# CHAPTER 5

# CONTROL IDENTIFICATION FOR E-COMMERCE PAYMENT SECURITY

## INDEX

## 5.1 INTRODUCTION

The approach of the IS Auditor to an audit, including an audit of e-commerce (EC) payment security is (CISA, 2001); (Perry, 1983); (SAICA, 1998) firstly to gather information related to the area being audited. Secondly, to identify the risks prevalent in the environment being audited, and thirdly, to identify possible controls that, if implemented, will mitigate the identified risks. The last step is to develop an audit approach to serve as a framework for the area under review. These steps are designed so that there is an inter-dependency between the steps. The output of each step will serve as the input of the following step. For example, the controls identification process cannot take place effectively without the risks being identified.

In chapter 3, information was provided to serve as background to EC payment security. In that chapter an introduction was also given to the risks in EC payment systems. Chapter 4 provided more detail regarding security and the risks around EC payments. This chapter will address the possible controls that, if implemented, will mitigate the risks. This is an essential step for the IS auditor, because, without this control identification process, the IS auditor cannot develop an audit program.

The objectives of this study is to provide background information for the IS auditor when auditing EC payment security and ultimately to develop an audit approach for this area. The controls identification process therefore serves a twofold purpose. Firstly, from the audit approach highlighted above, it is clear that the control identification process is essential before the approach can be developed. Secondly, the control identification process also assists the auditor in obtaining a better understanding of the technology available to address the risks prevalent in the EC payment security environment.

Once the possible controls have been identified as described in this chapter, the next step will be to combine the risk and control identification processes to provide the foundation that will enable the IS auditor to formulate the audit approach for the audit of EC payment security.

This Chapter is structured as follows:

1 Firstly provide an understanding of control and the role of controls in an organisation;

2 secondly, controls will be identified for each of the risk areas identified in chapter 4; and

3 thirdly, the technology available to provide the controls will be explained in more detail.

With the knowledge obtained in this chapter and the previous chapter, the IS auditor is able to identify the risks, identify possible controls to mitigate the risks, and develop an audit approach.

## 5.2 CONTROLS DEFINITION

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. According to ISACA (1999): "Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide. Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources." "Internal control system provides the discipline, consistency, and guidance to carry out organisation's mission and objectives" (Vallabhaneni, 1991).

Internal control (BC, 2001); (CICA, 1986); (Ams, 2001); (Vallabhaneni, 1991); (ISACA, 1999) comprises the plans, policies, practices, organisational structures, and procedures of an organisation and all the coordinate systems established by the management of the enterprise to assist in achieving management's objectives in the following categories:

- Safeguard its assets and records (Vallabhaneni, 1991); (Ams, 2001); (CICA, 1986); (Cooper, 1982),

- Verify the accuracy and reliability of its accounting data. (Ams, 2001); (BC, 2001), (CICA, 1986); (Cooper, 1982),
- Provide relevant (e.g. strategic, operational, tactical) information to management. (Ams, 2001),
- Promote operational efficiency and system economy and effectiveness. (Ams, 2001); (BC, 2001), (CICA, 1986),
- Encourage adherence to prescribed managerial policies, procedures, and standards. (Ams, 2001), and
- Comply with laws and regulations. (Ams, 2001); (BC, 2001).

Internal controls should also help recover from disasters of any kind (Vallabhaneni, 1991). According to Pomeranz (1992) "Internal control is management's procedure for addressing risk". Information systems control form part of the entity's internal control system. An entity's internal control system is composed of a number of individual controls. A control is described as "a procedure or a set of procedures that, individually or in combination with other controls, can assist in achieving the internal control objectives of the entity" (CICA, 1986).

Internal controls are either detective, corrective, or preventive by nature (Vallabhaneni, 1991); (Ams, 2001). Detective controls are designed to detect errors or irregularities that may have occurred. Corrective controls are designed to correct errors or irregularities that have been detected. Preventive controls are designed to keep errors or irregularities from occurring in the first place.

According to ISACA (1999):

> "Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same "leap frog" manner as the underlying computing and networking technologies are evolving. Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfill their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise

reasonable and prudent judgments in evaluating control practices found in typical business or governmental organisations."

According to the AARF (2000): "Although an IT security infrastructure and systems controls can help to manage risks, there is a degree of uncertainty which cannot be eliminated. For example, the use of evolving technology, and the risk of determined hackers overriding security means that some residual risk will remain despite controls put in place by the entity. Management decides on the level of acceptable risk to balance costs and benefits in the control system relating to e-com."

"Security isn't a technology problem, but a business problem" (PWC, 2000). Even with the best controls and mitigation strategies, there is still risk. Internet transactions can be made relatively secure but security to prevent unauthorised access is highly complex and technical, and residual risks mean that the risk of unauthorised access cannot be completely eliminated. Residual risk relates to that aspect of risk which remains after security controls have been implemented, and which arise in a dynamic electronic environment (AARF, 2000); (Lindner, 2001). For example, controls in place may become less effective as new technologies are introduced.

A total information security solution includes policy and procedure, access control, user authentication, encryption, and content security. The security of transactions over the Internet may be established by the implementation of various security measures or controls to address different risks. For example, security measures include encryption, digital signature or digital certificates (or public key encryption which collectively supports a digital certificate-based encryption system), firewalls, secure socket layers, etc. All these control aspects will be described in more detail in this chapter.

By focusing a security solution on an individual component, such as access control or an encryption method, there is a risk of leaving holes in the security shield that are available to be exploited by a hacker.

Approaching security as a concept and not as individual components is therefore the best way to develop and implement secured network environments. As shown in the above descriptions, the IS auditor needs to be aware of the evolving technologies due to the fact that with the changes required by the new technology, new risks are introduced and new controls are therefore required. The technologies highlighted in this chapter will enable the IS auditor to understand the technology and identify possible controls in EC payment security audit environments.

## 5.3 ELECTRONIC COMMERCE CONTROLS BY RISK AREA

According to Mehta (1999) "the threats faced by business conducted through the Internet are not the same as those faced by storefront operations. Differences are in method, scale and geographical area." Keeping up with the risks in the Internet environment is challenging due to the Internet technology moving at a rapid pace. The technology has also not been used for extended periods of time and is therefore considered "not mature". "In addition, developments are typically made without careful consideration to security" (Mehta, 1999). In Chapter 4 on Risk, the following threats were identified:

- Breach of confidentiality
- Data alteration/integrity
- Unauthorised access
- Non-repudiation
- Denial of service
- Authentication
- Client and web-side vulnerabilities

The controls to minimise these threats will be covered in the remainder of Section 5.3 and also in Section 5.4. It is important for IS auditors to understand the controls available so that the IS auditors will be able to identify the controls applicable in each environment where they are involved in the audit of security of EC payments. Section 5.4 below highlights the controls available to address the risk.

### 5.3.1 INTERNET SECURITY ISSUES - PRIVACY AND CONFIDENTIALITY

Confidentiality is a security property that ensures that data is disclosed only to those authorized to use it, and that it is not disclosed to unauthorised parties (Techguide, 2000); (Dekker, 1997); (E-witness, 2001). This also means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, card expiration dates, and so on (Asokan et al, 1997); (VISA, 1997). This information provides the key elements needed to create counterfeit cards and/or fraudulent transactions. The reason behind ensuring the confidentiality of information on the network is to deny information to anyone who is not specifically authorized to see it or use it and to ensure that information is not intercepted during transmission (Techguide, 2000); (Verisign, 1999).

Encryption is a frequently used mechanism for guaranteeing confidentiality (Techguide, 2000); (Rapp, 2001); (VISA, 1997); (Netscape, 2001); (E-witness, 2001); (Mackey & Gossels, 2000), since only those recipients who have access to the decrypting key are able to decode the messages. Encryption will be discussed in Section 5.4.1 below in more detail as one of the tools for controlling Internet payments.

### 5.3.2 INTEGRITY

Integrity refers to the completeness and reliability of the message as it passes through the network. The key is to make sure that the data passes from the source to the destination without alteration and to prove that information has not been manipulated (Techguide, 2000); (VISA, 1997); (Verisign, 1999); (Dekker, 1997); (E-witness, 2001); (IEC, 2000).
Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions (VISA, 1997). If any component is altered in transit, the transaction will not be processed accurately. To eliminate this potential source of fraud and/or error, a means must be provided to ensure that the contents of each order and payment message received matches the contents of the message sent.

The integrity of data in storage and in transit is assured through encryption and the use of digital certificates/signatures (Norton, 2000); (VISA, 1997); (E-witness, 2001); (Mackey & Gossels, 2000). Encryption, digital certificates, and digital signatures will be discussed in more detail in Section 5.4 below.

### 5.3.3 ACCESS CONTROL AND AUTHORISATION

Authorisation relates to the aspect of accepting or rejecting a particular requester to have access to some service or data in any given system (Techguide, 2000); (Kabay, 1998); (Dekker, 1997). In this context a requester could be a user, program or process; a service could be a program, a device such as a printer or a file system;

and data could be a text file, an image, a collection of files, or any combination of the above. For example, authorisation takes place every time a merchant queries VISA or MasterCard service to see if a customer is authorised to spend a certain amount of money at their establishment.

The risks involved in allowing access to individuals to system services or information must be considered. For example, in the case of advertising the Web page of an organization, allowing access means that limited damage could occur. The objective cf such a page is to spread the word about the organization, and therefore access control is not an issue. On the other hand, access control is a major issue if someone requests access to the file, which contains the passwords of all of the users of the system. It is therefore necessary to define a set of access rights, privileges, and authorizations, and assign these to appropriate people within the domain of the system under analysis.

Authentication and authorization go hand in hand (E-witness, 2001) (Dekker, 1997). Users must be authenticated before carrying out the activity they are authorized to perform. According to Jones (2001), "authorisation is the final stage of access control." Therefore, when considering the controls for authorisation, the controls for authentication as discussed in 5.3.6 below also needs to be taken into account.

"A payment system with integrity allows no money to be taken from a user without explicit authorization by that user" (Asokan et al, 1997). Authorisation constitutes the most important relationship in a payment system.

In the mainframe environment, authorisation depends on the operating system and the level of security that system administrators have imposed (Kabay, 1998). Identification and authentication (I&A) begin when a session is initiated. A session is "an activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff)" (Kabay, 1998). Web interactions require I&A only when the user and the Web owner agree to establish a secure session. Typically, secure Web transactions do require some form of logon and logoff even if these steps are not explicitly labeled as such.

Access Controls are those policies, procedures, and tools that control access to resources (Norton, 2000). Logical access controls typically come into play in the form of system user profiles for access to network resources.

In essence, access control is implemented as a database of users and their privileges. At the infrastructure level, the Kerberos standard is commonly employed (PWC, 2001). Kerberos is a trusted authentication software system that through the use of shared secrets or keys, establishes a trusted end-to-end path or connection for use by two parties or processes (Deloitte & Touche, 1997); (Mackey & Gossels, 2000). Many application software suppliers also offer access mechanisms. In addition, the digital certificate is available to be used as the basis of access control. Firewalls are access control tools designed to provide access control protection. All these tools used in access controls (i.e., digital certificates, firewalls, etc.) are discussed in more detail in Section 5.4 below.

In summary, identification, authentication and authorization are normal components of any business transaction and must be guaranteed by the communications systems and software used between supplier and customer.

### 5.3.4 NON-REPUDIATION

This security concept protects against the sender or receiver denying that they sent or received certain communications and therefore ensuring that transactions, once committed to, are legally valid, irrevocable (Techguide, 2000); (Verisign, 1999); (Kabay, 1998); (Dekker, 1997); (E-witness, 2001) and cannot be disowned (Baltimore, 1999).

One definite way to ensure non-repudiation is established through the following key aspects (Martin1, 2000):

- Participating parties must authenticate each other.
- The integrity of the messages exchanged between the two parties must be controlled (e.g., encryption).
- Give a means whereby parties can electronically sign the contract (i.e., digital signature). This will ensure integrity and the signature will support non-repudiation.
- Keep the transaction confidential (privacy, access control).

As stated in Chapter 4, there is a very close relationship between repudiation and authentication and the controls used for authentication will also be used to establish non-repudiation. According to Kabay: "Authentication leads to a related concept, that of non-repudiation. Non-repudiation depends on asserting that authenticity has not been violated when identifying the source of that transaction or message." The controls used for authentication are mentioned in Section 5.3.6 below and this section on non-repudiation needs to be reviewed/ interpreted in conjunction with Section 5.3.6. Control technology used to address non-repudiation include encryption, digital signatures and digital certificates (Martin1, 2000); (Mehta, 1999), and these aspects/technologies will be discussed in Section 5.4 below.

### 5.3.5 AVAILABILITY – DENIAL OF SERVICE (DOS)

It is possible for information to be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need (Dekker, 1997). Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable (Asokan et al, 1997); (Verisign, 1999). All parties require the ability to make or receive payments whenever necessary. According to Asokan (Asokan et al, 1997), "payment transactions must be atomic: they occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash."

In a DoS attack, a hacker gains access to several computers connected to the Internet and installs code on those systems. At the hacker's signal, the systems start sending data to targeted Web sites. The sudden burst of network traffic overloads the Web servers and the networks they are connected to, slowing performance and eventually crashing the site (PWC, 2000); (Scit, 1998).

