Secured Delivery of Record of Rights: A G2C Strategy and Implementation

Ganesh Khadanga[1]*, Vinay Thakur[1], D.S Venkatesh[1] and D.C Mishra[1]

ABSTRACT

Maintenance of land records, processing of mutations and delivery and access of documents are key areas which have been revamped as a result of successful Computerisation of Land Records project. Efforts have been also made to share data; contents and documents over Internet with relevant stakeholders. Hand-written copies with manual signatures of competent authority have an assurance value for consumers or citizens. This authenticity can also be introduced into electronic documents through different mechanisms like Digital Signature, Bar Code and Digital Pen. This paper describes these mechanisms of introducing the authenticity into the electronic documents. It is one of the key factor for success of governance projects at grass root level.

Keywords: ROR, I T Act, Digital Signature, Authentication, PKI, XML

1. Introduction

In accordance with priority accorded by Government of India, Computerisation of Land Records has been successfully implemented in more than 3000 Revenue Circles spread across various states as a joint venture between NIC, MRD and State Governments. An expected outcome of project is to enhance quality of service delivery to common citizens in domain of Revenue Administration within Egovernance framework. Maintenance of land records; processing of mutations and delivery and access of documents are key areas which have been revamped as a result of successful Computerisation of Land Records project. Efforts have been also made to share data; contents and documents over Internet with relevant stakeholders. But it is observed that "Computerized copies of documents" need to satisfy basic purpose and value of document from Consumer's point of view as was getting delivered by handwritten documents with manual signatures. Some of these requirements are being listed as follows:

- Hand-written copies with manual signatures of competent authority have an assurance value for consumers or citizens.
- A copy with manual signature has authenticity and admissible as a legal document for evidence.
- It could be preserved for longer periods by using most conventional ways.

It is required that electronic or computerized document should satisfy above requirements in IT enabled delivery scenarios in land management domains.

The relevant section of IT Act 2000: 65B. (1) Notwithstanding anything contained in this Act, any information contained in a electronic record which is printed on a paper, stored, recorded or copied in

[1] National Informatics Centre, Head Quarter, 5th Floor CGO Complex, New Delhi, India
* Corresponding Author: (Email: ganesh@nic.in, Telephone: +91-1124305639)

optical or magnetic media produced by a computer (hereafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or any fact stated therein of which direct evidence would be admissible. (Source: I T Act 2000, Page 43 Section 65B)

Objective

This paper aims at presenting an approach for providing "Secure delivery of documents (Record of Rights)" using various electronic devices and tools such as digital signatures; barcode scanners and e-note takers. This approach is primarily based upon following:

- Using digital signatures for legal authentication as well as for maintaining integrity of electronic document
- Using barcode and image signatures secured by digital signatures so as to facilitate value of paper prints of WEB-enabled delivery of documents.
- Preservation of electronic copies of documents with proper identification

Scope

The scope of functionalities covered by security utility (product) is being given as follows:

- Securing & authenticating operational database at tehsil/Revenue Circle level.
- Validating and securing contents of E_ROR. Generating authenticated and validated electronic document of ROR (E-ROR) from delivery databases in deliverable format.
- Storage and issuance of Identification number for each E-ROR for future references.

Existing setup for generating and delivering Record of Rights at Tehsil level computer centers.

The Record of Rights (ROR) is a document issued by Tehsildar (Revenue Circle officer) to an individual who is possessing land rights under its jurisdiction. It gives an account of plot details and nature of property rights of owner or enjoyer. Further, it acts as documentary proof for ownership as per Revenue registers. Currently, any citizen can visit Tehsil level computer centers to acquire a certified copy of Record of Rights. It could also be viewed over WEB or KIOSK in certain states like Rajasthan; Tamilnadu; Uttaranchal; UP etc. There are approx 10 states which have hosted their Land Records for public viewing over WEB. However, web-copies of ROR_document can not be regarded as a legal document for the reasons of authentication and validation of contents.

Operational Site

In accordance with guidelines issued by Govt of India, computer centers (Figure 1) have been established at Tehsil level for operations and issuance of Record of Rights; Mutations and other related functions of revenue administration. Revenue functionaries are carrying out basic operations like data entry and mutation updation, notification at circle/tehsil level/anchal level.

As per existing operations, any citizen can visit to Tehsil level computer centers and apply for a copy of ROR after paying fixed user charges. Tehsildar or village accountant or any other authorized operators could provide him a computer print out of ROR with proper manual signatures. In number of states, manual copies of ROR have been replaced with computerized copies by Government order and accorded a legal status. Each Tehsil level computer center is equipped with One Server and two clients m/c. These systems are connected over LAN. In certain cases mutation is being carried out online. The access to system and data is being restricted by USER/PWD (challenge /response) as well as biometrics authentication.

