

# LEGAL INFRASTRUCTURE IN E-COMMERCE

**Dr. Mahesh Saran**

*Lecturer in Basic P. G. College*

*(M.A in Eco. M.Com in A.B.S.T., B.M., E.A.F.M., M.Phil, M.B.A., NET,PhD)*

---

## ABSTRACT

The development and implementation of a harmonized legal infrastructure for commerce can facilitate the development of e-commerce by providing parties with certainty that their transactions will be recognized in multiple jurisdictions.

The term legal infrastructure is a well recognized term in international law that refers to the combination of elements required to make laws work effectively. This paper also provides an overview of the four core elements that might make up a successful E-commerce legal infrastructure. This paper needs to be considered within the context of international developments. UNCITRAL has completed work on Model Laws on Electronic Commerce (1996) and Electronic signatures (2001) and is currently drafting an international convention on Electronic Contracting.

## Introduction

The development and implementation of a harmonized legal infrastructure for ecommerce can facilitate the development of e-commerce by providing parties with certainty that their transactions will be recognized in multiple jurisdictions. The term 'legal infrastructure' is a well-recognized term in international law that refers to the combination of elements required to make laws work effectively.

Legal infrastructure includes:

- **Laws**

The law itself, as passed by Parliament.

- **Regulations and Codes**

Any additional regulatory instruments which provide more specific guidance on how to apply the law, such as regulations and codes of conduct.

- **Regulators**

The regulatory agencies that is responsible for administering and enforcing the law, regulations and codes.

- **Registration, licensing and accreditation**

The system, if applicable, for registering, licensing and/or accrediting individuals and organizations who may provide services under the law. This may include the establishment of licensing and accreditation agencies (although sometimes the regulator may also take this role).

- **Standards**

Government and/or industry may develop technical standards which play a particular role in ensuring compliance with the law. In some instances the law may require compliance with the standard or it may be a licensing or registration requirement.

- **Enforcement and review**

Some legal infrastructures will include a specific forum for review and enforcement of the particular law (such as a specialist Tribunal). In many situations this role will be undertaken by the general court system.

- **Training, education and awareness raising**

The provision of training and education to ensure that the law is understood and complied with, and the raising of awareness of the legal requirements amongst service providers and end users.

**This paper provides an overview of the four core elements that might make up a successful**

**E-Commerce Legal Infrastructure:**

**1. Online formation of contracts**

The ability to form contracts via electronic means, free of legal restrictions which would require paper records or hand-written signatures.

**2. Jurisdiction**

The ability to determine the jurisdiction of any e-commerce transaction, including determining the applicable law and the appropriate forum for the resolution of disputes.

**3. Authentication**

The ability to reliably authenticate the parties to an e-commerce transaction and the content of any messages exchanged in the transaction.

**4. Electronic Payment**

The ability to complete an e-commerce transaction via a secure and reliable electronic transfer of value.

This paper needs to be considered within the context of international developments. UNCITRAL has completed work on Model Laws on Electronic Commerce (1996) and Electronic Signatures (2001) and is currently drafting an international convention on Electronic Contracting.

**ONLINE FORMATION OF CONTRACTS**

A contract is a legally binding agreement between two or more people or organizations. The terms of a contract may be expressed in writing or orally, implied by conduct, industry custom, and law or by a combination of these things.

A binding contract is usually formed when the following elements are satisfied:

- One party makes an offer setting out the terms of the proposed contract to another party or parties. The terms must be sufficiently certain.
- An unequivocal acceptance of the offer is communicated to the party who made the offer.
- In some jurisdictions, the contract must be supported by consideration or 'value'. Consideration is sometimes described as a 'promise for a promise'.
- The parties to the transaction must have an intention to create legal relations. Courts will not force people into a contract if they did not intend to be legally bound.

If any one of these elements does not exist, or is negated (for example, due to fraud), there will not be a contract between the parties.

