Card Payment Systems

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

IIT Bhilai

November 16, 2019

Overview

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

1. Technologies Used
   - Magnetic Stripe Cards
   - Chip Based Smart Cards
   - Contactless Smart Cards
2. Financial Transactions- ISO/IEC 8583
3. TLS

Technologies Used

The most common technologies used to carry information on cards are as follows:

- Magnetic Stripes
- Contact-Based Chips
- Contactless Chips

Magnetic Stripe Cards

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

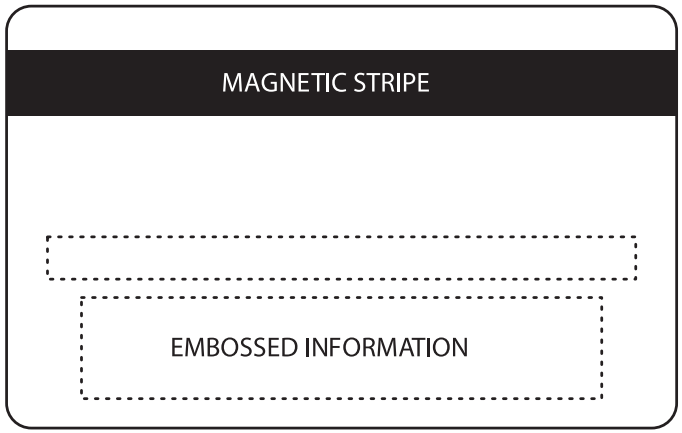
Magnetic stripe cards are used in various industries due to their ease of use, low manufacturing costs and the simple data formatting. Their extensive use has led to the establishment of various standards (and their subsequent revisions).
As time progressed, newer and safer technologies like contact-based cards have been introduced but have not been able to entirely phase out the magnetic stripe.

Magnetic Stripe Cards: Working Principle

- The magnetic stripes contain a recording medium to retain the information. The high retentivity of fer- romagnetic material makes such materials ideal for storage. The particles of these materials are analogous to bits in that their two orientations are used to store data in a binary manner.
- In the initial state (demagnetized/non-active) all the particles point in the same direction. The writing head of a device may write data onto the card by applying a strong magnetic field to change the direction in which the particles are polarized in. The reading head of a device simply captures the magnetic field of each particle and converts it to the corresponding (pre-agreed) bit.

Magnetic Stripe Cards: Physical Properties

- Length and breadth: 85.72 to 85.47 mm and 54.03 to 53.92 mm respectively.
- Radius of edge rounding: 3.48 to 2.88 mm
- Thickness: 0.84 to 0.68 mm



Magnetic Stripe Cards: HiCo and LoCo

- The basic difference between the two is the strength of the magnetic field used to write onto the tracks of the magnetic card.
- The HiCo cards are require a higher magnetic field to encode, and thus can be used for credit cards and other cards that are routinely used.
- On the other hand, cards that contain data that needs to be changed frequently (like hotel room cards) are mainly LoCo cards, as the magnetic energy used to encode these cards is less than that used to encode HiCo cards.

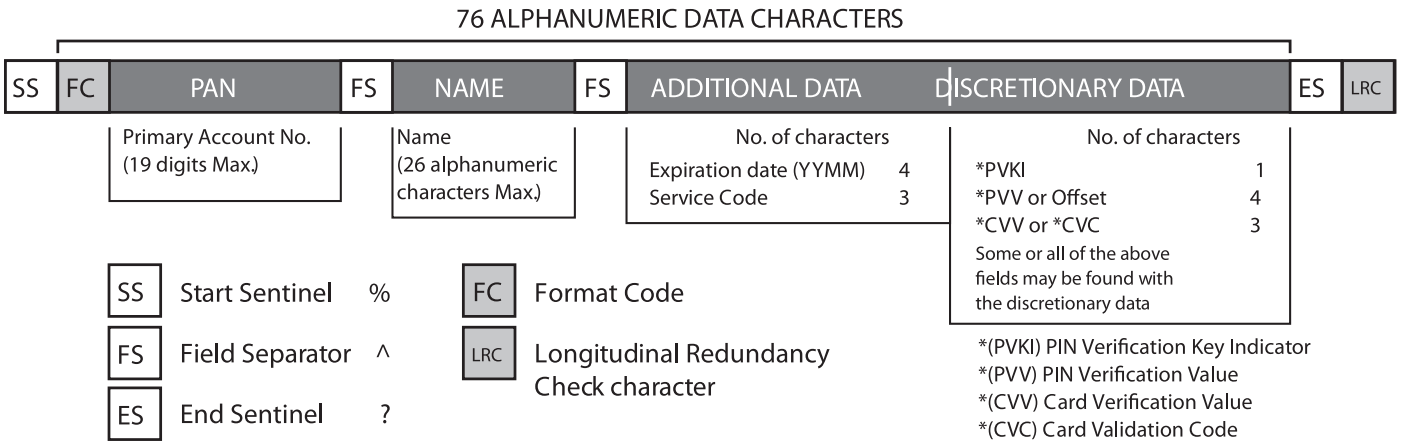
Magnetic Stripe Cards: Magnetic Tracks

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

Each card has a minimum of two tracks (track 1 and 2). Each track has an encoding format and configuration. There are cards with three tracks, however the third track is rarely seen in the ususal cards we are familiar with. Thus, the placement of the stripe differs.

