"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

Co-funded by the European Union

Electronic Business

Types of Electronic Payments

dr Danijela Zubac

dr Ermina Habibija

UNIVERSITY OF LJUBLJANA
Faculty of Electrical Engineering

University of Pristina
Kosovska Mitrovica

Co-funded by
the European Union

Types of electronic payments

- Electronic payment mechanisms and instruments
- Payment cards
- P2P payments
- Electronic money
- Economic consequences of electronic money
- Data protection in the case of electronic transfer of funds
- Intelligent (Smart) payment cards

Electronic payment mechanisms and instruments

Electronic transfer of funds

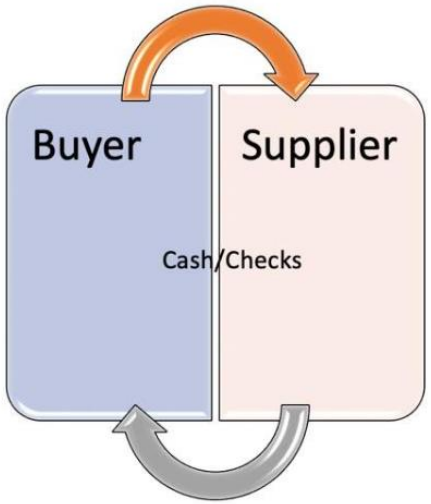
- In the early 1970s, banks began to explore solutions for accessing funds through electronic terminals
- Many financial institutions offer both approaches - the so-called electronic fund transfer (EFT - Electronic Fund Transfer), and the classic transfer of funds based on paper documents.
- EFT can be done using the banks own computer network
- In that case, each customer can access their funds through an electronic terminal within the bank network
- There are more and more financial institutions that integrate their own networks into one large network that serves the users of many banks and financial institutions

Electronic payment mechanisms and instruments

Traditional payment systems

- The customer sees the product, makes a purchase decision and then pays with cash, check or card.

Electronic payment system



Traditional Methods of Payment

Electronic payment mechanisms and instruments

- Compared to traditional payment models, electronic payment systems require greater trust and acceptance of the rules.
- The customer cannot see the product live at the time of purchase, and payment methods are implemented electronically.
- The main goal of the electronic payment system is to increase:

✓ efficiency,
✓ profitability,
✓ improved security and
✓ ease of use.

Electronic payment mechanisms and instruments

- **Customer.** The customer initiates the payment process and chooses a payment method (for example, PayPal, Visa card, payment by bank transfer, payment by cash on delivery, etc.). The average online customer typically uses two or three electronic payment methods.

- **Seller.** The seller can enable multiple payment methods and systems on his website, and the customer chooses which of the available methods to use. A greater number of available payment systems in the electronic store should to attract more customers.

- **Payment processor.** A payment processor is an intermediary that enables sellers to pay with payment cards in e-commerce. The most famous global payment processors are: PayPal, Verisign, 2Checkout, Worldpay and others. Most payment processors operate in local markets.

Co-funded by the European Union

Electronic payment mechanisms and instruments

- In the initial stages of the development of the payment system on the Internet, it was not possible to realize complete transactions, but hybrid payment models were applied.

- Examples of hybrid mechanisms are cash on delivery, a combination of telephone and Internet, payment via general payment slips after ordering via the Internet, and the like.

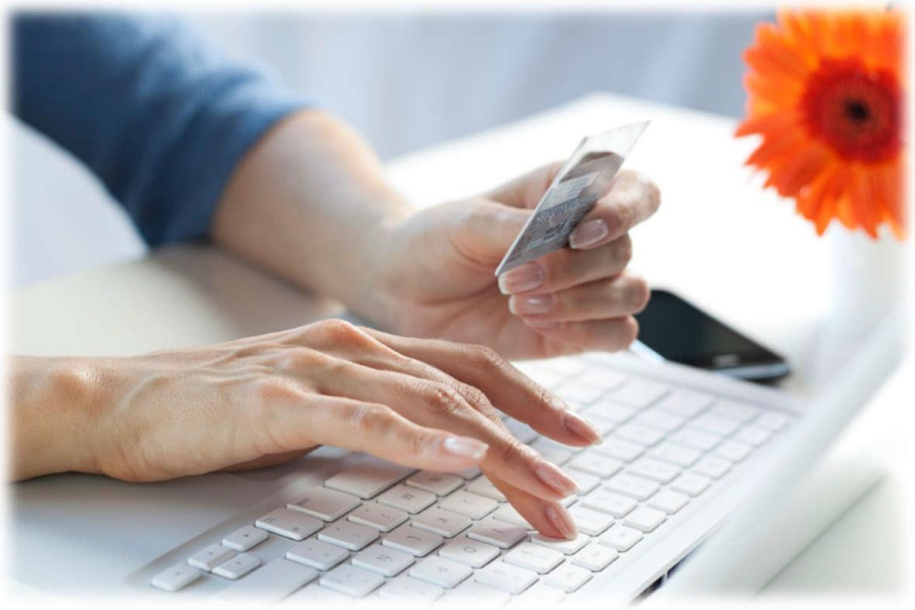
- Today there are a number of different divisions when it comes to electronic payment mechanisms.

- It can be seen that the payment models and methods during times change, so the classification of these models and methods is also variable.

Co-funded by
the European Union

Electronic payment mechanisms and instruments

- The most commonly used payment systems on the Internet can be singled out:
- payment cards;
- electronic checks;
- electronic cash;
- electronic wallets;
- P2P payments;
- voucher payments;
- micropayments;
- mobile payments;
- gold-based systems;
- cryptocurrencies.



Payments in electronic commerce

All payments in electronic commerce can be divided into two categories, namely:

- credit-based payment instruments and
- account-based payment instruments - provide direct access to existing bank accounts (electronic checks, debit cards) or to which payment has already been made in advance (electronic cash).

