



ಕರ್ನಾಟಕ ರಾಜ್ಯಪತ್ರ

ಅಧಿಕೃತವಾಗಿ ಪ್ರಕಟಿಸಲಾದುದು

ವಿಶೇಷ ಪತ್ರಿಕೆ

ಭಾಗ - IV-A	ಬೆಂಗಳೂರು, ಕುಕ್ಕವಾರ, ಆಗಸ್ಟ್ ೦೭, ೨೦೦೭ (ಶ್ರಾವಣ ೦೯, ಶಕ ವರ್ಷ ೧೯೫೯)	ಪು. ೦೮೫೩
------------	---	----------

Personnel & Administrative Reforms Secretariat

NOTIFICATION

No. DPAR 13 EGM 2007, Bangalore dated 10th August 2007

In exercise of the powers conferred by section 90 read with section 6 of the Information Technology Act, 2000 (Central Act No.21 of 2000), the Government of Karnataka hereby, makes the following rules, namely:-

RULES

1. Title and commencement.- (1) These rules may be called the Karnataka Information Technology (Issue of Digital Extracts and Certificates for e-Governance Projects) Rules, 2007.

(2) They shall come into force from the date of their publication in the Official Gazette.

2. Definitions.- In these rules, unless the context otherwise requires,-

- "appropriate authority", in relation to any e-Governance Service means the Secretary to Government incharge of the departmental service allocated under the Karnataka Government (Allocation of Business) Rules, 1977;
- "competent authority", in relation to any e-Governance Service means the Secretary to Government, in-charge of e-Governance, or such other authority appointed by the State Government for this purpose by notification;
- "departmental digital certificate controller" means an officer designated by the appropriate authority for managing the issue maintenance and archival of issued digital certificates issued for the purpose of delivery of e-Governance services at the departmental level;
- "departmental digital systems controller" means an officer designated as such by the appropriate authority, for the purpose of ensuring the security of the computer systems used including the software and peripheral devices used for the delivery of e-Governance services;
- "departmental documents security controller" means an officer so designated by the appropriate authority to ensure the security of documents and data in electronic form related to the department's e-Governance services;

- (f) "departmental e-Governance delivery agent" means a person so appointed for the purpose of delivery of any e-Governance Service at the departmental e-Governance delivery centres;
- (g) "departmental e-Governance delivery centre" means those e-Governance service centres which are established and operated, maintained by a department and where e-Governance services are delivered by e-Governance delivery agent;
- (h) "deputy commissioner" shall have the same meaning as given in section 8 of the Karnataka Land Revenue Act, 1964 (Karnataka Act 12 of 1964);
- (i) "Director, EDCS" means Director, Electronic Delivery of Citizen Services;
- (j) "e-Governance delivery agent" means a person so appointed under these rules for the purpose of setting up of a e-Governance delivery centre and delivery of any e-Governance Service from such Center;
- (k) "e-Governance delivery centres" means e-Governance centres other than departmental e-Governance delivery centre which are established and maintained by e-Governance delivery agents or e-Governance delivery organisations with the approval of the competent authority under these rules to deliver e-Governance services;
- (l) "e-Governance delivery organization" means any organization which are permitted under these rules for setting up and maintaining e-Governance delivery centres;
- (m) "e-Governance digital certificate controller" means an officer so designated by the competent authority for the purpose of specifying the procedures of e-Governance service by departmental digital certificate controllers for the purpose of delivery of e-Governance services and to audit and certify the implementation of the prescribed procedures;
- (n) "e-Governance digital systems controller" means an officer so designated by the competent authority for the purpose of specifying the procedures for maintenance of the security of the computer systems including the software and peripheral devices used for the purpose and to audit and certify the implementation by departmental digital system controller used for the delivery of e-Governance services;
- (o) "e-Governance documents security controller" means an officer so designated by the competent authority to specify the procedures to be followed by department documents security controller for the security of the electronic documents and data related to e-Governance Services and to audit and certify the implementation of the specified procedures;
- (p) "e-Governance service" means services pertaining to matters specified in Schedule I and such of those matters notified by the competent authority by notification and includes services like receiving applications, petitions and other similar representations, collecting specified charges and issuing acknowledgments thereof, delivery of print-outs of any digital extracts, certificates, documents or permissions maintained in electronic form, or of any other electronic communications received from the principal office or any office or functionary; and services delivered to various Government departments using the IT infrastructure through the e-Governance delivery centres or departmental e-Governance delivery centres;
- (q) "Karnataka document integrity protection system" means the system of secured storage of electronic records, and issuance of the same in the form of documents to citizens as per rule 13;
- (r) "Principal Office" with respect to a service means the office of that department of the State Government which is accountable under law for the time being for delivery of the service through e-Governance project;
- (s) "specified charge" means any duly authorised tax, charge, due or any other money payable by any person interested in remitting the same to appropriate principal office through the e-Governance delivery agent who is authorised to collect under these rules or under general or special orders of the State Government or the competent authority and includes service charges;