Operational access to databases is restricted by various security measures to authorized users such as Village accountants/Tehsildars/Operators. But in entire process of ROR issuance and delivery a citizen has

to establish a manual interface with ISSUING AUTHORITY which could sometime lead to renting practices and inconvenient delays. Keeping in view of an efficient and transparent delivery of ROR, it is required to provide authenticated copies of ROR from KIOSK or WEB-site in ONLINE mode. From this perspective, Govt of India is encouraging the states to setup WEB-SITES for facilitating delivery of ROR to common citizen. An outline of proposed framework is being given for general understanding.

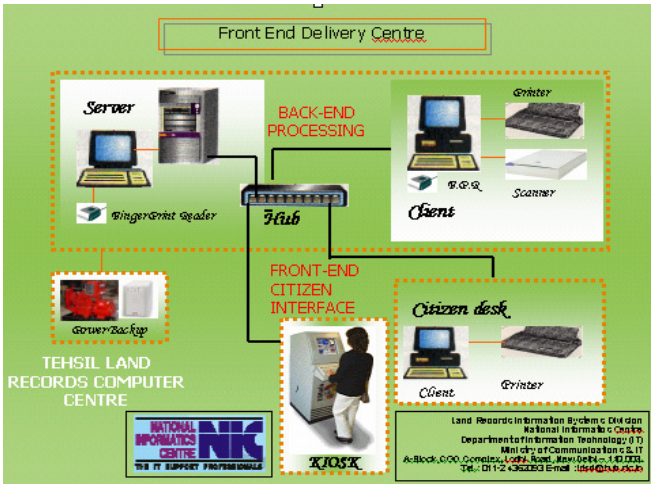


Figure 1: Basic Tehsil Setup for CLR

Table 1: List of Hardware and software as available in a *Tehsil* Computer Center

Sl. No	Hardware/Software systems	Desired functionality
1	One Server	Hosting LR-database (1-4 GB RAM)
2	2 Client m/c	For official operations like notice generation; data entry
3	Land record application s/w loaded at client system	User functions/ Access control/Printouts etc.
4	Biometric system	Bioauthentication/Non-repudiation
5	LAN	Connecting Systems; Printers/scanners etc/Kiosk
6	KIOSK	Delivery of document (not very common)

2. Proposed Framework for Secure Delivery of Documents (Record of Rights)

In order to achieve a successful operational infrastructure for ROR delivery, it is recommended to use SDC (State Data Center) as single point delivery of E-ROR. This would in turn require

- Secure connectivity between *tehsil* (operational site (OS)) and SDC for online data transmission (>256 Mbps)
- Mirror databases at SDC to accept copy of transactions at each tehsil
- General as well as secured web sites over Internet and Intranet respectively
- Availability of digital signature for authorized users (DSC)
- Redundant backup site at district data server

Functional requirements to be taken into account while determining a secured way of ROR delivery.

As is evident that a citizen could obtain an electronic copy of ROR with proper authentication from

- Tehsil level LR centers or Kiosks
- Web based delivery from authorized sites
- From authorized private outlets

