# Chapter 1
# An Introduction to Smart Cards

**Keith Mayes**

**Abstract** When we released the original version of this book, back in 2008, we stated that the concept of a smart card was not particularly new, but that the practical use of smart cards in a range of diverse applications had never been more popular. Eight years on and the statement is still valid, although we have seen some trends towards certain types of smart card and applications, and indeed more focus on embedded smart/secure chips that do not rely on the card form factor. Furthermore, we have seen the introduction of Near Field Communication (NFC), which permits mobile phones to emulate smart cards and readers. This chapter provides a first introduction to a wide range of smart cards and tokens, considering the various types, capabilities, popular applications and the practicality of their development and deployment, covered in detail within subsequent chapters.

**Keywords** Smart cards · Tokens · Security · Applications · Java · MULTOS · RFID · SIM · ID Contactless · Microprocessor cards · Chip card · Magnetic Stripe card · Memory card · Development · Lifecycle · Tags · IoT · NFC · MIFARE Classic

## 1.1 Introduction

Smart cards, and in particular the specialist chips within them, are perhaps some of the most widely used, but underestimated electronic security devices in use today. In many cases these devices are in the front line, defending citizens and systems alike against attacks on information[1] security. Because they have tended to be small and often concealed, smart cards have carried on their important work, largely unnoticed, but this is changing. High profile use of smart cards for IDs [1], passports [2], credit cards [3] and e-tickets [4] means that the smart card is now a regular topic for the

[1] Note within this book we use the terms information security and cyber security interchangeably.

K. Mayes (✉)
Director of the Information Security Group, Head of the School of Mathematics and Information Security, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
e-mail: keith.mayes@rhul.ac.uk

© Springer International Publishing AG 2017

K. Mayes and K. Markantonakis (eds.), *Smart Cards, Tokens, Security and Applications*, DOI 10.1007/978-3-319-50500-8_1

popular press. With all this activity and positive momentum, one would expect that the term smart card has a clear definition and the physical devices would be easy to identify. Unfortunately this is not the case and ambiguity abounds, so the first priority in this book is to provide some clarity and definitions to be used within the chapters.

## 1.2 What Is a Smart Card?

It is perhaps a little surprising to start a smart card text book with such a trivial sounding question as "What is a smart card?". However, judging by some press articles and even technical reports, the answer seems to elude even the great and the good.

Normally at this point, a text book would dive into the ancient history of card evolution, which basically says we have such wonders because some rich guy forgot his wallet one day. However, this can add to the confusion regarding what is, or is not, a modern-day smart card, so the history trip will come later once we have a few definitions to work with.

Part of the problem stems from the use of *smart*. If a system is much more convenient because a particular card is being used then that is a pretty smart thing to do, even if by technical standards the card is unremarkable. The next problem comes from *card* which to most people would imply say a credit card sized piece of plastic, whereas various sizes are possible and indeed the innards of the device could be embedded in something completely different, such as a passport or phone.

The candidates that could be described as smart cards are therefore numerous and so our definition will be refined a little to weed out some of the least relevant.

A smart card

1. has a unique identifier,
2. can participate in an automated electronic transaction,
3. is used primarily to add security and
4. is not easily forged or copied.

   In support of (2) and (3), two more definitions will be added, i.e.
5. can store data securely,
6. can host/run a range of security algorithms and functions.

This definition will now be applied to a few well-known card types to see if they are truly *smart*.

### *1.2.1 Magnetic Stripe Cards*

Magnetic stripe cards are still widely used in a range of applications. They are characterised by being low cost and relatively easy to read/write. An example is

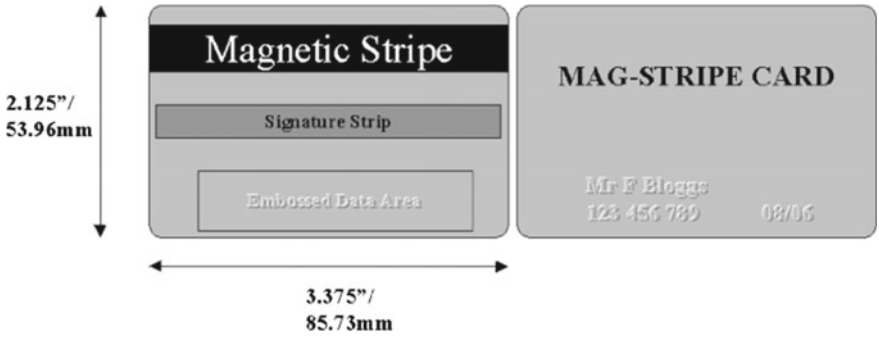


**Fig. 1.1** A typical magnetic stripe card

shown in Fig. 1.1. For many years this type of card was used for credit and debit card financial applications, although in Europe it is being phased out by EMV cards described in Chap. 5. The cards are used throughout the world and indeed for a diverse range of applications including entitlement cards, tickets and access control systems.

In terms of our smart card definitions, the magnetic stripe card can be regarded as follows:

- It has a unique identifier,
- it is clearly involved in electronic transactions and
- in many cases it is *meant* to provide some security element; unfortunately it is very poor when tested against the fourth definition, as it can be copied or forged.

Considering Fig. 1.1 in closer detail, we have a piece of plastic which is used as a carrier for a stripe of magnetic tape. The plastic card may also carry some text or images designed more for human interpretation and checking rather than the electronic transaction that is of primary interest. Invisible to the human eye is the information stored within the magnetic stripe. The stripe is not dissimilar to that used in an old cassette recorder, i.e. a strong magnetic field controls the alignment of magnetic dipoles into various orientations along the length of the tape. The alignment is preserved even when the polarising field is removed and so information is stored by the dipoles. The alignment can be simply tested and the information recovered by a tape reader head. Because the tape and the equipment used are relatively crude, the information storage capacity is quite limited. To maximise this in a practical manner, multiple tracks are stored along the stripe, again similar to an audio tape recording. On each track one can store a few bits of identity-related information and the method of storage is known as Wiegend [5] format. A fairly exhaustive description of these cards is beyond the scope of this book and the curious reader can consult another reference [6].

The important thing to say about magnetic stripe cards is that they are not smart cards because they fail the fourth smart card definition and quite disastrously too. It is therefore astonishing to see how long they survived in financial applications. The root of the problem is relatively easy to find. The magnetic stripe is not much

more than a piece of audio tape and so it can be easily read and indeed rewritten with relatively simple equipment. This means that it is quite trivial to forge/clone magnetic stripe cards. A lot of effort has gone into making the plastic carrier harder to duplicate (although with limited success), but there is not much that can be done about the magnetic stripe used in the automated transactions. Two types of magnetic stripe fraud [7] have become legendary:

- Skimming—here the information from a valid card's magnetic stripe is copied to another card for use in fraudulent automated transactions.
- Counterfeiting—here the plastic carrier/card is very carefully copied, but the magnetic stripe may be blank or invalid.

How a skimmed card may be exploited is fairly obvious, but counterfeiting deserves a few word of explanation. Although there are various countermeasures on cards to discourage counterfeiting, such as special graphics, embossed printing and holograms, they really just represent more inconvenience and time for an attacker, rather than serious obstacles. The counterfeit is to fool a human operator rather than an automated process, so how can this be useful when most physical transactions tend to be automated? The reason is that it is a very common occurrence for the magnetic stripe on a valid card to be unreadable due to wear and tear. This has lead to an acceptance for the manual fall back mechanism. For example, a person goes into a petrol station to buy fuel. The assistant swipes the card once, twice, rubs the stripe on his/her sleeve and tries once more but in vain. He/she then simply reads the numbers printed on the card plastic and types them into the point of sale terminal to complete the transaction. For Internet purchases it is even easier as there is no attempt at an automated process and the attacker only needs to have read the required information from the source card, rather than create the counterfeit.

Because of the prevalence of skimming and counterfeiting, magnetic stripe cards are no longer be recommended to safeguard significant financial transactions. Far better is the electronic chip-based solution standardised by EMV and described in detail within Chap. 5. The EMV solution is now the standard in some countries such as the United Kingdom where it has drastically reduced fraud for card-holder-present transactions [8] (e.g. physical transactions in a store). However, EMV has not yet delivered similar safeguards for the increasing volume of Internet transactions which is now the most worrying form of fraud and hence the industry focus for countermeasure development.

There can be a future for magnetic stripe cards where the solutions are very cost sensitive and the cards are not protecting anything of significant value, for example a loyalty card or a library access card. The lack of reliability of the stripe is perhaps not a problem when the cards are only required to have a limited lifetime and usage. For all other applications the trend is towards the use of electronic chips embedded within the card, in order to improve, functionality, reliability and security.