### **E-Commerce and Contracts**

Often in e-commerce transactions the parties never meet each other face to face. This creates obvious trust issues between the parties and also makes it difficult to ensure the parties act lawfully and that the transaction itself is legal. This is a particular concern where there is unequal bargaining power between the parties. Online contracts therefore play an important role in e-commerce as they stipulate the terms and conditions governing the transaction. A body of law is developing to ensure certainty in e-commerce and the online contracting process.

There is no reason, in principle, that most contracts cannot be formed online either by email exchanges, 'click through' agreements or executed by use of digital signatures. In each case, the question will be whether anything in the formation of the contract might leave either party at risk that the other party will later challenge the enforceability of the contract.

### **Legal Infrastructure Required for Online Formation of Contracts**

The following legal infrastructure may be required to enable the online formation of contracts:

- **Laws**

A broad law may be required which confirms that contracts can be formed via electronic means. This law may contain some limited exceptions.

- **Regulations and Codes**

Usually no further regulation or codes are required for this aspect of e-commerce law.

- **Regulators**

Usually no specific regulator is required for this aspect of e-commerce law. There is no specific regulator in most jurisdictions for contract law.

- **Registration, licensing and accreditation**

Usually no specific registration, licensing or accreditation is required for this aspect of e-commerce law. All parties are presumed to have the capacity and ability to enter into online contracts in accordance with the law, without the need to be registered or obtain particular accreditation.

- **Standards**

Technical standards for the formation of online contracts may be useful, but are not an essential

element of this element of e-commerce law. They should not be required in jurisdictions where a 'technology neutral' approach has been taken.

- **Enforcement and review**

The general court system is likely to provide adequate enforcement and review of the online formation of contracts. However, there may need to be some minor changes to court rules and procedures regarding the admission of evidence, discovery procedures etc.

- **Training, education and awareness raising**

Education regarding the correct formation of online contracts may be important amongst industry and consumers. There may also need to be some general awareness raising activity to overcome any assumption by parties that all contracts must be 'in writing'.

### JURISDICTION

In broad terms, jurisdiction refers to the power and authority of a government to legislate, adjudicate and enforce its laws. Jurisdiction is dependent on the sovereignty of the government and therefore is usually territorial. It is bound by territorial limits and usually does not extend beyond the territory.

The basis of jurisdiction can be either:

1. The party (for example, the party's nationality, domicile, presence or residence in the forum, possession of property in the forum, etc); or
2. The cause of action (usually whether the act or event giving rise to the proceedings occurred wholly or partly in the forum).

The term 'forum' refers to the geographical place where jurisdiction is asserted. Obviously this can be a difficult concept to apply to e-commerce transactions.

### **E-Commerce and Jurisdiction**

As discussed above, jurisdiction is usually subject to territorial limits. How does this apply to the Internet where there may be no territorial borders and where the defendant may not have any physical presence in the forum?

The question of jurisdiction for online transactions is divided into two parts:

- The applicable law is the law under which a dispute should be decided.

- The forum is the location in which a court should sit to consider the dispute.

Unfortunately, attempts to agree on how the jurisdiction of an Internet transaction should be determined have, to date, failed. The OECD attempted to settle this matter when writing their Consumer Protection in Electronic Commerce Guidelines in 1999. However, the members could not agree on an appropriate formula, with some countries supporting the ‘location of the business’ test and others supporting the ‘residence of the consumer’ test.

In the absence of a general agreement on the jurisdiction of Internet transactions, existing legal principles must apply. There have been a number of cases worldwide that have considered this issue, but unfortunately they have been inconclusive, with various courts arriving at opposite rulings.

### **Legal Infrastructure Required for E-commerce Jurisdiction**

The following legal infrastructure may be required to resolve questions of E-commerce jurisdiction:

- **Laws**

On this issue national laws do not play a significant role. Public international law and international and regional agreements and treaties are more significant.

- **Regulations and Codes**

Regulations and codes are unlikely to be required.

