

Course: Information Security Management in e-Governance

Day 3

Session 2: Regulatory framework of e-Governance

Agenda

- Need for regulatory framework for e-Governance
- IT Act 2000, its amendments and related provisions
- Other policy frameworks related to e-Governance (data protection, privacy, cyber laws, IPR...)
- Impact of e-Governance on existing legislations and act

Why a Regulatory Framework?

- E-Commerce & E-Government service delivery involves:
 - ✓ Use of Electronic Records
 - ✓ Electronic Transactions
 - ✓ Electronic Contracts
 - ✓ Handling of citizen data & privacy issues
 - ✓ Issue of Certificates electronically...
- Other e-Governance specific aspects include:
 - ✓ Legal backing to e-Governance initiatives
 - ✓ Formalisation of Standards and Interoperability norms
 - ✓ Data Protection, Privacy and IPR issues
 - ✓ Mechanism for socially inclusive service delivery

Most of these issues are common also to the wider e-Commerce landscape of the country, and need to be addressed to build trust in electronic transactions

Electronic Transactions: How are they different?

- Challenges posed by e-Commerce:
 - Classification difficulties: the virtual goods
 - New contract types: web hosting, web server etc.
 - Transactions taking place in open platforms
- ... but the essence of business transactions remains the same.
- Conventional law has not become obsolete...
 - “On line” contracts are not different from “off line”
 - Medium of a transaction is generally irrelevant for the law.
- ...and nevertheless, it requires some adaptation.

Legal Obstacles to e-Commerce

- Legal concepts are based on the existence of a tangible medium:
 - “instrument”, “document”, “original”, “signature”



- Legal concepts based on geographic location:
 - “delivery”, “receipt”, “dispatch”, “surrender”
- Functional Equivalence needs to be established between the Manual and Electronic media used (electronic records, signatures, documents, communication)

Achieving Functional Equivalence

- Paper-based requirements (“writing”, “record”, “signature”, “original”) specify certain purposes and functions
- Consider criteria necessary to replicate those functions and give electronic data the same level of recognition as information on paper
 - A paper document signed by an individual fulfils the following criteria:
 - The document can be attributed to the individual as the signature is unique to the person (authenticity, non repudiation and integrity)
 - If the electronic document can replicate these functions (e.g. by use of a Digital Signature Certificate attached to the document), it is functionally equivalent to the paper document



Providing legal backing for Functional Equivalence

If certain conditions are fulfilled, the legal value of electronic transactions shall be equivalent to that of other forms of communication, such as the written form.

Indian IT Act, 2000 achieves this by defining the conditions by which equivalence can be ascertained between paper based and electronic documents

This can be achieved by a single enactment of Law without having to review every single piece of existing legislation establishing formal requirements

Genesis of IT Act - The UNCITRAL Model Law

- As electronic transactions extends across national boundaries, there is a need for international harmonization in IT Laws
- The United Nations Commission on International Trade Law (UNCITRAL) is the legal body of the United Nations system in the field of international trade law
- UNCITRAL drafted the “UNCITRAL Model Law on Electronic Commerce - 1996” for adoption by countries
- The e-Commerce / IT Laws of most countries are modelled on UNCITRAL Model Law

Objectives of the Model Law

- To *facilitate* rather than *regulate* electronic commerce
- To *adapt* existing legal requirements
- To provide basic *legal validity* and raise *legal certainty*

- Basic Principles of Model Law

- Functional Equivalence
- Media and Technology Neutrality
- Party Autonomy

Law to provide conditions for equivalence of handwritten (manual) and electronic records, signatures etc

Law to provide the transacting parties the autonomy to choose to use e-Commerce and decide security levels

Law to treat all technologies on an equal footing

Slide 9

IT Act, 2000

- Came into effect from October 17th, 2000 on the lines of the UNCITRAL Model Law
- India is the 12th nation in the world to adopt Cyber Laws
- The Act applies to the whole of India and also applies to any offence or contravention there under committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India
- 94 Sections segregated into 13 Chapters and 4 Schedules
- IT Act 2000 was amended through the Information Technology Amendment Act, 2008 which came into effect from October 27, 2009

