**UNIT – I**

E- Cash and virtual money: electronic data interchange (EDI) – NEFT/ RTGS Electronic payment mode- foundation of e-cash and issues; Anonymity, intractability, virtual currencies, bit coin

**Electronic data interchange:**

Electronic Data Interchange (EDI) is the electronic interchange of business information using a standardized format; a process which allows one company to send information to another company electronically rather than with paper. Business entities conducting business electronically are called trading partners.

Many business documents can be exchanged using EDI, but the two most common are purchase orders and invoices. At a minimum, EDI replaces the mail preparation and handling associated with traditional business communication. However, the real power of EDI is that it standardizes the information communicated in business documents, which makes possible a "paperless" exchange.

The traditional invoice illustrates what this can mean. Most companies create invoices using a computer system, print a paper copy of the invoice and mail it to the customer. Upon receipt, the customer frequently marks up the invoice and enters it into its own computer system. The entire process is nothing more than the transfer of information from the seller's computer to the customer's computer. EDI makes it possible to minimize or even eliminate the manual steps involved in this transfer.

**Advantages of EDI:**

There are several advantages to Electronic Data Interchange:

* **The paper usage reduced:**The expense of storing, printing, recycling, reduces up to the maximum amount due to the EDI.
* **Improved quality of Data:**The data entry errors are reduced due to EDI.
* **Speed Increases:**The best advantage is the increase in the speed of the data interchange. With everything going online, the speed of the information transfer increases exponentially.
* **Security:**By following the Protocols and the standard rules, the security of all the important documents is always secure and safe.
* **Information accuracy:**Since the information exchanged is based on standards agreed by the sender and receiver both, the correct information is always transferred regardless of where they belong to.
* **Less Cost:**With very less errors, fast response time, every thing becoming automated, and no use of paper, the cost automatically reduces.

**Disadvantages of EDI:**

* The initial setup of the EDI is very Time-consuming.
* EDI standards keep on changing after some amount of time.
* A very systematic and proper back up is required as the entire data relies on EDI.
* The setup and maintenance of the EDI is very expensive.

**How Does EDI Work?**

EDI (electronic data interchange) works in minutes by using either a software system or an outsourced managed service to automatically send business documents and data between trading partners from computer to computer in EDI standard format, without humans.

EDI implementation in-house (on-premises) is done by on boarding business trading partners, mapping document fields, and achieving  EDI integration with an [enterprise resource planning (ERP) system](https://tipalti.com/erp-integrations/).

Small businesses and medium-sized companies may outsource an EDI solution using cloud-based SaaS or PaaS EDI software through a managed service that integrates with ERP and [AP automation software](https://tipalti.com/ap-automation/). Automation software may include a supplier portal for on boarding vendors and sharing documents and status and use flat-file or API integration with an ERP.

EDI standards include ANSI (including ASC X12),EDIFACT (also called UN/EDIFACT from the United Nations), TRADACOMS, and ebXML, with each EDI standardized format including different versions that must be the same version for both trading partners.

An EDI translator within the EDI software or outsourced EDI managed service translates EDI data elements formats to enable real-time business document processing by integrated ERP and AP automation systems at each business trading partner.

**NEFT: (National Electronic Funds Transfer)**

NEFT means National Electronic Funds Transfer. It is a mode of money transfer that enables one-to-one payments within India. NEFT is owned and operated by the Reserve Bank of India, and through this facility, you can transfer money from one account to another. You may initiate transfers between two bank accounts you own or from your account to others’ accounts in different banks. However, you can make this type of transaction only if your bank is NEFT-enabled.

Advantages of NEFT

Now that it is clear what NEFT means let us look at some of its advantages.

* You can transfer funds from any account of another account of any NEFT-enabled bank within India.
* This facility is available 24/7, throughout the year, including holidays.
* Money is transferred within half an hour in a secured manner.
* Confirmation of transaction is sent to the remitter by SMS and email.
* You do not have to pay any charges for online NEFT transactions.
* You do not need cheques or demand drafts for these transactions.
* You need not visit your bank branch to send money via NEFT.
* You can also pay your credit card bill, loans, EMIs, and utility bills via NEFT.

How to Initiate NEFT Transactions?

Use the steps below to transfer funds via NEFT.

1. Log in to your [internet banking](https://www.dbs.com/digibank/in/banking/internet-banking/ibanking) account on your laptop or mobile app.
2. Go to the ‘Fund Transfer’ tab and select ‘NEFT’.
3. Choose your beneficiary or add a new one by clicking on the ‘Add Beneficiary’ tab. Enter their details, such as their account number, bank name, branch and IFSC code, their name, and mobile number. Once you add a new beneficiary, you can initiate the transaction after another 30 minutes.
4. Confirm beneficiary details – name, account number, and mobile number (for SMS notifications).
5. Complete the transaction by entering the OTP sent on your Registered Mobile Number (RMN).

Your bank will send both you and your beneficiary an SMS confirming the transaction.

## Real-Time Gross Settlement: (RTGS)

## The term real-time gross settlement (RTGS) refers to a funds [transfer](https://www.investopedia.com/terms/t/transfer.asp) system that allows for the instantaneous transfer of money and/or securities. RTGS is the continuous process of settling payments on an individual order basis without [netting](https://www.investopedia.com/terms/n/netting.asp) debits with credits across the books of a central bank. Once completed, real-time gross settlement payments are final and irrevocable. In most countries, the systems are managed and run by their central banks.

## How Real-Time Gross Settlement (RTGS) Works:

When you hear the term real-time, it means the settlement happens as soon as it is received. So, in simpler terms, the transaction settles in the receiving [bank](https://www.investopedia.com/terms/b/bank.asp) immediately after it is transferred from the sending bank. Gross settlement means transactions are handled and settled individually, so multiple [transactions](https://www.investopedia.com/terms/t/transaction.asp) aren't bunched or grouped together. This is the basis of a real-time gross settlement system.

An RTGS system is generally used for large-value interbank funds transfers operated and organized by a country’s [central bank](https://www.investopedia.com/terms/c/centralbank.asp). These transfers often require immediate and complete clearing. As mentioned above, once transactions are settled, they cannot be reversed.

In 1970, the U.S. Fed wire system launched. It was the first system resembling a real-time gross settlement system. It was an evolution of the telegraph-based system used to transfer funds electronically between U.S. Federal Reserve banks.The British system, called the Clearing House Automated Payment System (CHAPS), is currently run by the [Bank of England](https://www.investopedia.com/terms/b/boe.asp). France and other [Euro zone](https://www.investopedia.com/terms/e/eurozone.asp) nations use a system called Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2).Other developed and developing countries have also introduced their own RTGS-type systems

## Benefits of Real-Time Gross Settlement (RTGS)

RTGS systems, increasingly used by central banks worldwide, can help minimize the risk to high-value payment settlements among [financial institutions](https://www.investopedia.com/terms/f/financialinstitution.asp). Although companies and financial institutions that deal with sensitive financial data typically have high levels of security in place to protect information and funds, the range and nature of online threats are constantly evolving.

## Real-time gross settlement can allow a smaller window of time for critical information to be vulnerable, thus helping mitigate threats. Two common examples of cybersecurity threats to financial data are social engineering or [phishing](https://www.investopedia.com/terms/p/phishing.asp)—tricking people into revealing their information—and data theft, whereby a hacker obtains and sells data to others.

### ELECTRONIC PAYMENT MODES:

### Credit/Debit card payments:

As a global payment solution, by enabling payment acceptance via cards merchants can reach out to an international market.Credit cards are simple to use and secure. The customer just has to enter the card number, expiry date, and CVV, which has been introduced as a precautionary measure. The CVV helps detect fraud by comparing customer details and the CVV number.Debit cards are considered the best payment method for e-commerce transactions.Debit cards are usually preferred by customers who shop online within their financial limits. The main difference between credit and debit card is with a debit card one can only pay with the money that is already in the bank account, whereas in the case of a credit card, the spent amount is billed, and payments are made at the end of the billing period.

### Prepaid card payments:

They usually come in different stored values and the customer has to choose from them. Prepaid cards have virtual currency stored in them. Though the adoption rate of prepaid cards is low, they are gradually becoming popular for certain niche categories.

### Bank transfers:

Though not popular nowadays but still bank transfer is considered as an essential payment method for ecommerce.It is considered as ‘if all else fails’ kind of payment method. Some of the ecommerce stores are also keen on using bank transfer payment options.It is a simple way of paying for online purchases and does not require the customer to have a card for payment purposes

### E-Wallets:

E-wallet is one of the upcoming trends which gives a new shopping experience altogether. The use of e-wallets is becoming popular at an alarming rate.E-Wallets require a sign up from merchants as well as customers. After creating an e-wallet account and linking it to the bank account they can withdraw or deposit funds.The whole procedure with an e-wallet is easy and fast. Considered as an advanced and instant digital payment method, e-wallets can be integrated with mobile wallets using advanced functionalities like NFC.Prepaid e-wallet accounts store customer information and multiple credit/ debit cards and bank accounts. It needs one-time registration and eliminates the need for re-entering information every time while making payments.

### Mobile payments:

Payment acceptance was no exception for mobile penetration.This digital payment solution offers a quick solution for customers. To set up a mobile payment method, the customer just has to download software and link it to the credit card.As ecommerce is becoming mobile mainstreamed, customers are finding it more convenient to use mobile payment options.

**FOUNDATION OF E- CASH AND ISSUES:**

## What is eCash?

ECash was a digital-based system that facilitated the transfer of funds anonymously. A pioneer in crypto currency, its goal was to secure the privacy of individuals that use the Internet for [micropayments](https://www.investopedia.com/terms/m/micropayment.asp). ECash was created by Dr. David Chaum under his company, DigiCash, in 1990. Though there was interest in the platform from large banks, eCash never took off and DigiCash filed for bankruptcy in 1998. DigiCash, along with its eCash patents, was eventually sold off. In 2018, Chaum launched a new startup focused on cryptography.

## Understanding eCash

The idea for eCash came from Dr. David Chaum in 1983. He was ahead of his time in thinking about privacy concerns in the age of the Internet. And not only did he advocate for privacy but he took it a few steps further in creating an anonymous based payment system for the digital age. This was even before the Internet was available for public use. In 1990, Chaum created the company, DigiCash, to realize his idea for eCash.

The core concept behind eCash was blind signatures. A blind signature is a type of digital signature in which the message's content is invisible prior to signing. In this manner, no user is able to create a link between withdrawal and spend transactions. The money used in the system was called "Cyber Bucks."

## eCash's Rise and Fall:

DigiCash gained a lot of traction in the 1990s when Internet companies were taking off. The company signed deals with many banks that intended to use the platform. These banks included Deutsche Bank ([DB](https://www.investopedia.com/markets/quote?tvwidgetsymbol=db)), Credit Suisse ([CS](https://www.investopedia.com/markets/quote?tvwidgetsymbol=cs)), and other banks across the globe. Microsoft was also interested in eCash for Windows 95 but the two companies couldn't agree to a deal.

The banks that decided to implement eCash started testing the platform but never sold it as a viable product to its customers. The only bank that actually used the platform was Mark Twain Bank in St. Louis, Missouri. The service was free to buyers, but sellers had to pay a transaction fee. Mark Twain Bank had signed up 300 businesses and 5,000 individual users but the platform never gained traction. According to Chaum, "As the Web grew, the average level of sophistication of users dropped. It was hard to explain the importance of privacy to them."

DigiCash eventually filed for bankruptcy in 1998. It was sold off to eCash Technologies along with its patents for eCash. The trademark for the name is now with Due Inc. Due was founded in 2015 and is ranked one of the top 10 e-wallets in the world

**Issues and Challenges Regarding E Cash or E Payment Systems**

 1. Lack of Usability:

 Electronic payment system requires large amount of information from users or make transactions more complicated by using complex elaborated websites interfaces. For example, credit card payments through a website are not that easy as this system requires large amount of personal data and contact details in web form.

2. Lack of Security:

Online payment systems for the internet are an easy target used by hackers for stealing money and personal information. The main problem of e-cash is that it is not commonly accepted because it is necessary that the commercial institution accept it as payment method. Another problem is that when we make payment by using e-cash, the client and the businessmen have accounts in the same bank which issue e-cash.

 3. Lack of Trust:

Electronic payments have a very huge record of fraud, misuse and low reliability as well as it is new system which don’t have established positive reputation. Potential customers often remark this risk as the key reason why they do not make online purchases.

4. Lack of Awareness:

 Making online payment is not an easy task and educated people also face problems in making online payments. Therefore, they always prefer traditional way of shopping over online shopping. Sometimes there is a technical problem in server and when customers tried to make online payments due to this they fail to make payments. As a result, they avoid online purchases.

5. Lack of Feasibility:

 Online Payments are not feasible. Mainly the population of rural areas is not digitally literate even they are not able to operate computers. As they are not aware about technological innovations, they do not show interest in online payments. So, the online payment systems are not feasible for rural areas.

## ECash and Online Security:

Despite the failure of DigiCash and with it eCash, online security is an ongoing issue in the digital realm to this day. Financial information, stored on a computer or electronic device, or the Internet more generally (e.g., the cloud) is vulnerable to hackers. Crypto currencies are extremely popular today and owe their foundations to eCash. The most popular crypto currency is Bit coin, which was created in 2009 by an anonymous creator and had a better luck gaining traction quickly. Overall, many consider Dr. Chaum to be the father of digital currency.

In 2018, Chaum launched a new [startup](https://www.investopedia.com/terms/s/startup.asp) called Elixxir, whose purpose is to create a [cryptography](https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/) network focused on communication anonymity that is controlled by users to protect their information, as opposed to the current setup, where companies have detailed access to consumer information and use it for targeting ads to generate revenue.

