a result can be used for much longer periods of time. Ticket longevity also benefits from the relative lack of wear and tear during automatic inspection since no mechanical components are involved in the process. Ticket inspection at the gates is also facilitated by the far higher read accuracy of RFID compared with magnetic, which helps maintain the steady flow of commuters in and out of the system, especially at peak times. Finally, RFID tickets can hold considerably more data, which allows the use of personalized unique identifiers that can be used to virtually eliminate fare evasion.



**Fig. 2.3.** An RFID ticket validator at the gates of the London Underground network.

Many RFID ticketing systems employ the ISO 14443 standard, which provides specific facilities for transport applications. It is also common to use proprietary extensions to improve security through the cryptographic protection of communication between reader and tag as well as access to the tag memory (common choices include the Philips MIFARE protocols and the Sony FeLiCa system). ISO 14443 uses inductive coupling, has a relatively short range, and has several other useful features for ticketing which we discuss in more detail in Section 3.2.2. Its short read range in particular is used to the advantage of this application, as even in cases where readers are installed in relatively dense configurations, it is always clear which ticket corresponds to the tag presented by a specific passenger. Finally, data throughput requirements for ticket validation and inspection are very low compared with the available read performance, and the timing overhead as perceived by commuters is minimal.

## The Oyster card

One of the largest RFID-based ticketing systems is the Oyster card [69] in London, UK, which supports more than 10 million active passengers and has deployed over 27,000 readers. The Oyster card can be used in all modes of public transport operated by Transport for London (TfL), including the Underground, the Docklands Light Railway, the Croydon Tramlink, and the London River Services. A measure of the complexity of this system is the fact that management of the London Underground services alone involves approximately 500 trains running at peak times, 253 stations owned (275 served) and in use for 19 hours per day, over 12,000 staff and numerous engineering assets. Moreover, the London Underground has been in continuous operation since 1863 and as such has inherited a variety of components and facilities that were created using legacy technologies but cannot be completely or concurrently overhauled due to the disruption this would cause to the operation of the service.

One area where efficiency improvements are critical is streamlined ticketing, which has a central role to play in reducing the time required to access trains. To this end, TfL has recently introduced improvements in self-service ticketing (for example through the operation of credit card processing facilities by passengers without the involvement of staff) and payment, faster entry and exit, and better transportation between the gates and the platform. Except for the latter issue, these improvements were the core objective of the Prestige project, which supported the implementation of RFID and included a number of additional aims, including the prevention of fare evasion.

Reduction of ticket counterfeiting, and “fare dodging” in particular, is estimated to cost 5 to 6 million British pounds on average each year. Prestige provided for major upgrades in all aspects of the entry and transfer subsystems over a five-year period and this has been estimated to cost over 10 billion British pounds. Of these, only about 1% is associated with the implementation of RFID technology. Clearly, the cost of the technology itself in this case can be easily justified, and indeed to a significant extent it can be directly recovered by the gains due to fraud reduction.

## Interaction design, system affordances and performance

RFID was selected to replace magnetic strip ticketing because it can deliver improved performance in terms of higher throughput of passengers from the station entrance to the platform. RFID systems only require the card and the reader (which in this case is also capable of writing) to be in close proximity, thus eliminating the need for magnetic systems to insert the ticket into a reading unit for precise positioning. Instead, RFID readers can be placed in any convenient location on ticket vending machines and the gates, for example on the entry gate’s top side and within easy reach for the majority of the passengers, as seen in Figure 2.4. Moreover, the card itself can be made out

of durable strong plastic, which reduces wear and tear on the card and makes reading errors virtually impossible. This fact results in considerably shorter times required to operate the turnstiles.



**Fig. 2.4.** Entering The Tube using the Oyster card. Note the placement of the Oyster on the special indicator, which ensures accurate reading and the displays embedded on top of the gates, which provide visual and sound feedback.

The colocation of both magnetic and RFID card readers on the same gating equipment (see Figure 2.3) and the fact that both magnetic and RFID cards have the same size gave rise initially to some interesting behavior. One of the early findings of user research was that commuters used to magnetic strip tickets frequently inserted their new Oyster cards into the slot of the magnetic strip reader, which compressed and damaged the card. Subsequently a provision was made that the plastic enclosure of the RFID chip be able to withstand at least 100 such events.

Although RFID cards can be operated at a distance and thus do not require contact between the reader and the tag antenna, in practice two considerations also had to be factored into an appropriate design and the selection of reading range. First, it must always be clear what card is presented to which gate by whom to ensure that correct charges are applied. This is so even in locations where gate density is high, resulting in a large number of individuals using the system concurrently and at close proximity to each other. To achieve this effect, the range of the system was restricted to only a few centimeters, a choice that provided the desired effect.