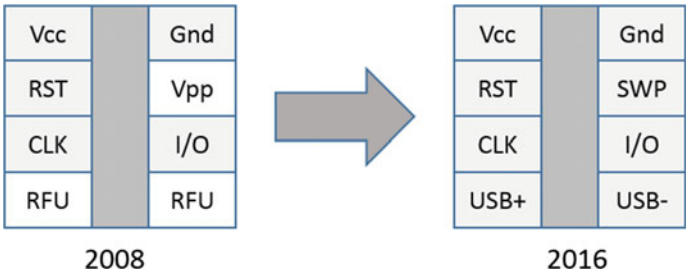


**Fig. 1.2** Contacts of a chip card

### *1.2.2 Chip Cards*

As the name suggests a chip card is basically a plastic card, rather like the magnetic stripe card, that has an electronic chip embedded in it. Historically, these cards were easy to identify by virtue of the contacts that were usually gold or silver coloured. The use of these contacts is described within standards [9] and a traditional example is shown on the left-hand side of Fig. 1.2. As a minimum, the contacts provide power to the chip via Vcc/GND, a communications I/O line, plus clock (CLK) and reset (RST) lines. The Vpp pin was once used for re-programming old-style EEPROM memories, but is now obsolete. Because the two lower pins were historically unused and Reserved for Future Use (RFU), some cards and readers only make use of the six upper contacts. However, some industries have already standardised the use of the old RFU and Vpp contacts for new services. Referring to the right-hand side of Fig. 1.2, we can see how mobile communication standards have re-specified the spare pins for a high-speed USB interface and for a Near Field Communication Single-Wire Protocol (SWP) [10], as described in Chap. 4.

A contact chip card is accessed by placing it within a card reader which simply makes physical contact with the metal pads, allowing the chip to be powered, clocked and for communication to take place. The low-level electrical interface is described in ISO standards [9]. Communication is half-duplex, with the reader/host taking the role of master and the card the slave. There are in fact two low-level protocols that can be used to exchange information, known as T = 0 and T = 1 and both are defined in ISO standard [9]. The T = 0 protocol is favoured by the mobile communication industry and is simply a byte interface where information is sent a byte at a time, rather like communicating with a modem over a serial link. By contrast, T = 1 is a block protocol favoured by financial institutions.

One could fall into the trap of assuming that all chip cards are more secure than magnetic stripe cards and that the presence of the gold contacts implies that this is a smart card. These assumptions are incorrect and dangerous.

The simplest chip card could contain a single fixed value. The application protocol would simply be to read this fixed value for comparison. It would be trivial for an attacker to read the value from a valid card and produce a copy and so this type of card fails our fourth smart card definition in the same way as the magnetic stripe card.

Another type of card is the memory card that may be used to perhaps keep a count of purchased telephone call minutes or accumulated loyalty points. Such cards might not have added security and so contents may be easily read and copied. Moreover, the memory may be rewritten to undermine the application or change IDs. The simple memory card also fails our fourth requirement for a smart card as it can be easily copied or modified. Note that there are memory cards that incorporate fixed functionality security (often proprietary), which we may refer to as secured memory cards (e.g. MIFARE DESFire EV1) used in popular systems. However, as we are interested in more general-purpose security devices the focus moves towards microprocessor chip cards. Sometimes these chips are referred to as secure microcontrollers rather than microprocessors; we will use the terms interchangeably within this book.

### *1.2.3 Microprocessor Chip Cards*

Microprocessor cards have the scope to satisfy the requirements for a smart card because they are not only able to store and communicate stored values, but can do so within the context of security protocol programmes. The protocol interface to the device can be defined such that it is logically impossible to extract information, or to reprogramme the contents without appropriate permissions which are checked and enforced by cryptographic functionality. At first glance one would think that the search is over and that the presence of a microprocessor chip card is synonymous with a smart card, but this is not the case. A conventional non-specialised microprocessor card can give you logical security, but that is insufficient for a smart card. Attackers are not put off by logical security, but would employ a range of techniques that attack the chip directly or exploit information leakage from an operating device. These attacks are described in detail within Chap. 9, but suffice to say that a microprocessor used in a smart card is designed in a very specialised way to be "tamper-resistant" [11]. This is perhaps the most important property to remember about a smart card. When considering conventional smart cards our definition could be as shown below.

- A smart card contains a tamper-resistant microprocessor chip (incorporating countermeasures against known attacks) that is difficult to forge or copy. It includes a unique ID, can participate in automated electronic transactions, can store data securely and run/host a range of security protocols and algorithms.

The consideration so far has focused on traditional smart cards that make use of electrical contacts to the chip. However, there is growing interest and usage for cards that do not have physical contacts, but exploit radio techniques instead.

### 1.2.4 Contactless Smart Cards and RFIDs

The smart card industry tends to talk about cards with contacts or contactless smart cards; however, industries that have been concerned with tagging, product coding and tracking, tend to talk about Radio Frequency Identification (RFIDs). If the definition of a smart card has been much abused then so too has RFID. Because of this someone may refer to a contactless smart card as an RFID or vice versa. This section will try and remove some of the ambiguity, but there will still be a grey area of overlap.

In principle, RFID is very simple to define. It is a device that presents an ID to a reader device via Radio Frequency (RF) means. It does not imply any protocol security, clone prevention, or tamper resistance; however, some real-world devices may incorporate such measures. It might even be argued that a magnetic stripe card should be regarded as a RFID, as it makes use of an electromagnetic field to communicate, although its probably best to ignore this possibility as there is enough confusion already.

A chip card that presents an ID (perhaps for door access) could therefore be considered as a special case of an RFID.

Generally, RFIDs tend to be less sophisticated than contactless smart cards (although there is no fundamental technical reason for this) and are not restricted to the physical card format. Whilst lower layer protocols tend to be standardised [12], a worrying aspect is that the application layer is often proprietary and the design information is held secret. From a security perspective the reliance on secret proprietary protocols and algorithms is always treated with much scepticism and nowadays we have a *classic* example to show why.

### 1.2.5 The MIFARE Classic

When we were writing the first edition of this book we knew a few things about the MIFARE Classic [13] product from NXP.

- It used a proprietary secret algorithm (CRYPTO1).
- It was intended as a medium (rather than high) security memory card.
- It was very widely used.
- It was quite old, and newer products were available.
- Its keys were small (48-bit) compared to best practice.
- There were data sheets (from 2004) of seemingly *unauthorised* products.

With such small keys the security was reliant on the secrecy of the CRYPTO1 design, which violates Auguste Kerckhoffs principle [14] and is a example of the much criticised *security by obscurity*. If the algorithm becomes known then it can be coded into a key cracker to determine the secret keys, and therefore the existence of the data sheets was worrying. It suggested that no later than 2004, the product design, including the algorithm, had already been reverse engineered or otherwise

copied. In simple terms, the demise of this product was a question of when and not if. It actually came about from some more reverse engineering [15], but this time the goal was publication rather than commercial gain. Publishing the algorithm was enough to compromise the product; however, once exposed to expert scrutiny, major flaws were discovered, as is often the case with ageing proprietary designs. To cut a long story short, a key cracker was not necessary; a simple laptop would do. It was possible to tease secret keys out of readers and eventually access and modify keys and data in legitimately issued cards. In defence of the MIFARE Classic it was a very popular and useful product, and when first launched there was little to better it as a contactless secured memory card. It was geared towards speed and usability rather than high security, and NXP had higher security alternatives at the time the Classic was hacked. The system owners that used the products bear some responsibility as although the algorithm was secret, the key size was known to be 8-bits smaller than the already obsolete single-key DES, so would not have passed a system security review.

### *1.2.6 Smart Tokens*

In this book we may mention smart tokens. A smart token can be considered as a personalised device that has all the useful security, functional and tamper-resistant properties of the smart card, but is not provided in a normal plastic card format. Interestingly the smart card that is most prevalent in the world, the mobile Subscriber Identity Module (SIM), might be regarded as a smart token. Whilst it started life in the full-card format and is still produced by a card manufacturing process, it is commonly used in the plug-in format, see Fig. 1.3, although mini and nano formats are now in use that are even smaller than the plug-in, being not much bigger than the contact module. Just about any format is possible and a range of communication and powering methods could be considered.