**ANONYMITY:**

David Chaum [Cha83] originally proposed electronic cash which offers anonymity even against a collaboration of shops and the bank. The primary reason for incorporating user anonymity into e-cash was to simulate electronic cash resembling physical cash. And indeed, one of the motivating aspects of using physical cash is that it reduces the ability to link a user with a purchase, therefore providing some degree of privacy to the user. It should be noted that even physical cash is not completely anonymous since the shop can see the buyer during a purchase (potentially taped with an in-store video), Legal issues about anonymity: Governments have a great interest in controlling their currency since they have a vested stake in making sure that electronic cash does not hurt their economies. Also, governments have rules and regulations electing monetary exchanges across different countries and when the transaction amounts are large. Electronic cash can make money laundering more difficult since a coin must make a full cycle from the bank during withdrawal to the same bank for deposit. However, making many small purchases in seconds is possible with e-cash unlike physical cash. Hence large exchanges of funds could potentially be hidden. An interesting overview of these issues is available in [Fro96b]. It should also be noted that recently the National Security Agency has stated that escrowing of e-cash is vital for the United States' national interest. Fingerprints may be on the notes, or serial numbers and locality of purchase may reveal the user to some degree [Fro96b]. Electronic cash has the potential for providing added anonymity. On the other hand, electronic cash purchases performed over digital networks require anonymous re-routers to provide a strong level of anonymity. There are two issues in providing anonymity in e-cash: 1) The strength of the anonymity protection mechanism and 2) likability amongst different coins of a single user. The cryptographic strength of anonymity pertains to what cryptographic assumptions are made to guarantee user anonymity, whereas likability of coins is related to whether coins from an account are linkable to each other but not directly to the account.

**UNTRACEABILITY:**

Anonymity and Untraceability are often used as synonyms. We prefer to make a difference between these terms, grasping in this way different levels of protection. Each customer is characterized by an identifier (e.g. name, account number, social security number). A customer is said to be anonymous if his or her identifier cannot be linked to the sent messages. However, it may be feasible to link the different messages transmitted by the same customer. An anonymous customer is said to be untraceable if no message can be linked not only to the customer's identifier, but also to any previously sent messages; so untraceability is stronger than anonymity. A system providing either anonymity or untraceability is said to protect privacy.

 **VIRTUAL CURRENCY:**

A virtual currency is a digital representation of value only available in electronic form. It is stored and transacted through designated software, mobile, or computer applications. Transactions involving virtual currencies occur through secure, dedicated networks or over the Internet. They are issued by private parties or groups of developers and are mostly unregulated.

Virtual currencies are a subset of digital currencies and include other types of [digital currencies](https://www.investopedia.com/terms/d/digital-money.asp), such as [cryptocurrencies](https://www.investopedia.com/terms/c/cryptocurrency.asp) and tokens issued by private organizations. The advantages of virtual currencies include faster transaction speeds and ease of use. The disadvantages of virtual currencies are that they can be hacked and do not provide much legal recourse to investors because they are not regulated. Virtual currencies are a form of digital currency. They are issued by private parties, such as a group of developers or organizations, and are intended only for online use—they do not have a physical incarnation like paper money. Thus, they are different from digital representations of central bank-issued currency, also known as [central bank digital currency (CBDC)](https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp).

The term virtual currency came into existence in 2012, when the [European Central Bank (ECB)](https://www.investopedia.com/terms/e/europeancentralbank.asp) defined it to classify types of "digital money in an unregulated environment, issued and controlled by its developers and used as a payment method among members of a specific virtual community." The [Internal Revenue Service (IRS)](https://www.investopedia.com/terms/i/irs.asp) in the United States describes virtual currencies as "digital representations of value that function as a unit of account, a store of value, and a medium of exchange.

Virtual currencies have also failed to take off as a payment method or medium of exchange in mainstream society. They have restricted usage, sometimes in gaming communities and other times as a speculative investment asset. Whether they have emerged as a store of value, like gold, also remains questionable.There's also the question about regulation. Though virtual currencies remain unregulated in the vast majority of financial jurisdictions, that situation is slowly beginning to change. [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp), the cryptocurrency with the biggest market capitalization, [is legal tender](https://www.investopedia.com/el-salvador-accepts-bitcoin-as-legal-tender-5200470) in El Salvador.

In the United States, home to the world’s most sophisticated financial markets, virtual currencies are unregulated. But regulation is seriously being considered by authorities. The trading watchdog [Securities and Exchange Commission (SEC)](https://www.investopedia.com/terms/s/sec.asp) wants to [bring cryptocurrency](https://www.investopedia.com/sec-chief-reiterates-call-for-cryptocurrency-regulation-5201311) exchanges under its supervision. Regulation for [stablecoins](https://www.investopedia.com/terms/s/stablecoin.asp), another form of virtual currency, is also in the cards. The IRS taxes trades that involve certain types of virtual currencies, such as cryptocurrencies.

**BITCOIN:**

Bitcoin is a cryptocurrency for online payments between two parties in a decentralized manner and without an intermediary. Bitcoin uses peer-to-peer technology and exhibits characteristics of money but it is unlike conventional cash. For example, just like cash, it is a bearer instrument, meaning the person who has keys to an online wallet containing Bitcoin, owns the coins. It is also fungible. This means that one Bitcoin is equivalent in value to another Bitcoin, making it possible to use them for trading. But transactions that utilize Bitcoin are not anonymous. Publicly-available [ledgers](https://learn.financestrategists.com/finance-terms/ledger-definition/) on blockchain, Bitcoin’s underlying technology, ensure that anyone can see the transfers and withdrawals taking place in the cryptocurrency’s network. In contrast, cash-based transactions are anonymous. A rapid appreciation in price and limited availability has converted Bitcoin into a store of value for investors. In this role, it acts in a fashion similar to gold. Bitcoin is one of the most well-known virtual currencies today, with its value rising dramatically since its launch in 2009. Satoshi Nakamoto, the pseudonym of Bitcoin's creator, stated the purpose of Bitcoin is as an electronic payment system that is based on [cryptographic](https://www.techtarget.com/searchsecurity/definition/cryptography) proof, instead of trust. Some holders buy bitcoin as an investment, wanting it to increase in value, while individuals and businesses use or accept payments as currency. PayPal, for example, currently supports Bitcoin transactions, and the country of El Salvador has accepted Bitcoin as a currency.Bitcoin-to-bitcoin transactions are made by digitally exchanging anonymous, heavily encrypted hash codes across a peer-to-peer ([P2P](https://www.techtarget.com/searchnetworking/definition/peer-to-peer)) network. The P2P network monitors and verifies the transfer of bitcoin between users. Each user's bitcoin are stored in a program called a [digital wallet](https://www.techtarget.com/whatis/definition/digital-wallet), which also holds each address the user sends and receives bitcoin from, as well as a private key known only to the user.

**UNIT-2**

Automated clearing and settlement: process of real time gross settlement system - Network settlement – ATM Network – Fed wire, CHIP and SWIFT

**Automated clearing and settlement:**

The Automated Clearing House (ACH) is an electronic funds-transfer system run by Nacha. The Automated Clearing House traces its roots back to the late 1960s but was officially established in the mid-1970s. The payment system provides many types of ACH [transactions](https://www.investopedia.com/terms/t/transaction.asp), such as payroll deposits. It requires a debit or credit from the originator and a credit or debit on the recipient's end.

## How the Automated Clearing House (ACH) Works:

The ACH Network is an electronic system that serves [financial institutions](https://www.investopedia.com/terms/f/financialinstitution.asp) to facilitate financial transactions in the U.S. It represents more than 10,000 financial institutions and ACH transactions totaled more than $72.6 trillion in 2021 by enabling over 29 billion electronic financial transactions. The network essentially acts as a financial hub and helps people and organizations move money from one bank account to another. ACH transactions consist of [deposits](https://www.investopedia.com/terms/d/deposit.asp) and payments, including:

* [Business-to-business](https://www.investopedia.com/terms/b/btob.asp) (B2B) transactions
* Government transactions
* Consumer transactions

Here's how the system works. An originator starts a [direct deposit](https://www.investopedia.com/terms/d/directdeposit.asp) or direct payment transaction using the ACH network via debit and credit. The originator's bank, also known as the originating depository financial institution, takes the ACH transaction and batches it together with other ACH transactions to be sent out at regular times throughout the day.

An ACH operator, either the [Federal Reserve](https://www.investopedia.com/terms/f/federalreservebank.asp) or a [clearinghouse](https://www.investopedia.com/terms/c/clearinghouse.asp), receives the batch of ACH transactions from the originating institution with the originator's transaction. The ACH operator sorts the batch and makes transactions available to the bank or financial institution of the intended recipient, also known as the receiving depository financial institution. The recipient's bank account receives the transaction, thus reconciling both accounts and ending the process.

### Automated Clearing Settlement System

The Automated Clearing Settlement System (ACSS) clears cheques and electronic items, such as pre-authorized debits, direct deposits and Interac debit payments. The system provides for the exchange of payment items between members of Payments Canada who participate in the ACSS and the subsequent clearing and settlement of those payment items.ACSS is owned and operated by Payments Canada.

**Real time gross system:**

The acronym 'RTGS' stands for Real Time Gross Settlement, which can be explained as a system where there is continuous and real-time settlement of fund-transfers, individually on a transaction by transaction basis (without netting). 'Real Time' means the processing of instructions at the time they are received; 'Gross Settlement' means that the settlement of funds transfer instructions occurs individually.

When you hear the term real-time, it means the settlement happens as soon as it is received. So, in simpler terms, the transaction settles in the receiving [bank](https://www.investopedia.com/terms/b/bank.asp) immediately after it is transferred from the sending bank. Gross settlement means transactions are handled and settled individually, so multiple [transactions](https://www.investopedia.com/terms/t/transaction.asp) aren't bunched or grouped together. This is the basis of a real-time gross settlement system.

An RTGS system is generally used for large-value interbank funds transfers operated and organized by a country’s [central bank](https://www.investopedia.com/terms/c/centralbank.asp). These transfers often require immediate and complete clearing. As mentioned above, once transactions are settled, they cannot be reversed.

In 1970, the U.S. Fedwire system launched. It was the first system resembling a real-time gross settlement system. It was an evolution of the telegraph-based system used to transfer funds electronically between U.S. Federal Reserve banks.The British system, called the Clearing House Automated Payment System (CHAPS), is currently run by the [Bank of England](https://www.investopedia.com/terms/b/boe.asp). France and other [Eurozone](https://www.investopedia.com/terms/e/eurozone.asp) nations use a system called Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2). Other developed and developing countries have also introduced their own RTGS-type systems.

**Benefits:**

RTGS offers many advantages over the other modes of funds transfer:

* It is a safe and secure system for funds transfer.
* RTGS transactions / transfers have no amount cap.
* The system is available on all days on 24x7x365 basis. There is real time transfer of funds to the beneficiary account.
* The remitter need not use a physical cheque or a demand draft.
* The beneficiary need not visit a bank branch for depositing the paper instruments.
* The beneficiary need not be apprehensive about loss / theft of physical instruments or the likelihood of fraudulent encashment thereof.
* Remitter can initiate the remittances from his / her home / place of work using internet banking, if his / her bank offers such service.
* The transaction charges have been capped by RBI.
* The transaction has legal backing.

**Net settlement system:**

Net settlement is a bank's routine resolution of the day's transactions at the end of the business day. Since many or most bank transactions are now sent electronically, this is no longer a matter of counting the cash in the drawer. Instead, the bank has to add up all of their electronic credits and debits.The bank then sends its settlement file to a Federal Reserve Bank, which credits it with any funds that are due to be paid to it via the interbank settlement system.

**Understanding Net Settlement**

The net settlement system permits banks to accumulate credits and debits with each other throughout the business day. Only at the end of the business day are the totals calculated and only the net differential needs to be transferred between the banks.

A bank's net settlement is similar to balancing individual’s checkbook. The balancing process gets complicated if you have money coming in as cash, checks, and direct deposits, and money going out as cash purchases, checks, and credit card purchases. All of those transactions, including purchases, returns, bills paid, and paychecks received, must be netted to get the full picture.

Net settlement makes it easier for banks to manage their [liquidity](https://www.investopedia.com/terms/l/liquidity.asp). That is, they need to know that they have enough real cash on hand to pay out to their customers over the counter and at the ATMs. There are two types of net settlement systems:

* Bilateral settlement systems require the final resolution of payments made between two banks over the course of a day. These are due to be settled at the close of business, typically via a transfer between their accounts at the central bank.
* Multilateral settlement systems allow a bank to have a net balance with the system as a whole, rather than with an individual bank or banks.

**Asynchronous Transfer Mode (ATM):**

Wide-area network (WAN) technology, **asynchronous transfer mode (ATM)** is a transfer mode for switching and transmission that efficiently and flexibly organizes information into cells; it is asynchronous in the sense that the recurrence of cells depends on the required or instantaneous bit rate. Thus, empty cells do not go by when data is waiting. ATM’s powerful flexibility lies in its ability to provide a high-capacity, low-latency switching fabric for all types of information, including data, video, image and voice, that is protocol-, speed- and distance-independent. ATM supports fixed-length cells 53 bytes in length and virtual data circuits between 45 megabits per second (Mbps) and 622 Mbps. Using statistical multiplexing, cells from many different sources are multiplexed onto a single physical circuit. The fixed-length fields in the cell, which include routing information used by the network, ensure that faster processing speeds are enabled using simple hardware circuits. The greatest benefit of ATM is its ability to provide support for a wide range of communications services while providing transport independence from those services.