IT Act and amendments is equivalent to:

- at least 45 (and counting) U.S. Federal enactments
- at least 598 (and counting) U.S. State enactments
- at least 16 (and counting) UK enactments

Objectives of IT Act, 2000

- Legal Recognition for transactions carried out by means of electronic data interchange
 - Digital Signatures and Regulatory Regime for Digital Signatures
 - Admissibility of Electronic Documents at par with paper documents
- E-Governance
 - Electronic Filing of Documents and E-Payments
- Define Civil wrongs, Offences, punishments
 - Investigation, Adjudication of Cyber crimes
 - Appellate Regime
- Amend existing Acts to address IT Act provisions
 - Indian Penal Code & Indian Evidence Act - 1872
 - Banker's Books Evidence Act – 1891 & Reserve Bank of India Act – 1934

IT Act – Important Definitions

- “access” means gaining entry into ,instructing or communicating with the logical, arithmetic or memory function resources of a computer, computer resource or network;
- "computer" means electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or relates to the computer in a computer system or computer network;
- "computer network" means the inter-connection of one or more computers through-
(i) the use of satellite, microwave, terrestrial lime or other communication media;
and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

IT Act – Important Definitions

- "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- "security procedure" means the security procedure prescribed by the Central Government under the IT Act, 2000.
- secure electronic record – where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification

Admissibility of Electronic Records

As per the definition provided in IT Act, 2000

- "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche

Section 4 of the IT Act provides legal recognition to electronic records

- *“If any information is required in printed or written form under any law the Information provided in electronic form, which is accessible so as to be usable for subsequent use, shall be deemed to satisfy the requirement of presenting the document in writing or printed form”*

Electronic Records in Government Service Delivery

Section 4: Where any law provides for:

- the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government;
- the issue or grant of any license, permit, sanction or approval in a particular manner;
- the receipt or payment of money in a particular manner;

Section 9 of the Act clarifies that no person can insist that a government body should accept, issue, create, retain and preserve any document in electronic form

*“Such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by **means of such electronic form** as may be prescribed by the appropriate Government”*

The Law also gives recognition for publication of Rules, Regulation etc in Electronic Gazette

Authentication of Electronic Records

- Section 3: Any electronic record may be authenticated by a subscriber using a Digital Signature

“The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record”

Digital Signature Regime will be discussed in detail in the next session

Retention of Electronic Records

Section 7: Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if:

- the information contained therein **remains accessible** so as to be usable for a subsequent reference;
- the electronic record is **retained in the format** in which it was originally generated, sent or received or in a format **which can be demonstrated** to represent accurately
- the details which will facilitate **the identification of the origin, destination, date and time of dispatch or receipt** of such electronic record are available in the electronic record:

Attribution of Electronic Records

An electronic record can be attributed to the originator:

- if it was sent by the originator himself;
- by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
- by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgement of receipt of Electronic Records

An electronic record can be attributed to the originator:

- If Originator has not specified particular method - Any communication automated or otherwise from the addressee or conduct from the addressee indicating the receipt of the record
- If specified that the receipt is necessary, then unless acknowledgement has been received Electronic Record shall be deemed to have been never sent
- Where acknowledgement is not received within time specified or within reasonable time the originator may give notice to treat the Electronic record as though never sent

Digital Signatures – IT Act Amendment

- The PKI Digital Signature Regime proposed by IT Act of 2000 is Technology specific
- This is against the global best practices as envisaged in the UNCITRAL Model Law on e-Signatures – 2001:
 - ✓ Any electronic signature technology which fulfills the criteria of equivalence between handwritten and electronic signatures, should be admissible
- Accordingly, the IT Act Amendments of 2008 provided recognition to other electronic signature technologies, which are identified by the Central Government

