Chapter 1
An Introduction to Smart Cards and RFIDs

Keith Mayes and Konstantinos Markantonakis

Abstract Security systems often include specialised modules that are used to build the foundations of attack-resistant security. One of the most common modules has been the smart card; however, there are often misconceptions about the definition of the smart card and related technologies, such as Radio Frequency Identification (RFID), as well as the requirement and justification for using them in the first place. These misconceptions are fuelled by the ever evolving nature of applications, security technology, personal devices and the growing threats that they must deal with. There is also a question of whether smart cards/RFIDs should really be in a book about embedded security, but we will see that the "embedded" aspect is growing ever stronger especially with developments in the mobile phone area. This chapter will consider a range of smart cards and RFIDs, and associated applications. It will also briefly cover the traditional manufacture, personalisation and management aspects, illustrating how they are challenged by new mobile developments.

1.1 Introduction

Book chapters describing smart cards and Radio Frequency Identity (RFID) often put a lot of focus on early history. This is all very interesting, but not really the primary focus for a new book. We will direct our discussions towards the electronic "chips" that are utilised in smart cards and RFIDs and which are now also being incorporated into other electronic equipment such as mobile phones. However, for

K. Mayes (✉) · K. Markantonakis
Information Security Group, Smart Card Centre, Royal Holloway, University of London, London, UK
e-mail: keith.mayes@rhul.ac.uk

K. Markantonakis
e-mail: k.markantonakis@rhul.ac.uk

K. Markantonakis and K. Mayes (eds.), *Secure Smart Embedded Devices, Platforms and Applications*, DOI: 10.1007/978-1-4614-7915-4_1,

readers that would feel disappointed without a little history, here are a few critical developments.

- 1940: A generally held view is that the earliest RFID system appeared during WWII and was based on RADAR transmissions to/from aircraft. It was called Identification Friend or Foe (IFF), although strictly speaking it could only identify friends that still had functioning equipment. In one mode, a radar pulse striking an aircraft would trigger a "friendly" coded response, i.e. an identity transmitted by radio means.
- 1968: This is probably the earliest appearance of what might one day be regarded as a smart card. At the time it was referred to as the automated chip card; and the invention was attributed to Helmut Grttrup and Jrgen Dethloff. The associated patent was granted much later in 1982 to Giesecke and Devrient.
- 1974: The first memory card appeared and was attributed to Roland Moreno.
- 1977: The first microprocessor card was attributed to Michel Ugon from Honeywell Bull.
- 1978: Honeywell Bull also patented the first Self-Programmable On-chip Microcomputer.
- 1991: The first GSM [1] mobile SIM [2] card was manufactured by Giesecke and Devrient.
- 1996: The first EMV [3] card specifications were issued by Mastercard and Visa.
- 1996: The first Java Cards [4] were introduced by Schlumberger.
- 1997: The Octopus [5] smart card travel ticket was launched in Hong Kong.
- 2003: The Oyster [6] transport card was launched by Transport for London.
- 2004+: The introduction of European e-passports in accordance with International Civil Aviation Organisation (ICAO) [7].
- 2006: Nokia launched the 6131 NFC phone.

Note that throughout this chapter we will use the term smart card to indicate both smart cards and RFIDs, unless there is a need to differentiate between them. The meaning of the other terms and smart card types mentioned in the previous list will become clearer as we move through the chapter, although it is worth emphasising from the outset that whenever such a technology has been introduced it has been subject to attack. Even back in WWII an enemy would generate "fake" friendly radar signals to trick aircraft into responding with information and location. More than 70 years on this approach has similarities with fake reader attacks on modern RFIDs.

The study of smart cards has a very broad scope in which we find a wide range of devices with diverse functional and attack-resistant capabilities. However, it would not be a good start to our discussions if we did not explain why these devices are at all necessary, so we will begin by extracting some requirements from relevant applications.

1.2 Application Requirements

The fact that smart cards exist in their billions might be grounds to waive analysis of requirements as they must surely exist in overwhelming strength. This would be rather dangerous as we should satisfy ourselves that smart cards were actually needed for these applications or that those deployed are actually fit-for-purpose. We will base our brief analysis around a few well-known applications of smart cards:

- Mobile Communications.
- Banking Cards.
- Satellite TV.
- Passports/Identity Cards.
- Transport Tickets.
- Product tagging.

The reason for putting mobile communications at the top of the list is due to its dominance of the smart card market, as illustrated by Fig. 1.1.

The total size of the market is immense with 6.5 billion units shipped in 2011 rising to a predicted 8 billion by 2014. Note that Fig. 1.1 does not include an entry for the RFIDs used in tagging, which is expected to reach 3 billion units by 2014.

1.2.1 Mobile Communications

Mobile communications uses a smart card which is typically referred to as a Subscriber Identity Module (SIM) [2]; although these days it is strictly speaking a Universal Integrated Circuit Card (UICC) with a SIM application (and/or UMTS [8] variant USIM) hosted on it. It came about initially in GSM standards because the early analogue systems had poor security protection implemented in the phone, which led to call eavesdropping and account cloning. The fundamental SIM requirements were as follows:

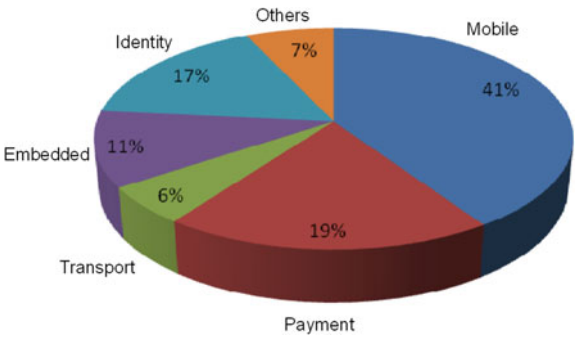

Fig. 1.1 Smart card market by application in 2011 (*source* Infineon)

Fig. 1.2 SIM example (*source* Giesecke and Devrient)

- A portable identity/security element for easy transfer between phones.
- An attack-resistant chip.
- Algorithms/protocols for authentication and cipher key generation.
- Protected storage for unique identity and diversified cryptographic secret keys.
- Internationally standardised solutions.
- High security with supplier attested evaluation.