One thing that is clear from looking at the types of device and their names is that there is a lot of overlap. The literal explanation of the device name and or acronyms might once have been simple and accurate; however, the names have

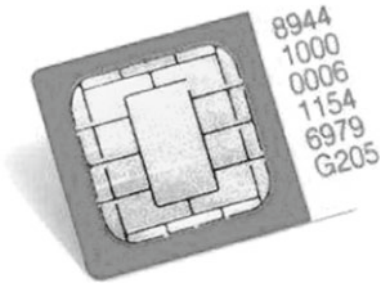


**Fig. 1.3** A plug-in format SIM card

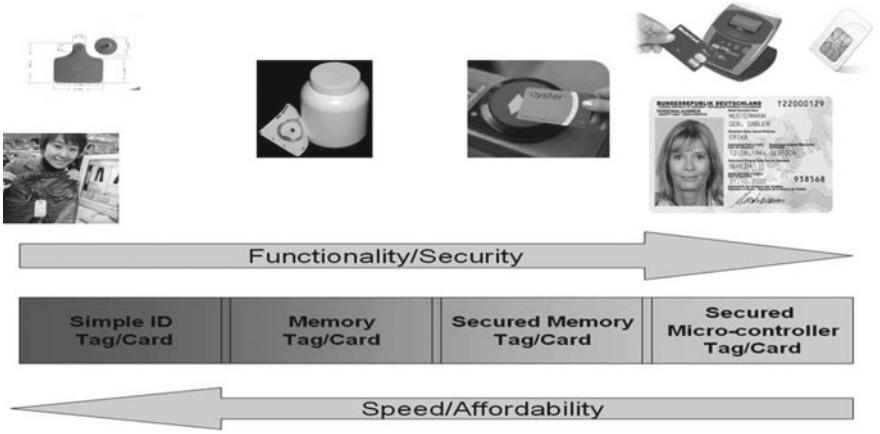


**Fig. 1.4** Smart card-RFID range and trade-offs

evolved in the public perception, e.g. no one thinks of a card that is smart in some way, but rather of a smart card. Similarly it is doubtful that anyone will remember that RFID is strictly an ID presented via radio frequency means, because RFID has simply become a modern word. Most often we are concerned with passive contactless cards/RFIDs that extract their power from the readers' electromagnetic field and then modulate the field to communicate. A range of these devices are illustrated (along with contact card types) in Fig. 1.4. On the left-hand side of the figure we see the simpler types that may just present an ID without and security protection, as might be found in simple product or animal tagging. The memory cards might have very simple access control or none at all, put permit storage of information additional to an ID such as description and place and date of issue. The contents of memory cards can be protected by cryptographic Message Authentication Codes (MACs) and kept confidential by means of cryptography; however, a major weakness is that the contents may be copied, swapped or used in clones. Secured memory tags may offer mutual authentication and strong confidentially, integrity and access protection; however, a careful choice of product is required to avoid the kind of problems that arose with the MIFARE Classic vulnerabilities. The right-hand side of Fig. 1.4 illustrates the most significant types of secured microcontroller devices such as those found in passports, bank cards and mobile phones. One might imagine that using the more inferior types is just due to cost constraints; however, this is not always the case. For example, smart transport tickets have very tight operational time constraints in order to avoid throughput and safety issues at station gates, and it is easier to achieve this with a fast secured memory card than a sophisticated microcontroller. If you are fortunate to have a service or system where security risk is not an issue then the ID cards will do; giving you not only a cheap/fast tag, but avoiding key management and reader security issues. You may also be constrained in your choice by other factors such as temperature, waterproofing, lifetime, robustness and tolerance to read range and shielding.

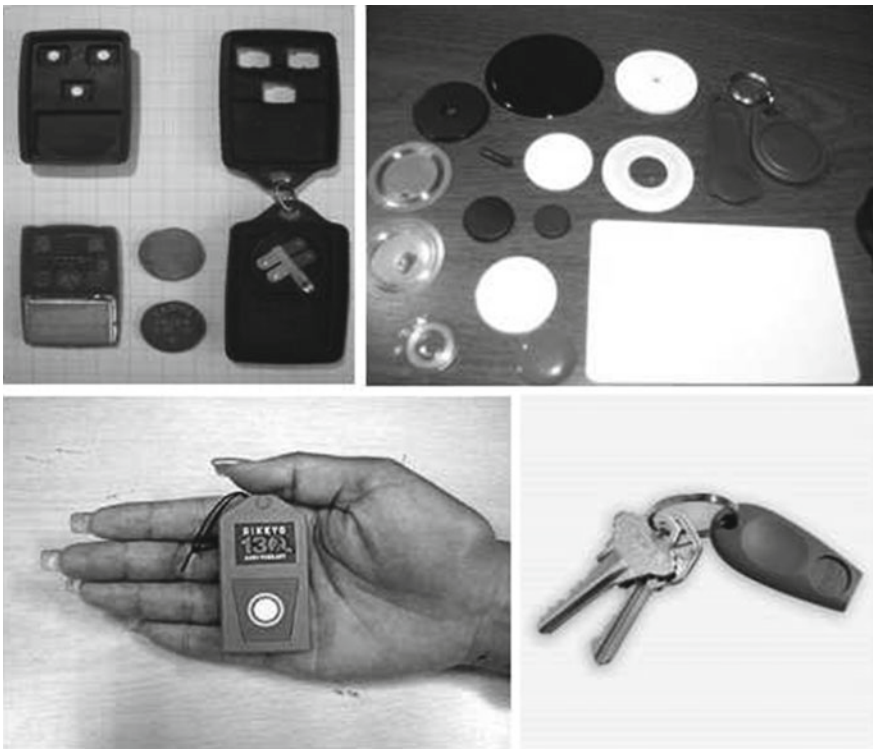


**Fig. 1.5** Active RFIDs

There are also active RFIDs that incorporate their own power sources. A common example is the keyfob for remote central locking of a car. Active RFIDs/tags also tend to be used where passive devices would struggle, for example, situations requiring a long read range or where there is a lot of metal that can adversely affect the electromagnetic fields used by passive devices. Some conventional examples are shown in Fig. 1.5. Although it is not normally thought of this way, the mobile phone is the most widespread active RFID, as it has a unique ID, a power source and its own radio transmitter. Furthermore, the mobile phone is a very sophisticated and location aware RFID, with multiple radio bearers, support for cryptographic protocols, application hosting and a direct user interface. This has led to some privacy concerns, because for a mobile network to function it has to dynamically track the location of mobile phones (and hence their users) in order to route calls.

Just in case we do not have enough names and confusion, we must also be aware of Near Field Communication (NFC) [10]. The simplest way to describe this is as a contactless/RFID interface for a mobile phone. Essentially this now standardised functionality allows the phone to act as a contactless smart card/RFID or indeed as the reader to communicate with an external card. For the card emulation aspects a hardware Secure Element (SE) is normally used, which has much in common with

a conventional attack-resistant smart card chip, but can be provided in the phone in a variety of ways; within the SIM itself, as a separate chip on the phone Printed Circuit Board (PCB), or as a chip in a plug-in memory card. It is also possible to have a software emulation of a SE, such as in Android Host Card Emulation (HCE), although the attack-resistant capabilities of this approach are considered inferior to specialist hardware.

For the remainder of this book, unless there is a particular need to differentiate devices, the name smart card may be used to represent all types of device incorporating a tamper-resistant microprocessor chip supporting secure data storage and security functions/algorithms. In most cases the actual physical format and low-level communications interfaces will be ignored. This serves to illustrate that what is of real interest and value is the chip at the heart of the device. The term RFID may be used for simpler radio frequency tags.

## 1.3 Smart Card Chips

The microprocessor found in a smart card bears little resemblance to the processor you will find in a modern PC although the core of the smart card chip is not dissimilar to some of the PC's early ancestors. Smart card chips tend to be very small and so there is always a limit to what functionality and resources can be crammed in. There are several historical reasons for the size limitation. First, the cost of a chip is proportional to the area of silicon used and although individually, this may not be a lot, smart cards may be ordered in their millions and so are always very cost sensitive. Second, because smart cards are often delivered via the normal post they must withstand bending and twisting stresses. If the chip is too large then these stresses will break the chip or the wires connecting the chip to contact pads or antennas. Third, as the chip gets larger and more complex, its power requirement would normally increase. Host devices tend to be quite miserly when supplying power and even if they were not, there could be heat dissipation problems within the module. Finally, because of its security purpose, the essential code and functionality should be kept as small and as simple as possible, so it can be exhaustively reviewed and tested to the stringent levels required by standardised evaluation criteria. The amount of code that any CPU must trust in order to enable a secured operation is known as the Trusted Computer Base (TCB), and in a smart card this is very small indeed.