Systems based on the entered value from the account (provide direct access to existing bank accounts):

- electronic cash (eg Net Cash, E-cash)
- electronic checks (eg Net Cheque)
- smart cards or debit cards (eg Mondex Electronic Currency Card)
- credit-based systems - credit cards with encryption (eg CyberCash, SET protocol)
- authorization of intermediaries (eg First Virtual).

Payments in electronic commerce

There are three types of electronic funds transfer (EFT) according to the functional characteristics of individual instruments and technologies:

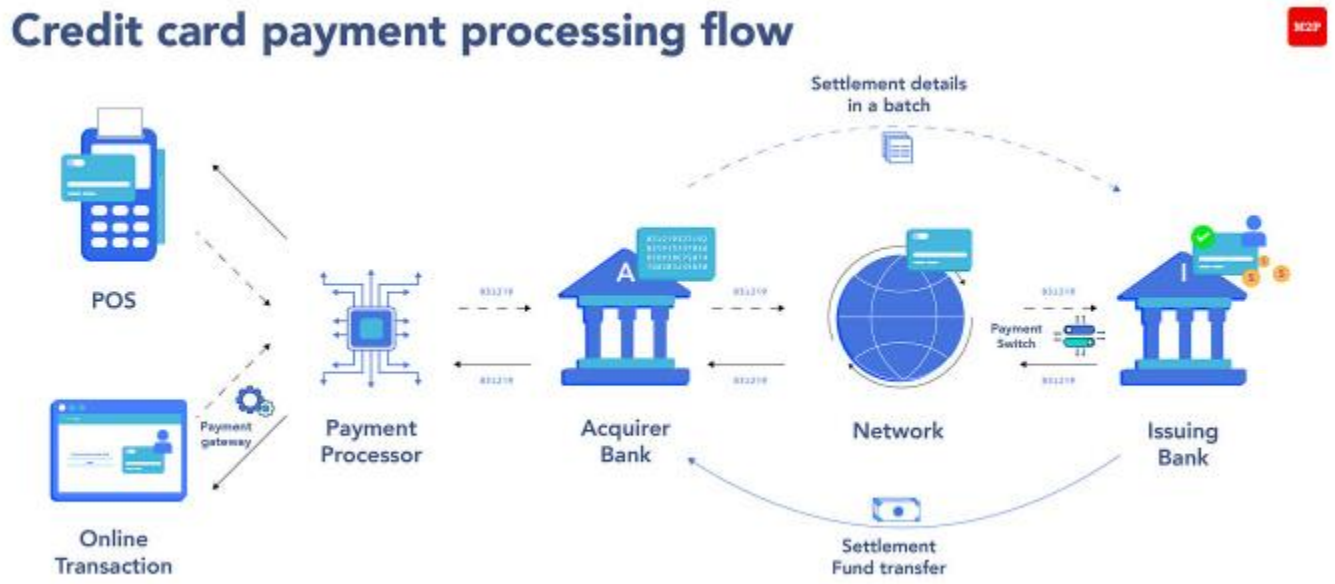
- **Payments in the financial sector**:
  - ✓ payments of large amounts (e.g. interbank payments)
  - ✓ small amount payments (e.g. ATM)
  - ✓ home banking (e.g. paying bills)
- **Retail payments**:
  - ✓ debit and credit cards (e.g. VISA, DinaCard)
  - ✓ shopping cards (e.g. M&S card, Rodic MB Card, C-market)
- **Payments in electronic commerce:**
  - ✓ credit-based payment instruments and
  - ✓ account-based payment instruments

Payment cards

- The most widespread type of payment via the Internet are payment cards (credit and debit).
- Customers surf the Internet in search of a sales website and the product and/or service they want to buy.
- The customer's account is routed through the Online Transaction Sever, which ensures security.
- Transactions (“withdrawal" of the amount from the credit card) are processed through the gateway to the CC Processing Network, where the charge is executed (or canceled).

Payment cards

- The use of payment cards for payments on the Internet is based on expanding the functionality of payment cards used for payments at physical points of sale.
- All types of payment cards can be used for payments on the Internet.
- Regardless of the card type, the payment process is similar.



Payment cards

- A key role in the payment system is played by the payment gateway, which is equivalent to a terminal at a physical point of sale (POS).
- Payment gateway enables the authorization of payment cards and the secure transfer of information between the place of payment via the Internet (website, mobile application, etc.) and the payment processor of the corresponding bank.
- Payment gateway protects sensitive information from credit cards with encryption.

Payment cards

- The payment card payment process begins with the card user (customer) choosing an item at the Internet point of sale, then choosing the check out option.
- After entering the personal data required for delivery and payment, the customer confirms the purchase.
- After receiving the order from the customer, the seller sends information about the start of payment to the payment gateway.
- In response, the customer receives a purchase code and the address of the payment page.
- The customer is then redirected to the appropriate web page to enter their card details, where they confirm the payment.

Co-funded by
the European Union

Payment cards

- With the payment card payment model, there are two approaches in redirecting the customer from the seller's website to the payment processor's website:
- **Redirection.** When the user selects a card to pay with, they are redirected to the payment processor's website. In the address of the web browser, the address changes, and the user is from that moment on the website of the payment processor.
- **Tunneling.** A form for entering payment card data opens on the seller's website page. The customer still has the impression that they are on the seller's website, but they are actually on the processor's website.

Payment cards

Electronic cards as payment instruments can be divided according to:

- **applied technology:** cards with a magnetic strip and smart cards with a silicon microprocessor chip,
- **according to the time of payment and anonymity of transactions:** debit cards, credit cards and cards with pre-paid amounts of money (pre-paid),
- **location of application:** national (valid in the country where they were issued) and international (valid equally, both in the country and abroad),
- **cardholder:** basic, additional, business, etc.

