A Simple and Secure Credit Card-Based Payment System

Chapter · August 2008

DOI: 10.4018/978-1-60566-014-1.ch175

Chi Po Cheong
PJ

A Simple and Secure Credit Card-based Payment System

Chi Po Cheong
University of Macau, Macau SAR, China
webster@macau.ctm.net

Abstract

Today, online shopping plays an important role in our life. More and more people are changing their shopping behavior. They prefer online shopping to face-to-face trading as it is more convenient, and more choice. Electronic Payment System (EPS) is essential in the online shopping. A successful EPS supports the transfer of electronic money or sensitive information with security, accuracy, and integrity between the seller and buyer over the telecommunication network. SET, CyberCash, Paypal and iKP are the most popular Credit Card-based EPSs (CCBEPS) or protocols. Some of the existing CCBEPS only use SSL to provide a secure communication channel. Hence they only prevent the "Man in the Middle" fraud but not protect the sensitive cardholder information such as credit card number to be passed to the merchant, who may be unscrupulous. Moreover, many existing credit CCBEPSs use complex mechanisms such as cryptography, certificate authorities, etc. to fulfill the security schemes but factors such as ease of use for the cardholder and implementation cost for the parties are not considered. The objective of this paper is to propose a new credit card-based payment system, which has a balance of security and simplicity. As the proposed system is simple and easy to use, cardholders and merchants will have more confidence in online shopping.

1. Introduction

Credit card is the most popular payment method used in Internet shopping. The idea of credit card payment is to buy first and pay later. The cardholder can pay at the end of the statement cycle or they can pay interest on the outstanding balance. Therefore, there are many credit card-based **electronic payment systems** (EPSs) that have been developed to facilitate the purchase of goods and services over the Internet such as CyberCash [1], iKP [2], SET [3], CCT [4], etc. Usually a credit card-based EPS involves five parties: cardholder, merchant, acquirer bank, issuer bank and financial institution.

Internet is an open system and the communication path between each other is insecure. All communications are potentially open for an eavesdropper to read and modify as they pass between the communicating endpoints. Therefore the payment information transmitted between the cardholder and the merchant through Internet is dangerous without a secure path. SSL [5] is a good example to secure the communication channel. Besides the issue of insecure communication, there are a number of factors that each participant must consider. For example, merchant concerns about whether the credit card or the cardholder is genuine. There is no way to know the consumer is a genuine cardholder. As a result, the merchant is incurring the increase in losses due to cardholder disputes and frauds. On the other hand, cardholders are worried about the theft of the privacy or sensitive information such as the credit card number. They donȸt want any unauthorized usage of their credit cards and any modification to the transaction amount by a third party. These security issues have deterred many potential consumers to purchase online.

Existing credit card-based EPSs solve the problems in many different ways. Some of them use cryptography mechanisms to protect private information. However, they are very complicated, expensive, and tedious [6]. Some EPSs use the Certificate Authority (CA) model to fulfill the **authentication**, **integrity**, and **non-repudiation** security schemes. However, each participant requires a digital **certificate** during the payment cycle. These certificates are issued by independent CAs but the implementation and maintenance cost of this model is very high. In addition, the validation steps of Certificate-based system are very time-consuming processes. It requires access to an online certificate server during the payment process. Moreover, the certificate revocation list is a major disadvantage of the PKI-based certification model [7]. The cardholderȸs certificate also includes some private information such as cardholderȸs name. The requirement of a cardholderȸs certificate means software such as e-Wallet is required to be installed on the cardholderȸs computer. It is the barrier for the cardholder to use Certificate-based payment systems. To solve this problem, Visa Company has developed a new payment system called Verified by Visa (VbV) [8]. However, sensitive information such as credit card number is still passed to the merchant. Therefore, the cardholder is not protected by the system.

1.1 Evaluation Factors

A successful credit card-based EPS should be simple, secure and easy to use and has low deployment and maintenance cost. A set of evaluation criteria is described by Sahut [9]. Security is one of the important factors in identifying a good EPS. However, factors such as cost, convenience, ease of use, etc. must be also considered when designing a new EPS.

The new EPS must have a balance between security and convenience especially on the cardholder side. This paper proposes a new payment system called **Simple and Secure Credit Card-based Payment System** (SSCCPS) which is a ñcryptography freeò and ñcertificate freeò system.