When a DoS attack comes from several sources it is known as a "distributed denial of service" attack (or DDoS Attack) (Gregg, 2000); (Kessler, 2000). This is a method available to hackers to explore and exploit weaknesses in a company's Internet site. The method involves bombarding the web site with packets of information similar in nature to requests that would be sent by legitimate users. These attacks are usually performed via a series of compromised staging sites. This disguises the origin of the attack and preserves the anonymity of the hacker (Gregg, 2000); (Todd, 2000). The web site under attack may react in one of several ways. It will either shut down under the strain; continue to operate normally but legitimate users won't be able to access the site; or (worst case scenario) the defense mechanisms of the site break down allowing the hackers complete access to the site and potentially the corporate networks behind it. "In most cases, disruption is highly likely" (Gregg, 2000).

DoS attacks may result in significant loss of time and money for many organisations (Fuller, 2000). Organisations should consider the extent to which they could afford any service outage and take steps to mitigate unacceptable risks. These steps/controls that are available to be implemented involve many of the other tools mentioned in Section 5.4 of this chapter. The following control options should be taken into account. (Note that for each option mentioned below, the tools that address the weakness are also identified. These tools are described in Section 5.4 of this chapter.)

- Establish and maintain regular backup schedules and policies, particularly for important configuration information (Fuller, 2000). Addresses server vulnerabilities.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts (Fuller, 2000); (Levy, 2000). Server vulnerabilities and access control.
- Implement properly designed firewalls. These track traffic in and out of the site, logging and inspect every packet of information to ensure its legitimacy (Fuller, 2000); (Gregg, 2000); (Mackey & Gossels, 2000); (Todd, 2000); (Kessler, 2000); (PCIS, 2000); (Cknow, 2000); (CERT, 1999). Firewalls.
- Keep all software up-to-date: Implementing all security fixes and patches as they are released will go a long way to reducing vulnerability to these attacks (Fuller, 2000); (Gregg, 2000); (Kessler, 2000); (PCIS, 2000); (Cknow, 2000); (CERT, 1999). As available, install patches to guard against TCP SYN flooding. Firewalls.
- Disable any unused or unneeded network services (Fuller, 2000); (Todd, 2000); (PCIS, 2000); (CERT, 1999). Firewalls and server vulnerabilities.
- Enable quota systems on operating system if available: limit users and programs to a specified amount of resources only (Fuller, 2000); (Levy, 2000). Server vulnerabilities.
- If the operating system supports partitions or volumes, partition the file system so as to separate critical functions from other activities (Fuller, 2000). Server vulnerabilities.
- Establish system performance baselines and observe daily activity for aberrations (Fuller, 2000). Server vulnerabilities.

- Routinely examine the physical security environment with respect to current needs (Fuller, 2000); (Unixtools, 2001). Server vulnerabilities and physical security.
- Use tools (e.g., Tripwire) to detect changes in configuration information or other files (Fuller, 2000); (Mackey & Gossels, 2000); (PCIS, 2000). Server vulnerabilities.
- Invest in fault-tolerant network configurations. (Fuller, 2000). IDS.
- Switch on audit logs for all key servers: when efficiently and effectively configured and monitored, these logs will provide adequate information to identify and investigate any problems (Gregg, 2000); (Kessler, 2000); (CERT, 1999); (Unixtools, 2001). IDS.
- Install intrusion detection software. If properly configured, this software will quickly identify known patterns of attack and immediately shut out only the attacker, while sounding the appropriate alarms (Gregg, 2000); (Mackey & Gossels, 2000); (Levy, 2000); (PCIS, 2000). IDS
- Hire the right people: make sure your technical personnel completely understand the issues, the technologies and the solutions (Gregg, 2000); (PCIS, 2000); (Ghostship, 2001).
- Test defenses regularly. The rapid rate of change in both the technology area and the hacking community means defenses must be tested on a regular basis (Gregg, 2000); (Mackey & Gossels, 2000); (Kessler, 2000); (PCIS, 2000); (Unixtools, 2001). IDS.
- Design the network to isolate attacks. If the worst happens and the hacker gets inside, appropriate network configuration, firewalls and other tools will ensure any damage the hacker could cause is isolated to a small area (Gregg, 2000). IDS and Firewalls.
- Have an incident response plan. Identifying, reacting to and resolving the problem immediately is the real business challenge. Most organizations implement the right preventative measures, but do not prepare and train for the worst. Identify who should respond and test the plan; establish procedures for determining the seriousness of the breach (Gregg, 2000); (PWC, 2000); (PCIS, 2000). IDS.
- Focus on preventative measures. Swift, large volume, automated attacks require sophisticated, automated defense mechanisms. Identifying a problem an hour later and then trying to trace and resolve it is not an option (Gregg, 2000); (Todd, 2000).

- Gather evidence. Understanding how to identify, gather and manage legal evidence to ensure the appropriate legal action can be taken against a hacker should be a key element of defense system design (Gregg, 2000).
- Educate the users. Constant awareness and updating of knowledge is the best defense to any attack (Gregg, 2000); (Pethia et al, 1991). Server vulnerabilities.
- Use network or file scanning tools to detect DdoS attacks and keep these up to date with new developments and types of attacks (Levy, 2000).

According to Gregg (2000), "even if these activities are all implemented correctly, an organisation may still not be able to guarantee 100% security - at least not as long as human error is a factor. That's the nature of doing e-business. What can be guaranteed is that the hacker will quickly tire of attempting to break down a company's defenses and move onto the next poorly protected site."

### 5.3.6 AUTHENTICATION

A primary tool in securing any computer system is the ability to recognize and verify the identity of users (individual, group, system, or application) (Techguide, 2000); (Verisign, 1999); (Kabay, 1998); (PWC, 2000); (Jones, 2001). This security feature is known as authentication. After being authenticated, the object is granted access to the services required, and its activities may be monitored (PWC, 2001). Authentication and authorisation together are the foundation of any security plan, and is often a key part of other security solutions (PWC, 2001). The authentication technology used to protect a particular resource should be determined by the resource's importance to the business. Authorisation was discussed in 3.3 above.

There are three generally accepted techniques for authenticating users to host servers (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998). These three factors are also sometimes referred to as multifactor authentication (PWC, 2001), and are detailed below.

1. *Authentication by something the user knows*. This is the password/username concept. Traditionally, special names and secret passwords have been used to authenticate users, but the password is only as good as the users' ability to keep it secret and protect it from being abused by unauthorized users (PWC, 2000); (Kabay,

1998); (Norton, 2000); (PWC, 2001); (Techguide, 2000); (Mehta, 1999); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998).

One of the methods for hackers and crackers to break into systems is by breaking into legitimate user accounts via cracking (or guessing) passwords. There are tools freely and publicly available to crack passwords for all sorts of systems. These tools are easily able to crack passwords due to the type of passwords selected by system users. Due to human nature, people tend to select passwords easy for them to retain such as children and pets' names, and other common English words (E-witness, 2001). Thus, using passwords for user authentication and authorisation is inherently weak (Mehta, 1999). Even encryption requires the use of codes and passwords (see encryption Section 5.4.1). Passwords are often the only wall between a hacker and privileged, proprietary and networked information.

2. *Authentication by something the user has.* In this technique, the user is given some kind of token, such as a magnetic stripe card (smartcard), or key (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000); (Dekker, 1997); (ZDnet2, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998).

3. *Authentication by physical characteristics.* (PWC, 2000); (Kabay, 1998); (Norton, 2000); (James, 1999); (Techguide, 2000), (VISA, 1997); (Martin1, 2000); (Mehta, 1999); (Dekker, 1997); (ZDnet, 1997); (E-witness, 2001); (Jones, 2001); (Scit, 1998). Here, the mechanism is to recognise some measure of the individual, which cannot be duplicated. Biometric techniques such as fingerprint ID, palm print ID, retinal scan, manual and digital signature, or voice recognition are used to validate the identity of the potential user.

"Authentication is also necessary when two computers communicate with each other" (Mehta, 1999). For example, if another computer asks a host computer to have a disk mounted which contains all of an organisation's personnel data, it must be determined that the requesting computer has a legitimate reason to access that information, and that it is not some external network hacker trying to steal information from the organisation.

All of these categories of authentication are used on the Internet (Kabay, 1998).

Authentication is made possible by using shared-key or public-key cryptography, digital certificates, encryption and secure protocols (Asokan et al, 1997); (Feindt & Culpin, 1998). These methods will be discussed in Section 5.4 below.

The six areas mentioned in Section 5.3 above are all important in an EC payment security environment. The controls present in each of these areas will have an impact on the overall conclusion on the control environment. The detailed controls available for each of these six sections are through the various technologies mentioned in Section 5.4 below. The IS auditor must understand the controls required for each of these six areas in Section 5.3 above so that it will enable the IS auditor to develop an audit approach for EC payment security.

## 5.4 TECHNOLOGIES USED FOR CONTROL PURPOSES

To secure information and EC payment details on the Internet, many different technologies are being used in various combinations.

Integrated security architecture includes new mechanisms such as firewalls, VPNs, IDS, PKI, Digital certificates and secure protocols (these technologies will be described in Section 5.4 below). To secure the connected enterprise, the collection of techniques must be managed as a whole to ensure that enterprise assets are appropriately guarded i.e., no one solution alone is enough to secure the payments. The IS auditor needs to be aware of the different technologies being used (i.e., the IS auditor needs to have an understanding of technologies and what control each technology provides). This stems from the general requirement that the auditor needs to have "adequate technical training and proficiency as an auditor. (For example as prescribed by the AICPA General Standard ET201 (AICPA, 1997). Armed with this information, the IS auditor considers the relevance of the control in the area being reviewed and evaluate whether the effectiveness and efficiency of each control should be tested. The technology areas described in Sections 5.4.1 to 5.4.7 below should be considered while keeping this aspect in mind.

### 5.4.1 ENCRYPTION AND SECURE PROTOCOLS

### 5.4.1.1 Encryption

While information travels between the server and the browser, it may be stored on intermediate devices and may be intercepted and even modified by third parties (Dallas, 1998). Without additional effort, this structure provides neither privacy (confidentiality), nor integrity, nor authentication (Dekker, 1997); (CSE, 2001);

(Dallas, 1998). Encryption is the foundation for safe Internet commerce (Zimits & Montano, 1998); (Feindt & Culpin, 1998); (Hartman, 2001). It covers not just the coding or scrambling of messages but authentication, message integrity, non-repudiation, confidentiality of data, digital signatures and other security related issues (Asokan et al, 1997); (Feindt & Culpin, 1998); (Certicom, 1997).

Without encryption, messages containing sensitive private information or financial details, such as credit card numbers, may be read at numerous points as the messages pass through the net. Cryptographic techniques are essential tools in building secure payment systems over open networks that have little or no physical security. Using no cryptography at all means relying on out-band security (Asokan et al, 1997) e.g., goods ordered electronically are not delivered until a fax arrives from the payer confirming the order.

Encryption is a very old technique (Techguide, 2000); (James, 1999) used to protect sensitive information as it is transmitted from one location to another (Martin1, 2000). It is simply the scrambling of the transmitted text using a set of rules (called algorithms, which means mathematical manipulations) to produce unintelligible (encrypted) data (Techguide, 2000); (Norton, 2000); (Landrum, 2001); (Baltimore, 1999); (James, 1999); (Feindt & Culpin, 1998); (Rapp, 2001); (Dekker, 1997); (Widman, 1999); (Terena, 2001); (Jones, 2001); (Scit, 1998). This ensures confidentiality. The recipient may then use the same set of rules in reverse to unscramble the coded text and read the intended message. The key used must be kept secret between the two parties (Baltimore, 1999).

Powerful encryption exists with which to insure the confidentiality, integrity, authenticity, and non-repudiation of data (Cobb, 1999) (Dekker, 1997); (ZDnet, 1997); (Deloitte & Touche, 1997); (McDow, 2001). There are two primary encryption methods in use today (Cobb, 1999); (Martin1, 2000); (VISA, 1997); (Widman, 1999); (ZDnet, 1997); (Overly & Howell, 1998); (Terena, 2001); (Dixon, 1999); (Deloitte & Touche, 1997); (IEC, 2000); (Mackey & Gossels, 2000); (Certicom, 1997): private key (symmetric) encryption (e.g. Triple DES, IDEA, Blowfish, RC4, and RC5), and public key encryption (asymmetric) (e.g. RSA, SEEK, PGP, and ECC). The primary difference between the two methods is the number of passwords or "keys" that are used (Overly & Howell, 1998). “The central problem in most cryptographic applications is managing these keys and keeping them secret” (Baltimore, 1999).

Encryption mechanisms rely on keys or passwords. The longer the password, the more difficult the encryption is to break (IEC, 2000).

A symmetric key uses only one key to encrypt or decrypt a message; an asymmetric key uses two keys for encryption and decryption (Dixon, 1999); (Halsey, 1996). The symmetric encryption is faster, but the key is difficult to distribute securely. An asymmetric key is slower but a public key may be distributed. Public key cryptography replaces the secret key of symmetric encryption with a pair of keys (Baltimore, 1999); (Asokan et al, 1997); (Dfat, 2000), one private and one public. Information encrypted using the public key can only be retrieved using the complementary private key (Pei, 2001); (Martin1, 2000). This allows the sender of a message to encrypt it using the sender's private key. Any recipient may determine that the message came from the sender by decrypting the message using the sender's public key. For example, if a user called Alice encrypts a known piece of data, such as her telephone number, with her private key and transmits it to another user called Bob, Bob then decrypts the message using Alice's public key and compares the result to the known data. He therefore ensures that that the message could only have been encrypted using Alice's private key (Martin1, 2000).