P2P payments

- Peer-to-peer payments, i.e. person-to-person payments, allow the buyer to pay the seller, even if the seller does not have the ability to accept payment cards.
- The most famous P2P payment systems via the Internet are Western Union money transfer, PayPal, Square, Skrill (previously known as Moneybookers), Stripe and others.
- PayPal is a payment and money transfer system over the Internet.
- It implies a direct transfer of money from one account to another. It has been owned by E-bay since 2003.

Western Union money transfer

Western Union is a global company that provides users of its services with fast and reliable money transfers around the world.

Who needs Western Union services?
Everyone who needs to send money quickly, and the recipient receives the full amount safely and does not have to travel far to collect it.

Open account?
It is not required by either the sender or the recipient.

Costs of sending money
The cost of sending money is paid by the sender, while the recipient is paid the full amount - free of charge.

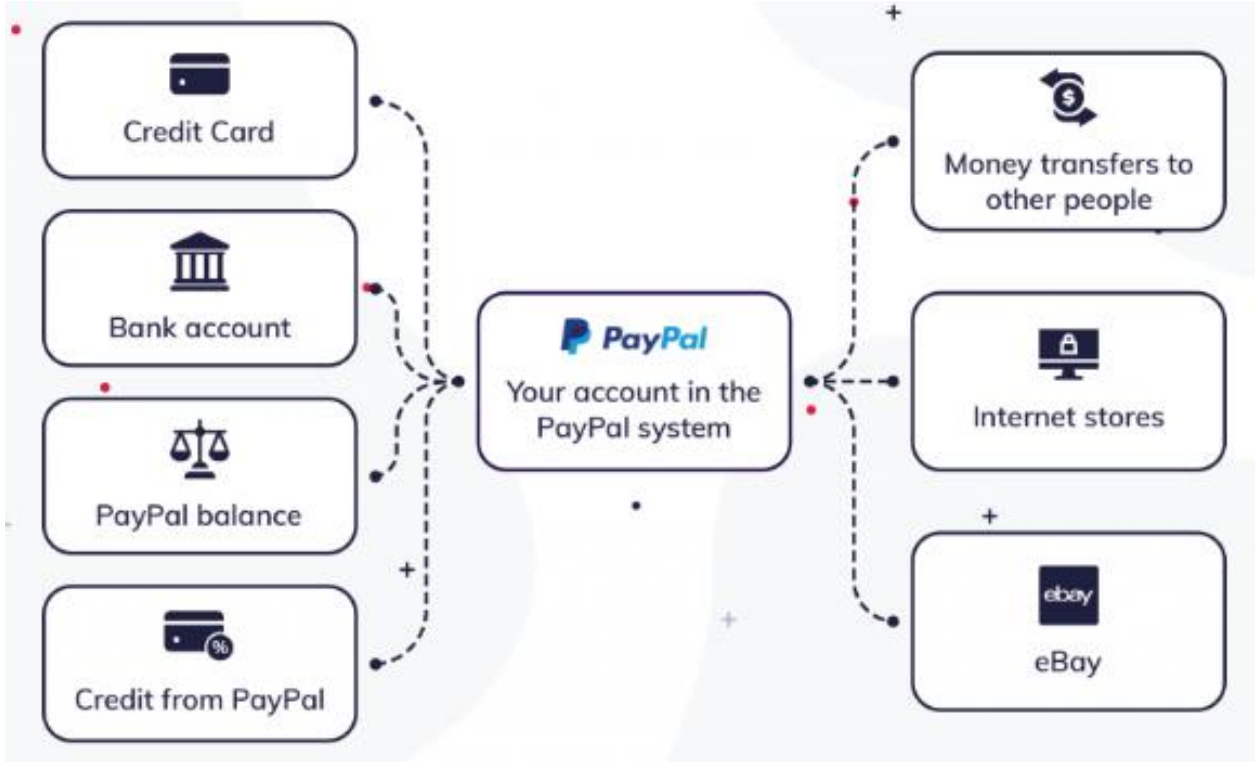
WESTERN UNION®
TRANSFER NOVCA

PayPal

PayPal is a type of P2P service. The P2P payment method allows anyone with an email address to send money to someone else who also has an email address. The initiator of the transaction via PayPal must first register on the PayPal pages, and then transfer a certain amount of money to his user account. The amount can be transferred directly from a bank checking account or using credit/debit cards. The recipient of a PayPal transfer can request a check from PayPal, can open their own account, or can request a transfer of funds to their bank account. PayPal is an example of a payment intermediary that facilitates and enables the global Internet economy.

PayPal also enables payments between suppliers, auction sites and other commercial users, for which it charges a certain amount.