- (t) "specified computer resource" means the computer resource including both the hardware and software as specified, whether generally or specifically, by the State Government or the competent authority and for different purposes different computer resources may be specified;
- (u) "specified manner" means the manner specified, whether generally or specifically, by the State Government or the competent authority, and any functionality, instruction, procedure, etc., built into or indicated by the specified computer resource;
- (v) "Schedule" means schedule appended to these rules;
- (w) "service charge" means amount payable to authorized e-Governance delivery agent or departmental e-Governance delivery agent in lieu of services provided thereof in accordance with the directions of the State Government or the competent authority as the case may be;
- (x) "Verification official" means a Government official appointed by the appropriate authority to certify the genuineness of the certificates issued from the e-Governance delivery centres or departmental e-Governance delivery centre by putting his ink signature with seal.

3. Powers and functions of the appropriate authority.- The appropriate authority shall,-

(a) appoint the departmental documents security controllers, departmental digital certificate controllers, and departmental digital systems controllers and departmental e-Governance delivery agents and supervise their functioning;

(b) supervise the departmental e-Governance centers and conduct periodical audit of their activities;

(c) may appoint a Verification official in various subordinate offices.

4. Powers and functions of the competent authority.- The competent authority,-

(a) may appoint the e-Governance documents security controllers, e-Governance digital certificate controllers and e-Governance digital systems controllers and supervise their functioning;

(b) may notify e-Governance service in accordance with rule 9;

(c) may specify the manner of proper and secure custody, and of maintenance, safety and operation of specified computer resources;

(d) may notify the principal offices on whose behalf the e-Governance delivery agent or departmental e-Governance delivery agent shall be authorised to provide notified e-Governance services;

(e) may notify such e-Governance delivery centres;

(f) may appoint e-Governance delivery organization;

(g) may specify terms and conditions under which e-Governance delivery organisations or agents are appointed like the form of an agreement which the e-Governance delivery agent or e-Governance delivery organization shall execute providing for the hours of functioning, location and other relevant details relating to e-Governance delivery centre, as well as for indemnifying the State Government and the principal offices for any loss or damage arising out of negligence, default or breach of conditions thereto and the agreement shall also ensure sufficient security for any money received by such agent on behalf of the principal office through sureties, insurances, bank guarantees or in any other manner;

(h) may by notification specify the minimum infrastructure required for the e-Governance delivery organisation or departmental e-Governance delivery centre in order to enable it to provide e-Governance services;

(i) may specify the procedure for functioning of the e-Governance delivery agent or departmental e-Governance delivery agent and e-Governance delivery organisation;

(j) may issue, from time to time, directions regarding any matter that it may consider necessary or expedient for effective and efficient provision of any notified e-Governance service or for the effective functioning of the e-Governance delivery centre or departmental e-Governance delivery centres.

5. Powers and functions of Director, EDCS.- The powers and functions of the director, EDCS shall be the following, namely:-

(a) to enter into agreement with the e-Governance delivery organization, as appointed by competent authority, for discharging of responsibility of both parties for delivery of e-Governance services;

(b) to review the working of e-Governance delivery organizations and agents;

(c) to enforce service level agreement (SLAs) and make payment to e-Governance delivery organizations, and e -Governance delivery agents after deducting penalty if any, towards its share of service charges as per agreement;

(d) any other task or functions notified by the competent authority.