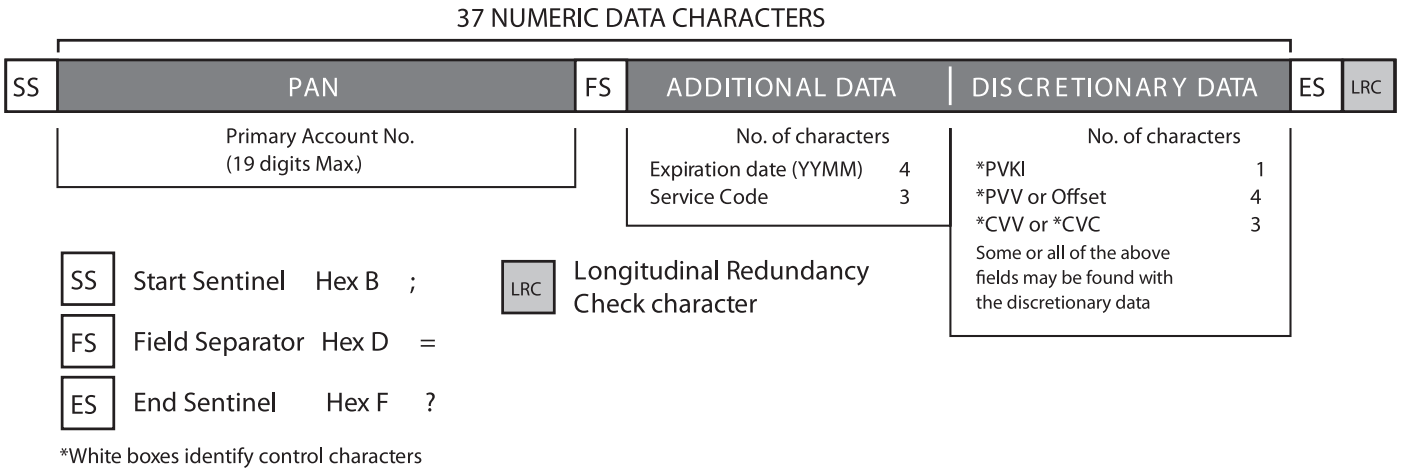
Magnetic Stripe Cards: Track 1

- Average Recording Density (bits per inch) = 210 bpi ± 8%
- 7 bits per character
- 79 alphanumeric characters (including control characters). The control characters (! & * + , : ; ¡ = ¿ @ _) may not be used for any information data.



Magnetic Stripe Cards: Track 2

- Average Recording Density (bits per inch) = 75 bpi ± 5%.
- 5 bits per character.
- 40 numeric characters (including control characters).The control characters (: ¡ ¿) may not be used for any information data.



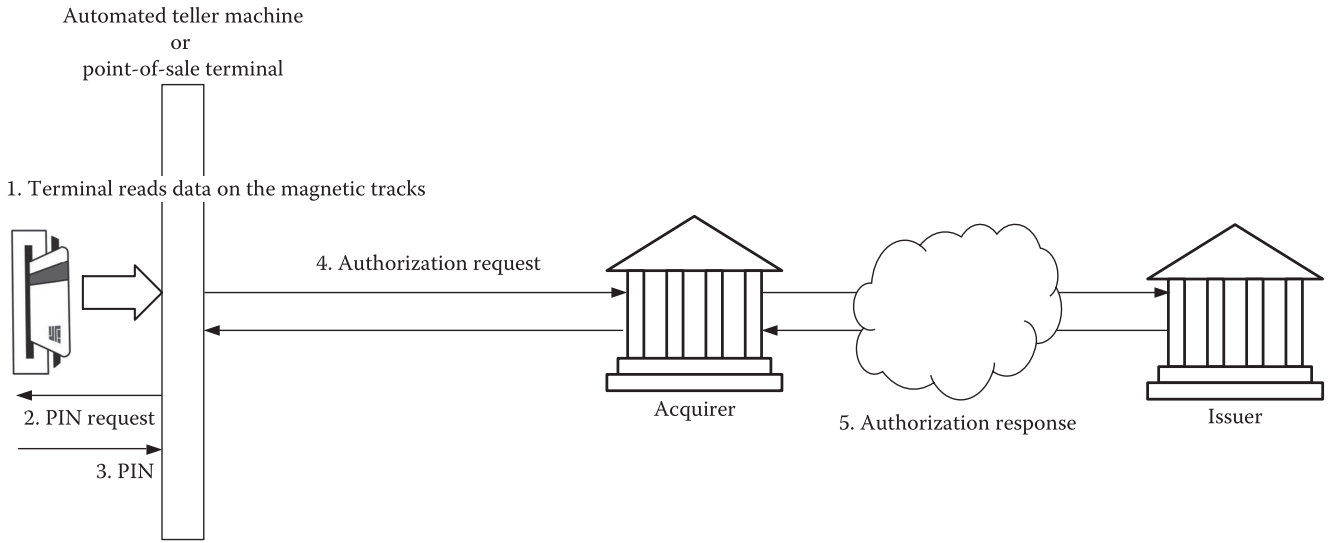
Magnetic Stripe Cards: Track 3

- Average Recording Density (bits per inch) = 210 bpi $\pm$ 8%.
- 5 bits per character.
- 107 numeric characters (including control characters).

Magnetic Stripe Cards: Financial Transactions

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

The widespread use of magnetic stripe cards is evident in their applications in credit cards and debit cards. The general process of a transaction is as follows:



Magnetic Stripe Cards: Drawbacks

Due to the inherent simplicity of the manner in which data is stored, magnetic stripe cards are often considered as easy to manipulate. A few drawbacks are as listed:

- The card holder's details are not encrypted.
- The exchanges between the card and card reader are not encrypted.
- The card is a passive participant in the transaction. This means that as the card has no computational abilities and therefore the stored data is a lot less secure than when it is stored in the IC cards due to their ability to perform cryptographic computations for confidentiality, integrity, and authentication.
- Data recorded on the magnetic stripe can easily be altered using a standard read/write device, and it is difficult to prove such changes afterward.

Chip Based Smart Cards

Chip Based Smart Cards

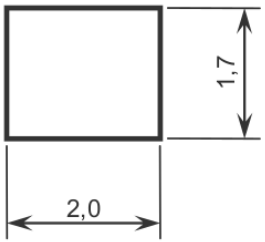
A chip-based smart card is a plastic card with a computer chip embedded in it. This chip can either be a memory-only or a microprocessor chip. Their ability to do several complex computations make them most suitable for banking. There are several other applications of chip-based smart cards such as healthcare, transportation, SIM etc. They provide better security of data than magnetic stripe cards that is why most of the banking services now use chip-based cards.

