Part I

Introduction

1 Background

1.1 Smart cards in daily life

Cards are so much part of our daily lives that we do not even think about their functions, the technology behind them or the things that make them special.

Cards are behind some of the biggest changes in behaviour in the Western world since 1970 – the way we enter buildings, pay for goods in shops, speak to our friends and business partners. Back in 1970 it would have been difficult to imagine the ease with which we now draw money from ATMs in foreign countries, or that many ten-year-olds would have their own telephones.

Many of these changes have helped to spread technology as well, benefiting a wide range of people in poorer countries and remote areas. Where there is no reliable telecommunications network, the ability to store a patient's health records in a card can save lives. In most African and many Asian countries, there are many more mobile telephones than fixed lines; these telephones not only use cards to provide security and added functions, but may themselves act as terminals for other card-based applications, such as microfinance.

It's not all good news, of course: some of these changes have been made necessary by the increasing need for security, while others have increased efficiency but have incurred a cost in reduced personal service and social interaction. And not all card projects have been equally successful.

Most users do not need to think about how they work, in much the same way as an artist or writer does not need to think about the pencil he or she uses. Occasionally, though, it is worth thinking carefully about cards: how we use them, their functions and technology, and how we can use them to improve life and business. Not only can those involved in the cards business benefit from this reflection, but also everyone who manages, controls, designs or operates a business in which cards are used – and that means virtually every business.

This book aims to provide some of the background as to how businesses can use cards more effectively. In particular, it focuses on the most advanced card technology in use today: the multi-application smart card. But along the way we will see some situations in which much simpler card technology may do just as good a job.

1.2 Card functions

1.2.1 From identification. . .

When people do think about cards, it is mostly about the cards in their purse or wallet: their bank cards, office access cards, health cards or identity cards. Nearly all of these cards have *identity* as their main function – they help us to identify ourselves to a system.

Where we are identifying ourselves to a person, the simplest solution is a 'flash card' (carrying a photograph or just a name and signature); these identities are rarely checked for validity. Where we are identifying ourselves to a machine, or where there will be a check against a database, the most widely used technologies are magnetic stripes and bar codes, both of which work extremely well. We can also use contactless (wireless) technologies such as Wiegand tags (the rather thicker cards often used for office access) or contactless smart cards.

Objects can benefit from identification too – goods in industrial processes and in the retail supply chain have traditionally been identified using bar codes, while there is a growing use of radio-frequency identification (RFID) tags (see Figure 1.1) to track high-value goods and prevent theft in shops, and in libraries to track books.

These tags only transmit a string of data to the reader. In fact, the characteristic of all the technologies described so far is that they are read-only: they provide a reference number that allows a system to access a record in a database.

1.2.2 . . .to authentication

Increasingly, though, the real requirement is not only to *identify* the record in the database, but also to *prove* that the person presenting the card is actually the person referenced by the database, or that the card itself has not been forged or altered. This is where the smart card starts to come into its own.

Smart cards not only contain data but can also perform operations, such as comparing the data with an external source, computing an electronic signature from some data or incrementing and decrementing counters. Their other important feature is their ability to store data in secret areas that cannot be accessed from outside the card, but only by the software on the card – this makes them particularly good for cryptographic purposes such as protecting the confidentiality of encrypted files, or providing proof of a transaction.

Where a requirement for identification includes an underlying requirement for authentication, smart cards are usually the best tool for the job. So smart cards are now the standard form of bank card in Europe and Asia, and increasingly in other parts of the world, to prove that the card has not been copied or altered, and that the user is the correct card-holder. There is a smart card in every GSM mobile telephone, to authenticate the account and protect the confidentiality of the conversation.

Where governments issue machine-readable passports or identity cards, the only generally accepted way to prove reliably that the card and the data on it are genuine is to use a smart card: these are now the standard form of identity card for 7 million