Major themes of IT Amendment Act, 2008

- To make the Act Technology Neutral:
 - ✓ Enabling provision added to replace Technology specific “Digital Signatures” to technology neutral “Electronic Signatures”. Central govt to specify accepted forms of electronic signatures in the Rules
- To enable the IT Act to be easily amendable with advances of Technology
 - ✓ Exclusion of applicability modified to allow Central Government to change the list by executive orders (Rules)
- Enabling provision for PPP in e-Gov service delivery
- Provisions for more extensive coverage of Cyber Crimes including Cyber Terrorism

Other Amendments in ITAA 2008

To be taken up in subsequent sessions:

- Amendments in Cyber Crime Regulation (Session 6)
- Amendments to Schedules concerning existing Acts (Session 7)

Statutory bodies under IT Act and its Amendments

- Controller of Certifying Authorities: Regulating agency for the working of Licensed Certifying Agencies (already discussed in the Digital Signature Regime)
- Indian Computer Emergency Response Team (CERT – in): National Nodal Agency in the area of Cyber Security
- Cyber Appellate Tribunal: Appellate body in Cyber Crime related cases (discussed in Session 6)



Indian Computer Emergency Response Team (CERT – in)

- Sub section 70A (1) of the ITAA 2008:
 - ✓ The Central Government may, by notification published in the Official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection
- Accordingly, 70B (1), stipulates that the identified nodal agency be called Indian Computer Emergency Response Team
- CERT – in to be headed by a Director General and perform functions related to ensuring Cyber Security in the country

CERT – in : Mission and Mandate

Mission: ‘Alert, Advice and Assurance’

‘Ensure security of cyber space in the country’

by

‘Enhancing the security of communications and Information infrastructure’

through

‘Proactive action and effective collaboration aimed at security incident prevention, prediction, response & recovery and security assurance’

Functions of CERT - in

- Following are the the functions of CERT-in:
 - ✓ collection, analysis and dissemination of information on cyber incidents;
 - ✓ forecast and alerts of cyber security incidents;
 - ✓ emergency measures for handling cyber security incidents;
 - ✓ coordination of cyber incidents response activities;
 - ✓ issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
 - ✓ such other functions relating to cyber security as may be prescribed.
- Section 70B (6): CERT – in may call for information and give direction to the service provides, intermediaries, data centres, body corporate and any other person.
- No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by CERT - in

Agenda for the session

- Impact of GPR / e-Governance projects on Legal Framework: Institutional Structures, Statutory Powers
- Legislation that may need amendments, specific to e-Governance initiatives (e.g. Changes in Public Procurement Act, Financial Rules to enable e-Procurement, e.g. Changes in Land Revenue Act to allow for electronic Land Records, etc.)

Impact of e-Governance on Legal Framework

Government Processes are related to Legal Framework..

- Processes are designed /processes evolve in accordance with the legislation governing that particular domain
- Some of these Legislations may be old and antiquated:
 - ✓ E.g. Laws governing the Land Record Management include - Registration Act 1905, Stamp Act 1899, Survey & Boundaries Act 1923, Revenue Code 18xx
- Basis of the legal system is to put in controls, and not better service delivery
- Acts are department-centric, not citizen-centric
- Rules are complex and tedious
 - ✓ 10,000 rules, 0.1 million forms!
- E-Government allows for controls to be enforced in a cost-effective manner, allowing departments to concentrate on better service delivery

Many a time, process / service delivery problems can be traced back to legislative intent...



- Legislation was well intentioned and relevant at the time it was drafted
- Focused more on control and ensuring compliance, rather than service delivery
- Rules added along the way, making the legal framework complex and tedious

Process problems arose due to the focus on control...



