4.1 Electronic Payment Systems (EPS)

Issues of trust and acceptance play a more significant role in the e-commerce world than in traditional businesses as far as payment systems are concerned. Traditionally, a customer sees a product, examines it, and then pays for it by cash, check, or credit card (Figure 4.1). In the e-commerce world, in most cases the customer does not actually see the concrete product at the time of transaction, and the method of payment is performed electronically.

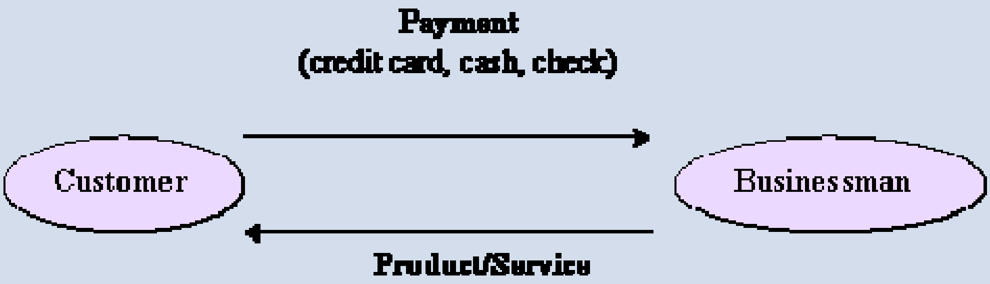


Figure 4.1 Traditional payment scheme

EPSs enable a customer to pay for the goods and services online by using integrated hardware and software systems. The main objectives of EPS are to increase efficiency, improve security, and enhance customer convenience and ease of use. Although these systems are in their immaturity, some significant development has been made. There are several methods and tools that can be used to enable EPS implementation (Figure 4.2)

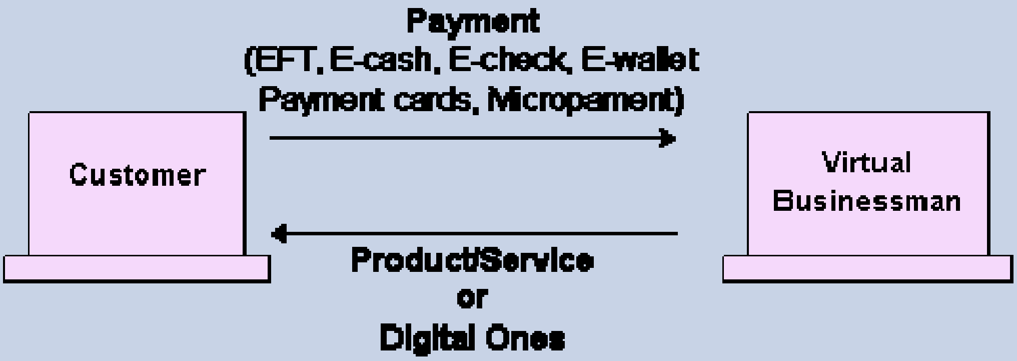


Figure 4.2 Electronic payment scheme

While customers pay for goods/services by cash, check, or credit cards in conventional businesses, online buyers may use one of the following EPSs to pay for products/services purchased online:

- Electronic funds transfer (EFT): EFT involves electronic transfer of money by financial institutions.
- Payment cards : They contain stored financial value that can be transferred from the customer's computer to the businessman's computer.
- Credit cards : They are the most popular method used in EPSs and are used by charging against the customer credit.
- Smart cards: They include stored financial value and other important personal and financial information used for online payments.
- Electronic money (e-money/e-cash): This is standard money converted into an electronic format to pay for online purchases.
- Online payment: This can be used for monthly payment for Internet, phone bills, etc.
- Electronic wallets (e-wallets) : They are similar to smart cards as they include stored financial value for online payments.
- Micro-payment systems : They are similar to e-wallets in that they include stored financial value for online payments; on the other hand, they are used for small payments, such as kurus in Turkey .
- Electronic gifts : They are one way of sending electronic currency or gift certificates from one individual to another. The receiver can spend these gifts in their favorite online stores provided they accept this type of currency.
-

Although these groups appear to be separate, there is some overlap among them. When the industry matures, this duplication in naming and function ought to be renamed. For example, *e-wallets* can be classified as *payment cards* when they are used to store credit card information or as *e-money* when they store electronic currency.

The standardization of payment mechanisms on the Internet is essential to the success of e-commerce. Businesses offering domestic and international services must have assurance that payment will be received, that it is secure and that it is valid. Addressing security issues is crucial to the acceptance of online payment standards: consumers and merchants must be able to trust that their information is kept intact and remains secure during transmission. SET and SSL are two standards that protect the integrity of online transactions.

4.2 Electroni̇c Funds Transfer (EFT)

Electronic funds transfer is one of the oldest electronic payment systems. EFT is the groundwork of the cash-less and check-less culture where and paper bills, checks, envelopes, stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. The most popular application of EFT is that instead of getting a paycheck and putting it into a bank account, the money is deposited to an account electronically. EFT is considered to be a safe, reliable, and convenient way to conduct business. The advantages of EFT contain the following:

- Simplified accounting
- Improved efficiency
- Reduced administrative costs
- Improved security

4.3 Payment Cards

Credit cards, debit cards, charge cards, smart cards are payment cards. They are the most popular tool for electronic payment transactions.