With this system the public keys of all users may be published in open directories, facilitating communications between all parties. In addition to encryption, the public and private keys may be used to create and verify 'digital signatures'. These may be appended to messages to authenticate the message and the sender (Baltimore, 1999; (Asokan et al, 1997). PKI (discussed in 5.4.2 below) use public and private key encryption algorithm keys for encoding and decoding information (Dfat, 2000); (Asokan et al, 1997). Public key encryption is used for creating digital signatures and also to ensure integrity of a document. The transaction however may only be trusted if the total framework for supporting issue and maintenance of the keys is also trusted. "A widespread system of cryptographic keys will therefore inevitably lead to a need for a complex support system" (Asokan et al, 1997). This aspect is further discussed in Section 5.4.3.1 below.

These protocols also provide anonymity. Anonymity is desired, except that there must be some assurance that participants are who they claim to be. "Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authenticated" (VISA, 1997). For example before a user called Bob accepts a message with another user called Alice's digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network. One way to be sure that the public key belongs to Alice is to receive it over a secure channel directly from Alice.

However, “security through encryption is never an absolute” (Hartman, 2001). All encryption is vulnerable to be broken, eventually. The key is to stay ahead of processing power and to limit the amount of information that be gained by cracking a single key. Technically speaking, there is a big difference between an algorithm and its implementation (Cobb, 1999). To quote leading cryptographer Schneier: "The technology is not weak in and of itself, it is just badly implemented" (Cobb, 1999).

This Internet connection needs to be made secure because of the Internet's public nature and the risk of fraudulent interception of private information. For effective use in electronic commerce situations, additional steps must be taken to make the web an acceptable medium (Dallas, 1998). To answer these concerns, two types of standard protocols have been developed (Le Tocq & Young, 1998); (Dixon, 1999); (Dallas, 1998) for securing the online purchase process:

- Secure protocols (e.g., Secure Sockets Layer (SSL), and Secure Hyper Text Transport Protocol (S-HTTP))
- Secure Payment protocols (e.g., Secure Electronic Transaction (SET) protocol)

These security protocols all use encryption techniques to provide adequate security (Zimits & Montano, 1998); (Le Tocq & Young, 1998); (Mehta, 1999), but “SET and SSL are targeted at different applications” (Zimits & Montano, 1998).

As described above, encryption forms the basis of many other controls as well and is used to ensure confidentiality and integrity. Secure protocols are also used in the digital certification process. The IS auditor needs to understand this technology and the role that it plays in the control process, because the control will be evaluated as part of the audit process (i.e. during the performance of the steps in the audit program).

#### 5.4.1.2 Secure Protocols

SSL and S-HTTP are examples of general security- related protocols. There are other encryption methods such as IPSec and Tunneling that are also mentioned below. Also, separate payment related protocols have been developed to handle financial transactions. Examples include SET (Secure Electronic Transaction), CyberCash and First Virtual. These will be further explained under the SET section in 5.4.1.2.2 below. Most of these protocols secure only the payment information such as the credit card numbers but not necessarily other information that may be confidential such as the customer order (Mehta, 1999).

Network transport security by default does not include encryption and strong authentication (Dixon, 1999). HTTP, FTP, and Telnet security features are generally limited to user identification and password authentication. Two methods of attack have been developed to compensate for the lack of security. The first is Virtual Private Networking (VPN) protocols to provide encrypted links between systems to extend internal networks and to connect with external systems, networks, and users. VPN is discussed below in Section 5.4.6. The second is Secure Transport protocols that use encryption to provide confidentiality and authentication between systems and applications. Network transport security is provided using one of five different protocols (Dixon, 1999). These are:

1. **IPSec (Ipv6)** - A network level protocol that is an enhancement of the TCP/IP protocol commonly used. IPSec encrypts network traffic and authentication from machine to machine. Its weakness is that it does not provide the granularity needed to connect individual users without additional controls that provide physical security and strong user authentication.
2. **Secure Socket Layer (SSL)** - The most popular protocol in use today (Dixon, 1999); (Pei, 2001); (CPG, 1999); (McDow, 2001). SSL is discussed in more detail in Section 5.4.1.2.1 below.
3 **Private Communication Technology (PCT)** - A technology introduced by Microsoft that mimics SSL v3.0 (Dixon, 1999); (Overly & Howell, 1998). PCT incorporates a separates authentication and key exchange providing stronger authentication keys.
4 **S-HTTP** - (Secure HyperText Transfer Protocol) An application layer transport method that provides for protected communication using Privacy Enhanced Mail. S-HTTP runs at the application layer of the OSI ISO standard. In other words, it stacks up at the same level as http. This protocol is flexible in terms of the type of encryption used. It includes private key, public key and message digests. S-HTTP is a security-enhanced variant of HTTP, which provides similar capabilities to SSL, and the two may easily co-exist in a complementary fashion by layering S-HTTP on top of SSL (Walder, 1999). S-HTTP is used to encrypt information that

has been entered into an HTML document by a client and sent to a server, or to encrypt information being sent by a server to a client (Dallas, 1998). S-HTTP is incapable of handling streaming voice and data, and it is not widely accepted (Dixon, 1999); (Dallas, 1998); (Mehta, 1999).

5 **Transport Layer Security (TLS)** - A protocol that is based on Netscape's SSL v3.0 and portions of Microsoft's PCT to create a standard security protocol (Dixon, 1999); (Overly & Howell, 1998). TLS has yet to be promulgated for use, and is still under revision.

The IS auditor needs to be aware that there are several different secure protocols in use and that secure protocols also play an important role in the controls identification and evaluation process. The IS auditor therefore needs to have an understanding of the role that secure protocols play in the controls process. Because SSL has been accepted as the most popular protocol in use (as shown in point 2 above), SSL will be discussed in more detail below.

#### 5.4.1.2.1 Secure Sockets Layer (SSL)

The use of secure protocols is one way to enhance security (Mehta, 1999). SSL, developed by Netscape (Walder, 1999); (Zimits & Montano, 1998); (Pei, 2001); (McDow, 2001) is supported by the leading browser software such as Netscape and Internet Explorer from Microsoft (Walder, 1999); (Rapp, 2001); (ZDnet, 1997); (Overly & Howell, 1998); (Terena, 2001); (Pei, 2001); (McDow, 2001); (Sun, 1998). SSL is a protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP, offering data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection (Rapp, 2001); (Techguide, 2000); (Mehta, 1999); (Walder, 1999); (Dallas, 1998); (Pei, 2001). SSL uses public-key technology (Zimits & Montano, 1998); (Asokan et al, 1997); (Martin1, 2000); (McDow, 2001). SSL is a socket-layer communication interface that allows two parties to communicate securely over the Internet (Zimits & Montano, 1998); (Asokan et al, 1997). It is not a payment technology per se, but has been proposed as a means to secure payment messages. SSL does not support non-repudiation.

An encrypted SSL connection requires all information to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality (Pei, 2001); (McDow, 2001); (Martin1, 2000). Confidentiality is important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering, i.e., for automatically determining whether the data have been altered in transit.

SSL is in common use today in many e-commerce servers, and offers "session-level" security (Le Tocq &Young, 1998); (Walder, 1999); (Dixon, 1999); (Mehta, 1999). This means that once a secure session is established, all communication over the Internet is encrypted, including the URL the client is requesting, any submitted form contents (including things like credit card numbers), any HTTP access authorisation information (user names and passwords), and all the data returned from the server to the client. This is also known as end-to-end encryption of data sent between web client and web server (Mehta, 1999). Additionally, since SSL encrypts everything (Le Tocq & Young, 1998); (Dallas, 1998); (Dixon, 1999); (Mehta, 1999), the display of complex pages may be slow, and therefore SSL protected sites often use minimal graphics to minimize the performance impact (Le Tocq & Young, 1998); (Dixon, 1999).

A SSL session is the equivalent of using a scrambler on the telephone line to the catalog merchant (Dixon, 1999); (Le Tocq & Young, 1998). When the data arrives at the merchant's web site, all the information is decrypted and whether or not it is stored in a secure format is the responsibility of the merchant: the user has no control over the security of their information and the data is only as secure as the host machine. (Le Tocq & Young, 1998); (Mehta, 1999); (Dixon, 1999); (Pei, 2001). The purchaser therefore:

- Has to trust that the merchant will guard their credit card information securely and the purchaser is assuming a risk in doing so (Dixon, 1999); Le Tocq & Young, 1998).
- Has no assurance that the merchant is authorized to accept credit card payment (Dixon, 1999); Le Tocq & Young, 1998).

SET (as discussed in 5.4.1.2.2 below) overcomes this problem. In an on-line transaction the merchant also suffers a security risk, as with any mail-order or telephone-order transaction, because he has no proof that the user is the true owner of the credit card (Le Tocq & Young, 1998); (Dixon, 1999); (Pei, 2001). This is a risk that the merchant and the credit card vendor assume and factor in to their cost of doing business. This risk increases with the purchase of "soft goods" and intellectual property (software, games, etc.) where the purchase is actually delivered on-line as well as being ordered on-line.

The SSL protocol operates in two phases. In the first phase, the sender and receiver agree on the read and write keys to be used, and then in the second phase data is encrypted using the keys chosen (McDow, 2001); (Techguide, 2000). Authentication and secure key exchange is also achieved using the RSA public key encryption algorithm. At the opening of the SSL session there is a negotiation to determine the level of security (Martin1, 2000); (Pei, 2001); (McDow, 2001); (Mehta, 1999). The security level is determined by the 'weakest party'. The other one may consider the level as unacceptable and refuse the connection. For example, one party may only be able to cipher with 40 bits DES encryption and the other party does no accept less than 56. SSL users authentication allows a server to confirm buyer and supplier identity. SSL verifies that digital certificates are valid and have been issued by a certificate authority (CA) listed in the server's list (Martin1, 2000).

Here are the steps taken during a SSL transaction (McDow, 2001):

1. The client sends a request for a document to be transmitted using the S-HTTPS protocol by prefixing the URL with "https".
2. The server sends its certificate to the client.
3. The client checks to see if a trusted Certification Authority (CA) issued the certificate. If not, it gives the user the option to continue or to terminate the transaction.
4. The client compares the information in the certificate with the information it just received concerning the site: its domain name and its public key. If the information matches, the client accepts the site as authenticated.
5. The client tells the server what ciphers, or encryption algorithms, it can communicate with.
6. The server chooses the strongest common cipher and informs the client.
7. The client generates a private (or session) key using the agreed cipher.
8. The client then encrypts the session key using the server's public key and sends it to the server.
9. The server receives the encrypted session key and decrypts it with its private key.
10. The client and the server then use the session key for the rest of the transaction.

"Holes in SSL have already been identified, arising not from weaknesses in the underlying encryption technology, but from shortcomings in the implementation." (Cobb, 1999).

As shown above SSL is used in two of the major browsers used by users of the Internet. The IS auditor therefore needs to understand the importance of SSL as well as having a background understanding of how SSL works. The IS auditor also needs to be aware that the implementation of SSL creates weaknesses if it is not done correctly. The evaluation of the implementation controls will be performed as part of the audit steps.

#### 5.4.1.2.2 Secure Payment Protocols

Secure payment protocols are usually independent of the transport protocols mentioned above in 5.4.1.2 and are network architecture independent. Secure payment protocols generally send encrypted data that requires a key in order for the merchant to complete the transaction (Dixon, 1999). Some of the more common secure payment protocols are:

1. **First Virtual** - A user has an account and receives a password in exchange for a credit card number, but the password is not protected as it traverses the Internet. "Such a system is vulnerable to eavesdropping" (Asokan et al, 1997). When the user makes a purchase, the vendor forwards the request to First Virtual (First) for authentication; First Virtual then queries the user to verify the purchase request. Upon acceptance by the user First Virtual then notifies the vendor of the successful transaction where upon the vendor sends the merchandise.

   First Virtual achieves some protection by asking the payer for an acknowledgment of each payment via e-mail, but the actual security of the system is based on the payer's ability to revoke each payment within a certain period. In other words, there is no definite authorization during payment. Until the end of this period, the payee assumes the entire risk. "This method is protocol independent and slow" (Dixon, 1999). "First Virtual is a cryptofree system" (Asokan et al, 1997).
2. **DigiCash** - Tokens are purchased from a bank or created by a user that is routed through a bank to guard against fraud. The token's amount is exposed

but the serial number is hidden. The transaction is complete when the token is accepted.

3. **Cybercash** – This protocol uses wallet software on the user's desktop that responds to the purchase request. The wallet software is activated when the vendor responds the sales data. It is routed to CyberCash where the ability to pay is validated for the user and the transaction completed. A major drawback is that the wallet is tied to one particular desktop.
4. **MilliCent** – This is ideal for buying and selling digital products costing from 1/10th of a cent to $10 or more. Accounts may be opened directly with MilliCent or through a MilliCent broker. Funds are held in the account until needed and then spent at vendor websites with the click of a mouse. MilliCent takes care of the actual payment, the currency conversion, resolves content delivery problems and automatically processes refund requests. Users fund their accounts through an online debit or credit card, by billing their monthly ISP statement or telephone bill or through pre-paid cards purchased anonymously through convenience stores (MilliCent, 2000).
5. **Open Market** - A user issues a purchase request. The seller sends a "Digital Order" to the user where it is forwarded to a financial institution that verifies the ability to pay. The financial institution then forwards a digital request back to the seller. Buyers do not have to disclose the payment method (Dixon, 1999).
6. **Smart Cards** - Smart cards contain a microchip embedded into a standard plastic card. Information may be stored on a smart card, and software programs may be loaded and run on those cards with microprocessors. By storing digital certificates or a secret encryption key, smart cards may be used as identification cards, electronic cash, credit cards, remote access tokens, and storage of medical records (Zimits & Montano, 1998). Smart cards may also be a card issued with a fixed monetary value. The value is reduced with every transaction. The monetary value is tied to the card. The holder gets to use it. If the card is lost the monetary value is lost also (Dixon, 1999).
7. **Secure Electronic Transaction** (SET) - A protocol backed by MasterCard and Visa and supported by many other organizations that use Public Key Infrastructure (PKI) (VISA, 1998); (Dixon, 1999). The user makes a purchase request and the vendor checks with a payment gateway to verify the ability to pay. SET is discussed in more detail in 5.4.1.2.2.1 below.