6. Permission to e-Governance Delivery Organisation.- (1) The competent authority shall evaluate the responses of any firm or a person who applied in response to notification under rule 4 and shall select such firms or persons through a transparent process in accordance with Karnataka Transparency in public procurement Act or any law fro the time being in force.

(2) The e-Governance delivery organization shall appoint such number of e-Governance delivery operators permitted by the competent authority to work in such places subject to such conditions as may be specified in these rules and by the competent authority.

7. Appointment, termination and eligibility criteria etc., of e-Governance delivery agents and operators.- (1) The Deputy Commissioners shall appoint e-Governance delivery agents in respect of those centres which are so notified by the competent authority after giving wide publicity in more than one widely circulated news paper of which one shall be in Kannada. Equal opportunity shall be given to all who are eligible for appointment as agent. An appointment of departmental e-Governance delivery agent shall be for a period of two years on completion of which it shall be subject to renewal. All appointments shall require approval from the competent authority.

(2) The Deputy Commissioners may terminate the agency of e-Governance delivery agent after issuing a show cause notice in case his performance is not found to be satisfactory or if he is found violating conditions stipulated in the agreement of agency.

(3) The competent authority shall be at liberty to relax the eligibility criteria for appointment of agents and operators to persons belonging to disadvantaged sections of the society like women, schedule caste/schedule tribes and the physically challenged.

(4) The competent authority may issue suitable guidelines and circulars from time to time to clarify any issues relating to eligibility and to further refine or enhance the eligibility criteria.

8. Functions of the e-Governance delivery agent and operators.- (1) The e-Governance delivery agent and operators appointed by E-Governance Delivery Organisations shall perform the following functions, namely:-

- (i) he shall receive requests for all the e-Governance services offered like BHOOMI, NEMMADI and any other e-Governance projects by collecting the service charge as specified by Government;
- (ii) he shall submit the applications generated through software and all other related documents attached to the application to concerned principal office for processing the request;
- (iii) he shall allow field level executives of different departments to use the hardware and other related peripherals at his tele centre to approve transaction or upload physical verification reports;
- (iv) he shall ensure that requests submitted by them on first come first serve basis and getting processed with the required speed so that; service can be delivered in specified time. He has to check status of the requests regularly and should take-up matters with senior officials if there is inordinate delay;

- (v) he shall ensure that, certificates/orders to be issued to citizens are collected in time from taluka/district offices and delivered to citizens concerned.

(2) Since these tele centres would act as virtual offices of the government in villages e-Governance delivery agent and operators shall ensure the credibility of the Government is maintained.

9. e-Governance service to be notified.- (1) In addition to the services mentioned in Schedule I the competent authority may by notification in the official Gazette add or omit any entry in Schedule I.

(2) Any addition in relation to a matters of e-Governance service shall be made only when the matters of service fulfills the requirements laid down in Schedule II.

10. Eligibility for appointment as e-Governance delivery agent and operator.- No person shall be eligible for appointment as an e-Governance delivery agent of an e-Governance delivery centre or operators in an e-Governance delivery organisation unless he fulfills the conditions specified in Schedule III.

11. Departmental support system.- The appropriate authority shall ensure that such measures as are essential and are required within the department to discharge the functions of the documents security controller, digital systems controller and digital certificate controller at the departmental level are introduced.

12. Equivalence of delivery centres.- Departmental e-Governance delivery centers are deemed to be e-Governance delivery centers as far as the delivery of e-Governance service is concerned.

13. Specified Computer resources at delivery centers.- (1) The specified computer resources used at a departmental e-Governance delivery centre and at the e-Governance delivery centres for storing electronic records and issuing documents for notified e-Governance services shall be either those provided by the State Government or if not provided by the State Government, may be audited by the State Government before or after those are used for the delivery of e-Governance services.

(2) The provision of auditing of the specified computer resources by the State Government shall be applicable for both the hardware and software.

(3) The specified computer resource shall be used in the specified manner and the same may be audited by the State Government.

14. Karnataka Document Integrity Protection System.- (1) The documents issued at the departmental service delivery centres and e-Governance delivery centers shall be secured as per procedure outlined in Schedule IV which shall be referred to as the Karnataka Documents Integrity Protection System (KDIPS).