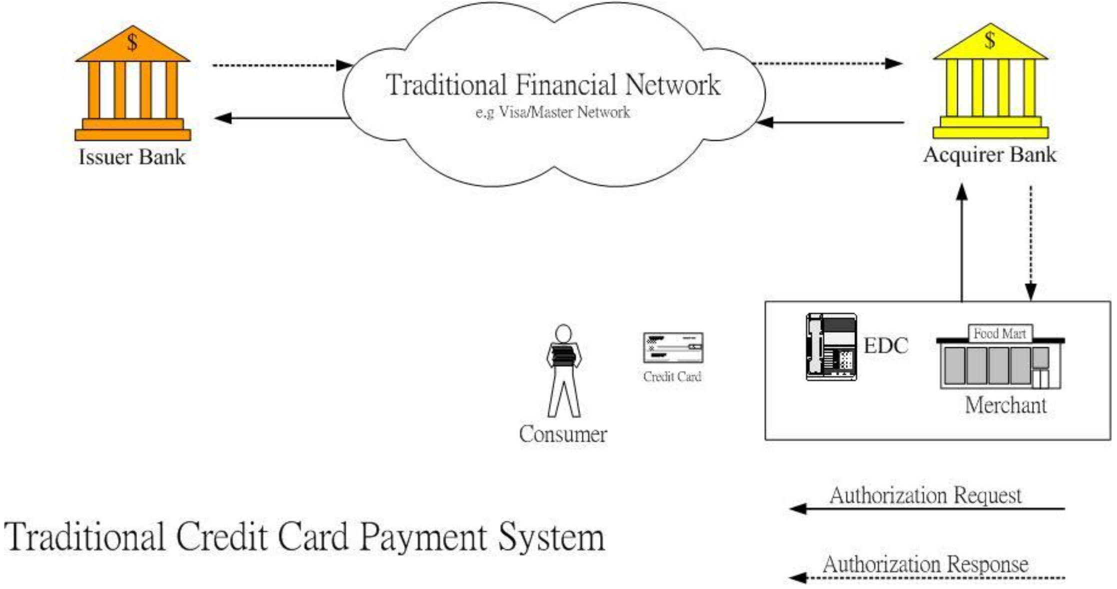
2. Traditional Credit Card Payment Systems

Most credit card-based EPSs do not utilize on the traditional credit card payment infrastructure. Many credit card-based EPSs have been designed and developed but most of them such as SET have been poorly received by consumers. The main problem is that lots of requirements must be fulfilled in all participants especially the cardholder. However, the complex or technical requirements to the cardholder will prevent the successful implementation of the system in the marketplace. For example, during the authentication process, cardholder has to use a smart card reader, which is to be installed at home. In addition, software such as e-wallet and e-certificate has to be installed in the cardholderôs computer. All the requirements act as barriers to the adoption of credit card-based EPSs. The objective of this paper is to design a simple and secure credit card payment system which utilizes the existing infrastructure and minimizes the complex mechanism.

2.1 Traditional Payment Flow

The payment flow of the traditional transaction is shown in the figure 1, consists of five participants including Issuer Bank, Acquirer Bank, Consumer, Merchant and financial institution. The cardholder gives the credit card to the merchant cashier. The cashier swipes the credit card through an Electric Draft Capture (EDC) or Point of Sale (POS) equipment and keys in the transaction amount. The EDC/POS dials a stored telephone number to call a gateway and sends the captured data to the acquirer bank. The acquirer bank constructs an ISO 8583 [10] authorization request message and sends it to the issuer bank through tradition financial network. The issuer bank extracts the information from the authorization request message such as primary account number, expiration date, currency code, merchant type, transaction date time, etc. and goes through the local validation policies. The issuer bank constructs the authorization response message and sends it to the acquirer bank either approved or declined. The acquire bank forwards the response code to the merchant to complete the transaction.

Figure 1: The Payment Flow of Traditional Credit Card Payment System



There are many different types of **financial messages** defined in ISO 8583. Each type of message is composed of different data fields. The values in each data field may be redefined by individual credit card company. Table 1 shows the typical message types and Table 2 shows data fields used in traditional credit card payment system.