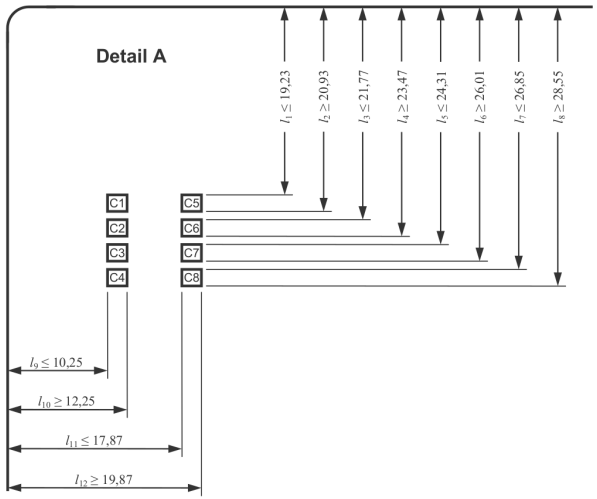
Chip Based Smart Cards: Working Principle

Chip-based cards store data in chip embedded in the card. These chip have a operating system (depends upon the purpose of card) which provides access control. When the card is connected to a interface device, the card authenticates the device via challenge-response mechanism and gives access to relevant data. This data is used by the interface device to perform the transaction.

Chip Based Smart Cards: Physical Properties

There are a total of 8 contacts from C1 to C8. Each of which have a minimum dimension of $2mm \times 1.7mm$.





Chip Based Smart Cards: Contacts

The contacts of chip has following usage:

C1: Supply power Input(V_{CC})

C2: Reset signal Input(RST)

C3: Clock signal Input(CLK)

C5: Ground (GND)

C6: Standard or Proprietary use(SPU)

C7: Input/Output for serial data(I/O)

We don't use C4 and C8. These are reserved auxiliary functions.

Chip Based Smart Cards: Operating Procedure

There are three operating classes based on V_{CC} supply by interface to card.

1. 5V for class A
2. 3V for class B
3. 1.8V for class C

The card supports atleast one of the above classes.

Chip Based Smart Cards: Activation

The interface device performs an activation by doing the following:

- puts RST to L.
- supplies power to V_{CC}.
- puts I/O in the interface device in reception mode.
- provides CLK with a clock signal.

Chip Based Smart Cards: Cold Reset

- The clock signal is applied to CLK at time T_a.
- The card should set I/O to state H within 200 clock cycles after the clock signal is applied to CLK.
- The cold reset results from maintaining RST at state L for at least 400 clock cycles after the clock signal is applied to CLK.
- After at least 400 clock cycles RST is put to state H. The answer on I/O shpuld begin between 400 to 40,000 clock cycles after RST is put to H otherwise, interface performs deactivation.

Chip Based Smart Cards: Deactivation

When information exchange is completed or aborted, the interface device deactivates the circuit in the following order:

- puts RST to state L.
- puts CLK to state L.
- puts I/O to state L.
- deactivates V_{CC} .

Chip Based Smart Cards: Answer-to-Reset

Answer-to-Reset has the following structure:

- Initial character TS followed by a sequence of at most 32 characters.
- Format character T0 is mandatory. Others are optional.
- The interface charaters TA, TB, TC, TD.
- The historical characters $T_1, T_2, T_3 \ldots T_K$
- The check character TCK.

Chip Based Smart Cards: Initial character TS

The initial character TS has two possible patterns.

- (H)LHHL LLL LLH sets up the inverse convention: state L encodes value 1 and moment 2 conveys the most significant bit (msb first). When decoded by inverse convention, the conveyed byte is equal to '3F'.
- (H)LHHL HHH LLH sets up the direct convention: state H encodes value 1 and moment 2 conveys the least significant bit (lsb first). When decoded by direct convention, the conveyed byte is equal to '3B'.

Chip Based Smart Cards: Format Byte T0

- Bits 8 to 5 form an indicator Y_1.
- Bits 4 to 1 encode a number K.

The Bits of Y_1 (from msb) state whether TD_1, TC_1, TB_1, TA_1 are present or not.

Chip Based Smart Cards: Interface Bytes

The coding structure of TD_i is as following:

- Bits 8 to 5 form an indicator Y_{i+1}.
- Bits 4 to 1 encode a number T.

Here, Bit 5 corresponds to TA_i, Bit 6 to TB_i, Bit 7 to TC_i and Bit 8 to TD_i.These bits of Y_i state whether corresponding interface bytes are present or not.
The number T refer to transmission protocol.

Chip Based Smart Cards: Interface Bytes

- Bits 8 to 5 of TA_1 encodes the maximum frequency(f_{max}) supported by the card and clock rate conversion integer(F_i) and Bits 4 to 1 indicate the value of Baud rate adjustment integer(D_i).
- TB_1, TB_2 are deprecated and are no longer used i.e. the interface should ignore them.
- TC_1 encodes the extra Gaurd Time integer ranging from 0 to 255.

Chip Based Smart Cards: Historical Bytes and TCK

- Historical bytes describe the operating charcteristics of card. If $K = 0$ then Historical Bytes are not present.
- For check byte(if present), the XOR of all the Bytes from T0 to TCK shall give '00'.Any other value is invalid. If T=0 is indicated by default only then TCK is absent.

Chip Based Smart Cards: Protocol and Parameter Selection

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

A PPS request and response each consists of initial bytes PPSS and PPS0 followed by three optional bytes PPS_1, PPS_2, PPS_3 and a check byte PCK.

