**The Indian IT Act and National e-Governance Plan**

1. The Information Technology Act was notified by the Indian Parliament in
	1. August 2008
	2. **June 2000**
	3. April 2000
	4. January 2008
2. The IT Act is based on:
	1. The British Information Technology Act
	2. Gramm-Leach-Blily Act, 1999
	3. **UN Model Law on Electronic Commerce,** 1996
	4. The Sarbanes Oxley Act, 2002
3. The IT Act was passed to:
	1. Provide legal recognition e-Commerce related transactions
	2. Allow e-filing of documents with the Government
	3. Address the issue of cyber crime
	4. **All the above**
4. Major amendment of the IT Act, which introduced the controversial section 66A happened in:
	1. 2008
	2. 2010
	3. 2002
	4. **2014**
5. Which of the provisions of the IT Act was revoked by the Supreme Court of India in 2015
	1. Section 69
	2. Section 66
	3. Section 43
	4. **Section 66A**
6. The controversial section 66A of the IT Act deals with:
	1. Sending offensive, false or threatening information through an electronic device
	2. Child pornography
	3. Video piracy
	4. Refusal to decrypt data
7. State whether true or false: The IT Amendment Act 2008 replaced the words ‘digital signature’ in the original act of 2000 with the words ‘electronic signature’ in several places.
	1. **True**
	2. False
8. The applicability of the IT Act is:
	1. To the whole of India
	2. To the whole of India excepting specified states
	3. To whole of India as well as to offences thereunder committed by Indian citizens
	4. **To whole of India as well as to offences thereunder committed by any person**
9. According to Section 3 of the Act, an electronic record may be authenticated using:
	1. Manual signature
	2. Digital signature
	3. **Electronic signature**
	4. Digital biometric device
10. According to the above, two essential aspects of an authentication method are:
	1. Public key and private key
	2. Symmetric cryptosystem and PKI
	3. Symmetric cryptosystem and hash function
	4. **Asymmetric cryptosystem and hash function**
11. An algorithm mapping a sequence of bits into another, smaller bit in such a way that the electronic record yields the same result every time the algorithm is executed is called:
	1. Private key
	2. **Hash function**
	3. Public key
	4. Data encryption
12. State whether true or false: If any law required an information or matter to be in writing or in type written or printed form, then that requirement is not satisfied if the information is in electronic form, unless a print out is taken and signed by the appropriate authority.
	1. True
	2. **False**
13. State whether true or false: If any information or document is required by law to be authenticated by affixing the signature of any person, then such requirement is deemed to be satisfied if the said document is authenticated by an electronic signature.
	1. True
	2. False
14. Which section under the Act legalizes the e-filing of IT returns
	1. Section 3
	2. Section 4
	3. Section 5
	4. Section 6
15. Existing law provides that all returns and financial documents are to be retained for a certain number of years. If a clear electronic copy of the same is retained, does it satisfy the requirement of the law?
	1. Yes
	2. No
	3. Yes, only if the information is accessible and can be used for subsequent reference and is retained in a format in which it was originally created or received
16. Which section of the Act provides for audit of electronic documents
	1. Section 6
	2. Section 6A
	3. Section 7
	4. **Section** 7A
17. The authority created vide Chapter VI, Section 17 of the Act for exercising supervision over the activities of Certifying Authorities is:
	1. Root Certifying Authority of India
	2. **Controller of Certifying Authorities**
	3. National Informatics Centre
	4. Centre for Development of Advanced Computing
18. Who certifies the public keys of subscribers of digital signatures
	1. **The Certifying Authorities**
	2. The Controller of Certifying Authorities
	3. The Root Certifying Authority of India
	4. The Ministry of Information Technology
19. Who certifies the public keys of the certifying Authorities?
	1. The Certifying Authorities
	2. **The Controller of Certifying Authorities**
	3. The Root Certifying Authority of India
	4. The Ministry of Information Technology
20. State whether true or false: Foreign Certifying Authorities are not recognized in India
	1. True
	2. **False**
21. The license issued to a Certifying Authority by the Controller is transferable
	1. True
	2. **False**
22. Upon death of a subscriber, his digital signature certificate
	1. Passes on to the legal heir
	2. **Should be revoked**
	3. No action need to be taken
	4. None of the above
23. Any person, aggrieved by an order of the controller, may approach
	1. The High Court
	2. **The Cyber Appellate Tribunal**
	3. The Supreme Court
	4. The order of the controller is final
24. The Cyber Appellate Tribunal is bound by
	1. The code of civil procedure, 1908
	2. **Principles of natural justice**
	3. All of the above
	4. None of the above
25. Which section of the Act prescribes legal recourse against cyber terrorism
	1. Section 62
	2. Section 66 E
	3. **Section 66 F**
	4. Section 67 A
26. The National e-Governance Plan of the Government of India was launched in
	1. January 2010
	2. May 2000
	3. April 2009
	4. **May 2006**
27. Under NeGP, specific activity focusing on one aspect of e-Governance, such as banking, land records etc., is called a
	1. **Mission Mode Project**
	2. Central Project
	3. e-Governance Project
	4. CBS
28. Which of the following is an example of a Central MMP?
	1. **Passport**
	2. eDistrict
	3. PDS
	4. e-Courts
29. Which of the following is an example of a State MMP?
	1. Banking
	2. Insurance
	3. e-procurement
	4. **Road Transport**
30. Which of the following is an example of an Integrated MMP?
	1. Banking
	2. Insurance
	3. e-**procurement**
	4. Road Transport
31. How many additional MMPs can a State define to meet its specific needs
	1. One
	2. **Five**
	3. Ten
	4. None
32. Core connectivity infrastructure under NeGP involving network connectivity from Head Quarters upto block level is called:
	1. Virtual Private Network
	2. State Wide Area Network
	3. National Knowledge Network
	4. State Data Centre
33. NeGP Infrastructure element for providing functionalities like disaster recovery, central repository, secure data storage etc., is called
	1. State Wide Area Network
	2. Common Service Centre
	3. State Data Centre
	4. **State Repository**
34. The NeGP initiative for provision of web enabled e-Governance services in rural areas is called
	1. **Common Service Centre**
	2. Service Delivery Gateway
	3. eTaal
	4. Open Data
35. NeGP initiative in the area of public procurement is called
	1. Common Service Centres
	2. E-tendering gateway
	3. Government e-Marketplace (GeM)
	4. **E-procurement gateway**
36. Meghraj is an NeGP initiative in the area of
	1. **Cloud computing**
	2. Email
	3. Internet
	4. Astronomy
37. The National Informatics Centre (NIC) developed software for computerization of State Transport Departments under State MMP are:
	1. **Vahan and Sarathi**
	2. e-Registration and e-licensing
	3. e-payment of Motor Vehicle Taxes
	4. Sugam and e-pass
38. The software for vehicle registration, fitness, taxes, permits and enforcement activities of the Transport Departments developed under NeGP is called
	1. Sarathi
	2. **Vahan**
	3. e-Permit
	4. e-Registration
39. The software for issue of various kinds of licenses like Learners License, Driving License, Conductor License etc., in the Transport Departments developed under NeGP is called
	1. Sarathi
	2. Vahan
	3. e-Permit
	4. e-Registration
40. The NeGP project aimed at enabling seamless service delivery to citizens at district level is called
	1. E-panchayat
	2. E-sugam
	3. E-tehsil
	4. **E-district**
41. The front end of the e-district project is conceptualized as:
	1. Kiosks
	2. Citizen Facilitation Centers
	3. Gram panchayats
	4. Citizen Support Centers
42. The e-District project is envisioned to facilitate online filing of applications and receipt of information relating to the Right to Information Act.
	1. **True**
	2. False