Credit Cards

There are two types of credit cards on the market today:

- Credit cards issued by credit card companies (e.g., MasterCard, Visa) and major banks (e.g. Is Bankasi, Ziraat Bankasi, Yapi Kredi, etc.)

Credit cards are issued based on the customer's income level, credit history, and total wealth. The customer uses these cards to buy goods and services or get cash from the participating financial institutions. The customer is supposed to pay his or her debts during the payment period; otherwise interest will accumulate. Two limitations of credit cards are their unsuitability for very small or very large payments. It is not cost-justified to use a credit card for small payments. Also, due to security issues, these cards have a limit and cannot be used for excessively large transactions.

- Credit cards issued by department stores (e.g Boyner), oil companies (e.g. Shell)

Businesses extremely benefit from these company cards and they are cheaper to operate. They are widely issued to and used by a broad range of customers. Businesses offer incentives to attract customers to open an account and get one of these cards.

Debit Cards

The difference between credit cards and debit cards is that in order to pay with a debit card you need to know your personal identification number (PIN) and need a hardware device that is able to read the information that is stored in the magnetic strip on the back [3].

Debit cards task similar to checks in that the charges will be taken from the customer's checking account. The benefit for the customer is the easiness of use and convenience. These cards also keep the customer under his or her budget because they do not allow the customer to go beyond his or her resources. The advantage to the merchant is the speed at which the merchant collects these charges.

Charge Cards

Charge cards are similar to credit cards except they have no revolving credit line, so the balance must be paid off every month. Credit, debit, and charge card methods of payments have been successfully utilized in the pre-Internet period, and they are often used in the e-commerce world as well. Some of the reasons for their popularity in the e-commerce world are their availability (most customers own one of these cards), ease of use, and acceptance. To use these cards as an online payment system, a well-defined process is followed. A brief description follows.

To accept payment cards payments, a merchant must have a merchant account with a bank. The buyer will be required to submit their credit-card number, expiration date and shipping and billing information when making a purchase online using a payment card. (Figure 4.3) A customer using his/her browser clicks on a product on the merchant's web site and adds it to an electronic shopping cart. The customer provides the shipping instructions and payment card information. This information is sent securely over the Internet to the merchant's commerce site (Step 1). The server software adds the merchant identification to the information transmitted. The merchant then submits this information to the acquiring bank with which the merchant holds an account (Step 2). The merchant bank transmits this information to the customer's bank for authorization. Then, the buyer's account information is verified. This involves the issuing bank from which the buyer obtained the credit card, and the credit-card association (Step 3). Verification is received by the acquiring bank (Step 4) and is passed on to the merchant (Step 5) who then ships the product (Step 6). Payment cannot be issued to the merchant until the product has been shipped. This entire process (not including shipment) takes approximately less than 30 seconds [2]!

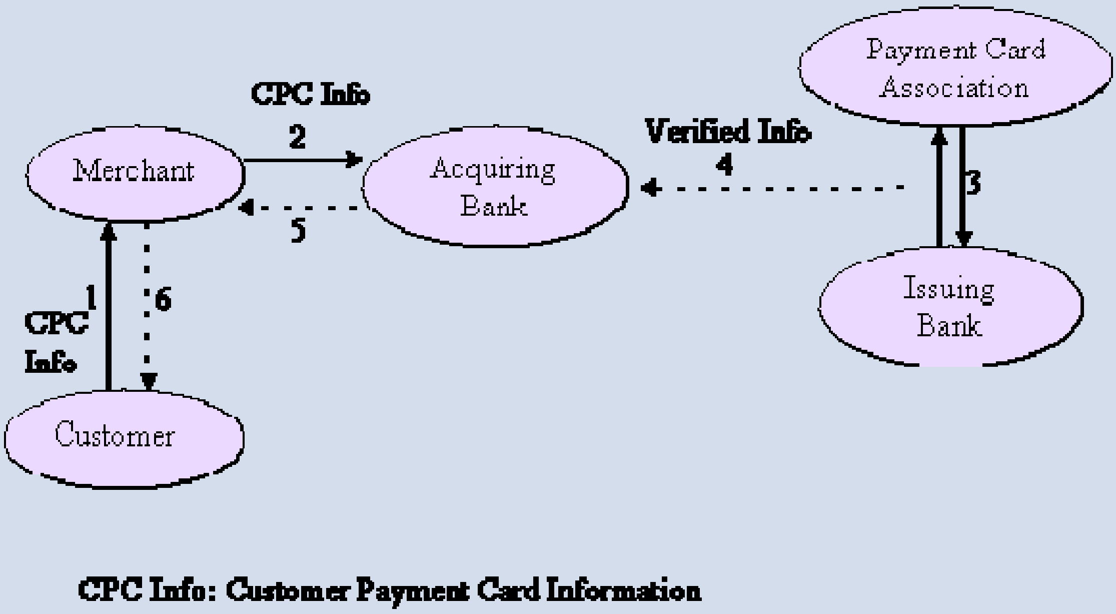
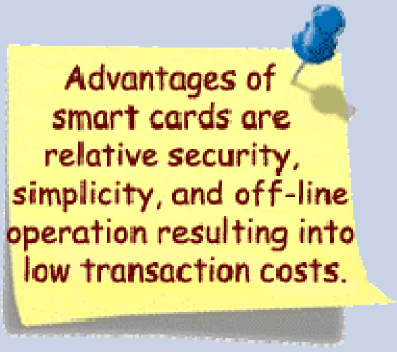


