



Assam e-District Project

Digital Signature Training

Participant Reference Guide
for Statewide Rollout of Assam e-District Project



Assam Electronics
Development Corporation Ltd.

Information Technology Department
Government of Assam



Medhavi Solutions (India) Pvt. Ltd.

PREFACE

Electronic signature is a broader term that refers to any electronic data that carries the intent of a signature. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit (tamper-proof). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.

IT Act 2000/ 2008 (amended) and it also recognizes electronic records, such as, information or any other matter in electronic form. The use of electronic records and digital signatures in Government and its agencies has been approved as a policy matter within the meaning of IT Act. The Govt. of India has started using the Digital Signature across all platforms such as granting of licenses, permits, filing of applications, payment of charges and other financial transactions through electronic means. Both the central and state governments are in the midst of developing full infrastructure for all-round electronic transactions, which will see use of Digital Signature substantially.

This training material titled “**Digital Signature**” provides an overview to the digital signatures, with details about its working, components and classifications. It would surely help the participants how to install and use digital signature in dealing with e-District service delivery in electronic mode.

Disclaimer: The information contained herein is subject to change without notice. We shall not be liable for technical or editorial errors or omissions contained herein. The name used in the participant reference material for this course is that of a fictitious company. Any resemblance to any company name is purely coincidental. We do not believe we have used anyone’s name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Use of screenshots, photographs of another entity’s products name, or service in this reference material is only for editorial purposes. No such use should be construed to imply sponsorship or endorsement of the book by, nor any affiliation of such entity. This courseware may contain links and reference from sites on the Internet that are owned and operated by third parties.

TABLE OF CONTENTS

Chapter 1: Introduction to Digital Signature

DIGITAL CERTIFICATE	2
DIGITAL SIGNATURE	2
HOW DIGITAL SIGNATURE WORKS?	4
PUBLIC KEY INFRASTRUCTURE (PKI)	5
PUBLIC KEY CRYPTOGRAPHY ENCRYPTION TECHNOLOGIES	6
DIGITAL CERTIFICATE: COMPONENTS	7
DIGITAL CERTIFICATE: CLASS CLASSIFICATION	8
LEGAL VALIDITY OF DIGITAL SIGNATURES OVER IT ACT 2000/2008	8
INSTALL TOKEN DRIVER FOR FIRST TIME USERS - EPASS 2003	9
STEPS FOR ENROLLING DIGITAL SIGNATURE CERTIFICATE WITH EPASS 2003	12
INSTALLING RSA PRIVATE KEY IN THE TOKEN.....	15
ANNEXURE: DeitY, GOVERNMENT OF INDIA GUIDELINE.....	21

Introduction to Digital Signature

Chapter Objectives:

A Digital Signature unlike hand written signature, is used while sending any documents or message while transmitting through Internet or electronically. Today digital signature has gained the value of digitally equivalent of a hand written signature due to various unique features like security, authenticity and long term preservability etc. This chapter gives presents an overview to the Digital Signature and its usage.

Chapter in a Nutshell:

DIGITAL CERTIFICATE

DIGITAL SIGNATURE

HOW DIGITAL SIGNATURE WORKS?

PUBLIC KEY INFRASTRUCTURE (PKI)

PUBLIC KEY CRYPTOGRAPHY ENCRYPTION TECHNOLOGIES

DIGITAL CERTIFICATE: COMPONENTS

DIGITAL CERTIFICATE: CLASS CLASSIFICATION

LEGAL VALIDITY OF DIGITAL SIGNATURES OVER IT ACT 2000/2008

INSTALL TOKEN DRIVER FOR FIRST TIME USERS - EPASS 2003

STEPS FOR ENROLLING DIGITAL SIGNATURE CERTIFICATE WITH EPASS 2003

INSTALLING RSA PRIVATE KEY IN THE TOKEN

Digital Certificate

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Digital Signature

- A digital signature is an electronic signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document.
- To provide Authenticity, Integrity and Non-repudiation to electronic documents.
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance.
- A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Sample of digitally signed certificate issued in e-District pilot, Assam:

[illegible]

Fig.1.1: Sample of Digitally Signed Certificate issued in Pilot e-District Project

How Digital Signature Works?