Second, cards must be read and updated with very high accuracy which implies good placement of the card antenna within the field created by the



reader. A well-known limitation of inductive RFID systems is that when the plane defined by the coils of the tag antenna is approximately perpendicular to the field created by the reader, then the coupling effect is weak and leads to a failure to charge the RFID chip. In early trials with the system, such erroneous use of the card was observed far more frequently than expected, likely due to the location of the Oyster card reader on the gate. As a result, usage guidance provided by TfL now suggests that the card be “touched in and out” with the card placed flat on the reader. Despite the fact that contact is not required, touching the card guarantees that the orientation of the antenna is appropriate and a successful read or write very likely.

A clear benefit of the new RFID-based approach is the reduction by approximately 3–4 seconds of the time required by commuters to get from the point of entry to the station until their arrival at the platform. This is primarily due to the fact that removing ticket validation errors, which disrupt the incoming flow, results into a smoother distribution of commuters along the system. This has been perhaps the biggest success of Oyster in terms of service improvement, together with its use in buses.

Using magnetic strip technology it was not practical to operate read-write equipment on buses, and as a consequence ticket issue and validation of passes was carried out manually by the driver. The small form factor and the lack of any mechanical parts in the RFID reader have made viable the use of the Oyster card in this context also and have accelerated the ticketing process, which is now conducted automatically. This has improved bus performance especially during the morning rush hour, which has benefited the most from the efficiency afforded by RFID ticketing. In the longer term, the introduction of Oyster is expected to have even more significant implications for buses in particular, as it allows the possibility of operating with cashless carriers, with additional security and safety gains.

From a user perspective, the biggest success of the Oyster card seems to be removing the “fumble factor”. Users must take a magnetic ticket out of their wallet, put it into the reader, walk through the gate, and pick up the ticket on the other side, none of which are necessary with Oyster. So radically reducing the fumble factor was a major service offering and probably the biggest motivation for people to use it.

Another system design challenge has been how best to provide feedback of successful or unsuccessful operations to the passenger. Again, the emphasis in Oyster has been to support the highest possible throughput, which in this case implies that feedback should be simple and unambiguous. The Oyster system uses sound and simple red or green LEDs to provide confirmation of successful authorization as well as embedded displays in the gates and on ticketing machines for more complex interactions. In this way, access authorization is separated from general travel management and payment issues: the former is optimized for speed and is carried out using simple feedback, and the latter is designed with ease of use and adequate information provision in mind.

## **Organizational changes**

Another lesson learned from the Oyster system is that while technology can be developed and deployed relatively speedily, organizational issues and ensuring stakeholder involvement require much longer time frames for developing successful solutions. To this end, a guiding principle that proved successful in Prestige was to set significant and realistic targets that required a limited number of changes to occur at any one time. When engaging the organization internally, it is necessary to identify all the roles and processes affected and allow the inevitable learning curve to catch up. In particular, staff training and internal communications are critical, but providing for these tasks increases in complexity with the size of the organization.

Common sense, if not due diligence, dictates that systems that have millions of users on a daily basis should be durable and easy to use and thus be designed accordingly and heavily tested. Nevertheless, even in cases where adequate provisions are made, it is still unlikely that the transition will be seamless. For this reason, it is necessary to take into account that even the simplest system when operated at large scale, will cause some degree of confusion that must be dealt with. Consequently, supportive measures should be in place beforehand and cater to the issues raised during the user's learning curve. This was clearly something that the Prestige project did especially well; for example, staff training started three years before the first cards were issued to the public, and planning for system re-engineering tasks started well in advance of that.

A longer term issue is the development of the Oyster card into a general purpose mobile electronic payment system. This approach has been adopted by other ticketing systems, notably the Octopus card in Hong Kong and the Suica card in Tokyo (see Figure 2.5), both used for micro-payments in a large number of retail outlets in each city. This extension of card use has been very successful and very popular with consumers in both cases mentioned above. But it also implies entry into a fundamentally different market, that of financial services, which is associated with significant risks and may not be desirable, especially in an organization that is publicly held.

## **Network support for the Oyster card**

The operation of Oyster is supported by an extensive multi-tiered back-end information system that processes payments, records and validates transactions, identifies fare evaders and prohibits their future entry, and records transactions. Recent travel details are held on the RFID tag (last seven trips taken), in a local system at the station level, and at a centralized data warehouse. Updates to the data warehouse are carried out in nightly batches, where incoming data are cross-validated, cleaned, and updated. These supporting network services are proprietary applications delivered over a secured virtual private network, which despite its complexity and strict performance requirements,



**Fig. 2.5.** Using the Suica card as a general-purpose payment mechanism.

is nevertheless a fully controlled environment. In particular, the store-and-forward approach selected as a core architectural feature has been a very successful choice and has provided the basis for uninterrupted and robust performance.

Unique identifiers are used in combination with suitable cryptographic protocols to authenticate a card to the system and to provide protection of the communication between the card and the reader. As a result, ticket counterfeiting is very hard unless the cryptographic keys are cracked (a brute-force attack is unlikely to succeed in this case, as the wireless communication overhead incurs a considerable delay, which makes such attempts impractical). Moreover, the use of unique card identifiers ensures that specific cards can be pinpointed and associated with activities that violate the rules of acceptable use. Such cards can be subsequently blacklisted, thus preventing their holders from entering the system.