Figure 4.3 Basic steps in an online payment card deal

Smart Cards

A smart card is about the size of a credit card, made of a plastic with an embedded microprocessor chip that holds important financial and personal information. The microprocessor chip is loaded with the relevant information and periodically recharged. In addition to these pieces of information, systems have been developed to store cash onto the chip. The money on the card is saved in an encrypted form and is protected by a password to ensure the security of the smart card solution. In order to pay via smart card it is necessary to introduce the card into a hardware terminal. The device requires a special key from the issuing bank to start a money transfer in either direction. Smart cards can be disposable or rechargeable. A popular example of a disposable smart card is the one issued by telephone companies. After using the pre-specified amount, the card can be discarded.



Advantages of smart cards are relative security, simplicity, and off-line operation resulting into low transaction costs.

Smart cards have been extensively used in the telecommunications industry for years. Smart-card technology can be used to hold information on health care, transportation, identification, retail, loyalty programs and banking, to name a few. Smart cards enable information for different purposes to be stored in one location. The microprocessor chip can process different types of information, and therefore, various industries use them in different ways. Due to their multipurpose functions, their popularity in Turkey is also on the rise.

Smart cards are broadly classified into two groups:

Contact: This type of smart card must be inserted into a special card reader to be read and updated. A contact smart card contains a microprocessor chip that makes contact with electrical connectors to transfer the data.

Contact-less: This type of smart card can be read from a short distance using radio frequency. A contact-less smart card also contains a microprocessor chip and an antenna that allows data to be transmitted to a special card reader without any physical contact. This type of smart card is useful for people who are moving in vehicles or on foot. They are used extensively in European countries for collecting payment for highway tolls, train fares, parking, bus fares, and admission fees to movies, theaters, plays, and so forth.

Smart cards can accommodate a variety of applications that allow the customer to make purchases from a credit account, debit account, or stored value on the card. These cards can even have multiple applications operating at the same time. The customer, for example, could have a frequent flyer program working on the same card as the customer debit or credit account. This enables the customer to earn points in his or her favorite program.

Several computer manufacturers (e.g. Compaq) are developing keyboards that include smart card slots that can be read like bank credit cards. A smart card can be programmed for different applications. Some cards contain programming and data to support multiple applications, and some can be updated with new applications after they are issued. IBM, Microsoft, Schlumberger, and Bull are among the major players in smart card development and utilization [1].

Some of the advantages of smart cards include the following:

- Stored many types of information
- Not easily duplicated
- Not occupy much space
- Portable
- Low cost to issuers and users
- Included high security

The disadvantages of smart cards are the lack of universal standards for their design and utilization. On the other hand, smart card applications are expected to increase as a result of the resolution of these disadvantages in the near future.

4.4 ELECTRONİC CASH (E-CASH)

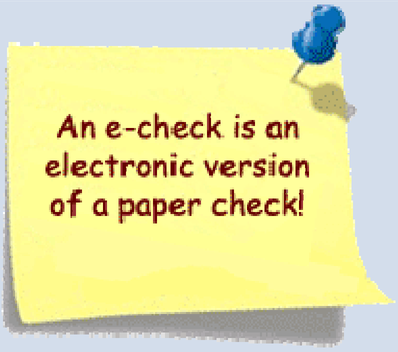
Similar to regular cash, e-cash enables transactions between customers without the need for banks or other third parties. When used, e-cash is transferred directly and immediately to the participating merchants and vending machines. Electronic cash is a secure and convenient alternative to bills and coins. This payment system complements credit, debit, and charge cards and adds additional convenience and control to everyday customer cash transactions. E-cash usually operates on a smart card, which includes an embedded microprocessor chip. The microprocessor chip stores cash value and the security features that make electronic transactions secure. Mondex, a subsidiary of MasterCard (Mondex Canada Association) is a good example of e-cash. (Appendix I)

E-cash is transferred directly from the customer's desktop to the merchant's site. Therefore, e-cash transactions usually require no remote authorization or personal identification number (PIN) codes at the point of sale. E-cash can be transferred over a telephone line or over the Web. The microprocessor chip embedded onto the card keeps track of the e-cash transactions. Using e-cash the customer has two options: a stand-alone card containing e-cash or a combination card that incorporates both e-cash and debit .

How a typical e-cash system works: A customer or merchant signs up with one of the participating banks or financial institutions. The customer receives specific software to install on his or her computer. The software allows the customer to download “electronic coins” to his or her desktop. The software manages the electronic coins. The initial purchase of coins is charged against the customer's bank account or against a credit card. When buying goods or services from a web site that accepts e-cash, the customer simply clicks the “Pay with e-cash” button. The merchant's software generates a payment request, describing the item(s) purchased, price, and the time and date. The customer can then accept or reject this request. When the customer accepts the payment request, the software residing on the customer's desktop subtracts the payment amount from the balance and creates a payment that is sent to the bank or the financial institution of the merchant, and then is deposited to the merchant's account. The attractive feature of the entire process is its turnaround time which is a few seconds. The merchant is notified and in turn ships the goods.

