MODULE 6

Secure Electronics transactions: Framework, strength and weakness, Security in current applications : Online banking , Credit Card Payment Systems.

Web Services security: XML, SOAP, SAML, RFID

SECURE ELECTRONIC TRANSACTION

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario.

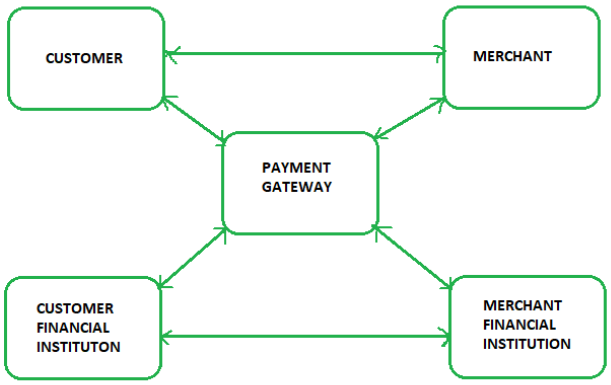
- Developed by Visa and MasterCard
- Designed to protect credit and debit card transactions
- SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards.
- SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft
- SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

It provides

• Confidentiality: all messages encrypted

• Trust: all parties must have digital certificates

• Privacy: information made available only when and where necessary



Example for SET is online shopping.

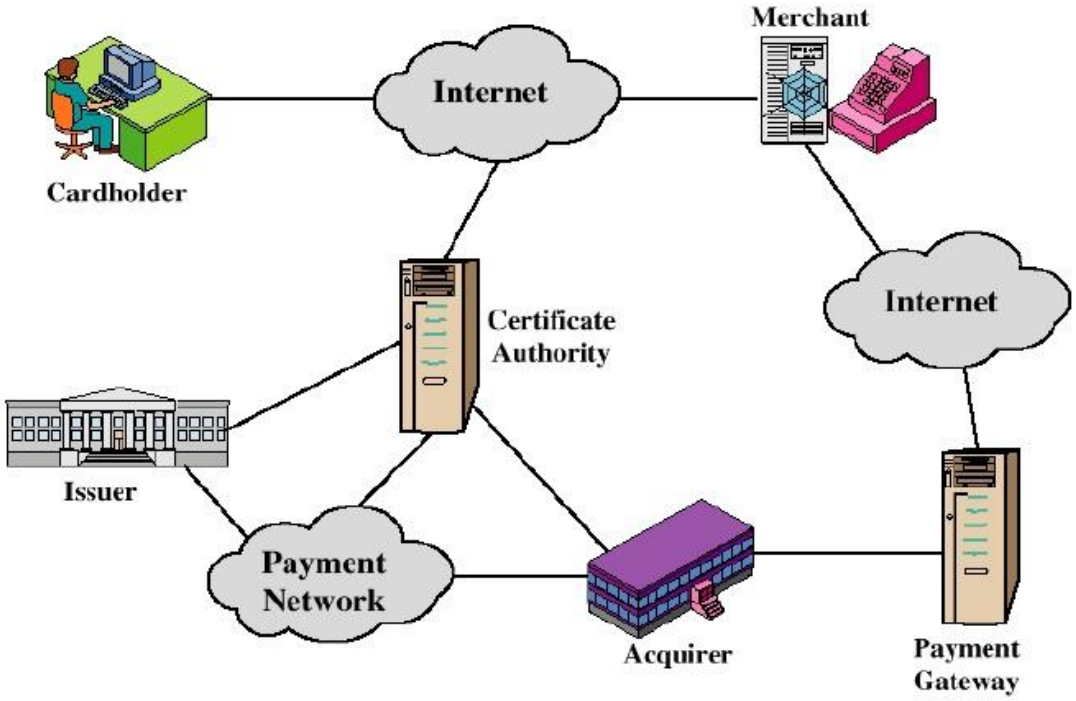
SET Business Requirements (1)

- Provide confidentiality of payment and ordering information
- Ensure the integrity of all transmitted data
- Provide authentication that a cardholder is a legitimate user of a credit or debit card account
- Provide authentication that a merchant can accept credit or debit card transactions through its relationship with a financial institution

SET Business Requirements (2)

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
- Create a protocol that neither depends on transport security mechanisms nor prevents their use
- Facilitate and encourage interoperability among software and network providers