(2) The software used for creating, modifying and storing electronic records that are used to issue documents at e-Governance service and department e-Governance service delivery centres shall implement the procedure as specified by the KDIPS.

(3) The appropriate authority shall specify for each service an authority to certify that electronic records are maintained and secured as per KDIPS.

(4) The documents issued at the departmental e-Governance service delivery centers and at the e-Governance service delivery centers for notified e-Governance services as per KDIPS shall also be physically signed (handwritten signature) by the authorized departmental e-Governance service delivery agent and the e-Governance service delivery agent or the operators respectively to confirm that the system and its working complies with clause (b) of section 65 of the Indian Evidence Act, 1872 (1 of 1872).

(5) The competent authority may amend the procedures provided under KDIPS through a notification published in the Official Gazette.

15. Charges.- (1) Specified charges to be paid by a person to avail any e-Governance service shall be notified by appropriate authority from time to time.

(2) Service charges to be paid to e-Governance delivery agent or e-Governance delivery organization as the case may be for various notified e-Governance Services shall be specified by the competent authority from time to time.

(3) No e-Governance delivery agent shall collect an amount exceeding the specified charges. Any e-Governance delivery agent who collect an amount exceeding the specified charges shall be liable for cancellation of his agency and shall be liable to forego any deposit made in Government at the time of getting agency.

16. Presumption with regard to specified charges paid to e-Governance delivery agent.- In case of any specified charges, including service charge, paid by any person to an e-Governance delivery agent or to department e-Governance delivery agent in respect of any e-Governance service, the print-out of the electronic acknowledgment generated by the specified computer resource, signed and provided to such person by the Agent shall, prima facie, be proof of such payment and it shall be presumed that the dues or claims, for which the acknowledgment is purportedly issued, have been satisfied to that extent:

Provided that mere payment by itself shall not create any right, title, condonation of delay, extension in the period limitation or relaxation in favour of such person for which he is not otherwise entitled.

17. Resolution of disputes.- (1) Disputes if any between the Director, EDCS and the e-Governance delivery organisation or between Deputy Commissioner and e-Governance delivery agent shall be settled by the Director, EDCS or Deputy Commissioner as the case may be, on the basis of the terms set out in the agreement entered into between the Deputy Commissioner and the e-Governance delivery agent or between Director, EDCS and e-Governance delivery organisation.

(2) The e-Governance delivery agent or e-Governance delivery organization may appeal to competent authority or to any other authority as notified by competent authority for the purpose if it feels that the decision of Deputy Commissioner or Director, EDCS is not as per the agreement.

18. The Director, EDCS for e-Governance delivery organization and Deputy Commissioner for e-Governance delivery agent may designate officers for receiving complaints against the e-Governance delivery organization or e-Governance delivery agents or for providing clarifications to citizens regarding any matter related to functions of e-Governance delivery centres. The contact details of such officers shall be displayed in every e-Governance delivery centre or department e-Governance delivery centre.

19. Appeals against decisions.- Any person aggrieved by any decision of an e-Governance delivery agent or e-Governance delivery organization may file an appeal before the Deputy Commissioner and Director, EDCS respectively within thirty days of the date of the receipt of such decision.

20. Rules not in derogation of any other law.- The provisions of these rules shall be in addition to and not in derogation of the provisions of any other law for the time being in force.

Schedule II
(see rule 9 (b))

Requirements for notification of a service as e-Governance service provided through e-Governance delivery centers:

- (1) When a service is to be notified as e-Governance service delivered through e-governance delivery center, the following requirements need to be satisfied, namely:-
 - (a) The documents issued by the service shall be integrity protected by KDIPS or by an equivalent alternate mechanism;
 - (b) In case the mechanism is not projected by KDIPS, the alternate mechanism needs to be audited and approved by an auditor appointed by the competent authority
- (2) The computers and other electronic systems used in service delivery shall be subject to audit and approval by the e-Governance digital systems controller, e-Governance document security controller and the e-Governance digital certificate controller.