When the first edition of this book was written we were wondering whether in the future, some of the restrictions on smart cards might ease, especially for mobile communication smart cards, with the capability for devices with large memories, faster interfaces and processors [16]. While some of this has appeared in standards, practical adoption is harder to find. In fact the smart card has been kept steadfastly simple, with manufacturing and technology advances being used to mainly reduce the size and cost of chips. Therefore, we will stick to conventional chips and an old-style layout is shown in Fig. 1.6. As mentioned previously, the device has no clock or in-built power supply, but it does have a CPU and three types of memory as well

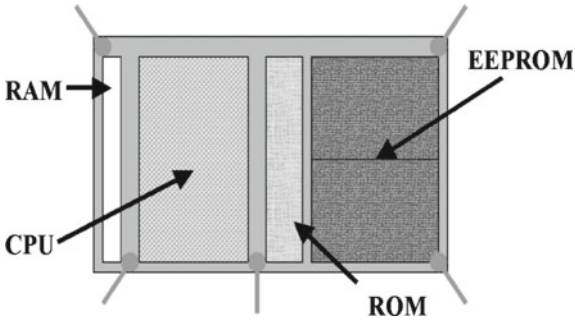


**Fig. 1.6** A smart card chip (old)

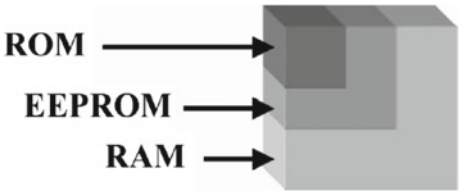


**Fig. 1.7** Comparison of chip area needed for various memory types

as the interconnecting circuitry. Understanding the types of memory is important as what is stored where is usually a trade-off decision for the designer.

The Read Only Memory (ROM) is some times referred to as the chip mask. It is characterised by the fact that its contents (which are identical for all cards in the batch) can only be set/written to, during card production and then only read during normal card operation.

The Random Access Memory (RAM) is used for fast dynamic storage of programme run-time variables and the stack. In this respect it is similar to the RAM in a PC although there is much less of it. When power is removed the RAM loses its contents.

Electrically Erasable Programmable Read Only Memory (EEPROM) is very useful as it can be programmed after manufacture and does not lose its contents when the power is removed, i.e. it is non-volatile.

Looking at Fig. 1.6 one could easily get the wrong idea about the likely proportions of RAM, ROM and EEPROM. This arises because the memories have different packing densities, i.e. how many bits fit into a given silicon area. ROM packs best of all so is an area and cost efficient method of storage; however, the fact that it cannot be rewritten is a serious drawback, making it useless for user data and flexible function storage. For well-tested common functionality and constant data it is fine. Next best for efficiency is the EEPROM, which can be used for all kinds of data and application storage. RAM packs poorly and is very restricted, which is a challenge for programme developers that is only likely to get worse as application sophistication increases.

A typical relationship between the memory types and areas is shown in Fig. 1.7.

We must also mention another important type of storage known as flash memory. This is well known for memory sticks, but it took a while to be adopted in smart cards.

Flash memory takes the place of the ROM and the EEPROM and is becoming the dominant non-volatile memory type in smart cards. It has a number of advantages that make it attractive when compared to EEPROM. First, an EEPROM memory ages, i.e. it can only be written to a certain number of times (few hundred thousands), which can limit the lifetime of certain card applications. A flash memory does not have this problem and is also much faster to write. The designer does not have the same ROM/EEPROM dilemma as the split can be adjusted during the design phase, although it must lock down the flash equivalent to ROM space after production, for security reasons. RAM is still at a premium, as for the traditional smart card case. For the manufacturer there are also advantages as it is not necessary to create many different customer masks as the different configurations can be soft loaded. One potential drawback is that any soft loading may take extra time in production and whereas the chip cost is proportional to chip area, the cost of the final smart card is proportional to the production time. Finally, some card Issuers still have concerns about the security of flash memory technology and may simply forbid its use in their product specifications; although this viewpoint is becoming less common.

For now we will stick with the concept of real RAM, ROM and EEPROM within our smart card device, although remembering that flash can replace both ROM and EEPROM. The use of RAM is quite evident and so the first question to consider is what can be put in the ROM for maximum benefit. Typically, the ROM would contain the operating system, well-tested common functions and constant data. The EEPROM can be used for user data, user programmes as well as general application data and functions that require modification during operational life. Sometimes a proportion of the EEPROM is used for functionality that would just not fit in the ROM and/or patches to compensate for the bugs and extensions of the ROM programmes. The EEPROM is used for essential non-volatile application data storage, including personalisation information.

EEPROM is a very useful resource, especially as there are techniques to update its contents whilst in the field. Therefore, to create a future proof device one would try and issue a larger smart card with plenty of spare EEPROM to accommodate fixes and new functionality. However, this increases the chip area and hence cost, which means it will be resisted by whoever is signing the cheque for the next million devices. The battle between the alien mindsets of designers/strategists and purchasers is quite a common occurrence. On the one hand you have the purchasers arguing for savings today, whereas the designers/strategists push to spend more now to avoid future problems from built in obsolescence. Unfortunately modern business has a very short-term focus and so the head-in-the-sand savings argument wins far too often.

## 1.4 Tamper Resistance

One of the key strengths of the smart card (which really means the chip) is its tamper resistance, i.e. the ability to resist known and anticipated attacks. Looking at the

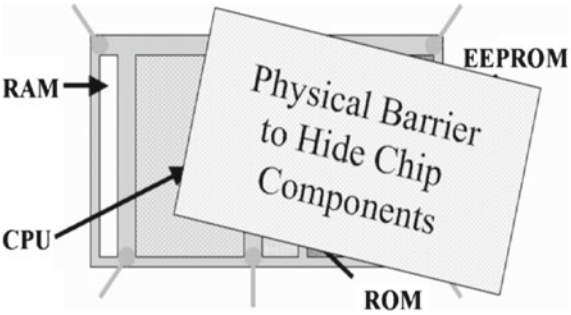


**Fig. 1.8** Smart card chip anti-probing layer

picture in Fig. 1.6 one might think that the attackers job is not so hard as its very easy to identify the attack targets such as memories and busses that might yield valuable secrets and permit card cloning. However, this is not the case and the chip layout shown is very old and presented for clarity of explanation. In reality the first thing that an attacker may encounter is a physical layer of silicon that prevents probing of the circuit (see Fig. 1.8).

If this can be overcome then there may be an active current-carrying layer, so that any break renders the chip useless to the attacker. Get beyond this layer and you may find that the circuitry has been scrambled making it difficult to find the attack target. If a bus or memory is eventually found then it may well be encrypted. Clearly if an attacker has expensive equipment, expertise and is prepared to destroy many cards, he may eventually extract some information, but unless this is a global secret arising from a bad design it is difficult for much advantage to be gained. Smart card attacks and countermeasures are covered in detail within Chap. 9 but for now it suffices to say that the smart card chip mounts a very robust defence, even when faced with sophisticated attacks from well-equipped experts.

## 1.5 Smart Card Characteristics

So far, a fairly glowing report has been given of smart cards; however, like any device they have both strengths and weaknesses. In order to exploit smart cards appropriately it is just as important to appreciate the weaknesses as well as the strengths. Table 1.1 presents this is a summary form. Note that the memory capacities and CPU capabilities are just typical indications, as they evolve over time.

Bearing in mind that the smart chip might only be less than 9 $mm^2$ then the processor and memory capabilities are surprisingly good. However, compared to a PC or mobile phone processor the card is rather feeble and would not be a good choice for handling large amounts of data or time critical processing. However, cards with co-processors are no slouches when it comes to specialised cryptographic processing. The main positive features include the tamper-resistant security, the precise standardisation and the resulting consistency and control. Obvious weaknesses include

**Table 1.1** Summary of smart card strengths and weaknesses

| Features | Limitations |
|---|---|
| CPU (16–32 bit) | **Helpless Alone** |
| RAM (4–16 kb) | No internal power supply |
| ROM/Flash (128–256 kb) | Externally restrictions on power consumption |
| EEPROM (64–256 kb) | No user interface |
| Crypto-processor option | No clock |
| Very small | **Limited (by PC comparison)** |
| Low power | Memory |
| Low cost | CPU speeds |
| Secure | **Issued device** |
| Standardised | Legacy cards may be inflexible |
| Operating systems | New cards require deployment |
| Development tools | |
| Multiple suppliers | |
| **Consistent and Controllable** | |

the fact that the card is helpless on its own and thus is always reliant on other system elements. For example, a conventional smart card has no internal power source, no direct user interface and (with few exceptions) not even a clock. From a system management perspective another significant feature is the ability to personalise the smart card to a particular customer or account. Smart cards tend to be issued in very large numbers and so one of the ever present problems is dealing with legacy devices. A great new service that only works on newly issued cards may take years to reach a large proportion of the customer base. Legacy problems can be minimised by forward-looking design and the use of lifecycle management systems; however, legacy problems are often "designed-in" to satisfy short-term cost savings.