4.5 Electronic Checks (E-Check)

E-check is the result of cooperation among several banks, government entities, technology companies, and e-commerce organizations. An e-check uses the same legal and business protocols associated with traditional paper checks. It is a new payment instrument that combines high-security, speed, convenience, and processing efficiencies for online transactions. It shares the speed and processing efficiencies of all-electronic payments. An e-check can be used by large and small organizations, even where other electronic payment solutions are too risky or not appropriate. The key advantages of e-checks are as follows:



- Secure and quick settlement of financial obligations
- Fast check processing
- Very low transaction cost

E-check is being considered for many online transactions. Appendix II shows an e-check transaction.

4.6 Electronic Wallets (E-Wallets)

Electronic wallets being very useful for frequent online shoppers are commercially available for pocket, palm-sized, handheld, and desktop PCs. They offer a secure, convenient, and portable tool for online shopping. They store personal and financial information such as credit cards, passwords, PINs, and much more.

Electronic wallets allow higher speed and efficiency for online shoppers!

To facilitate the credit-card order process, many companies are introducing electronic wallet services. E-wallets allow you to keep track of your billing and shipping information so that it can be entered with one click at participating merchants' sites. E-wallets can also store e-checks, e-cash and your credit-card information for multiple cards.

A popular example of an e-wallet on the market is ***Microsoft Wallet*** . To obtain Microsoft Wallet, one needs to set up a Microsoft Passport. After establishing a Passport, a Microsoft e-wallet can be established. Then, e-wallets can be used for micro-payments. They also eliminate reentering personal information on the forms, resulting in higher speed and efficiency for online shoppers. Microsoft Passport consists of several services including the following [5]: A single sign-in, wallet and kids passport services. A single sign-in service allows the customer to use a single name and password at a growing number of participating e-commerce sites. The shopper can use to make fast online purchases with a wallet service. Kids' passport service helps to protect and control children's online privacy.

4.7 MİCRO-PAYMENT

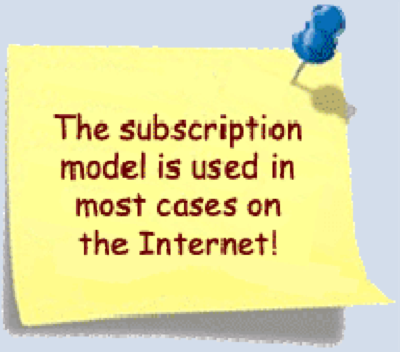
Merchants must pay a fee for each credit-card transaction that they process; this can become costly when customers purchase inexpensive items. The cost of some items could actually be lower than the standard transaction fees, causing merchants to incur losses. Micro-payments are used for small payments on the Web. The process is similar to e-wallet technology where the customer transfers some money into the wallet on his or her desktop and then pays for digital products by using this wallet. Using micro-payment one will be able to pay for one article from a professional journal, a chapter from a scientific book, or one song from a CD on the Web.

There are many vendors involved in micro-payment systems. **IBM** offers micro-payment wallets and servers. IBM micro-payment systems allow vendors and merchants to sell content, information, and services over the Web. It provides universal acceptance and offers comprehensive security. This micro-payment system can be used for billing by banks and financial institutions, Internet service providers (ISPs), content providers (offering games, entertainment, archives, etc.), telecommunications, service providers (offering fax, e-mail, or phone services over the Web), and by premium search engines and specialized databases.

Figure 4.4 The initial screen of Qpass.

A number of companies will allow for outsourcing the payment-management systems. Many of these systems can handle multiple payment methods including micro-payments. **Qpass** is an example of a company that can manage micro-payments for pay-per-download, subscription-based and pay-per-click systems. Qpass enables periodicals such as *The New York Times* and *The Wall Street Journal* to offer subscriptions over the Web. Customers who buy products and services through a Qpass-enabled company receive monthly bills that include descriptions of all purchases made during that month. Additional services offered by Qpass include the Qpass Power Wallet, which registers passwords, credit-card information and other preferences necessary to make online transactions more efficient customer service marketing and sales assistance (Figure 4.4).

Psychology at Micro-payment: Many developers have tried to push micro-payment solutions to the Internet, but only very few have succeeded. The difficulty was never the technical implementation but the Internet itself. Every company on the Internet gives away small pieces of information for free. Thus it is hard to validate the need to pay for small bits of information. The other issue is a psychological difficulty .


The subscription model is used in most cases on the Internet!

If you have the choice of paying a one-time fee of 20 YTL or paying 50 kurus for every transaction, about 80 percent of the people will either pay the one-time fee or use the service only very seldom as it requires a new payment each time. It makes financial calculations more difficult as you do not know in advance how much money the service will cost and spending money means always thinking about it for a while. Most people will prefer to think once about it and use the system as often as they need it. Otherwise they will first think about the costs and how they can be justified and then decide maybe not to use it [3]. Examples to Micro Payment Systems are given in Appendix III.