PayPal



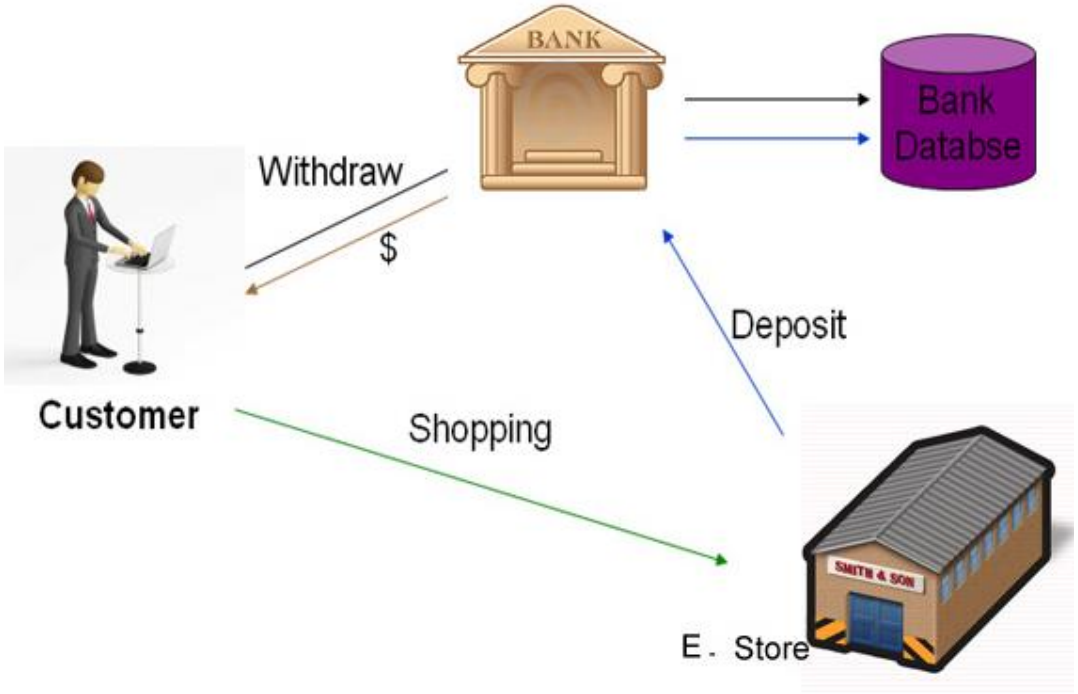
PayPal

Moneybookers (Skrill)

Moneybookers is an internet account (e-wallet), which serves to pay for services on the internet in a very simple way.
Through it you can send and receive money as well as pay for various other online necessities (books, wardrobe, etc.) waits up to 48 hours.

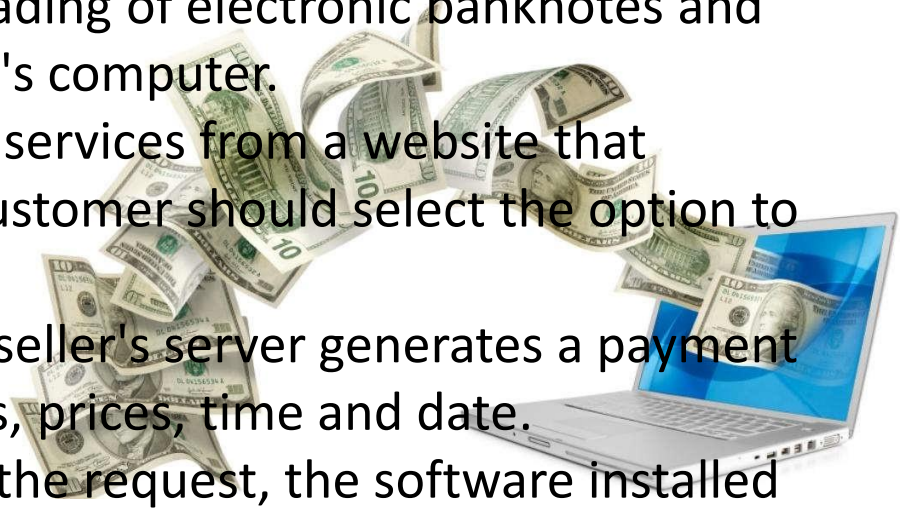
Electronic money

- Similar to traditional cash, electronic cash enables transactions without the need to use the services of a bank or a third party.
- E-cash is transferred directly and instantly between sellers and buyers.
- E-cash is most often stored on smart cards, by storing monetary value on the card's chip.



Electronic money

- The customer receives special software for working with the electronic cash system from the bank or financial institution.
- Digital money can be bought for real money using that software. The software enables downloading of electronic banknotes and placing them on the customer's computer.
- When purchasing products or services from a website that accepts electronic cash, the customer should select the option to pay by electronic cash.
- The software installed on the seller's server generates a payment request, with a list of products, prices, time and date.
- When the customer confirms the request, the software installed on the customer's computer sends a payment instruction. Electronic cash is transferred to the seller's bank account.



Co-funded by the European Union

Electronic money

- Every electronic banknote is issued by a bank in the name of deposited real money, just as every paper banknote is issued on the basis of a gold backing
- Unlike payment cards, electronic money can achieve complete anonymity of the customer
- The idea of electronic money is that the value, instead of on paper, is stored in digital memory as a series of digits

Electronic money

- The electronic money system should also enable small payments (so-called micro payments)
- The payment system must have mechanisms for recognizing and preventing repeated payments with the same digital banknotes
- Due to international transactions, as well as the lack of transaction tracking records in certain electronic money systems, the problem of taxation of transactions on the Internet may arise

Electronic money

- Systems based on digital notes have a face value problem

- In order to pay a certain amount there must be digital notes of the appropriate value, or else the system would have to be able to "return the change" in the form of new digital notes
- Alternative solution - all banknotes have the same face value

Electronic money

- Provided that the above problems are solved, one can enjoy the numerous advantages of electronic money

❖ It is more portable and easier to handle than paper money

❖ The costs of transferring money via the Internet are significantly lower than the costs of transferring money through the conventional banking system

❖ As electronic money uses the already existing network and computers of its users, there are almost no transfer costs

❖ If the money is lost, it can be immediately replaced by canceling the missing electronic notes and replacing them with new ones

❖ It can be used by anyone who has access to a bank on the Internet

Online and offline payments with electronic money

- The electronic money payment process can be online or offline
- When it comes to online payments, the authenticity of digital banknotes must be verified immediately
- In the case of online payment, a digital banknote is used only once