Management of blacklists is an interesting aspect of the system. Lists are downloaded to gates and bus ticketing equipment which locally carry out the verification of the access credentials presented by the cards. The lists are refreshed daily to include new card codes that have been found in violation and are purged monthly to remove cards that have appeared inactive for longer periods. This strategy does not completely guarantee the elimination of fare evasion by well-organized and determined commuters who are committed to performing complex usage patterns employing multiple cards. Nevertheless, it does provide a good compromise in the context of the overall risk management approach adopted by the system and fits well with the system design philosophy, which gives precedence to robustness and failure tolerance.

Indeed, system design driven by appropriate risk management considerations is a tactic employed consistently by the Prestige project. Notably, a core design trade-off relates to balancing system survivability against its ability to authenticate users accurately and provide access to transport services even when the card management back end becomes unavailable. In this case, the transport system as a whole will continue to operate for at least seven

days without any noticeable disruption to passengers at the minor additional risk of increased unauthorized access. This design decision has had great success up to now, and in practice the system has been operating without any high-profile or large-scale disruptions for several years.

The main ingredient that has guaranteed such undisrupted operation is the heavy use of caching and replication architectures at all system levels. The Oyster card itself employs its extra storage capacity—in addition to the unique identifiers and in some cases some personal identification data—to hold records of the most recent read-write events observed and the active value of the ticket. Even in cases when the information stored in the card cannot be verified in real time at the gate, passengers are still allowed into the transport system and the transaction is stored locally until network connectivity and communication to the central servers is restored. While this opens up a small window of opportunity for fare dodgers, the financial impact would be localized and still compares favorably against the magnetic strip system. The success of this approach is also highlighted by the fact that since the introduction of the Oyster, revenue under similar traffic conditions has been increased by 10%, while at the same time ticket inspectors carry out far fewer controls.

A complication that in smaller installations of RFID would be a mere annoyance or could be addressed effectively through longer user training (which is not an option here given the scale of this system) is that RFID cards, despite being successful in authenticating passengers who gain access to the system, frequently fail to confirm the successful update of the transaction history maintained on the card itself with the new trip details due to synchronization errors. This happens with some regularity and results in an increased degree of uncertainty regarding the status of the system. This problem has been addressed by differing the processing of incomplete transactions to the back end, which can do a better job of establishing the true status of the system, as it can view the totality of the sequence of recorded transactions and the local status of the card is discarded in subsequent writes.

## 2.3 Supply Chain Management

Supply chain management (SCM) deals with the movement of goods between organizations from raw material to finished product. Each supply chain is distinct and reflects the unique needs of the range of products that have to be processed, from supplying fresh food from the farm to the supermarket shelf to delivering uniforms from the manufacturer to the soldier in the desert. Nevertheless, all supply chains share a common goal: to keep the process simple, standard, speedy, and certain.

To achieve this goal, it is necessary that all participating organizations across the supply chain exchange accurate information at frequent intervals and that supply chain costs be unequivocally identifiable at all times. An

essential element of any solution that can meet these requirements is the use of open, worldwide data standards for globally unique product identifiers and product classification systems combined with internet-based information services that can be used to track and trace goods and services [14].

### 2.3.1 Creating Consumer Value

Among all retail sectors, grocery is the most competitive, as it operates with minimal profit margins. It is thus important that grocery retailers exploit any possible efficiency improvement opportunities offered by technology, and indeed over the past 50 years they have pursued this objective with considerable success. In particular, the supply chain of grocery products, also known as fast moving consumer goods (FMCG), has attained considerable operational gains through the implementation of information technologies, including bar codes, resource-planning software, and optimized logistics.

### Efficient Consumer Response

The need to respond to consumer demand with greater efficiency has also produced Efficient Consumer Response (ECR), an initiative to raise performance levels across the entire retail sector [80]. ECR aims to achieve this through the re-examination of processes and procedures for the industry as a whole, recommending improvements, and overseeing the implementation of recommendations. ECR started in the United States but due to its clear business advantages has rapidly extended its reach to the rest of the world, with national and regional initiatives in action.

ECR has identified three priorities for the supply chain:

- (i) to increase consumer value,
- (ii) to remove costs that do not add consumer value, and
- (iii) to maximize value while at the same time minimizing inefficiency throughout the supply chain.

In practice, these priorities are used to identify and fulfill specific goals, for example providing consumers with the products and services they want, reducing inventory, eliminating paper transactions, and streamlining product flow. To meet these goals, distributors and suppliers may need to make significant changes to their business processes that can only be applied through the implementation of novel information and communication systems.