   SET technology protects transaction information over open networks in four ways:

a. The cardholder is able to authenticate that a merchant is authorized to accept payment cards in a secure manner using SET technology.

b. The merchant is, in turn able to authenticate the payment card used in the transaction.

c. Advanced encryption technology protects personal payment information during transfer over the network.

d. Only the intended recipient may read payment information. Only the merchant and the financial institution using valid SET technology may read the information. As SET is distributed today, buyers are assured that the vendor is an authorized acceptor of the payment card. Merchants are assured that the user of the card is the authorized user of the card. SET offers a more secure form of purchasing for merchants because of the "client-side authentication". The merchant is assured that the purchaser cannot deny that they entered into the transaction process.

In summary, secure transactions must be considered in the light of competing goals depending on who is being considered. Customers want to protect their credit, credit card information and personal information from unscrupulous activity. The merchant wants to know who is buying their products, with assurance that they will be compensated for the purchase. Financial institutions want to protect against fraud and to increase the activity based on their particular financial infrastructure. The protection methodologies described depend upon public key infrastructures (PKI) for the validation and authentication of the participants in e-commerce transactions. The IS auditor therefore should understand that there are several different payment protocols available although some are more popular than others. One of the most well-known payment protocols is SET and SET is discussed in 5.4.1.2.2.1 below.

### 5.4.1.2.2.1 Secure Electronic Transaction (SET)

By using sophisticated digital certificates, SET makes the Internet a safe place for conducting business (VISA, 1997). SET focuses on authenticating the parties involved in a transaction, ensuring message integrity, and maintaining confidentiality of information (VISA, 1998); (Overly & Howell, 1998). The SET specification is an open specification available from several software and browser providers. SET duplicates and extends identification and authentication, while it adds authorization and repudiation (VISA, 1997). How these security aspects are addressed in SET, will be explained in more detail below.

SET is a system for ensuring the security of financial transactions on the Internet (Peixian, 2000); (VISA, 1998); (James, 1999); (Le Tocq & Young, 1998); (Pei, 2001); (McDow, 2001). It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others (Peixian, 2000); (VISA, 1988); (Zimits & Montano, 1998), (Walder, 1999); (Overly & Howell, 1998); (Terena, 2001); (Pei, 2001); (CPG, 1999). With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures between the purchaser, a merchant, and the purchaser's bank (Peixian, 2000); (Pei, 2001). The cardholder application or digital wallet is stored on the consumer's computer or Internet access device that also stores the card holder identity, digital key, and reference information from the card to be charged for the transaction (VISA, 1997).

SET provides confidentiality of payment and ordering information, since even the merchant never gets to see the customer's payment details, which are passed directly to the card company whilst still encrypted (Walder, 1999); (Dixon, 1999); (Overly & Howell, 1998); (Pei, 2001); (CPG, 1999); (McDow, 2001). This ensures integrity for all transmitted data, and provides authentication that a cardholder is a legitimate user of an account. The major advantage of SET over existing security systems is the addition of digital certificates that associate the cardholder and merchant both with a financial institution and the Visa or Mastercard payment system in a way that ensures privacy and confidentiality (Dixon, 1999); (Peixian, 2000); (Martin1, 2000) as well as non-repudiation (Martin1, 2000); (Dixon, 1999); (VISA, 1998); (James, 1999). Digital certificates provide the foundation for SET (McDow, 2001); (Walder, 1999); (CPG, 1999); (Pei, 2001).

SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP) as well as companies like IBM, Verisign, and American Express (Walder, 1999). SET uses some but not all aspects of a public key infrastructure (PKI) (Dixon, 1999); (Peixian, 2000); (Walder, 1999). With SET, merchants authenticate cardholders through SET certificates. According to VISA (1998): "Merchants can more readily accept credit cards without need for merchant-based credit card registration processes. And consumers only have to register their cards once with their financial institution to use SET at all participating merchants." Like the signature on the back of a credit card, digital certificates verify that the consumer is authorized to use a payment card and the merchant is authorized to accept it (VISA, 1998); (Dixon, 1999). The digital certificate is automatically sent from the consumer to the merchant as part of the order instructions (VISA, 1998). SET software automatically checks that the merchant has a valid certificate representing their relationship with their financial institution. "This provides consumers with the confidence that their payments will be handled with the same "Visa promise" of trust as used in credit cards" (VISA, 1998).

SET was designed to use public key encryption technology for credit card-based commerce on the Internet (Zimits & Montano, 1998); (James, 1999); (Dixon, 1999). According to James (1999): "In practice, banks will give both keys to a customer together with a digital certificate for authenticity. When customers wish to purchase over the Internet, they firstly give the public key to the merchant along with the certificate to prove its authenticity. Likewise, the merchant provides its own public key and certificates to prove its own bona fides to allow the transaction to proceed." Problems may arise in key distribution and customer identification while attempting to ensure that accounts and clients match (James, 1999); (Martin1, 2000); (Dixon, 1999). SET enables credit card transactions on the Internet by replacing every step in the existing processing system with an electronic version (Zimits & Montano, 1998); (Dixon, 1999). These steps are described as follows (Peixian, 2000); (James, 1999); (VISA, 1998); (Pei, 2001); (McDow, 2001):

1. The customer opens a Mastercard or Visa bank account.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been digitally signed by the bank to ensure its validity.
3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
4. The customer places an order over a Web page, by phone, or some other means (Peixian, 2000) (James, 1999).
5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment may only be used with this particular order.

7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
8. Then, the merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate. Next, the purse at the merchant's Web server sends a payment request to the consumer's purse (James, 1999). Thirdly, the consumer confirms the payment and sends a message to the merchant to clear the payment with the bank. The merchant's Web site then contacts the bank for confirmation that the purse is valid and has unspent funds. The bank then sends confirmation to the merchant's Web server and at the same time allocates the funds to a safe created on the bank's system for that merchant
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant, who may then fill the order.
11. Finally, the merchant software provides a receipt to the customer.

“Fortunately, this long-winded process is completed by modern on-line systems within a second or two” (James, 1999). Various layers of encryption are applied to protect these transactions. When a customer purchases funds from the bank, these are debited to the consumer's account, but after that, the use of the funds remains unknown to the bank, since they are submitted by the merchant, not the consumer, for reasons of privacy. “As typically implemented today, SET offers a much more secure purchasing process from the merchant’s standpoint by using “client-side authentication” (Le Tocq & Young, 1998). This means that the merchant is sure that the purchaser cannot deny that they entered into the transaction.

Within SET, only the sensitive information in the transaction (name, address, credit card, etc.) is encrypted. When the consumer views the web pages, the pages are not encrypted as they travel to the consumer, enabling the web site designer to use graphics more liberally. An important point from a security angle is that SET is designed to protect only financial information, not electronic messages or other documents, so it is not subject to U.S. government export restrictions (Walder, 1999); (McDow, 2001). This means that SET-based systems will be able to incorporate full 128-bit encryption outside the USA and Canada.

SET may be used with SSL (Pei, 2001); (CPG, 1999). In such an environment SSL is used to communicate with customers, while SET is used at the back-end. This process will sidestep the need to deploy wallet software to customers. It provides the customer with merchant authentication, but not the merchant with consumer identification, as the consumer is not required to have an electronic wallet or digital certificate. SSL is designed to secure communications between a browser and a server. "However, most common usage of the Internet today is via browsers, and it has been suggested that SSL used in combination with LDAP can accomplish everything SET can without expensive software infrastructure upgrades" that are usually required for SET (Le Tocq & Young, 1998).

"The sluggish reception the market has given SET may indicate it is too complex and costly for current applications" (Zimits & Montano, 1998). "A downside of both SSL and SET is that they require the use of cryptographic algorithms that place significant load on the computer systems involved in the commerce transaction" (Le Tocq & Young, 1998). SSL has a lower impact on the e-commerce server but does less to eliminate the security risk. SET has a higher performance impact, but allows for a much more secure transaction. However, SET has its weaknesses: "its implementation is not as clean as the specification, so interoperability is an issue; it is complex and makes the transaction quite slow" (ECA, 2000), and some protocols, such as Secure Sockets Layer has taken the lead by integrating security directly into the browser.

The requirement to invest in additional hardware to support SET has been noticed in some early implementations, and some commentators have predicted that SET will not be able to cope (Le Tocq & Young, 1998); (CPG, 1999). "Many merchants are willing to take the risks inherent in SSL (which is true) and have not thought through the positive impact that can result if additional consumers are willing to participate when security is demonstrably high, or the risk of consumer confidence dropping when stories of fraud start to emerge" (Le Tocq & Young, 1998). Merchants are opting for a secure server environment that supports a larger traffic volume despite the larger risk. The performance impacts mentioned above have raised concern that despite its advantages in risk reduction, the SET protocol is impractical or too expensive to implement at today's required performance levels (CPG, 1999); (Le Tocq & Young, 1998); (McDow, 2001).

According to CPG (1999):

> "Another newly announced standard, the Electronic Commerce Modeling Language (ECML), may help make digital wallets - both SET- and SSL-based - more palatable to consumers. The standard, developed by a group of industry leaders, including Visa, MasterCard, Trintech and America Online Inc., aims to standardize the formatting of data in digital wallets and merchant payment systems. This would enable consumers to maintain one digital wallet rather than multiple wallets for different vendor sites, and would eliminate having to fill out a separate HTML payment form for every purchase. Trintech is supporting the standard in its new product, the ezCard, a JavaBeans-based virtual credit card that sits on a consumer's desktop and contains a digital certificate and personal ID from the issuing bank. What ECML allows you to do is issue virtual credit cards that are compatible with the payment forms at retailers."

The IS auditor should be aware of the payment protocols and the controls provided through the implementation of these protocols. SET is being used currently and is backed by the major credit card companies, so the IS auditor may come across SET as part of the audit of EC payment security. The IS auditor needs to be aware of the controls provided as well as the limitations and this will aid in the design and determination of the audit testing to be performed.

### 5.4.2 PUBLIC KEY INFRASTRUCTURE (PKI)

In Chapters 1 and 3 it was noted that lack of security is often cited as a major barrier to the growth of e-commerce, which can only be built on the confidence that comes from knowing that all transactions are protected by core functions. PKI is a mechanism for both authentication and encryption, combining software, encryption technologies and services to protect network communications and e-business transactions (PWC, 2000).

The following describe PKI and its importance.

- According to Mehta: "Public Key Infrastructures (PKI) are one of the ways businesses can deploy e-commerce from a security and authentication perspective." PKI comprises the processes and systems needed to effectively manage digital certificates (Mehta, 1999); (PWC, 2000); (E-witness, 2001). "PKI is a system that provides the basis for establishing and maintaining a trustworthy networking environment through the generation and distribution of keys and certificates. This function can be performed internally or outsourced to a third party specialising in it" (Mehta, 1999); (PWC, 2000).

- Another argument for PKI is made by iStory, which states: "Public key technology is emerging as the cornerstone of the future business infrastructure, and a set of applications, policies, practices, standards, and laws will emerge from public key technology that are referred to as the public key infrastructure (PKI). It is the public key infrastructure that will serve as the arbiter of security and trust on the Internet, ultimately unleashing its economic potential" (Zimits & Montano, 1998).
- "A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust" (Baltimore, 1999).
- In order to employ public-key based security solutions one often needs an infrastructure for secure user registration, public-key certification, and directory services. Usually this is called PKI (Peixian, 2000).
- In Public Key Cryptography (as discussed in 4.1 above), each user is given two key pairs, one pair to encrypt/decrypt messages and one to sign/verify them. In PKI, these are issued as digital certificates by the Certification Authority (CA) who acts as a trusted third party and who vouches for the digital certificates they issue. "But public key cryptography, on its own, is not enough if we are to truly re-create the conditions for traditional paper-based commerce in an electronic world. Security experts generally agree that Public Key Cryptography and the adoption of a Public Key infrastructure (PKI) are today the best available means of providing the highest level of security on the Internet" (Sinnreich et al, 1999).
- Yet another argument for the use of PKI to address Internet security risks is made by Verisign (1999): "One element has now emerged as the foundation for secure distributed applications, including supply chain management, secure messaging, e-commerce, virtual private networks, and intranet applications – that element is Public Key Infrastructure (PKI). An enterprise's PKI constitutes the core of its Internet security infrastructure. The success of an enterprise's PKI will have a major impact on core business operations." The foundation for secure Internet applications is a Public Key Infrastructure (PKI)."

- "PKI is becoming the cornerstone of many organisations' security strategy" (Globalsign, 1999).

From the above statements the conclusion is made that PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the desired levels of protection of assets (including information). This objective is achieved through the five principle security functions for commercial transactions mentioned earlier in this chapter and briefly repeated below.