It is important to realise that the SIM (in common with many other smart cards) is a personalised device. The industry way of working was to have separate supply chains for phone manufacturer and SIM card manufacture and personalisation. An example SIM card is shown in Fig. 1.2.

The example shows three supported SIM sizes. The full-card (ID-1) format, the more common and smaller "plug-in" and the even smaller "third" form factor.

The first requirement in the above list is not as significant as it once was. Originally phones were very expensive and the SIM was a full size card moved between say your portable handset and your car kit. Today, the SIM is usually in a plug-in format and may be pre-installed in a purchased mobile phone, in which case the user may not even be aware of it. The SIM is a bit of an oddity in that it is the most widely used smart card (2 billion+), but is used more like an embedded, yet removable chip, i.e. it is almost never used like a "card". However, the card form is still very useful as the SIM can be produced and configured using conventional smart card manufacturing and personalisation machinery and associated processes. The SIM supports the mobile network authentication and cipher key generation (see Ref. [9] for GSM/UMTS description and comparison) in which the SIM and the back office Authentication Centre are the trusted end points in the security protocol. This means that the mobile phone does not need to be trusted and there is direct back-office control means to disable individual SIM Identities (IDs) from accessing the network. Historically, the mobile network operators have been more concerned that a communication service/call will be paid for (the SIM ID is associated with a valid account in credit) rather than proving that the legitimate phone owner is making use of the services.

1.2.2 Banking Cards

Banks make use of many Automatic Teller Machines (ATM), Point of Sale terminals (POS) and credit/debit cards to secure financial transactions. Their core requirements include those listed below:

- A portable identity/security card for use at standardised ATMs and POSs.
- An attack-resistant chip.
- Algorithms/protocols for authentication, ciphering.
- Protected storage for unique identity and diversified cryptographic secret keys.
- Support for user identity checking via Personal Identification Numbers (PIN codes).
- Card body authenticity check mechanisms (for manual inspection).
- Mag-stripe support for legacy systems.
- Internationally standardised solutions.
- High security requirements with independent evaluation.

An example banking card is shown in Fig. 1.3.

The example shown is a rather special card as not only is it a conventional EMV [3] contact bank card, but it is also a contactless card (RFID) that permits travel on the London Oyster [6] card system. Clearly, the bank card is much more card-like than the SIM and the body is part of the overall security solution, especially for human checks and fall-back situations. Because the transfer of significant amounts of money is involved it is usually a requirement to determine that the legitimate owner is using the card and hence the support for PIN codes. This is in contrast to the approach taken with SIM cards.

Transactions of significant value are still online, so effectively managed by a back-office. The POS/ATMs are intended to be controlled and trustworthy (as compared to the mobile phone) and so can form part of the overall security solution. An interesting aspect is that the banking industry has a history of trading security against cost and accessibility. A first example of this is the continued support of the mag-stripe for

Fig. 1.3 OnePulse bank card (*source* Barclaycard)

locations where the chip card cannot be used and indeed the long use of the magstripe before chip and PIN was introduced, despite the fact that the security was extremely weak. A more current example is the use of touch & pay contactless transactions in which there is an offline transaction and the PIN is not used. Moving from a two-factor (card and PIN) to a single factor authentication reduces security, however, the potential losses are intended to be contained by caps on the number of transactions and associated value. The business thinking is that the easy/simple customer experience will generate more transactions, and fees will be captured that outweigh any money lost to fraud.

1.2.3 Passports

Passports have existed for many time without smart card functionality and because of their relatively long lifetime, legacy and chip-enabled passports exist side by side. Therefore the body of the passport is very important, and some requirements are listed below:

- A portable identity/security card for use at border control.
- An attack-resistant chip.
- Algorithms/protocols for authentication, ciphering.
- Protected storage for unique identity and diversified cryptographic secret keys.
- Support for user identity checking (PIN codes).
- Advanced passport body authenticity check mechanisms (for manual inspection).
- Optical machine readable support for legacy systems.
- Internationally standardised solutions—ICAO [7] compliant.
- High security requirements and independent evaluation.

The picture in Fig. 1.4 shows the symbol used to recognise an e-passport, i.e. one containing the special RFID.

Fig. 1.4 UK e-passport showing logo (*source* www.direct.gov.uk)

The use of the chip provides an additional anti-counterfeit measure as well as traveller convenience for automated checks (compared to presented machine readable printed strips). Improved security is possible as the chip may contain secret credentials to support protocols that are not based on printed information on the passport.

1.2.4 Satellite Pay-TV

Satellite TV companies broadcast valuable media content (e.g. TV programmes, films, sports, etc.) and use smart cards within Set Top Boxes (STB) as part of their conditional access systems. Their core smart card requirements are as follows:

- A replaceable identity/security card for use in the satellite TV company's STBs.
- An attack-resistant chip.
- Algorithms/protocols for ciphering and privilege /access control.
- Protected storage for unique identity and diversified cryptographic secret keys.
- Support for user identity checking (PIN codes).
- Usually proprietary/non-standardised solutions.
- High security requirements—proprietary.