The following flow chart shows how the digital signature works:

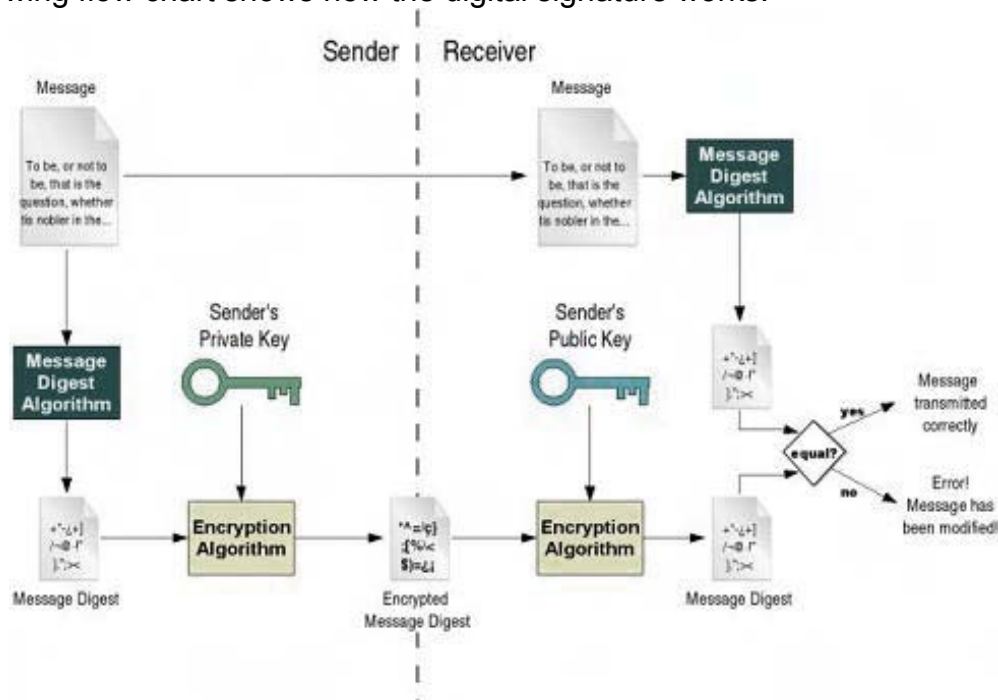


Fig. 1.2: Working of Digital Signature

The processes are:

- Key Generation
 - Random Numbers
 - RSA Key Pair
- Digital Signature
 - Generate Message Digest
 - Encrypting Digest using Private Key
 - Attaching the Signatures to the message.
- Verification of Signatures
 - Run the test for Authentication, Integrity and Non repudiation.
- Digital Signature Certificate

The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner. The key can be secured using:

1. PIN protected soft tokens:

- The Private key is encrypted and kept on the Hard Disk in a file, this file is password protected.



- This forms the lowest level of security in protecting the key, as
 - The key is highly reachable
 - PIN can be easily known or cracked.
- Soft tokens are also not preferred because
- The key becomes static and machine dependent.
- The key is in known file format.

2. Smart Cards

- The Private key is generated in the crypto module residing in the smart card.
- The key is kept in the memory of the smart card.
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (Having smart card reader)



3. Hardware Tokens

- They are similar to smart cards in functionality as
 - Key is generated inside the token.
 - Key is highly secured as it doesn't leave the token.
 - Highly portable.
 - Machine Independent.
- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.