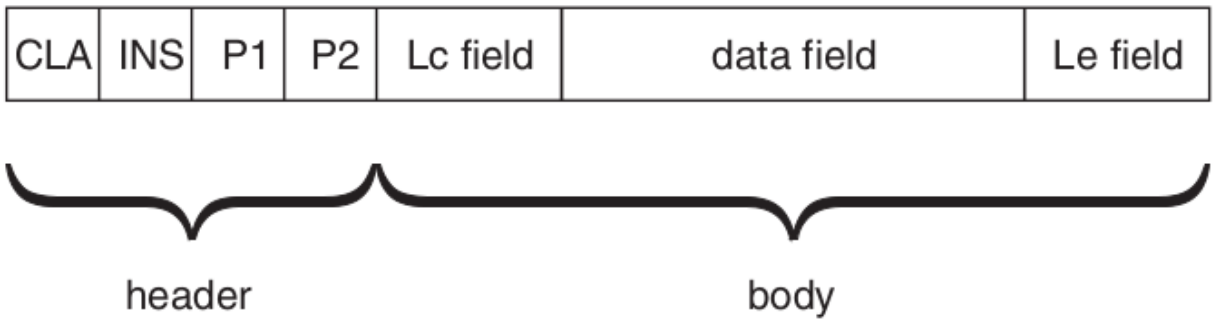
- PPSS identifies PPS request and response and is set to 'FF'.
- In PPS0, bit 5,6,and 7 indicate the presence of PPS_1, PPS_2, and PPS_3 while bit 4 to 1 indicate the value of T (Transmission Protocol). Bit 8 is reserved for future use.
- PPS_1 allows the interface device to propose values of F and D to the card. If it is not present default values are used.
- PPS_2 allows the interface device to propose a use of SPU.
- PPS_3 is reserved for future use.
- XOR of all bytes from PPSS to PCK should give '00'.

Chip Based Smart Cards: Message Structure

APDU(Application protocol data unit)s are used to exchange data between the card and the interface device. The design of the APDU that comply with ISO/IEC 7816-4 does not depend on the transmission protocol.

Command APDU Structure :

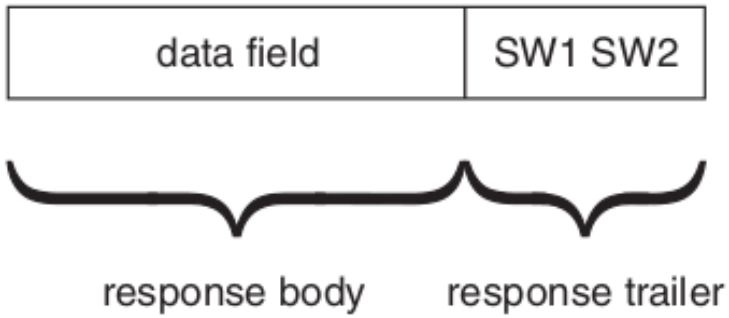
The APDU command structure consists of a header and a body.



Chip Based Smart Cards: Message Structure

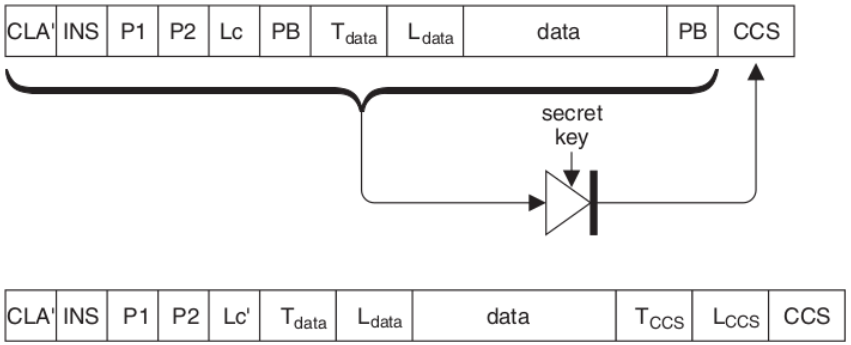
Response APDU Structure :

The response APDU sent by the card in reply to a command APDU consists of an optional body and a mandatory trailer.



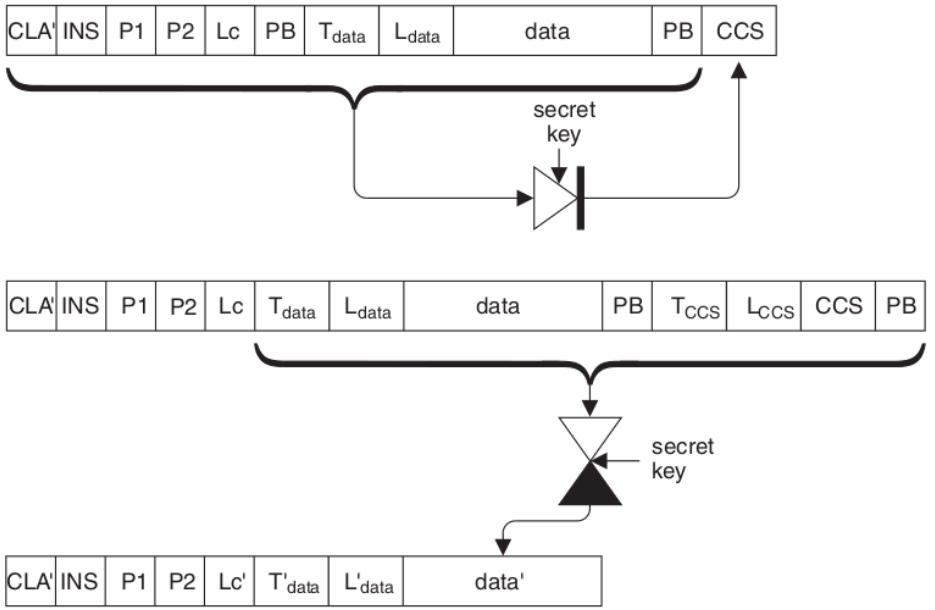
Chip Based Smart Cards: Data transmission Security

- To protect the data against manipulation during transmission first the command APDU in its initial format is generated.
- Then the data field of the APDU is converted into TLV coded data with the appropriate padding.
- The cryptographic checksum(CCS) of the datagram is calculated and a data object containing the CCS is appended to the APDU.
- The new command APDU as shown in Figure 18 is now sent to the card.