Answers

1. b. The IT Act was signed by the President Shri. K. R. Narayanan on 9 June 2000
2. c. The IT Act is based on the United Nations Model Law on Electronic Commerce 1996  adopted by the General Assembly of United Nations by a resolution dated 30 January 1997. The model law was adopted by the UN Commission on International Trade Law (UNCITRAL). The UN General Assembly in its resolution adopting the model law had recommended that all states give due consideration to the same while enacting their own cyber laws so as to have uniformity of law concerning adoption of alternate means of recording and storing documents
3. d
4. a.
5. d. The Supreme Court of India revoked section 66A of the IT Act as unconstitutional in entirety as it violated the freedom of speech guaranteed under Article 19(1)(a) of the constitution of India
6. a. Section 66A:any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.
7. a. True. An electronic signature is any electronic means of attestation including scanned image of a hand signature, biometric attestation, video or voice signature or simply a mouse click on the ‘I Agree’ tab. A Digital Signature is a kind of electronic signature which is executed through the means of asymmetric key encryption and third party attestation of the identity of the signer. Through digital signatures it is also possible to ensure the qualities of confidentiality, integrity and non-repudiation as shown below:



1. d
2. b
3. d

Chapter II of the Act deals with digital signatures. The Act empowers the use of digital signatures (Section 3) to authenticate electronic documents. The section goes on to specify that a method of such authentication should involve the use of:

1. asymmetric cryptosystems
2. hash function.