And there is ample room for improvement. Decades after the introduction of information systems in production and logistics control, there are still significant inefficiencies in modern supply chains that adversely affect the cost of retail operations. Upstream supply chain inefficiencies affect the relationships of all trading partners and result in high out-of-stock conditions at the point of sale, a high returns rate, and long lead times. Inefficiencies in the downstream direction negatively affect the accuracy of demand forecasts, which

results in low on-shelf availability and thus loss of revenue despite the fact that products are available on-site. Moreover, information-sharing ineffectiveness between trading partners reduces the accuracy of demand forecasts and the scheduling of the replenishment process.

A direct consequence of low demand forecast accuracy is that trading partners have to maintain increased inventory levels to address unpredictable increases, which in turn result in increased logistics costs. Common practice today is to forecast consumer demand by processing historical point-of-sale data using decision support systems that utilize data warehousing and data mining techniques. However, using point-of-sale data to make forecasts results in lower accuracy because demand patterns change rapidly and such fluctuations cannot be captured at the point of sale but have to be identified earlier in the consumption process. Moreover, historical forecasts cannot effectively take into account the influence of promotions and other marketing instruments, since the success rate of such mechanisms is generally hard to quantify beforehand.

The actual effects of this situation were quantified recently, with estimates that 53% of out-of-stock conditions are due to store replenishment inefficiencies. Even worse, a further 8% of on-the-floor out-of-stock conditions occur despite the fact that the necessary supplies are in storage on-site. To improve these results, it is necessary to record consumption data earlier in the replenishment process so as to allow for greater prediction accuracy, which leads to reduced inventories and optimized supply chains both upstream and downstream.

### **Vendor-managed inventory**

One contribution toward the ECR goals is the so-called Vendor Managed Inventory (VMI), where the vendor rather than the customer specifies delivery quantities sent through the distribution channel. This reversal in the procurement process has become possible only through the deployment of Electronic Data Interchange (EDI) systems, a computer-to-computer exchange protocol for business data. VMI has succeeded in reducing stock-outs and inventory buffers in the supply chain. Common features of VMI include reduction in supply chain length, centralized forecasting, and frequent communication of inventory levels. From a fleet management perspective, delivery vehicles are loaded in a prioritized manner: items that are expected to stock out have top priority, then items that are furthest below the targeted stocking levels, then advance shipments of promotional items, and finally items that are least above targeted stocking levels.

In addition to EDI, a second technology critical for VMI is the standardization of bar codes for the automatic identification of products. This technology has played a central role in the automatic initiation and entry phases of the order cycle, which can be reduced by days. The two technologies together help develop collaborative relationships in which any combination of retailers,

wholesalers, brokers and manufacturers work together to seek out inefficiencies and reduce costs by looking at the net benefits for all participants in the chain.

Overall, VMI has been successful in significantly reducing inventory levels and the number of stock-outs. The latter issue is particularly important not only because of lost sales but also because shelf availability is central to supermarket strategy. Indeed, a significant proportion of supermarket profit margins are due to interest-free periods for products already available on the shelves. Thus, one of the main concerns of retailers implementing VMI has been the perception that reduced inventory will result in less product being available on the shelves and therefore loss of market share.

### 2.3.2 The Role of RFID in SCM

The traditional way to automatically capture product information in the supply chain, as employed by ECR and VMI, has been through the use of bar codes. Bar codes were invented for this reason and indeed have a long and interesting history [100]. Each printed bar code symbol represents a number that can be used to identify the labeled product and possibly link to stored information about it. For example, on the back cover of the citation just referenced, a bar code provides a representation of ISBN code 1846280354. ISBN (International Standard Book Number) is a numbering scheme specifically developed for books and provides a unique identifier for every book published. Using this number, it is possible to search one of several internet databases to retrieve further information, including its title, author, and publisher, and in some cases even retrieve a considerable proportion of the published material, for example on Google books.

Despite their great success and popularity, bar codes have several limitations:

1. Reading a bar code requires a line of sight between the label and the scanner. For instance, a truckload full of products will have to be unloaded and each individual item scanned to retrieve full information about its contents.
2. A label is typically printed and affixed to the product packaging and for this reason exposed and likely to be damaged. In this case, it is no longer possible to identify the marked product.
3. General-purpose bar code symbols can store only a small amount of data, which in the vast majority of cases identifies the particular product item as one of a certain type but cannot differentiate between distinct items from the same product line.