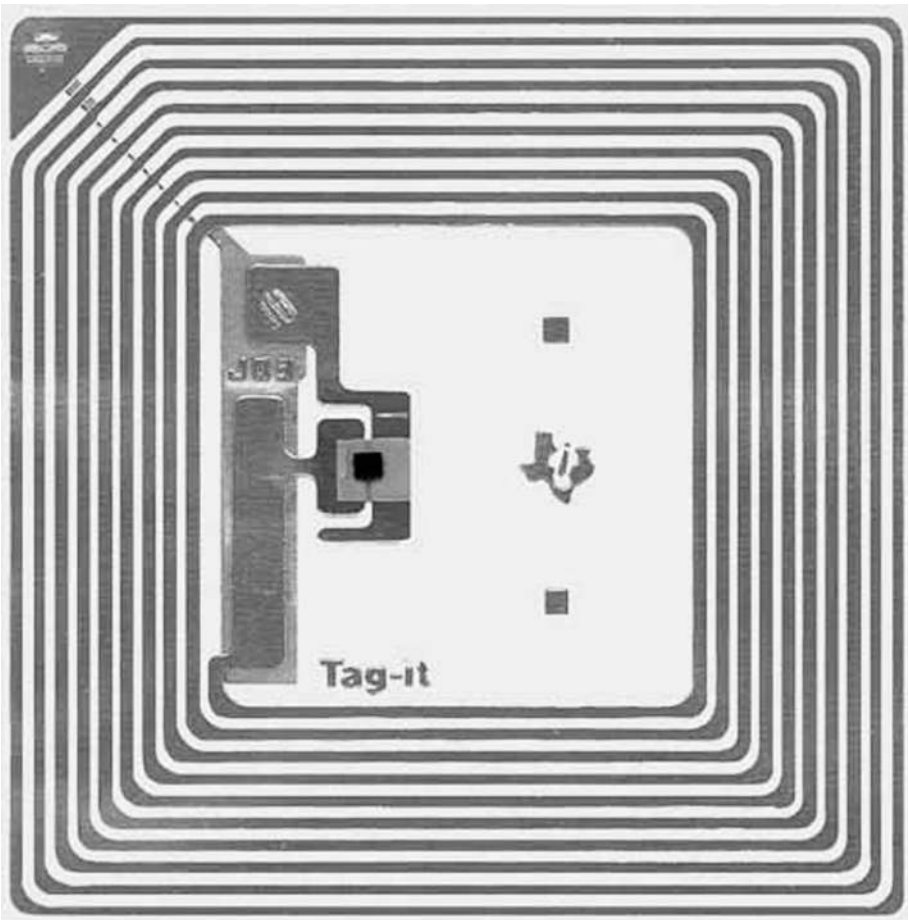

Figure 1.1 RFID tag (courtesy of Texas Instruments, Inc.)

Hong Kong residents, 23 million Malaysians and even 4 million US service personnel and Department of Defense employees. Over the next ten years, most countries will adopt this technology for inclusion in passports.

1.2.3 Data storage

Although it may seem obvious that we use smart cards to store data, actually this is not usually a core function of a card. Most smart cards have a quite small data storage capacity (a few kilobytes, or tens of kilobytes at the most), and when in use they are always connected to a terminal or reader, which almost certainly has a much greater storage capacity and in turn is connected to a server with access to a database.

So smart cards are used when the storage performs a special function: for example, when the data belong to the card-holder and not to the system operator the card can protect the card-holder's privacy and ownership rights. In a GSM telephone, the SIM card stores data and applications that are under the control of the network operator,

not the handset manufacturer. With a biometric application, storing and comparing the template on the card ensures that it cannot be copied or inspected whilst being transmitted from the host system to the terminal.

1.3 Advanced applications

1.3.1 Cryptography

Although the notion of keys and secrets underpins almost every smart-card application – even the most basic memory card today uses keys to control reading and writing of the data on the card – relatively few cards actually have the special hardware needed for fast computation of the variable-length arithmetic functions and public-key algorithms used in modern cryptography.

Nonetheless, smart cards play an important rôle in many cryptographic systems; they provide the token that represents the physical factor in multi-factor authentication (these terms and concepts will be covered in Chapter 4). It is equally important to recognise that the card is only a part of such a system and cannot provide security on its own; many critical analyses of smart-card security have missed this point.

Chapter 5 will address the ways that smart cards can help to provide the five main security services, and the standards that smart-card-based security should follow.

1.3.2 Database access and linking

Although smart cards themselves are an expensive and limited storage medium by modern standards, we are moving towards a world in which almost every piece of information is available in some form of online database; the problem is to identify the data we are seeking and to control access to that information.

Smart cards can greatly assist in both of these functions: not only by carrying reference fields that point to a record in the database, but also by identifying the category to which the user belongs and their rights to view or change the data. This is very important, for example, in health records systems, where different groups of health professionals have different needs and rights to view patient records, or with government data, where data protection and separation of functions must be enforced.