Chip Based Smart Cards: Data transmission Security

- For confidential transmission of data First the command APDU is generated and its Cryptographic checksum is calculated in the same way as in authentic transmission.
- After calculation of CCS the whole data field is then encrypted using a secret key and the new data object with the encrypted value is then attached to the APDU.



Contactless Smart Cards

Contactless Smart Cards: Basic Working Principle

Akash Diwaker (11740080), Harsh Lathi (11740380), Satyam Sachan (11740890)

In Contactless smart cards, the chip communicates with the card reader through RFID induction technology. These cards require only close proximity to an antenna to complete transaction. They are often used when transactions must be processed quickly or hands-free, such as on mass transit systems, where smart cards can be used without even removing them from a wallet.

Contactless Smart Cards: Communication Protocols

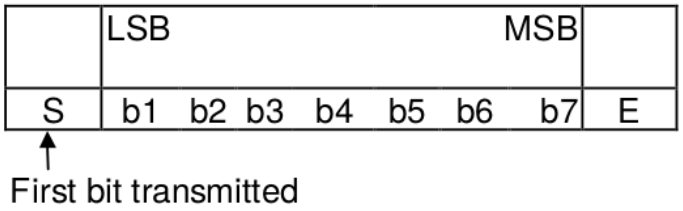
The initial dialogue between the PCD and the PICC shall be conducted through the following consecutive operations:

- activation of the PICC by the RF operating field of the PCD
- PICC waits silently for a command from PCD
- transmission of a command by PCD
- transmission of a response by PICC

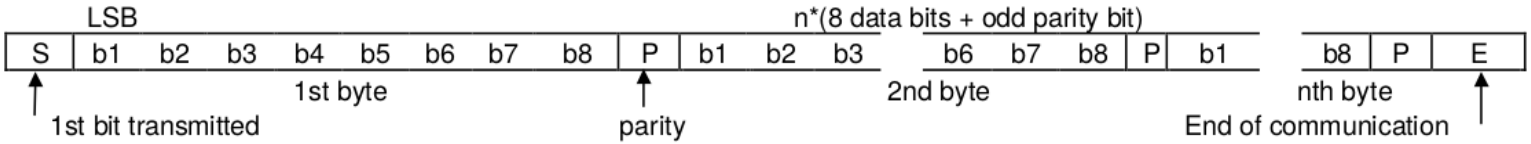
The ISO/IEC 14443 standard defines two different communication interfaces, which are designated Type A and Type B.

Contactless Smart Cards: Interface Type A

Data is stored the form of frames. A short frame is used to initiate communication. It has the following structure.

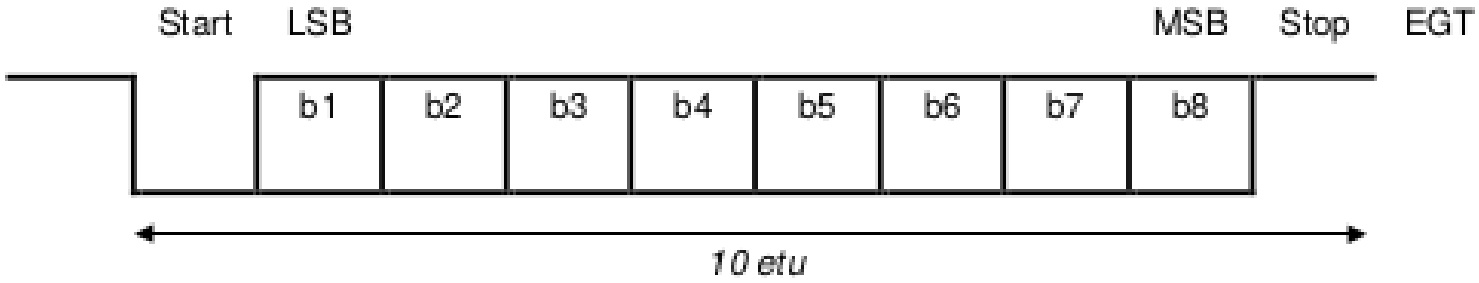


Standard frames are used for data exchange. Following figure shows the structure.

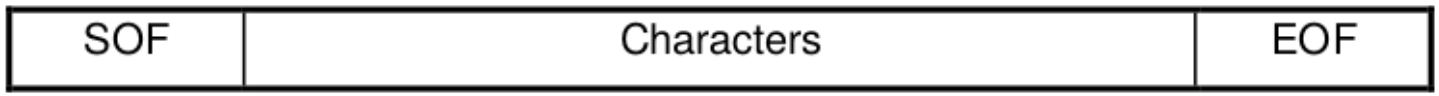


Contactless Smart Cards: Interface Type B

Data is stored the form of frames. A frame is composed of characters. A character has the following structure:



A frame has the following structure:



Contactless Smart Cards: Cryptographic Security

RFID systems are increasingly being used in high-security applications, such as access systems and systems for making payments or issuing tickets. However, the use of RFID systems in these applications necessitates the use of security measures to protect against attempted attacks, in which people try to trick the RFID system in order to gain unauthorised access to buildings or avail themselves of services (tickets) without paying.High-security RFID systems must have a defence against the following individual attacks:

- skimming of a data carrier in order to clone and/or modify data;
- placing a foreign data carrier within the interrogation zone of a reader with the intention of gaining unauthorised access to a building or receiving services without payment.