- **Regulators**

Usually no specific regulator is required for this aspect of e-commerce law. In any case, there is no appropriate regional or international regulator who could fulfil this role. Some national regulators may play a role in restricting the scope of ‘choice of jurisdiction’ clauses.

- **Registration, licensing and accreditation**

Usually no specific registration, licensing or accreditation is required for this aspect of e-commerce law.

- **Standards**

Some international standards have already been developed for the allocation of jurisdiction in online contracts. For example, the International Chamber of Commerce publishes ‘model clauses’ which can be included in e-commerce contracts. These help to improve consistency in e-commerce transactions and promote best practice.

- **Enforcement and review**

The courts will have a significant role in enforcement and review of jurisdiction. In the absence of international and regional agreements and treaties, the courts will decide the jurisdiction of e-commerce transactions.

- **Training, education and awareness raising**

Education regarding jurisdiction may become an important requirement, especially if no international or regional agreement is reached on this matter.

### **AUTHENTICATION**

A technical definition of authentication is the process of establishing whether someone or something is who or what its identifier states it is. An authentication process may be enabled by:

- **Something you know**

Such as a PIN or password;

- **Something you have**

Such as smartcards, challenge-response mechanisms, or public-key certificates; or

- **Something you are**

Such as positive photo identification, fingerprints, and biometrics.

The key benefit of electronic authentication is that it enables electronic transactions to take place in an environment of trust and confidence. The Internet, for example, is an open network where the community has a low level of trust. However, authentication tools can provide greater confidence in the identity, validity and authenticity of participants, sites and objects.

Authentication helps to address some of the legal risks in electronic transactions

- **Confidentiality** - people communicating information such as trade secrets, medical records, lawyer-client communications, credit card and bank account details may be required by law or agreement to keep that information confidential.
- **Authentication** - the identification and verification of parties and data transmission is essential to the formation of a binding contract and may assist the allocation of liability for fraud between the parties.
- **Message integrity** - the formation of a binding contract requires a 'meeting of minds' on the same terms of the contract. The communication sent must be the same as the

communication received. A contract may not be enforceable if one party can establish that data relating to the formation of the contract have been corrupted or interfered with.

- **Repudiation of contract** - where parties agree on the authentication and security methods to be used to form a contract, a party may be prevented from denying the existence, accuracy or validity of a communication which conforms to the agreed methods.

### **E-Commerce and Authentication**

For the purposes of this paper, we consider the role that digital signatures might play in authentication for e-commerce transactions. A digital signature is not a computerized image of a hand written signature. It is unique for each electronic document produced as it is derived from the document itself. Any change in the document would result in a different signature allowing the recipient to ascertain whether an alteration has occurred after the first digital signing.

A digital signature uses cryptography to provide a method for signing electronic contracts which establishes the:

- **Identity** of the parties to the contract;
- **Integrity** of the terms and conditions governing the contract;
- **Timeframe** of the terms and conditions; and
- **Acceptance** of the terms and conditions by the parties to be bound.

### **Legal Infrastructure Required for Authentication**

The following legal infrastructure may be required to enable the authentication aspects of E-commerce:

- **Laws**

National laws, based on the UNCITRAL Model Laws, may be required to ensure that digital signatures can be used with confidence in e-commerce transactions.

- **Regulations and Codes**

Additional regulations and codes may be required which provide more specific guidance on particular forms of authentication. In addition some form of regulation or code may be required to establish the rules for recognizing digital certificates issued in other jurisdictions.



- **Regulators**

Either an existing regulator or a new regulator may need to take responsibility for establishing and maintaining the integrity of the Public Key Infrastructure. However, this role may also be undertaken by a non-Government agency under certain conditions.

- **Registration, licensing and accreditation**

Some service providers and parties within a Public Key Infrastructure will need to be registered. Mandatory or voluntary licensing may be required. Some form of accreditation will be essential to ensure that high standards are maintained in the issuing of digital certificates.

- **Standards**

Technical standards will play an important role in ensuring interoperability. These standards may be referred to in the law or regulations, or their use might be left to market forces.