An example of a typical Pay-TV card is shown in Fig. 1.5.

Satellite TV differs from most other smart card applications in that it is a broadcast system so transmissions can be potentially received by anyone and also that there is often no return channel for the protocol. The Satellite TV companies are quite secretive and are suspected of having non-standardised proprietary defensive measures within their conditional access solutions, i.e. security by obscurity. These facts coupled with the value/desirability of the protected contact have led to a great

Fig. 1.5 Skytv card (*source* www.skytv.co.nz)

deal of attacker activity and so the requirements for security countermeasures are high. Given that the STB is under the company control it would be reasonable to suggest an alternative strategy in which the full conditional access security solution is implemented in the STB, thus avoiding the need for smart cards. The reasons for not doing this tend to be economic. The Satellite TV industry recognises that its security and possibly account details may need to be updated over time and so the companies that use smart cards have decided that it is simpler and cheaper to personalise and issue them than replace STBs.

1.2.5 Transport Ticketing

Transport service providers are increasingly turning to smart cards as electronic tickets. Their core requirements are summarised below:

- A portable identity/security card for use at their station gates/buses.
- A fast transaction.
- An attack-resistant chip.
- Algorithms/protocols for authentication, ciphering.
- Protected storage for unique identity and diversified cryptographic secret keys.
- Protected wallet/ticket functionality/storage.
- Moderate security usually supplier attested evaluation.

Figure 1.6 shows two popular examples of contactless/RFID travel cards. The Oyster [6] card is the most well known in the UK and has been very successful since its introduction in 2003. However, the Octopus [5] card from Hong Kong was introduced much earlier (1997) and is now being used for a range of purchases in addition to travel.

Smart card tickets are often used alongside legacy tickets, and are popular with customers for their ease of use and avoiding the need to queue for tickets. They also help with fraud control at gated stations and reduced cash handling as well as

Fig. 1.6 Oyster and Octopus travel cards (*source* Transport for London)

supporting statistical journey analysis and optimisation. Transport tickets have been attacked in a public manner (notably the MIFARE Classic [10] -based cards) and in response the security of the solutions has been improving, albeit driven more by reputational issues than actual measured losses from fraud.

1.2.6 Product Tagging

Product tagging and logistics is a growth area for smart card devices, although in this field they are most often exclusively referred to as RFIDs. There is in fact a wide range of devices to consider from extremely simple IDs to high-end smart cards with similar capabilities to SIMs. Core requirements include:

- Storage/memory including at least an ID—preferably protect by a security protocol.
- A fast transaction.
- Algorithms/protocols for authentication, integrity—optional.
- Low to moderate security usually supplier attested evaluation.

Product tagging was originally driven mainly by convenience, and the choice of tags by cost; however, tag sophistication and security is growing as manufacturing costs reduce.

The examples in Fig. 1.7 illustrate the diversity of tag types. The left-hand side image shows a typical self-adhesive tag which in this case is being used for medicine identification, by being stuck onto the container. The tag on the right can be used for the identification of pets and is inserted under the skin of the animal, yet can still

Fig. 1.7 Medicine and animal tags

Table 1.1 Comparison of application requirements for smart cards

	Speed	Security protocols	Storage amount	Portability	Low cost	Standards	Security evaluation
Mobile	M	H	H	L	M	H	L
Banking	M	H	M	H	M	H	H
Passport	M	H	H	H	L	H	H
Satellite	M	H	M	L	M	L	L
Transport	H	M	M	H	M	M	L
Tagging	H	L	L	M	H	L	L

be accessed by an external reader device. The diversity is possible because of the contactless interface and so the form factor is far less restricted than a contact smart card, and RFID tags can be made smaller, physically robust and reliable.

1.2.7 Comparing Requirements

The above discussions are summarised in a subjective manner within Table 1.1. Each characteristic is rated by importance as High Medium or Low (H:M:L).

We can explain some of the differences in the table, using the mobile SIM as a reference.

- In terms of speed, the SIM may have complex functionality and so needs to be reasonably swift; however, it is within a powered device and most transaction times do not inconvenience the user. By contrast, a transport card (such as an Oyster card) has to be extremely fast to maximise safe throughput at station gates during busy times.
- A SIM will support secure protocols, however, the impact of such protocols has more significance for bank cards and passports where considerable sums of money or proof of identity may be at risk.
- SIMs tend to have the highest storage of any mass market smart cards, whereas a simple RFID tag might just have a few bits of memory to hold a fixed ID.
- The SIM is not very card-like and today is not really portable, but rather transferable between devices, and in this respect is not unlike the cards used in Satellite pay-TV systems. Bank cards, passports and transport tickets rely far more on portability.
- Because they are produced in huge volumes, SIM cards are not expensive compared to their high level of functionality, however, cost is perhaps the biggest issue for RFID tagging of products where just a few pennies are available for tag purchase. Passports are perhaps the least cost-sensitive, especially as in the UK the citizen is required to pay a significant amount to obtain a passport.
- Standards are well developed in the mobile, banking and passport applications, whereas proprietary solutions are still common in satellite pay-TV and tagging.

The transport industry is also still dominated by proprietary solutions, although there are some moves towards a more interoperable approach.

- Formal security evaluation (e.g. common criteria) has historically been important to banking and passport applications. In principle, the mobile industry could also insist on formally evaluated SIMs, although cost and process delay issues have prevented this in the past.