Online and offline payments with electronic money

- The most famous online systems are
- ✓ E-Cash (DigiCash)
- ✓ NetCash
- ✓ Bitcoin
- The most famous offline systems are
- ✓ Mondex (MasterCard)
- ✓ VisaCash (Visa)
- Although there are differences, the potential steps in electronic money transactions are as follows
- The consumer opens an account with the issuer (e.g. virtual bank) by depositing funds with him
- The issuer keeps the consumer's funds for future withdrawals, which will be made by those who receive the digital banknote from the consumer

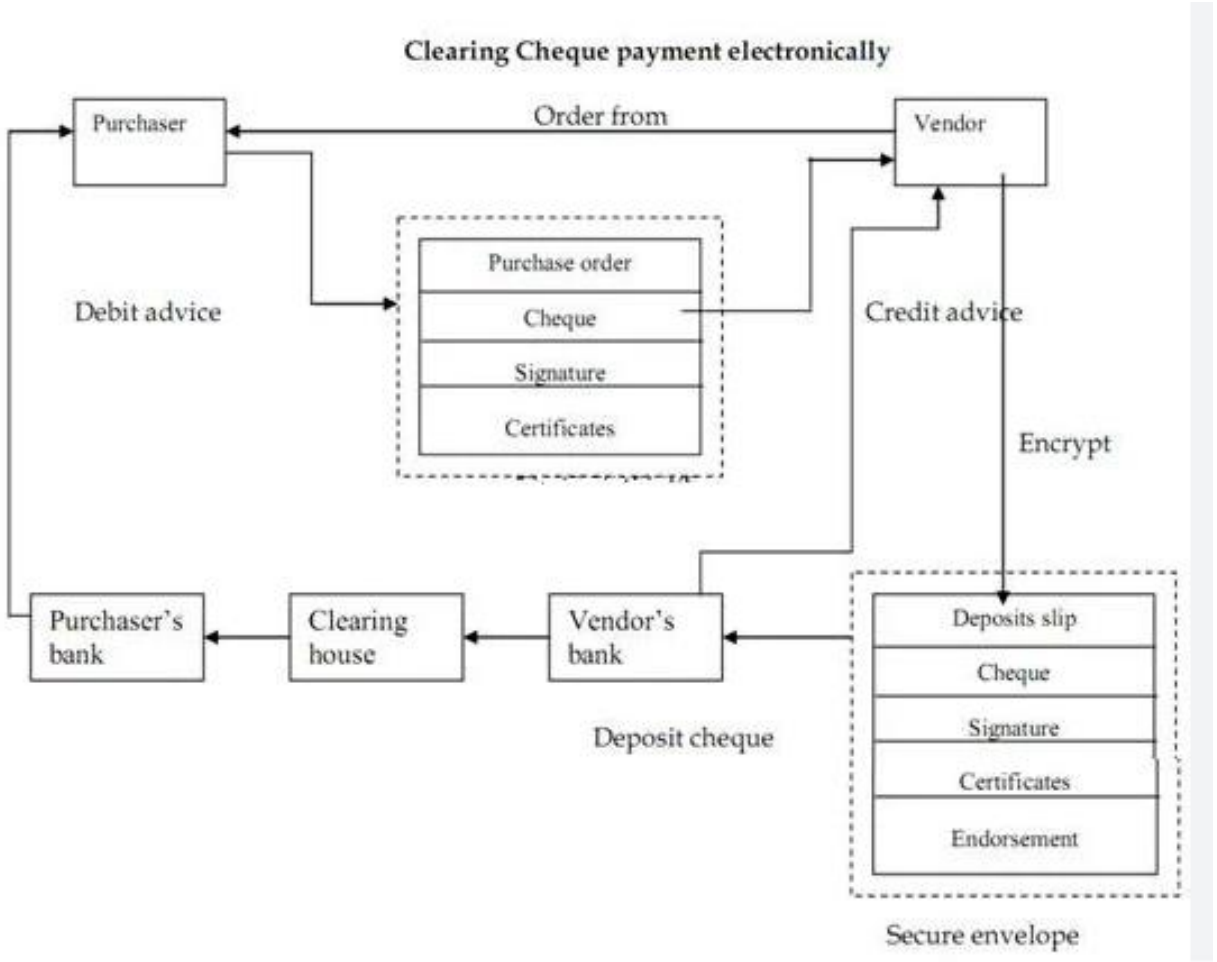
Online and offline payments with electronic money

- When a consumer wants to make a purchase over the Internet, he sends an encrypted message with a digital signature to a virtual bank requesting financing
- The virtual bank debits the consumer's account and sends digital money to the consumer's computer or mobile device
- Digital money systems can create an audit trail of transactions or they can be anonymous
- In anonymous systems, the virtual bank assigns digital signatures that only it can create
- Users can decrypt such a signature using the key provided by the virtual bank, to verify that it has issued the money
- The consumer transfers the digital money to the seller, who can verify its authenticity and transfer it to their virtual bank account, send it to another person, or transfer it to another account
- Virtual Bank will charge the consumer and/or seller a transaction fee or a system service fee

Electronic check

- Electronic check systems should extend the functionality of existing checking accounts to enable their use for online shopping payments.
- The electronic check system requires the user to obtain an electronic check book from his bank on the appropriate hardware (CD, USB memory, smart card, etc.).
- The electronic checkbook contains the digital signature of the user, as well as the public key of the issuing bank.

Electronic check



Electronic wallets

- Electronic wallets (E-wallets) are applications that are an extension of standard payment instruments, such as cards or bank transfer.
- They are based on user accounts opened with the electronic wallet provider.
- After paying the deposit, the user can shop on the websites by logging into their electronic wallet.

Electronic wallets

- A digital wallet has a software and data component. The software provides security and encryption related to personal data and current transactions.
- The data component contains data such as shipping address, billing address, payment methods (credit card number, expiration date, security numbers) and other information.
- The most important providers of electronic wallets are Google and PayPal.