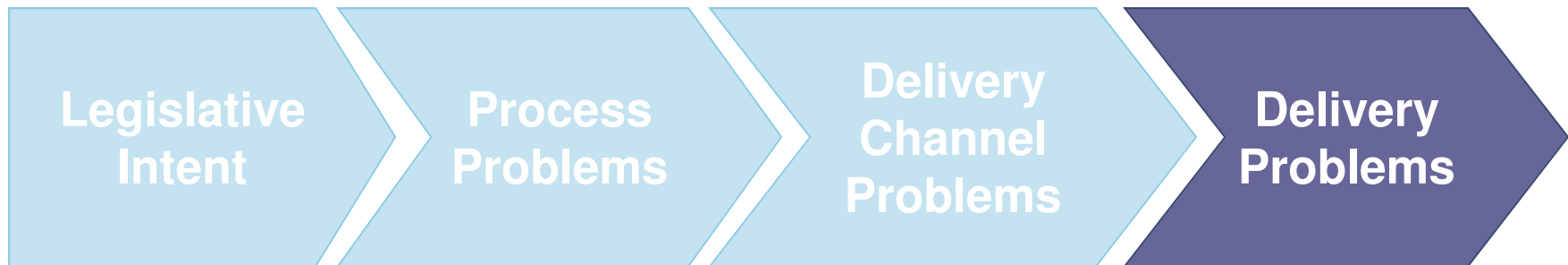
- Asking for too much information (by every agency, on every occasion)
- Burden of proof thrown on Citizen (Attachments, Annexures, Attestations)
- Complexity of rules & regulations (Anything to do with money is more complex!)
- Heavy reliance on manual systems
- No concept of Quality Assurance

Which was compounded by problems in delivery channels...



- Jurisdiction (too many 'narrow domestic walls!', too many 'single windows')
- Restricted timings
- Disparate and sub-optimal delivery networks
- No choice of delivery channels
- Process & Delivery Channel often combined resulting in delay, malpractice

Which ultimately resulted in degraded service delivery...



- Mindset & attitudinal problems
- Delivery Agents unsuitable (Unqualified/ Untrained/ Unequipped)
- Lack of empowerment of front-end people
- Lack of dedicated delivery teams
- Delivery is handled on a part-time basis
- Lack of service levels, measurement systems

Some of the considerations when processes were designed...