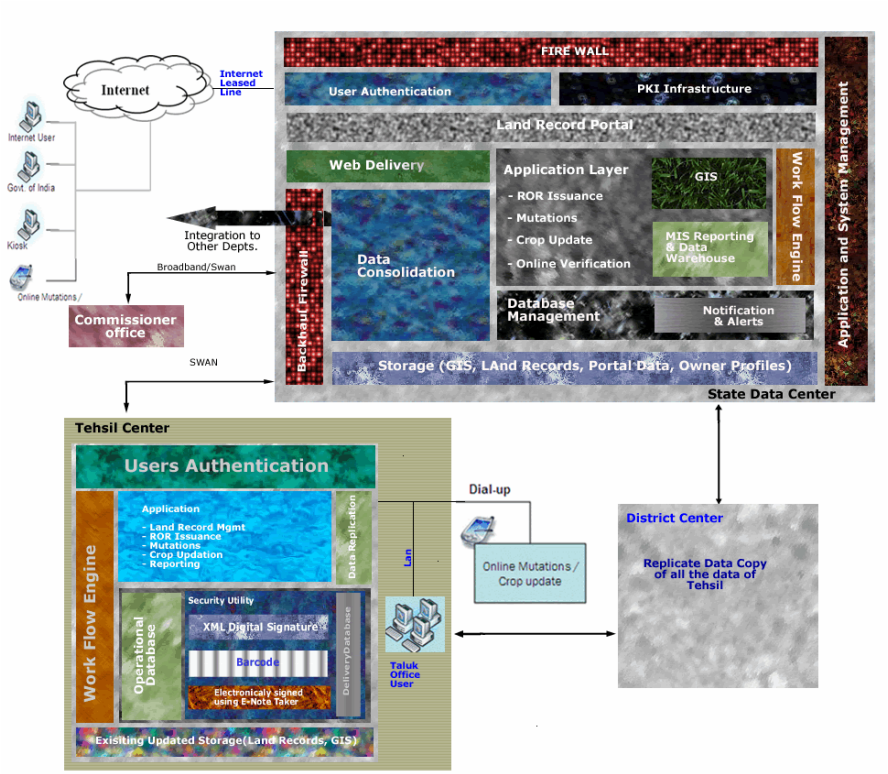


Figure 2: Proposed Framework for Delivery of Secure ROR

In order to facilitate such operations, one needs to address following issues:

1. How to authenticate existing operational database having legacy data to the volume of 1-3 GB.
   Highlights: There are solutions to sign the whole database at the end of operations in a day. When we start the database on the next day, the first operation should be that the data is same with that of the last shutdown. This will ensure that some body has not made any tampering during the night when the office is closed.
2. Who does this authentication and how?
   Highlights: This can be done automatically by the software. And it needs to be developed.
3. How to capture updation of ROR in during workflow.
   Highlights: Once the ROR is updated because of mutation the ROR once again can be signed and the final ROR in XML/XPS format can be stored in our delivery database.
4. Do all tables (4-20) or records need to be authenticated?
   Highlights: It can be done by signing against each record and storing the hash in an additional column in the tables. There are also solutions at hardware level which can sign bulk data with limited time. The smart functionality can be fused inside a card and attached to the system itself.
5. Authentication needs to be done Record by Record (4KB) or as a whole.
   Highlights: It is possible to have the complete ROR in an XML/XPS doc and can be stored in SQL Server 2005. The ROR as issued to public can be given an ID.
6. Authenticated contents need to be stored in a table or database.
   Highlights: It is possible to have the complete ROR in an XML/XPS doc and can be stored in SQL Server 2005 in a table in the same database. Or it can also be stored in another database.(called deliver database)

7. What is the procedure and technology for authentication?
   Highlights: The PKI infrastructure can be used for authentication.
8. How to enable secure transmission of data and content?
   Highlights: We are suggesting VPN or Secured connection over SSL for secured transmission of the data content.
9. What is structure of remote database at SDC?
   Highlights: SDC will have the structure with national perspective. It should have to follow the uniform coding's for locations and the general code types like land, crop and caste.
10. How to generate Secure ROR document?
    Highlights: The Secure ROR can be generated from the central repository of the ROR database.(XML/XPS files with digital sign in sql 2005 database)
11. How to keep backup of authenticated copies of registers/ror and database?
    Highlights: The PKI infrastructure can be used for this.
12. What is tenure for archiving digitally signed documents and their validity?
    Highlights: This depends of the official acts as issued by different State and Central Govt.
13. What are hardware / software requirements at each operational site?
    Presently for CLR verification is suggested that the sites should be connected with each other through a network.
14. Is there any business process modifications would be required?
    Some business needs to be modified as per the new requirements and digital signing process.
15. Would it require any legal changes?
    The legal requirements are yet to be analyzed with respect to latest IT Act and the rule of the State. In page 2 of IT act it is mentioned that "Nothing in this Act shall apply to,-
    (a) a negotiable instrument as defined in section 13 of 26 of 1881. The negotiable instrument Act, 1881;
    (b) a power-of-attorney as defined in section 1A of the 7 of 1882. Powers–of-Attorney Act, 1882;
    (c) a trust as defined in section 3 of the Indian Trusts 2 of 1882 Act, 1882;
    (d) a will as defined in clause (h) of section 2 of the Indian 39 of 1925. Succession Act, 1925 including any other testamentary disposition by whatever name called;
    (e) any contract for the sale or conveyance of immovable property or any interest in such property;
    (f) any such class of documents or transactions as may be notified by the Central Government in the official Gazette.

The points (e) and (f) needs to be reviewed based on the State Government policies and principles.

16. What are tools\technology requirements for tehsil/mandal/anchal or at state data center level?
    It needs to be reviewed based on the provisions of the s/w and data center facilities. However the tehsils needs to be connected to CA for an online CRL verification process.

Why a separate database/content management is required for document delivery:

From legal perspective, following points must be taken into account:

- "Record of Rights" is essentially a legal document, which is having evidentiary value in court of law for cases related with land matters. Thereby we have to ensure that E-ROR also should be also having legal status as per IT act. In order to comply with IT act, it is recommended to opt for "digital signatures" for authentication of electronic document of ROR.
- Secondly, the document, which has been given to citizen, needs to be stored or archived to be reproduced for future requirements.
- As per existing rules, digital signature certificates are issued for two years and may be maintained by concerned CA for stipulated period as agreed between user and CA.