Participants in the SET System

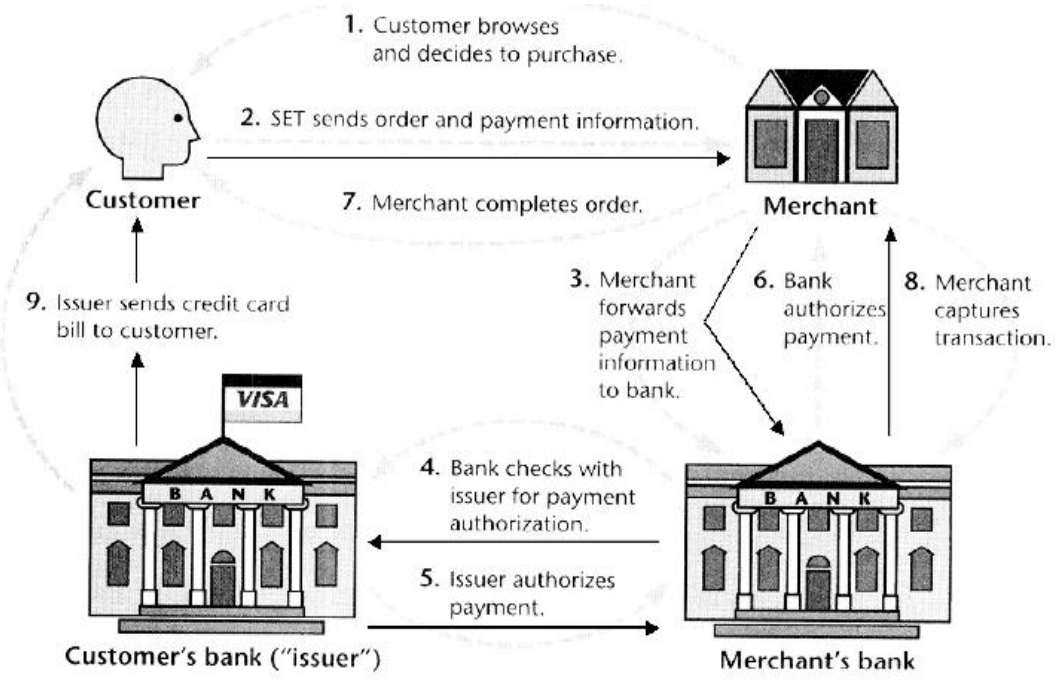


1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

   Certificate of card holder:- It contains card holder name and public of card holder.