...are no longer true with advances in technology

Information can appear at only one place at a time

Only experts can perform Complex work

We should choose between Centralization & Decentralization

Managers make ALL the decisions

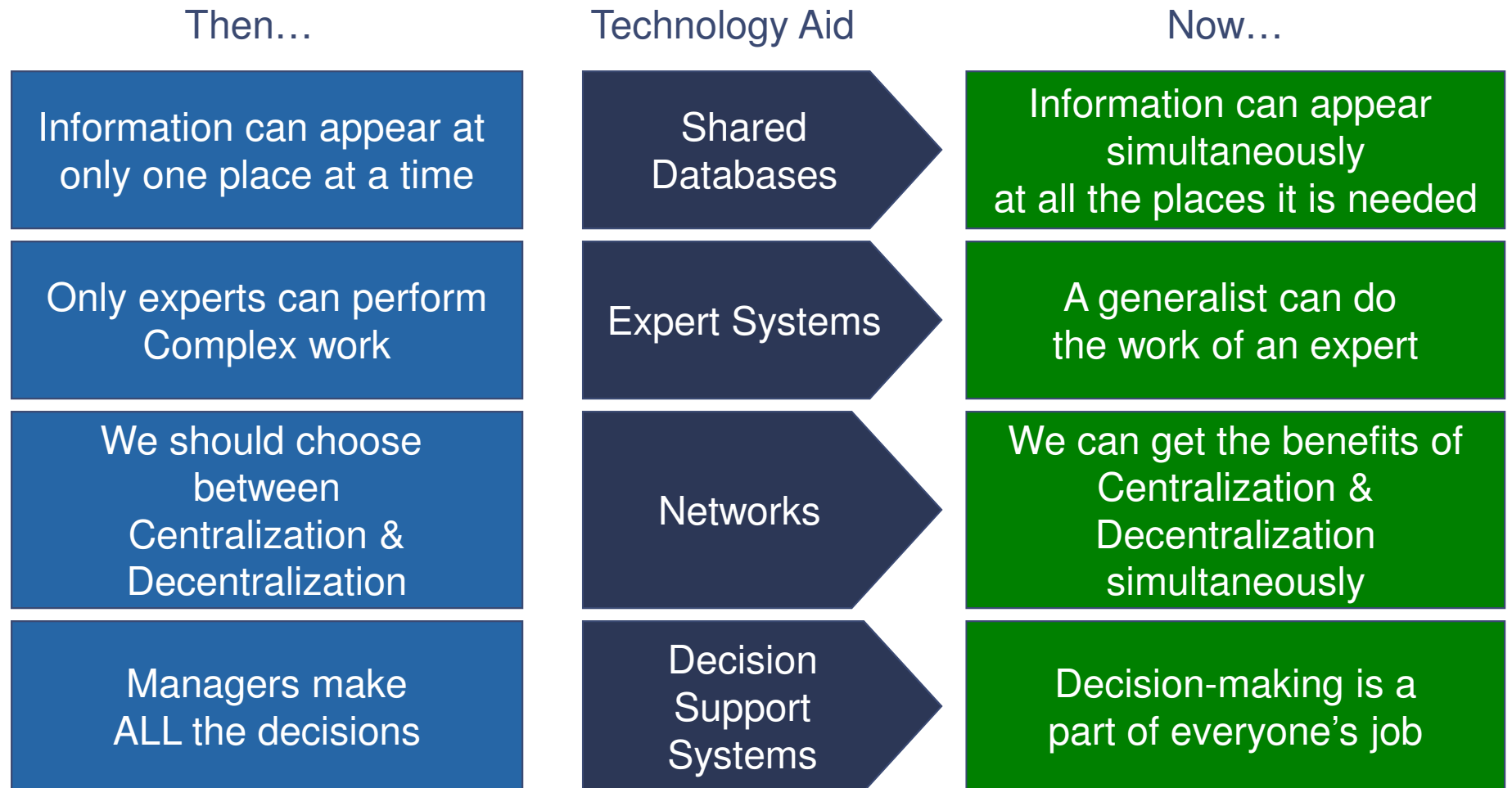
Field personnel need a fixed place for communications

Personal contact with customer Is the best contact

You have to find out where things are..

E-Government allows for best of both worlds – better controls and better service delivery

But they are no longer valid in the e-Government context (1/2)



But they are no longer valid in the e-Government context (2/2)

Then...

Field personnel need a fixed place for communications

Personal contact with customer is the best contact

You have to find out where things are..

Plans get revised periodically

Technology Aid

Wireless, Laptops & PDAs

Interactive Video

RFID

High Performance Computing

Now...

Field personnel can send and receive Information anytime, anywhere

Virtual contact with Customer is more convenient

Things tell you where they are !

Plans get revised dynamically

Illustrative Case: MCA21

- MCA21 is one of the Central Mission Mode Projects, designed for electronic service delivery by the Ministry of Company Affairs (MCA)
- The project involved large scale Government Process Re-engineering and IT enablement of processes
- The Legal framework governing the regulation of corporate sector in India (companies registration, compliance filing etc) was amended to give sufficient legal backing to the e-Governance initiative
- As on date, all company registrations and compliance filings are mandated to be filed online

MCA21 – Background

- Ministry of Company Affairs' primary function is the administration of Companies Act, 1956, other allied Acts and rules & regulations framed there-under
- The following services were proposed to be made online through the MCA21 project:
 - Registration and incorporation of new companies
 - Filing of Annual Returns and Balance Sheets
 - Filing of forms for change of names/address/Director's details
 - Registration and verification of charges
 - Inspection of documents
 - Applications for various statutory services from MCA
 - Investor grievance redressal

Situation before MCA21

- Company incorporation and compliance filing was done manually at Registrar of Companies (RoC) offices in States and Union Territories
- Each RoC also acted as the registry of records relating to the companies registered with them, which are made available for inspection by members of public on payment of prescribed fee