Presently, this computer-generated copy of ROR is being authenticated by manual signature of authorized local official. As such there is no provision to store/archive these computerized copies of ROR, which are being given to citizens. It may not be required as concerned officers are signing each copy and an office copy is to be preserved in form of register.

In case of digitally signed electronic document, it may not be possible to reproduce same copy if any changes have occurred in local database or report formats during the interval between two demands. For example, we may consider a scenario: An electronic ROR has been issued with digital signature at time=t1 with application s/w version=V1 and database state=s1. After some time application s/w and database as well as issuance authority may change. Under the circumstances at time=t2, it may not be possible to generate exact copy of same document which was delivered at time=t1. Since each document given to citizen has its own evidentiary value, it may be required to protect each delivered document similar to provision available in existing manual system. This may require that each issued document should be stored with document-id. In order to ensure protection of document as delivered; it is required to keep it as a record in document_database with identification for retrieval. This provision would also ensure that there is no effect of software modifications or data-updation over already delivered document.

Secondly delivery database consisting of document may also be used for verification of digital signatures as is being done by various service providers like MTNL etc. This database may also support INTRANET with adequate security and its subscription may be extended to various stakeholders like banks; courts etc.

3. Description of technical scheme for enabling security

For the purpose of this document, we are confining ourselves to discuss techniques and approach which could be adopted for defining a secured delivery of ROR either from Tehsil level centers or over WEB**.** There are number of related issues like overall security of systems and operations; networking and databases are not being covered within the existing scope. As discussed above, confidentiality; integrity and authentication are key requirements, which need to be fulfilled by a secured solution within the ambit of legal framework. Keeping it in view, a technical scheme was worked out using following tools/devices or methods:

Table 1: Relationship between desired functionality and appropriate technology

Sl. No.	Technical interface	Functionality offerings
1	Digital Signature for Village accountants; Tehsildar	Authentication by signature/ Verifiability against any tempering
2	Digital signature on smart card	Security and physical presence for individual signature
3	Access to CA from user's site	Verification of signatures/ revocation list
4	Online access to CA	Time stamping
5	Bulk signing device for database	Authenticating Operational legacy databases
6	2D-Barcode	For verification of official contents and making it temper proof document where access to net is not available
7	E-Pen note taker	Analogues to existing manual signatures as most people would be still comfortable with hand signatures and it would be possible to take a paper print out with signatures from WEB
8	Digitally signed PDF of ROR	Protecting the delivery documents

- XML digital signature: For authentication and exchange of desired fields for generating ROR.
- Barcode: For generating a barcode over printed output to secure and validate content of records.

- E-pen: To provide manually signed printed copy over WEB in pdf formats, which is digitally signed, and time stamped. (optional)

The relationship between desired functionality and appropriate technology is being given in Table 1

3.1 Digital Signature

Digital Signature PKC (Public Key Cryptographic) enables electronic messages with a mechanism analogous to signatures in the paper world, known as a *digital signature.* However, a digital signature verifies the authenticity of electronic documents and provides stronger security than do signatures on paper documents.

The digital signature protocol helps to ensure the following:

- The signature is authentic. When the receiver verifies the message with the sender's public key, the receiver knows that the sender signed it.
- The signature cannot be forged. Only the sender knows his or her private key.
- The signature is not reusable. The signature is a function of the document and cannot be transferred to any other document.
- The signed document is unalterable. If there is any alteration to the document, the signature verification will fail at the receiver's end because the hash value will be recomputed and will differ from the original hash value.
- The signature cannot be repudiated. The sender cannot deny previous committed actions, and the receiver does not need the sender's help to verify the sender's signature.

3.2 Bar codes

Barcodes provide a simple and inexpensive method of encoding text information that is easily read by inexpensive electronic readers. Bar coding also allows data to be collected rapidly and with extreme accuracy. A bar code consists of a series of parallel, adjacent bars and spaces. Predefined bar and space patterns or "symbologies" are used to encode small strings of character data into a printed symbol. Bar codes can be thought of as a printed type of the Morse code with narrow bars (and spaces) representing dots, and wide bars representing dashes. A bar code reader decodes a bar code by scanning a light source across the bar code and measuring the intensity of light reflected back by the white spaces. The pattern of reflected light is detected with a photodiode, which produces an electronic signal that exactly matches the printed bar code pattern. This signal is then decoded back to the original data by inexpensive electronic circuits. Due to the design of most bar code symbologies, it does not make any difference if you scan a bar code from right to left or from left to right.