6. Payment Gateway:- eg- master or visa card
   - Who will do the payment

SET Transactions

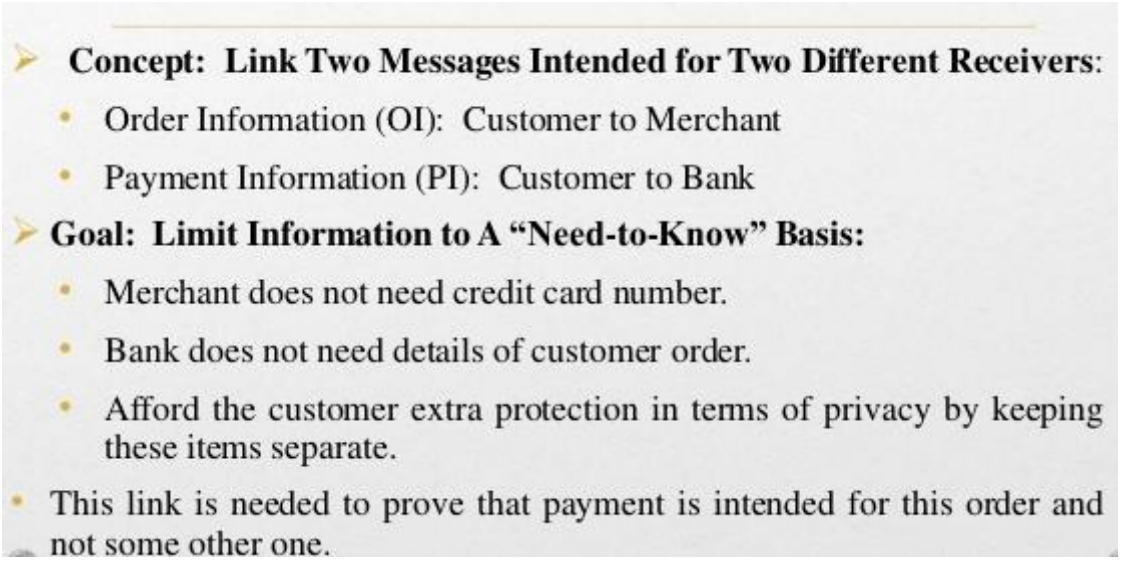


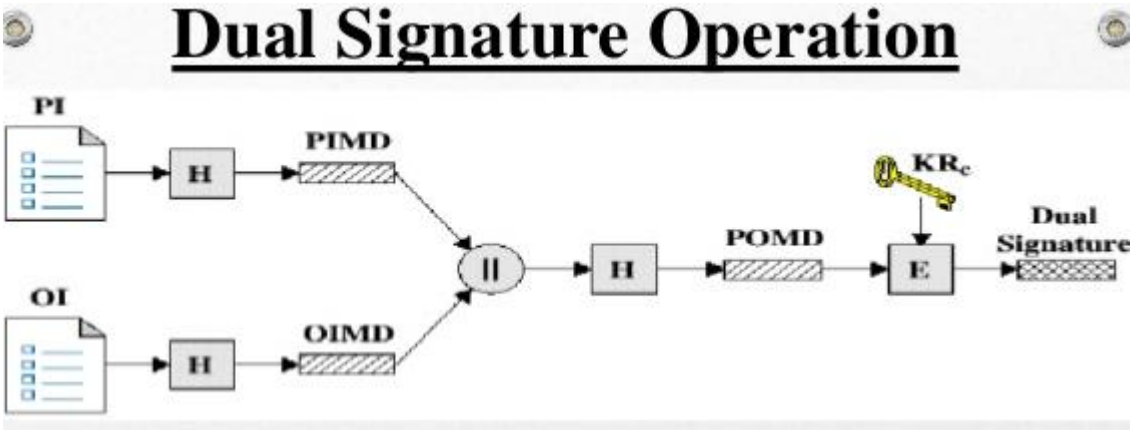
- The customer opens an account with a card issuer.
  - MasterCard, Visa, etc.
- The customer receives a digital certificate signed by a bank.
- A merchant who accepts a certain brand of card must possess two digital certificates.
  - One for signing & one for key exchange
- The customer places an order for a product or service with a merchant.
- The merchant sends a copy of its certificate for verification.

- The customer sends order and payment information to the merchant.
- The merchant requests payment authorization from the payment gateway prior to shipment.
- The merchant confirms order to the customer.
- The merchant provides the goods or service to the customer.
- The merchant requests payment from the payment gateway.

Dual Signature of SET

In order to achieve authentication and integrity we use dual signature





The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service. The message digest (MD) of the OI and the PI are independently calculated by the customer. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. Protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved

Duel Signature Operation:

- PI stands for payment information
- OI stands for order information
- PIMD stands for Payment Information Message Digest
- OIMD stands for Order Information Message Digest
- POMD stands for Payment Order Message Digest
- H stands for Hashing
- E stands for public key encryption
- KPc is customer's private key
- || stands for append operation
- Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])

The operation for dual signature is as follows:

Take the hash (SHA-1) of the payment and order information.

These two hash values are concatenated [H(PI) || H(OI)] and then the result is hashed.

Customer encrypts the final hash with a private key creating the dual signature.