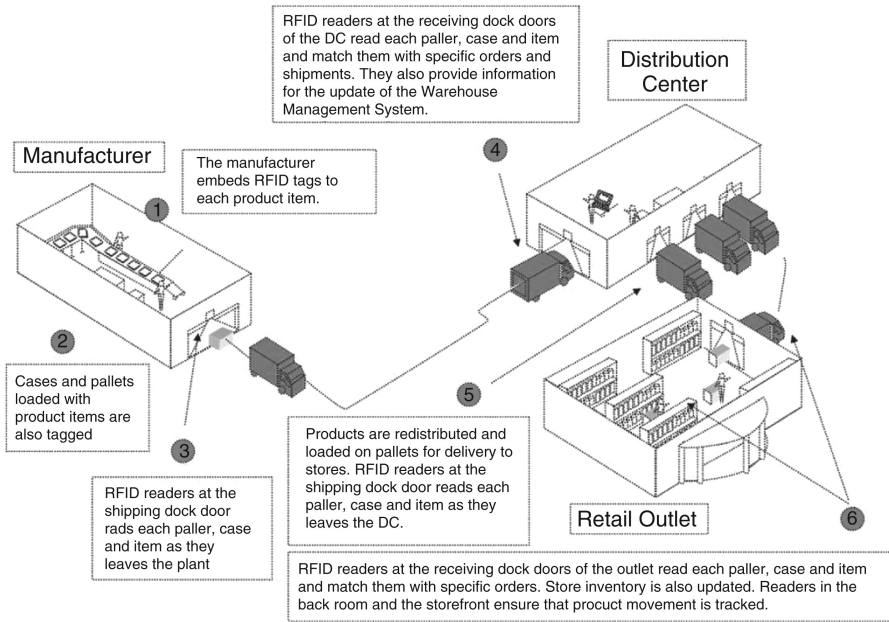
Of course, products also have significant advantages, as they are a well-established, open, and robust technology and can be produced at minimal cost. In fact, in many cases bar codes are part of the design of a product's packaging and as such have almost no cost at all.

Similarly to bar codes, RFID can be used to store globally unique product identifiers, which moreover can provide item-level rather than class-level identification granularity. RFID tags can also provide the means for automatic capture and processing of this information with the added benefit that they do not require line of sight and that since they can be embedded inside a product, they are far less likely to be damaged. As a result, RFID is seen as a good candidate to replace bar codes, although this requires that the additional cost not exceed the potential gains from its implementation. Such gains would be due to a number of efficiency improvements that can be roughly outlined as follows.

- *Reduce inventory levels.* Highly accurate data allow all partners in a supply chain from the manufacturer to the retailer to maintain lower inventories and plan deliveries and shipments in a just-in-time manner. Currently, it is not possible to predict such patterns accurately, and as a result all partners need to maintain excess stock as a buffer against sudden surges.
- *Reduce out-of-stock.* Despite increased inventory levels, it is still common that supply chains run out of stock and as a result cannot respond to consumer needs. Of course, unavailability of stock is directly responsible for lost sales.
- *Reduce order and lead times.* By increasing the visibility of information held in the systems of supply chain partners, it is possible to implement aggressive ordering strategies driven by the vendor rather than the client, which can significantly shorten lead times for orders.
- *Reduce shrinkage.* By marking individual products, it is far easier to identify when and where items have been lost and as a result considerably reduce not only internal theft but also shrinkage due to products expiring.
- *Increase on-shelf availability.* Effective replenishment processes developed on the facilities outlined above would result in higher product availability at the retail outlet shelves. Lost sales due to products not being available on shelves, in some cases despite the fact that they are available in the store, account for a significant proportion of lost revenue.
- *Increase consumer service levels.* Detailed information about individual items can support higher service levels both at the point of sale and for after-sales services, especially safety through more effective management of product recalls. When all product items are tagged, it is also possible to provide fully automated quick checkouts that minimize waiting times at exit.

RFID is well-suited to provide the features required to collect exactly the kind of information that is needed in achieving these objectives. Such tracking and tracing of products can be achieved by establishing prominent control points at all levels of the supply chain (see Figure 2.6), so that items, cases, and pallets are quickly inspected and recorded. Of course, the collected data also highlight the role for integrated enterprise resource-planning systems. ERPs maintain and manage information related to the complete lifecycle of





**Fig. 2.6.** RFID-enabled supply chain management.

business processes, and as a result a successful RFID deployment critically depends on the availability of such systems.

In any case, a typical example of a supply chain control point would be a dock door at a manufacturing or warehouse facility that is equipped with RFID readers that record the codes embedded in pallets loaded with incoming and outgoing products, and automatically update the company's ERP. Subsequently, RFIDs could be used for taking quick inventories using handheld devices [32]. We will often return to this example in subsequent chapters and will discuss in some detail how such a portal would operate as well as all the components required for its construction and operation.

### 2.3.3 A Brief History of RFID in the Supply Chain

The utility of RFID in this role was highlighted in the early 1990s in work carried out by the US Department of Defense (DoD). A feasibility study was conducted as a result of a new doctrine for land operations that was first employed during the First Gulf War, which dictated the rapid advance of mechanized forces at speeds unprecedented in military operations. This approach caused considerable problems in downstream information flows and upstream in the supply chain: intelligence about possible targets often had a lead time of over 12 hours and combat units often found themselves without

supplies due to the inability to replenish materials—in many cases despite the fact that the required resources were available in storage nearby.

This situation prompted the DoD to propose standard systems and protocols for the transmission of information in the so-called Network Centric Warfare model, but more relevant to this discussion, the management of the supply chain using RFID at the container level. At that time, the technology was not cost-efficient for commercial use, but it did highlight the advantages of a system for automatic identification and tracking of products.