A barcode (also bar code) is a machine-readable representation of information in a visual format on a surface. Originally barcodes stored data in the widths and spacings of printed parallel lines, but today they also come in patterns of dots, concentric circles, and hidden in images. Barcodes can be read by optical scanners called barcode readers or scanned from an image by special software. Barcodes are widely used to implement Auto ID Data Capture (AIDC) systems that improve the speed and accuracy of computer data entry.

3.3. Epen Notetaker

Electronically signed document using Epen Notetaker: A User can add their signature note to the document using Epen Note taker. It is useful to identify the person who signed the received document. For this purpose we use the *hitech_cleonpen-OCX control*. It captures the signed note, which is added to the documents.

3.4 Steps for application of various techniques with LR databases (Method described here is applicable for single record)

- Generally Record of Rights consists of 8-10 columns, which varies from state to state. To generate the Record of Right, first we select required fields (attributes) from relevant tables (for example Owner_details; Plot_details; District master; Crop_details , RPT Khasara) as usual from existing LR_database. Once query is processed, output or record set may be derived to a xml_file. This file could be digitally signed using an appropriate API. This procedure has a merit over normally signing entire record set by digital signature as it is based on canonicalization of XML file. [The canonical form of an XML document is important when you look at signing. Signing an XML document consists of calculating a message digest (hash) to ensure message integrity and signing the message and the hash with the private key of the sender. The receiver would then use the public key to verify. The verification procedure should go successful regardless of the physical representation of the XML_document. It is important to calculate the message digest on the canonical form of the XML document]. This XML file is temporary in nature and gets deleted automatically after entire process of signing and storing is over. It will consist of "signature node" (signature value and digest value) as well as values of desired columns (plot-no, area, owner_details etc). SQL server –2005 extends a feature to store digitally signed XML object in database. Alternatively, instead of creating a XML, desired attributes may be selected and digitally signed and stored in database.
- Generate the barcode image for selected column (plot-no, area, owner_details) consequently; an encrypted image of selected columns is generated.
- At the same time "signnote": a utility for capturing personal signatures is activated using E-NoteTaker.
- Final output in terms of xml file; barcode image and personal signature-image is directed for delivery database (created only to store delivery documents and contain only one table (signed_ror).
- Finally Record of right is generated.

When the authenticate Record of Right is saved to the database an automated Id is generated for that ROR through which we can access that record in future. If any one changes the Record of Right then the xmlsignature cannot verify and it means record is changed and it needs to be authenticate again. To authenticate the record of right we generate the xmlsignature using smart card (PKCS #7 compliant), sign note using E-Note Taker and barcode utility. These techniques could be interfaced with existing application and database as depicted Figure 3.

When we open a form to print a signed ROR, we choose District, Tehsil, RI, Halka, Village and Kasra Number and then write a signed note on a Paper using E-Pen. Whatever we write on the paper using E-Pen it automatically display on the screen white box.

After completing my note we click on Print ROR, it displays the Record of Right with my note and Barcode. If we want to verify the digital signature of ROR then first we select the ROR then click on verify Digital Signature. It there is no change found in the ROR then it shows verify otherwise it display signature not verified.