- **Confidentiality** - To keep information private and ensure that information is not intercepted during transmission (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000).
- **Integrity** - To prove that information has not been manipulated (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000); (E-witness, 2001).
- **Authentication** - Validating the identity of parties or applications in communications and transactions through digital certificates (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (PWC, 2000).
- **Non-repudiation** - To ensure that information cannot be disowned, and ensuring that transactions, once committed, are legally valid and irrevocable (Sinnreich et al, 1999); (Verisign, 1999); (Baltimore, 1999); (Martin1, 2000); (E-witness, 2001).
- **Availability** – Ensuring that transactions or communications may be executed reliably upon demand (Verisign, 1999); (Baltimore, 1999).

According to the above definitions, Public Key Infrastructure therefore consists of the following building blocks and key components:

- **Encryption algorithms** - The basic mathematical algorithms used to scramble information. Symmetric (private) encryption uses the same keys to encrypt and decrypt, whereas asymmetric (public) encryption uses separate keys to encrypt and decrypt information. This was described in 4.1 above.
- **Private and public keys** - A secret private key and a mathematically related public key are generated for each party in a transmission. Given the public key, it is nearly impossible to determine the private key. This was described in 4.1 above.

- **Digital signatures** - An electronic signature that is irrefutable, unique, and virtually impossible to copy or transfer. PKI is based on digital IDs known as 'digital certificates', which act like 'electronic passports', and bind the user's digital signature to his or her public key. (Baltimore, 1999). Digital signatures are described in more detail in Section 5.4.3 below.
- **Digital certificates** - An electronic document comprising a public key, digital signature, owner identity, serial number, issuer, and expiration date. This is described in 4.3 below.
- **Certificate Authorities** (CA) - Issuers of digital certificates acting as a "trusted third party" in electronic transactions (Zimits & Montano, 1998); (Baltimore, 1999); (Jones, 2001). This is described in Section 5.4.3 below.
- **Security Policy** - defines the rules under which the cryptographic systems should operate (Baltimore, 1999); (Martin1, 2000). This is briefly described below as well as in Section 5.4.7.1 below.
- **Registration Authority** (RA) (Baltimore, 1999); (Jones, 2001). This is described in Section 5.4.4 below.
- **Certificate distribution system** including repository, revocation system, generation, registration, and certification (Baltimore, 1999); (Mehta, 1999); (Martin1, 2000). This is described in Section 5.4.3 below.
- **PKI-enabled applications** (Baltimore, 1999). This is described below.
- **Procedures** to dictate how the keys and certificates should be generated, distributed and used as described in the Certificate Practice Statement (CPS) of a CA (this is also described in more detail below).

As indicated, the PKI components of security policy, CPS, and PKI applications is described in more detail below:

- **Security Policy**

  A security policy defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography (Baltimore, 1999). Typically it will include statements on how the organisation will handle keys and valuable information, and will set the level of control required to match the levels of risk. Other aspects of the security policy are described in more detail in Section 5.4.7 below.

- **Certificate Practice Statement (CPS)**

  Some PKI systems are operated by commercial Certificate Authorities (CAs) or Trusted Third Parties, and therefore require a CPS. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users (Baltimore, 1999). In other words, a CPS explains the practices CAs employ when issuing certificates, the security it employs to protect its own environment and the legal rights and obligations of the CA and those who rely on its certificates (Wilson, 1999); (Sun, 1998); (Stewart, 1998).

  According to Feindt & Culpin (1998): "VeriSign Inc is an example of a CA providing digital ID/certificates for "trusted electronic commerce. VeriSign's Certification Practices Statement (CPS), a 107-page website document is accepted by the end-user during the registration process (probably without careful reading)." "A CA's trustworthiness remains essential to digital signature authentication" (Stewart, 1998).

  There are differences between the USA and Europe regarding the regulation of CAs. According to Feindt & Culpin (1998): "A Memorandum of Understanding from European Industry therefore recommends a non-regulatory approach: the development of a set of guidelines regarding the operating procedures of the CAs, reflected in Certification Practice Statements. The establishment of trusting relationships between the CAs could be handled by an industry-led body which oversees the EU guidelines for Certification Practice Statements." The US favours a non-regulatory approach relying on private initiatives. For Europe, under the common framework for electronic certification services proposal, data authenticated with an electronic signature issued by an accredited CA may be used as evidence at court in the same manner as if the data had existed in a manually signed form (Feindt & Culpin, 1998).

- **PKI-enabled applications**

"A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits" (Baltimore, 1999).

Examples of applications are:

- Communications between web servers and browsers (Baltimore, 1999); (Jones, 2001).
- E-mail (Baltimore, 1999); (Jones, 2001).
- Electronic Data Interchange (EDI).
- Credit card transactions over the Internet.
- Virtual Private Networks (VPNs) (Baltimore, 1999); (Jones, 2001).

Although PKI has been described above as an important factor in EC security, the auditor also needs to be aware that there are certain shortcomings to PKI. "Like any new, business-critical technology, the evaluation and implementation of a PKI solution is a challenging and intricate process, which requires a great deal of planning, management and clear guidance" (Baltimore, 1999). "Its effectiveness has been hampered however by the fact that several PKIs are in use, and no standard yet exists" (PWC, 2000). "Although many companies have started implementing this, PKI is in its infancy. Besides lack of industry standards, the PKI itself needs infrastructure" (Mehta, 1999).

However, the following conclusion is made:

> "It is easy to get caught up in the mathematical complexity of public key encryption and lose sight of the fact that the public key infrastructure is about much more than technology. The PKI is best thought of as a framework of accepted business practices and legal statutes supported by systems and software. The PKI resolves the fundamental problem of trust in the Internet. Providing strong privacy, authentication, data integrity, and non-repudiation, the PKI fulfills fundamental security requirements. A great deal of time and attention has been devoted to heralding the economic potential of the Internet – it is the Public Key Infrastructure and the trust it adds that will realise that potential" (Zimits & Montano, 1998).

To summarise, technically, PKI refers to the technology, infrastructure, and practices needed to enable use of public-key encryption and/or digital signatures in distributed applications on a significant scale. The main function of PKI is to distribute public keys accurately and reliably to those needing to encrypt messages or verify digital signatures (used to sign transactions or to authenticate people prior to granting access to resources). This process employs digital certificates issued by an enterprise CA to users who register with that CA. Issuance of a certificate requires authentication of the user, usually by a RA. The scope of PKI also extends to functions such as certificate renewal, certificate revocation/status checking, and user private key backup/recovery. Digital certificates will be discussed further in Section 5.4.3 and CAs in Section 5.4.3.1 below.

PKI includes many of the components important in the controls process of EC payment security. The IS auditor needs to understand what components make up a PKI and evaluate the individual PKI components relevant to the EC payment security audit to the extent to which the component serves as a control to minimise the risk.

### 5.4.3 DIGITAL CERTIFICATION

Digital certificates and signatures have been mentioned above as one of the key components of PKI. Digital certificates and signatures will be described in more detail below.

Digital certificates are used to endorse an electronic document in a way that may be later validated for authenticity. The CA that endorses a server's Web site certificate uses these. This process aids achieving non-repudiation (Martin1, 2000); (Mehta, 1999); (Walder, 1999); (Zimits & Montano, 1998); (Asokan et al, 1997); (ZDnet, 1997); (Feindt & Culpin, 1998); (Jones, 2001); (Scit, 1998); (Yasuda, 1997).

Digital certificates are like electronic fingerprints that positively authenticate the identity of the person or Web site (Martin1, 2000); (Mehta, 1999); (Feindt & Culpin, 1998). The certificate itself is simply a collection of information to which a digital signature is attached (PWC, 2000); (Mehta, 1999); (Walder, 1999). The digital signature is attached by a CA, a third party authority that is trusted by the community of certificate users (Walder, 1999); (Zimits & Montano, 1998); (Asokan et al, 1997); (Terena, 2001); (James, 1999); (Pei, 2001); (Certicom, 1997). By electronically signing a digital certificate, a CA vouches for the certificate owner's identity. The main function of a digital certificate is to validate the public key of an individual or network device (e.g., to validate content) (Zimits & Montano, 1998); (Dixon, 1999).

Typically, the digital certificate includes the unique name of the owner; name of the CA who is vouching for the identity of the certificate holder; a unique serial number; the period of validity of the certificate, and a digital key (Mehta, 1999); (Mackey & Gossels, 2000); (James, 1999); (Pei, 2001); (Yaacov, 1997). CA's will also be discussed in more detail in Section 5.4.3.1 below. However, digital certificates may also contain information that defines user privileges, and so play a role in managing access control.

Before understanding digital certificates, knowledge of digital signatures is essential. When combined with message digests, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message (or document) that is unique to that message. A message digest is generated by passing the message through a one-way cryptographic function; that is, one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message (Martin1, 2000); (Mehta, 1999); (Dekker, 1997); (Widman, 1999). The algorithm used by SET generates 160-bit message digests. The algorithm is such that changing a single bit in the message will change, on average, half of the bits in the message digest. It is computationally unfeasible to generate two different messages that have the same message digest (Martin1, 2000); (Mackey & Gossels, 2000). The message digest is signed using the CA's private key to create a message authentication code (MAC). The MAC may be verified by anyone processing the CA's public key (Halsey, 1996); (Asokan et al, 1997).

It may be proved that the transaction originated from a particular source (authentication), since certificates are based on the sender's private signing key, and authenticated by the public verifying key (Walder, 1999); (Dekker, 1997); (IEC, 2000); (Baltimore, 1999), but it may also be proven that the transaction has not been tampered with in any way during transit (i.e., integrity), since any tampering after signing invalidates the signature (Dekker, 1997); (Walder, 1999); (Kabay, 1998); (Norton, 2000); (Martin1, 2000); (Widman, 1999); (Scit, 1998); (IEC, 2001); (Baltimore, 1999). This is done by decrypting the digital signature using the originator's public key, and comparing the result with a summary produced by passing the received message through the same mathematical function (Martin1, 2000); (Scit, 1998). "While it sounds complicated, in practice the entire process can be as simple as selecting an icon on a computer screen" (Martin1, 2000).

Public key cryptography makes digital signatures possible (Martin1, 2000). As with encryption, digital signatures may make use of either secret key (where both parties require copies of the same shared key), or public key (with a public/private key pair) methods. The public key methods – such as DSS and RSA – are more popular since key management is very much more straightforward (Walder, 1999); (Asokan et al, 1997). Digital Signature Standard (DSS) provides electronic signature capabilities to Federal agencies and departments (Halsey, 1996). It was developed for use by companies that do business with the US Government and is a signature-only system, whereas RSA may be used both for signing and generally encrypting a message (Walder, 1999). An example of the use of a digital signature is provided by VISA (1997).

> "Alice computes the message digest of a property description and encrypts it with her private key yielding a digital signature for the message. She transmits both the message and the digital signature to Bob. When Bob receives the message, he computes the message digest of the property description and decrypts the digital signature with Alice's public key. If the two values match, Bob knows that the message was signed using Alice's private key and that it has not changed since it was signed."

The portability and scalability of a digital certificate supports a wide variety of applications. For example, digital certificates and private encryption keys may be issued using various media depending on the level of assurance required (e.g., smart cards) (Zimits & Montano, 1998); (James, 1999); (Sinnreich et al, 1999). Those issued only on smart cards or other certified security tokens provide the highest level of user and server security/identification for electronic commerce and are used for high value transactions. Those issued on diskettes or stored on hard disks are used for lower-value transactions and authenticated access to online services. Over time, digital certificate-configured smart cards will likely become the standard for credentials such as passports, driver's licenses, and credit cards (Zimits & Montano, 1998).

As shown in the above description on digital certificates, they are used to secure confidentiality, authentication, non-repudiation, and integrity of EC payments and are therefore regarded as an important control to consider for the IS auditor. IS auditors need to understand the role that digital certificates play in the EC payment security process so that when they design an audit approach, this control may be included where required.

#### 5.4.3.1 Certification Authority (CA)

Certification authorities hold a central role in the PKI by acting as the repository of trust from which digital certificates derive legitimacy. Digital certificates are created, managed, administrated, and revoked by the CA. "Much like the government issues and guarantees the identity of the passport bearer, a CA acts as the guarantor of the validity of the digital certificate" (Zimits & Montano, 1998).

A CA is a trusted entity (Mehta, 1999); (Walder, 1999); (Zimits & Montano, 1998); (James, 1999); (Overly & Howell, 1998); (Stewart, 1998) that provides the function of an independent third party to authenticate the identity of the Web site or person (Sun, 1998); (Certicom, 1997); (Yaacov, 1997). "It is important that the CA is trusted in order that the certificate can be considered genuine" (Walder, 1999). A system is needed to authenticate the identity of public key holders, as otherwise, illicit organisations might distribute sham public keys among users (James, 1999). In order to be able to get this service, companies must register with the CA. Applications of certificate authorities range from private companies administrating network privileges to broad-scale electronic commerce linking suppliers and manufacturers (Zimits & Montano, 1998); (James, 1999) and government affiliates (Zimits & Montano, 1998). Virtually any transaction requiring proof of identity or validation of privileges provides an opportunity for a CA to act as a trusted third party. Probably the best know CA at the moment is VeriSign (Walder, 1999); (Feindt & Culpin, 1998), though other systems such as IBM's World Registry, GTE's CyberTrust and Nortel's Entrust have also been introduced (Walder, 1999); (ZDnet, 1997); (Mackey & Gossels, 2000).