**Why ATM networks?**

1. Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).
2. Telephone networks support a single quality of service and are expensive to boot.
3. Internet supports no quality of service but is flexible and cheap.
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

**Working of ATM:**

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

**Fedwire:**

Fedwire refers to a real-time gross settlement system of [central bank](https://www.investopedia.com/terms/c/centralbank.asp) money used by Federal Reserve (Fed) banks to electronically settle final U.S. dollar payments among member institutions. The system processes trillions of dollars daily and includes an overdraft system that covers participants with existing and approved accounts.

Along with Fedwire, the [Fed](https://www.investopedia.com/terms/f/federalreservebank.asp) operates two other payment systems: The Fedwire Securities Service and the National Settlement Service.

## Understanding Fedwire:

The Fedwire system is an electronic funds transfer system used by banks, businesses, and government agencies for large, same-day transactions. Banks that use the system include depository [financial institutions](https://www.investopedia.com/terms/f/financialinstitution.asp) (FI) in the U.S., as well as the American branches of certain foreign banks or government groups, provided they maintain an account with a Fed Bank.

The Fed holds accounts for both senders and receivers and settles transactions individually and immediately. Once settled, all transactions are final and irrevocable, and the receiving bank is notified of the [credit](https://www.investopedia.com/terms/c/credit.asp).

Although Fedwire is not managed for profit, the law mandates that the system charge fees in order to recoup costs; thus, both participants in a given transaction pay a small fee. Participating institutions can initiate fund transfers online or on the phone. They can send money from their accounts for themselves or on behalf of their clients to settle commercial payments or positions with other institutions, remit tax payments, and buy and sell federal funds.

The Fedwire system is owned and operated by the 12 Fed Banks. It is a networked system for payment processing between the member banks themselves, as well as other participating institutions. Fedwire operates Monday through Friday between 9 p.m. Eastern Time (ET) on the prior calendar day to 7 p.m. ET. The Fed may extend its hours, and the system is closed on all federal holidays.

**Clearing House Interbank Payments System (CHIPS):**

The Clearing House Interbank Payments System (CHIPS) is the primary [clearing house](https://www.investopedia.com/terms/c/clearinghouse.asp) in the U.S. for large banking transactions. As of 2015, CHIPS settles over 250,000 of trades per day, valued in excess of $1.5 trillion in both domestic and cross-border transactions. CHIPS and the [Fedwire](https://www.investopedia.com/terms/f/fedwire.asp) funds service used by the Federal Reserve Bank combine to constitute the primary network in the U.S. for both domestic and foreign large transactions denominated in U.S. dollars.

The Clearing House Interbank Payments System differs from the Fedwire transaction service in several respects. First and foremost, it is cheaper than the Fedwire service, albeit not as fast, and the dollar amounts required to use this service are lower. CHIPS is the main clearing house for large transactions; the average transaction that uses CHIPS is over $3,000,000.

CHIPS acts as a [netting](https://www.investopedia.com/terms/n/netting.asp) engine, where payments between parties are netted against each other instead of the full dollar value of both trades being sent. From 9 p.m. to 5 p.m. ET. banks send and receive payments. During that time, CHIPS nets and releases payments. From 5 p.m. until 5:15 p.m. the CHIPS system eliminates credit limits, and releases and nets unresolved payments. By 5:15 p.m., CHIPS releases any remaining payments and sends payment orders to banks via Fedwire.

## How The Clearing House Interbank Payments System Works

There are two steps to processing funds transfers: clearing and settlement. [Clearing](https://www.investopedia.com/terms/c/clearing.asp) is the transfer and confirmation of information between the payer (sending financial institution) and payee (receiving financial institution). [Settlement](https://www.investopedia.com/terms/s/settlement_period.asp) is the actual transfer of funds between the payer's financial institution and the payee's financial institution. Settlement discharges the obligation of the payer financial institution to the payee financial institution with respect to the payment order. Final settlement is irrevocable and unconditional. The finality of the payment is determined by that system's rules and applicable law.

general, payment messages may be credit transfers or debit transfers. Most large-value funds transfer systems are credit transfer systems in which both payment messages and funds move from the payer financial institution to the payee financial institution. An institution transmits a payment order (a message that requests the transfer of funds to the payee) to initiate a funds transfer. Typically, large-value payment system operating procedures include identification, reconciliation, and confirmation procedures necessary to process the payment orders. In some systems, financial institutions may contract with one or more third parties to help perform clearing and settlement activities.

The legal framework for institutions offering payment services is complex. There are rules for large-value payments that are distinct from retail payments. Large-value funds transfer systems differ from retail electronic funds transfer (EFT) systems, which generally handle a large volume of low-value payments including [automated clearing house](https://www.investopedia.com/terms/a/ach.asp) (ACH) and debit and credit card transactions at the point of sale.

**SWIFT Banking System:**

Need to transfer money overseas? Today, it is easy to walk into a bank and transfer money anywhere around the globe, but how does this happen? Behind most international money and security transfers is the [Society for Worldwide Interbank Financial Telecommunications (SWIFT)](https://www.investopedia.com/terms/s/swift.asp) system. SWIFT is a vast messaging network banks and other [financial institutions](https://www.investopedia.com/terms/f/financialinstitution.asp) use to quickly, accurately, and securely send and receive information, such as money transfer instructions.

More than 11,000 global SWIFT member institutions sent an average of 42 million messages per day through the network in 2021, marking an increase of 11.4% over 2020.

SWIFT is a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes. Although SWIFT has become a crucial part of global financial infrastructure, it is not a financial institution itself: SWIFT does not hold or transfer assets. Rather, its utility lies in its power to facilitate secure, efficient communication between member institutions.

SWIFT assigns each financial organization a unique code that has either eight characters or 11 characters, known as a bank identifier code, or BIC. The BIC may also go by the terms SWIFT code, SWIFT ID, or ISO 9362 code. To understand how the code is assigned, let’s look at the Italian bank UniCredit Banca, headquartered in Milan. It has the eight-character SWIFT code UNCRITMM.

**UNIT-3**

**E-PAYMENT SECURITY AND DIGITAL SIGNATURE**

**What is an electronic payment?**

Electronic payments allow customers to pay for products or services electronically. Electronic payments are what allow you to purchase clothes via your favorite online store or pay your cable bill online. So if you’re planning to [create an online store](https://squareup.com/townsquare/how-to-start-an-online-store), you need to have an eCommerce payment system and learn exactly how it works.

Even if you’re not planning to invest in [eCommerce](https://squareup.com/us/en/ecommerce), it’s important to understand how electronic payments work (as a customer) and the role they play in the evolution of the [payment processing](https://squareup.com/us/en/hardware/reader) ecosystem.

Twenty-four percent of Americans make no purchases with cash during the week, according to the [Pew Research Center](http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/). And the [Wall Street Journal](https://www.wsj.com/articles/why-your-business-should-ditch-cash-1485698400) said that in 2016, credit cards eclipsed cash in transactions worldwide for the first time. We know that online shopping is on the rise — 8 in 10 Americans are online shoppers (according to Pew). What we’re seeing in this evolution is that consumers are gravitating toward the payment and shipping methods that offer more convenience and flexibility.

**How do electronic payment systems work?**

Understanding how an electronic payment works can get technical since there are a lot of moving parts. Here’s a breakdown of the main participants required for an electronic payment transaction:

* The **cardholder** is identified as the consumer who purchases a product or service online.
* The **merchant** is the person or business that sells goods and services to the cardholder.
* The **issuer** is the financial institution that provides the cardholder with the payment card. This is usually the cardholder’s bank.
* The **acquirer**, or [merchant account provider](https://squareup.com/payments/merchant-services#basics), is the financial institution that establishes an account with the merchant. The acquirer authorizes the legitimacy of the cardholder account.
* The **payments processor** handles the official transaction between the cardholder and merchant.
* The [**payment gateway**](https://squareup.com/us/en/townsquare/how-to-start-a-business) processes merchant payment messages and uses security protocols and encryptions to ensure transaction safety.

Electronic payment transactions are divided into two types: one-time vendor payments and recurring customer vendor payments.

* **One-time vendor payments** are commonly used on eCommerce websites. A cardholder types in the card or banking information on a checkout page and simply clicks to purchase.
* **Recurring customer vendor payments** are used when the cardholder is paying for a product or service regularly. Customers enter their information once and then opt in for a recurring billing option with a set date for the payment to go through. This is often used by car insurance agencies, phone companies, loan management companies, and other [types of businesses](https://squareup.com/gb/en/solutions).

## Electronic payment methods

All transactions require a method of payment. With traditional payment processing systems, a customer can use cash, checks, [magstripe cards](https://squareup.com/us/en/hardware/reader), [EMV](https://squareup.com/us/en/townsquare/emv) chip cards, or [mobile payment](https://squareup.com/us/en/townsquare/how-to-start-a-business) options.

Electronic payment methods differ slightly. E-payments are orchestrated by an electronic funds transfer (EFT), which is the process of transferring money from one bank account to another without any exchange by hand. Online payment methods that use EFT include:

* **Credit and debit cards.** Businesses must have [eCommerce software](https://squareup.com/us/en/ecommerce) to accept payments online. A customer enters the debit or credit card information in a [virtual terminal](https://squareup.com/us/en/payments/virtual-terminal) or [online invoice](https://squareup.com/us/en/invoices) when a product or service is purchased.
* **eChecks.** Instead of inputting card information, a customer can use an electronic check to pay online by entering the checking account and routing numbers from the bank.

## Are electronic payments secure?

Credit card security is a top priority for any business, especially if you have an online store or use the internet to complete transactions in any way. But don’t worry, there are a number of security standards and protocols in place to ensure the security of online transactions.

He’s how you can abide by industry standards and keep sensitive data secure.

### Learn about the Secure Electronic Transaction system.

The Secure Electronic Transaction system ([SET](http://www.investopedia.com/terms/s/secure-electronic-transaction-set.asp)) is a set of security protocols used to facilitate electronic payments. With SET, a few components are integrated to authenticate and ensure confidentiality: digital wallet software, merchant software, and [payment gateway](https://squareup.com/us/en/townsquare/how-to-start-a-business) server software.

**Why do electronic payments benefit your eCommerce business?**

Now you understand how electronic payment systems work. How do they work for your business?

### Reach a new audience:

eCommerce opens up your target market substantially. Because you don’t have geographic or time limits, customers can access your website and purchase products from anywhere and at any time.

### Improve purchasing efficiency:

Customers don’t have to wait in line to buy products or services when using an electronic payment system. This kind of purchasing efficiency can actually encourage consumers to buy from your business more often.

**Increase payment security:**

There are a plethora of security measures and protocols in place to ensure your online transactions are safe and secure.

**DIGITAL SIGNATURE:**

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.In many countries, including the United States, digital signatures are [considered legally binding](https://www.techtarget.com/searchcontentmanagement/answer/Are-electronic-signatures-legally-binding) in the same way as traditional handwritten document signatures.

### How do digital signatures work?

Digital signatures are based on [public key](https://www.techtarget.com/searchsecurity/definition/public-key) cryptography, also known as [asymmetric cryptography](https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography). Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.Digital signatures work through public key cryptography's two [mutually authenticating cryptographic keys](https://www.techtarget.com/searchsecurity/answer/Which-private-keys-and-public-keys-can-create-a-digital-signature). The individual who creates the digital signature uses a [private key](https://www.techtarget.com/searchsecurity/definition/private-key) to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

### What are the benefits of digital signatures?

Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. Security features and methods used in digital signatures include the following:

* **Personal identification numbers (PINs), passwords and codes.** Used to authenticate and verify a signer's identity and approve their signature. Email, username and password are the most common methods used.
* **Asymmetric cryptography.** Employs a public key [algorithm](https://www.techtarget.com/whatis/definition/algorithm) that includes private and public key encryption and [authentication](https://www.techtarget.com/searchsecurity/definition/authentication).
* [**Checksum**](https://www.techtarget.com/searchsecurity/definition/checksum)**.** A long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. A checksum acts as a data fingerprint.
* **Cyclic redundancy check (**[**CRC**](https://www.techtarget.com/searchnetworking/definition/cyclic-redundancy-checking)**).** An error-detecting code and verification feature used in digital networks and storage devices to detect changes to raw data.
* **Certificate authority (**[**CA**](https://www.techtarget.com/searchsecurity/definition/certificate-authority)**) validation.** CAs issue digital signatures and act as trusted third parties by accepting, authenticating, issuing and maintaining [digital certificates](https://www.techtarget.com/searchsecurity/definition/digital-certificate). The use of CAs helps avoid the creation of fake digital certificates.
* **Trust service provider (TSP) validation.** A TSP is a person or legal entity that performs validation of a digital signature on a company's behalf and offers signature validation reports.

Other benefits to using digital signatures include the following:

* **Timestamping.** By providing the data and time of a digital signature, timestamping is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings.
* **Globally accepted and legally compliant.** The public key infrastructure ([PKI](https://www.techtarget.com/searchsecurity/definition/PKI)) standard ensures vendor-generated keys are made and stored securely. Because of the international standard, a growing number of countries are accepting digital signatures as legally binding.
* **Time savings.** Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.
* **Cost savings.** Organizations can go paperless and save money previously spent on the physical resources and on the time, personnel and office space used to manage and transport them.
* **Positive environmental impact.** Reducing paper use also cuts down on the physical waste generated by paper and the negative environmental impact of transporting paper documents.
* **Traceability.** Digital signatures create an audit trail that makes internal record-keeping easier for business. With everything recorded and stored digitally, there are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something.

**CRYPTOGRAPHIC METHODS:**

Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary. Based on the security needs and the threats involved, various cryptographic methods such as **symmetric key cryptography or public key cryptography** can be used during transportation and storage of the data.

There are two types of encryptions in widespread use today: **symmetric** and **asymmetric** encryption. The name derives from whether or not the same key is used for encryption and decryption.