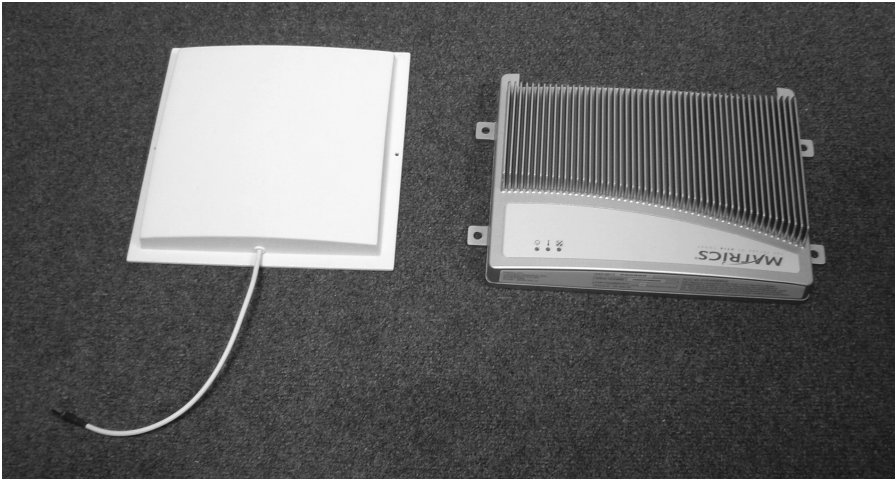
The falling cost of RFID technology over the following decade meant that by the early 2000s tags had become cost-effective in a variety of situations. As a result, several pilot projects highlighted the possible benefits of the technology, and subsequently some of the largest retailers decided to deploy it: Wal-Mart in the United States, Tesco in the United Kingdom and Metro in Germany are all actively implementing RFID to track products across their supply chains. Although the vast majority of these deployments deal with product containers (that is, pallets and cases) rather than individual product items, the technology employed is being developed with a view towards supporting item-level tagging if and when it becomes cost-efficient.

These recent RFID developments have been driven to a certain extent by the Auto-ID Center, established with the support of several manufacturers, suppliers, and retailers of consumer goods for this reason [27]. The early work conducted at the Auto-ID Center has been taken over and further developed within EPCglobal, which operates as a subsidiary of GS1, a global standards organization of automated open supply chain systems previously known as EAN/UCC. GS1 was established through the merger of previously separate bar code standards organizations to ensure that a unique system will be used globally in the supply chains.

The main contributions of EPCglobal are being developed around the so-called Electronic Product Code (EPC) that has been formalized and provides an unambiguous numbering scheme to identify goods containers, services, companies, locations, and assets worldwide [27, 100]. This identifier scheme has evolved into a full system of specifications that define all aspects of network RFID, including tag operation and communication, identifier schemes for several types of entities, network resolution, and meta-data repository services. In subsequent chapters, we examine several of these specifications in detail, as they often represent the state-of-the-art in network RFID technology (see Figure 2.7 for an example of modern EPC-enabled RFID equipment).

### 2.3.4 Implementing RFID in SCM

Unlike ticketing and e-passport applications, supply chain management (SCM) is a far more complex and challenging environment for computing. One special requirement of SCM is the need to read large numbers of tags in a very short period of time while products are physically moved through warehouse portals or other supply chain control points. This task is made even more complex



**Fig. 2.7.** EPCglobal has introduced its own specifications on tag memory layout and communication with readers. Several manufacturers have developed hardware specifically to support these standards, in this case a stand-alone networked reader that can support up to eight antennas.

by the fact that tags read at the same time may represent different types of objects and so they must be filtered and aggregated. Another complication is due to the fact that readers may need to be deployed in dense constellations causing their reading ranges to overlap and complicating communication with individual tags. Unreliable reads and writes at the media access layer cause cascading effects in applications and thus to reliably identify significant events additional smoothing of the data has to be performed.

Finally, despite the fact that early SCM applications focused on container-level tagging, it is becoming increasingly common to extend RFID to the item level, with several retailers currently implementing the technology in commercial applications [69]. This fact can potentially have the greatest impact, as it creates a situation where large collections of objects are directly available to computing systems for auto-identification and can be used to develop end-user applications. A back of the envelope estimation gives a sense of the size of the problem at hand: there are roughly 500 million pallet shipments per year across the globe and across industrial sectors, which correspond to 100 billion cases of products and approximately 2 trillion items. Each item would be scanned and recorded several dozen times as it moved through the supply chain and to its final destination. Without doubt, this will produce a massive volume of data that must be processed and used effectively by applications.

## 2.4 Other Applications

In the previous sections we touched upon three of the numerous applications that employ some form of RFID technology. Since an exhaustive review of applications would require a book in itself, in the closing sections of this chapter we will only summarize a few of the more popular areas that highlight the capabilities of RFID.