Having established some requirements related to the real-world applications of smart cards, the next step is to consider the available devices that might satisfy those requirements, and this is discussed in the following section.

1.3 Contact and Contactless Smart Cards/RFIDs

Smart card products exist to satisfy the full range of application requirements mentioned in the preceding section. Before considering the product categories we need to first cover some basic characteristics and differences of contact and contactless smart cards, passive RFIDs and active RFIDs.

1.3.1 Cards with Contacts

Referring back to Fig. 1.2 we can see some electrical contacts behind which sits the chip. In normal use the card is inserted into a reader that makes electrical connection to the chip via these contacts. The pin-out for the contacts has changed a little over the years and Fig. 1.8 shows the traditional definitions.

VCC is the power input and GND is the ground (0V) return. CLK provides the chip with a clock signal (it does not have an internal clock), I/O is used for input/output and RST is there to reset the chip. Vpp is a throw-back to old EPROM technology when a voltage higher than VCC was need to actually write to the chip memory. These days this pin is used in SIM cards for the Single Wire protocol (SWP) which enables a SIM hosted Security Element (SE) to communicate with the phone's Near Field Communication (NFC) modem. Furthermore, in the most modern SIMs, the contacts marked RFU are now used for the USB connection which is much faster

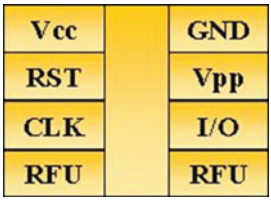

Fig. 1.8 Smart card contacts

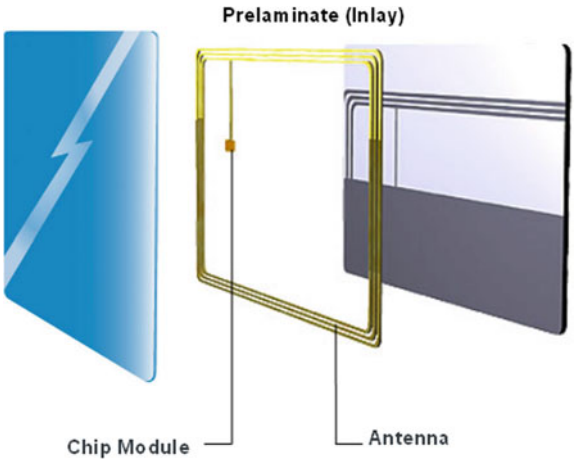

Fig. 1.9 Laminated construction of a contactless smart card (source Giesecke and Devrient)

than the traditional I/O PIN interface. More information on general contact cards can be found in Ref. [11], and [2] is a good starting point for SIM information.

1.3.2 Contactless Smart Cards/RFIDS

Clearly a contactless smart card/RFID requires a different method for powering and communication. This is typically achieved by connecting the chip to an antenna as shown in Fig. 1.9. Although we have shown a card example, the great flexibility of RFIDs is that they can be made in all manner of shapes and sizes, provided that the antenna design and size is sufficient to provide powering and support chip communication. The basic operation is described in the following text, although the interested reader is referred to Ref. [12] for a more detailed description.

The reader device has no contacts, but instead creates an electromagnetic field. When the card is placed in this field, the antenna gathers energy from it (rather like a transformer) in order to power the chip. The field is modulated by the reader in a controlled manner so that the card can detect a clock signal and the information transmissions/requests from the reader. The card communicates back to the reader by modulating the field amplitude. This is basically achieved by the chip switching on a load so that the electromagnetic field strength momentarily shrinks lower than normal. This is rather like the way a battery voltage will drop when you switch on a connected electrical load. This can be seen more clearly with reference to Fig. 1.10, which represents the electromagnetic field for the reader and card transmissions.

In the upper trace the reader is able to exert strong control over the electromagnetic field that it generates, whereas in the lower trace the card can only weakly modulate the field.

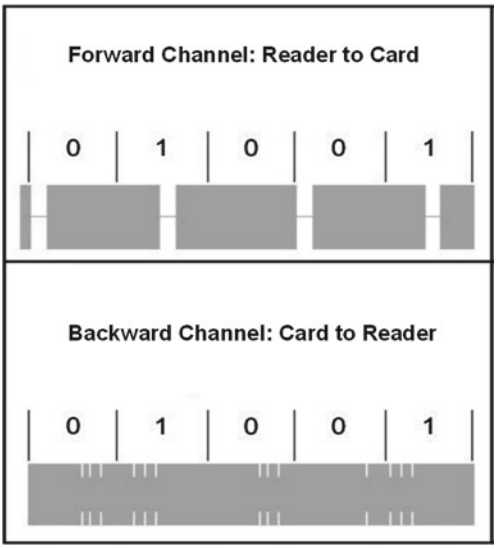

Fig. 1.10 RFID Reader and card signal modulation examples

Active RFIDS: What we have just briefly described is a passive RFID which is by far the most common type in use. However, there are also active RFIDs that have their own batteries and transmitters, with perhaps the most common being used for remote locking in vehicles. Whilst active RFIDs are useful devices, their cost, size and maintenance aspects means that they are used far less than passive RFIDs, so they will not be considered further within this chapter. Instead we will focus on the family of passive devices that support standard Application protocol Data Unit (APDU) communication.

1.3.3 APDU Communication

Whether we are using a smart card with contacts or a contactless device, the relevant reader needs some logical way to communicate with the chip, once we have got beyond the physical interfaces (wires or RF). This is achieved via a simple command-response protocol in which the reader issues command messages and expects appropriate responses from the card. The commands are structured into APDUs and an example of command and response formats is shown in Fig. 1.11.