Bitcoin

- **Bitcoin** is a P2P electronic payment system introduced in 2009 that is gaining more and more popularity
- The software on which it is based is open-source
- It is called a "decentralized currency" because it is not tied to any particular bank or financial institution
- Distributed servers contain ledgers that store details of account balances and transactions

Co-funded by the European Union

Online and offline payments with electronic money

Bitcoin

- Anyone can join the server network, as well as the user network
- Users use the currency using a digital "wallet" - software for personal computers and other devices
- Users can access currency in two ways:
- In exchange for classic currency
- By "mining", i.e. by "socially useful work" in maintaining registers
- Security is achieved by asymmetric cryptographic algorithms
- Anonymity is not guaranteed
- BitCoins can be stolen, in such a way that refunding the damage is impossible

Economic consequences of electronic money

- Most costs will be eliminated with electronic money
- The fee for exchanging electronic money should be very small
- Electronic money users will use the Internet to expand their spending patterns geographically
- Consumers can have a large number of currencies stored on their computer's hard drive
- In the event that one of these currencies depreciates, consumers will likely seek to exchange that type of electronic money for a more valuable and stable form of electronic money.
- The real presence of digital money on the market is still marginal, and it can be concluded that despite all the advantages, electronic money has a difficult path to wider acceptance.

Protection problems with electronic payment

- Protecting the PIN, and therefore the bank card, is crucial for the overall security of EFT transactions

- Bank cards can be lost, stolen or forgotten

✓ In such cases, the only existing countermeasure against unauthorized access is a secret PIN

✓ This is why the PIN should only be known by the legitimate cardholder, and should never be stored or transmitted in open form

Protection problems with electronic payment

- The length of the PINs should be long enough so that the possibility of guessing the correct value in the case of a brute force attack is acceptably small
- PINs should be short for owners to remember (recommended length is four to eight digits)
- PINs can be chosen either by the bank or by cardholders

Protection problems with electronic payment

If the bank chooses a PIN, it adopts one of two procedures:

1. PINs are generated cryptographically from cardholder account numbers
   - ✓ The advantage of this procedure is that the PIN record does not need to be stored within the EFT system
   - ✓ The disadvantage is that changing the PIN requires selecting either a new user account or a new cryptographic key
   - ✓ As all PINs are calculated using the same key, changing one requires changing all PINs
2. The bank chooses the PIN randomly and simultaneously stores the record in the form of a suitable cryptogram (the exact form of the PIN should never be displayed within the EFT system)

Protection problems with electronic payment

- ❑ Cardholders can also choose PINs
- The best procedure for cardholders is to choose a random PIN
- Once a PIN is selected, the bank should be notified
- PINs can be sent to the bank by registered mail, or entered through secure terminals, which encrypt the PIN, and store it in the bank's archive.
- ❑ People often forget their PIN
- Banks should prepare special procedures in advance that will resolve such cases
- ❑ Procedures may adopt one or two different approaches
- The first one works to find out the forgotten PIN, and returns it back to the owner
- The second generates a new PIN

Protection problems with electronic payment

PIN number requirements

- There are several requirements for security, which refer to the identification of users based on PINs and bank cards, and they are as follows:

✓ The PIN must be kept secret at all times
✓ The PIN must not be written on the card
✓ The card should contain a unique number (CVV - Card Verification Value/Code)
✓ The identification process must be time-dependent (to prevent re-attack)

Intelligent cards
Smart payment cards

- The forerunners of intelligent are classical:
- – credit and debit cards
- Despite all the improvements they have brought, classic cards have proven to be unsuitable for electronic transfer of funds, i.e. online trading
- The Internet is a network through which unprotected or weakly protected sensitive data, such as credit or debit card numbers and corresponding activation codes, should not travel.
- It should also be avoided if possible to store card numbers on the servers of their recipients, because the endpoints of Internet communication are often tempting targets for unauthorized access.
- There have been many discovered abuses of payment cards that occurred for the above reasons, and it is quite certain that even more have remained undetected.

Intelligent cards
Smart payment cards

- A smart card is a plastic card, which looks like a regular credit or debit card, with one detail that separates it from them, which is an integrated circuit, i.e. a chip, on which the processor and memory are located.

- A traditional credit or debit card stores data on a magnetic stripe

✓ The strip is made up of three tracks on which store data
✓ None of these tracks have the capacity to store large amounts of data
✓ The entered data is subject to external influences, and can be changed, deleted or damaged, accidentally or intentionally.
✓ Although the possibility of both reading and writing data is left, due to insufficient security and practical reasons, writing is almost never used, so we can call this card only a memory card, i.e. a card on which data is only stored

Smart payment cards

- The smart card has about 100 times more memory space and a processor that enables the execution of various algorithms
- ✓ The whole process (e.g. encryption) starts, lasts and ends on the card itself and no data leaves the card making the system isolated from the outside world
- ✓ Only the cardholder can activate it by entering the appropriate personal identification number (PIN).