The CA will use its private key to place its digital signature on the certificate. When a user hits over an SSL session, the certificate of registration is downloaded to the user's browser. The signed certificate is decoded using the public key of CAs stored in the browser software. If the decoded information matches the information in the browser, the web site is authenticated. “However, CAs only help in authentication. This does not necessarily mean that the Web site can be trusted in terms of the types of goods and information that are sold” (Mehta, 1999).

The creation of a PKI involves integrating public key technology with law in order to form a "trusted" infrastructure suitable for commerce activity. In the USA, more than 50% of states have digital signature laws or are in the legislative process to create digital signature laws. Other countries include Germany Malaysia, etc. (Zimits & Montano, 1998). “A public CA must understand how to coordinate its policies and procedures with existing domestic and international laws. Additionally, a well-formed policy with prescribed practices and formal auditing is fundamental to operating as a public CA” (Zimits & Montano, 1998).

As things progress, it should be possible (and desirable) to have a hierarchy of CAs, going from banks or reputable organisations at the bottom, all the way up to government bodies and even, perhaps, a global controlling body such as the United Nations. “This means that if you don’t trust the first CA you can check the certificate on its digital signature with the next CA up the tree, and so on up the hierarchy until you reach the "root" CA” (Walder, 1999).

When implementing a PKI, an organisation may either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party. “While installing a server and other components of a CA system are well within the reach of most companies' information technology teams, the primary challenges lie in management and policy, not cryptography and systems” (Zimits & Montano, 1998). The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle (Baltimore, 1999); (Jones, 2001); (Certicom, 1997); (Zimits & Montano, 1998). Unique elements to a CA system's operations include:

- Key management.
- Certificate validation.
- Issuing certificates by binding the identity of a user or system to a public key with a digital signature.
- Scheduling expiry dates for certificates.
- Ensuring certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs).

- Key updates.
- Key recovery.
- Policy administration and maintenance.

Central to a CA system's flexibility are its use of directories (Zimits & Montano, 1998); (Baltimore, 1999). Directories are similar to databases, however, directories are primarily used for reading information rather than transactions or complex queries. In a CA system, directories are used to store and distribute digital certificates, keys, cross-certification lists, entries for distribution of certificate revocation lists (CRLs) and to retrieve keys. "An open CA system must be able to perform these basic functions and most importantly, support individual customisation in order to meet security requirements while achieving business objectives" (Zimits & Montano, 1998).

"Perhaps the thorniest issue facing all CA systems is the life-cycle management of digital certificates" (Zimits & Montano, 1998). One element of management is validation. It is important to be able to determine if a certificate is valid at any given time. CAs are responsible for providing the current status of any digital certificate they have issued. For example, a CA within a company will experience new hires, changes in employee privileges, lost passwords, and employee departures. In all circumstances, the digital certificate directory must be updated to accurately reflect these changes. "While publishing a new certificate is relatively straightforward, certificate revocation and validation are more challenging" (Zimits & Montano, 1998).

The X.509 standard is the most commonly used standard for certificates (Walder, 1999); (ZDnet, 1997); (Halsey, 1996); (Halsey, 1996); (Yaacov, 1997). Certificates based on the X.509 standard incorporate an expiry date to ensure that old certificates are revoked automatically after a given period of time. However, there also needs to be a system in place to allow certificates to be revoked before expiration time (e.g., the private key or CA signature is compromised) (Levi & Koc, 2001); (Fratto, 2000) or immediately in certain cases – say where a certificate (perhaps contained in a smart card) has been stolen. The X.509 standard defines what information may go into a certificate and describes how to write it down (Sun, 1998). This includes the version, serial number, issuer name, validity period, public key information, certificate ownership, etc. This provides for complete "non-repudiation", whereby digitally signed messages may be proved authentic to a third party, thus allowing such transactions to be legally binding. Certificates are given a set life span when issued e.g., a certificate may be valid for one year. Then it expires and a new certificate must be issued. According to Fratto (2000) "there is an indirect relationship between the information contained in a certificate and its useful lifetime. The more information in the certificate, the shorter its usefulness, because information may change and a new certificate will have to be issued before it expires.

Electronic commerce requires that certificates be validated each time they are used, in the same manner that credit cards are authorized. CAs validate certificates using three methods (Zimits & Montano, 1998); (Genuity, 1998):

- certificate revocation lists (CRLs),
- online certificate status protocol (OCSP), and
- certificate revocation trees (CRTs).

Certificate revocation lists are simply lists containing all certificates that are no longer valid (including certificates revoked before their scheduled expiration date (Zimits & Montano, 1998); (Halsey, 1996); (Apacheweek, 2000); (RSA, 2001); (SSE, 2001); (Levi & Koc, 2001); (Fratto, 2000). Each CA ideally maintains and updates the list in a timely fashion so anyone may check a digital certificate against the list and validate a certificate issued by a CA (Zimits & Montano, 1998); (SSE, 2001); (La Macchia, 2001). For small scale applications this works well. "But for geographically dispersed organizations with several hundred thousand employees or far-flung Internet commerce transactions, CRLs can quickly scale to an unmanageable size" (Zimits & Montano, 1998). Updated CRLs are made available according to the policy of the organisation (i.e. the CA). Expiration is checked against the most recent list.
The more critical an application's security requirements are, the more important real-time certificate validation becomes. For example, delays in updating CRLs in large monetary transactions such as settlements and funds transfers create credit risk. Other alternative methods of validation (i.e. CRT and OCSP) seek to address the problem of updating CRLs.

Online Certificate Status Protocol (OCSP) is meant to provide real-time validation for certificates (Zimits & Montano, 1998); (Levi & Koc, 2001); (Globalsign, 1999). While real-time validation makes sense, OCSP is an early stage standard (Zimits & Montano, 1998). Currently, an IETF working group has defined methods for using OCSP with the http protocol. Other protocols, such as ftp or smtp, are currently in discussion. "While OCSP does not address all concerns regarding scalability and performance, in our view, real-time validation will be indispensable for large scale business-to-business electronic commerce" (Zimits & Montano, 1998).

"One method offering relief from update delays and scalability is the CRT model for certificate validation developed by ValiCert. Hash functions reduce any size message to a fixed length as well as confirming data integrity (e.g., a 15k byte number may be reduced to a unique 20 byte number)" (Zimits & Montano, 1998). Using these properties of hash functions, ValiCert's patent-pending method hashes the serial numbers of revoked certificates and reduces the volume of validation data as well as verifies the integrity of the revocation tree.

Another alternative in the use of CAs is to also use a Registration Authority (RA). An RA provides the interface between the user and the CA (Baltimore, 1999); (Jones, 2001). It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that is placed in the certificates. An RA therefore performs some of the functions that a CA will perform if the RA and CA combination is not used.

Where digital certificates are used, a certification authority is also required. The IS auditor needs to understand the role of the CA and the validation of certificates. These are important aspects to control the security of EC payments and an understanding of the role of the CA and certificate validity, expiration and control is important to the IS auditor when determining the audit approach and the testing to be performed.

#### 5.4.3.1.1 Key Recovery/Escrow

Communications agencies require access to data for the purposes of system recovery after failure. Since all transmissions may have the same key, the agencies may wish to keep a register of private keys. Some governments propose that a copy of every private key be held in trust by national security agencies for their use in criminal investigations (James, 1999); (Abelson et al, 1998).

Key escrow is a system to provide encryption of user traffic, such as voice or data, so that the session keys used are available to properly authorised third parties under special access circumstances (James, 1999); (Abelson et al, 1998). Law enforcement agencies promoted the concept while other uses might be for recovery of encrypted data following its loss or destruction due to equipment failure (James, 1999); (Abelson et al, 1998). The United States “Escrowed Encryption Standard” involved a computer ('Clipper') chip with a unique identity number and a two-piece secret key stored by two different agencies. However, users may already backup keys and there is no guarantee for liability or that any escrow agency itself is trustworthy. “However, key backup is useful for good management reasons in applying to archival data” (James, 1999).

Initial proposals for Key Recovery are based around "Key Escrow", also known as "Trusted Third Party" (Walder, 1999); (Abelson et al, 1998). There are a number of implementations of this, each of which involves providing a Key Recovery Centre (KRC) with the means to decrypt your encrypted sessions. One way this could work, for instance, is to provide the KRC with copies of your private keys. Another method is to embed the keys used to encrypt the message within the message itself in a "Key Recovery Field". This is then encrypted using yet another public key provided by the KRC, whilst the corresponding private key remains known only to the KRC.

In all implementations, however, the theory is that KRC’s may only be forced to recover keys on presentation of a court order, thus protecting the interests of end users. “At the moment, products incorporating Key Recovery can make use of one of three proprietary, dynamic key management protocols – Internet Security Association/Key Management Protocol (ISA/KMP) Oakley (backed mainly by Cisco); Simple Key Exchange Internet Protocol (SKIP), backed by Sun; and Photuris Session Key Management Protocol, backed by Radguard” (Walder, 1999).

Key Recovery has been criticised by most of its likely users due to the potential for the criminal element to target Key Recovery Centres in an attempt to gain access to thousands of sets of data in a single swoop (Walder, 1999); (Abelson et al, 1998). To the hacker, KRCs represent an extremely valuable single point of failure for the system as a whole, made worse by the proposal that some KRCs would use a single key for many users (Walder, 1999). “There is also the feeling, of course, that it does not make commercial sense to allow any third party – even a "trusted" one – to hold keys which could provide access to sensitive corporate data” (Walder, 1999).

The IS auditor should be aware that there are many risks involved in key recovery/ escrow solutions, as well as to what extent the risks may be controlled. The controls evolve around third party reliance and here the IS auditor may have to rely on the work of other IS auditors if access to the key recovery third party is not available.

### 5.4.4 FIREWALLS

Firewalls are relatively simple and very effective combinations of software and hardware that act as a barrier to protect an enterprise's perimeter (PWC, 2001); (Dekker, 1997); (Mika et al, 2001); (IEC, 2000). Firewalls separate internal systems from external systems (e.g. the Internet) (Lindner, 2001); (PWC, 2000); (Landrum, 2001); (E-witness, 2001); (Tyson, 2001); (Stewart, 1998); (Deloitte & Touche, 1997) and control the flow of communications in and out of the enterprise. They create a shield between the secure environment inside the system and the open potentially hostile external environment (Landrum, 2001); (Widman, 1999); (Stewart, 1998). A firewall is a device or system that enforces an access control policy between two networks (Cott, 2001); (Lindner, 2001); (Norton, 2000); (PWC, 2000); (Landrum, 2001); (Hartman, 2001). In principle, the firewall provides two basic services: (1) blocks undesirable traffic, and (2) permits desirable traffic. A firewall provides a single point of entry into a corporate network from an un-trusted network (i.e. the Internet). It is at this 'choke point' (Cott, 2001); (Hartman, 2001) that the access control policy and auditing capability are enforced.

The job of a firewall is to examine data as it enters the network and to block traffic that doesn't meet specified criteria (Jones, 2001). There are several types of firewalls and all may be used in combination and each has strengths and weaknesses depending on the needs and uses. The types of firewalls are (PWC, 2000); (Tremblay, 2000);(Landrum, 2001); (Hartman, 2001); (Techguide, 2000); (Jones, 2001); (Tyson, 2001); (Mika et al, 2001); (Deloitte & Touche, 1997); (Mahadevan, 2001); (Scit, 1998):

- Proxy server.
- Packet filter.
- Application gateway/ dynamic packet filter.

#### 5.4.4.1 Proxy server

A proxy server is a firewall implemented in a hardware unit such as a workstation on a NT server, rather than in a router (Techguide, 2000). A proxy server performs several functions:

- Eliminates direct contact between a trusted resource and an un-trusted user and therefore acts as the middle-man between an un-trusted resource and a resource located within the trusted network (Jones, 2001); (Tyson, 2001); (Lindner, 2001); (Dekker, 1997).
- Hides the identities of resources within the protected network (PWC, 2000); (Dekker, 1997).
- Provides additional authentication and auditing capabilities (Dekker, 1997).

This device looks at all of the data in each packet, not just address and headers (Techguide, 2000), (PWC, 2000). In most cases, the proxy examines the content and replaces the network address in the packet with proxy destinations that are known to be secure (Techguide, 2000); (Mahadevan, 2001). Besides hiding the network from the outside world, they provide more control over the actual data at the application level. However, because they inspect all of the data in each packet, there have been reports of some significant performance degradations in high traffic areas (Techguide, 2000); (Jones, 2001).

#### 5.4.4.2 Packet Filter/Screening router

A packet filter examines data packets entering and leaving the network and grants (users are known by their IP address) or denies them access to specified applications (determined by their port address) on the basis of specific criteria/filters (Tyson, 2001); (PWC, 2000); (Mika et al, 2001); (Stewart, 1998); (Mahadevan, 2001); (Mackey & Gossels, 2000); (Cott, 2001); (Techguide, 2000); (Tremblay, 2000); (Dekker, 1997); (Zwicky et al, 2000). This limits the connections of even those users allowed to enter through the firewall, and completely denies any connections to those not authorised to access any applications. These are also called network level firewalls. They are fast and transparent to users, but also the easiest to penetrate and are especially prone to "spoofing" attacks (Stewart, 1998); (Deloitte & Touche, 1997); (Mahadevan, 2001).

Routers may be used to filter packets as well (Cott, 2001); (Scit, 1998). This device would only be used to filter data and should not be considered a first line of defense. The main function of a router is to use header information and forwarding tables to determine the best route for packets to travel.