The CLA represents the "class byte" which is a static value for a given type of application. INS indicates the instruction/command and is what the reader wants the card to do, which could be to read a memory location or perhaps run an algorithm. P1 and P2 are parameters relevant to the particular INS and P3 is a data length indicator. P3 can be used to indicate the length of data that is supplied with the command, or the length of data field expected in the response from the card.

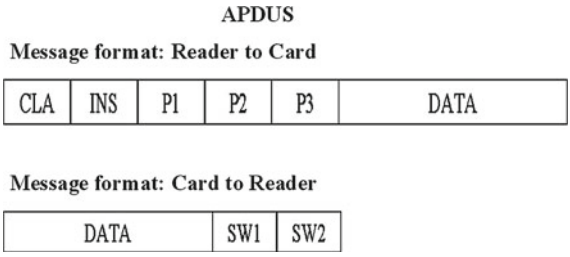

Fig. 1.11 APDU format

The card response will always provide the status words SW1 and SW2 indicating the outcome of the request and depending on the INS some data may also be returned.

1.4 The Range of Smart Card Devices

Smart card products are not simply split into contact and contactless, and RFIDs are not just passive and active. There is in fact a very wide range of products with differing capabilities and costs, designed to satisfy the variety of application requirements. The product range for passive devices is depicted in Fig. 1.12 and the generic types are described below.

1.4.1 Simple ID Tag/Card

The simplest devices offer convenience and fast machine readability, but not much more. They are usually called tags or RFIDs and almost never smart cards. They contain a very small amount of memory to represent an ID which is transmitted when the device interacts with a reader. In tags that are used as barcode replacements the ID need not be unique, but perhaps represents a product type. Tags can also have unique IDs in which case the only security feature is if the ID field is read-only. There is no security protocol other than reporting the ID to the reader and so it is

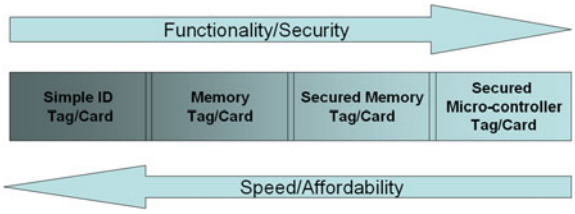

Fig. 1.12 The range of smart card/RFID devices

very easy for an attacker to discover the ID and program it into an emulator device or a similar ID/Tag that permits control of the ID field. In the latter case it could be a legitimate tag in its pre-configured state, i.e. before personalised with its ID.

Anyone with some interest in information security might wonder why such tags (which are usually proprietary) are used when they have almost no security protection and there are better devices available. Cost is not far from the answer, but you also avoid the trouble of key management (as there are none!). This is not to say that the use of such tags is inappropriate, it depends on the application. For tagging your groceries it could be fine, although using it as a building access control card would be very worrying. It also depends on what you are replacing. A system based on paper vouchers and human inspection could be revolutionised by the introduction of automated inspection of machine readable tags and whilst this could introduce potential opportunity for fraud, it might be far less than for the legacy system it replaces.

1.4.2 Memory Tag/Card

Some applications require more data to be stored on the tag than just the ID and so need more capable devices, which we will refer to as memory tags. Usually they have a unique read-only ID (like the ID/Tag) plus a small open memory with read/write access, although in principle the whole memory could be read/write. In common with the simplest ID tags they are usually proprietary and there is no low-level security protocol and so it is possible for anyone to read the memory contents and re-use them in an emulator or clone platform. The tags are quite fast and speed is a function of the memory size, or at least how much data are read or written during a transaction. The tag system operator can add some security measures at the application level if required. There is not too much that can be down about tag authentication, but the data integrity and authenticity could be protected by an associated stored Message Authentication Code (MAC) or digital signature and/or the data privacy could be maintained by encryption. If the tag data is effectively interpreted by an online secure server then this is reasonably secure and manageable, but otherwise it means that keys will need to be distributed to reader devices that must also run algorithms, which makes them and the associated Key Management System (KMS) processes critical parts of the system. If you are going to this trouble it might be better to opt for a Secured Memory Tag/Card.

1.4.3 Secured Memory Tag/Card

These tags/cards have key-based cryptographic protocols to control access to memory contents. They are perhaps the first devices in the card family that deserver the "smart" description. Typically, the tag and reader will mutually authenticate before

allowing access to memory; usually with data transfers encrypted under session keys. Some cards divide the memory up into smaller partitions that have different keys, so multi-application support is possible with different keys assigned to various application providers. There are other devices that divide the memory into a hierarchical file structure using the security protocol to establish access rights and privileges. One of the most maligned products in this class is the MIFARE Classic [10], yet it has also been one of the most popular and successful products. Although its security has been comprehensively compromised by widely published attacks (see Chap. 6), it at least has some security measures to attack, which cannot be said for the simpler Tag/Card products, and so for very simple low risk applications it may still be useful. It would be better to opt for the newer MIFARE Plus [13] which takes the same basic product approach, but uses the AES [14] algorithm. For the file-based secured memory tag/card there is the DESFIRE EV1 [15], which despite the name can also use AES. The products are fast and although proprietary, the more modern types have undergone independent security evaluation.