Intelligent cards
Smart payment cards

- The greatest strength of Smart Card technology lies precisely in the variety of possible applications
- ✓ It is possible to develop various applications in areas such as: information technology, telephony, banking, healthcare, etc.
- Currently, there are hundreds of millions of smart cards in circulation in various areas with a tendency for further development
- There is no doubt that the transition from magnetic tape to chip is an inevitable sequence of events

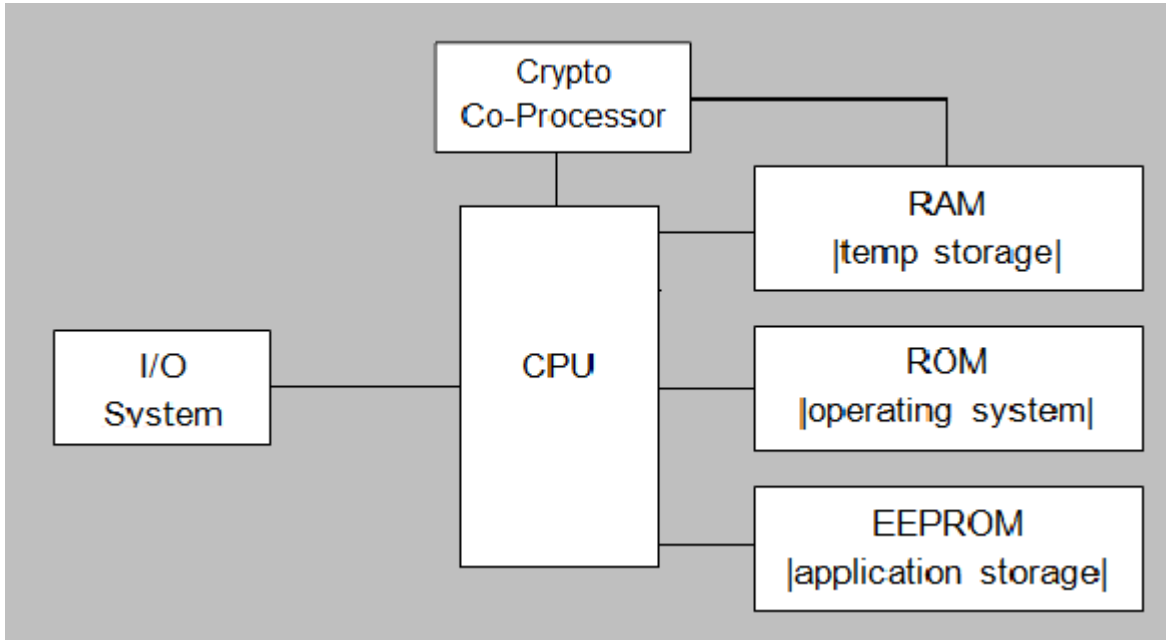
Intelligent cards
Development of smart technology

- A smart card is a miniature personal computer
- Includes:

✓ processor (CPU) with which various calculations are performed
✓ Read-Only Memory (ROM) - the memory on which the operating system is located
✓ Random Access Memory (RAM) - memory used for temporary storage during processor operation
✓ Electronically Erasable and Programmable Read Only Memory (EEPROM) - memory in which the data of interest is stored

- Older models of smart cards typically have an 8-bit processor that operates at a frequency of around 5Mhz, while in the last few years, 32-bit RISC processors, operating at 25-32 MHz, have become more common.
- The operating system is responsible for data security, and it takes care of access rights to individual files

Intelligent cards
Development of smart technology



Smart card architecture

Development of smart technology

- The smart card does not have a keyboard or any display
- It can only function in combination with a suitable device for reading smart cards - **CAD (Card Acceptance Device**).There are two basic types of smart cards - contact and contactless
- Contact smart cards have electrical contacts with which they come into contact with the electrical contacts of the reader, and they need to be inserted into the reader.
- Contactless cards have a thread of wire inside them which acts as an antenna, and through it they communicate with the environment, which is especially useful for transactions which must be done at high speed
- Smart cards can also differ in size, in addition to standard cards dimensions (the size of a classic payment card) also exist SIM-cards, which are smaller in size, adapted for use in mobile telephony

Intelligent cards

Development of smart technology

Production phase

- it is carried out by chip manufacturers, and during that phase, the so-called manufacturer's key, unique for each smart card, but based on the manufacturer's master key

Pre-personalization phase

- the chip is placed on the card and tested, and the manufacturer's key is replaced by the so-called with a private key, physical access to the memory is still prohibited, and only logical access is allowed

Personalisation phase

- user data is entered, PIN, unblocking PIN, applications and other data of interest are entered, and the phase ends with the placement of a key indicating that the card is still in the usage phase

Utilisation phase

- the user regularly uses the card, and access rights to certain data are regulated by an active application controlled by the operating system

Blocking phase

- for technical and security
- reasons, it is not recommended to pass into the hands of another owner

Development of smart technology

- Creating a multi-functional cheap smart card that will be both a payment and an identification card and enable access to the mobile network is a serious task, but it is necessary if it is to be widely accepted.
- There are several ways to achieve this:

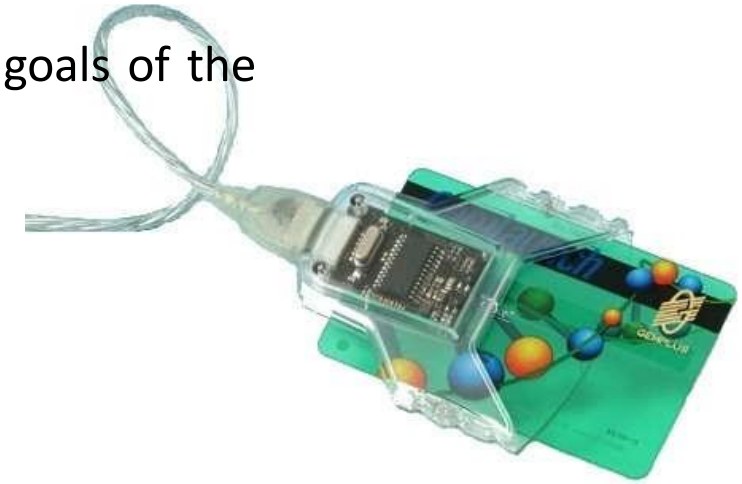
✓ By creating common standards for the operating system
✓ By creating a common interface between applications and the operating system
✓ By adopting one operating system that is in the widest application

- As a contribution to the standardization of the operating system for cards, standards should be harmonized for software applications that use smart cards as part of the system