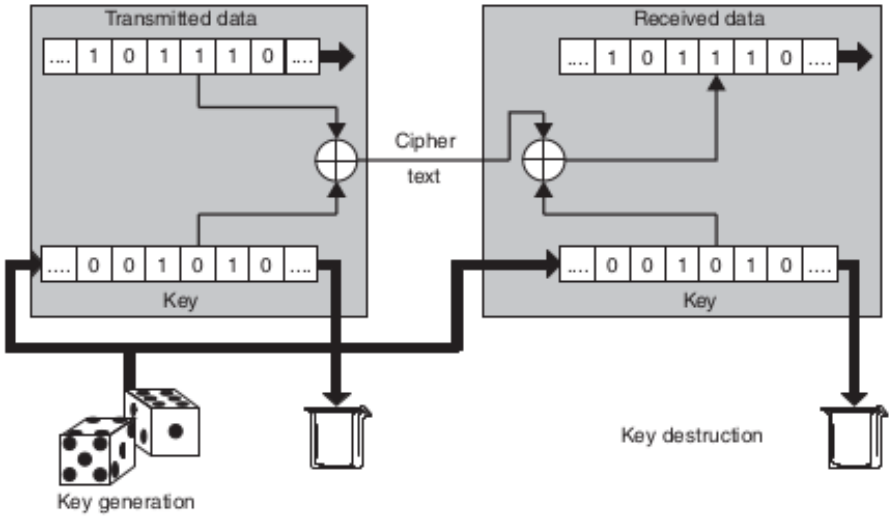
Contactless Smart Cards: Mutual Authentication

The mutual authentication procedure has the following advantages:

- The secret keys are never transmitted over the airwaves, only encrypted random numbers are transmitted;
- Recording an authentication sequence for playback at a later date (replay attack) would fail;
- A random key (session key) can be calculated from the random numbers generated, in order to cryptologically secure the subsequent data transmission.

Contactless Smart Cards: Stream Ciphers

Here, a random key is generated before transmission of encrypted data and it is made available to both parties. The random sequence must be as long as the message to be encrypted because periodic repeatitions of a short key would favour cryptanalysis and it creates an attack on transmission.



Contactless Smart Cards: Drawbacks

- Theft and Fraud - Contactless technology does not necessarily prevent use of a PIN for authentication of the user, but it is common for low value transactions not to require a PIN. This may make such cards more likely to be stolen, or used fraudulently by the finder of someone elses lost card.
- Multiple cards detection - When two or more contactless cards are in close proximity the system may have difficulty determining which card is intended to be used. The card-reader may charge the incorrect card or reject both.

Financial Transactions- ISO/IEC 8583

Financial Transactions- ISO/IEC 8583

- The standard ISO/IEC 8583 specifies how data is exchanged between systems during electronic transactions initiated by cardholders using payment cards. This includes all sorts of cards along with the PoS devices and ATM machines.
- Major financial services companies like Mastercard and VISA base their communications on this standard. It is important to note that although the standard defines the fields used in communication, it is also adaptible to individual networks and custom usage by the service providers. For example, VISA uses BASE1 and BASE2, two protocols that define the messsage structure. ISO/IEC 8583:1987 is used by Mastercard and VISA even after all the current revisions to the standard.

Financial Transactions- ISO/IEC 8583: Message Structure

This structure is often prepended by a network-specific header. It may be different for each network as per their requirements and is therefore not standardized.

Financial Transactions- ISO/IEC 8583: Message Structure (MTI)

The Message Type Identifier is 4 digits long, and describes the overall message class and function of the message. The four digits identify the following fields:

- The first digit indicates the version of ISO/IEC 8583 used in the message.
- The second digit specifies the purpose of the message.
- The third digit specifies the message function, which later defines the flow of information within the communication channels.
- The fourth digit defines the source of the message.

Financial Transactions- ISO/IEC 8583: Message Structure (Bitmap)

- The bitmap is a binary sequence that tells us if a particular data element is present in the message body or not. The data element is said to be present if the bit corresponding to that element is set to 1.
- A bitmap can indicate the presence of upto 192 field elements. The entire bitmap is divided into the sections depending upon the data element it can represent. The primary, secondary and tertiary bitmaps can represent 0-64, 65-128 and 129-192 elements (the numbers are the pre-defined index of the data elements).
- It is important to note that the secondary and tertiary bitmaps are optional, and their presence is indicated in the previous bitmap.
- The bitmap can be represented in two forms, by a byte representation or hex-value representation.

Financial Transactions- ISO/IEC 8583: Message Structure (Data Elements)

- Data elements are the actual data carrying fields, and contain data in a specified format. As the data is linearly written, it is important to consult the bitmap regarding which field element is written, which is then delimited by some value. Also, as not every field element may be of a fixed size, the length indicator is used.
- Along with the 'index' of the data element in the message body, the size of the element is also defined. For example, if a field is defined as `n 4`, the field is a fixed 4 digits in length. Similarly, a definition `b 4` would mean 4 bits of data.
- An `LLVAR` field element is of variable length, and can take values upto 100 digits. Similarly, `LLLVAR` is used to denote field value lengths of upto 1000 digits. For example, the Primary account number (PAN) is defined as a `19VAR` variable.

Financial Transactions- ISO/IEC 8583: Message Structure (Data Elements)

A few examples:

Data Field	Type	Definition
1	b 64	Second Bitmap
2	n ..19	PAN
3	n 6	Processing Code
4	n 12	Amount, transaction
7	n 10	Transmission date and time
65	b 1	Extended bitmap indicator
64	b 64	Message Authentication Code (MAC)

Financial Transactions- ISO/IEC 8583: Issues

ISO/IEC 8583 is a standard that defines the message format. However, multiple implementation details have not been standardized (to allow for the individual preferences of a provider to be integrated into the system). This leads to multiple interoperability issues.