Schedule III
(see rule 9)

Eligibility qualification for e-Governance delivery agents and operators

1. The following is the eligibility required for appointment of an e-Governance delivery agent:
 1. Every prospective E-Governance Delivery Agent shall have the minimum computer hardware, peripherals and internet connectivity as specified by the competent authority from time to time.
 2. The agent shall be a Computer literate must have passed 12th Standard examination. He must be acquainted with basic skills required to operate a PC. He must have the knowledge of switching on/off a computer, managing files and folders, common office documents like spreadsheets, applications forms and knowledge of taking computer printouts. The agent shall manage the computer which would imply creating, data entry, modifying, saving, moving, closing and deleting of application forms, files and folders.
 3. The agent must know how to read, write and speak in Kannada.
 4. The agent must have a minimum typing speed of 25 wpm in both Kannada and English.
 5. The competent authority shall conduct a competitive test, written or online, for selection of E-Governance Delivery Agents.
 6. Before appointment the agent shall have to undergo a formal training on the E-Governance applications as determined by the competent authority.
 7. The agent shall qualify an online test administered by the competent authority to assess basic computer skills and knowledge of the E-Governance applications.
 8. The competent authority shall be at liberty to relax the eligibility criteria for agents from disadvantaged sections of the society like Women, SC/STs and the Physically Challenged.
 9. The Government shall have powers under the scheme to issue suitable guidelines and circulars from time to time to clarify any issues and to further refine or enhance the eligibility criteria.
 10. The Competent Authority shall provide adequate reservation for SC/ST and OBC and other classes in accordance with DPAR guidelines for reservation for appointment in appointment of e-Governance delivery agents.
 11. Shall remit such amount as deposit in Government as may be specified by the competent authority which will be forfeited on violating of conditions of permit.

2. The following is the eligibility required for appointment of an operator by the e-Governance Delivery Organisation:
1. The operator must be a holder of a Diploma in computer Application and should have an educational qualification of a minimum of 12th Standard.
 2. The operator should know how to read, write and speak in Kannada.
 3. The operator should have a minimum typing speed of 25 wpm in both Kannada and English.
 4. The competent authority shall conduct test, written or online, for selection of operator.
 5. Before appointment the agent shall have to undergo a formal training on the E-Governance applications as determined by the competent authority.
 6. The agent shall qualify an online test administered by the competent authority to assess basic computer skills and knowledge of the E-Governance applications.
 7. The e-Governance Delivery Organisation shall also provide reservations for SC/ST and Other Backward Classes to the adequate extent in accordance with the DPAR guidelines for appointments.
 8. Shall remit such as deposit in Government, as may be specified by the competent authority which will be forfeited on violating of any of the conditions of agency.

Schedule IV
(see rule 13(a))

Karnataka Digital Documents Authentication System (KDIPS)

Subject to the application specific parameterization specific to certain applications, the technical details involved in the document integrity protection mechanism envisaged under Rule 11 of the notification common to all applications that use the integrity protection mechanism are as follows:

1. Pre-requisites that shall be satisfied

a. Published Document structure and field mapping:

- i. **Electronic Document Structure:** As a pre-requisite to the signing process, for each type of document to be digitally signed, the structure of the electronic form of the document to be signed will be specified. This electronic document structure shall be expressed in XML schema definition (XSD) language and will provide the complete details of the field names, their data types, constraints on values and the arrangement and grouping of fields. The actual electronic document to be signed shall be represented as an XML document.
- ii. **Canonicalization Steps:** Additional steps to be followed to remove ambiguities in representing the electronic document in accordance with the XSD shall be specified for each document type.
 1. These shall include
 - a. The character encoding scheme (ASCII/UNICODE)
 - b. The inclusion/removal of white-space characters (TAB, SPACE, CARRIAGE RETURN) that separate structuring elements, character casing convention (UPPER/LOWER case) and other document specific rules to be followed in arriving at an electronic document prior to the application of a digital signature

- b. Mapping scheme from electronic to printed form:** In addition to publishing of the electronic document structure, an unambiguous mapping scheme shall be published

that specifies the means of exactly and completely mapping the fields in the electronic representation form with the fields printed in the printed document.