This requires some understanding of cryptography. Cryptography is the science of effecting secret communication by encrypting a message using a key. When A sends a secret message to B, the message is encrypted using a secret key and the encrypted message is send to B. The key used for encryption is also separately communicated to B. Now B can use the key and ‘decrypt’ the encrypted message. Here the message is encrypted and decrypted using the same ‘key’. This kind of encryption is symmetric.

There are some disadvantages with this system, the most important of which is that the key also has to be securely communicated. Moreover, any cryptosystem is expected to provide features like integrity and non-repudiation also, in addition to confidentiality. A symmetric cryptosystem cannot guarantee these.

A solution to this problem is to adopt an asymmetric crypto system. In this, each person has two complementary keys called public key and private key forming a key pair. A message encrypted using one can be decrypted using the other only. That is, if a message is encrypted using A’s public key, it can be decrypted using A’s private key only and vice versa.

The public key of the pair is ‘public’ as the name suggests, in that it can be shared with anyone. The private key, on the other hand, should not be shared at all.

Now, if A wants to secretly communicate with B, under asymmetric cryptosystem process, A can encrypt the message using B’s public key. Such a message can be read only by B, because it can be decrypted using B’s private key only. Hence the confidentiality of the message is ensured.

However, A can always claim that he did not sent the message, because B’s public key with which it was encrypted is available to anyone. In other words, the quality of ‘non-repudiation’ is not satisfied here. Further, there is no guarantee that the message that has been sent is the same one, without any changes at all, is the one that has been received (the quality of integrity).

To address this issue, it is necessary that A should digitally sign the document. This requires the use of another technology called hash function. A hash function is an algorithm that can irreversibly convert a message of any size to a ‘digest’ of a fixed size. The peculiarity of this algorithm is that the same message will yield exactly the same digest every time it is used, but even the minutest change in the message will result in an altogether different digest. It is also not possible to regenerate the message from the digest. Hence hashing is not encryption. The former is a one way process and the latter is two way.

To affix a digital signature, A has to first hash his message to obtain a digest. This digest has to be encrypted using A’s private key. Thus a digital signature is the hash of a message encrypted using the senders private key. Like manual signatures, a digital signature is unique to the sender (since it is encrypted using the senders private key), but in addition, it is also unique to the message, because the hash of the message is unique to that message. Once the digital signature is affixed the sender cannot repudiate the message, since none but himself has access to his private key.

The digital signature is affixed on the original message and send to B. B receives the message, decrypts the digital signature using A’s public key (since it was encrypted using A’s private key) to obtain the digest. Now he takes the original message and applies the hash function to make another digest. Both digests can be digitally compared, and, if there is a match, it means that the message has not been manipulated in between sending and receiving.

1. b
2. b. Section 4 of the Act: Legal Recognition of Electronic Records, states that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is— (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.
3. a. Section 5 of the Act: Legal recognition of electronic signatures:

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

1. d. Section 6 of the Act: Use of electronic records and digital signatures in Government and its agencies: Where any law provides for— (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner; (b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; (c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, 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.
2. c. Section 7 of the act for ‘Retention of electronic records’ states that “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— (a) the information contained therein remains accessible so as to be usable for a subsequent reference; (b) 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 information originally generated, sent or received; (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received”
3. d
4. b

Note:

**Certifying Authority:** A certifying authority is an entity which is licensed to issue digital signature certificates. To understand this one needs to know about what is known as the Public Key Infrastructure (PKI).

We have already learned that digital signatures are effected through the use of asymmetric key cryptography which involves a key pair – a public key and a corresponding private key. Hence when a subscriber is granted a digital signature, what he gets is essentially the key pair, and a certificate by a trusted entity attesting to the fact that this public key belongs to this person whose name is mentioned on the certificate. This certificate is called the Digital Signature Certificate. It links the public key to the identity of its owner.