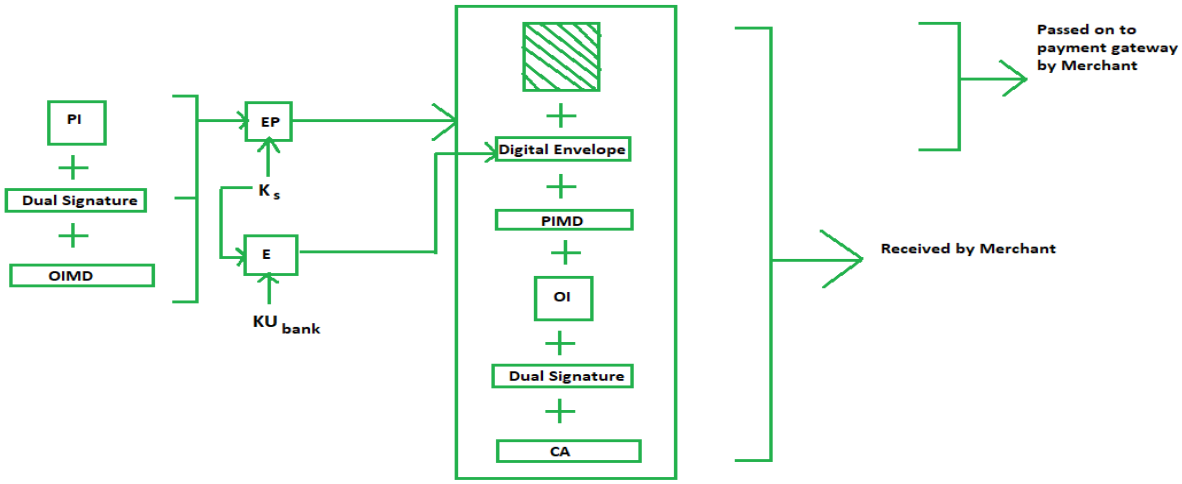
$$DS = E_{KRC}[H(H(PI) || H(OI))]$$

Purchase Request Generation :

The process of purchase request generation requires three inputs:

- Payment Information (PI)
- Dual Signature
- Order Information Message Digest (OIMD)

The purchase request is generated as follows:



Here,

PI, OIMD, OI all have the same meanings as before.

The new things are :

EP which is symmetric key encryption

Ks is a temporary symmetric key

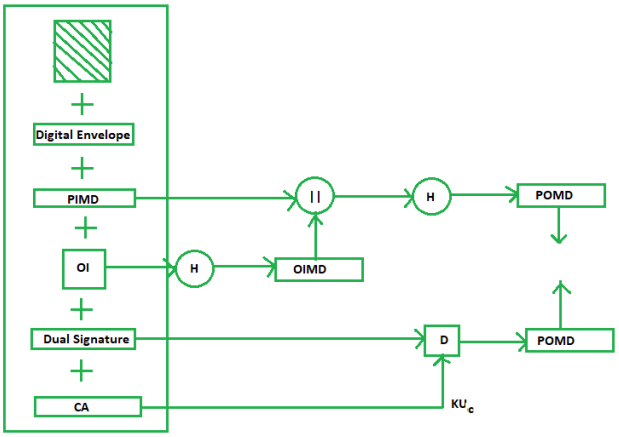
KUbank is public key of bank

CA is Cardholder or customer Certificate

Digital Envelope = E(KUbank, Ks)

Purchase Request Validation on Merchant Side :

The Merchant verifies by comparing POMD generated through PIMD hashing with POMD generated through decryption of Dual Signature as follows:



Strength and weakness of SET

Strength of SET

• It is secure enough to protect user's credit-card numbers and personal information from attacks

• Hardware independent

• World-wide usage

• Confidentiality of information

• Integrity of data

• Cardholder account authentication

• Merchant authentication

✔ **Time savings**

Money transfer between virtual accounts usually takes a few minutes, while a wire transfer or a postal one may take several days. Also, you will not waste your time waiting in lines at a bank or post office.

✔ **Expenses control**

Even if someone is eager to bring his disbursements under control, it is necessary to be patient enough to write down all the petty expenses, which often takes a large part of the total amount of disbursements. The virtual account contains the history of all transactions indicating the store and the amount you spent. And you can check it anytime you want. This advantage of electronic payment system is pretty important in this case.

✔ Reduced risk of loss and theft

You can not forget your virtual wallet somewhere and it can not be taken away by robbers. Although in cyberspace there are many scammers, in one of the previous articles we described in detail how to make your e-currency account secure.

✔ **Low commissions**

If you pay for internet service provider or a mobile account replenishment through the UPT (unattended payment terminal), you will encounter high fees. As for the electronic payment system: a fee of this kind of operations consists of 1% of the total amount, and this is a considerable advantage.

✔ **User-friendly**

Usually every service is designed to reach the widest possible audience, so it has the intuitively understandable user interface. In addition, there is always the opportunity to submit a question to a support team, which often works 24/7. Anyway you can always get an answer using the forums on the subject.

✔ **Convenience**

All the transfers can be performed at any time, anywhere. It's enough to have an access to the Internet.