1.4.4 Secured Microcontroller ID/Tag

At the head of the family we find the most sophisticated products based on secured microcontroller chips. In card form this is what we most definitely refer to as a "smart" card, although it is really the chip that matters and this could be used within many other form factors and assemblies. These devices can be used for just secure data storage, but more importantly for hosting secure functionality and especially advanced security and transaction protocols. A modern device would typically have be a Java Card [4] and include GlobalPlatform [16] support for management. The most advanced products include cryptographic co-processors for common symmetric and asymmetric cryptographic functionality such as encryption, verification and signing. These products tend to conform to international standards and industry guidelines and are often security evaluated either in an internationally recognised manner (e.g. common criteria [17]) or via private lab tests. The downside of such devices is that they tend to be slower and more expensive than the alternatives; and usually more complex to develop and manage.

Note: It is of fundamental importance to understand that the Secured Memory and Secured Microcontroller products can only be used with confidence in target applications because they are based on tamper-resistant hardware, incorporating physical countermeasures against all known practical attacks. Attacks on security devices are covered in detail elsewhere within this book, but given the importance it is worthwhile just briefly recapping on these capabilities.

1.5 The Importance of Providing Attack/Tamper-Resistance

When we talk of attack/tamper-resistance we are referring to attacks that can be performed on the implementation of sensitive applications, algorithms and protocols, etc., of a particular device. This is not to be confused with the logical design of the solution, e.g. algorithm and keysize choices, which are covered by best-practice considerations (see Sect. 6.8). For an assembly, tampering may be removing the lid, rewiring the connections, probing chips, etc., and with smart cards we are concerned with similar things at the chip level. There are a lot of tools from the manufacturing world that facilitate this and there is evidence of physical attacks and reverse engineering. An attacker may seek to physically inspect the chip design, probe memories and buses and make changes to low-level hardware. To hinder this the special smart card chips have shields which can be simple fixed barriers or current carrying meshes, they scramble the design layout so it is hard to access areas of interest and the low-level encrypt buses and memories. The designers also add environmental sensors for detecting light, temperature and voltage. Light is an indicator that the chip is outside of its package and so a reason to render the device inoperable. Temperature and voltage extremes may be associated with fault attacks whereby the attacker seeks to disrupt normal operation for a security advantage. The chip will also include measures to disguise/break the linkage between chip current and operation performed to prevent exploitation of side-channel leakage attacks. At chip level these measures usually include power smoothing, noise addition and variable processing delays. The very intrusive physical attacks are usually only attempted for reverse engineering, whereas the fault and side-channel attacks could be justified against individual cards and need not destroy the test target.

Just looking at a chip it is impossible to appreciate its level of tamper-resistance and physical attack resistance and given the sensitive nature of the protection measures they will not be detailed within a data sheet. It is therefore very important for someone seeking a smart card product to be able to gain assurance of the implementation security. Fortunately there are well-known means to do this. The Common Criteria [17] framework is a means to achieve an internationally recognised level of evaluated security on a range of products including smart cards. The levels start at EAL1 and rise to EAL7, with smart cards commonly evaluated to EAL4+, where the + means that some higher level features are included. Where such an evaluation certificate is not available the next best thing is a report from a credible expert lab stating that the products resisted all known attack strategies during the period of the tests.

To finally hammer home the point, many common smart card applications would be flawed and indeed pointless without the property of attack/tamper-resistance. Fortunately, these principles have been well understood in the smart card world and products, specifications and processes have emerged to successfully provide the necessary safeguards. However, these measures are now being stressed by the emergence of new technologies, which challenge the way that we implement smart card (and particularly RFID) functionality.

1.6 Mobile and NFC

Conventional smart cards show little sign of disappearing from the market and more and more are used each year. However, there is a disruptive technology that might change this in the longer term and which is already challenging assumptions and processes related to security modules. The technology in question is Near Field Communication (NFC) [18]. This is discussed in detail within Sect. 14.5.2.3, so here it will suffice to say that it gives a mobile phone the ability to act as a smart card reader, to emulate a smart card or to communicate with another phone in peer-to-peer mode. In our discussions here we will just focus on card emulation and the challenges for evaluated tamper-resistance and associated security processes.

A good example for this is shown in Fig. 1.13. This represents a collaboration between Orange and Barclaycard to offer the first NFC wallet (Quicktap [19]) in the UK, whereby the mobile phone may be used in place of a contactless bank card. Clearly, as financial transactions are involved there will be interest from attackers and so it is important to emulate the bank card in a secure manner. In NFC the smart card is emulated by something called a Security Element (SE). In the early NFC phones this was provided in the form of a chip embedded within the phone hardware. As the chip

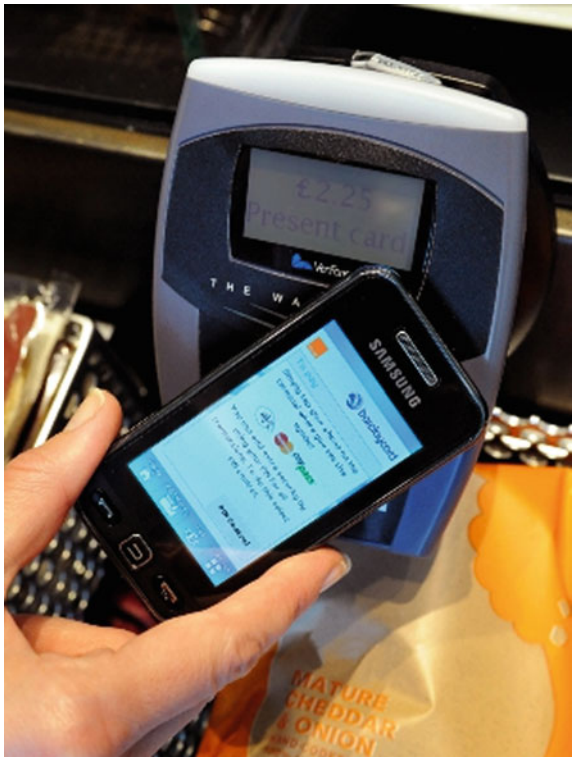

Fig. 1.13 Quick-tap application (Orange/Barclaycard)