- Company data in silos in RoC offices in paper form
- Time consuming process for filing and inspection
- Lack of transparency and reduced service levels
- Investor grievances given low priority
- Difficulty in doing any quantitative analysis of corporate information

MCA21 impact

After MCA21 rollout

- Online registration and incorporation of companies
- Simplified and easy mode of filing of e-forms / returns
- Online registration and verification of changes
- Centralized Data repository and online inspection of documents by public

Impact

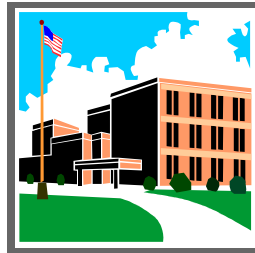
- Anytime / anywhere service to corporate
- Corporate centric approach
- Increased transparency
- Enhanced service levels
- MCA employees devote more time to doing value added tasks including data analysis
- Timely grievance redressal

Snapshot of MCA21 implementation (1/3)

Front Office



e-Filing



Facilitation centres

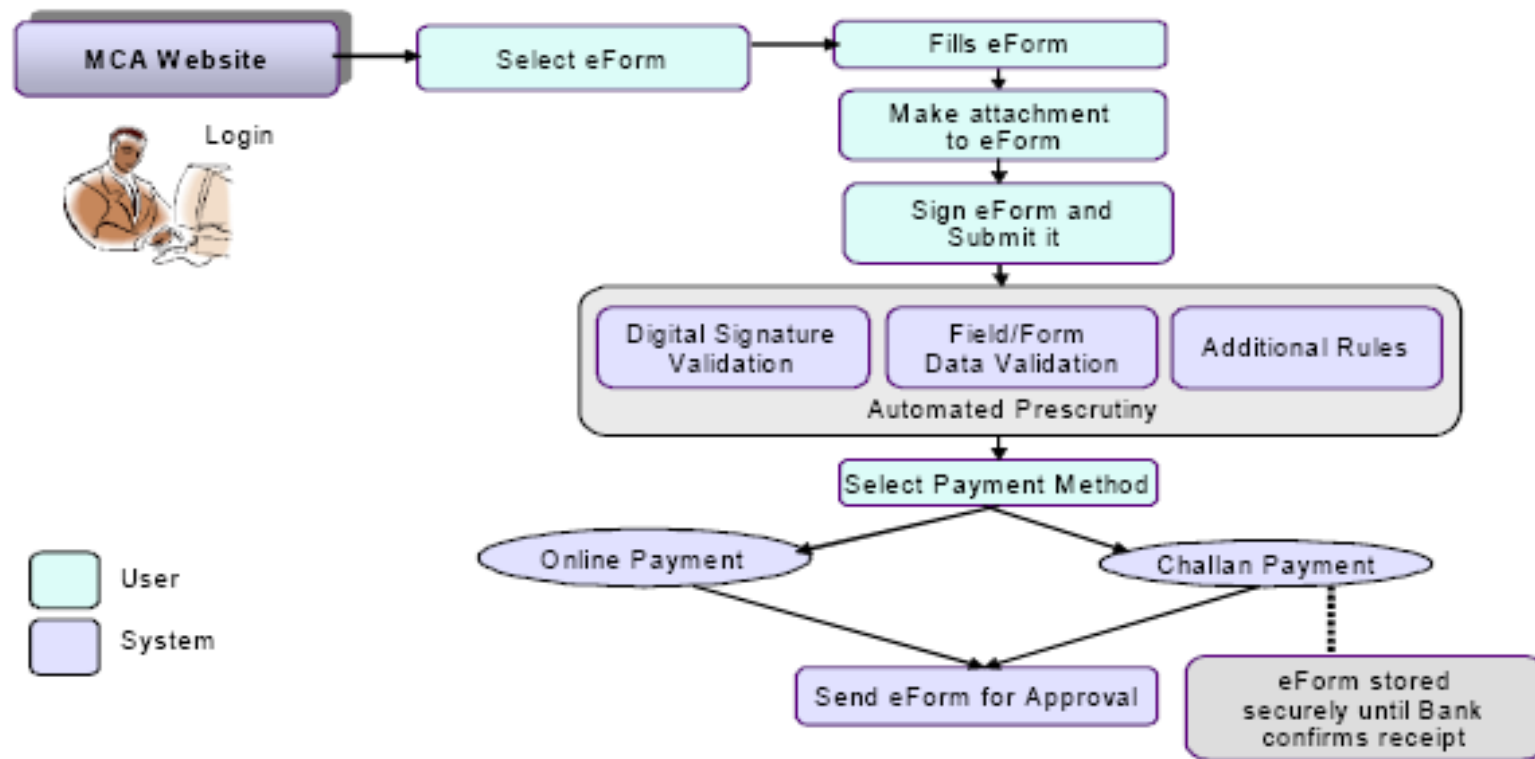
Back Office

- Automation of processing at RoC offices
- Centralised Repository of Company Information

- MCA21 portal as the single window for filing of information online
- Facilitation centres set up at select location to ease transition from manual to e-filing
- Processing of filings and Internal functions of MCA computerized
- Old records at each RoC digitized and made available online

Snapshot of MCA21 implementation (2/3)

Filing eForm



Each transaction uniquely identified by a Service Request Number (SRN)

Snapshot of MCA21 implementation (3/3)

- E-filing made mandatory, with Digital Signature Certificates
- All payments to be made through e-Payments (Online banking / credit cards / payment at designated bank branches)
- E-Stamping mandated wherever stamp duty is to be paid
- Unique Company Identification Numbers (CIN) assigned to each registered company
- Directors of Companies to obtain Director Identification Number (DIN)
- Facilitation counters gradually being phased out in favour of filing at customer's premises

Legal Framework for the MCA21 project

- The processes of Company Registration and Compliance filing were based on the Companies Act, 1956 (and the Rules made there-under) and the Monopolies and Restrictive Trade Practices Act 1969