Weakness of SET

• User must have credit card

• It is not cost-effective when the payment is small

• None of anonymity and it is traceable

• Network effect - need to install client software (an e-wallet). Cost and complexity for merchants to offer support, contrasted with the comparatively low cost and simplicity of the existing SSL based alternative.

Restrictions

Each payment system has its limits regarding the maximum amount in the account, the number of transactions per day and the amount of output.

✘ **The risk of being hacked**

If you follow the security rules the threat is minimal, it can be compared to the risk of something like a robbery. The worse situation when the system of processing company has been broken, because it leads to the leak of personal data on cards and its owners. Even if the electronic payment system does not launch plastic cards, it can be involved in scandals regarding the Identity theft.

✘ **The problem of transferring money between different payment systems**

Usually the majority of electronic payment systems do not cooperate with each other. In this case, you have to use the services of e-currency exchange, and it can be time-consuming if you still do not have a trusted service for this purpose. Our article on how to choose the best e-currency exchanger greatly facilitates the search process.

✘ **The lack of anonymity**

The information about all the transactions, including the amount, time and recipient are stored in the database of the payment system. And it means the intelligence agency has an access to this information. You should decide whether it's bad or good.

✘ **The necessity of Internet access**

If Internet connection fails, you can not get to your online account.

Security in current domain

Credit Card Payment System

A credit card is a payment card issued to users (cardholders) to enable the cardholder to pay a merchant for goods and services based on the cardholder's promise to the card issuer to pay them for the amounts plus the other agreed charges.

Credit card security is based on privacy of the actual credit card number. This means that whenever a person other than the card owner reads the number, security is potentially compromised. Since this happens most of the time when a transaction is made, security is low. However, a user with access to just the number can only make certain types of transactions. Merchants will often accept credit card numbers without extra verification for mail order, but then the delivery address will be recorded, so the thief must make sure he can have the goods delivered to an anonymous address (i.e. not his own) and collect them without being detected.

Some merchants will accept a credit card number for in-store purchases,where upon access to the number allows easy fraud, but many require the card itself to be present, and require a signature. Thus, a stolen card can be cancelled, and if this is done quickly, no fraud can take place in this way. For internet purchases, there is sometimes the same level of security as for mail order (number only) hence requiring only that the fraudster take care about collecting the goods, but often there are additional measures. The main one is to require a security PIN with the card, which requires that the thief have access to the card.

Credit card numbering

The numbers found on credit cards have a certain amount of internal structure, and share a common numbering scheme. The card number's prefix, called the Bank Identification Number, is the sequence of digits at the beginning of the number that determine the bank to which a credit card number belongs. This is the first six digits for MasterCard and Visa cards. The next nine digits are the individual account number, and the final digit is a validity check code.

In addition to the main credit card number, credit cards also carry issue and expiration dates (given to the nearest month), as well as extra codes such as issue numbers and security codes. Not all credit cards have the same sets of extra codes nor do they use the same number of digits.

Credit cards in ATMs

Many credit cards can also be used in an ATM to withdraw money against the credit limit extended to the card but many card issuers charge interest on cash advances before they do so on purchases. The interest on cash advances is commonly charged from the date the withdrawal is made, rather than the monthly billing date.

Many card issuers levy a commission for cash withdrawals, even if the ATM belongs to the same bank as the card issuer. Merchants do not offer cash back on credit card transactions because they would pay a percentage commission of the additional cash amount to their bank or merchant services provider, thereby making it uneconomical.