Public Key Infrastructure (PKI)

- Some Trusted Agency is required which certifies the association of an individual with the key pair.
 - Certifying Authority (CA)
- This association is done by issuing a certificate to the user by the CA
 - Public key certificate (PKC)
- All public key certificates are digitally signed by the CA

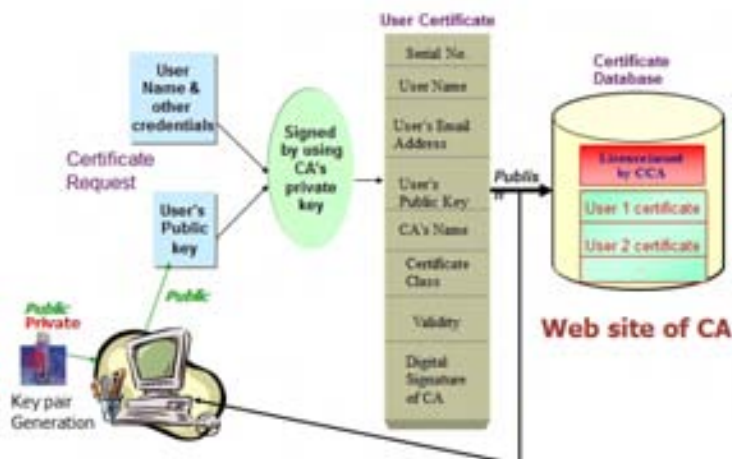


Fig. 1.3: Public-Key certification process

- Private key of CA or CCA require highest level of security
- Hardware Security Module (HSM) is used for storing the Private Key
- More than one person are required for signing
- Controller is the Root certifying authority responsible for regulating Certifying Authorities (CAs)
- Controller certifies the association of CA with his public key
- Certifying Authority (CA) is the trusted authority responsible for creating or certifying identities.
- CA certifies the association of an individual with his public key

Public Key Cryptography Encryption Technologies

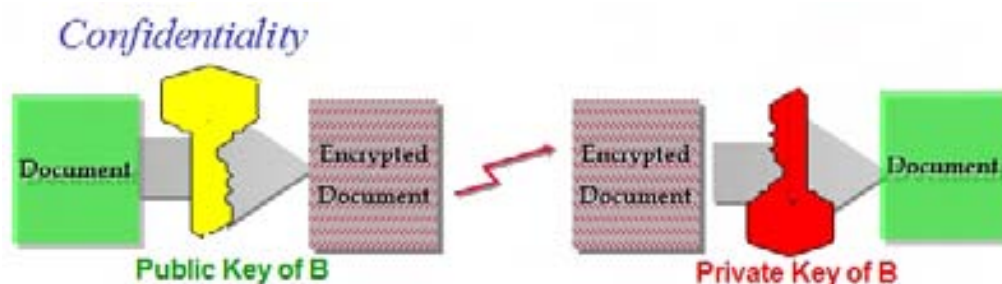


Fig. 1.4: Public-Key certification process



Digital Signature also ensures that no alterations are made to the data once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which it can be renewed.

- A Digital Signature is a method of verifying the authenticity of an electronic document.
- Digital signatures are going to play an important role in our lives with the gradual electronization of records and documents.
- The IT Act has given legal recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification.
- The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems (system meant for encoding and decoding secret messages). The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

Digital Certificate: Components

Contents of Typical Digital Certificate:

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person, or entity identified.
- Signature Algorithm: The algorithm used to create the signature.
- Signature: The actual signature to verify that it came from the issuer.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date the certificate is first valid from.
- Valid-To: The expiration date.
- Key-Usage: Purpose of the public key (e.g. encipherment, signature, certificate signing).
- Public Key: Public-key encryption uses a key pair for encryption and decryption of data associated with it.
- Thumbprint Algorithm: The algorithm used to hash the public key.
- Thumbprint: The hash itself, used as an abbreviated form of the public key.

Digital Certificate: Class Classification

- Class 1 Digital Signature is used primarily for authenticating email message or any other electronic communication by individual
- Class 2 Digital signature certificates are issued to Individual or organization for various purposes. Class 2 A digital signatures for individuals is personal certificate that provides second highest level of assurance within the RCAI hierarchy setup by CCA (Controller of Certifying Authorities) in India which is mainly used for MCA21, ROC, Income Tax e-filing, sign a word or excel file, sign e-mail sent through Outlook etc.
- Class 3 digital Certificate
 - **Individual (Class 3 a Digital Signature Certificates):** Class 3a Individual certificates issued to individuals or devices and encompass primarily high end security-sensitive online activity.
 - **Organization (Class 3b Digital Signature certificates):** Class 3b Organization certificates those are used for signing, encryption, electronic access control, e-commerce, and online financial transactions that require a strong assertion of the customer's identity. The validation procedures for class 3 Organization certificates include confirmation that the org. does in fact exist, authorization from the org. for the certificate applicant.