4.8 Peer-to-Peer Payments

A peer-to-peer payment service allows the transfer of digital cash (e-Cash) via e-mail between two people who have accounts at e-Cash-enabled banks. Peer-to-peer transactions allow online financial transfers between consumers. One example of peer-to-peer payment service is **PayPal** . Transactions through PayPal are immediate, the service is free for individuals sending money to one another and the payee is not required to enter any credit-card information. Businesses pay a small transaction fee.

PayPal offers a digital-payment system!

PayPal allows a user to send money to anyone with an e-mail address, regardless of what bank either person uses, or whether or not the recipient is pre-registered with the service. People wishing to send money to others can log on to PayPal at www.x.com open an account and register the amount to be sent. That amount is hilled to the person's credit card, Payment notification is sent to the recipient, and an account is established in the recipient's name. When the person to whom the payment is sent receives the e-mail notification, he or she simply registers with PayPal and has access to an account containing the payment. The funds in this account can he transferred to the recipient's bank account by direct deposit or mailed by check from PayPal.

The Paypal system can also be used to enable credit-card payment for auction items in real time. Credit card information is checked before a transaction is initiated. This means that the transaction begins processing immediately after it is initiated, reducing the risk of fraud or overdrawn accounts. The buyer or the seller can initiate the service. If one refers someone to PayPal the person will receive a small monetary reward. More information on PayPal can be found at Appendix IV.

4.9 B2B and B2C Transactions

The fastest grossing sector of e-commerce payments is business-to-business (B2B) transactions. These payments are often much larger than business-to-customer (B2C) transactions and involve complex business accounting systems [10]. For example, Paymentech [11] is one of the largest payment solutions providers for point-of-sale transactions on the Internet. The service provides reporting and processing tools and services to help manage a merchant account and electronic check processing. Paymentech supports all types of credit and debit cards and conducts all transactions in a secure environment. Merchants using Paymentech can customize their payment-processing plans. PaymentNet allows merchants to track their expenses in a secure environment on a 24-by-7 basis. Its features include custom reporting, e-billing and cross-compatibility with other third-party expense reporting tools.

B2C market transactions are less complicated than B2B transactions. Using Electronic Bill Presentment and Payment (EBPP) a company can display a bill on multiple platforms online and offer actual payment processes. Payments are generally electronic transfers from consumer checking accounts. This is conducted through the ACH (Automated Clearing House), the current method for processing electronic monetary transfers. You can look at http://www.checkfree.com for different related information.

4.10 Secure EPS Infrastructure

Secure electronic funds transfer is crucial to e-commerce. In order to ensure the integrity and security of each electronic transaction and other EPSs utilize some or all of the following security measures and technologies directly related to EPSs: *Authentication, public key cryptography, digital signatures, certificate, certificate authorities, SSL, S-HTTP, secure electronic transmission (SET).*

Authentication

This is the process of verification of the authenticity of a person and/or a transaction. There are many tools available to confirm the authenticity of a user. For instance, passwords and ID numbers are used to allow a user to log onto a particular site.

Public Key Cryptography

Public key cryptography uses two keys , one public and one private , to encrypt and decrypt data, respectively. Cryptography is the process of protecting the integrity and accuracy of information by encrypting data into an unreadable format, called cipher text. Only those who possess a private key can decrypt the message into plain text.

Public key cryptography uses a pair of keys, one private and one public. In contrast, private key cryptography uses only one key for encryption. The advantage of the dual-key technique is that it allows the businesses to give away their public key to anyone who wants to send a message. The sender can then encrypt the message with the public key and send it to the intended businessman over the Internet or any other public network; the businessman can then use the private key to decrypt the message. Obviously, the private key is not publicly known [6].

Digital Signature

Rather than a written signature that can be used by an individual to authenticate the identity of the sender of a message or of the signer of a document; a digital signature is an electronic one. E-check technology also allows digital signatures to be applied to document blocks, rather than to the entire document. This lets part of a document to be separated from the original, without compromising the integrity of the digital signature. This technology would also be very useful for business contracts and other legal documents transferred over the Web.

A digital signature includes any type of electronic message encrypted with a private key that is able to identify the origin of the message. The followings are some functions of digital signature.

- **The authentication function:** The term digital signature in general is relevant to the practice of adding a string of characters to an electronic message that serves to identify the sender or the originator of a message.
- **The seal function:** Some digital signature techniques also serve to provide a check against any alteration of the text of the message after the digital signature was appended.
- **The integrity function:** This function is of great interest in cases where legal documents are created using such digital signatures.
- **The privacy function:** Privacy and confidentiality are of significant concerns in many instances where the sender wishes to keep the contents of the message private from all hut the intended recipient

Certificate

A certificate can be thought of as similar to a driver's license!

A driver’s license is accepted by numerous organizations both public and private as a form of identification due to the legitimacy of the issuer, which is a government agency. Since organizations understand the process by which someone can obtain a driver’s license, they can trust that the issuer verified the identity of the individual to whom the license was issued. A certificate provides a mechanism for establishing confidence in the relationship between a public key and the entity that owns the corresponding private key.

Certificate Authorities

Certificate authorities are similar to a notary public, a commonly trusted third party. In the e-commerce world, certificate authorities are the corresponding of passport offices in the government that concern digital certificates and validate the holder’s identity and authority.