Certifying authorities, as mentioned above, are agencies licensed to issue the key pair and the accompanying digital signature certificates. Hence, if you want to use digital signatures, you should apply to a certifying authority (like Verisign, (n)Code or CDAC)

The certifying authorities, in turn, are regulated by the Controller of Certifying Authorities, created as per the provisions of this Act.

1. a
2. b

**Note:**Section 18 of the Act outlines the functions of the Controller of Certifying Authorities as:

(a) exercising supervision over the activities of the Certifying Authorities; (b) certifying public keys of the Certifying Authorities; (c) laying down the standards to be maintained by the Certifying Authorities; (d) specifying the qualifications and experience which employees of the Certifying Authorities should possess; (e) specifying the conditions subject to which the Certifying Authorities shall conduct their business; (f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key; (g) specifying the form and content of a Digital Signature Certificate and the key, (h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities; (i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them; (j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems; (k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers; (l) resolving any conflict of interests between the Certifying Authorities and the subscribers; (m) laying down the duties of the Certifying Authorities; (n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

1. b

Note: As per section 19 of the Act, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

1. b. License for practicing as Certifying Authority is neither transferable, nor heritable. It is valid for a period mentioned in the license. (Section 21)
2. b

Note: Conditions of grant, maintenance and revocation of digital signature certificates is detailed in Chapter VII of the Act.

1. b

Note: Chapter 10 of the Act details the provisions for constitution and conduct of business of the Cyber Appellate Tribunal

1. b
2. c

Note: Please find below a summary of the various offences and prescribed penalties under the IT Act.

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Offence** | **Description** | **Penalty** |
| 65 | Tampering with computer [source documents](https://en.wikipedia.org/wiki/Source_code) | If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 66 | [Hacking](https://en.wikipedia.org/wiki/Computer_crime) with computer system | If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)500,000 |
| 66B | Receiving stolen computer or communication device | A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66C | [Using password of another person](https://en.wikipedia.org/wiki/Identity_theft) | A person fradulently uses the password, digital signature or other unique identification of another person. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66D | [Cheating using computer resource](https://en.wikipedia.org/wiki/Internet_fraud) | If a person cheats someone using a computer resource or communication. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 66E | Publishing [private images](https://en.wikipedia.org/wiki/Voyeurism) of others | If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 66F | Acts of [cyberterrorism](https://en.wikipedia.org/wiki/Cyberterrorism) | If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism. | Imprisonment up to life. |
| 67 | Publishing information which is [obscene](https://en.wikipedia.org/wiki/Pornography_in_India) in electronic form. | If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. | Imprisonment up to five years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 |
| 67A | Publishing images containing [sexual acts](https://en.wikipedia.org/wiki/Pornography_in_India) | If a person publishes or transmits images containing a sexual explicit act or conduct. | Imprisonment up to seven years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 |
| 67B | Publishing [child porn](https://en.wikipedia.org/wiki/Child_porn) or [predating children](https://en.wikipedia.org/wiki/Sexual_predator) online | If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18. | Imprisonment up to five years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)1,000,000 on second conviction. |
| 67C | Failure to maintain records | Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence. | Imprisonment up to three years, or/and with fine. |
| 68 | Failure/refusal to comply with orders | The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)200,000 |
| 69 | Failure/refusal to [decrypt data](https://en.wikipedia.org/wiki/Key_disclosure_law) | If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime. | Imprisonment up to seven years and possible fine. |
| 70 | Securing access or attempting to secure access to a protected system | The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence. | Imprisonment up to ten years, or/and with fine. |
| 71 | [Misrepresentation](https://en.wikipedia.org/wiki/Misrepresentation) | If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate. | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)100,000 |
| 72A | Breach of confidentiality | If anyone, while providing services under terms of lawful contract, has secured access to personal information of another person discloses, without his/her consent, to another | Imprisonment up to three years, or/and with fine up to [₹](https://en.wikipedia.org/wiki/Indian_rupee)500,000 |