1.3.3 Biometrics

Every form of identification has its drawbacks: cards can be stolen or shared, passwords and PINs can be viewed, signatures and photographs are very difficult to verify. But there are many situations in which it is very valuable to be able to verify (with a reasonably high degree of certainty) that people are who they claim to be.

A smart card is an ideal tool for this: a person can carry a card that records his or her identity, a biometric and a certificate linking the two. We can regard these as three statements:

- 'I am John Smith; my reference is 123456789.'
- 'This is my fingerprint (or iris scan, signature, etc.)'
- 'We (The US Government, Acme Manufacturing Corporation ...) assert that the person whose fingerprint matches this one is indeed John Smith, reference 123456789.'

Provided the person relying on this card trusts the US Government and knows its public key, this is a very dependable form of authentication.

We will see in Chapter 4 that many forms of biometric data can be stored very efficiently in a smart card.

1.3.4 Multiple applications

Smart cards are particularly valuable when they combine a number of functions. As we will see in the next chapter, there are several ways to create a multi-function card, but the smart card's unique ability to carry several different programs (normally known as card applications) makes them capable of performing a much wider range of functions than other card types.

For example, the Malaysian identity card (described in more detail in Chapter 17) also carries a driving licence, health services entitlement, electronic cash and a digital signature to permit signing of e-commerce transactions. Some Mexican bank customers can store the URLs of their favourite websites, together with their usernames and passwords, on their bank cards.

1.3.5 The universal helper

This general ability to carry out seemingly unrelated tasks has led to many futuristic descriptions of the single card that accompanies its holder through daily life, giving access to trains, buildings and computers, keeping appointments, making payments, and even making coffee to the user's exact taste.

The user, of course, would own such a card and determine what applications are loaded. It may not actually be card-shaped; it could be contained in a mobile phone, wristwatch, key-fob or ring.

Although these are all technically possible, this is not how users see their cards today. In practice, most cards embody a *relationship* of the holder with the card issuer: an employer, service company, bank or government. As we will see, there are several categories of use type and relationship, and the second half of this book is concerned with the ways in which those translate into business requirements for a smart-card project.

1.4 The smart-card business

After a slow start, the smart-card industry has grown steadily over the last 15 years as new applications have been developed using this technology and subsequently rolled out to new countries.

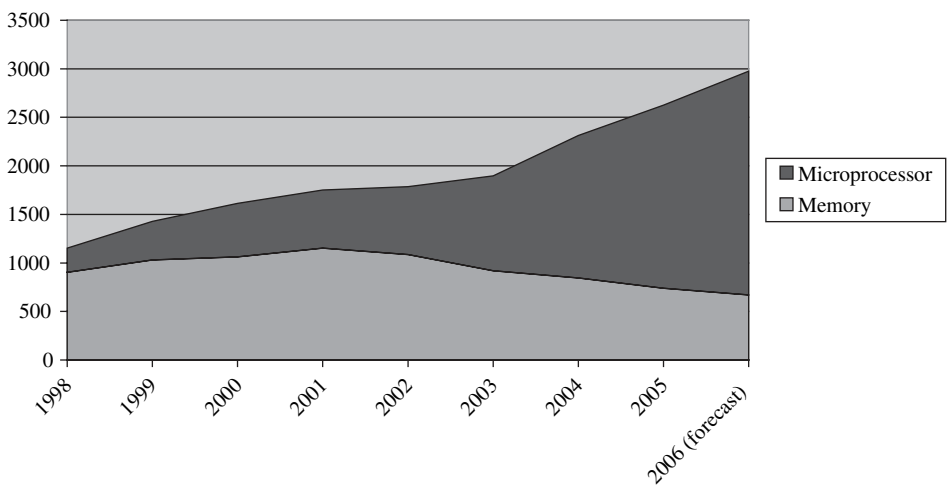

Figure 1.2 Growth in smart-card shipments 1998–2006 (source: Eurosmart)

Figure 1.2 shows the growth of smart-card shipments over the last eight years; this also shows how memory cards have become less important and microprocessor-based cards form a larger proportion of the total. The differences in the technology will be discussed in more detail in Chapter 3, but it is important to note that memory cards can still offer a level of security that is often adequate for closed systems: many transportation schemes, for example, will continue to use memory cards for years to come.

Figure 1.3 Smart-card market by region 1998 and 2005 (source: Eurosmart)

Figure 1.3 shows the way in which the geographic balance of the market has changed; whereas this technology originated in Europe, the main feature of the first few years of the 21st century has been the growth of Asian, and in particular Chinese-speaking, markets. China now accounts for one third of all SIM cards sold in the world, and the new generation of Chinese national ID cards will represent a further massive increase in this market over the next few years.