Credit Card Electronic Payment System

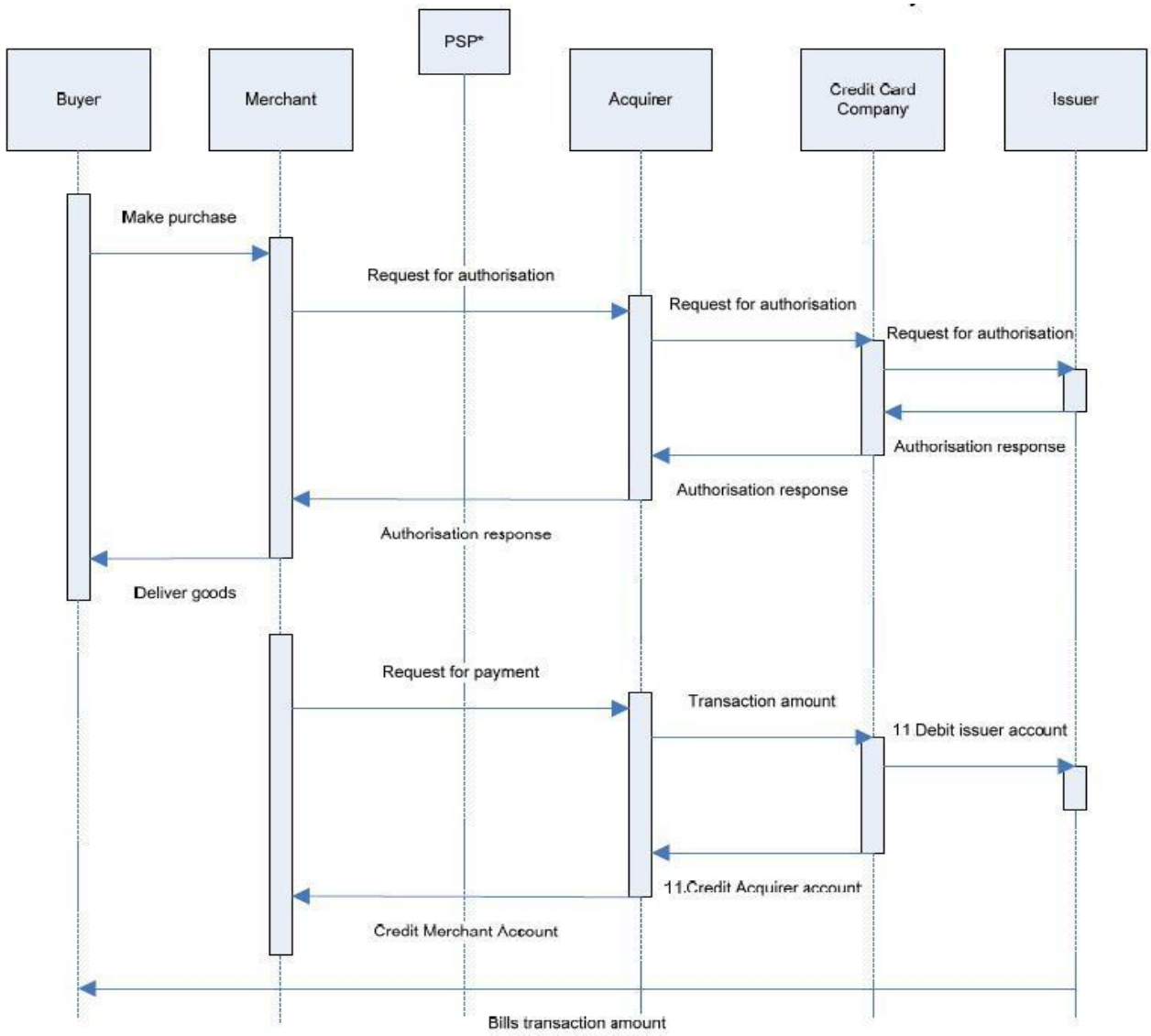
Many credit card companies will also, when applying payments to a card, do so at the end of a billing cycle, and apply those payments to everything before cash advances. For this reason, many consumers have large cash balances, which have no grace period and incur interest at a rate that is (usually) higher than the purchase rate, and will carry those balances for years, even if they pay off their statement balance each month.

Credit card- based payment over the internet is one of the earliest forms of epayment commonly used in E-commerce.

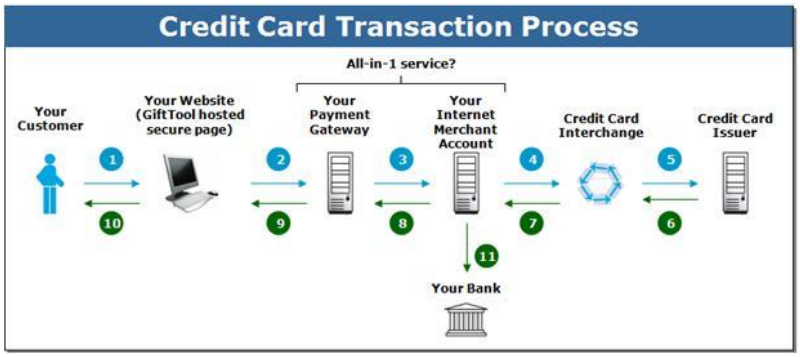
- A customer C, browses the website of an online store.
- When the customer finishes loading his shopping cart, he is asked to choose the payment option.
- If he chooses credit cards, he is asked to enter payment details such as credit card number(CCN).