Legal Validity of Digital Signatures over IT Act 2000/2008

The Indian Information Technology Act 2000 came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000.

The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country.

The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users. Section 5 of the

Act gives legal recognition to digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.

Install Token Driver for First Time Users - EPASS 2003

Step: 1 Select **ePass2003-Setup** file in order to install the driver in your system as shown in the figure below:

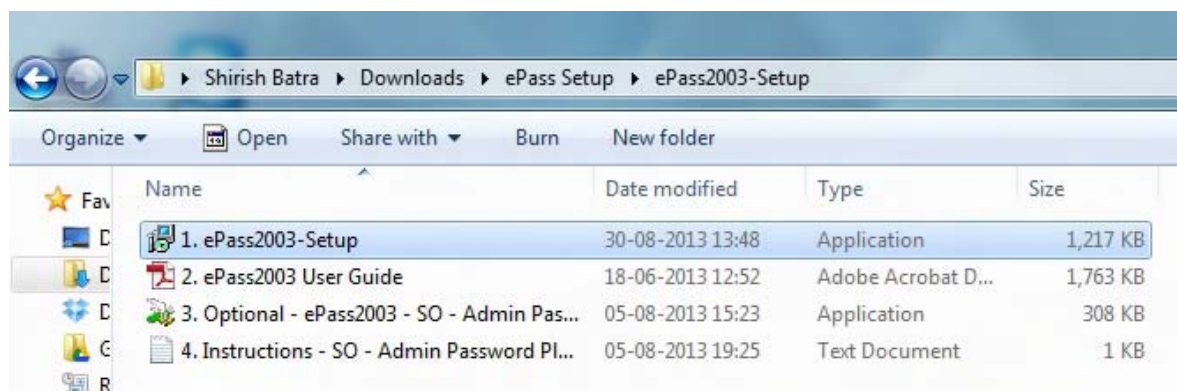


Fig. 1.5: ePass2003 setup files

Step: 2 Open ePass2003 Token Manager. Click on the **arrow** displayed above the **Exit** button as shown in the figure below:

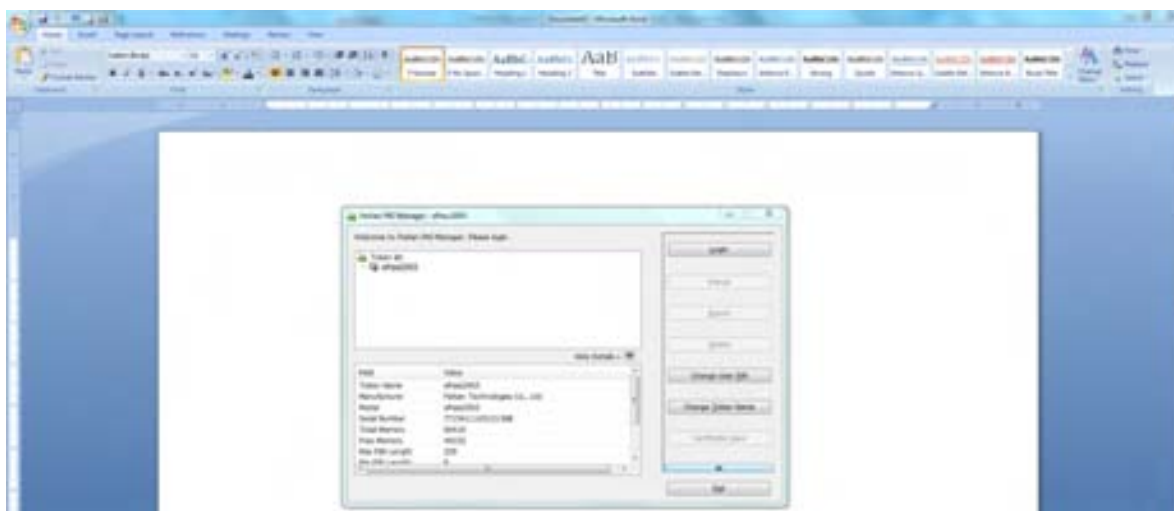


Fig. 1.6: Feitian PKI Manager ePass 2003

Step: 3 Click on **Initialize** button and click on **OK** button to confirm the initialization process as shown in the figure below:

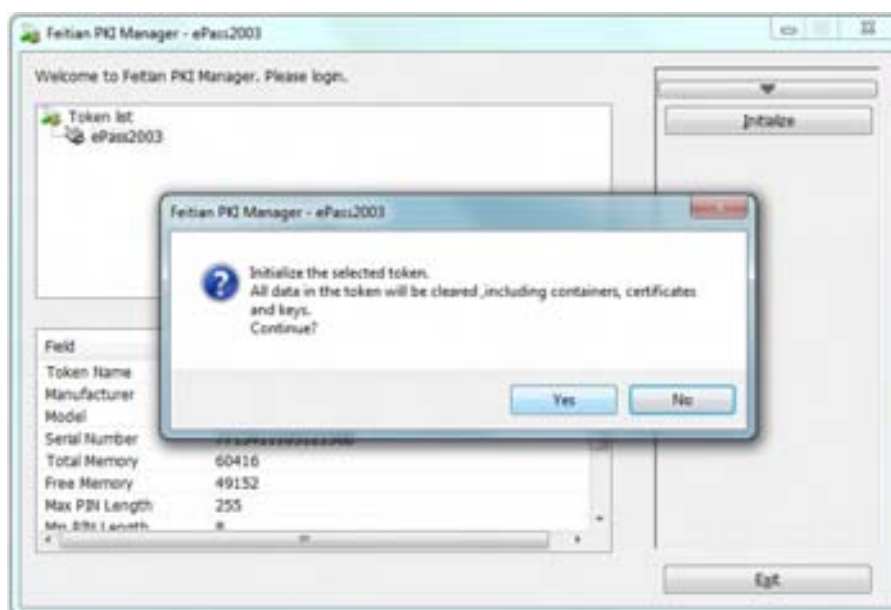


Fig. 1.7: Feitian PKI Manager ePass 2003: Initialization process

Step: 4 Once the initialization process is completed, the system will prompt with a message as shown in the figure below:

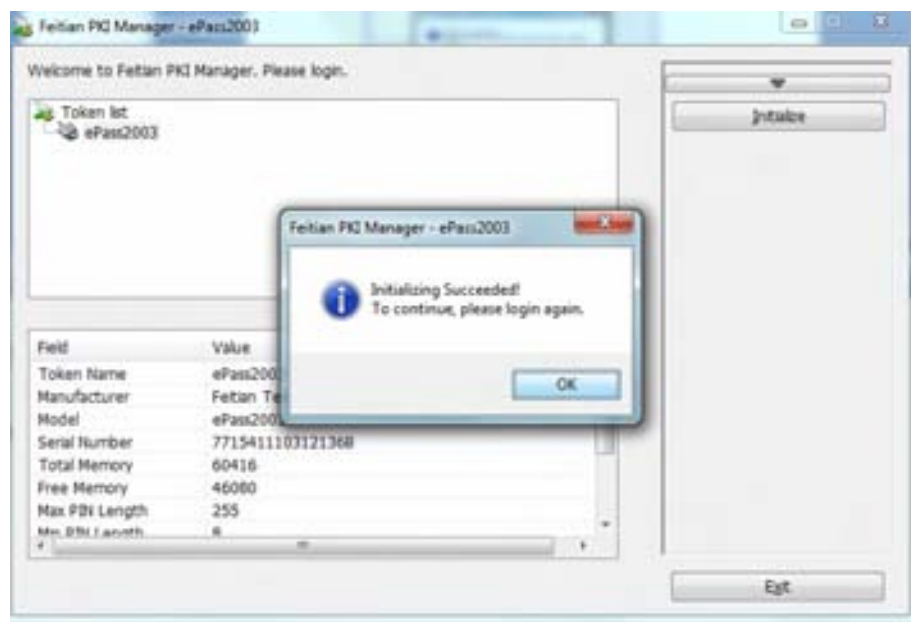


Fig. 1.8: Feitian PKI Manager ePass 2003: Initialization success message

Step: 5 Once the ePass2003 initialization is completed, you can click on **Change User Pin** to change the pin of your ePass2003 system.