- c. **Unique Representation:** The document structuring scheme, additional common/document-specific steps to be followed and the electronic to printed form mapping shall ensure that the document is "unique" in the sense that:
 - i. For a printed document there shall be one and only one electronic document that corresponds exactly.
 - 1. The translation of electronic to/from printed document shall therefore be unambiguous
- d. The above structure, canonicalization steps and mapping scheme shall be available for open inspection any-time on-demand through a web-site whose address shall be specified.
- e. Two software applications shall be created and published that can
 - i. Accept an (electronic) XML document and generate the printed form of the document and display the same on a computer display
 - ii. Allow for and accept the re-entry of printed data and regenerate the (electronic) XML document from the re-entered data.

2. Digital Signing Process:

- I. **Representation:** The electronic document shall be represented as an XML document structured according to the published document structure described and canonicalization steps described previously
- II. **Digital Signature Generation:**
 - i. **Signer:** This document shall be digitally signed by an Authorized Document Signer using the private signature key of this authorized official.
 - ii. **Application Specific Parameterizations:** The details below are application specific and shall be specified in the application parameterization sections for each application
 - 1. The designation of the authorized document signer
 - a. The place where the signer's his/her private key is to be stored
 - b. Whether a document is a single unit or a composite of parts each of which requires a separate digital signature possibly by separate authorized document signers.
- III. **Certificates for signing:** The certificate issued to the authorized signer shall be retrieved from the certificate store for signing the documents
- IV. **Detached Digital Signature:** The digital signing will involve the creation of a detached digitally signed data as specified in PKCS7. In a simplified sense, the digital signature will involve the encryption of the hash of the electronic data with the (asymmetric) private key of the signer that corresponds with the public key in the signer's certificate. The signed data will be a "detached" digitally signed data in the sense that the signed data will contain only the digital signature and not the electronic data. In addition, no digital certificates shall be included as part of the digitally signed data. However, several further technical details are involved in the creation of the detached digitally signed data. For exact details on the creation and formatting of digitally signed data, refer PKCS7.

1. Algorithms: The algorithms/standards used in the digital signing process shall be as follows:

1. **Hashing Algorithm:** SHA1
2. **Signing Algorithm:** RSA
3. **Signed Data Formatting:** PKCS7
4. **Certificate Format:** X509

3. Storage Process:

- I. The electronic detached digital signature shall be stored in the application database for retrieval and printing.
- II. When a document needs to be printed, the application software shall ensure that only the stored electronic signatures are printed onto documents according to the printing process described below.
- III. The electronic documents and the electronic detached digital signatures shall be stored at a Secure Data Store.

1. Application specific parameterization: The choice of the secure data store shall be an application specific decision that shall be provided in the application specific parameterization section for each application.

4. Printing Process

- I. **Base 64 Encoding:** The electronic detached digital signature shall be Base64 encoded
- II. **2D Barcode Printing:** The Base64 encoded detached digital signature shall be converted to an electronic 2D barcode according to a specified **PDF417** 2D barcode algorithm.
- III. The electronic document shall be printed on physical paper following the mapping scheme described in the pre-requisites section.
- IV. The electronic 2D barcode shall be printed on the same physical paper

5. Document Change Management Process

- I. Whenever a document is changed, the digital signature (for the whole document or for the changed part in the case of a composite document) shall be generated afresh by the authorized official/s by resigning the document (or changed parts)

1. Application specific parameterization: The change management process for each application shall be described in the application specific parameterization section for each application which shall provide the details regarding the document resigning.

6. Document Signature Verification Process

The technical details involved in verifying a given document with a bar-coded digital signature are below:

a. 2D Bar Code decoding: The printed barcode on the document shall be decoded using a 2D barcode scanner to obtain the encoded detached digital signature. The algorithm used to decode the barcode into electronic data shall be specified.

- I. If the barcode reading fails, the document verification shall be deemed to have failed for the document in question

b. Base64 Decoding: The electronic data obtained above shall be Base64 decoded to recover the electronic form of the detached digitally signed data, whose format shall be verified to be a PKCS7 signed data with a detached signature and no certificates included.