### 2.4.1 Asset Management

Asset tracking, monitoring, or management is an integral task of doing business, especially for large organizations. Similar to SCM, asset management can potentially offer increased efficiencies and lower operational costs. For example, deploying and re-deploying equipment in quick successive cycles to meet the needs of business operations requires a detailed inventory of what assets are available, their condition, and where they are located. Tagging with RFID has the potential to lower the overhead of tracking and tracing and provide more up-to-date information thus improving flexibility.

One task for which RFID can offer significant improvements is prescriptive maintenance, whereby equipment use is constantly monitored and maintenance tasks are communicated proactively to staff that can carry out repairs before actual failure happens. Such facilities improve overall field service efficiency, reduce outages, and offer savings in parts costs. Of course, as in all other applications we have considered, RFID alone will not achieve this, but it requires the support of network-based information systems that manage and communicate tasks.

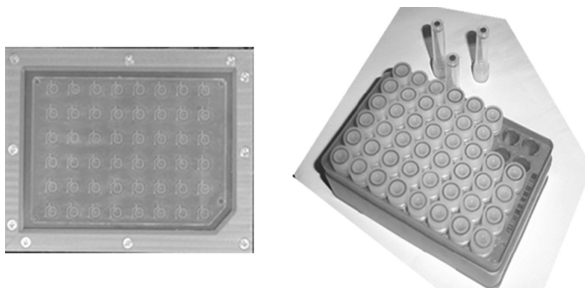
There are many different situations where asset management would be involved that offer widely diverse profiles and requirements, including document management, aircraft maintenance, management of building materials for the construction industry, baggage handling, and cleaning equipment auditing. Although each of these applications employs RFID as a core component of its solution, systems as a whole are fundamentally different and require specific domain expertise. For instance, Figure 2.8 shows the TrakSens software used to monitor the auditing of robotic cleaners.

Finally, RFID is becoming increasingly popular for tracking assets in healthcare applications including anti-counterfeiting for drugs and the control of bio-samples (see Figure 2.9). As regards the latter application, a particularly interesting flavor of RFID has been developed with reader antennas using coil-on-chip technology and tags embedded in test tubes, which offer an interesting alternative for the automation of laboratory records.

### 2.4.2 Electronic Payment

Over the past decade, electronic payments carried out either through the use of a physical token, for example a credit or debit card or a mobile phone, or over





**Fig. 2.9.** Maxell Seiki coil-on-chip technology and RFID-enabled test tubes for asset management of bio-samples.

multi-cards which combine a magnetic credit card, a (contact) smart card for cash payments, and an RFID ticket.

### 2.4.3 Animal and Human Tagging

One of the first applications of RFID has been in tagging cattle for automated accounting in farms. Such tags facilitate accurate record-keeping, including recording the locations where particular animals have been kept, immunizations, and feeding patterns. In this context, RFID has been used as a more effective solution than bar codes, which would often be destroyed due to soiling and the generally difficult conditions under which cattle live. Tags of this type are typically molded as cattle ear rings and use LF frequencies.

Another use of RFID with animals is in tagging pets. This type of tagging can take two distinct forms:

- Collar tags are used to operate pet doors that allow tagged animals to move freely in and out of the house but remain locked at all other times.
- Embedded glass-enclosed tags are used in some cases to provide identification for pets, so that if lost and later recovered, they can be returned to their rightful owner.

This type of RFID also commonly uses LF frequencies and has fairly simplistic operation with minimal security controls.

There are also uses of RFID for tagging humans. A common application concerns the identification of hospitalized patients, who can be issued an RFID bracelet that verifies their particulars. This approach has been developed in response to increasing numbers of errors that lead to either unnecessary surgery or the administration of the wrong medication, with detrimental health effects. There are already several hospitals that have experimented with this technology, but currently uptake remains restricted to specific wards, often those involving extensive surgery and lengthy recuperation periods.

A variant of the embedded glass tag for pets has recently been certified for use with humans. The so-called Verichip is easily implanted using a syringe but requires a minor surgical procedure for its extraction as it binds to

human flesh. It has been used in a small number of applications (for more details see Chapter 9) notably to establish the VIP status and provide payment facilities to patrons of a nightclub chain in Europe, which has attracted extensive publicity. Other applications are less benign, and there have already been proposals for its use to tag military personnel and migrant workers in the United States. Unsurprisingly, the availability of this tag has raised very considerable concerns and highlights the ethical issues related to RFID use.

## 2.5 RFID Standards

Looking at the different applications of RFID, it immediately becomes evident that each specific domain has its own priorities, norms, and preferences. This is reflected in the standardization process, which has followed distinct and often incompatible paths in establishing the operating parameters of RFID systems as specified for a particular domain of application. This is despite the fact that many of these systems share many common features and could potentially benefit from lessons learned in a different domain. This is not the case, though, and in practice RFID standards are numerous, often incompatible, or mutually exclusive. Yet support for standards is a core ingredient, especially for open systems.