These developments have driven business at both the top and bottom ends of the market: in China, many new manufacturers have been established and are supplying a

large proportion of local demand, for low-capacity SIM cards in particular. Countries like Taiwan, Korea and Malaysia, on the other hand, are the main motors for large multi-application cards.

Companies in the smart-card business have been through some rough periods: when demand was high, semiconductor supplies limited sales, and now as both demand and supply have grown, it has become difficult to maintain sufficient margins to pay for development of the new products that users are seeking.

The multi-application smart card, in particular, offers the opportunity for vendors throughout the supply chain to increase the value they add by creating more revenue streams, and at the same time to differentiate themselves from their competitors through both the products and services they offer.

1.5 Structure of this book

Part I sets the scene for the rest of the book: in Chapter 2 we look at the different ways of defining a multi-application smart-card scheme, and the different technologies that can be used to construct one. Chapter 3 covers the basics of smart cards and could be skipped by those who are already familiar with the technology.

Part II describes the different technologies used in multi-application smart cards, starting with two disciplines that are critical to most multi-application usage: biometrics and cryptography. In Chapter 6 we turn back to card technology, and look in more detail at the current state of the art, particularly in relation to microcontrollers and interfaces, including contactless interfaces. Chapter 7 does the same thing for reader and terminal technology, then Chapter 8 looks in more detail at the multi-application functions built into the core ISO 7816 family. Chapters 9 and 10 describe the two main families of multi-application operating system: JavaCard – GlobalPlatform and Multos, and in Chapter 11 we look at other operating systems with specific multi-application features. Chapter 12 addresses the complexities of card management systems for multi-application cards, and in particular what functions are needed in a card management system according to the type of scheme.

Part III is concerned with applications. It covers, in turn, the main application sectors for smart cards: telecommunications, banking and finance, transportation and government, and closes with those applications used by corporations, as well as universities, schools and other organisations for ‘campus cards’ and other closed user-group schemes. This part of the book looks at a very wide range of applications, including many that are today most often implemented on single-application cards. It seeks to show the business drivers and relationships behind each application and the implementation barriers, so that users from other sectors can see whether these applications would be suitable for inclusion in their cards, and how these drivers and relationships go together to construct a business case and a specification for a multi-application card project.

The book closes with three chapters on implementing multi-application cards: Chapter 19 looks at how to organise and structure a project team, and the difficulties

of working with unmatched structures. Chapter 20 draws some lessons on specification and project management, while Chapter 21 attempts to draw some conclusions as to the applications and sectors most likely to succeed in the coming years.

Throughout the book, there are many case studies drawn from practice, in most cases contributed by the project managers responsible. They cover a wide range of sectors, countries and technology solutions, but each has some useful lessons for would-be implementors and will, the author hopes, increase the chances of success for those willing to learn from history and experience.

The book also includes as Appendices a glossary, references for further reading and a list of standards relevant to multi-application smart cards.

2 When is a card multi-application?

The term 'multi-application card' is used in different ways by different groups of people: the marketing department sees the card in terms of selling features, the IT department according to the technologies used by the card, and the operations department looks at the number of processes the card supports.

This chapter explores the definitions of the term and sets the framework within which the remainder of the book will use it.

2.1 Single-function cards

Most smart cards have a single function. There is a simple reason for this: the card issuer has issued the card to solve a specific problem or to provide a specific service. The relationship between the card issuer and the card-holder is generally not complex, while most card issuers are in one well-defined business. So there is no reason for the card issuer to provide multiple functions on the card, which in most cases would add to the cost.

Smart cards are, in many cases, replacing a magnetic stripe or visual identification card, which generally had only one function. So, for example, the earliest smart cards were used mainly for public telephones: they held value that could be loaded by the telephone company and decremented by the user making calls, and this was their only function. Many schools issue cards to their pupils for recording attendance at classes, while companies issue cards to their employees for access to buildings. These cards need no further functions.

Most single-function cards are either memory cards or microprocessor cards with only a very small fixed program. To be very precise, we do need to be careful when we talk about cards where only one function is used, because in some cases the card itself is capable of performing other functions . . . but that will become clear later.

2.2 Multi-function cards

From the card-holder's perspective, the card becomes more useful when it can perform more *functions*. This has nothing to do with the number of applications, since multiple functions can be provided in several other ways: