SOFTWARE CONTROL SERVICES (PTY) LTD

475 King's Highway, Lynnwood
P.O.Box 36675, Menlo Park
Pretoria, South Africa
0102

(t) +27 12 348 7301
(f) +27 12 348 1129
(e) techsupport@softconserv.com
www.softconserv.com

Smart Card.

Version 0. 1

Prepared by: Michael Davis- Hannibal

Softcon Software Control Services (Pty) Ltd.

7 March 2017

Revision History

Name	Date	Reason For Changes	Version
MDH	28-Jul-10	Initial document	0.1

Contents

1. General

A smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps dedicated security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate . Smart cards may also provide strong security authentication for single sign-on within large organizations.

Figure 1:Many different pad layouts can be found on a contact Smart card

2. Overview

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.370 × 2.125 in). Another popular size is ID-000 which is nominally 25 by 15 millimetres (0.984 × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimetres (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services via card-reading devices, such as ticket readers, ATMs, etc.

a. Benefits

Smart cards can provide identification, authentication, data storage and application processing.

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

Governments gain a significant enhancement to the provision of publically funded services through the increased security offered by smart cards. These savings are passed onto society through a reduction in the necessary funding or enhanced public services.

Individuals gain increased security and convenience when using smart cards designed for interoperability between services. For example, consumers only need to replace one card if their wallet is lost or stolen. Additionally, the data storage available on a card could contain medical information that is critical in an emergency should the card holder allow access to this.

3. History

In 1968 German rocket scientist Helmut Gröttrup and his colleague Jürgen Dethloff invented the automated chip card, receiving a patent only in 1982. The first mass use of the cards was as a Télécarte for payment in French pay phones, starting in 1983.

French inventor Roland Moreno[2] patented the memory card concept[3] in 1974. In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card. In 1978, Bull patented the SPOM (Self Programmable One-chip Microcomputer) that defines the necessary architecture to program the chip. Three years later, Motorola used this patent in its "CP8". At that time, Bull had 1,200 patents related to smart cards. In 2001, Bull sold its CP8 division together with its patents to Schlumberger, who subsequently combined its own internal smart card department and CP8 to create Axalto. In 2006, Axalto and Gemplus, at the time the world's no. 2 and no. 1 smart card manufacturers, merged and became Gemalto.

The second use integrated microchips into all French Carte Bleue debit cards in 1992. Customers inserted the card into the merchant's POS terminal, then typed the PIN, before the transaction was accepted. Only very limited transactions (such as paying small highway tolls) are processed without a PIN.

Smart-card-based "electronic purse" systems store funds on the card so that readers do not need network connectivity and entered service throughout Europe in the mid-1990s, most notably in Germany (Geldkarte), Austria (Quick), Belgium (Proton), France (Mon€o[4]), the Netherlands (Chipknip and Chipper), Switzerland ("Cash"), Norway ("Mondex"), Sweden ("Cash", decommissioned in 2004), Finland ("Avant"), UK ("Mondex"), Denmark ("Danmønt") and Portugal ("Porta-moedas Multibanco").

The major boom in smart card use came in the 1990s, with the introduction of smart-card-based SIMs used in GSM mobile phone equipment in Europe. With the ubiquity of mobile phones in Europe, smart cards have become very common.

The international payment brands MasterCard, Visa, and Europay agreed in 1993 to work together to develop the specifications for smart cards as either a debit or a credit card. The first version of the EMV system was released in 1994. In 1998 a stable release of the specifications became available. EMVco, the company responsible for the long-term maintenance of the system, upgraded the specification in 2000 and in 2004.[5] EMVco's purpose is to assure the various financial institutions and retailers that the specifications retain backward compatibility with the 1998 version.

With the exception of countries such as the United States EMV-compliant cards and equipment are widespread. Typically, a country's national payment association, in coordination with MasterCard International, Visa International, American Express and JCB, jointly plan and implement EMV systems.

Contactless smart cards that do not require physical contact between card and reader are becoming increasingly popular for payment and ticketing applications such as mass transit and highway tolls. Visa and MasterCard have agreed to an easy-to-implement version that was deployed in 2004–2006 in the USA. Most contactless fare collection implementations are custom and incompatible, though the MIFARE Standard card from Philips has a considerable market share in the US and Europe.