One of the features that could be described as an advantage or limitation, depending on your viewpoint, is the Issuer control of the smart card platform.

## 1.6 Issuer Control

Most smart cards are given to customers by Issuers such as banks, mobile network operators, government and transport companies. Usually in the fine print of an agreement it will say that the card still belongs to the Issuer, even if the customer has parted with some money to obtain it. The reason for this is that the cards are important to the Issuers both from a business and security point of view, and so the Issuers want to retain management rights, e.g. decide what data and functionality is offered. In that respect the smart card is very different to a PC on which the customer can usually

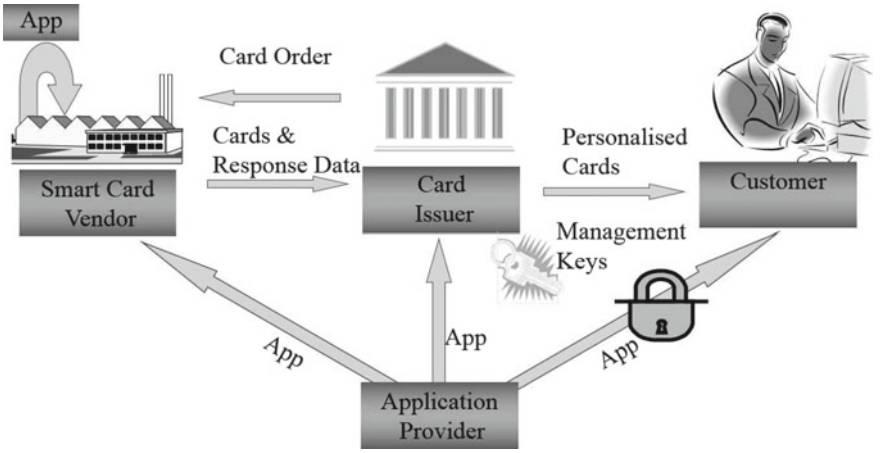


**Fig. 1.9** Smart card platform management

download any data and applications that he/she chooses. If we look at Fig. 1.9 we can see where card contents are typically created and/or modified.

Consider Fig. 1.9 and the case of putting a value added application onto a smart card. Historically the *Card Issuer* would give a specification to the various *Smart Card Vendors* who would then implement the functionality in a proprietary manner and deliver this only in newly ordered batches of cards. These days card implementations need not be so proprietary (e.g. Java Card [17] or MULTOS [18]) and there is the capability to load new data and functionality after manufacture (e.g. directly or via GlobalPlatform [19]) so the situation is more flexible. The *Issuer* or its sub-contractor could personalise the cards and load appropriate data and applications not only prior to issue to the *Customer*, but could also load/manage the card contents after issue to the *Customer*. It is therefore technically feasible for third party *Application Providers* to develop card applications and offer them direct to customers, however in practice this is extremely rare. Basically all the functionality that permits the card to be managed must also be secure to prevent abuse from attackers. The secure protection is provided in the form of cryptographic functions that rely on secret *Management Keys*. Card management is therefore only possible for the *Issuer* who holds onto these secret keys. The management functionality is quite flexible and supports the idea of multiple security domains on a smart card with delegated management, although it is unlikely to be used in practice. An *Issuer* would likely argue that its control is a positive thing as it ensures tight management of the card contents and behaviours and thereby maintains security; however, there is a risk that frustrated application developers will implement on alternative and more open devices, in order to give customers the services that they desire.

## 1.7 Current Applications for Smart Cards

Smart cards are used in many current and real-world systems and are proposed for many future applications. In fact the capability and numbers of cards are growing rapidly in just about all areas of use. Some of the most notable applications include

- Mobile Communications
- Payment/Banking
- Transport
- Government Identity Cards/Passports
- Entitlement Cards/Health Cards
- Physical Access Control
- IT access control
- Satellite TV

For mobile communications the focus has long been on SIM cards; however, a smart phone with Near Field Communications (NFC) capability may incorporate a hardware Secure Element (SE). The embedded SE (eSE) is very much like an attack-resistant smart card chip that could be found in a SIM, and indeed its presence may eventually challenge the requirement for a removable operator SIM card. Computers and perhaps phones may also include a Trusted Platform Module (TPM), designed to give assurance in the correct state of the computing platform and software. The TPM chip has a very specific role and so it is not as flexible as a smart card chip; however, the attack-resistant properties are very similar.

Figure 1.10 shows an estimation (original source Infineon 2014) for the secure microcontroller chip annual market, including both smart card applications and

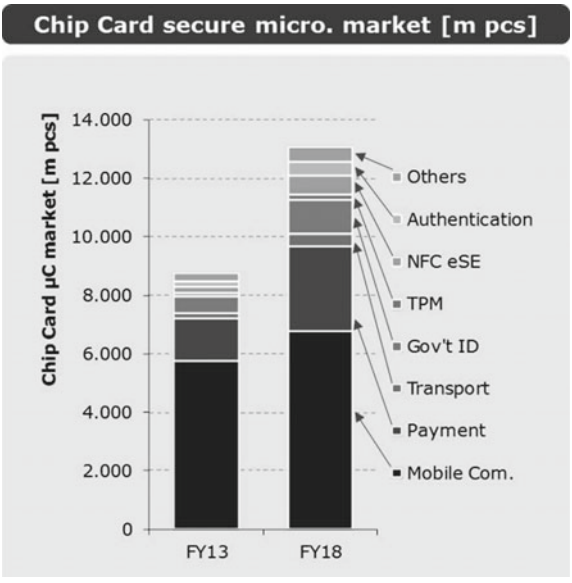


**Fig. 1.10** Market snapshot for secure microcontrollers

embedded usage. The total market volume is enormous and still growing, and was predicted to rise from around 9 billion in 2013 to approximately 13 billion in 2018. These figures are even more remarkable when it is realised that they *do not* include the simpler types of RFID, and that the forecasts did not address potential demand due to the drive towards the Internet of Things (IoT). Referring to Fig. 1.10, we see that mobile communications still dominates the market in the form of the GSM [20] SIM card and the 3G/UMTS [21] equivalent USIM card (we use the term SIM to refer to both). Although there is always discussion around SIM cards being abandoned for embedded chips, it has not happened in a big way yet, and Mobile Network Operators (MNO) are resisting the change. At the time of writing there are over 4.5 billion mobile phone subscribers and as SIMs have become throw-away items it is not surprising that around 6 billion SIMs are being issued each year. Despite their ubiquity and reducing lifetime, SIMs tend to be amongst the most technically advanced cards in use, which is in contrast to the very simple call-credit phone cards that first appeared in fixed phone networks. After communications, payment is still in second place and its volumes have grown as the EMV chip and PIN standard has gained momentum around the world. The 3 billion estimates for 2018 might even be an underestimate considering that EMV is now establishing itself in the USA. Smart phones with NFC may eat into the touch and pay (PIN-less) EMV card transactions, but this is still quite new and users may have conventional cards even if they use their mobiles. Previous attempts to use mobiles for conventional mass-market payments have not always gone well, not because the technology is unsuitable, but because users struggle to configure, operate and manage the facility, especially when they wish to change phone type, bank or network. The use of transport smart cards is growing, although many are security protected memory cards, rather than secure microcontrollers. In the UK volumes have been driven by the very successful London Oyster card system [4], although the system now accepts EMV cards too and so the number of transport-specific cards issued in London could dwindle in the coming years.

The numbers of identity cards and passports with chips are growing steadily, and in the future national security concerns will place even greater importance on reliable proof of identity. Proving the integrity of computer platforms is also a major concern which should be aided by TPM chips. However, their numbers are not showing much growth; and in fact many of the issued chips have not be enabled for use. This is not the fault of TPM technology, but rather the cumbersome process to enable it, requiring the user to take ownership of the chip. The process steps arose to protect the user against a computer or OS provider taking unauthorised control. This user protection was a laudable intention, but in reality it has largely destroyed the usefulness of the TPM and so where platform protection does exist it is often handled by proprietary secret techniques. The number of NFC eSE chips is growing. NFC when used for card emulation has had a faltering and long drawn out start, but we are now seeing serious and potentially mass market services such as Apple Pay and Android Pay. The Apple variant, at least, makes use of a hardware SE, whereas the Android version may be making use of Host Card Emulation (HCE). The latter emulates the card in software on the main CPU of the phone, so has less all round attack resistance than

the hardware SE, but that does not necessarily mean that the overall solution has insufficient security protection.