#### 5.4.4.3 Application Gateway/ Dynamic Packet Filter

Authenticating Servers are often used in conjunction with Screening Routers to provide authentication (Techguide, 2000). According to Tyson (2001) this "does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded." An application gateway secures specific applications. Security mechanisms are applied when a connection is established; after that, network traffic flows without further checking (PWC, 2000). All packets are addressed to an application on the gateway that relays the packets between the two communication points. In most application gateway implementations, additional packet filter machines are required to control and screen the traffic between the gateway and the networks (Techguide, 2000). Typically, this is a use of bastion hosts (Techguide, 2000); (Deloitte & Touche, 1997). These are secure but inefficient, since they are not transparent to users and applications. According to Mackey & Gossels (2000) "they determine whether information is correctly formatted and decide whether it should be allowed or denied to the network."

The term "firewall" has become a generic term, which encompasses a spectrum of technologies intended to provide protection from communications attacks on an organization. It is possible, and often desirable, to combine these different technologies according to the needs of the organization and their budget limitations (Techguide, 2000); (Stewart, 1998).

Audit considerations for firewall security include:

- Avoiding remote firewall administration, especially over the Internet (Mehta, 1999) (Hartman, 2001). The firewall also needs to be securely managed to limit the possibility of someone breaking into it. As the protector of the network, the firewall is a target for intruders. “Managing the firewall via the Internet interface is probably the least desirable situation, especially if the management connection is of questionable encryption strength or can be spoofed” (Hartman, 2001). Taking care not to allow management ports to be available to the Internet also helps prevent fingerprinting the type of firewall used.

- Upgrading firewall software on a regular basis with patches and upgrades (Hartman, 2001). Firewall software is like anti-virus software: effectiveness goes down over time as new vulnerabilities are discovered (Mehta, 1999); (Landrum, 2001); (Deloitte & Touche, 1997); (Mahadevan, 2001). For software-based firewalls, this applies to the operating system and the firewall software (Hartman, 2001).
- Having the firewalls reviewed periodically (Mehta, 1999); (Mahadevan, 2001). There are a number of commercial products that may help make this task easier such as the Internet Security Scanner ISS - http://www.iss.net. “Another alternative is to have knowledgeable information systems auditors help in this process” (Mehta, 1999).
- Improper configuration (Landrum, 2001); (Hartman, 2001); (Dekker, 1997); (Mehta, 1999) and not monitoring and auditing logs (Landrum, 2001); (Tremblay, 2000). The firewall product will deny access to unauthorized connections and show where those attempts originated and what ports they were dispatched to. There are many types of firewalls that may exist on the host. There are also firewalls that are used to protect networks. Information gathered from logs can be used to find patterns, misconfigured equipment and break-in attempts. This information can be used to communicate those attempts to the owners of the originating hosts.
- As with most operating systems Firewalls never come out-of-the-box configured to secure any given site and are only as good as the staff administrating them (Landrum, 2001); (Mehta, 1999).
- Filters should also be as specific as possible. Permissions for inherently dangerous traffic, such as rules that allow remote management, should always be as specific as possible. But less obvious threats are often overlooked (Hartman, 2001).
- “If you have different systems for your web site and your mail, don’t just allow web and mail traffic to the entire subnet. Specify mail traffic allowed to the mail server and web traffic to the web server” (Hartman, 2001).

- Allowing SMTP traffic to a web server may not seem to be all that large a risk, but it is an unnecessary one (Hartman, 2001), i.e., evaluate whether SMTP traffic is needed.

It's important to note that in the Internet-enabled business environment, firewalls alone are no longer sufficient to provide all of the levels of security that are needed (Symantec, 2000); (Jones, 2001); (Deloitte & Touche, 1997); (Lindner, 2001). "Firewalls are not very effective at screening for viruses and cannot protect the network against attacks that do not go through it. Industry statistics show that a majority of security breaches originate from internal sources unseen by the firewall" (Lindner, 2001). Firewalls will not protect the network from vulnerabilities introduced by a lapse in security-consciousness by the user community (Lindner, 2001). Other levels of security needed include internal access control, encryption, backup and recovery, audit, logging and monitoring, and these aspects are also discussed in this chapter.

Firewalls are generally very effective at keeping unwanted people out of enterprise networks. They do this by establishing what types of network connections will be allowed and what session services will be supported. This works well when the boundaries of the network are clearly defined.

As shown above, firewalls are an important component used in EC payment security. Although the audit of a firewall may be considered for an independent review based cn the time required to ensure that the firewalls are properly controlled, the auditor involved in EC payment security audits should consider the controls over firewalls as part of the EC payment security review.

### 5.4.5 INTRUSION DETECTION SYSTEMS (IDS)

"As the use of the Internet as a cost-effective transport mechanism increases, so does the need for a real-time, automated intrusion detection and reporting capability" (Lindner, 2001). Since the paper trail in e-commerce is limited, it is critical to detect, prevent or at least limit intrusion to systems and data (Martin1, 2000). Firewalls and authentication servers act as 'passive' deterrents to unauthorised access to network and computer assets. However, in the event that a hacker is not deterred, network and computer assets are immediately at risk. "In many cases, a breach will not be detected until the damage is done and the hacker is long gone" (Lindner, 2001).

"Another layer may be to deploy an IDS system" (Tremblay, 2000). IDS may generally be configured to give you much more information than a firewall. They may also be set up to perform some action based on rules that are set for the IDS. The entire packet may also be captured to review later. Software applications or hardware devices known as an Intrusion Detection System (IDS) automate this process (Landrum, 2001); (PWC, 2000). IDS, like firewalls and other mechanisms mentioned, have limitations. Intrusion detection is therefore defined as the process of monitoring a network to identify, alert operators, or even take some action on network-based attacks or malicious activity (Tremblay, 2000); (Landrum, 2001); (Cott, 2001); (Hartman, 2001); (Dekker, 1997); (Mahadevan, 2001). An IDS provides a wide range of monitoring techniques including packet sniffing, file integrity monitoring, and even algorithms that detect deviations in network traffic. Real-time intrusion detection and reporting systems are 'proactive' deterrents, constantly scanning the network for suspicious activity and automatically logging and terminating those activities before any damage may be done (Lindner, 2001); (Cott, 2001); (PWC, 2000).

There are three approaches to intrusion detection: network based; host-based or a hybrid of the two approaches (PWC, 2000); (Norton, 2000); (Tremblay, 2000); (Jones, 2001). Each of these will be addressed below.

- **Network-based Intrusion Detection** is advantageous because it detects threats and attacks before they reach critical systems (Norton, 2000). "Agents or sensors are typically placed along the perimeter of the network behind firewalls and other access points to detect unauthorized activity that may compromise the perimeter defenses" (Norton, 2000). Network agents may also be placed on subnets in order to scan traffic that may cross the backbone. Placing agents or sensors in front of perimeter devices has the added advantage of detecting probes and attacks that may be stopped by the perimeter devices, and provides substantial information as to the value and effectiveness of those devices. Network-based systems "sniff" the wire, comparing live traffic patterns to a list of known attacks (Hartman, 2001); (PWC, 2000). According to Hartman (Hartman, 2001): "The problem is, if the signature-matching strategy is too specific, any small change by the attacker will allow it to slip through without detection. On the other side, if the signatures are too general, then there are many false alarms that desensitize the user. Striking the right mix is generally difficult and time consuming."

- **Host-based Intrusion Detection** detects threats and attacks on critical systems that may not be detectable by network-based systems including file access and encrypted transmissions (Norton, 2000). Host-based agents may be better than network-based agents at capturing user identifiers (Norton, 2000). Critical systems should be identified and protected (PWC, 2000). Host-based systems use software "agents" that are installed on all servers and report activity to a central console.

  Both methods (network or host based) require a regularly updated list of known attacks, just like anti-virus software. But they also detect an electronic attacker trying different password combinations and alert the operations center or even automatically shut down that part of the network. Neither (network or host based) system is able to detect all known threats and attacks.

- The most effective method is to **combine the two** into a real-time system that detect known attack signatures and patterns, as well as suspicious activity, including probes of the network or critical systems and unauthorized attempts to modify access control mechanisms (Norton, 2000); (PWC, 2000); (Dekker, 1997); (Jones, 2001). The system should be configurable to provide for immediate and automated alerts to such activity, and provide for configurable actions such as logging and automatically terminating the session (Norton, 2000); (PWC, 2000). Immediate and tactful response is necessary in the event of a threat, attack, system compromise, or misuse of network resources. An Incident Response Team should be formed and trained to respond to an identified security event. Automated response capabilities should be incorporated whenever possible (Martin1, 2000).

Tools for intrusion management therefore will include: use of monitoring software, the results of which are checked within a specific time-frame; automatic timeout; trends analysis; bench-marking; survey of markets for latest detection tools, patches, and anti-virus (Martin1, 2000), as well as a system wide audit program. A system-wide audit program should be implemented to provide for immediate and full logging of activity to enforce / achieve user accountability (Norton, 2000); (Martin1, 2000). A central repository for the audit logs will provide immediate and historical reference for an investigation or management request for information. The program should also include security and statistical analysis tools to evaluate the audit logs. The audit program should include procedures to verify the integrity of individual systems and for compliance with existing system and security policies and procedures.

The IS auditor must be aware of the technology and the level of control provided by IDS, but must also be aware that IDS may be a strong addition to security and should never be deployed as a stand-alone solution. IDS should be considered as complementary to defense provided by the firewalls, border, host-protections, etc., not as a replacement for them. IDS must be considered in the design of the audit approach as it provides additional control when it is combined with other technologies mentioned in this chapter.

### 5.4.6 VIRTUAL PRIVATE NETWORKS (VPN)

VPN technology provides the medium to use the public Internet backbone as an appropriate channel for private data communication (Peixian, 2000); (Tyson2, 2001); (Rademacher & Tunstall, 1998). With encryption and encapsulation technology (Peixian, 2000); (PWC, 2000); (Hartman, 2001), a VPN essentially establishes a private passageway through the Internet (Jones, 2001); (Mika et al, 2001).

VPNs will allow remote offices, company road warriors, and even business partners or customers to use the Internet (Peixian, 2000); (PWC, 2001), (Rademacher & Tunstall, 1998) rather than pricey private lines, to reach company networks. So the companies may save a lot of money (Techguide, 2000); (PWC, 2000); (Peixian, 2000); (Zwicky et al, 2000). “This differs from credit card and consumer ordering transactions in that the volume of data between the two parties is greater and the two parties are well known to each other. This means that complex and proprietary encryption and authentication techniques can be used since there is no pretense to offer universal connectivity through this channel” (Cobb, 1999).

According to Hartman (Hartman, 2001):

> “This usually takes advantage of an encryption algorithm with a scheme to regularly exchange keys and can mask all traffic traveling through the ‘tunnel’. The only thing visible to anyone on the Internet is encrypted data between the two VPN end points: all the services used, source / destination addresses utilized, and the data is hidden. An attacker is left without some of the clues that can help determine which traffic is valuable and which is not. All traffic would

have to be decrypted, hopefully at great expense, in the hope that some of it is valuable."

According to Tyson (Tyson2, 2001) "a well designed VPN should incorporate: security, reliability, scalability, network management, and policy management." A VPN should use several methods for keeping a connection and the data secure (Tyson2, 2001); (Rademacher & Tunstall, 1998), amongst others:

- **Firewalls** – firewalls may restrict the number of open ports and the packets and protocols allowed through. Firewalls were discussed in Section 5.4.4 above.
- **Encryption** – encryption was discussed in detail in Section 5.4.1 above.
- **IPSec** – IPSec was mentioned in Section 5.4.1.2 above. IPSec is a secure protocol that provides enhanced security features such as better encryption algorithms and comprehensive authentication and integrity checking. (Tyson2, 2001); (Rademacher & Tunstall, 1998).
- **Tunneling** – VPNs rely on tunneling to create a private network that reaches across the Internet. Tunneling is the process of placing an entire packet within another packet and sending it over the network. The protocol of the outer packet is understood by the network and by the points where the packet enters and exits the network.

The IS auditor should be aware that VPNs provide another alternative to EC payment security control. VPNs in turn use other technologies already described in this chapter (e.g., encryption). When designing an audit approach, the IS auditor must therefore be aware of the control provided by a VPN, and include the evaluation of the VPN as part of the overall control solution where applicable.

### 5.4.7 CLIENT-SIDE AND WEB SERVER VULNERABILITIES

According to AARF (AARF, 2000): "Highly secure cryptographic systems will fail to make significant improvements in security if they operate within an insecure IT infrastructure, which fails to address the basic security issues. Management considers the security infrastructure before evaluating the effectiveness of other security measures."

One of the obvious risks to Web servers as highlighted above is the denial of service attacks. Another issue is related to confidentiality of information that may be stored on Web servers or areas that are accessible by Web servers, such as database servers. If proper controls are not in place, this information could be retrieved, manipulated or destroyed.

Many security weaknesses of Web servers come from configuration issues, because typically, when installing the system, whether it is the firewall or the operating system, by default, a number of network services and protocols are made available. The more services available, the more routes a hacker or cracker will have to penetrate the internal private network.

Components of e-commerce security and controls include documented policies and procedures, thorough top management understanding and support of security, competent (and satisfied) employees and regular monitoring for compliance with standards. The aspects of policies, physical security, server controls, and other related controls will be discussed below for consideration by the IS auditor when the possible control to secure EC payments is considered.