Table 1: Typical Message Types

Message Number	Description
0100	Authorization request
0110	Authorization request response
0120	Authorization advice
0130	Authorization advice response
0400	Acquirer reversal request
0410	Acquirer reversal request response

Table 2: Typical Data Fields

ISO Bit Num	Field Name	Length
2	Primary account number (PAN) (e.g. credit card number)	19
4	Amount, transaction	12
7	Transmission data and time	10
11	System trace audit number	6
12	Time, local transaction	6
13	Date, local transaction	4
14	Date, expiration	4
18	Merchant type	4
32	Acquiring institution identification code	11
38	Authorization identification response	6
39	Response code	2
42	Card acceptor identification code (e.g. merchant number)	15

2.2 Trust Relationships

A well-defined **trust relationship** is based on the existing established physical relationship. For example, the relationship between the cardholder and the issuer bank is gradually building up since the credit card was issued. The proposed system is based on the trust relationships among the participants described as follows:

2.2.1 Existing Trust Relationships

- Cardholder and issuer bank

The cardholder trusts the issuer bank as it issues the card. The cardholder applies the credit card in his/her favorable bank and is normally a customer of the bank for a long time. Therefore the relationship has been built. During the online payment process, any online electronic message from the issuer bank is trusted by the cardholder, which is based on the physical relationship.

- Merchant and acquirer bank

The merchant bank is usually called the acquirer bank because it acquires payment records, such as payment charge slips from the merchant. To provide the online payment in the Internet, the merchant must register in the acquirer bank before starting the business. In the online credit card-based EPS, the same relationship has built between merchant and acquirer bank. The difference is that the merchant receives the response from the Internet and not from the Electric Draft Capture (EDC).

- The financial institution and the member bank

The financial intuition is a large data center acting as a gateway between the acquirer bank and the issuer bank such as Visa and MasterCard Company. When the issuer or acquirer banks carry out the credit card business, they have to apply to the financial institution for the network. Then each participant bank or member bank will be assigned a unique bank identification number (BIN). As a result, both the acquirer bank and the issuer bank have built the trusted relationship when they registered in the financial institution.

2.2.2 Transitive Trust Relationships

- Acquirer bank and Issuer Bank

The relationship between issuer bank and acquirer bank is interrelated with financial institution. They must become a member bank in the financial institution before running the credit card business. The acquirer and issuer bank must accept and follow the rules or policies of the financial institution. The financial institution not only supports but also monitors individual member bank. Therefore each member bank has built a trusted relationship.

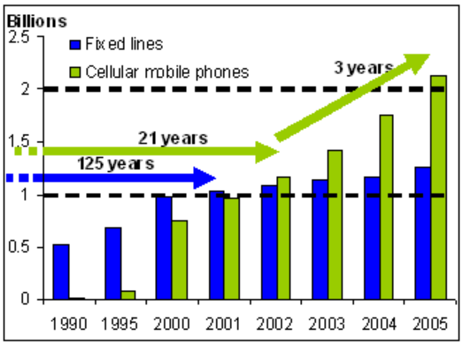
- The cardholder and merchant

The cardholder and the merchant can extend the trust relationship based on the two way trust relationship between their actors.

3. Simple and Secure Credit Card-based Payment System (SSCCPS)

The proposed payment system uses mobile phone as an authentication device. Figure 2 [11] shows the growth of mobile phone users between 1990 and 2005 compared with the fixed lines. The total number of mobile phone subscribers in the world was estimated at 2.14 billion in 2005. Around 80% of world's population have mobile phone coverage as of 2006 and is expected to increase to 90% by the year 2010. As the number of mobile phone users increase rapidly, it will support the adoption of SSCCPS.

Figure 2: Mobile telephones growing faster than fixed lines (source ITU [11])



The Simple and Secure Credit Card-based Payment System (SSCCPS) aims to improve the confidence and simplify the payment process for the cardholder and the merchant over open networks. It can reduce disputes and fraudulent activities related to the use of credit cards. SSCCPS uses the Bank