### What is symmetric encryption?

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.



Figure 2: Symmetric encryption – Using the same key for encryption and decryption

### What is asymmetric encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.
Data encrypted with the recipient’s public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.



Figure 3: Asymmetric encryption – Using a different key for the encryption and decryption process.

**HASH FUNCTION:**

Hashing is the process of generating a value from a text or a list of numbers using a mathematical function known as a [hash function](https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/).

A **Hash Function**is a function that converts a given numeric or alphanumeric key to a small practical integer value. The mapped integer value is used as an index in the hash table. In simple terms, a hash function **maps** a significant number or string to a small integer that can be used as the **index** in the hash table.

The pair is of the form **(key, value)**, where for a given key, one can find a value using some kind of a “function” that maps keys to values. The key for a given object can be calculated using a function called a hash function. For example, given an array A, if i is the key, then we can find the value by simply looking up A[i].

**Types of Hash functions:**

There are many hash functions that use numeric or alphanumeric keys. This article focuses on discussing different hash functions:

1. **Division Method.**
2. **Mid Square Method.**
3. **Folding Method.**
4. **Multiplication Method.**

Let’s begin discussing these methods in detail.

**1. Division Method:**

This is the most simple and easiest method to generate a hash value. The hash function divides the value k by M and then uses the remainder obtained.

**Formula:**

***h(K) = k mod M***

*Here,****k****is the key value, and****M****is the size of the hash table.*

It is best suited that **M**is a prime number as that can make sure the keys are more uniformly distributed. The hash function is dependent upon the remainder of a division.

**Example:**

*k = 12345
M = 95
h(12345) = 12345 mod 95
               = 90*

*k = 1276
M = 11
h(1276) = 1276 mod 11
             = 0*

**Pros:**

1. This method is quite good for any value of M.
2. The division method is very fast since it requires only a single division operation.

**Cons:**

1. This method leads to poor performance since consecutive keys map to consecutive hash values in the hash table.
2. Sometimes extra care should be taken to choose the value of M.

**2. Mid Square Method:**

The mid-square method is a very good hashing method. It involves two steps to compute the hash value-

1. Square the value of the key k i.e. k2
2. Extract the middle **r** digits as the hash value.

**Formula:**

***h(K) = h(k x k)***

*Here,****k****is the key value.*

The value of **r**can be decided based on the size of the table.

**Example:**

Suppose the hash table has 100 memory locations. So r = 2 because two digits are required to map the key to the memory location.

*k = 60
k x k = 60 x 60
        = 3600
h(60) = 60*

*The hash value obtained is 60*

**Pros:**

1. The performance of this method is good as most or all digits of the key value contribute to the result. This is because all digits in the key contribute to generating the middle digits of the squared result.
2. The result is not dominated by the distribution of the top digit or bottom digit of the original key value.

**Cons:**

1. The size of the key is one of the limitations of this method, as the key is of big size then its square will double the number of digits.
2. Another disadvantage is that there will be collisions but we can try to reduce collisions.

**3. Digit Folding Method:**

This method involves two steps:

1. Divide the key-value **k**into a number of parts i.e. **k1, k2, k3,….,kn**, where each part has the same number of digits except for the last part that can have lesser digits than the other parts.
2. Add the individual parts. The hash value is obtained by ignoring the last carry if any.

**Formula:**

***k = k1, k2, k3, k4, ….., kn******s = k1+ k2 + k3 + k4 +….+ kn******h(K)= s***

*Here,****s****is obtained by adding the parts of the key****k***

**Example:**

*k = 12345
k1 = 12, k2 = 34, k3 = 5
s = k1 + k2 + k3
  = 12 + 34 + 5
  = 51
h(K) = 51*

**Note:**
The number of digits in each part varies depending upon the size of the hash table. Suppose for example the size of the hash table is 100, then each part must have two digits except for the last part which can have a lesser number of digits.

**4. Multiplication Method**

This method involves the following steps:

1. Choose a constant value A such that 0 < A < 1.
2. Multiply the key value with A.
3. Extract the fractional part of kA.
4. Multiply the result of the above step by the size of the hash table i.e. M.
5. The resulting hash value is obtained by taking the floor of the result obtained in step 4.

**Formula:**

***h(K) = floor (M (kA mod 1))***

*Here,****M****is the size of the hash table.****k****is the key value.****A****is a constant value.*

**Example:**

*k = 12345
A = 0.357840
M = 100*

*h(12345) = floor[ 100 (12345\*0.357840 mod 1)]
               = floor[ 100 (4417.5348 mod 1) ]
               = floor[ 100 (0.5348) ]
               = floor[ 53.48 ]
               = 53*

**Pros:**

The advantage of the multiplication method is that it can work with any value between 0 and 1, although there are some values that tend to give better results than the rest.

**Cons:**

The multiplication method is generally suitable when the table size is the power of two, then the whole process of computing the index by the key using multiplication hashing is very fast.

## PUBLIC KEY CRYPTOGRAPHY:

**Public-key cryptography**, or **asymmetric cryptography**, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a **public key** and a corresponding **private key**. Key pairs are generated with [cryptographic](https://en.wikipedia.org/wiki/Cryptographic) [algorithms](https://en.wikipedia.org/wiki/Algorithms) based on [mathematical](https://en.wikipedia.org/wiki/Mathematical) problems termed [one-way functions](https://en.wikipedia.org/wiki/One-way_function). Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.

In a **public-key encryption** system, anyone with a public key can [encrypt](https://en.wikipedia.org/wiki/Encryption) a message, yielding a **ciphertext**, but only those who know the corresponding private key can decrypt the ciphertext to obtain the original message.

For example, a journalist can publish the public key of an encryption key pair on a web site so that sources can send secret messages to the news organization in ciphertext. Only the journalist who knows the corresponding private key can decrypt the ciphertexts to obtain the sources' messages—an eavesdropper reading email on its way to the journalist cannot decrypt the ciphertexts. However, public-key encryption does not conceal [metadata](https://en.wikipedia.org/wiki/Metadata) like what computer a source used to send a message, when they sent it, or how long it is. Public-key encryption on its own also does not tell the recipient anything about who sent a message—it just conceals the content of a message in a ciphertext that can only be decrypted with the private key.

In a [**digital signature**](https://en.wikipedia.org/wiki/Digital_signature) system, a sender can use a private key together with a message to create a **signature**. Anyone with the corresponding public key can verify whether the signature matches the message, but a forger who does not know the private key cannot find any message/signature pair that will pass verification with the public key.

## PRIVATE KEY CRYPTOGRAPHY:

A private key, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt data. Secret keys should only be shared with the key's generator or parties authorized to decrypt the data. Private keys play an important role in symmetric cryptography, asymmetric cryptography and [cryptocurrencies](https://www.techtarget.com/whatis/definition/cryptocurrency).

A private key is typically a long, randomly or pseudo-randomly generated sequence of bits that cannot be easily guessed. The complexity and length of the private key determine how easily an attacker can execute a [brute-force attack](https://www.techtarget.com/searchsecurity/definition/brute-force-cracking), where they try out different keys until the right one is found.

## Understanding Private Keys

Cryptocurrency is controlled through a set of digital keys and addresses, representing ownership and control of virtual tokens. Anyone can deposit bitcoin or other tokens in any public address. But even though a user has tokens deposited into their address, they won’t be able to withdraw them without the unique private key.

## Private keys can take a few different forms. In ordinary, base-ten notation, a private key would be hundreds of digits long–so long that it would take years to crack a private key by brute force. For simplicity, private keys are usually expressed as a string of alphanumeric characters.

The [public key](https://www.investopedia.com/terms/p/public-key.asp) is created from the private key through a complicated mathematical algorithm. However, it is near impossible to reverse the process by generating a private key from a public key.A similar algorithm is then used to create a receiving address from the public key. Think of the address as a mailbox, and the private key as the key to the box.1

The mail carrier, and anyone really, can insert letters and small packages through the opening in the mailbox. However, the only person that can retrieve the contents of the mailbox is the one who has the unique key. It is, therefore, important to keep the key safe because if it is stolen or lost, the mailbox can be compromised.

# RSA Algorithm in Cryptography:

The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- **a suite of cryptographic algorithms that are used for specific security services or purposes** -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network.

**RSA algorithm** is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

**An example of asymmetric cryptography:**

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client’s public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

**The idea!** The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

**Digital Signature**

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

1. **Key Generation Algorithms**: Digital signature is electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

**The steps followed in creating digital signature are :**

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender’s public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.

**Digital Certificate**

Digital certificate is issued by a trusted third party which proves sender’s identity to the receiver and receiver’s identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant’s public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.
**Digital certificate contains: -**

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder’s public key. (Used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

**Digital certificate vs digital signature:**
Digital signature is used to verify authenticity, integrity, non-repudiation, i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users

## What is Digital Identity Verification?

Digital identity verification is a remote ID verification process that’s designed for today’s customers. The global pandemic massively boosted the need for identity verification services since many businesses moved to the digital sphere. With such a shift came increased numbers of cyberattacks. For this reason, responsible businesses started to look for new and improved digital fraud prevention solutions, such as remote identity verification.

Modern [identity verification](https://www.idenfy.com/) implementations combine artificial intelligence and smart, automated technological services into one smooth customer onboarding process. Digital identity verification uses face recognition, biometric verification, and quick document scanning algorithms to help other businesses or government agencies battle fraud. ID verification ensures that the customer’s identity document isn’t forged and that it meets all of the security requirements.

Digital identity verification services are in high demand due to the convenience that they bring. By reviewing the customer’s identity, financial institutions are able to welcome trusted and safe clients. Scammers and fraudsters who use fake identities or tamper with documents aren’t verified during the ID verification process. Spoofing, [deepfakes](https://en.wikipedia.org/wiki/Deepfake), and scammers that wear masks during the identity verification process – are all techniques that are used by online criminals with fraudulent intentions.

**What are the Benefits of Identity Verification?**

When it comes to digital identity verification, part of its widespread success comes from the convenience factor. The fact that this process eliminates the need for customers to be physically present during the procedure also fits for newly emerged e-commerce players or, for instance, the cryptocurrency industry. Even though there’s no universal “one-size-fits-all” ID verification for all businesses, it’s clear that simple and secure ID verification solutions for businesses are crucial.

Digital identity verification solutions bring customers and businesses closer by providing universal access to various services remotely. On top of easy-to-use functionality, identity verification helps avoid data falling into fraudsters’ hands. The main benefits of remote ID verification for businesses are:

* ID verification helps detect and fight fraud more efficiently.
* Digital verification services eliminate the need for physical presence.
* This process enhances customers’ trust and protects the business’ reputation.

Today’s innovative technology pushes boundaries, making it easier for businesses to adapt and use digital identity verification. In general, ID verification can also be used to speed up traditional processes. For example, [identity](https://identitymanagementinstitute.org/what-is-reusable-identity/) verification can be used in airports to scan passports at electronic gates. As more industries adopt digital identity verification, the corporate and political world is also encouraging the masses to follow the digitization process by pushing digital identity schemes. This way, remote ID verification slowly became the new normal.

**How Does ID Verification Improve Your Business?**

If you want to secure your business and play a significant role in the digitization process, you’ll need to choose a responsible digital identity verification provider. It’s a necessary procedure that improves and automates internal processes, minimizes human error, and reduces operational costs. Not to mention, ID verification protects your clients’ data and prevents fake identities as well as money laundering.

To sum it up, remote identity verification improves your business by:

* Reducing costs.
* Improving customer experience.
* Ensuring data security
* Maintaining high fraud prevention standards.
* Adapting to regulations.

That said, remote ID verification improves your business reputation by maintaining regulatory compliance and taking a responsible approach toward [cybersecurity](https://identitymanagementinstitute.org/cyber-and-data-security-considerations-for-remote-workers/). In other words, identity verification guarantees that the person behind the screen is legitimate and has good intentions. Looking from a business perspective, ID verification provides a competitive advantage.

**digital identity documentation:**

A digital identity is an electronic way of identifying someone. It consists of **a certificate containing a “public key”, which is viewable, and a “private key”, which is kept secret**. Your private key lets you sign an electronic document with a signature that others can verify using only your public key.

## How Does the Digital Identity Verification Process Work?

Digital identity verification works by comparing a readily available proof of identity proof (e.g., a facial biometric or an ID document) to a confirmed data set (e.g., government-issued credential, such as a passport, or a biometric stored on a user’s registered mobile phone). The purpose is to verify that a person is who they say they are.

A variety of identity verification methods help verify a person’s identity, and each works in a distinct manner. Let’s take a look at each of these methods:

### 1. ID Document Verification:

Verifies the legitimacy of an ID document (such as a driver’s license, passport, or government ID)

### 2. Biometric Verification:

Selfies are used in biometric verification to ensure that the person presenting the ID is the same person whose portrait appears on the ID

### 3. Liveness Detection:

Detects spoofing attacks such as face masks or doctored images to determine whether a selfie is genuine

### 4. Knowledge-Based Authentication (KBA):

A type of authentication that relies on the user’s knowledge, such as from the applicant’s credit file to generate “out of wallet” questions

### 5. OTP Verification:

During the verification procedure, the applicant receives a one-time passcode through SMS or email

### 6. Database Methods:

Uses information from social media, offline databases, and other sources to verify the applicant’s information.

**Digital Identity Use Cases**

Due to the advanced methods used by fraudsters for nefarious actions, not a single industry is secure these days. Every industry needs digital identity verification checks, but the ones that require it the most are:

### 1. Online Gaming

Given the significant increase in e-gaming market revenue, this sector is more prone to criminal activities. Malicious users can be kept at bay with identity verification services. They can save gaming companies a lot of money by avoiding costly lawsuits and data theft.