was a high-end smart card device (e.g. SmartMX [20]), then from a physical point of view there should be no problem with it, although there are serious challenges for personalisation, ownership and management that we will defer until later. Other options include the SE as an integrated part of the SIM and a plug-in on a memory card port, which again should be capable of satisfying physical protection requirements. More of a concern is the Soft-SE approach whereby the SE emulation is running in the phone CPU. The history of mobile phone security is very poor and the complexity and fast moving nature of modern smart phone hardware and software development is unlikely to see the problem resolved overnight. There are efforts to improve mobile phone security, however, even if an enterprising company comes up with a physically (and not just logically) secure solution there is the problem of convincing application and service providers that this is the case and bearing in mind that the general market will not be restricted to products from one supplier.

Whichever solution is used there are big challenges for the associated processes and trust management. Typically, a smart card has an Issuer who owns, personalise, issues and securely manages the device during its useful life. The processes for this are very well established and proven. The disadvantage is that you end up with a lot of smart cards in your wallet, although some might argue that this provides some diversity; if you lose one card you still have others. An NFC phone could in principle replace all your cards which can be very convenient, but potentially disastrous if it fails to function or gets lost or stolen. Exactly what types of smart cards might be displaced by NFC is not yet known although low value applications such as metro travel or touch & pay purchases seem reasonable candidates.

The first NFC payment services in the UK are likely to be constrained and proprietary. The Quicktap [19] is available from Orange and uses Barclaycard for the financial aspects. Whilst other products are expected, it is doubtful that they will be compatible beyond the card to reader interface. It therefore seems very likely that the configuration management of SEs will be a major issue, especially as customers often change, phone, SIM, credit cards and sometimes banks. This will challenge the lifecycle processes used for conventional smart cards, which are briefly described in the following section.

1.7 Conventional Smart Card Lifecycle Management Processes

The typical stages in the preparation, issuance and management of a smart card or RFID are shown in Fig. 1.14. The overall process is normally triggered by the Issuer (who provides cards to end users) placing an order with the Manufacturer (sometimes called the Smart Card Vendor) for a batch of cards according to a specification (profile) and using Issuer input data (input file). The Issuer will eventually receive the smart cards (or perhaps they are shipped direct to end-users) plus the response file containing data, keys and PINS to securely manage the smart cards.

Chip Manufacture is handled by the chip fabrication plant (FAB) and for a masked Read Only Memory (ROM) style device would include the Operating System (OS)

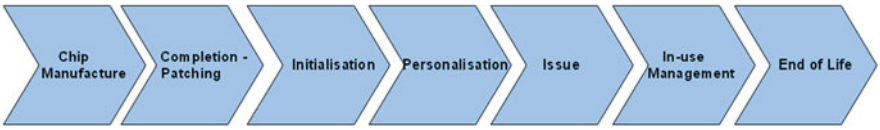

Fig. 1.14 Typical smart card lifecycle stages

from the particular smart card vendor. Completion is getting the chip into a usable state which may mean patching the OS using some of the chip's non-volatile memory. Initialisation is the process of getting all the standard data and functionality loaded onto the card. Here the word "standard" means for the particular Issuer's product and other Issuers may have very different requirements. Personalisation is configuring a smart card for a particular account, or if known, a particular end-user. The Issue stage represents the ways and means to get the card into the hands of the end-user. In-use Management includes updates to keep the smart card functioning in an optimum manner, including data and functional updates, which have to be applied in a security protected manner. End of Life can be a tangible update that disables the card, the removal of its corresponding back office data/functionality or simply a soft ending, e.g. that the card is probably not in use any more.

The Completion through to Issue stages are often all handled by the smart card vendor. Basically, the Issuer requests smart cards to a certain specification (profile) from the vendor and also provides an input file for personalising them to either generic unique accounts or particular end-users. In the latter case, the vendor may also pack/send the cards to end-users via the mail. Thereafter the smart cards are deemed In-use and any updates are handled by the Issuer using credentials received from the vendor in the form of a response file. The response file is highly sensitive as it contains all the security credentials, IDs, keys, PINs, etc., for the issued cards and gives the holder the ability to manage the smart card contents and functionality. This includes the capability to disable the card at end of life should this be necessary and indeed the means to create a clone of the smart card.

The time span of the lifecycle is quite different depending on the application. A banking card might be expected to have a lifecycle of about five years after which it will be expired and no longer work. A mobile communications SIM card might be used for less than a year, but then again some continue 10+ years as there is no fixed expiry limit. Chips in passports would be expected to last for 10 years. If we think ahead to chips within electronic assemblies such as phones and even cars we again have a wide variation. Mobile smart phones fall rapidly out of fashion, whereas a chip in an automobile subsystem might have to survive 15+ years.

Returning to NFC SEs the above situation is not much changed if we have a SIM-based SE or indeed a memory card-based version. However, the embedded chip is markedly different. The chip should go through Completion before it ends up in the phone hardware. If we buy the phone as an unlocked device then it has in a way been issued to us, but without the Initialisation and Personalisation stages and (at the moment) no real certainty over where the response data/credentials are

and indeed who now has the privileges and responsibilities of the Issuer. If we get the phone locked to a network, the SE might have been through Initialisation for the network, but Personalisation probably requires some subsequent effort/set-up. Bearing in mind that Initialisation and Personalisation are conventionally carried out in highly secured physical environments there is quite a challenge to replicate the same level of security in the field. There is of course a queue of companies lining up to meet the challenge with the ambition of becoming the Trusted Service Manager (TSM) who would be in charge of the remote security management of SEs. However, whilst agreement on technical issues is eventually likely, agreement on who should be the TSM seems far more elusive and indeed a battle ground for conflicting business interests.