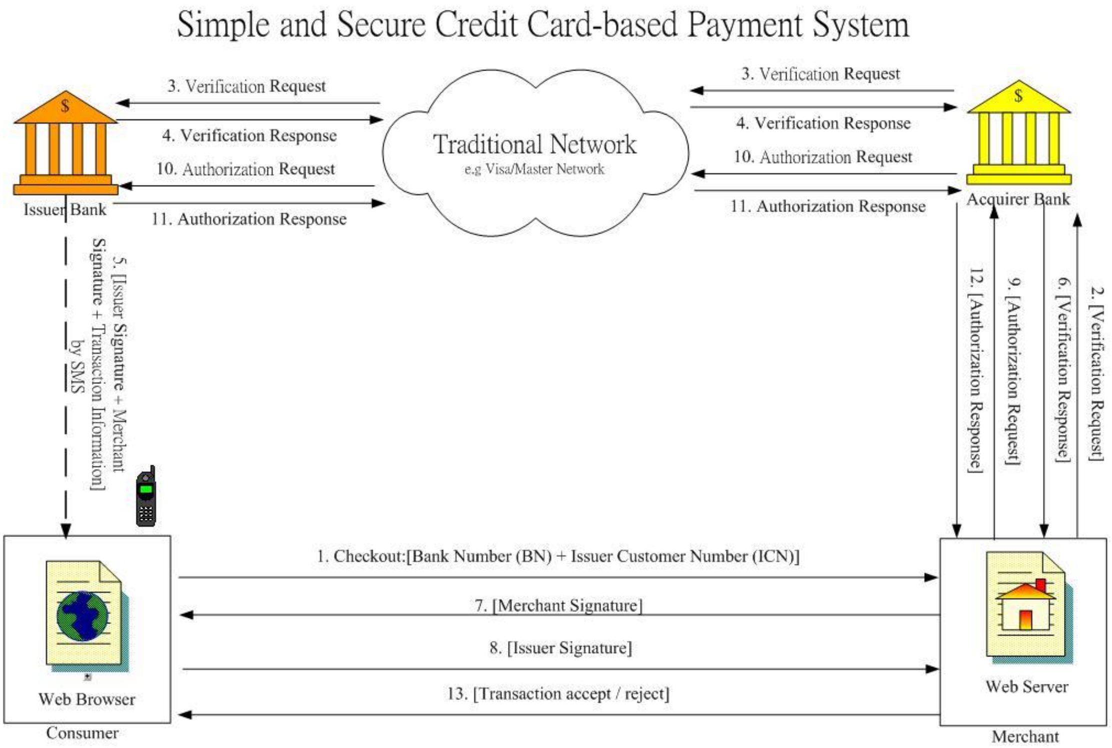
Identification Number (BIN) provided by participating issuers and Issuer Customer Number (ICN) to authenticate the cardholder. The cardholder sends the merchant information with the use of mobile phone to the issuer bank, which will authenticate the merchant. The cardholder inputs the Issuer Pre-Approval Number (IPAN) in the merchant web site for the final confirmation. Therefore the confidence of consumer can be gained. In SSCCPS, no software is required and there isnôt any complex cryptographic mechanism between cardholder and merchant.

3.1 Payment Cycle of SSCCPS

The basic cycle of SSCCPS is shown in Figure 3 and the details are as follows:

1. A cardholder selects the desired items and clicks the checkout button in the merchant online shop. The merchant requests the cardholder to fill in non-sensitive information including Issuer Identification Number (IIN), Issuer Customer Number (ICN), and other billing information such as delivery address, telephone number, etc. The cardholder then wait for the Issuer Pre-Approved Number (IPAN) and Merchant Signature (MS) from the issuer bank before going to step 8.
2. The cardholderôs order request is sent to the merchant. The merchant will send a verification request message to the acquirer bank. The verification request message includes merchant number and merchant trace number and the information of the cardholder.
3. The acquirer bank receives the verification request message from the merchant. It will modify the message and forward it to the issuer bank through the traditional financial network.
4. The issuer bank will verify the verification request message from the acquirer bank. The issuer bank checks the validity of the issuer customer number, the adequacy of the credit line and other authorization rules or policies. After the check, a verification message will then sent to the merchant.
5. If it is a valid transaction, the issuer sends the transaction summary i.e. IPAN and MS to the cardholderôs mobile phone through Short Message Service (SMS).
6. The merchant receives a verification message from the issuer through the acquirer. If it is a valid response, the merchant follows the payment step; otherwise it rejects the transaction.
7. For a valid transaction, the merchant prompts the cardholder to input the IPAN and also displays the transaction details and MS at the same time. The IPAN is provided by the issuer bank through SMS to the cardholderôs mobile phone in step 5.
8. The cardholder inputs the IPAN after verifying the MS and transaction summary and then send the IPAN to the merchant by clicking the confirm button.
9. The merchant will send an authorization request message to the acquire bank with some data added into the traditional message such as IPAN.
10. The acquire bank receives the authorization request message from the merchant and will forward it to the issuer bank.
11. When the issuer bank receives the authorization request from the acquirer bank, it will obtain the IPAN from the authorization request and compares it with the IPAN sent to the cardholder. If they are identical, it will accept the transaction otherwise reject it. The issuer bank then sends an authorization response back to acquirer bank either approved or declined.
12. When the acquirer bank receives the authorization response message, it will send the authorization response message (either approved or declined) to the merchant.
13. Based on the response code, the merchant sends an approved or declined response to the cardholder.