- I. If the barcode decoded data cannot be successfully base 64 decoded, the document verification shall be deemed to have failed for the document in question.
- c. **Certificate Retrieval:** Using the certificate retrieval information in the PKCS7 signed data, the digital certificate used to sign the data (and the remainder of the digital certificate chain needed for completing the signature verification including the root certificate) shall be searched for in the certificate store.
- I. If any of the certificates in the certificate chain cannot be found or are found but are invalid (expired/revoked), the document verification shall be deemed to have failed for the document in question.
 - II. It shall be the responsibility of the verification system to ensure that the root certificate is not substituted in the certificate store.
- d. **Obtain the electronic document:**
- I. **Option 1 (Recreate the electronic data from printed data):**
 - I. The published XSD which defined the formatting and the mapping mechanism for mapping the printed document fields to the XSD shall be firstly obtained.
 - II. The characters from the printed document may be reentered into an electronic system. The characters shall be represented in the XML format conformant with the XSD exactly in accordance with the mapping scheme provided treating all mapping rules as significant to produce a 'regenerated' electronic data.
 - III. Alternatively, for ease of verification, the published software application that accepts the re-entry of data and regenerates the XML identically may be used to recreate the regenerated electronic data.
 - II. **Option 2 (Retrieve the electronic data from SDS):**
 - I. The electronic data may be retrieved from the 'Secure Data Store' using a secure retrieval mechanism. The 'retrieved' electronic data can then be used in place of the 'regenerated' electronic data in the verification process.
 - III. If electronic data cannot be successfully retrieved or regenerated, the document verification shall be deemed to have failed for the document in question.
- e. **Digital Signature Verification:** The electronic data retrieved or regenerated shall be verified against retrieved/regenerated electronic data using the standard process for verifying PKCS7 signed data. The core part of this verification process would involve obtaining the hash of the electronic data from the electronic detached digital signature and comparing it with the freshly computed hash of the obtained electronic data for an exact match.
- I. If the match is exact, the digital signature is deemed to have been verified. For complete technical details in signature deformatting and verification refer to PKCS7.
- f. **Physical content verification:** After the signature has been verified, the obtained electronic data shall be visually verified against the printed data and checked for an exact match.

7. Application Specific Parameterizations

1. Bhoomi RTC:

a. Digital Signing Process:

- i. **Authorized Signer:** The authorized document signers shall be the Village Accountant (VA) and the Revenue Inspector (RI). The document/document parts signed by the above signers shall be notified.
- ii. **Private Key Storage:** The private key of the authorised signer shall be stored in a smart card issued to the VA. The private key of the authorized signer shall be stored in a smart card issued to the RI.
- iii. **Document Parts:** The RTC is a composite document. The document parts that shall require independent (individual) signatures shall be the crop data and the ownership data.
 1. The crop data shall always be signed by the VA
 2. Whenever ownership change takes place, the RI shall sign the mutation order and the VA shall sign the updated RTC.
 3. Both the digital signatures of the crop data mutation data shall be generated and printed in accordance with the signature generation and printing process described previously.
- iv. **Secure Data Store:** For Bhoomi RTC there shall be 2 secure data stores which can be used for document verification (for the option of a retrieving the electronic document during document verification)
 1. The primary store shall be the Taluk database at each Taluk
 2. The secondary store shall be the State Data Center (SDC).

2. RDS Certificates:

a. Digital Signing Process:

- i. **Authorized Signer:** A notification shall be published for RDS which lists all the certificates issued by RDS and specifies the authorized signer for each certificate
- ii. **Private Key Storage:** The private key of the authorized signer shall be stored in a smart card issued to the village accountant. The private key of the authorized signer shall be stored in a smart card issued to the village accountant.
- iii. **Document Parts:** The RDS certificate is a single atomic document with no document parts.
- iv. **Secure Data Store:** For Bhoomi RTC there shall be 2 secure data stores which can be used for document verification (for the option of a retrieving the electronic document during document verification)
 1. The primary store shall be the Taluk database at each Taluk
 2. The secondary store shall be the State Data Center (SDC).

By order and in the name of the Governor of Karnataka.

G. SATHYAVATHI
Joint Secretary(e-Governance)
Dept. Personnel & Administrative Reforms (AR)