1.8 Conclusion

In this chapter we have briefly introduced smart cards and some of the major applications that make use of them. There is no absolute right or wrong choice for a smart card device as it depends on the requirements of the particular application. The most successful application in terms of number of standards-compliant devices has been mobile communications, which has used SIMs with advanced functionality, yet paid less attention to formal security evaluations than other standardised solutions such as bank cards or passports. Furthermore, the SIM today is far more like an embedded security module than a conventional smart card and there are suggestions that it should simply be replaced by a chip in the phone, although this raises all kinds of issues related to personalisation, ownership and control. In some respects the SIM is similar to the cards used in proprietary satellite Pay-TV security systems as all they are manufactured and distributed in the card form, but once installed they are used like embedded modules. The bank card is most obviously still a conventional and portable smart card, making full use of personalised card body features as well as the chip security. Historically, the less sophisticated and usually proprietary devices are found in tagging and transport systems. For tags the capabilities are normally restricted due to very tight cost constraints, whereas for transport it is the speed of operation that is critical.

The diversity of application requirements has led to a wide range of available products that offer varying degrees of functionality and security for a given cost. For many applications the tamper resistance of the chip is of vital importance and a wide range of attacks against the implementation should be resisted, including physical tampering, side-channel and fault attacks. For the cryptographic algorithm and protocol design aspects it is highly advisable to make a selection based on best-practices of information security (see Sect. 5.9), however cost and legacy compatibility often mean that a compromise has to be made and indeed much of information security is about working with imperfect solutions. It is important to appreciate that the less secure products can be quite suitable for some applications, although one should always check that the security of a device has not been compromised, otherwise the

wrong design decisions will be made. A good example is the MIFARE Classic, as it was originally offered as a small key secured memory card, although today it is best considered as a basic memory card; so extra security protection may need to be added at the application layer.

A lot of industry experience has been gained from the manufacture, initialisation, personalisation and management of smart cards, however, new technological developments may challenge the conventional way of working. In particular, an NFC phone may emulate several smart card devices via the SE. Whilst the hardware SEs are based around smart card chips and should offer attack resistance, the configuration, personalisation, management and ownership of the phone-embedded and memory module SE options may be quite different from that of the SIM card, or indeed any other issued smart card. The security challenges and added complexity has led some parties to suggest the use of software SEs hosted by the phone processor. This is a worrying development and history risks repeating itself if too much trust is placed in mobile phone software security, without proper consideration. What may eventually emerge is a hybrid solution using mobile phone software underpinned by specialist hardware features, either provided by separate chips or possibly included within the phone processor itself.

As a final remark, there appears little sign that the billions of smart cards and RFIDs produced each year will reduce and in fact they are expected to rise significantly. NFC will not make much difference in the short term, especially while companies are squabbling over roles and standards options, however it might result in an acceptable security solution for the remote management of SEs. If this is the case then the same solution might be used to logically justify the use of embedded SIMs, although this would no doubt be resisted by mobile network operators.

References

1. Mouly, M., Pautet, M.B.: The GSM System for Mobile Communications, Cell & Sys. Correspondence, 1992.
2. ETSI, 3GPP TS 11.11 V8.14.0 Specification of the Subscriber Identity Module -Mobile Equipment (SIM - ME) interface, (2007–06)
3. EMV Books 1–4, Version 4.3, November 2011. www.emvco.com
4. Java Card Platform Specifications V3.04, Oracle, 2011. www.oracle.com/technetwork/java/javacard/overview/index.html
5. Octopus, www.octopus.com.hk/home/en/index.html
6. Transport for London, Oyster Card, www.tfl.gov.uk/oyster
7. International Civil Aviation Organisation (ICAO) Doc 9303, www.icao.int
8. Friedhelm Hillebrand: GSM & UMTS - The Creation of Global Mobile Communication Wiley, 2002, ISBN: 978-0-470-84322-2.
9. Mayes and Markantonakis: Smart Cards, Tokens, Security and Applications, Springer 2008, Chapter 4, p 85–112.
10. Philips Semiconductors (NXP), MIFARE Standard Card IC MF1 IC S50 Functional Specification, revision 4.0 1998.
11. International Organisation for Standardisation, ISO.IEC 7816 1–4, 1999.

12. International Organisation for Standardisation, ISO.IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards, 2000.
13. NXP, MIFARE Plus data sheet MF1SPLUSx0y1, February 2011. www.nxp.com/documents/short_data_sheet/MF1SPLUSX0Y1_SDS.pdf
14. Federal Information processing Standards, Advanced Encryption Standard (AES), FIPS publication 197. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
15. NXP, MF3ICx21_4_81 MIFARE DESFire EV1 contactless multi-application IC short data sheet, revision 3.1, December 2010
16. GlobalPlatform, GlobalPlatform Card Specification 2006 www.globalplatform.org
17. Common Criteria V3.1, 2009, www.commoncriteriaportal.org
18. NFC Forum, NFC Forum technical Specifications, www.nfc-forum.org/specs/spec_list
19. Orange UK, Quicktap, www.shop.orange.co.uk/mobile-phones/contactless
20. NXP, SmartMX Platform features, Revision 1.0 Short form Specification, 2004