Aside from the monetary considerations, safe identity verification is critical for fostering trust in the gaming community. Verified profiles not only aid in the identification of rogue actors, but they also enhance the overall online gaming experience.

### 2. Financial Services

Banks, crowdfunding platforms, insurance firms, and virtual payment systems are all working hard to make customer transactions as simple as possible. However, illegal activity has become a major issue.

Digital ID can alleviate systemic issues by reducing some of the barriers to participation in the digital economy for individuals with restricted access. To begin, a legally recognized, unique digital identity can be used in place of physical documents. You can leverage technology to meet regulatory goals such as validating proof of address using GPS. This process will enable an individual to meet the KYC standards for opening a transaction account, which will open up a world of financial possibilities.

### 3. Travel and Tourism

Fake travel agencies, fabricated identities used to escape, and a variety of other activities make it difficult for the travel industry to adhere to KYC standards. Fraudulent activities in the travel industry cost it almost[$21 billion USD](https://shuftipro.com/blog/travel-industry-trends-scams-and-a-solution-to-combat-fraud/#:~:text=According%20to%20Finextra%2C%20the%20travel,for%20more%20than%20%2425%20billion.)annually.

Face and other forms of identity verification can assist the travel sector in adhering to the rules while aiding in preventing fraudsters from fleeing with all of their activities.

**REMOTE AUTHENTICATION:**

For any organization, access management holds immense importance. During the pandemic organizations across the world switched overnight to modern access management systems for remote user authentication.

Remote user authentication, the process of verifying users remotely to grant access to the organization’s system over a network, is now widespread. Hybrid work and the growing adoption of modern unified communication tools have just accelerated its growth. Nearly all businesses today have clients and employees interacting remotely through a network.

Still, many companies have fallen prey to unauthorized access debacles. It is necessary to vet the identity of remote users gaining access to the system. Among the attack vectors, security leaders do not really view employee or internal incidents as top threats. Though [research](https://www.forrester.com/blogs/breaches-by-the-numbers-adapting-to-regional-challenges-is-imperative/) suggests the frequency of breaches is evenly spread.  With breaches increasing in frequency due to remote work, it is important to reassess remote user authentication methods.

**How does remote user authentication work**

To thwart such attempts, many companies deploy an array of security measures. From passwords and OTPs to biometrics, in recent years organizations have beefed up security using multi-factor authentication methods.

Usually, the remote user authentication method comprises:

1. Identification (Step 1): The user needs to perform certain identity verification activities, like face authentication, fingerprint scan, voice authentication, password verification, etc. This step is the first and is often clubbed with other identification methods for better security.
2. Verification (Step 2): In this step, the information generated is matched with records to ascertain the identity presented in Step 1.

The means of authenticating a user can be:

1. User knowledge: passwords, answers to specific questions, PIN or OTP.
2. Organization-issued assets: smart cards, cryptographic keys, physical keys.
3. Biometric features: face, retina, fingerprints
4. Biometric characters: Voice recognition, typing rhythm, handwriting

In a [Statista](https://www.statista.com/statistics/1276705/eu-us-remote-work-information-security-protocols/) survey last year, 28% of respondents from the US and Europe said that multi-factor authentication for endpoints and servers is used more frequently to secure a hybrid workforce.

Here’s a breakdown of ways how companies are deploying remote work security protocols.

**Advantages of remote user authentication**

For your organization, the best solution will deliver the appropriate level of security, and high completion rates, and will be inclusive to the largest number of customers or citizens.

1. Quick access

Remote access allows quick access to systems and files through a network connection.

1. Cost- effective: Remote authentication is a cost- effective method for distributed teams, and to onboard vendors and contractual workers. With the surge in third-party remote authentication vendors, remote authentication technology has advanced. Companies can now support different devices for remote user authentication. Location is not a constraint.
2. Secure: Remote user authentication extends security to the organizational systems by ascertaining the identity of users off-site. Even for customers and clients, a robust remote authentication method guarantees that the user is genuine, abating risks of fraud.
3. Private: Today’s modern authentication methods afford privacy. There are many methods of remote user authentication that companies can deploy. They can choose the most suitable framework considering their user privacy.
4. Convenience: Remote user authentication makes it easy for companies to employ remote talent, or communicate with third parties securely.

**Drawbacks of remote user authentication**

1. **Detecting threats**

Even though remote user authentication offers convenience in the form of easy onboarding, customer sign-ins, and contract workers’ access, it is not easy to remotely keep a check on everyone.

Security teams need to a monitor host of endpoints and devices for threats that can target remote users and in particular identify an attacker gaining access to the network. Due to the increasing number of users detecting, the visibility to detect advanced threats is often overlooked.

1. **New devices, new threats**

The marketplace for remote work devices has burgeoned suddenly. Users are deploying new and advanced devices for endpoints at home that are sometimes unsecured too. New devices pose own unique challenges for security teams.

1. **Network dependent:**Most organizations have a stable network infrastructure for on-premise set up. However, it is not always feasible to obtain the same level of network reliability and security at home or in remote work.

**UNIT-4**

**MOBILE PAYMENTS**

## What Is a Mobile Payment?

A mobile payment is a money payment made for a product or service through a portable electronic device such as a tablet or cell phone. [Mobile payment technology](https://www.investopedia.com/best-payment-apps-5180406) can also be used to send money to friends or family members, such as with the applications PayPal and Venmo.

## Understanding Mobile Payments

Many banks have recently adopted technology into their banking apps that allow customers to send money instantly to friends and family members directly from their bank accounts. Mobile payments are also made on site at stores by scanning a barcode on an app on your phone, accepting payments from convenience stores to large, multi-national retailers.

The cost of the purchase may be deducted from a pre-loaded value on the account associated with the particular store, or paid by credit or [debit card](https://www.investopedia.com/terms/d/debitcard.asp). Payment information is encrypted during transmission, so it is thought of as being a safer payment method than paying with a debit or credit card.

Mobile payments first became popular in Asia and Europe before becoming more common in the United States and Canada. Early on, mobile payments were sent by text message. Later, technology allowed for pictures of checks to be taken via cell phone camera and sent to the payment recipient. This technology eventually morphed into mobile check deposit capabilities for banking apps.

Since 2014, apps such as PayPal1 and Apple Pay2 were developed that allow payment by passing a smartphone screen displaying a special [barcode](https://www.investopedia.com/terms/b/barcode.asp) under a store's barcode scanner. They also allow the user to simply tap their phone against a contactless credit card terminal, paying instantaneously.

Soon to develop applications were competitors to Apple, companies like Google and Samsung, who released their respective mobile payment apps in the wake of Apple pay's success.

## Benefits of Mobile Payments

The most obvious benefit of mobile payments is the elimination of a physical wallet. Not reaching and pulling out cash not only saves time but is safer as well as nobody is able to see the contents of your wallet or purse.

Touch ID in the form of a fingerprint scan or PIN input makes [mobile payments](https://www.investopedia.com/articles/personal-finance/040616/best-mobile-payment-apps-tap-and-pay.asp) more secure than a physical credit card. Since individual security codes are generated by the mobile service for each transaction, this method of payment is significantly safer than using a physical card. Merchants will usually not check identification, so accepting mobile payments is a smart move for them as well, as they will not have to deal with fraudulent activity as much.

An additional benefit—though a minor one for most people—is that when you are with other people they are not able to tell what card you have. Users with low credit scores and credit cards with low limits and high APRs might not want, say, an interviewer or date to know these things, and mobile payments offer an additional level of personal privacy.

**WIRELESS PAYMENTS / CONTACTLESS PAYMENTS:**

The term contactless payment refers to a secure method for consumers to purchase products or services using a debit, credit, smartcard, or another payment device by using [radio frequency identification (RFID)](https://www.investopedia.com/terms/r/radio-frequency-identification-rfid.asp) technology and [near-field communication (NFC)](https://www.investopedia.com/terms/n/near-field-communication-nfc.asp). This payment method works by tapping a payment card or other device near a [point-of-sale terminal](https://www.investopedia.com/terms/p/point-of-sale-terminal.asp) equipped with contactless payment technology. Contactless payment is also referred to as tap-and-go or tap by some banks and retailers.

##  How Contactless Payment Works

Contactless payment allows consumers to pay for goods and services using their [debit or credit cards](https://www.investopedia.com/articles/personal-finance/050214/credit-vs-debit-cards-which-better.asp) with RFID technology—also known as [chip cards](https://www.investopedia.com/terms/c/chip-card.asp)—or other payment devices without the need to swipe, enter a [personal identification number (PIN)](https://www.investopedia.com/terms/p/personal-identification-number.asp), and/or sign for a transaction. Merchants that accept contactless payment have point-of-sale terminals with a special symbol identifying the technology, which is similar to the wifi logo but turned onto its side.

Here's how it works. When the merchant's system prompts the customer to pay, they bring the card between close to the contactless payment symbol on the terminal. Information is transmitted electronically using information from the chip from the card to the bank. When the system accepts the tap, it signals the customer with a beep, green light, or checkmark. Once the approval is received, the [transaction](https://www.investopedia.com/terms/t/transaction.asp) is complete.

With the rise in wireless technology and the popularity of smart devices, consumers can also connect their [credit cards](https://www.investopedia.com/terms/c/creditcard.asp) to a device—a smartphone, smartwatch, or fitness tracker—to pay using the contactless system as well. This is done by downloading a payment app such as Apple Pay, allowing consumers to securely store credit and debit card information to make purchases by tapping a smartphone or Apple iWatch.

## In most cases, transaction sizes on cards are limited for contactless payment. The allowable amount for a contactless transaction varies by country and by the bank. Some merchants and retailers may set a low limit for their tap system in order to further prevent [fraud](https://www.investopedia.com/terms/f/fraud.asp), while others still allow large transactions to go through.

## Advantages and Disadvantages of Contactless Payment

Fraudsters are able to steal and clone information from magnetic stripes on the back of payment cards. This allows them to clone the information and make new cards, leading to fraud and [identity theft](https://www.investopedia.com/terms/i/identitytheft.asp). Contactless payment cuts down the [risk](https://www.investopedia.com/terms/r/risk.asp) to both the consumer and the merchant. That's because they're more secure than using [magnetic stripes](https://www.investopedia.com/terms/m/magnetic-stripe-card.asp) on the back of payment cards. Information submitted through the merchant terminal through contactless payment, on the other hand, is encrypted, meaning it is difficult to intercept and steal.

Despite these security features, criminals are still able to [skim](https://www.investopedia.com/terms/s/skimming.asp) cards in consumers' wallets using [smartphones](https://www.investopedia.com/terms/s/smartphone.asp) to read. The range at which a card can be read is very short and, even if the thief is close enough to grab data, they can't create a copy of the card. This is not true of cards with magnetic stripes. That said, chip and PIN cards are still the most secure, as they can't be duplicated and require data not contained anywhere else on the card.

Consumers are now able to dispute fraudulent transactions and get replacement cards. There are also protective card sleeves and wallets that block readers from getting to your card data in the first place. As of 2015, merchants and credit card companies became [liable](https://www.investopedia.com/terms/l/liability.asp) for any fraudulent activity that took place through their systems if they had no chip technology in place.

**What Is a Digital Wallet?**

A digital wallet (or electronic wallet) is a financial transaction application that runs on mobile devices. It securely stores your [payment](https://www.investopedia.com/terms/p/payment.asp) information and passwords. These applications allow you to pay when you're shopping using your device so that you don't need to carry your cards around. You enter and store your credit card, debit card, or bank account information and can then use your device to pay for purchases.

Digital wallets can also store:1

* Gift cards
* Membership cards
* Loyalty cards
* Coupons
* Event Tickets
* Plane and transit tickets
* Hotel reservations
* Driver's license
* Identification cards
* Car keys

**How a Digital Wallet Works**

Digital wallets are applications designed to take advantage of the abilities of mobile devices to improve access to financial products and services. Digital wallets essentially eliminate the need to carry a physical wallet by storing all of a consumer's payment information securely and compactly.

Digital wallets use a mobile device's wireless capabilities like Bluetooth, wifi, and magnetic signals to transmit payment data securely from your device to a point of sale designed to read the data and connect via these signals.

Currently, the technologies used by mobile devices and digital wallets are:

* **QR codes**: Quick response codes are matrix bar codes that store information. You use your device's camera and the wallet's scanning system to initiate payment.
* **Near field communication (NFC)**: NFC is a technology that allows two smart devices to connect and transfer information using electromagnetic signals. It requires two devices to be within about an inch and a half (4 centimeters) from each other to connect.
* **Magnetic secure transmission (MST)**: The same technology used by magnetic card readers that read your card when you swipe it through a slot on a point of sale. Your phone generates this encrypted field that the point of sale can read.

The card information you've stored in your wallet and choose to use for a transaction is transmitted from your device to the point of sale terminal, which is connected to payment processors. Then, through the processors, gateways, acquirers, or any other third parties involved in credit and debit card transactions, the payment is routed through the credit card networks and banks to make a payment.

Because cryptocurrency has made its way into the financial system, companies like Bit pay invented cards that let you pay with cryptocurrency. Digital wallets like Apple Pay and Google Pay allow you to add a Bit pay debit card. The Bit pay card converts cryptocurrency to dollars at the current market value, which your wallet then uses to pay for your purchase.

**Types of Digital Wallets**

There are several digital wallets available. Here are some of the most well-known:

* Cash App
* Apple Pay
* Google Wallet
* Samsung Pay
* PayPal
* Venmo
* Alipay
* Walmart Pay
* Dwolla
* Vodafone-M-Pesa

Most wallets attempt to distinguish themselves from their competitors using different methods. For example, Google's digital wallet service allows you to add funds to the wallet on your phone or device. Then, you can spend this cash in-store and online at businesses that accept Google payments.