Smart cards are also being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, drivers’ licenses, and patient card schemes are appearing. In Malaysia, the compulsory national ID scheme MyKad includes eight different applications and has 18 million users. Contactless smart cards are part of ICAO biometric passports to enhance security for international travel.

4. Contact smart card

Contact smart cards have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pad provide electrical connectivity when inserted into a reader.[6]

The ISO/IEC 7810 and ISO/IEC 7816 series of standards define:

- physical shape and characteristics
- electrical connector positions and shapes
- electrical characteristics
- communications protocols, including commands sent to and responses from the card
- basic functionality

Cards do not contain batteries; power is supplied by the card reader.

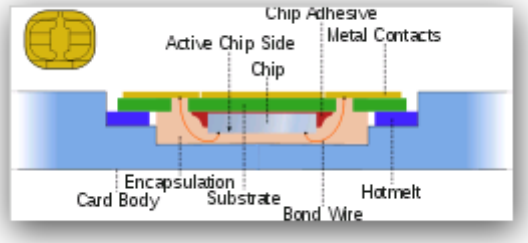

Figure 2: Illustration of smart card structure and packaging

a. Reader

Contact smart card readers are used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone.

Because the chips in financial cards are the same as those used in Subscriber Identity Modules (SIMs) in mobile phones, programmed differently and embedded in a different piece of PVC, chip manufacturers are building to the more demanding GSM/3G standards. So, for example, although the EMV standard allows a chip card to draw 50 mA from its terminal, cards are normally well below the telephone industry's 6 mA limit. This allows smaller and cheaper financial card terminals.

5. Contactless

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology (at data rates of 106–848 kbit/s). These cards require only proximity to an antenna to communicate. They are often used for quick or hands-free transactions such as paying for public transportation without removing the card from a wallet.

ISO/IEC 14443 is the standard for contactless smart card communications. It defines two types of contactless cards (A and B). Proposals for ISO/IEC 14443 types C, D, E, F and G have been rejected by the International Organization for Standardization.[citation needed] An alternative standard is ISO/IEC 15693, which allows communications at distances up to 50 cm (20 in).

Examples of widely used contactless smart cards are Montreal's Opus card, Hong Kong's Octopus card, Shanghai's Public Transportation Card, Moscow's Transport/Social Card, Bucharest's Cardul Activ used as a cash card for public transport within Bucharest, South Korea's T-money (bus, subway, taxi), Melbourne's myki, the Netherlands' OV-chipkaart, Milan's Itinero, London's Oyster card, London's sQuidcard which is used for small payments in Thames Ditton, Bolton and Dundee, Japan Rail's Suica card, Iran's Metropolitans Subway Corp., Israel's Rav-Kav, Mumbai's Brihanmumbai Electric Supply and Transport and Beijing's Municipal Administration and Communications Card. All of them are primarily designed for public transportation payment and other electronic purse applications.

Like smart cards with contacts, contactless cards do not have a battery. Instead, they use a built-in inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

a. Credit cards

These are the best known payment cards (classic plastic card):

- Visa: Visa Contactless, Quick VSDC—"qVSDC", Visa Wave, MSD, payWave
- MasterCard: PayPass Magstripe, PayPass MChip
- American Express: ExpressPay

Roll-outs started in 2005 in USA. Asia and Europe followed in 2006. Contactless (non PIN) transactions cover a payment range of ~$5–50. There is an ISO/IEC 14443 PayPass implementation. Some, but not all PayPass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is a typical USA card technology (PayPass Magstripe and VISA MSD). The cards do not hold/maintain the account balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.

EMV cards have contact and contactless interfaces. They work as a normal EMV card via contact interface. Via contactless interface they work somewhat differently in that the card command sequence adopts contactless features such as low power and short transaction time.

6. Hybrids

Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, that uses a chip with both contact and contactless (ISO/IEC 14443 Type B) interfaces.

7. Cryptographic smart cards

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA. Today's cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signature and secure identification, (see applications section).

The most common way to access cryptographic smart card functions on a computer is to use a vendor-provided PKCS#11 library.[citation needed] On Microsoft Windows the CSP API is also supported.