Figure 3: The payment flow of the SSCCPS


Simple and Secure Credit Card-based Payment System
3. Verification Request
4. Verification Response
10. Authorization Request
11. Authorization Response
Issuer Bank
Traditional Network
e.g Visa/Master Network
3. Verification Request
4. Verification Response
10. Authorization Request
11. Authorization Response
Acquirer Bank
5. [Issuer Signature + Merchant Signature + Transaction Information] by SMS
12. [Authorization Response]
9. [Authorization Request]
6. [Verification Response]
2. [Verification Request]
1. Checkout:[Bank Number (BN) + Issuer Customer Number (ICN)]
7. [Merchant Signature]
8. [Issuer Signature]
13. [Transaction accept / reject]
Web Browser
Consumer
Web Server
Merchant

3.2 Security Schemes in SSCCPS

Four basic security schemes are used to evaluate the proposed system including Authentication, Confidentially, Integrity, and Non-repudiation.

3.2.1 Cardholder authentication: The merchant can determine a genuine cardholder by the use of IPAN. The IPAN is a unique number generated by the issuer bank and is used only once in the transaction. The issuer bank sends the IPAN to the cardholderǿs mobile phone by using SMS. Only the genuine cardholder will receive the SMS because the mobile phone number was registered to the bank. The cardholder submits IPAN to the merchant. The merchant will then send an authorization request message with IPAN. The issuer bank compares the value of IPAN when it receives the authorization request message. Only the genuine cardholder knows the IPAN. If they are identical, the consumer is a genuine cardholder. In SSCCPS, the merchant does not need to authenticate the cardholder. The authentication process is done by the issuer bank.

3.2.2 Merchant authentication: In SSCCPS, the merchant authentication process is unimportant during the payment process. The purpose for authenticating the merchant is for the cardholder to ensure that sensitive information is sent to a genuine merchant. In most of the credit card-based payment systems, the merchant authentication is performed by the use of the merchant certificate in the beginning of the payment process. However, in the SSCCPS, no sensitive information such as credit number is sent to the merchant directly. The authentication process is performed during the verification process. The merchant generates a merchant signature during the verification process. The merchant signature is divided in two parts: the merchant number and the merchant trace number. The merchant number is a unique identification number issued by the acquirer bank during the merchant registration. The merchant trace number is a one-time used number generated by the merchant to identify each transaction. During the payment process, the merchant web site pops up a window showing the merchant signature and requesting the cardholder to submit IPAN. Then the issuer bank receives the merchant signature from the verification request message. After passing the verification process, the issuer sends the merchant signature, Issuer Pre-Approved Number (IPAN) and transaction summary to the cardholderǿs mobile phone through SMS. The cardholder will compare two merchant signatures. If they are identical, the merchant is a genuine merchant.

3.2.3 Confidentiality: Most existing credit card-based EPSs only ensure a secure communication path between the cardholder and the merchant or use encryption mechanisms to encrypt the financial data. Financial information will eventually be sent to the merchant side regardless of whether the merchant is honest or not. In SSCCPS, no sensitive information is sent to the merchant. The merchant only knows the Issuer Customer Number (ICN), which is not sensitive financial information. Cardholders are willing to use SSCCPS because it hides their privacy information.

3.2.4 Integrity: Data Integrity ensures that the message or transaction cannot be altered from its source. Many existing payment systems are using digital signature mechanism to assure integrity. In SSCCPS, data integrity is done by the cardholder. The issuer bank sends the transaction summary such as transaction date, time, amount, etc. to the cardholderôs mobile phone. The cardholder can check the transaction summary such as transaction amount. If the data matches the original, the cardholder submits the IPAN through the merchant web site.

3.2.5 Non-repudiation: Non-repudiation is a way to guarantee that the cardholder and merchant cannot deny the transaction in later. It is usually provided through public key cryptography by digital signing. SSCCPS uses mobile phone as a non-repudiation mechanism instead of the public key infrastructure. Only the mobile phone owner can receive IPAN and the transaction summary. No one can abuse or read the message from the cardholderôs mobile phone. SSCCPS assumes that only the genuine cardholder can receive the IPAN during the payment process. If the merchant can obtain an authorization request message with a valid IPAN, it means that the cardholder has agreed and cannot deny the transaction.