- **Enforcement and review**

The general courts will play a limited role in the enforcement and review of the use of digital certificates. Some enforcement and review activities may also be undertaken by the regulator.

- **Training, education and awareness raising**

Training, education and awareness raising will all play an important role in the promotion of the use of digital certificates.

## **ELECTRONIC PAYMENT**

Payment is the means by which most e-commerce transactions can be successfully concluded. This will usually be achieved by the electronic transfer of value between the parties.

Of course, payment is not an essential element of all e-commerce transactions. Many e-Government services are provided without a requirement for payment.

### **E-Commerce and Payment**

There are a number of ways payment of goods can be effected online. A paramount concern when using such electronic payment systems is the security of the transaction, including ensuring that payment reaches the vendor, and the customer's personal information or identifier is not intercepted and used without the customer's knowledge.

The following are some of the common electronic payment systems in the e-commerce environment:

- **Internet banking**

Internet banking is one of the most successful applications of e-commerce, with high levels of registration and use, and medium levels of consumer confidence.

- **Credit cards**

Credit card details are usually entered into a merchant's web form on the Internet. The details may be manually sent by e-mail and verified by the merchant as a mail-order/telephone-order (MOTO) transaction, or encrypted using secure socket layer (SSL) techniques and then automatically processed by the relevant bank.

- **Digital cash**

Digital cash is a payment or transfer of value initiated and processed electronically within current inter-bank payment systems. Digital cash is effectively money stored as computer code. The digital cash is essentially a message issued by a bank containing its value, the bank's identity, the bank's Internet address and a serial number. The digital cash is securely transferred using data encryption methods.

- **Stored Value Cards (SVCs) (including smart cards)**

Stored value cards are plastic cards that can contain a microprocessor chip (more commonly known as smart cards). The chip stores more information than magnetic strip cards and can perform simple computing operations. The SVC represents a value of prepaid funds with a counter that keeps track of the amount which reduces with each payment until exhausted and then is either recharged or thrown away.

## **Legal Infrastructure Required for Electronic Payment**

The following legal infrastructure may be required to enable the electronic payment aspects of E-Commerce:

- **Laws**

National laws regulating banking, payment systems and the provisions of credit may have to be amended to include coverage of electronic payment systems.

- **Regulations and Codes**

Most of the detailed regulation of electronic payment systems will be contained in specific regulations and codes of conduct. Laws on this topic tend to be very broad.

- **Regulators**

Most electronic payment providers will fall within the existing jurisdiction of national financial system regulators, depending on the nature of the service provided.

- **Registration, licensing and accreditation**

Most electronic payment providers will require a licence at the national level.

- **Standards**

There are a plethora of international and national technical standards which apply to the electronic transfer of funds. These help to ensure interoperability and to encourage best practice.

- **Enforcement and review**

The general courts will play a limited role in the enforcement and review of the use of electronic payment systems. Some enforcement and review activities may also be undertaken by the relevant regulator/s.

- **Training, education and awareness raising**

Training, education and awareness raising will all play an important role in the promotion of the use of electronic payment systems. This is essential in developing consumer trust and confidence in e-commerce.

### Summary - Legal Infrastructure Matrix

<b>E-Commerce Legal Infrastructure Components</b>	<b>1. Online formation of contracts</b>	<b>2. Jurisdiction</b>	<b>3. Authentication</b>	<b>4. Electronic Payment</b>
<b>Summary</b>	The ability to form contracts via electronic means, free of legal restrictions which would require paper records or hand-written signatures.	The ability to determine the jurisdiction of any e-commerce transaction, including determining the applicable law and the appropriate forum for the resolution of disputes.	The ability to reliably authenticate the parties to an e-commerce transaction and the content of any messages exchanged in the transaction.	The ability to complete an e-commerce transaction via a secure and reliable electronic transfer of value.
<b>A. Laws</b>	A broad law may be required which	On this issue national laws will	National laws, based on the UNCITRAL	National laws regulating