Secure Sockets Layer (SSL)

Secure Sockets Layer transmits private documents via the Internet . SSL uses a cryptographic system that uses two keys to encrypt data - a public key known to everyone and a private or secret key known only to the recipient of the message. It operates between the transport and the application layers in the network stack and uses both public and private key cryptography. You can look at Appendix V for more information about OSI layers.

SSL is a protocol developed by Netscape Corporation

By convention, URLs that require an SSL connection start with https: instead of http: [7]. All the major web server vendors, including Microsoft (Internet Explorer) and Netscape (Netscape Navigator), support SSL. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers. Microsoft's current lines of e-commerce-related products and services can be seen at Appendix VI.

SSL provides a relatively secure method to encrypt data that are transmitted over a public network such as the Internet, also offers security for all Web transactions, including file transfer protocol (FTP), HTTP, and Telnet-based transactions. It provides an electronic wrapping around the transactions that go through the Internet. The open and nonproprietary nature of SSL is what makes it the preferred choice for TCP/IP application developers for securing sensitive data. The protocol is vulnerable to attacks on the SSL server authentication. Despite its vulnerabilities, when properly implemented, SSL can be a powerful tool for securing Web-sensitive data. SSL offers comprehensive security by offering authentication and encryption at the client and server sides. Authentication begins when a client requests a connection to an SSL server. The client sends its public key to the server, which in turn generates a random message and sends it back to the client. Then, the client uses its private key to encrypt the message from the server and sends it back. All the server has to do at this point is decrypt the message using the public key and compare it to the original message sent to the client. If the messages match, then the server knows that it is from the client communicating with the intended client.

To implement SSL in a web server, the following steps are followed:

1. Create a key pair on the server.
2. Demand a certificate from a certification authority.
3. Set up the certificate.
4. Activate SSL on a security folder or directory. It is not a good idea to activate SSL on all the directories because the encryption overhead created by SSL decreases system performance.

Advantages of SSL : Some of the advantages of SSL contain the following:

- *Authentication:* Permits Web-enabled browsers and servers to authenticate each other.
- *Access Limit:* Permits controlled access to servers, directories, files, and services.
- *Data Protection :* Guarantees that exchanged data cannot be corrupted without detection.
- *Information Share:* Permits information to be shared by browsers and servers while remaining out of reach to third parties.

Disadvantages of SSL: Some of the disadvantages of SSL contain the following:

- *Simple Encryption:* This might increase the chances of being hacked by computer criminals.
- *Stolen Certificate/Key:* One important drawback of SSL is that certificates and keys that originate from a computer can be stolen over a network or by other electronic means.
- *Point-to-Point Transactions:* SSL handles only point-to-point interaction. Credit card transactions involve at least three parties: the consumer, the merchant, and the card issuer. This limits its all-purpose applications.
- *Customer's risk:* Customers run the risk that a merchant may expose their credit card numbers on its server; in turn, this increases the chances of credit card frauds.
- *Merchant's risk:* Merchants run the risk that a consumer's card number is false or that the credit card won't be approved.
- *Additional overhead:* The overhead of encryption and decryption means that secure HTTP (SHTTP) is slower than HTTP.

Secure Hypertext Transfer Protocol (S-HTTP)

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP) . Whereas SSL creates a secure connection between a client and a server , over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

Secure Electronic Transmission (SET)

The Secure Electronic Transmission protocol imitates the current structure of the credit card processing system. SET replaces every phone call or transaction slip of paper with an electronic version. This can generate a large number of data packets. The SET protocol offers packets of data for all these transactions, and each transaction is signed with a digital signature. This makes SET the largest consumer of certificates, and it makes banks by default one of the major distributors of certificates.

Certificate revocation is an essential part of the certificate process. Who will pay for the SET certificate-revocation list is one of the most active debates in the SET community. When a user might change organizations or lose his or her key pair, or an e-commerce site using SSL may discontinue its operations; a certificate must be revoked before it expires. In all these cases, the certificate needs to be revoked before it expires so that it cannot be used intentionally or unintentionally.

The privacy of messages in the SET payment environment is accomplished through encryption of the payment information using a combination of public key and private key algorithms. In general, public and private key cryptographic algorithms are the process of transforming readable text into cipher-text and back again. These algorithms are used together to encrypt the actual message contents with a short private key, which is distributed securely via the public-private key pair.

The most important property of SET is that the credit card number is not open to the seller. On the other hand, the SET protocol, despite strong support from Visa and MasterCard, has not appeared as a leading standard. The two major reasons for lack of widespread acceptance are followings:

(1) The complexity of SET

(2) The need for the added security that SET provides.

Though, this might change in the future as encryption technology becomes more commonly utilized in the e-business world.

Advantages of SET: Some of the advantages of SET contain the following:

- *Information security:* Neither anyone listening in nor a merchant can use the information passed during a transaction for fraud.
- *Credit card security:* There is no chance for anybody to steal a credit card.
- *Flexibility in shopping:* If a person has a phone he/she can shop.