Source: Wikipedia.org

1. d
2. a
3. a

Note: The NeGP comprises of 31 Mission Mode Projects. The term ‘mission mode’ implies that projects have clearly defined objectives, scopes, and implementation timelines and milestones, as well as measurable outcomes and service levels. The following are the list of MMPs classified under Central, State and Integrated

| **Central MMPs** | **State MMPs** | **Integrated MMPs** |
| --- | --- | --- |
| 1. [Banking](http://meity.gov.in/content/banking)
2. [Central Excise & Customs](http://meity.gov.in/content/central-excise-customs)
3. [Income Tax (IT)](http://meity.gov.in/content/income-tax-it)
4. [Insurance](http://meity.gov.in/content/insurance)
5. [MCA21](http://meity.gov.in/content/mca21)
6. [Passport](http://meity.gov.in/content/passport)
7. [Immigration, Visa and Foreigners Registration& Tracking](http://meity.gov.in/content/immigration-visa-and-foreigner%E2%80%99s-registration-tracking-ivfrt)
8. [Pension](http://meity.gov.in/content/pension)
9. [e-Office](http://meity.gov.in/content/e-office)
10. [Posts](http://meity.gov.in/content/posts)
11. [UID](http://meity.gov.in/content/uid)
 | 1. [Agriculture](http://meity.gov.in/content/agriculture)
2. [Commercial Taxes](http://meity.gov.in/content/commercial-taxes)
3. [e−District](http://meity.gov.in/content/e-district)
4. [Employment Exchange](http://meity.gov.in/content/employment-exchange)
5. [Land Records(NLRMP)](http://meity.gov.in/content/land-records)
6. [Municipalities](http://meity.gov.in/content/municipalities)
7. [e-Panchayats](http://meity.gov.in/content/panchayats)
8. [Police(CCTNS)](http://meity.gov.in/content/police)
9. [Road Transport](http://meity.gov.in/content/road-transport)
10. [Treasuries Computerization](http://meity.gov.in/content/treasuries)
11. [PDS](http://meity.gov.in/content/pds)
12. [Education](http://meity.gov.in/content/education)
13. [Health](http://meity.gov.in/content/health)
 | 1. [CSC](http://meity.gov.in/content/common-services-centers-0)
2. [e-Biz](http://meity.gov.in/content/e-biz)
3. [e-Courts](http://meity.gov.in/content/e-courts)
4. [e-Procurement](http://meity.gov.in/content/e-procurement)
5. [EDI For eTrade](http://meity.gov.in/content/electronic-data-interchange-edi-trade-etrade)
6. [National e-governance Service Delivery Gateway](http://meity.gov.in/content/nsdg)
7. [India Portal](http://meity.gov.in/content/india-portal)
 |

Source: <http://meity.gov.in/content/mission-mode-projects>

1. d
2. c
3. b
4. b
5. c
6. a
7. c
8. a
9. a

**Note on Vahan and Sarathi:**

The State Transport Department is governed by both Central Motor Vehicle Regulation (CMVR) and state specific Motor Vehicle Regulation (State MVR). Consequently, Sarathi and Vahan were conceptualized as a product that would capture the functionalities as mandated by CMVR as well as state MVRs. Vahan core modules are developed by NIC, Delhi team. Sarathi mainly deals with the issuance of various categories of licenses viz learning license, driving license, driving school license and conductor license. It also uses the devices to capture biometrics like photograph, thumb impression and signature of license holder. Data of holder needs to be captured only once and will be used for further transactions when needed. Sarathi is integrated with STALL- computer based learning license test where computer decides the result and allow to issue learning license. Gujarat was the first state to implement Sarathi with STALL in all the offices of RTO in Gujarat. Sarathi is also integrated with Key Management System. KMS verify and authenticate the data on each license issued through Sarathi after printing on the smart card chip. This enhances the security of data on the card issued through Sarathi. Sarathi core modules are developed by NIC, Hydrabad team. VAHAN is a highly flexible and comprehensive system that takes care of all the burdensome activities of Vehicle Registration, leaving the Transport Department to deal with more important business issues. The software enables the processes at RTO involving Vehicle Registration, Fitness, Taxes, Permits & Enforcement to capture various data related to license and vehicle holder. Vahan has facility to issued choice numbers to vehicle after collecting stipulated fees. Registration numbers to vehicles are allotted using random selection process using software generated program. Vahan is also integrated with KMS to issue smart card based RC if required. Online dealer’s registration system is also developed and implemented to reduce the registration time. Each registered dealer is given account on the system where he can enter registration related data which can be used in Vahan for registration process. Status: Vahan and Sarathi are implemented in all RTO offices in Gujarat

Source: www.nic.in

1. b
2. a
3. d
4. b
5. a