In terms of authentication, there is also a lot of interest in entitlement cards and health cards and such systems may entail a roll out to every citizen within the service area, although national and internationally standardised and compatible systems seem some way off. Physical and IT access proliferate, but are not well standardised and proprietary solutions, still survive. There are many people watching satellite TV and quite a lot trying to hack the security. The smart cards are doing a reasonable job at defending the TV systems, but the future is not very clear as it seems there are all sorts of ways of delivering TV and other valued content to consumers and their many interface devices.

### *1.7.1 Mobile Telephony*

Chapter 4 will provide an in-depth study of the ubiquitous SIM/USIM devices found in modern mobile phones; however, no introduction would be complete without taking a quick look at the most widespread and successful smart card application of all time. It is particularly useful to understand why there are smart cards in mobile phones, especially when they are not really used like physical cards at all. To find the answer requires a little trip back into history and before the GSM digital phone standard was introduced. In the UK for example there was an analog mobile phone system in use, known as Total Access Communications System (TACS for short). Being an early pioneering system, the design emphasis was on simply making the radio/communications systems work. The fact that this was achieved with the technology of the time was an astonishing achievement, but it meant that other issues such as privacy and security were rather primitive. Essentially a mobile phone held two identifiers used to authenticate the phone/user to the network. One was the normal telephone number (MSISDN) and the other was a unique electronic serial number for the handset (ESN). When a user wanted to make a call there was a signalling exchange involving the two identifiers and if the network judged the parameters to be correct and appropriately paired, then this was a valid (authenticated) user. Unfortunately that is where the security stopped and so far "confidentiality" has not been mentioned. In fact with a radio receiver an eavesdropper could listen in to any call as there was no encryption. It was also possible to identify calling parties as the MSISDN was transmitted. Clearly, this was very bad from a confidentiality and privacy perspective and it lead to some embarrassing incidents that were bad for the industry. However, the worst was yet to come as the eavesdropper was also able to receive the ESN. In theory this should have offered no advantage as the handsets were supposedly designed to prevent unauthorised re-programming of the ESN/MISIDN pairs. Unfortunately the handset security proved weak and so it was possible to create "clones", i.e. phones with the MSISDN and ESN from legitimate accounts. The first sign of cloning was when a user received a huge monthly bill for call usage. In summary, there was a major problem coupled with a lack of confidence in handset

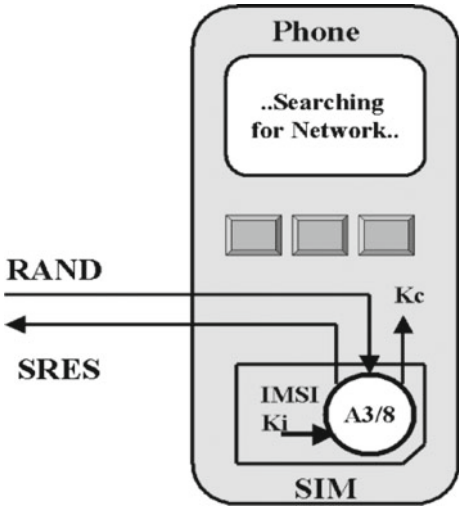


**Fig. 1.11** Phone and its SIM

security and so the mobile operators decided that in the next generation of phones (GSM) they would embed a security module in the form of the SIM card. Figure 1.11 shows the phone with its embedded SIM. The SIM incorporates a number of features that were meant to overcome the problems of the earlier analog systems, (see Chap. 4 for a more detailed description). First, it holds a customer (really card) ID called an International Mobile Subscriber Identity (IMSI). The IMSI is mapped to the real telephone number back in the network, making it harder to identify who is making a call; in fact there is also a Temporary IMSI (TMSI) that helps to further disguise the users identity. The SIM also hosts two algorithms and a secret key used for symmetric key cryptography. The naming of the algorithms is not very inspiring, but related to the candidate algorithm frameworks considered by the standards committees. Algorithm *A3* is used for authentication and *A8* is used to support ciphering. The mobile network operator has a server (called an Authentication Centre AuC) that has copies of all the card keys as well as the algorithms. Note that a network operator is free to design and use their own proprietary A3/A8 algorithms. The operation is quite simple. The AuC generates a challenge in the form of a random number RAND. It feeds this into its copy of A3 and works out the correct result for the particular card that is being authenticated. The challenge is sent to the SIM via the phone and the subsequent result SRES is then returned and compared with the expected result to decide if the SIM is authenticated. In parallel with this the A8 algorithm calculates a cipher key which is then used by the phone (A5algorithm*A5* algorithm) and the network to cipher subsequent communications. Whilst there have been a few avoidable problems (COMP128-1 algorithm [22]) the approach taken with GSM has been remarkably successful and the 3G USIM has now taken this even further by eliminating some potential weaknesses in the 2G solution (see Chap. 4).

### 1.7.2 Banking

In the last section we discussed how a major security and business problem justified the use of a smart card in mobile communications and now we see it is a similar story for credit and debit cards. In fact with bank cards you can not only improve security, but add new functionality in the form of off-line transactions supported by public key cryptography. The rationale for introducing the smart card and in particular the EMV smart card was the widespread fraud from using magnetic stripe cards. The reader is referred to Chap. 5 that explores banking cards and transactions in great detail.

### 1.7.3 Transport

The use of smart cards in transport is becoming a growth area because it offers flexibility, fraud reduction, speed and simply because users like it. The Transport for London Oyster card [4] is a prime example allowing customers to use public transport within London without the need to carry cash, queue for tickets or worry about getting the cheapest fare. There are similar systems around the world (e.g. Hong Kong [23]) and there has been interest in the use of multi-functional smart cards (e.g. credit card plus e-ticket) and mobile phones with contactless card interfaces (NFC) to make these systems even more convenient and popular.

It is worth noting that the challenges for a transport card system are a little different to say a mobile communications or financial transaction. Transport card transactions need to be fast because you cannot afford huge bottlenecks of customers at train stations or when entering a bus. This normally means that you cannot use an extra PIN code as you might with an EMV card and so we are restricted to single factor authentication (something you have). This is an operational rather than technical limitation, but it probably means you would wish to restrict the maximum value transacted in this manner. There are technical challenges in how to get enough power through the contactless interface to work rapidly. In fact there is always a very sensitive trade-off between the transaction speed, security and cost of the card. Perhaps the biggest challenge to transport systems comes from standardisation of the e-ticket. Customers would like to have one ticket that they can use for all travel nationally and ideally internationally. The use of contactless EMV cards is gaining ground in metropolitan systems, but has yet to be adopted for long-distance and expensive fare journeys. In the UK, the ITSO [24] organisation has been developing supporting national standards and requirements; however, at the time of writing the most successful UK system (Oyster [4]) is not an ITSO system, although the London card readers are expected to be compatible with ITSO standard cards.

### 1.7.4 Identity and Passports

As more and more government and regional systems move to electronic processes and transactions, it becomes necessary for citizens to have some kind of compatible electronic identity. For example, the modern passport includes a smart chip which can be accessed as part of normal travel processes. Many countries have national ID cards, some of which are based on smart card chips; however, the introduction of new cards can be emotive for countries that are not used to them. Some years back there was a planned scheme for the UK that sparked controversy, partly because of the biometric information to be stored on the card, but also because of the large amount of personal information that would sit on central databases and be accessible to numerous organisations. In the end the project was cancelled largely due to cost issues. The end user cost of passports and/or ID cards is often at least an order of magnitude greater than the best smart cards used in banking and mobile communications and so there is more than enough scope to include a technically advanced and secured chip. Perhaps the biggest problem is that the card/chip attracts all the attention, whereas much of the security challenge and indeed cost will be in the rest of the system and associated processes.

### 1.7.5 Entitlement and Health

Entitlement and health cards are perhaps good examples of smart cards that prove an identity and associate with it some private data and rights, but then so too are SIMs, EMV cards, IDs and passports. Clearly there are many reasons for a citizen to be able to identify themselves electronically and whilst smart card chips have the technical capabilities to satisfy the requirements of multiple systems and services, it appears that we will be burdened with more and more smart cards for the foreseeable future. Considering the entitlement card, how might it differ from say a passport? Well entitlement cards are likely to be issued regionally, perhaps for low-value privileges such as library access or discounted transportation. As they are part of public service delivery and often aimed at disadvantaged citizens, the cards are likely to be free issued. These factors taken together suggest that the smart card chips might be low cost with limited security and that systems from different national and international regions may not be standardised and/or compatible. Health cards by comparison are likely to have similar cost pressures, but are more likely to be standardised at least nationally. Data privacy is the major factor for any system that is used to secure health records, as misuse of this information could lead to discrimination and could damage an individual's relationships and reputation. It is therefore vital that a health smart card is not only very secure (despite the cost pressures), but that it underpins a complete system that has been rigorously evaluated for the protection of citizen's private health information.