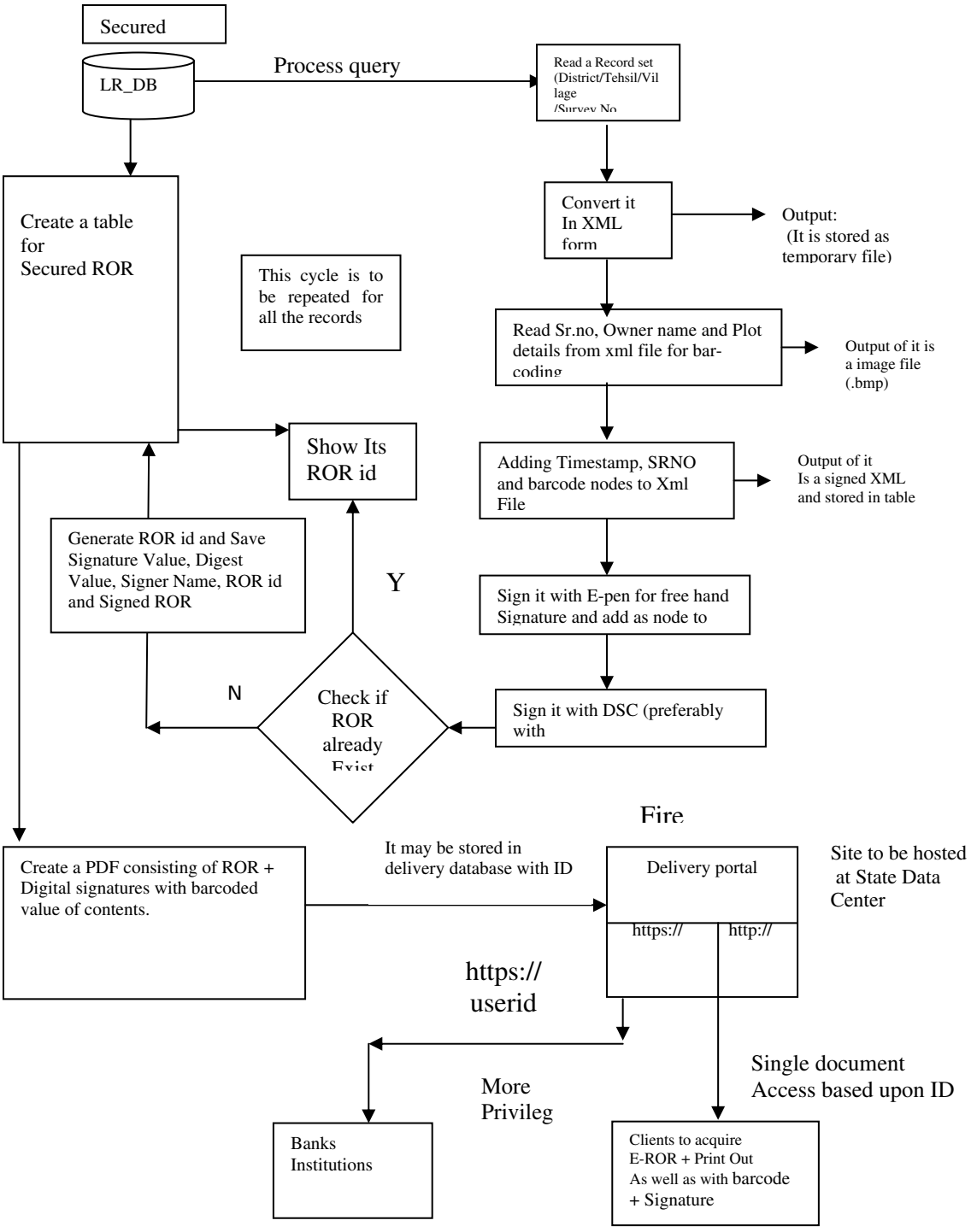


Figure 3: Procedure for Regenerating the ROR

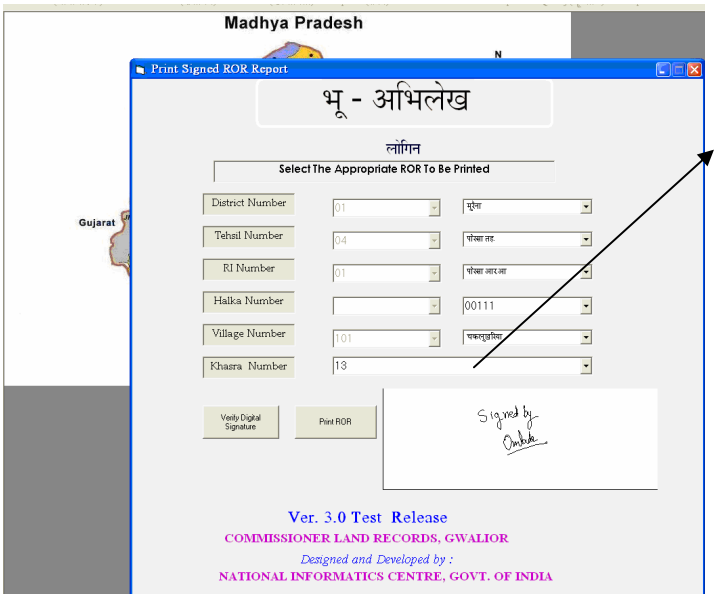
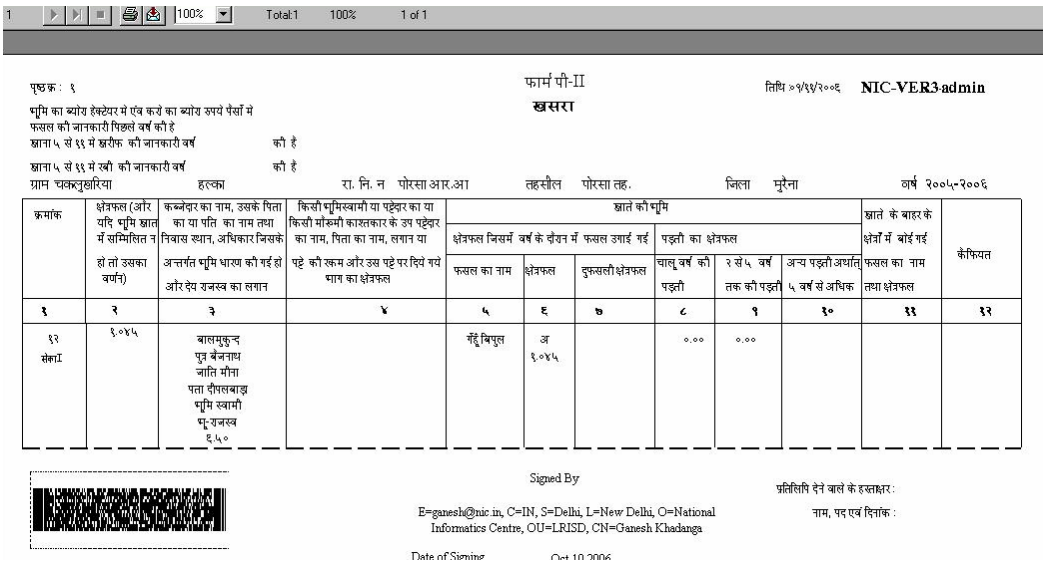