- The encoding scheme for data (hex, ASCII, etc.) has not been mentioned. This may lead to misinterpretation of data.
- The usage of different versions of the same standard by different vendors could possibly lead to interoperability issues, especially when the message format is only based upon ISO/IEC 8583 and is not a direct implementation of the standard. The changes in the ordering and other details could lead to miscommunication.

Financial Transactions- ISO/IEC 8583: Issues

To prevent this from becoming an issue, we use interworking functions that act to convert the data from some form of data into a globally understood format. The conversion of the above mentioned format into the XML and then HTTP and other formats is often undertaken to allow interoperability. The IBM Integration Bus is an example of one such interworking functions.

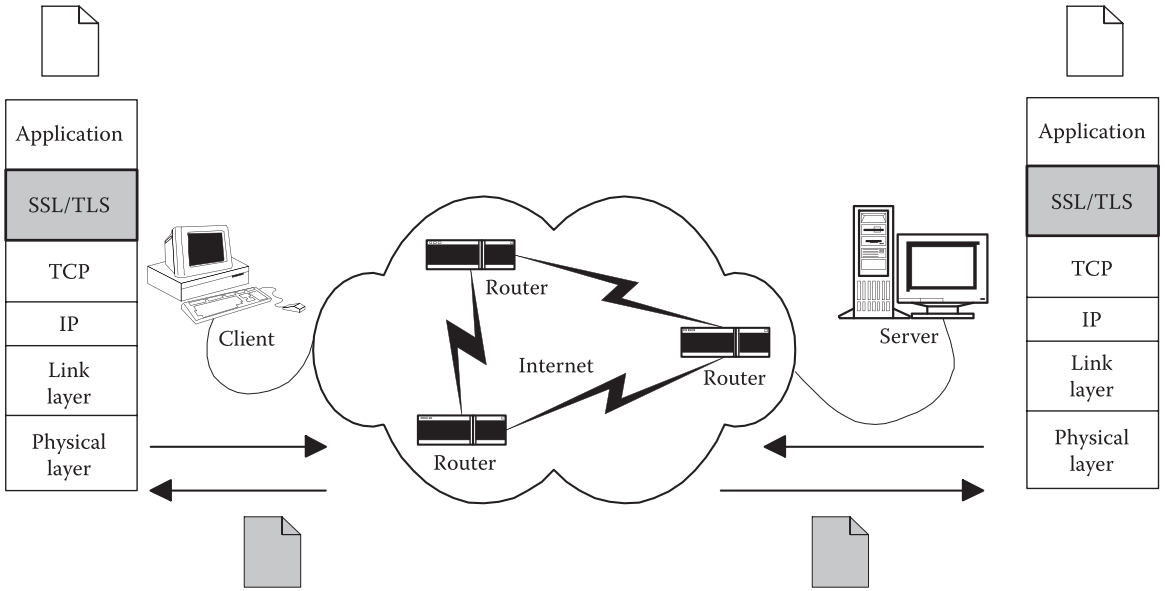
TLS (Transport Layer Security)

TLS

Multiple protocols were designed to secure bank card transactions initiated on open networks. TLS (Transport Layer Security) is the main focus of this report. SSL (Secure Socket Layer) is a predecessor of TLS and will be considered alongside TLS.

TLS: Architecture

SSL/TLS sits between the Application and Transport layers in the OSI (Open Systems Interconnection) networking model of the TCP/IP protocol stack.



TLS: Architecture

- It is important to note that only those transport protocols that can offer reliable transmission of data (such as TCP) can make use of the advantages of SSL/TLS. This is because an unreliable transport protocol (like UDP) may cause a flow interruption, which may be misinterpreted as a security break by the TLS protocol, thus causing a termination of the open session.
- The three goals of authentication, integrity and confidentiality are all served by TLS by combining all the functions that are needed to implement the three into a package called the cipher suite. The above-mentioned functions are decided upon during the 'handshake' phase of the transaction.

TLS: Handshake

The handshake is the very first event to occur during a transaction. It happens after the TCP handshake, another procedure that creates the reliable channel over which further communication will take place. The purpose of the handshake is to:

- Specify the version of TLS. The most recent version of TLS is `TLS 1.3`.
- Decide on which cipher suite they will use.
- Authenticate the identity of the server via the servers public key and the certificate authoritys digital signature.
- Generate session keys in order to use symmetric encryption after the handshake is complete.

TLS: Handshake

The actual implementation of this handshake depends upon various factors. The most important factor to consider is the version of TLS, as the handshakes across the different versions of TLS (such as `TLS 1.3` and `TLS 1.2`) differ in many ways. The handshake procedure in `TLS 1.3` is faster as a result of a change in what is sent across in every message. The increase in speed is thus attributed to a decrease in the number of round trips. Also, in `TLS 1.3` the 0-RTT (zero round trip) mechanism allows for data to be sent on the first message to the server on sites the client has previously visited.