	confirms that contracts can be formed via electronic means. This law may contain some limited exceptions.	not play a significant role. Public international law and international and regional agreements and treaties will be more significant.	Model Laws, may be required to ensure that digital signatures can be used with confidence in e-commerce transactions.	banking, payment systems and the provisions of credit may have to be amended to include coverage of electronic payment systems.
<b>B. Regulations and Codes</b>	Usually no further regulation or codes are required for this aspect of e-commerce law.	Regulations and codes are unlikely to be required.	Additional regulations and codes may be required which provide more specific guidance on particular forms of authentication. In addition some form of regulation or code may be required to establish the rules for recognising digital certificates issued in other jurisdictions.	Most of the detailed regulation of electronic payment systems will be contained in specific regulations and codes of conduct. Laws on this topic tend to be very broad.
<b>C. Regulators</b>	Usually no specific regulator is required for this aspect of e-commerce law. There is no specific regulator in most jurisdictions for contract law.	Usually no specific regulator is required for this aspect of e-commerce law. In any case, there is no appropriate regional or international regulator who could fulfil this role. Some national regulators may play a role in restricting the scope of 'choice of jurisdiction' clauses.	Either an existing regulator or a new regulator may need to take responsibility for establishing and maintaining the integrity of the Public Key Infrastructure. However, this role may also be undertaken by a non-Government agency under certain conditions.	Most electronic payment providers will fall within the existing jurisdiction of national financial system regulators, depending on the nature of the service provided.
<b>D. Registration, licensing and accreditation</b>	Usually no specific registration, licensing or accreditation is required for this aspect of e-commerce law. All parties are presumed to have the capacity and ability to enter into online contracts in accordance with the law, without the need to be	Usually no specific registration, licensing or accreditation is required for this aspect of e-commerce law..	Some service providers and parties within a Public Key Infrastructure will need to be registered. Mandatory or voluntary licensing may be required. Some form of accreditation will be essential to ensure that high standards are maintained in the issuing of digital certificates.	Most electronic payment providers will require a licence at the national level.

	registered or obtain particular accreditation			
<b>E. Standards</b>	Technical standards for the formation of online contracts may be useful, but are not an essential element of this element of e-commerce law. They should not be required in jurisdictions where a 'technology neutral' approach has been taken.	Some international standards have already been developed for the allocation of jurisdiction in online contracts. For example, the International Chamber of Commerce publishes 'model clauses' which can be included in e-commerce contracts. These help to improve consistency in e-commerce transactions and promote best practice.	Technical standards will play an important role in ensuring interoperability. These standards may be referred to in the law or regulations, or their use might be left to market forces.	There are a plethora of international and national technical standards which apply to the electronic transfer of funds. These help to ensure interoperability and to encourage best practice.
<b>F. Enforcement and review</b>	The general court system is likely to provide adequate enforcement and review of the online formation of contracts. However, there may need to be some minor changes to court rules and procedures regarding the admission of evidence, discovery procedures etc.	The courts will have a significant role in enforcement and review of jurisdiction. In the absence of international and regional agreements and treaties, the courts will decide the jurisdiction of e-commerce transactions.	The general courts will play a limited role in the enforcement and review of the use of digital certificates. Some enforcement and review activities may also be undertaken by the regulator.	The general courts will play a limited role in the enforcement and review of the use of electronic payment systems. Some enforcement and review activities may also be undertaken by the relevant regulator/s.
<b>G. Training, education and awareness raising</b>	Education regarding the correct formation of online contracts may be important amongst industry and consumers. There may also need to be some	Education regarding jurisdiction may become an important requirement, especially if no international or regional agreement is reached on this matter.	Training, education and awareness raising will all play an important role in the promotion of the use of digital certificates.	Training, education and awareness raising will all play an important role in the promotion of the use of electronic payment systems. This is essential in

	<p>general awareness raising activity to overcome any assumption by parties that all contracts must be 'in writing'.</p>			<p>developing consumer trust and confidence in e-commerce.</p>
--	--	--	--	--

IJSP