Figure 4: Screen for selecting the ROR



फार्म पी-II

खसरा

तिथि ०१/६१/२००६ NIC-VER3-admin

क्रमांक	क्षेत्रफल (और यदि भूमि खाते में सम्मिलित न हो तो उसका वर्णन)	कब्जेदार का नाम, उसके पिता का या पति का नाम तथा निवास स्थान, अधिकार जिसके अन्तर्गत भूमि धारण की गई हो और देय राजस्व का लगान	किसी भूमिस्वामी या पट्टेदार का या किसी मौऊमी काश्तकार के उप पट्टेदार का नाम, पिता का नाम, लगान या पट्टे की रकम और उस पट्टे पर दिये गये भाग का क्षेत्रफल	खाते की भूमि: क्षेत्रफल जिसमें वर्ष के दौरान में फसल उगाई गई			खाते की भूमि: पड़ती का क्षेत्रफल			खाते के बाहर के क्षेत्रों में बोई गई फसल का नाम तथा क्षेत्रफल	कैफियत
				फसल का नाम	क्षेत्रफल	दुफसली क्षेत्रफल	चालू वर्ष की पड़ती	२ से ५ वर्ष तक की पड़ती	५ वर्ष से अधिक		
१	२	३	४	५	६	७	८	९	१०	११	१२
९२ सेकाI	१.०४५	बालमुकुन्द पुत्र बैजनाथ जाति मौना पता दीपलबाड़ू भूमि स्वामी भू-राजस्व ६.५०		गेहूँ बिपुल	अ १.०४५		०.००	०.००			

Signed By

E=ganesh@nic.in, C=IN, S=Delhi, L=New Delhi, O=National Informatics Centre, OU=LRISD, CN=Ganesh Khadanga

Date of Signing Oct 10 2006

प्रतिलिपि देने वाले के हस्ताक्षर :

नाम, पद एवं दिनांक :

Figure 5: Signed ROR

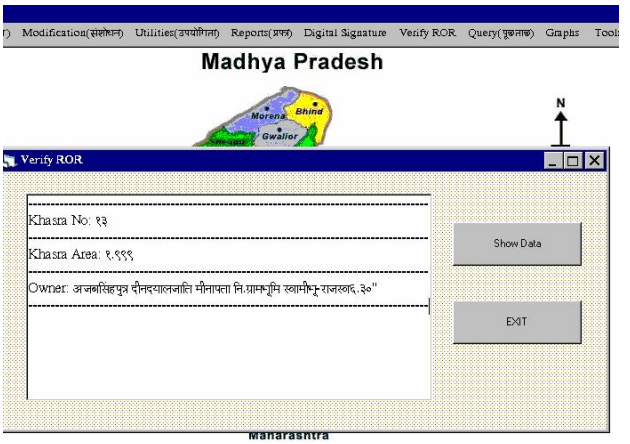


Figure 6: Read the Barcode printed on signed ROR (Source Ref. 5)