4. Conclusion

Most existing credit card-based EPSs are complex and expensive. And the payment systems using cryptography or certificate authorities are much more expensive. Using SSCCPS, cardholder can protect his/her sensitive information from merchant. During the payment cycle, the merchant doesnôt know the actual credit card information and obtains the Issuer Customer Number (ICN) only. In addition, it does not require any software such as e-wallet and cardholderôs certificate. Therefore, it is convenient for any cardholder to use SSCCPS. It is a true ñcryptography freeò and ñcertificate freeò payment system. Furthermore, it fully utilizes the traditional payment infrastructure without increasing the deployment and maintenance cost. With SSCCPS, the cardholder will gain more confident in online shopping. Hence it not only improves the security of online payment but also simplifies the process. In conclusion, SSCCPS will benefit all parties involved as disputes and fraudulent activities will be reduced.

REFERENCES

[1] VeriSign, Inc., http://www.cybercash.com/

[2] Mihir Bellare, Juan A. Garary, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steinerm Gene Tsudik, Michael Waidner, iKP ï A Family of Secure Electronic Payment Protocols, July 12, 1995

[3] Visa and MasterCard, SET Secure Electronic Transaction Specification Book 1: Business Description, Version 1.0, May 31, 1997

[4] Yingjiu Li, Xinwen Zhange, A Security-Enhanced One-Time Payment Scheme for Credit Card, in Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDEô04) 2004 IEEE

[5] Zeus Technology, SSL: Theory and Practice, 16 June 2000

[6] Xu Xianhua, Sung Sam Yuen, Ge Ling, Tan Chew Lim, Virtual Card Payment Protocol and Risk Analysis Using Performance Scoring, ipdps, p. 10018a, 15th International Parallel and Distributed Processing Symposium (IPDPS'01), 2001 IEEE.

[7] The Internet Engineering Task Force, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, www.ietf.org/rfc/rfc3280.txt

[8] http://www.visa-asia.com/ap/sea/merchants/productstech/vbv_implementvbv.shtml

[9] Jean-Michel SAHUT, Professor of Finance, GET, Internet Payment Solutions: Comparative evaluation and key factors of success, in Proceedings of the 2005 Symposium on Applications and the Internet Workshops (SAINT-Wô05) 2005 IEEE
[10] ISO 8583-1:2003 Financial transaction card originated messages ï Interchange message specifications ï Part 1: message, data elements and code values
[11] International Telecommunication Union ITU/UNCTAD, World Information Society Report 2006, and ITU World Telecommunication Indicators Database

Terms and Definitions

Certificate Revocation. The certificate can be revoked by the Certificate Authority (CA) before their scheduled expiration date. There are different revocation reasons defined in RFC 3280. A revoked certificate will be added to the Certificate Revocation List (CRL) and it should not be used by other system.

Digital Certificates. It is issued by a Certification Authority (CA). It contains the owner name, expiration date and the ownerôs public key and is to verify who are sending the message.

Encryption. It is the process to encrypt the message and make it unreadable without special knowledge. Encryption is to protect the public communication network such as Internet.

E-Wallet. It is also known as a digital wallet and likes a physical wallet used in the electronic payment system. It provides the security and encryption for the personal information.

Merchant. An organization or an individual accepts credit card payment by selling product or service.

Acquirer. An acquirer is an organization or a bank that collects authorization requests and sales slips from merchant. It directly connects to merchantôs POS/EDC in traditional payment system..

Issuer. A issuer is an organization or a bank which issues credit card to cardholder. It provides the authorization services to acquirer.

Financial Institution (Card Brand). A large data center that provides the financial services and network between acquirer bank and issuer bank.

Identification. Identification is a mechanism by which the system asks the user, ñWho are you?ò user identifies himself or herself to the system by a user name or user number in the computer system.

Authentication. It is a method to identify cardholder and merchant before payment. Authentication is the mechanism in which the system will identify the cardholder or merchant, ñIs that really you?ò

Integrity. Data integrity ensures that the transaction is unchanged from its source and cannot not been accidentally or maliciously altered.

Non-repudiation. A strong and substantial evidence is available to the sender of message that the message has been delivered, and to the receipt.

Short message service (SMS). The service is available on mobile phones, which permits the sending or receiving of short messages. SMS messages are two-way alphanumeric paging messages up to 160 characters that can be sent to and from mobile phone.