Apple, on the other hand, entered into a strategic partnership with Goldman Sachs to issue Apple credit cards and expand its ApplePay services.

**Advantages and Disadvantages of Digital Wallets**

One of the most significant advantages of digital wallets is that using one limits the amount of financial and personal information you need to carry as you go about your day. If you place everything in your digital wallet, you no longer need to carry physical cards or a physical wallet—there is no chance of a card falling out of your wallet or of leaving your card in the ATM slot. Additionally, you can't lose your entire wallet.

# Google Wallet:

Google Wallet is a mobile payment system that acts as a virtual wallet, allowing users to make payments and transfer money straight from their phones. The service is free for users and can store credit, debit, gift and loyalty card information. Available to anyone with a newer Android or Apple smartphone, Google Wallet gives users another fast way to make payments at ecommerce stores that accept it.

Mobile payments are a relatively new strategy that has the potential to greatly benefit online sales. Currently, mobile devices account for [just under 50 percent of ecommerce traffic](http://marketingland.com/mobile-drives-nearly-half-e-commerce-traffic-pc-still-rules-sales-report-118629), but when it comes time for users to purchase items online, nearly 77 percent of users do so exclusively on a personal computer instead. Customers avoid making actual purchases on mobile devices because of concerns about security and the inherent difficulty of entering bank card information using a touch screen interface.

Electronic wallets look to sidestep these concerns by [streamlining the mobile payment process](https://www.bigcommerce.com/blog/mobile-checkout-optimization/) via a secure service. Customers simply click to buy something and all of their payment info is already entered into the wallet. The fast checkout works both in-app and on participating mobile sites.

Google Wallet also gives merchants the ability to highlight special offers or discounts from their websites or emails directly to the shopper via the app. Customers can also add any gift card balances to their virtual wallets, which helps drive additional sales. According to Forrester Research, payments made with Google Wallet and other services like it are expected to [top $140 billion by 2019](http://blogs.forrester.com/denee_carrington/14-11-17-us_mobile_payments_will_reach_142b_by_2019).

#### **How it works**

Google Wallet is what is known as a server-side wallet, which means that all of a user's information is stored remotely on Google's system, rather than on the user's device. Transactions take place between Google's servers and the merchant's [existing payment processor](https://www.bigcommerce.com/payments/).

It acts somewhat like a gift card: users place a set amount of money into the wallet they can then spend as desired. As far as the user's bank is concerned, the transaction is identical to any other debit or credit, only the transactions go exclusively through Google rather than the merchant's point of sale. Assuming the merchant's point of sale is configured to accept Google Wallet, transactions work the same as any other accepted payment method.

While support for the mobile app is still sketchy, Google Wallet offers a physical card as well that can be used anyplace that accepts debit MasterCard.

How does Google Wallet stack up to other options?

Google Wallet's main competitor is Apple, although other companies such as Samsung and PayPal have their own digital payment systems as well (Samsung Pay and PayPal Wallet, respectively). While the products may have a few differences when it comes to the user, they offer similar features from the perspective of an online store owner. Both want to make it as easy as possible to facilitate transactions.

* Neither charge fees.
* Liability rules are the same as regular card transactions.
* Both can support rewards programs.
* Both make the purchasing process much faster.
* Both utilize NFC (near field communications) for in-store purchases.

The main difference between the two initiatives is the [companies behind them](http://thefinancialbrand.com/50720/mobile-payments-digital-wallet-analysis/). Google pioneered NFC technology years ago, which allowed users to pay with a mobile device at a point of sale using a secure, short-range signal. However, the technology was not widely adopted at the time, which put Google on the back foot, giving Apple an opening to push [their Apple Pay model](https://www.bigcommerce.com/blog/apple-pay-tips-mobile-payments/).

Apple, having an established and loyal user base, was able to roll out its system a great deal more effectively, coupling it with specific technology offerings, such as the Apple Watch. Seeing an opportunity to partner with the high-prestige Apple brand, retailers and banks have been a great deal more eager to adopt the technology now.

Google, however, is retooling its wallet to take advantage of their more flexible and open system. Unlike Apple, Google is allowing other developers [access to its API](http://www.androidpolice.com/2015/03/02/sundar-pichai-briefly-confirms-android-pay-at-mobile-world-congress/) in hopes that other companies will create innovative new ways to use the technology. [With 80 percent of global market share](http://9to5mac.com/2014/10/31/android-vs-ios-market-share-3q-2014/) for the [Android platform](https://smshare.fr/blog/app/faq/index.html), payment processors and merchants have good reason to support Google's initiatives.
When compared with other virtual wallets, Google Wallet and Apple Pay stand above most for online transactions. The focus of many other virtual wallets is in-store purchases. Most of them, like Samsung Pay, can only process offline purchases and PayPal Wallet is not widely supported.

**OBOPAY:**

Obopay is a mobile payment service in the US that lets consumers get, send and spend money from mobile phones. The Obopay management team is comprised of former executives from Visa International, Microsoft, Yahoo, Expedia, AT&T Wireless, Western Union, First Data Corporation, Norwest Bank and Chordiant Software.

OBOPAY is a global transformative pioneer in the mobile money technology space; offering stellar products, services, solutions and business consulting across banking, telecom, retail, MSME and government sectors since 2005. Headquartered in Bangalore, OBOPAY delivers cutting-edge, secure and scalable mobile-money platform and solutions. Rated amongst the best mobile money platforms, OBOPAY offers robust, cost-conscious and nimble implementation solutions with low deployment costs; powering three billion plus transactions with zero fraud cases and is driving 11% of global mobile money transactions.

## Mobile Payment Security Challenges

Despite the increasing demand for mobile payments, there is still hesitation among both businesses and end-users to fully adopt the technology due to security-related concerns.

Today’s [cybercriminals](https://www.onlinewhitepapers.com/information-technology/what-is-cyber-extortion-and-how-to-combat-it/) and fraudsters employ increasingly sophisticated techniques to procure sensitive and personal data. Hence, these concerns are not misplaced.

**Mobile payments are associated with several security risks. Here’s a list of some of the common mobile payment security risks:**

### 1. Applications with security flaws

Many security risks in an application are found in the programming of the app when the app creators fail to follow a secured-by-design approach. Besides this, some vulnerabilities may also be discovered once the app goes live.

### 2. No payment security when the phone is lost

Smartphones today, are all-in-one devices. In addition to easy payment options, there’s also personal information on it including contact information for you and others in your phone book, names, personal photos, social media connections, and so on. Through various payment apps, mobile wallets, online banking apps, and much more, phones also give access to bank accounts, debit cards, and credit cards.

If you lose your phone in a store, restaurant, or crowded place, all your information is available easily. The details of banking and mobile payments are thus at risk, which can result in fraud.

### 3. Inappropriate usage

Regardless of how secure your mobile phone is, the way you use your mobile phone can pose a security risk. Using your mobile phone’s website, fraudsters can make purchases and payments. Google Pay and Apple Pay are popular for making mobile payments on Android and Apple phones, which is highly risky once encryption is decoded.

### 4. Exposed mobile wallets

As mobile payment options became available, several payment apps emerged. A debit or credit card must be entered into the mobile wallet for these applications to work.

During the application process, details like the card number, VCC number, expiration date of the card, etc. are encrypted through codes. For making payments, the providers of mobile wallets also use a randomly generated verification number that is not visible to the merchants while transactions are being made. This means the data linked to your credit cards is also available on the multiple mobile wallets that you chose to use.

### 5. Cloned applications

Is your mobile phone set up with an authentic banking or mobile wallet application? Could it be a clone? Many app clones offer secure payment options exactly akin to the original apps.

If users use these clones of authentic apps and register their banking information with them, it will be easier for the criminals to commit fraud using details of their credit cards, debit cards, and other personal information. Criminals can easily access such clones due to their poor security features.

### 6. Making use of a variety of software options

Mobile phones also use a variety of hardware and software systems, just as do laptops and desktops. In some countries, iOS and Android are still used by users of the older versions. Security issues can arise because of this. The devices are not well-supported by the latest mobile security technologies, which makes them attractive to hackers and fraudsters.

Even if your mobile applications are secure, your device may not meet the security standards needed for mobile wallet transactions, thus making it risky for the users.

### 7. Risks related to networks

Older mobile devices that contain mPOS applications are more vulnerable to fraud and more likely to be hacked by criminals. Fraudsters use increasingly sophisticated methods to acquire sensitive information from businesses as they now have technology capabilities far more advanced than before.

Even though data breaches at large organizations tend to dominate the headlines, small-to-medium-sized businesses are more vulnerable to fraudsters, as they do not invest in security measures that are robust enough to protect their customers.

## How to Build Mobile Payment Security to Avoid Fraud

When it comes to mobile payment security, there are certainly some concerns to consider. However, that doesn’t mean you should abandon mobile payment options for a business altogether. With mobile payments, you can take a variety of security measures to reduce fraud risk. Here are some tips.

### Sensitive information shouldn’t be sent over public Wi-Fi

Securing internet networks for your business’ POS applications is critical. If you don’t offer secure networks for your customers’ devices on your Wi-Fi networks, you stand to lose trust and suffer severe harm to the business. When it comes to hacking mobile devices, cybercriminals have advanced technical know-how.

People may be wary of sending sensitive data such as financial information over public Wi-Fi networks due to the risk involved because information transmitted over these networks is accessible easily through the network.

### Use VPN for mobile payment security

If you absolutely must use a public network, please ensure that your customers’ information is encrypted properly. You can have them access the internet securely and safely with a VPN.

Financial transactions are encrypted end-to-end with [mobile payment apps](https://www.techfunnel.com/martech/why-smbs-should-consider-using-mobile-payment-technology/). When the financial data arrives at the other end, it is decrypted. Securing your customers’ financial data on unsecured networks with a VPN can be the way to protect them.

### Strengthen your passwords

Be sure to always lock your phone. Your phone can be easily accessed and the sensitive financial information on it stolen if it is unlocked. Consider using strong passwords and utilizing other security features, such as fingerprint recognition, iris scanning, and facial recognition, on your device.

### Turn on anti-theft features

Mobile phones can get lost all the time. Using your phone’s built-in anti-theft protection tools, you can lock a stolen or lost device so that an unauthorized person cannot use it. If you want to remotely erase the data on the device, including contacts, banking app data, mobile payment app data, emails, and photos, you can do that as well.

### Make sure your mobile payments are safe

Whenever you use a mobile payment platform, make sure to use only trusted platforms. To add information to your smartphone, make sure you have the latest version of the software. Verify that third-party platforms such as PayPal are trusted and verifiable.

## What Is a Debit Card?

A debit card is a payment card that deducts money directly from a consumer’s checking account when it is used. Also called “check cards” or "bank cards," they can be used to buy goods or services; or to get cash from an automated teller machine or a merchant who'll let you add an extra amount onto a purchase.

## How a Debit Card Works

A debit card is usually a rectangular piece of plastic, resembling any charge card. It is linked to the user's checking account at a bank or credit union. The amount of money that can be spent with it is tied to the account size (the amount of funds in the account).

In a sense, debit cards work as a cross between ATM cards and credit cards. You can use them to get cash from a bank's automated teller machine, as with the former; or you can make purchases with them, like the latter. In fact, many financial institutions are replacing their plain vanilla, single-purpose ATM cards with debit cards that are issued by major card-payment processors such as Visa or Mastercard. Such debit cards come automatically with your checking account.

Whether being used to obtain cash or to buy something, the debit card functions in the same way: It draws the funds immediately from the affiliated account. So, your spending is limited to what’s available in your checking account, and the exact amount of money you have to spend will fluctuate from day to day, along with your account balance.

Debit cards usually have daily purchase limits as well, meaning you can't spend more than a certain amount with them in one 24-hour period.

**Advantages and Disadvantages of a Debit Card**

With debit cards, consumers are effectively making their purchases in cash—that is, with money they actually have, as opposed to money borrowed on credit. But they are considerably safer than cash. [Every transaction made with a debit or check card](https://www.investopedia.com/ask/answers/050415/what-happens-when-my-bank-account-debited.asp) will appear on the account holder’s monthly statement, making it easy to "see where the money went."

And while lost or stolen cash is gone forever, a lost or stolen debit card can be reported to the bank, which can deactivate the card, remove any fraudulent transactions from the cardholder’s account, and issue a new card.

Debit cards are easier to get if you have poor credit—as long as the bank lets you set up an account, you're in—and you don't have to apply for them, as you do with credit cards. Nor do you pay annual fees. Because debit cards don't charge merchants much, merchants don't impose minimum-purchase amounts on debit cards, as they often do with credit cards.

Note that debit cards generally don't offer as many perks, or have as many protections against fraud, as credit cards. For one thing, if an identity thief gets into your actual bank account and withdraws funds, you lose the money immediately. Getting it refunded can be tough.

Also, your expenditures on the debit card are limited to the money you have in the bank. And what with auto-bill pay, auto deposits, and ATM withdrawals, it can be hard to remember how much is in a checking account at any given time, making it tricky to use a debit card for purchases. Your card could be declined, or you may incur overdraft fees.

Pros

* Safer than cash
* Doesn't incur debt
* Easy to get—no application necessary

Cons

* Limits expenditures to cash in bank and/or a daily amount
* Easy to incur overdraft fees
* Fewer perks and protections than credit cards

## What Is a Credit Card?

A credit card is a thin rectangular piece of plastic or metal issued by a bank or financial services company that allows cardholders to borrow funds with which to pay for goods and services with merchants that accept cards for payment. Credit cards impose the condition that cardholders pay back the borrowed money, plus any applicable interest, as well as any additional agreed-upon charges, either in full by the billing date or over time.