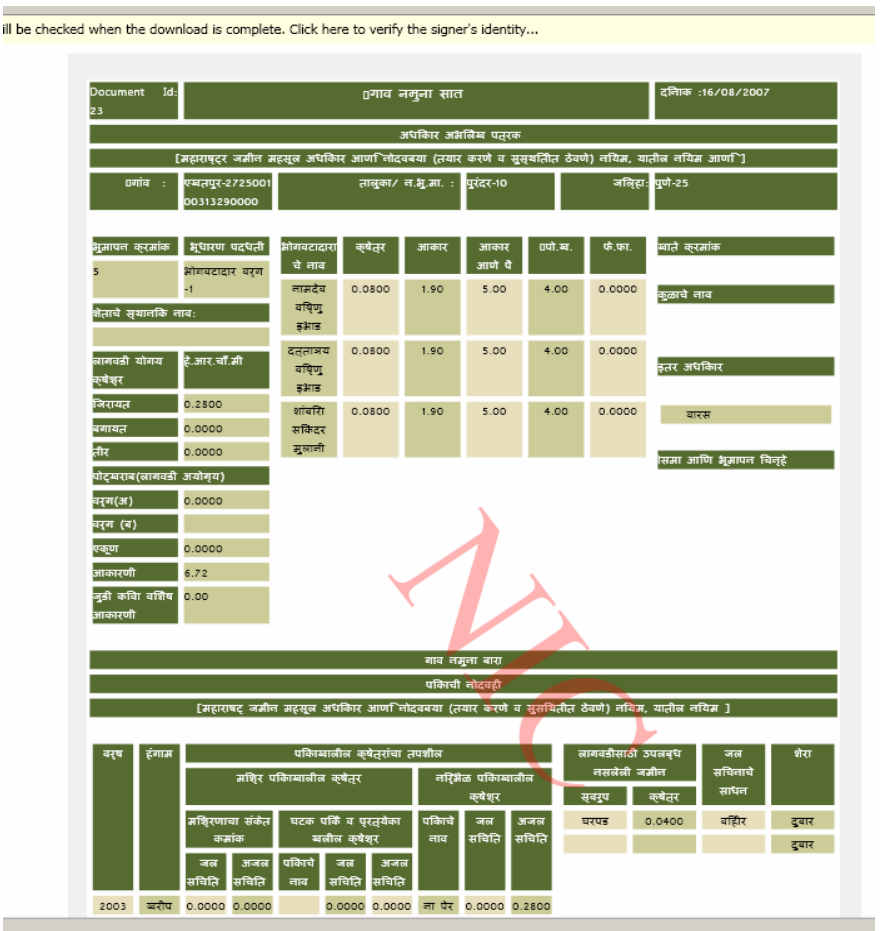


Figure 7: Sample ROR (Source Ref. 4)

References

1. Amaranathan L. C. (2002). Technological Advancements: Implications for Crime. *The Indian Police Journal.* April-June 2002, pp.7-16.
2. Deshmukh, S.G., Aggarwal V., Vijay K.V., and Pant A.K. (2004). Some Reflections on e-governance and Indian democracy, appeared in M. P. Gupta (Ed) "*Towards E-Government*". Tata McGraw-Hill, New Delhi, pp.568-573
3. West, Darrell M. (2007 August). *Global E-Government, 2007*. Providence: Center for Public Policy, Brown University.
4. Thong, James Y.L. (1999). An Integrated Model of Information Systems Adoption in Small Businesses. *Journal of Management Information Systems, 15(4)*, 187-214.
5. Mishra, P. (2005), *Cadastral Surveys in India*, Coordinates Journal.

About the Authors

Ganesh Khadanga is a software developer in National Informatics Center at New Delhi in India. He holds a B.Sc Engineering from University College of Engineering Orissa and a M.Tech from IIT Kanpur in Civil Engineering. He has published papers related issues of rehabilitation of people in Gohira Irrigation Project at Orissa, Land Records Comuterisation in India, discussion in ASCE, Journal of Irrigation and Drainage Engineering and authored a book on C# programming language. He has guided many graduate level students on their research projects and is having vast experience in local language translation from ISCII/ISFOC to Unicode and database applications in land records computerization in India.

Vinay Thakur is Technical Directors in National Informatics Center (NIC). Department of Information Technology, New Delhi. He holds BE from Jabalpur University and ME in computer Science from Delhi University. He has been associated with software design and development for Land Information System for last 15 years and published around dozen papers on Land Records System and e-Governance. He has guided many graduate and post graduate level students on their research projects.

D.S. Venkatesh is a Scientist-D (Principal Systems Analyst) in National Informatics Center (NIC), Headquarters in New Delhi. He holds a B.E in Electronics from Bangalore University. He is qualified Lead Assessor for Information Security Management System (ISMS) (ISO 27001:2005) accredited by IRCA UK. He has also qualified as a practioner for implementing ISMS. He has been associated in the design, development, documentation, ISO Quality testing and Certification and implementation of Application software and databases for the domain of Land Records for various States in India. He has co-authored papers related to Computerisation of Land Records.

D.C. Mishra is working as a Senior Technical Director and Head, Rural Development Informatics Systems (RDIS) Division, National Informatics Center, Ministry of Information Technology, Government of India. He is a Rural Informatics Specialist and is associated with the computerization of Rural Development Sector for more than 20 years.