#### 5.4.7.1 Policies

Effective security starts with the development and implementation of a security policy (PWC, 2000); (Techguide, 2000); (Cott, 2001); (Norton, 2000); (de Beaupré, 2001); (Symantec, 2000); (Lindner, 2001). The establishment of security policies is the critical first step in protecting vital enterprise information assets. These policies may also be used as a defense against potential legal liabilities. "Today enterprises must define or redefine their security policies to include rules regarding Internet access and acceptable use" (Symantec, 2000). "The security objective and core principles provide a framework for the first critical step for any organisation developing a security policy. The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organisation" (IFAC, 1998). A good policy unifies all aspects of your security measures into a single strategy and establishes an enforceable set of rules (Dekker, 1997). "Technical controls such as firewalls and IDS are only part of a properly developed security program" (de Beaupré, 2001). The security process is all about applying the appropriate policies through proper procedures and management practices.

According to Lindner (Lindner, 2001): "A security policy establishes the rules or protocol under which the entire organisation or company will be required to operate. The protocol established in an organisation's security policy must be incorporated into the daily habits of every employee. The policy is backed up by an ISO 17799-based standards or procedures document that specifies the access control requirements for information and other assets throughout the company." A security policy needs to lay out, in writing, the security processes of an organisation, and outlines the issues of who, what, when, how, and why of ongoing actions and procedures. It should be a detailed document that identifies risks, defines steps taken to reduce them to acceptable levels, and outlines the tasks and job-descriptions of those directly involved in the enforcement of security in an organisation. According to Hartman (Hartman, 2001) "it is both a checklist and a shield." The checklist portion forces the organisation to ensure it has performed due diligence to create a secure environment. It is also a shield because it outlines people's roles and responsibilities so that they may point to the document to show legitimacy and direction to their actions.

Formal security policies and security standards documents should be tailored specifically for each networking environment. The documents must be distributed to every employee throughout the organisation and be an integral part of an ongoing security education and awareness program (Lindner, 2001); (Pethia et al, 1991). Periodic assessment of systems, policies, and procedures provide for effective augmentation of existing security programs, and the implementation of new security measures and countermeasures (Martin1, 2000); (Mackey & Gossels, 2000).

As described above, security policies are the foundation of effective security and the IS auditor should understand the security environment of an organisation and ensure that aspects related to EC payment security are also covered in the policy. Adherence to the policy should be evaluated by the IS auditor as part of the detailed audit tests.

#### 5.4.7.2 Physical Security

Setting up the best, most-expensive, highest-technology network security is a waste of time and money if access to equipment is not controlled (Hartman, 2001); (Nim, 1998). "If the information is valuable enough to steal, then physical security needs to be up to the task." (Hartman, 2001). A really solid network defense is not complete if someone may physically gain access to equipment or private networks. Equipment should have several layers of physical security (Hartman, 2001); (Unixtools, 2001). Controlled access to the building, a secure network room, locked cabinets for the equipment, and maybe a screen to prevent wireless communications from leaving the room are examples of considerations for physical security. E-commerce servers must also be located in a secured building. Physical security aspects should be specified in the policies and procedures documentation (Martin1, 2000). "Allow only appropriate physical access to computers" (CERT, 1999).

Apart from the physical security aspects mentioned above, consideration should also be given to business continuity planning. Disaster Recovery procedures may be invoked if the severity of the event is high enough to require it. This could result from the destruction of a critical system through an intentional or unintentional event. It may also happen as the result of a natural disaster. Any plan in place should address specific e-commerce needs. Plans should be benchmarked with plans of other similar organisations or environments. Backups should be tested regularly for recovery purposes (Scit, 1998) and stored off-site (Unixtools, 2001). Unlimited Power Supply (UPS) should be used to provide backup electrical power in case of a power failure that affects the computer site and network.

Security Assessment is a tool that may be used to improve security on an ongoing basis. This requires detailed analysis of detected events and their responses lead to continual refinement of the controls. System weaknesses are identified for re-fortification, false positives are eliminated, and thresholds are revised. Security awareness programs are enhanced. This monitoring aspect will also assist the IS auditor to obtain information on possible problems in the security environment. Aspects such as physical security is important to the IS auditor as they form part of the baseline of controls in an organisation i.e., if the basic controls such as environmental controls are not present in an organisation, then the detailed controls over applications such as EC payment systems may be circumvented. The auditor therefore needs to evaluate the basic controls as part of the overall assessment.

#### 5.4.7.3 Server Controls

Securing the Operating System (OS) and Web service is very important (Landrum, 2001). Once it has been compromised, attacks into internal systems are possible.

There are numerous considerations to secure an OS and Internet/web server. Many of these issues have been mentioned in other sections of this chapter. The points below refer specifically to the web server and the operating system issues. Where applicable, the area in this chapter where the issues have been mentioned will be noted below. Areas to consider include:

- Removing default CGI scripts that are not needed -- these are typically not meant for commercial use. (Mehta, 1999); (CERT, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- The web server should utilize the minimum privileges to execute CGI scripts (for example, on a UNIX system, a web server should not execute as 'root'). (Mehta, 1999); (CERT, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Automatic directory listing should be turned off. If this is available, the program sources could be downloaded for examination for potential vulnerabilities. (Mehta, 1999)
- Disabled acceptance of SSIs (Server-Side Includes). SSIs are codes embedded within HTML documents. If these are uploaded to the web server they will execute under the web server privilege. (Mehta, 1999); (Ghosh, 1997).
- Restrict the directories from where CGI scripts are executed from the web server. This is because if CGI scripts are placed in user directories, there could be security threats (Mehta, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Check for proper configuration of cookie distribution. Cookies are sent between a web server and client. This could include authentication information. If the cookies are misconfigured, an unauthorized server might be able to retrieve that cookie, and in theory, could then try to gain unauthorized access to the original web server (Mehta, 1999); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Check to ensure all deadly defaults for the specific application and supporting operating systems are addressed. In order to find out information on the deadly defaults, one may visit the CERT sites (http://www.cert.org), vendor sites, and other security related sites such as http://www.ntsecurity.net for Windows NT. (Mehta, 1999); (Dekker, 1997); (Unixtools, 2001); (Interhack, 1997).
- Turn off network services that are not needed. If the server is a mail server, http and ftp may not be needed. Opportunities for attacks increase with the number of enabled network services. (Mehta, 1999); (Mackey & Gossels, 2000); (CERT, 1999).

- Keep up with the latest operating system (OS) patches. These typically address potential security related OS bugs and holes that have been discovered. (Mehta, 1999); (Interhack, 1997) (Dekker, 1997); (CERT, 1999); (Unixtools, 2001); (Ghosh, 1997); (Garfinkel & Spafford, 1997).
- Use of strong passwords (Landrum, 2001); (Hartman, 2001); (Dekker, 1997); (Terena, 2001); (Pethia et al, 1991); (CERT, 1999); (Unixtools, 2001). Weak passwords feature on the SANS Institute top-ten vulnerabilities list. (Martin1, 2000) Standard controls should apply, such as regular reviews of policies, password length and format, frequent forced change of password (e.g., every 30 days), access rights linked to staff movement, unique identifier, regular audit of the effectiveness of the procedures and applications by staff. This was also discussed in the authorisation section.
- Only installing services that are needed – as discussed in the firewalls and DoS sections (Mackey & Gossels, 2000).
- Document what is installed and monitor for any changes - DoS section.
- Run logging and monitor log files (Landrum, 2001); (Hartman, 2001); (Pethia et al, 1991). Actions of users should be logged and reviewed. (Dekker, 1997); (CERT, 1999).
- Limit open ports to required needs – network services (Fuller, 2000); (Todd, 2000); (PCIS, 2000); (CERT, 1999).
- Block the ability to know OS and web server information (Mackey & Gossels, 2000); (Landrum, 2001).
- Limit access to the system. (Landrum, 2001); (Hartman, 2001); (Unixtools, 2001) Proper authentication techniques are vital. This comes down to having users log onto the system with their own user IDs (never directly as root or administrator) and care being taken to ensure proper authority levels are granted. Different authentication schemes may be utilized such as Kerberos, Radius or LDAP but it comes down to enforcing logins with proper privileges and enforcing strong password usage. Care should also be taken in how a login is achieved. Remote connections across the Internet that use a non-secure medium should always be avoided as they could be easily captured and read (such as telnet) (Landrum, 2001); (Hartman, 2001). DoS section and authentication.
- Keep the system up to date with latest fixes and patches. (Landrum, 2001); (Hartman, 2001); (Cobb, 1999); (Pethia et al, 1991); (CERT, 1999); (Unixtools, 2001). Keep up to date on Bugtraq or CERT advisories, and apply the necessary

patches to ensure there is no exposure to any newly discovered vulnerabilities. (Dekker, 1997); (Mackey & Gossels, 2000). DoS section.

- Image, ghost, or back up the system at appropriate stages (Landrum, 2001); (Scit, 1998); (Martin1, 2000); (CERT, 1999). Backup is mandatory as more reliance is placed on the electronic audit trail. Organisational requirements should dictate the backup policy and this should be coordinated closely with a disaster recovery plan - www.interhack.net - Physical security section,
- Stage and test applications and systems on a staging server prior to implementation of systems, applications or changes in a production environment (Landrum, 2001),
- Change default configurations that may endanger security i.e. customise the operating system to the environment where it is implemented (Mehta, 1999); (Cobb, 1999); (Mackey & Gossels, 2000) – DoS section.

Web network traffic should be separated from the internal network (CERT, 1999); ('Landrum, 2001). This isolates the less secure systems from the more secure making it difficult for an attacker to pick up or sniff internal traffic for valuable information. Using a firewall as previously discussed will do this. Another option is to put all database and file servers providing web support service on a protected subnet. It is also important to disable any source routing that will allow the originator to influence routing decisions.

One component often overlooked in all the various security models, methods, and protocols, is the end user's computer (Rapp, 2001). No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end users' computer. That computer has stored all the digital certificates, most of the consumers' personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers, which store information in some very basic forms, even plain text. This use means the consumers' financial and banking data is only as secure as that computer. To further complicate matters, there are many lap top computers used at home and in business. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data. Controls that minimise this risk are physical security and policies as described above.

Other important considerations to address vulnerabilities on the client or web server site include change management; managing direct connections to server; regular reviews; reconciliation; audit trails; exception reporting, etc. It is not the intention to describe each of these aspects in detail as most aspects may be considered separate areas of audit to an IS auditor. The IS auditor needs to be aware that there are other aspects that could pose a risk to the audit of EC payment security and the results of the audits in the areas mentioned should be considered together with the EC payment security audit. This is required to evaluate the impact on the exposures and to determine whether other controls being evaluated may be strengthened to address those issues. These areas may be addressed by the IS auditor as they pertain to the EC payment security audit.

- **Change management** - There should be approval processes for upgrades and for the implementation of new systems, as well as control over the segregation of duties between the development staff and operational staff and a separate logical development and production environment.
- **Privacy assurance involves** tools that seek to ensure confidentiality, integrity, authenticity and non-repudiation. These are usually achieved through compliance certificates and independent audits.
- **Regular reviews** will provide Quality Assurance that all controls are working effectively. (Martin1, 2000).
- **Reconciliation** control is achieved through independent reconciliation of e-commerce transactions through adequate segregation of duties. (Martin1, 2000).
- **Audit / paper trail** - It is not feasible to envisage that a totally paperless system will have all the key controls to ensure that an adequate audit trail is maintained (Martin1, 2000). Documentation is critical as the paper trail is reduced. (Martin1, 2000). Whatever management decides is critical should be secured in hard copy form. An electronic audit trail must have the ability to follow a transaction from end-to-end and identify all critical steps. Testing of the audit trail should ensure that any errors/ irregularities could be promptly identified and corrected. (Martin1, 2000).
- **Exception reports** - Reports should be concise and should focus on critical activities. They must be in a format that allows prompt monitoring of the e-commerce activities highlighted in the report. (Martin1, 2000).

As soon as technology is developed to address vulnerabilities, new vulnerabilities tend to be identified. Thus, keeping up with security issues is always challenging.

The technologies mentioned above are all used in the effort to address the six major risk areas as mentioned in Section 5.3 above as well as in Chapter 4 of this study. These are all possible controls and it does not necessarily imply that all the above technologies will be present in all organisations that take part in EC payments. The IS auditor needs to understand the impact of the use of these technologies on the control environment. With an understanding of the available technologies, the IS auditor will be equipped with the necessary knowledge to develop an audit approach to EC payment security. This approach is dependent on the specific environment being audited.

## 5.5 CONCLUSION

As described in this chapter, the seven elements of a secure business environment are access control, authentication, availability, data privacy/ confidentiality, integrity, non-repudiation, and web/client side controls. Each is a necessary component for a complete solution. This chapter identified the technologies available to control each of the elements mentioned above.

When the IS auditor encounters electronic commerce activity on the Internet, the auditor needs to determine the sensitivity of the transactions. Transactions that contain confidential or sensitive information should be protected from unauthorised disclosure or alteration – usually through some form of encryption. Transactions that should create concern for the auditor are those that involve payments, shipment of goods, or commitments for services.

No system will, however, be one hundred percent secure. Measures are available to be taken to minimise the possibility of a successful attack. Detection, prevention, and reaction are the measures that do this. Securing a system is therefore the implementation of minimum controls necessary to protect the system with an acceptable degree of assurance.

The audit of the security of EC payments is not a single task or subject but involves many different technologies that need to be taken into account. As discussed in this chapter, many of the technologies aid in securing EC payments. The role of the auditor is to understand the available technologies, assess the risks of implementing the technologies and identify the controls required to ensure that the technologies will provide the assurance required. When the IS auditor understands the available technologies and the controls provided by these technologies, this enables the development of an audit approach.