In addition to the standard credit line, the credit card issuer may also grant a separate cash [line of credit (LOC)](https://www.investopedia.com/terms/l/lineofcredit.asp) to cardholders, enabling them to borrow money in the form of cash advances that can be accessed through bank tellers, ATMs, or credit card convenience checks. Such cash advances typically have different terms, such as no grace period and higher [interest rates](https://www.investopedia.com/terms/i/interestrate.asp), compared with those transactions that access the main credit line. Issuers customarily preset borrowing limits based on an individual’s [credit rating](https://www.investopedia.com/terms/c/creditrating.asp). A vast majority of businesses let the customer make purchases with credit cards, which remain one of today’s most popular payment methodologies for buying consumer goods and services.

## Understanding Credit Cards

Credit cards typically charge a higher [annual percentage rate (APR)](https://www.investopedia.com/terms/a/apr.asp) vs. other forms of consumer loans. [Interest](https://www.investopedia.com/terms/i/interest.asp) charges on any unpaid balances charged to the card are typically imposed approximately one month after a purchase is made (except in cases where there is a 0% APR introductory offer in place for an initial period of time after account opening), unless previous unpaid balances had been carried forward from a previous month—in which case there is no grace period granted for new charges.

By law, credit card issuers must offer a grace period of at least 21 days before interest on purchases can begin to accrue.1 That’s why paying off balances before the grace period expires is a good practice when possible. It is also important to understand whether your issuer accrues interest daily or monthly, as the former translates into higher interest charges for as long as the balance is not paid. This is especially important to know if you’re looking to [transfer your credit card balance](https://www.investopedia.com/best-balance-transfer-credit-cards-4801444) to a card with a lower interest rate. Mistakenly switching from a monthly accrual card to a daily one may potentially nullify the savings from a lower rate.

# RuPay card:

Rupay Debit Card comes in many categories, but mainly in two types: RuPay Platinum and RuPay Classic. These cards carry your savings account with you anytime, anywhere and you can shop, pay bills, and withdraw cash.

Introduced by National Payment Corporation of India (NPCI), Rupay Debit Card is an indigenous domestic debit card accepted at all ATMs (for cash withdrawal) and at most of the PoS machines--for making cashless payment for purchases--in the country. It is a highly secure network that protects against anti-phishing, and also the first-of-its-kind domestic Debit and Credit Card payment network of India, according to RuPay website.

The name, derived from the words ‘Rupee and ‘Payment’, states that it is India’s own initiative for Debit and Credit Card payments, besides being an answer to international payment networks. It also fulfils RBI’s vision of initiating a ‘less cash’ economy, thereby, offering electronic payments.

Rupay Debit Card comes in many categories, but mainly in two types: RuPay Platinum and RuPay Classic. These cards carry your savings account with you anytime, anywhere and you can shop, pay bills, and withdraw cash.

**RuPay Platinum**

* With this card, you can celebrate the joys of life every day as it offers several benefits given below. RuPay Platinum Card.
* Welcome Benefits: If you opt this card, you can avail a gift voucher from Croma worth Rs 500 or avail 15% Gift voucher from Apollo Pharmacy.
* Complimentary Lounge Program: With this card, you can make your travel experience hassle free with access to 30+ domestic lounges two times per calendar quarter per card.
* Cashback on Utility Bill Payments: You can also earn 5% cash back on your utility bill payments capped at Rs 50 per month per card.
* Comprehensive Insurance Cover: You can also keep yourself and your family safe with Personal Accident Insurance and Permanent Total Disability cover up to Rs 2 Lakhs, according to RuPay website.
* Exclusive Merchant Offers: You can celebrate round the year with exclusive merchant offers (POS and Ecom) available on your RuPay Platinum Debit Card, besides availing 24/7 host of referral services from travel assistance to hotel reservations to consultancy services.

**RuPay Classic**

* With RuPay Classic Card, you can benefit from a comprehensive insurance cover. The card also offers comprehensive accidental Insurance Cover, therefore, you can keep yourself and your family safe with Personal Accident Insurance and Permanent Total Disability cover upto Rs 1 Lakh.
* Under Exclusive Merchant Offers, you would be able to celebrate round the year with exclusive domestic merchant offers (POS and Ecom) available on your RuPay Classic Debit Card.

Notably, RuPay has collaborated with almost 600 international, regional and local banks across the country, and its ten core promoter banks are State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Union Bank of India, Bank of India, ICICI Bank, HDFC Bank, Citibank N. A. and HSBC, according to RuPay website.

## What is e-challan?

Since everything is on an electronic platform, the concept of e- challan system has been introduced. A vehicle e challan is a computer-generated challan used by the Traffic Police and is being issued to all the traffic defaulters in India. The Government of India has initiated this process to make the traffic services convenient, easy as well as transparent to the general public.

Also, with e- challan system effective and strong monitoring of the traffic violators becomes easy for the traffic police. In the age of digitalization, traffic defaulters will be able to now pay e-challan either online or offline, depending on the facility given by their city or state. E- challan system has been introduced to avoid cash transactions so that everything is very clear and transparent. The government of India has also introduced Traffic eChallan, which is an application and is combined with web portal applications which are namely Vahan and Sarathi. These two applications offer many benefits and features which cover all the main aspects of the Administration System. The traffic e challan can be paid both online as well as by the traffic violators.

## Traffic violations for which you might get an e-challan:

There are multiple reasons when an e-challan could be issued by the traffic policemen like:

* Violations of traffic rules,
* Jumping red lights,
* Travelling without a valid ticket,
* Refusal to share information when asked,
* Driving an unauthorised vehicle,
* Driving without a valid license,
* Over-speeding beyond the specified speed limit,
* Drunk driving,
* Driving without a valid insurance policy,
* Causing traffic obstruction, etc.

## How does e-challan work?

Well, with the advancement in technology, the online solution is coming up for many aspects in our daily life. E- challan system is one of the biggest examples. Now let us see how it works for you to understand it better. CCTV cameras are installed on the main roads that record and track the footage of the continuous traffic all the time. If you are found guilty of not obeying any traffic regulation, then the traffic police will see the footages of the offence from the respective CCTV and record the same in their books, get the details like name, full address, contact number, vehicle details of your vehicle from the RTO office. An SMS will be sent to you notifying you about the fault committed and the amount of fee which needs to be paid. Traffic police are given the swiping machines for them to generate and print the vehicle e challan instantly to the traffic violators. This e- challan system makes the payment process also smoother as the fine is mostly collected on the spot itself. The defaulter is then issued a receipt confirming that the payment has been received. The entire process is explained below:

1. The CCTV footage captures the defaulter. The Enforcement Officer gets the details of the defaulter with the Registration and the driving license number from Vahan and Sarathi database and chooses the offence committed
2. A message will be sent to the offender’s registered cell number. The fine amount is calculated automatically as per the offence and the Enforcement Officer then takes a print out of the traffic e challan with all the necessary details and gives the same to the offender
3. The defaulter is allowed to pay online by scanning the QR code received or can make cash payment at the RTO office or can deposit cash at onsite.

**UNIT-5**

**ELECTRONIC INVOICE AND PAYMENT SYSTEM**

## ****What is an e-invoice?****

An [**electronic invoice (e-invoice)**](https://www.pagero.com/solutions/e-invoicing/) is an invoice that is issued, transmitted, received, processed and stored electronically using specific document formats. E-invoices are digital throughout the entire document life cycle, from issuance to archiving.

E-invoicing solutions can help replace manual tasks with automated business rules and actions to increase efficiency, minimise error handling, and help businesses comply with e-invoicing legislation.

**What are the advantages of e-invoicing?**

The latest [**Billentis Report**](https://www.pagero.com/guides-and-reports/billentis-report/) reveals that “Compared to conventional paper invoice processing, the automated e-invoicing will result in cost savings of 60-80% in most cases,” (Bruno Koch, “The E-invoicing Journey 2019-2025,” 4.1.5).

Where does all that savings come from? When done right, e-invoicing gives you overview and insight for cutting costs and increasing profit margins that aren’t possible with PDF and paper-heavy invoicing. Here are some of the advantages of e-invoicing that add up to high ROI, long-term savings and better business in general:

* **Touchless operations**: E-invoicing enables the automation of time-consuming and error-prone tasks like data entry, matching and approvals so you can reallocate staff to higher-value initiatives.
* **Better cash flow and**[**lower DSO**](https://www.pagero.com/blog/reduce-dso/): Removing paper work and manual tasks can reduce your days sales outstanding by several days in most cases.
* **Secure document and data exchange**: Encrypted file transfer, digital signatures and secure networks all make e-invoicing the safest way to send and receive invoices. There’s also no risk of invoices being lost in the mail or sent to junk email.
* **Real-time delivery and processing**: View live delivery and processing status of documents on cloud-based platforms or directly from your ERP.
* **High quality data**: E-invoicing lets you access and analyse line-level data that [**drives business growth**](https://www.pagero.com/blog/accurate-invoice-data-drives-business-success/) through better financial and procurement decisions.
* **Accurate invoices**: Automated invoice validation and enrichment help ensure only correct transactional data enters your ERP system. Fewer discrepancies mean shorter cycle times and better business relations.
* **Track and traceability**: E-invoicing automatically tracks transaction history and entire document journey and so you don’t have to spend time doing it manually.
* **Environmentally friendly**: E-invoicing not only helps you lower paper use and CO2 emissions; this sustainable effort also lowers operations costs, [**leads to higher profitability**](https://www.pagero.com/blog/sustainability-in-business/), and creates a transparent, trustworthy brand reputation.
* **Fulfil legal requirements**: E-invoicing with the right service provider ensures you are always up to date and compliant with B2B and B2G tax and archiving legislation.
* **Remote work-ready**: E-invoicing tasks can be completed from anywhere without the need for extra resources like printers, scanners or the postal service.

**ELECTRONIC STATEMENT DELIVERY:**

The Electronic-only Statement Delivery service (also known as E-Statements) sends your monthly account summaries, balances, and disclosures to your online account in electronic-only format. Your electronic statements are exactly the same as your paper statements. To begin the process, we require your consent for the service so that we can send your statements in electronic-only format and suspend sending your paper statements in the mail. To access your account statement online, you will also need to meet the following minimum hardware requirements: x A computer with Internet connection and a hard drive with sufficient hard disk space to save any statements. x A printer connected to your PC to print statements x An Internet browser with 128-bit encryption and Internet access through an Internet Service Provider (ISP). x A home email address. You will be notified if these requirements change. If you select Electronic-only Statement Delivery but change your mind at a later time, you can opt-out of electronic-only statements and receive paper statements from JTNB at the next statement cycle.

## What Is an EIPP?

EIPP stands for Electronic Invoicing Presentment and Payment and is a type of software used by finance teams for [accounts receivable management](https://www.dnb.com/resources/accounts-receivable-management.html). With an EIPP, companies can automate the process of emailing invoices and account statements in bulk to their customers when it’s time for them to pay their bill. (That’s the Electronic Invoicing Presentment part of EIPP.) EIPP software also includes an online payment portal that enables companies to accept payments on those invoices from their customers (hence, the Payment part of EIPP).

### What Are the Benefits of an EIPP?

EIPP software can greatly improve a company’s efficiencies and optimize its invoicing and payment processes, as electronic invoicing (e-invoicing for short) can save both time and money for companies - as well as improve their customers' experience.

Think about it:

**Time Savings** – It takes a lot of time for someone to print invoices and mail them via the US Postal Service. It also takes a lot of time for someone to email monthly invoices to customers one by one. Nor is it sustainable to receive bank payments with disconnected remittances. Automating this process greatly reduces the time spent on manual work, allowing employees to focus on more important tasks. In addition, automated e-invoicing reduces the chance for human error (such as accidently notifying customers that don’t have an upcoming payment, notifying the branch office contact instead of the headquarters, or forgetting to attach the invoice). This also saves time that would be otherwise spent on corrections.

**Money Savings** – It’s also more expensive to print invoices and mail them via the US Postal Service and accept payments from fragmented channels. Automated e-invoicing reduces paper and postage costs and helps companies along their path to going paperless. Working to eliminate paper invoices, manual data entry, and fees from multiple payment channels can reduce costs for a company in the long run.

**Improved Customer Experience** – On the B2B payments side of an EIPP, online bill pay also improves the customers’ experience by making it easier to do business with their company. Their customers don’t have to tear remittances off the paper invoice, stuff them in envelopes, or mail checks at all. They simply click on the “pay now” link in an email – which can help them get paid faster. If customers have a question about their bill, they can message the vendor directly in the portal if they prefer e-communication over phone calls.

### What to Consider When Choosing an EIPP

Many software providers offer an EIPP as part of their larger [accounts receivable automation](https://www.dnb.com/resources/accounts-receivable-automation.html) platform. When choosing an EIPP for your business, consider the following questions:

* [Is it Easy to Integrate?](https://www.dnb.com/resources/eipp-electronic-invoice-presentation-payment.html#integrate)
* [Is it Customizable?](https://www.dnb.com/resources/eipp-electronic-invoice-presentation-payment.html#custom)
* [Is it Secure?](https://www.dnb.com/resources/eipp-electronic-invoice-presentation-payment.html#secure)
* Is it Easy to Integrate?

**ERP Integration -**Enterprise Resource Planning (ERP) systems are a core system for accounts receivable teams, but they tend to offer limited automation. Therefore, the expanded functionality that an EIPP provides can be appealing. Of course, EIPPs were designed to integrate with ERPs and their add-on modules for accounts receivable management, but some integrations can be difficult. Therefore, it’s important that any middleware or bolt-on software such as an EIPP be easy to integrate and interconnect with multiple ERP systems to better achieve process efficiency and truly optimize its invoicing and payment processes.