The most prolific producer of RFID standards over the years has been the International Organization for Standardization (ISO), which has issued almost 50 different specifications, several of which have many parts. Navigating the numerous ISO standards is a complex exercise, and we will not attempt to do so in this book. Instead, we note that especially in the context of the supply chain and UHF tags specifically, EPCglobal represents a considerable challenge to ISO, with several of its systems already established as the *de facto* standards.

### 2.5.1 EPCglobal

To be sure, EPCglobal provides the *de facto* standards for RFID tags in the UHF range. Since its founding as the Auto-ID Lab, EPCglobal has provided the critical mass of technology providers and FMCG sector support to develop and evolve a variety of standards for the supply chain. Without a doubt, this work has played a central role in extending the popularity of RFID. Unlike those of the ISO, EPC standards are tightly controlled by specific industrial interests, and it is doubtful that they can represent the concerns of all involved in the multifarious applications of RFID.

This point is of particular significance, especially in the context of general purpose computing, as the declared objective of the work of EPCglobal is to construct the Internet of Things in the sense of establishing a common ground for the development of open and shared infrastructures for auto-identifiable networked objects. However, this is where the similarities between EPCglobal



and the internet standardization process stop: the structures and aims of the two systems are fundamentally different.

EPC and related standards have been developed in competition with the ISO which has been working on a comparable system, albeit at a much slower pace. After several years of conflict, it seems that there are now encouraging signs of collaboration with the EPC Class 1 Generation 2 tags (further discussed in Section 3.2.4).

### **2.5.2 ISO 14443**

ISO 14443 specifies a class of RFID proximity tags that are particularly well suited for ticketing applications. This standard comes in different parts and is relatively complex as it provides for payment and as such support for relatively complex exchanges between the card and the reader. Such cards operate in the 13.56 MHz band and use the magnetic field created by a reader coil antenna, and they typically have a range of a few dozen centimeters. We will take a closer look at the structure of the tag and its supported protocols in Section 3.2.2.

### **2.5.3 ISO 15693**

ISO 15693 specifies a class of RFID vicinity tags similar to those of ISO 14443 in that they also operate in the 13.56 MHz band and use the magnetic field created by a reader coil antenna. However, ISO 15693 tags have a far greater operating range which can be between 1 and 1.5 meters, but support only relatively simple exchanges, primarily the transmission of a unique identifier code.

### **2.5.4 ISO 15459**

ISO 15459 defines a class of unique identifiers for transport units, including supply chain items and containers, returnable assets, and product groupings. It also outlines registration and code address space management processes that re-use existing ISO standards and procedures. In this role, it is roughly equivalent with the specifications of the different serialized electronic product codes developed by EPCglobal and similarly relates to pure identifiers that can be subsequently represented in multiple forms, including bar codes and RFID.

### **2.5.5 ISO 18000**

ISO 18000 is an all-encompassing specification for RFID air interfaces and aims to provide a comprehensive reference for all frequencies and types of tags, including LF, HF, UHF, and microwave active and passive tags. Each section



of the standard describes the physical layer specifications for communications between reader and tag, the protocol and the commands, and specific anti-collision and singulation methods (see Chapter 4).

ISO 18000 was first published in 2004 and has been in direct conflict with the EPC Gen2 specifications developed in parallel. The 2006 revision of the standard offers certain modifications (discussed in Chapter 5) that cater to better interoperability between the ISO and EPCglobal systems at the air interface layer. However, standards at higher levels of the protocol stack remain incompatible, and both systems follow their individual divergent paths. EPCglobal has distinct advantages, especially in terms of vendor support, but ISO compliant serialized identifier systems, for example ISO 15459, also have advantages related to intellectual property and subscription costs.

## 2.6 Summary

In this chapter, we outlined three applications of RFID that highlight how the technology is used in many practical situations. Yet RFID applications have very different characteristics and as such very different requirements. The result is that there is no single solution or system blueprint that would be appropriate for every application domain and every deployment. Instead, in this book we aim to describe a collection of different techniques, designs and solutions that system designers can mix and match and tailor to their specific requirements. One factor that plays a central role in this is related to system size and parameters. To help with the decision process, we summarize the different aspects of the three application domains discussed so far in Table 2.1 as a guide to similarities with the designs that we will discuss in subsequent chapters with reference to these applications.

**Table 2.1.** Characteristics of three large-scale industrial RFID applications.

	<i>Ticketing</i>	<i>e-Passport</i>	<i>Supply Chain</i>
Tag Density	Low	Low	High
Tag Range	Short	Short	Long
Tag Lifetime	Medium	High	Medium
Tag Complexity	High	High	Low
Tag Security	Strong Crypto	Crypto (known key)	Password (32-bit)
Network Support	Delay Tolerant	Local	High—real time

<http://www.springer.com/978-1-84800-152-7>

Networked RFID

Systems, Software and Services

Roussos, G.

2008, XVI, 187 p. With online files/update., Softcover

ISBN: 978-1-84800-152-7