Disadvantages of SET: Some of the disadvantages of SET include its *complexity* and *high cost for implementation.*

Appendix I

Commercial Example of Electronic Payment Systems: Mondex E-Cash [1]

Mondex e-cash is an example of e-cash that provides a secure and convenient alternative to bills and coins. The Mondex e-cash payment system complements credit, debit, and charge cards and adds greater convenience and flexibility to everyday customer cash transactions. Mondex e-cash operates on a smart card.The microprocessor chip on the card stores cash value and the security features. Similar to cash, Mondex e-cash transactions require no remote authorizations or PIN codes at point-of-sale terminals because Mondex e-cash is transferred directly from the buyer to the seller. Mondex e-cash can be reloaded onto the card's microprocessor chip as frequently as desired. Customers can request either a standalone card containing Mondex e-Cash or a combination card that incorporates both Mondex e-cash and debit.

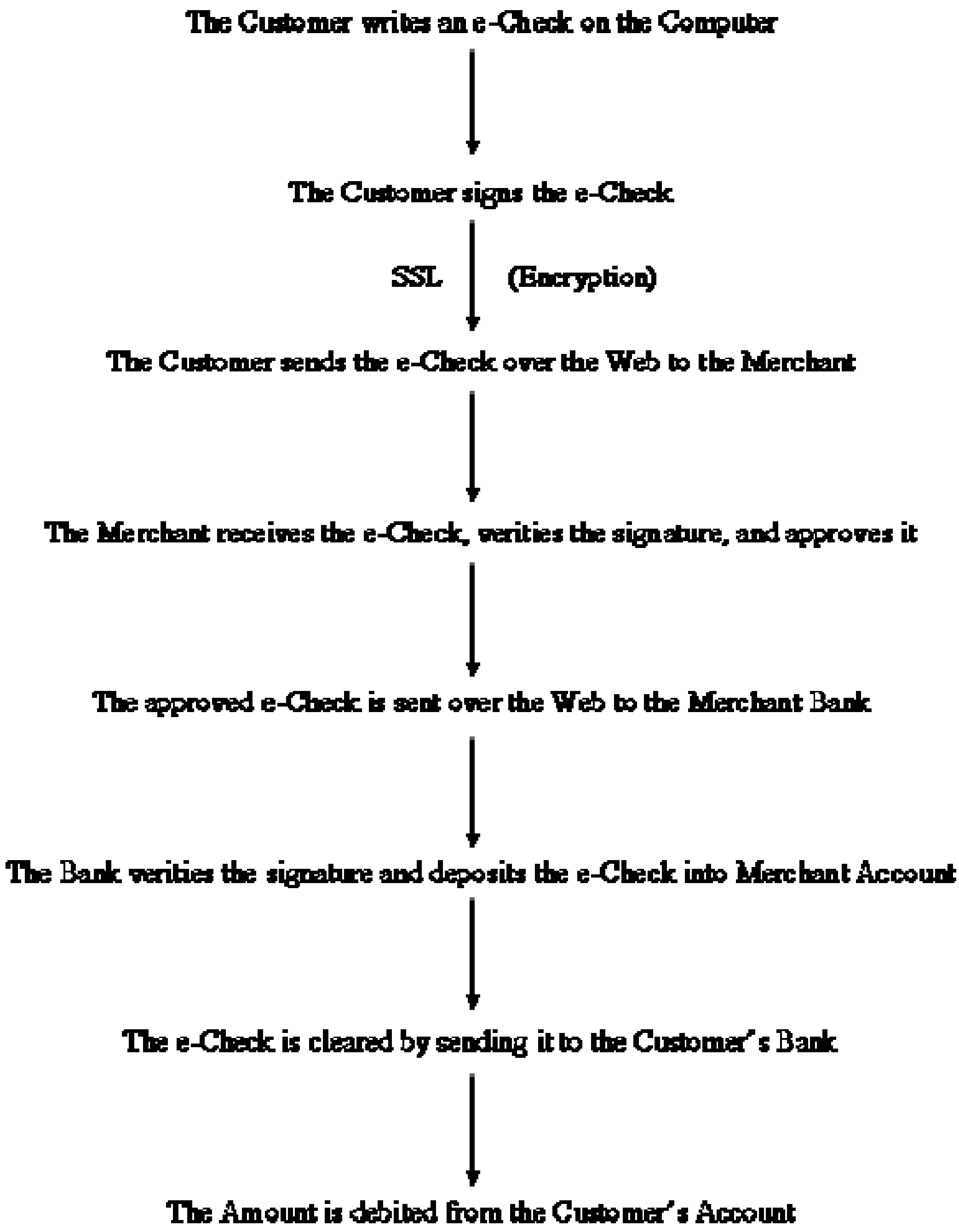
The Mondex e-cash function can be issued on its own or, soon, as part of a group of products on a multifunction card. The MULTOS (multipurpose operating system) smart card operating system makes this possible, allowing the card issuer and cardholder to combine a number of services on a single card that meets the specific lifestyle requirements of the customer. For example, the cardholder might choose to have one card that combines Mondex e-cash, debit, credit, and various retailer loyalty programs, all in one. Mondex e-Cash offers several advantages:

- It can be transferred over a telephone line or over the Web.
- The microprocessor chip maintains a private and up-to-date receipt of the card's last ten Mondex transactions.
- E—cash can be locked onto the card's microprocessor chip with a code chosen by the customer. When locked, the cash value stored on the card and the card's transaction records cannot be accessed.
- When used, e-cash is transferred directly and immediately to the merchant, vending machine, or other participating organizations.
- Like cash, e-cash enables transactions between individuals without the need for banks or other third-party intervention.