The merchant M, needs to determine whether the customers CCN is valid and whether he has sufficient balance in his credit account. M could contact the issuing bank-the bank that issued the credit card to C. To avoid having to deal with different banks, the Bankcard association employs a payment gateway (PG).

The PG act as a proxy between different merchants and the bankcard network. Communication between C and M is over the internet. It is usually the case that the merchant-payment gateway communication is also over the internet. The PG , communicates with the banks through a proprietary Bank Card network. For conducting business over net, the merchant must have an account with a bank in the Bank's card network- Acquiring bank. On-line credit card transactions shown below.



Payment service provider (PSP) offers shops online services for accepting electronic payments by a variety of payment methods including credit card, bankbased payments such as direct debit, bank transfer, and real-time bank transfer based on online banking. Typically, they use a software as a service model and form a single payment gateway for their clients (merchants) to multiple payment methods.



Once M(Merchant) has received order and payment information from C(Customer), it contacts the PG(Payment Gateway). The PG, in turn communicates customer information to the issuing bank. The issuing bank checks to see if the CCN(Credit card no) is valid and if the customer has sufficient balance in his credit account. If so, it authorizes payment. The PG accordingly informs M whether to proceed the transaction. M communicates this decision to C together with an order tracking number.

The most important part of a financial transaction is funds transfer-form the issuing bank to acquiring bank. The fund transfer takes place just after M has shipped the goods. Sensitive information like the CCN should not be sent in clear. One possibility is to set up an SSL connection between C and M. The CCN and other sensitive information can then be sent on the encrypted SSL channel.

The encrypted SSL connection between C and M secures the CCN from eavesdropper. However the payment information from C is decrypted at the merchant site. Thus, M is aware of the customer's CCN. M maintains a db of customer information including customers CCNs. This is an attractive target for hackers. Online and mail- order transactions belongs to the category of card not present transactions since the credit or debit card is not physically presented to the merchant.

Advantages and Disadvantage of credit cards:

• Credit cards have advantages over checks in that the credit card company assumes a larger share of financial risk for both buyer and seller in a transaction. Buyers can sometimes dispute a charge retroactively and have the credit card company act on their behalf. Sellers are ensured that they will be paid for all their sales—they needn't worry about fraud.

• One disadvantage to credit cards is that their transactions are not anonymous, and credit card companies do in fact compile valuable data about spending habits.

• Record keeping with credit cards is one of the features consumers value most because of disputes and mistakes in billing. Disputes may arise because different services may have different policies. In general, implementing payment policies will be simpler when payment is made by credit rather than with cash.

• The complexity of credit card processing takes place in the verification phase, a potential bottleneck. If there is a lapse in time between the charging and the delivery of goods or services, the customer verification process is simple because it does not have to be done in real time.

• Encryption and transaction speed must be balanced, Hence, on-line credit card users must find the process to be accessible, simple, and fast. Speed will have design and cost implications, as it is a function of network capabilities, computing power, available at every server, and the specific form of the transaction. The infrastructure supporting the exchange must be reliable.

ONLINE- BANKING

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.

Online banking facilities typically have many features and capabilities in common, but also have some that are application specific. The common features fall broadly into several categories:

- A bank customer can perform non-transactional tasks through online banking, including:
    - o Viewing account balances
    - o Viewing recent transactions
    - o Downloading bank statements, for example in PDF format
    - o Viewing images of paid cheques
    - o Ordering cheque books
    - o Download periodic account statements
    - o Downloading applications for M-banking, E-banking etc.
- Bank customers can transact banking tasks through online banking, including:
    - o Funds transfers between the customer's linked accounts
    - o Paying third parties, including bill payments and third party fund transfers (see, e.g., FAST)
    - o Investment purchase or sale
    - o Loan applications and transactions, such as repayments of enrollments
    - o Credit card applications
    - o Register utility billers and make bill payments
- Financial institution administration
- Management of multiple users having varying levels of authority
- Transaction approval process

Some financial institutions offer special internet banking services, for example:

- Personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

Security

Security of a customer's financial information is very important, without which online banking could not operate. Similarly the reputational risks to banks themselves are important.

Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted. The use of a secure website has been almost universally embraced.

Though single password authentication is still in use, it by itself is not considered secure enough for online banking in some countries.

Basically there are two different security methods in use for online banking:

1. The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter.

Another way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token.

More advanced TAN generators (chipTAN) also include the transaction data into the TAN generation process after displaying it on their own screen to allow the user to discover man-in-the-middle attacks carried out by Trojans trying to secretly manipulate the transaction data in the background of the PC. Another way to provide TANs to an online banking user is to send the TAN of the current bank transaction to the user's (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details, the TAN is only valid for a short period of time. Especially in Germany, Austria and the Netherlands many banks have adopted this "SMS TAN" service. Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.

2. Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation

Attacks

Attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well known examples for those attacks are phishing and pharming. Cross-site scripting and keylogger/Trojan horses can also be used to steal login information.

A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

A 2008 U.S. Federal Deposit Insurance Corporation Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

Another kind of attack is the so-called man-in-the-browser attack, a variation of the man-in-the-middle attack where a Trojan horse permits a remote attacker to secretly modify the destination account number and also the amount in the web browser.

As a reaction to advanced security processes allowing the user to cross-check the transaction data on a secure device there are also combined attacks using malware and social engineering to persuade the user himself to transfer money to the fraudsters on the ground of false claims (like the claim the bank would require a "test transfer" or the claim a company had falsely transferred money to the user's account and he should "send it back").Users should therefore never perform bank transfers they have not initiated themselves.

Countermeasures

There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, in signature based online banking variants (HBCI/FinTS) the use of "Secoder" card readers is a measurement to uncover software side manipulations of the transaction data.

In 2001, the U.S. Federal Financial Institutions Examination Council issued guidance for multifactor authentication (MFA) and then required to be in place by the end of 2006. In 2012, the European Union Agency for Network and Information Security advised all banks to consider the PC systems of their users being infected by malware by default and therefore use security processes where the user can cross-check the transaction data against manipulations like for example (provided the security of the mobile phone holds up) SMS TAN where the transaction data is sent along with the TAN number or standalone smartcard readers with an own screen including the transaction data into the TAN generation process while displaying it beforehand to the user to counter man-in-the-middle attacks.

Advantages of E-banking or Internet banking

1. Convenience: Banks that offer internet banking are open for business transactions anywhere a client might be as long as there is internet connection. Apart from periods of website maintenance, services are available 24 hours a day and 365 days round the year. In a scenario where internet connection is unavailable, customer services are provided round the clock via telephone.
2. Low cost banking service: E-banking helps in reducing the operational costs of banking services. Better quality services can be ensured at low cost.
3. Higher interest rate: Lower operating cost results in higher interest rates on savings and lower rates on mortgages and loans offers from the banks. Some banks offer high yield certificate of deposits and don't penalize withdrawals on certificate of deposits, opening of accounts without minimum deposits and no minimum balance.
4. Transfer services: Online banking allows automatic funding of accounts from long established bank accounts via electronic funds transfers.
5. Ease of monitoring: A client can monitor his/her spending via a virtual wallet through certain banks and applications and enable payments.
6. Ease of transaction: The speed of transaction is faster relative to use of ATM's or customary banking.
7. Discounts: The credit cards and debit cards enables the Customers to obtain discounts from retail outlets.
8. Quality service: E-Banking helps the bank to provide efficient, economic and quality service to the customers. It helps the bank to create new customer and retaining the old ones successfully.
9. Any time cash facility: The customer can obtain funds at any time from ATM machines.

Disadvantages of E-banking Internet banking

1. High start-up cost: E-banking requires high initial start up cost. It includes internet installation cost, cost of advanced hardware and software, modem, computers and cost of maintenance of all computers.

2. Security Concerns: One of the biggest disadvantages of doing e-banking is the question of security. People worry that their bank accounts can be hacked and accessed without their knowledge or that the funds they transfer may not reach the intended recipients.

3. Transaction problems: Face to face meeting is better in handling complex transactions and problems. Banks may call for meetings and seek expert advice to solve issues.

4. Lack of personal contact between customer and banker: Customary banking allows creation of a personal touch between a bank and its clients. A personal touch with a bank manager can enable the manager to change terms in our account since he/she has some discretion in case of any personal circumstantial change. It can include reversal of an undeserved service charge