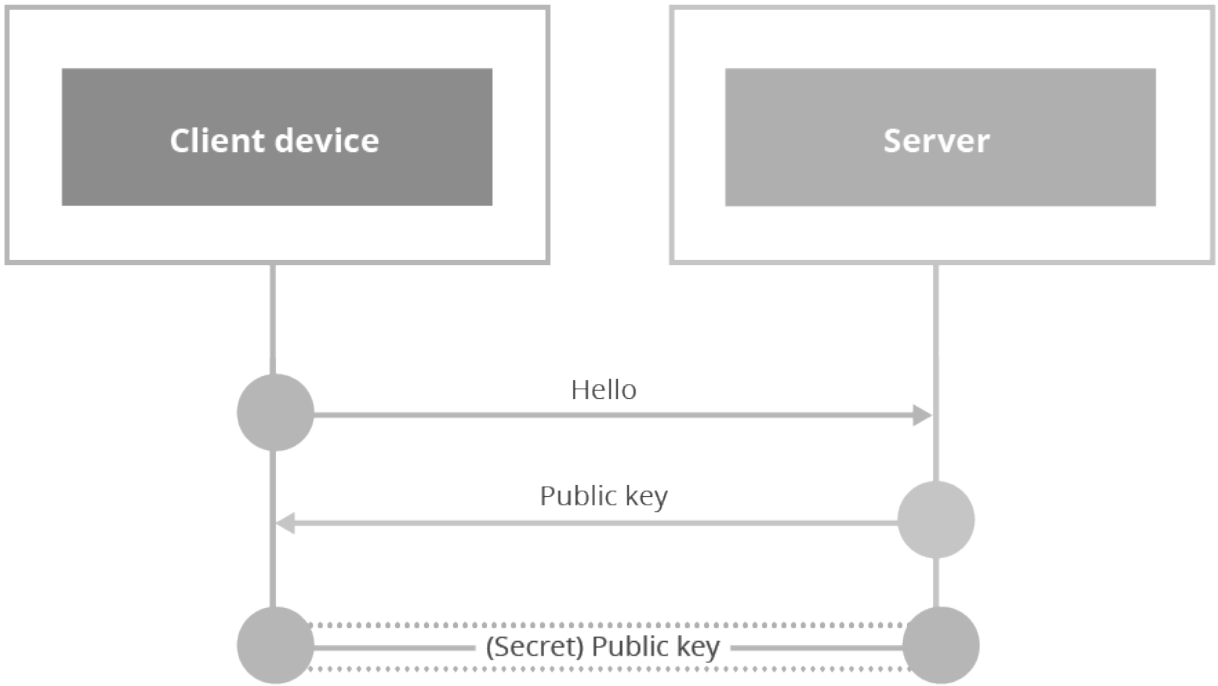
TLS: Authentication

Authentication takes place only at the session establishment and before the first set of data has been transmitted, which makes it a part of the handshake process. Authentication uses a X.509 certificate to authenticate a client to the server, which may then accept or reject the session establishment.

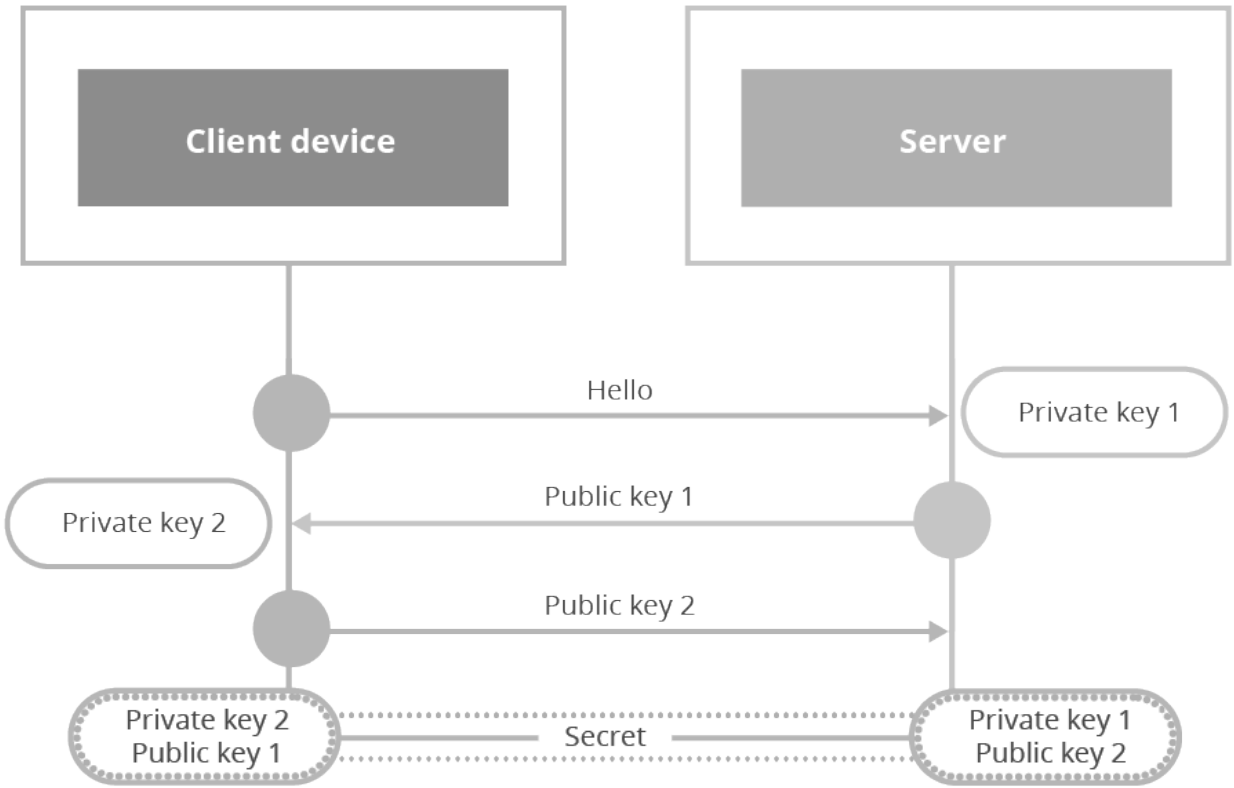
TLS: Key Exchange

TLS is a hybrid cryptosystem. It uses both symmetric key cryptography (encryption and decryption keys are the same) to exchange actual data and public key cryptography (encryption and decryption keys are different) to exchange the key to be used to encrypt data.

TLS: Key Exchange (RSA)



TLS: Key Exchange (Ephemeral Diffie-Hellman)



TLS: Confidentiality

Message confidentiality is based on the utilization of the symmetric encryption algorithms, whether stream encryption or block encryption. The same algorithm is used on both sides, but each side uses its own key, sharing it with the other party. Note that `TLS 1.2` allows stream ciphers, although `TLS 1.3` doesn't.

TLS: Integrity

The integrity of the data is assured with hash functions that employ the HMAC procedure.