### 1.7.6 Physical and IT Access Control

It is quite common for employees to be given an ID card to gain access to their place of work. Unfortunately, the cards are often not very smart, e.g. either the simplest of contactless smart cards or perhaps magnetic stripe cards. Where a magnetic stripe card has been replaced by a contactless card it may have had more to do with a desire to improve reliability than security. In fact the very simplest contactless cards are the classic RFIDs. They present an ID by radio means with no attempt at adding security or disguising the transmitted ID. As an RFID may be remotely eavesdropped (sniffed) you might even argue that the simplest cards are less secure than magnetic stripe as you at least need possession of the latter to read it! The real reason that these cards are used is that the companies consider that a sophisticated attack will not be used to gain access, basically because there are much easier ways. Cards often get left at home, lost or destroyed by various means and it is an operational challenge to know if every card in the company database exists (or not) and whether they are all still in the hands of authorised employees. Stealing a card is the easiest way to gain access, but you can raise the security bar a little by requiring employees to also enter a PIN code, although this impacts on the convenience and the flow through access points, as well as the operational management of PIN codes for forgetful humans. It is interesting to note that IT access control can be more sophisticated than physical access control especially as physical access might allow a criminal to steal all the company assets including the IT systems! Smart cards for IT access are issued for good security reasons and normally with the support of the IT department who are well used to managing user accounts, passwords and PINs. IT hardware and software is generally expensive and so the cost of the smart cards readers, whilst not negligible, is not a huge cost impact and so it should be possible to buy cards with reasonable capabilities. Normally these would be compatible with IT defacto standards, e.g. for access to Microsoft Windows.

### 1.7.7 Satellite TV

Whilst commerce used to centre around the exchange of physical items, today's customers are keen to buy less-tangible goods that have no less perceived value. In the digital multi-media domain we may want to watch something or listen to something for our entertainment and therefore have to pay for the right. The control of this is generally called Digital Rights Management (DRM) [25] and a good example is satellite TV where a customer can decode a transmitted programme, such as a football game, if he/she is in possession of a set-top-box receiver with appropriate security functionality and rights. Satellite TV is very desirable and not particularly cheap and so is a prime target for hackers. Defending the rights is not trivial as this is a broadcast media and so there has to be some global secret elements. Various security solutions exist [26–28] (see Chap. 6 for a detailed discussion) that can be crudely

grouped into smart card-based and non-smart card-based systems. The defenders of satellite TV systems have a realistic outlook on life, i.e. they expect to get attacked, to resist for a while, to update a few times to fix weaknesses and finally to roll out a new solution. This outlook is why the card-based solutions exist, because it is much cheaper to issue a new smart card to improve security than a whole set-top box. It is also a convenient way to adapt and configure a general set-top box to different security/content providers. Not a great deal is published about the cards used in satellite TV systems (aside from hacker forums) and the arguments against security by obscurity cut little ice with the security system providers. Everything is done to make the hackers' task as difficult as possible and so cards can be completely non-standard and armed with a few hidden tricks and surprises. Although cards and Set-Top Boxes (STB) have done their jobs at enforcing access rights to satellite-delivered content, the solution is looking rather dated. Television is now delivered over the Internet to PCs, phones, tablets and smart TVs, none of which are that likely to support a plug-in smart card from the satellite service provider. More flexible DRM solutions are required to match these new delivery channels and devices, and so the days of the DRM smart card may be numbered.

## 1.8 Smart Card Application Development

From the foregoing text it can be seen that the smart card is a secure microcontroller that has been successfully used in a wide variety of applications. There are in fact many more applications including e-purses, lottery, voting, loyalty, user menus, games, etc., but all of them had to be developed at some stage. An important consideration is therefore how to implement a smart card application and whilst this should not be beyond the capabilities of most programmers there are quite a number of ways to go about this, especially in the case of SIM/USIM cards. The obvious starting point is that a microcontroller can be programmed in a form of assembly code or perhaps via a *C* compiler. You can easily buy smart cards for this, but they tend not to be secure, i.e. they are not designed for attack resistance. Of course the secure chip manufacturers and smart card vendors have developed secure devices, but you would normally be prevented from accessing the very low-level code and have to content yourself with developing above the operating system and via some API or toolkit/interpreter. There are good security reasons for this and the API interfaces offer a lot of convenience to the programmer at the expense of speed. In the SIM world, one of the earliest programming facilities was known as a SIM Toolkit Scripting. The SIM Toolkit functionality was originally described in GSM 11.14 [29] and was implemented in the form of a primitive scripting language which could be understood by a script interpreter on the SIM card. The most common and successful use of this was for custom service menus that appeared (to the user) to be stored in the handset, but where actually hosted and managed by the SIM. Earlier implementations were not flexible and so it was difficult to correct or change the Menu services although this improved over time. The biggest problem was that the

scripting languages were vendor proprietary and so a network operator would have to implement/test the *same* functionality multiple times. Bearing in mind that the vendors used different development tools and that testing with many handsets requires a huge effort, the problem should not be underestimated.

As a solution, another development route was created which in principle offered many advantages over SIM Toolkit scripting. The idea was to implement a very simple Menu browser on the SIM so that it provided simple menu options and handled the user or network responses. There were a variety of browsers including the WIB (Wireless Internet Browser [30] from SmartTrust) and the S@T Browser (SIMAlliance Browser). The clever part was that the SIM services sat on a network server rather than in the SIM itself, so providing you did a good job of testing the browser implementations from the various card suppliers, you could implement new SIM-controlled services without changing its stored functionality or necessarily re-testing the SIM. In practice some re-testing was advisable, but all the changes were really in the network. This all held great promised until you realise that an SMS bearer was used, so when you selected a menu option an SMS message had to be sent to the server and a response message returned, also via SMS. At the height of the browser development, the SMS service was quite unreliable and transmission might take a few seconds, but could also take a minute. Measures to get a faster turnaround of SMS helped the situation and some operators went for a menu caching approach, but that really made it a conveniently managed set of SIM hosted services rather than the true browser approach. Another problem was that although the browser approach removed some of the problems from card vendor proprietary systems it risked bringing in a proprietary and single-vendor system component. The popular WIB needed a Wireless Internet Gateway (WIG) in order to be useful and whilst the WIB was free the WIG represented a considerable investment and potential dependency on a single supplier. This is one of the reasons why the Alliance of SIM vendors produced the S@T browser. Although the SIM browser seems to be rather side-lined as a development method, the idea was pretty good and faster communications plus a more open-source approach to the gateway might see a resurgence. The odds may not be great as in the meantime developers have found their favourite platform in the form of the Java Card [17].

Java is popular as it abstracts the programming environment from the underlying chip platform, which means that applications should in theory run unmodified on Java Cards supplied by different card vendors and using different chips. For a long time this was far from reality and even today it is wise to repeat testing for all card types. Of course someone still has to develop the low-level code to provide an operating system plus the Java virtual machine/run-time environment, but that is just done once and usually by the chip or card vendor. Flexibility and card management is provided by the GlobalPlatform [19] functionality which helps to support secure application and data loading, modification and quite sophisticated security domains and channels for isolating multiple applications. Java Card still suffers from the fact that the functionality has to be developed and loaded on the card itself (rather than a remote server), which in some applications creates testing and card management issues. Java Card and GlobalPlatform are described in detail within Chap. 3 along

with another multiapplication card that was in use whilst Java Card was in its earlier stages and that some would claim is more secure. Given that smart cards are usually used for their security attributes, it might therefore seem a little odd that MULTOS [18] was not the developers favourite in place of Java Card, especially as Java is one of the languages that can be used for MULTOS development. The reason is partly due to the fact that MULTOS was designed with the highest standards of security in mind and that meant the whole development and application processes were very controlled, requiring various approvals/certifications and accompanying paperwork before a developer could get his/her application approved and loaded onto a card. This seemed to deter developers and as the vast majority of smart cards were (and still are) for mobile networks that did not insist on formal security evaluations, a lot of the activity headed into the Java camp, which also meant that more freely available tools became available to ease development. MULTOS has not disappeared; however, and these days it is easy to develop with, and should still be given consideration particularly for very high security applications. There have also been recent moves to apply MULTOS to IoT security, exploiting the fact that personalisation and application loading is based on public key (rather than shared secret key) cryptography, making it easier to perform in untrusted and off-line environments.