Appendix II

An e-check transaction [1]

(SSL: Secure Sockets Layer**)**



The Customer writes an e-Check on the Computer

The Customer signs the e-Check

SSL (Encryption)

The Customer sends the e-Check over the Web to the Merchant

The Merchant receives the e-Check, verifies the signature, and approves it

The approved e-Check is sent over the Web to the Merchant Bank

The Bank verifies the signature and deposits the e-Check into Merchant Account

The e-Check is cleared by sending it to the Customer's Bank

The Amount is debited from the Customer's Account

Appendix III

Examples of micro-payment systems [1]

1ClickCharge assists customers to download a wallet and prepay for a block of micro-purchases by credit card. www.1clickcharge.com

Flooz is an online gift currency sent by e-mail. The recipient spends Flooz, just like money, at the online store of their choice. www.flooz.com

Trintech provides customers with simple and secure e-commerce payment instruments. www.trintech.com

AuricWeb system allows ISPs to document online transactions along with other user statistics. www.auricweb.com

Clickshare is another popular micro-payment system. Using Clickshare the customer can purchase information, music, video, software, and other digital products and services over the Web. You get one bill from a Clickshare service provider that you choose. www.clickshare.com

Beenz, E-gold, and **Mypoints** are other examples of currency used in the e-commerce world. www.beenz.com , www.egold.com , www.mypoints.com

Electronic gifts are one way of sending electronic currency or gift certificates from one individual to another. Electronic gifts are similar to regular gifts only they are transferred on the Web from the sender to the receiver. Electronic gifts are available from just about all major online stores, and their acceptance is on the rise. Paid for by credit card, they are usually nontransferable. Flooz, PayPal, are examples of electronic gifts. PayPal transfer funds to a recipient chosen by the sender. To use PayPal, the user is supposed to establish an account. Also, PayPal charges a service fee. These options are only practical for transferring a small amount of money without the recipient using or obtaining a credit card. www.flooz.com , www.paypal.com

Appendix IV

PayPal [4]

October 1999 saw the modest launch of a simple home page that would grow into one of the Internet's major success stories - a person-to-person payment (P2P) network called PayPal. As with many success stories, the growth of this good idea started with a slightly different and less successful proposition, and within a few months of its launch, had begun its heady rise in attracting millions of customers at amazing rates.

Peter Theil and fellow co-founder Max Levchin had teamed up in 1998 (aged 30 and 26 respectively) to start a company called Field Link that specialized in providing encryption software for wireless devices. The technology had nurtured the concept of moving money using devices such as palm-pilots. Theil (CEO of PayPal) was a chess-loving intense libertarian that had studied law at Stamford University . When approached by Levchin (CTO of Paypal), he was running a hedge fund.

Demand for their initial concept was sparse and the company changed direction to other areas as well as renaming itself Confinity. It was at that point that an application called PayPal was born; allowing users of handheld devices to beam money to each other. The company had a strong start with a capital investment of $3 million from Nokia. Despite this initial success, the original idea did not blossom and in 1999, both increasingly realized that there was not an easy way of making a payment on the Internet. Additionally, not everyone had a wireless device such as a palm-pilot, but almost all net users did have an e-mail address.

From these modest beginnings, a Web version of the PayPal application followed and started trading using established networks - e-mail and a universal currency, the US Dollar — whilst building a new person-to-person network platform. Without a doubt, one of the key observations and drivers were online auctions, such as eBay, which PayPal launched its service on in early 2000.Thiel had noted that as late as 1998, almost 90% of eBay's transactions were settled with checks or money orders.

The concept was simple. Money would be exchanged via cyberspace - all users needed was an e-mail address, a credit card or bank account number and an Internet connection. Recipients of funds would receive money in a new account (if they did not already have one) and PayPal would debit the sender's account (credit card or bank account) respectively. Anyone who received money therefore automatically became a new PayPal client.

The viral growth of PayPal was breathtaking. By end of 1999 there were 10,000 users. Two months later, that number was 100,000. By using confidence pricing techniques (the service was effectively free initially, with revenues being garnered from the cash locked into the PayPal system) new users were attracted to the service. Even when pricing models were introduced, these were much more attractive than those levied by the credit card companies. In March 2000, X.com merged with PayPal electing to ditch its banking business and its brand name in favour of the PayPal service.

At the time security was a continual area of focus, however Paypal was one of the propositions that forged ahead without the authentication of sellers. Although this afforded first mover advantages, the company had to work hard on enhancing risk management techniques and providing greater focus on authenticating sellers at the site.
Although eBay continued to be one of PayPals largest partner sites (generating approx 60% of revenues), it was already connected to over 2.6 million merchants and continued to grow at a fast pace. 15th February 2002 was also a significant day for PayPal as it went public, raising another $90 million with its shares surging 54% on the first day of trading, despite the downturn in the dotcom boom.