introduction:

an electronic payment system is needed for compensation for information, goods and services provided through the Internet - such as access to copyrighted materials, database searches or consumption of system resources - or as a convenient form of payment for external goods and services - such as merchandise and services provided outside the Internet. it helps to automate sales activities, extends the potential number of customers and may reduce the amount of paperwork.

---

requirements:

- **security**: payment systems are very likely to become a target for criminal attacks.
- **flexibility**: different models for different situations (anonymity, accountability, risk).
- **computational efficiency**: support for micropayment; per-transaction cost must be small enough so that they are insignificant.

---

payment methods:

- **secure (or non-secure) presentation**: the customer provides credit card information over a secure (or even clear) transportation means.
- **customer registration**: the customer gets a password or digital signature based on a credit card (hides the credit card information from the merchant, but still clears through the credit card).
- **credit-debit instruments**: similar to customer registration but only one bill per month either through credit card or debit check.
- **electronic currency**: this method has potential for anonymity but requires tamper resistant hardware.
- **server scrip**: the customer gets a kind of coupons from an agent that can be spend only with one particular merchant. this reduces the risk of double spending and allows off-line transactions.
- **direct transfer**: the customer initiates the transfer of funds to the account of the merchant. this method provides no anonymity.
- **collection agent**: the merchant refers the customer to a third party who collects payment using one of the methods mentioned above.

of all models, (non-)secure presentation is the only model that has a large customer base today. all other methods require a special hardware and/or software that most potential customers don't have.

---

systems available today:

- **secure socket layer (SSL)**: client submits credit card information using encryption based on public keys.

- **CyberCash**: customer registers credit card with CyberCash and selects a signature key. requires special software on the client, but hides credit card information from merchant.
- **secure electronic transaction (SET)**: the customer obtains a signature key from the card issuer. this method requires a special software running on the client to encrypt and sign credit card information.
- **Open Market**: provides multi-mechanism collection services for web browsers.
- **Mondex**: provides smart-card based electronic currency.
- **electronic check**: provides a PC card-based credit-debit payment instrument that can be sent across the Internet, but clears through the existing banking network.
- **USC/ISI's NetCheque**: implements an on-line "checking-account" against which payments are authorized.
- **USC/ISI's NetCash**: users purchase currency from the currency server using NetCheque. with multiple currency servers, the NetCheque system is used to clear cross-server payments.
- **CMU's NetBill**: provides a payment instrument analogous to a credit card slip authenticated by kerberos. goods are delivered to the customer encrypted, NetBill sends the key to decrypt the good.

systems gone:

- **first virtual**: customer established an account at First Virtual and sent account ID to merchant.
- **DigiCash**: required special software on the client to implement an electronic wallet to store and retrieve currency.

---

integration with banking systems:

needs to be efficient. customers can either deposit funds in advance or pay periodic statements (electronic credit card).

---

risks and security:

from the customer's perspective:

- stolen payment credentials and passwords
- dishonest merchants or financial service providers
- disputes over quality of services or goods

from merchant's perspective:

- forged or copied payment instruments
- insufficient funds in customers account, especially with off-line payment systems
- dishonest or slow financial service providers

from the financial service provider's perspective:

- stolen customer or service credentials
- forged or copied payment instruments
- customers not paying (applies only to credit models)

the risk may be shifted in one direction or the other by using a credit or debit model and by special agreements.

technical solutions to improve security:

- protect payment credentials with token or smart cards
- use on-line authorization to detect double spending, check for sufficient funds and anomal spending patterns

roles of and rewards for the financial service providers (FSPs):

- they are trusted to hold our money
- they facilitate clearing of the payments
- they insure against fraudulent transactions (risk management)
- they can charge account and transaction fees
- they may benefit from currency exchange

multiple FSPs should not compete on the basis of incompatible payment systems. to keep payment services simple, it shall be possible to clear payments between different systems.

CREDIT CARD

A **credit card** is a small plastic card issued to users as a system of payment. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services.[1] The issuer of the card creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.