Development of smart technology

- Applications communicate with smart card readers that read or write data from the smart card
- Readers can be connected to personal computers, integrated into ATMs, embedded in POS (Point of Sale) terminals, mobile phones, or stand-alone with their own small LCD screen and numeric keypad.
- Laser cards are a continuation of the development of smart technology in the direction of increasing hardware resources

- They have the ability to store up to several MB and represent the future of the development of multimedia cards with which it will be possible to perform monetary transactions as well as many other personal services.
- Its international character was set as one of the ultimate goals of the development of the smart card program



Smart card security

- To prevent misuse and copying, the smart card relies on controlling access to the data stored on the EEPROM by its own security operating system located on the ROM
- The EEPROM can contain a 1024-bit RSA key, personal data about the cardholder, current account number, certificates, and it is of great interest that these data are not exposed to misuse.
- It can be ensured that part of the data is visible to the smart card reader while part is not and cannot leave the card at all
- Well-designed systems use multiple security measures
- In order to use the card, it is necessary to know
- The corresponding activation code- PIN (Personal Identification Number)
- The existence of a PIN eliminates the possibility of misuse cards in case of theft or loss

Intelligent cards

Smart card security

- PIN identification is many times more secure than any other method of identification for the following reasons:

✓ The PIN never travels over the network and is resistant to brute force or dictionary attacks

✓ Policies governing the length and frequency of PIN changes can be less restrictive than those for passwords – thus avoiding staff compromising system security by writing down identification codes on paper or in files

- The development of smart technology leads to the generation of other techniques as well

✓ Thus, in terms of security, the method of generating the user's fingerprint on the card chip has been adopted, in order to ensure on-the-spot identity verification when paying in a bank or retail network via a reader.

✓ With the development of devices for the production of cards with ultra-graphics, the technology of generating an electronic photo of the user on the plastic base of the card itself through the so-called smart printer

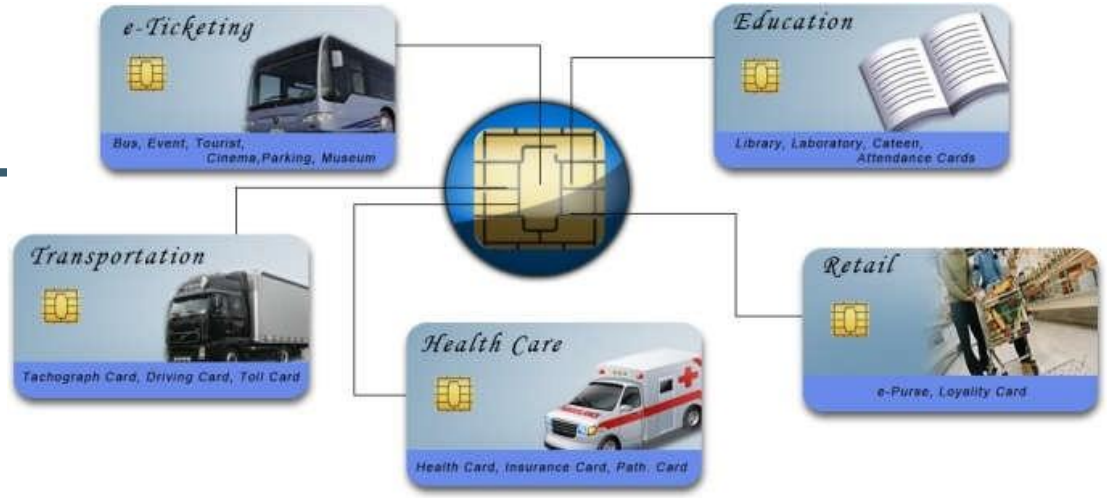
Smart card applications

- **Finances**
  - ✓ A smart card can serve as a universal payment card, similar to a classic payment card, but in a much more secure environment
  - ✓ Smart technology provides the possibility of designing certified bank cards that can be loaded with a cash deposit (electronic cash) based on a concept known as an electronic wallet (electronic purse).
- **Identification**
  - ✓ A smart card can serve as a driver's license, a student card, or simply as a universal identification card
  - ✓ It can also be used for authorization, that is, control of access to objects

Intelligent cards
Smart card applications

- **Telephony**
- ✓ Unlike an ordinary SIM card, which an unauthorized user can easily misuse if he finds out the PIN of its owner, a smart card ensures reliable identification of the user in the GSM system, and thus safe initiation of calls.
- ✓ There are services that enable online transactions by mobile phone, where the amount is automatically deducted from the prepaid card
- ✓ Scrambling of confidential telephone conversations, thereby preventing them from being eavesdropped by a third party
- **Information technologies**
- ✓ The most common application is the control of access to computers and computer networks
- ✓ The first modem with an integrated smart card reader was introduced back in 1996
- ✓ All major computer manufacturers have already produced hardware that supports smart card functionality

Smart card applications



- **Traffic**
  - ✓ Applications in this area are numerous, starting with electronic tickets and vouchers, which can greatly simplify the procedures related to seat reservations, baggage handover, etc.
  - ✓ Electronic tickets and vouchers can also provide additional comfort that was not possible until now
  - ✓ Smart cards can also be used to pay tolls, parking, etc.
- **Healthcare**
  - ✓ The smart card can serve as a health card and health record
  - ✓ It can contain information that can be vital in an emergency - what is the owner's blood type, what is he allergic to, is he a heart patient, etc.Information about the user's health insurance may also be stored

WBnet

Co-funded by the European Union

Questions & Answers

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

Network of centers for regional short study programs in the countries of the Western Balkans

Call: ERASMUS-EDU-2023-CBHE

Project number: 101128813

ATUCC

UNIVERSITY OF LJUBLJANA
Faculty of Electrical Engineering

POLITÉCNICA

University of Pristina
Kosovska Mitrovica