The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called "crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart card are also made to support the NIST standard for Personal Identity Verification (PIV).

8. Applications

a. Computer security

The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing.

Some disk encryption systems, such as FreeOTFE, TrueCrypt and Microsoft Windows 7 BitLocker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.

Smart cards are also used for single sign-on to log on to computers.

Smart cards support functionality has been added to Windows Live Passports.

b. Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters and vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and the accepting machine. No connection to the issuing bank is necessary, so the holder of the card can use it even if not the owner. Examples are Proton, Geldkarte, Chipknip and Mon€o. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

c. Health care (medical)

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives and mandates, and provide the platform to implement other applications as needed by the health care organization.

d. Identification

A quickly growing application is in digital identification. In this application, the cards authenticate identity. The most common example employs PKI. The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and various identification cards used by many governments for their citizens. Combined with biometrics, cards can provide two- or three-factor authentication. Smart cards are not always privacy-enhancing, because the subject carries possibly incriminating information on the card. Contactless smart cards that can be read from within a wallet or even a garment simplify authentication.

The first smart card driver's license system in the world was issued in 1995 in Mendoza province of Argentina. Mendoza had a high level of road accidents, driving offenses, and a poor record of recovering outstanding fines.[citation needed] Smart licenses hold up-to-date records of driving offenses and unpaid fines. They also store personal information, license type and number, and a photograph. Emergency medical information such as blood type, allergies, and biometrics (fingerprints) can be stored on the chip if the card holder wishes. The Argentina government anticipates that this system will help to collect more than $10 million per year in fines.

In 1999 Gujarat was the first Indian state to introduce a smart card license system. To date[when?] it has issued 5 million smart card driving licenses to its people.
“ a national ID card, protected by a 1,024-bit key code, is impossible to break without a supercomputer working away for a hundred years ”

By the start of 2009 the entire population of Spain and Belgium will have an eID card, that is used for identification. These cards contain 2 certificates: one for authentication and one for signature. This signature is legally enforceable. More and more services in these countries use eID for authorization.

e. Other

Smart cards are widely used to protect digital television streams. VideoGuard is a specific example of how smart card security worked (and was cracked).

The Malaysian government uses smart identity cards carried by all citizens and resident non-citizens. The personal information inside the MYKAD card can be read using special APDU commands.

9. Security

Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The chip usually implements some cryptographic algorithm. There are, however, several methods for recovering some of the algorithm's internal state.

a. Differential power analysis

Differential power analysis involves measuring the precise time and electrical current required for certain encryption or decryption operations. This can deduce the on-chip private key used by public key algorithms such as RSA. Some implementations of symmetric ciphers can be vulnerable to timing or power attacks as well.

b. Physical disassembly

Smart cards can be physically disassembled by using acid, abrasives, or some other technique to obtain unrestricted access to the on-board microprocessor. Although such techniques obviously involve a fairly high risk of permanent damage to the chip, they permit much more detailed information (e.g. photomicrographs of encryption hardware) to be extracted.

10. Problems

The plastic card in which the chip is embedded is fairly flexible, and the larger the chip, the higher the probability that normal use could damage it. Cards are often carried in wallets or pockets—a harsh environment for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction. Using a smart card for mass transit presents a privacy risk, because it allows the mass transit operator (and the government) to track an individual's movement. In Finland, the Data Protection Ombudsman prohibited the transport operator YTV from collecting such information, despite YTV's argument that the card owner has the right to a list of trips paid with the card. Prior to this, such information was used in the investigation of the Myyrmanni bombing. Client-side identification and authentication cards are the most secure way for e.g., internet banking applications, but security is never 100% sure. If the account holder's computer hosts malware, the security model may be broken. Malware can override the communication (both input via keyboard and output via application screen) between the user and the application. The malware (e.g. the trojan Silentbanker) could modify a transaction, unnoticed by the user. Banks like Fortis and Dexia in Belgium combine a smart card with an unconnected card reader to avoid this problem. The customer enters a challenge received from the bank's website, a PIN and the transaction amount into the reader, The reader returns an 8-digit signature. This signature is manually entered into the personal computer and verified by the bank, preventing malware from changing the transaction amount.

Another problem is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".

11. References

- en.wikipedia.org