**A/P Portal Integration -**An EIPP benefits not only accounts receivable teams, but accounts payable (A/P) teams as well. A/P portals are becoming a common method of how large enterprises choose to receive invoices. For companies that serve larger enterprises, A/R teams might need to do more than send an email and expect a prompt payment. Even though there are electronic data interchange (EDI) standards that most portals support, each vendor portal and implementation is unique and needs a configurable solution. A/R teams that spend additional time posting invoices to customers’ A/P portals, some of which specialized by industry (retail, for example), can greatly benefit from the automation that an EIPP provides.

## Is it Customizable?

Companies also might want to consider some level of customization for their online payment portal so that the platform does (and looks) exactly like they need it to. Some vendors provide this as part of the platform, while others charge additional fees for any customization. A platform that allows you to easily add your company’s logo and other branding requirements is helpful in providing a consistent and authentic user experience for your customers. Configuration is also helpful in how your customers can use the platform. Can the user set up payment plans? Access historical statements? Track new orders? Communicate with you? A platform that has limited capabilities – such as only accepting credit card and ACH payments and current statements – may not have the flexibility that your company needs. You may need to support multiple standard banking formats such as ACH, SWIFT, and EFT.

## Is it Secure?

Finally, security is top of mind for any B2B payments software implementation. Companies should search for a secure, end-to-end connection accessible for both small and large customers that provides straight-through processing between the customer’s and the supplier’s systems. When choosing an EIPP platform, consider if the vendor is PCI (Payment Card Industry) compliant or works with a third-party PCI compliant payment processer.

### D&B Finance Analytics Receivables Intelligence

Dun & Bradstreet offers an EIPP as part of [D&B Finance Analytics](https://www.dnb.com/products/finance-credit-risk/dnb-finance-analytics.html), its complete credit-to-cash platform. The EIPP is part of the [Receivables Intelligence](https://www.dnb.com/products/finance-credit-risk/dnb-finance-analytics/receivables-intelligence.html) application and provides users with a unified, AI-driven e-invoicing and payments platform. Its Payment Portal is a powerful customer self-service portal that provides users with their up-to-date A/R data to pay online, track orders, and manage their profile. Payments are automatically applied to invoices with a real-time sync to your ERP. In addition, transmission and formats can be customized for each customer using its mapping engine and customizable APIs.

Would you like to learn more about Receivables Intelligence from D&B Finance Analytics? [Contact us for a personalized demonstration today!](https://www.dnb.com/marketing/media/ri-demo.html)

## Bill Service Provider (BSP)

A bill service provider, otherwise known as BSP, is a third-party organization used by billers to provide customers with payment options and an electronic billing statement. To truly define a BSP, one must understand who the biller is. This is an individual, company or organization that requires payment for a product or service. Any merchant account with credit card processing capabilities will need a bill service provider, unless they decide to use Biller Direct. Biller Direct is a bill payment model that allows merchants to bill consumers through their own websites electronically. Depending on what your business model is and how you operate your credit card processing and payment structure, either Biller Direct or BSP could be right for you. Most businesses, however, use a bill service provider.

**What services does a Bill Service Provider offer?**

A merchant’s time is valuable, which is why having a BSP in place can alleviate some of the work load. One of the services it provides is providing multiple payment options to a biller’s customers. These may vary from paying in full, in installments or perhaps a deferment plan if one is arranged. Another feature of a BSP is the flexible spending plans. Some examples include paying via the mail, over the phone, online with a confirmation code or even through a mobile device. Any bill service provider is sure to have security measures in place to give customers a concise and safe method of payment. Also, merchant account holders may view reports and data regarding each billing statement, cycle, payment, etc. All information regarding revenue collection is made privy to the biller. When bill payment problems and discrepancies arise, contact information is available on each statement to ensure that customers receive support from the bill service provider. This also alleviates time and stress from merchants, adding to the benefits of a BSP.

There are a myriad of bill service providers available, as well as Biller Direct service providers. To learn more about which service is right for your business and its needs, contact a BSP or Biller Direct customer service representative.

## what Is Customer Service?

Customer service is the direct one-on-one interaction between a consumer making a purchase and a representative of the company that is selling it. Most retailers see this direct interaction as a critical factor in ensuring buyer satisfaction and encouraging repeat business.

Even today, when much of customer care is handled by automated self-service systems, the option to speak to a human being is seen as necessary to most businesses. It is a key aspect of [servant-leadership](https://www.investopedia.com/terms/s/servant-leadership.asp).

## Understanding Customer Service

Behind the scenes at most companies are people who never meet or greet the people who buy their products. The [customer service representatives](https://www.investopedia.com/articles/financial-advisors/110315/considering-career-client-service-associate.asp) are the ones who have direct contact with the buyers. The buyers' perceptions of the company and the product are shaped in part by their experience in dealing with that person.

For this reason, many companies work hard to increase their customer satisfaction levels.

### The Cost of Customer Satisfaction

For decades, businesses in many industries have sought to reduce personnel costs by automating their processes to the greatest extent possible.

In [customer service](https://www.investopedia.com/articles/financialcareers/07/multi-service.asp), that has led many companies to implement systems online and by phone that answer as many questions or resolve as many problems as they can without a human presence.

But in the end, there are customer service issues for which human interaction is indispensable, creating a [competitive advantage](https://www.investopedia.com/terms/c/competitive_advantage.asp).

Amazon is an example of a company that is doing all it can to automate a vast and complex operation. It has to, given that it delivered 4.2 billion packages to customers' doors in 2020.1

Nevertheless, Amazon still offers 24-hour customer service by phone, in addition to email and live chat services.

Most successful businesses recognize the importance of providing outstanding customer service. Courteous and empathetic interaction with a trained customer service representative can mean the difference between losing or retaining a customer.

**What is 'Bank reconciliation'**
**Definition:**
A bank reconciliation statement could be defined as the summary of the banking and business accounts that reconciles a company's bank account with its financial record. The statement contains a record of all the deposits, withdrawals and other financial activities with a bank over a certain period of time. It is a useful tool to control fraudulent activities.

**Preparing a bank reconciliation statement:**
To complete a bank reconciliation statement, the accountant needs the following data

* Current and previous month's bank statement
* The closing balance of the bank account
* Any outstanding payments or withdrawals (cheques that haven't been processed yet)
* Any fees charged by the bank on the account
* Interest earned on the bank balance

 **Steps to Prepare a bank reconciliation statement**

* Compare the financial record on the company book to the bank statement.
* For any errors ( unaccounted for deposits and represented withdrawals) changes are made to the corresponding bank statements
* Make necessary changes in the log book and bank statements for fees, charges deducted and interest credited.
* The final step is to compare the two records - the company's own financial statement and the account statement. If they are the same, your bank reconciliation is done. If not repeat the process.

**Benefits of a Bank Reconciliation Statement**
A bank reconciliation statement ensures that all payments made by the company are processed and all deposits are correctly made on time.

* Bank reconciliation statements are great for detecting frauds in financial transactions of large companies (which are difficult to keep track of, otherwise).
* Bank reconciliation statements also help to analyze errors that can affect the financial transactions of a company or business.
* Such statements help to assess the financial health of a company and take adequate financial decisions for the betterment of business
* Bank reconciliation statements are also a key to accurate tax reporting. Without a proper financial statement, a company may end up paying too much or too less taxes.

**Common problems with bank reconciliation statement**
Bank reconciliation statements, if done properly and accurately is nothing but good for the financial record of a company. However, when there are long gaps between reconciliation sessions, problems can arise (like urgently required information may not be available at the moment, or problems during tax filing). Inaccurate bank reconciliation statements can cause problems with the financial record. Therefore, it is advisable to use software for recording such statements.

**eliminate paper invoices**

If you still use a paper-based invoicing process, chances are you are so used to it that you may not even see how limiting it is. It may be a case of “that’s just how we’ve always done things,” but that doesn’t mean it’s the best option for the future of the business. There are so many digital tools available that can help finance and accounting teams improve the invoicing process.

The following challenges are all symptoms of sending paper invoices. If any (or all) of them describe your AR team’s experience, it’s a likely sign that it's time to make the shift to electronic invoicing.

* **Delayed payments:** Sending out paper invoices delays when payment terms start, meaning it takes longer for your business to get paid
* **Staff monopolization:** Your AR staff spends an overwhelming amount on shipping invoices and manual data entry
* **Problems with accuracy:** You're finding a number of errors appearing in customer invoices
* **Difficult communication:**You find it hard to communicate with customers about billing questions and disputes
* **Customer complaints:**You often receive complaints about inaccuracies and other problems pertaining to their invoices
* **Requests for digitization:** Your customers are asking you for digital invoicing and payment options
* **High costs:** Your invoicing process represents a major cost center
* **Limited talent pool:** You experience difficulties attracting and retaining top-tier AR professionals*.*

The following challenges are all symptoms of sending paper invoices. If any (or all) of them describe your AR team’s experience, it’s a likely sign that it's time to make the shift to electronic invoicing.

* **Delayed payments:** Sending out paper invoices delays when payment terms start, meaning it takes longer for your business to get paid
* **Staff monopolization:** Your AR staff spends an overwhelming amount on shipping invoices and manual data entry
* **Problems with accuracy:** You're finding a number of errors appearing in customer invoices
* **Difficult communication:**You find it hard to communicate with customers about billing questions and disputes
* **Customer complaints:**You often receive complaints about inaccuracies and other problems pertaining to their invoices
* **Requests for digitization:** Your customers are asking you for digital invoicing and payment options
* **High costs:** Your invoicing process represents a major cost center
* **Limited talent pool:** You experience difficulties attracting and retaining top-tier AR professionals*.*

**Scan-based trading** (**SBT**):

It is the process where suppliers maintain ownership of inventory within retailers' warehouses or stores until items are scanned at the [point of sale](https://en.wikipedia.org/wiki/Point_of_sale). Suppliers, such as manufacturers or farmers, own the product until it is purchased by the customer, with the store or venue then buying the product from the supplier and reselling it to the customer. Analysts in the grocery sector estimate scan-based trading accounted for $21 billion dollars in consumer goods purchased in the grocery industry alone in 2020, or nearly 3% of overall sales.

Scan-based trading is primarily applicable to products distributed through direct store delivery, commonly referred to as DSD. The most common application of scan-based trading to DSD products involves garden seeds, DVDs/[Blu-ray Discs](https://en.wikipedia.org/wiki/Blu-ray_Disc), newspapers and magazines. Nearly all newspapers and magazines are distributed to retailers by the DSD method of distribution. According to an analysis by one vendor, most major retailers in the U.S. – including CVS, Safeway, Kroger Ahold’s divisions, A&P and its subsidiaries, Hess, Barnes & Noble and Rite Aid – conduct their newspaper business using the SBT model." According to Poff "Most [retailers] rely on a third-party partner to provide oversight.

Scan-based trading means a supplier owns inventory until scanned at POS, while pay-on-scan is similar to a consignment system. Here are the features you need for an efficient process.

## Scan-Based Trading & Pay-On-Scan Features

The similarities between the two are in the supplier keeping ownership of the goods until they're sold. Other similarities come in when we're talking about how important data synchronization is to make both processes work. When you decide to use scan-based trading, communication between you and the supplier is essential to [eliminate](https://www.icontroldata.net/blog/supervalu-earns-2015-wholesaler-of-the-year-credits-partnership-with-icontrol-for-contributing-to-succcess)discrepancies and excessive downtime. So how do you accomplish this with [scan-based trading](https://www.icontroldata.net/blog/top-5-challenges-facing-the-industry-wide-acceptance-of-scan-based-trading) and pay-on scan procedures? Take a look at the features you'll need by using right management software.

## E-Invoice Processing

When you use scan-based trading, you'll need a better connection with your suppliers to pay them when their products sell in your store. If you're still using paper invoices for payment, you are likely fighting off constant errors from the data entry department.

Having discrepancies in what you pay to your suppliers only leads to internal blame games that bring a lack of morale and more downtime. E-invoicing is the answer to this, along with using the proper management software. It's no different with pay-on-scan procedures where complete accuracy prevents your supplier from having to contact you about mistakes.

Through automation, orders get automatically placed into an e-invoice system without having to worry about manual entry.

### Better Visibility On Inventory

You need to keep up on how much inventory you need, whether [using scan-based trading](https://www.icontroldata.net/bod/robert-lipman) or [pay-on-scan](https://www.icontroldata.net/blog/how-scan-based-trading-and-pay-on-scan-differ). Without centralized management, your supplier won't know how much inventory you need at a given time to keep up with demand. This is important for either scan method since confusion can lead to a supplier not sending you enough products. Or, you may end up with too much inventory you can't use.

With UPC levels updated daily through automation, both you and the supplier can keep up with inventory levels at each store location. Both of you having transparency will save time from fixing problems that could bring more confusion from different departments

### Improved Shrink Management

Keeping on top of inventory that's been stolen or damaged is equally vital to maintain efficient scan-based trading and pay-on-scan procedures. Again, with more visibility into analytics and what's occurring in each store and warehouse, you'll never have a disconnect on what items need replacing.

Don't forget about shrink reconciliation and how important this is for accurate financial reports. Suppliers can get better shrink reconciliation when having more detailed information like driver and route information.

### Enhanced Supply Chain Analytics

Analytics and reports are essential to keep [scan-based trading](https://www.icontroldata.net/blog/the-advantages-of-scan-based-trading-for-distributors) and pay-on-scan procedures working optimally. You've probably discovered that managing inventory can be far more complex than you might have imagined. Part of this involves forecasting and planning for what kind of inventory and how much you'll be needing in the coming months.

Through analytic structures focusing on your sales trends, you can set up a plan to accommodate future demand. Since the supplier keeps ownership of your products until a sale, timing when you need your products during specific times of the year can save you even more money.

Having instant reports available also helps get everyone on the same page so suppliers can access data at all times through the cloud.