## 1.9 Development, Roll Out and Lifecycle Management Issues

Developing software for smart cards is in many respects like any other software development, but if you make a mistake it can be a very big one that can haunt you for a long time. When you design the data content and functionality of a smart card you should capture all current and foreseeable future requirements, which is almost an impossible task as no one can accurately predict the future. If you are smart, you design in some flexibility to enable changes and to add more data and functionality in future. Unfortunately, this will likely be resisted by the purchasing department who believe in saving pennies today rather than the promise of rich, yet unspecified new services in the future. Whatever the final agreed compromise, it is translated to a smart card profile that is a definition of how the chosen smart card should be configured. Depending on the application, there may be a great many profiles and reader combinations in use. For example you could have 100 SIM profiles and 1000 s of phones in your network. Testing is really important and to really understand this, consider how much money you could lose your company if a bug slips through. Let us say we have a new mass-market commercial card that we think is properly tested and a big order of 1 million cards is needed, which for simplicity we will say costs £1 million. If you missed a serious bug you may need to recall and replace the cards, a process that is known to cost an order of magnitude more than the cards, i.e. £10 million, because it involves customer care and communication as well as the replacement card and its delivery. Indeed, the cost could be higher if disgruntled

customers chose an alternative service provider. This is one of the reasons you build in remote management, but changing 1 million cards would still be a major undertaking.

You might decide to live with a minor bug and so then the interest will be on the normal card lifecycle. For bank cards this is defined as a few years, but for other cards, e.g. SIM there are no expiry dates. Whilst a SIM might be discarded after a month it is not impossible to find SIMs in use that are over 10 years old. This comes to another important point regarding new service roll out. A company will want a great new service to reach all its customers instantly; however, card-based applications can rarely offer this. If the service requires a new form of card then on the launch date you will have zero customers. If you wait for the cards to expire or wear-out then you may wait many years and if you swap customer cards you know it will be expensive. This sounds like some unfortunate bad-luck situation, but often this legacy problem was actually designed in because of the catch-22 (conflicting logic) of smart card deployment. That is, you need spare capacity and perhaps the most advanced capabilities of the smart card for important services that are not identified when the card is designed, whereas the cost of the card is only justified by the applications that are known to be essential at design time. The situation is not helped by the fact that a marketing strategy or service plan is usually much shorter duration than the life of the card. Another way to get things wrong is to succeed in providing all the necessary and forward thinking card capabilities only to find that the envisaged local/remote management platform is deficient or has simply became a budget cut. One must always remember that a smart card is a sophisticated, personalised and managed computer platform that is vital to a users secure use of a system or service. With proper design and supporting management systems it can be used for many years. Over-specifying a smart card from the bare minimum has a very tangible cost and although it may only be a few pennies or cents per card this starts to become significant for large deployments. However, the true cost of issuing minimum specification devices is less simple to determine as it may be the denial of a new service to a customer, a reduced card lifetime (and earlier replacement cost), a poor service or perhaps the loss of the customer to a competitor.

## 1.10 In Conclusion

This chapter has attempted to provide an introduction to a very wide range of smart card-related issues, which has hopefully been a good starting point for newcomers to the field and those that have perhaps previously focussed on one business or technical area. Of course only an overview has been possible here, but much more detail can be found in the following chapters. A few words of wisdom might be useful to finally conclude this introduction.

- Smart cards are primarily used because they are tamper (attack)-resistant security tokens.
- They are often personalised and managed computer platforms that can be in operation for many years.
- They are not magic devices that make a system secure when it otherwise has bad design, implementation, algorithms, keys and processes.
- They are always part of a system solution, and they tend to be the simplest part.

**Acknowledgements** The author wishes to thank Vodafone, Giesecke and Devrient, Transport for London, The UK Cards Association, Orange Labs (UK), Visa and ITSO, plus all the ISG Smart Card Centre industry supporters for their encouragement and support over many years.

## References

1. CEN TC 224 WG15, European Citizen Card, 2007. More Information Available via http://ec.europa.eu/idabc/servlets/Doc59a8.pdf?id=28716, cited 09 Apr 2016.
2. International Civil Aviation Organisation (ICA0) Doc 9303, 7th Edition, 2015. More Information Available via http://www.icao.int/publications/pages/publication.aspx?docnum=9303, cited 09 Apr 2016.
3. EMV Books 1-4, Version 4.3, Mov 2011. More Information Available via https://www.emvco.com/specifications.aspx?id=223, cited 09 Apr 2016.
4. Transport for London Oyster Card. More Information Available via https://oyster.tfl.gov.uk/oyster/entry.do, Cited 09 Apr 2016.
5. HID Corp Technology Basics Whitepaper Understanding Card Data Formats, 2006. More Information Available via https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf, cited 09 Apr 2016.
6. W. Rankl and W. Effing - Smart card handbook, 4th edition, John Wiley, 2010.
7. Card Watch "Types of Card Fraud". More Information Available via http://www.cardwatch.org.uk/, cited 09 Apr 2016.
8. Financial Fraud Action UK, Fraud The Facts, The definitive overview of payment industry fraud and measures to prevent it, 2013. More Information Available via http://www.theukcardsassociation.org.uk/wm_documents/3533.
9. International Organization for Standardization, ISO/IEC 7816 1-4 Identification cards - Integrated circuit cards - Cards with contacts, 2011.
10. ECMA (Standard ECMA-340) Near Field Communication Interface and Protocol NFCIP-1, 3rd Edition, Jun 2013. More Information Available via http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf, cited 09 Apr 2016.
11. Anderson, R. and Kuhn, M., *Tamper Resistance - a Cautionary Note*, In the Second USENIX Workshop on Electronic Commerce Proceedings (pp. 1–11), 1996.
12. International Organization for Standardization, ISO/IEC 14443 Identification cards - Contactless integrated circuit(s) cards - Proximity cards, 2016.
13. MIFARE. More Information Available via https://www.mifare.net/en/, cited 09 Apr 2016.
14. Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.
15. K. Nohl, H. Plotz, Little Security Despite Obscurity, presentation on the 24th Congress of the Chaos Computer Club in Berlin (Dec 2007).
16. Mayes K and Markantonakis K On the potential of high density smart cards, Elseivier Information Security Technical Report Vol 11 No 3, 2006.
17. Oracle, 2011, Java Card Classic Platform Specification 3.0.4. More Information Available via http://www.oracle.com/technetwork/java/javacard/specs-jsp-136430.html, cited 09 Apr 2016.

18. MULTOS website. More Information Available via https://www.multos.com/, cited 09 Apr 2016.
19. GlobalPlatform, GlobalPlatform Card Specification v2.3, Oct 2015. More Information Available via http://www.globalplatform.org/, cited 09 Apr 2016.
20. M. Mouly, M-B Pautet, The GSM System for Mobile Communications, Cell & Sys. Correspondence, 1992.
21. Friedhelm Hillebrand, *GSM & UMTS - The Creation of Global Mobile Communication* - Wiley, 2002. ISBN: 978-0-470-84322-2.
22. COMP128-1 attack. More Information Available via http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html, cited 09 Apr 2016.
23. Octopus. More Information Available via http://www.hong-kong-travel.org/Octopus/, cited 09 Apr 2016.
24. ITSO, Specification v2.1.4, 2015. More Information Available via http://www.itso.org.uk, cited 09 Apr 2016.
25. Wikipedia, Data Rights Management, 2016. More Information Available via https://en.wikipedia.org/wiki/Digital_rights_management, cited 09 Apr 2016.
26. Canal+ website. More Information Available via http://www.canalplusgroupe.com/, cited 09 Apr 2016.
27. Irdeto website. More Information Available via http://www.irdeto.com, cited 09 Apr 2016.
28. NDS (now Cisco) website. More Information Available via http://www.cisco.com/c/en/us/solutions/service-provider/service-provider-video-solutions/index.html, Cited 09 Apr 2016.
29. 3GPP, TS 11.14 V8.18.0 Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 1999) version 8.18.0, Jun 2007. https://www.3gpp.org/, cited 09 Apr 2016.
30. Gisecke and Devrient, Smart Trust WIB, 2011. More Information Available via https://www.gi-de.com/gd_media/media/en/documents/brochures/mobile_security_2/smarttrust_1/SmartTrust_Wib.pdf, cited 09 Apr 2016.