- The other relevant Acts included:
 - The Competition Act, 2002
 - The Chartered Accountants Act, 1949
 - The Costs and Works Accounts Act, 1959
 - The Company Secretaries Act, 1980
 - The Partnership Act, 1932
 - The Societies Registration Act, 1860
 - The Companies (Donation to National Fund) Act, 1951

Why do we need legal amendments?

- The following questions arise...

How do I make it legally mandatory to file company information online?

Does the electronic records have the same validity as the paper records

The Companies Act does not talk about CIN / DIN..

What if a company goes to court insisting on its right to file returns in paper form?

Providing Legal Framework for the MCA21 project

- Some of these legal questions are answered by IT Act:
 - Digital Signature signing and submission of e-forms
 - Equivalence of electronic and paper records...
- But the domain legislation needs to be amended to reflect the new processes and procedures..
- Laws to be amended to incorporate enabling provisions, leaving procedural issues to be handled in subordinate legislation
- Subordinate legislation to be amended, detailing the new process regime

Amendment to Companies Act, 1956

Amendments to mandate Director Identification Number:

- Amendments to sections 253 & 266 A to 266F to mandate every Director to obtain a DIN.
No Director to be re-appointed without obtaining a DIN

Insertion of provisions 610B to 610E to mandate electronic filing:

- 610B: Filing of inspections, documents, applications etc through e-forms, as prescribed in the Rules
 - ✓ RoC to maintain such documents in electronic form
- 610C: Powers to central government to modify Act in relation to electronic records (including manner and form of filing)
- 610D: Provision for providing value added services
- 610E: Provisions of IT Act to apply in items relating to electronic records

Specifics of e-Filing, Payments, Inspection etc incorporated in Companies General Rules and Forms, 1956

In Summary...

E-Governance initiative (GPR, IT enablement, enabling structures)

Amend Laws to bring in enabling provisions

Amend sub-ordinate legislation to incorporate specific changes

End of Session