Step: 6 Type your current pin as **12345678** in the **Old user PIN** text box. Type your new pin in the **New user Pin** text box and confirm the same in the **Confirm** text box as shown in the figure below:

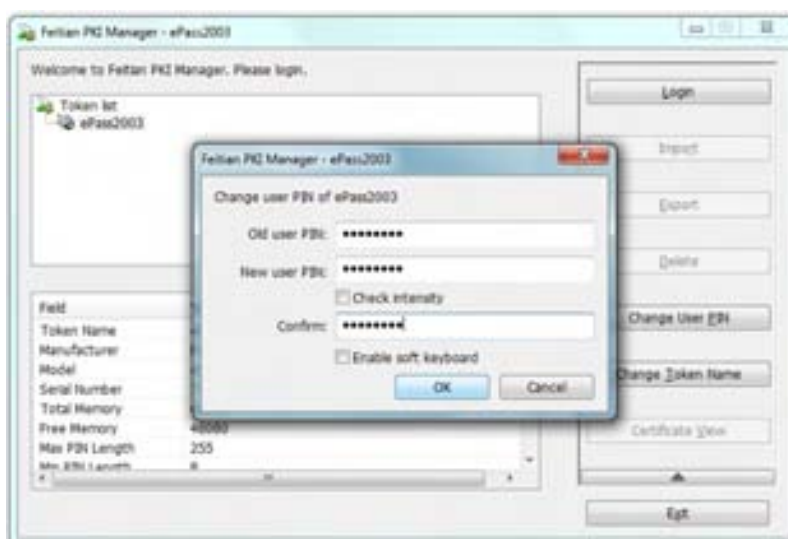


Fig. 1.9: Feitian PKI Manager ePass 2003: Change User PIN

Step: 7 Click **OK** button to continue and you will be prompted with successful PIN change message as shown below:

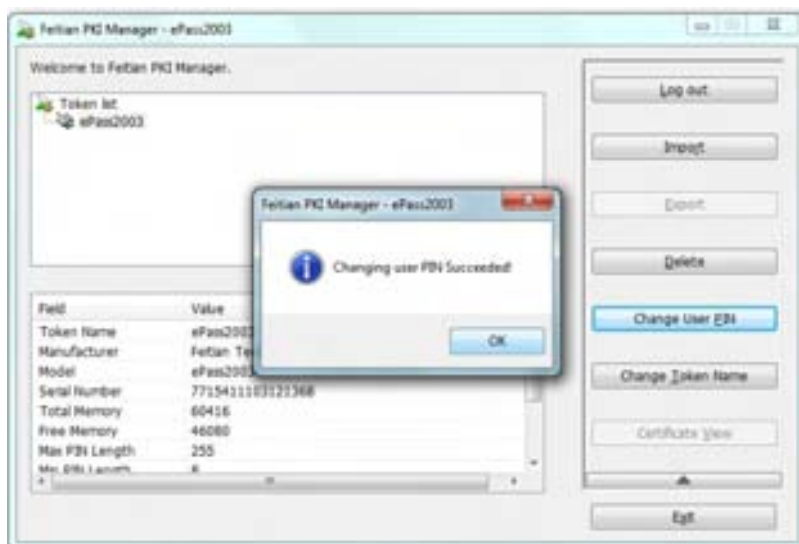


Fig. 1.10: Feitian PKI Manager ePass 2003: Change User PIN success message

Steps for Enrolling Digital Signature Certificate with ePass 2003

Step: 1 Open the enrolment link as shown in the figure:



Fig. 1.11: The Sify Safescript webpage

Step: 2 Select the certificate class and type with validity as shown in the figure below:

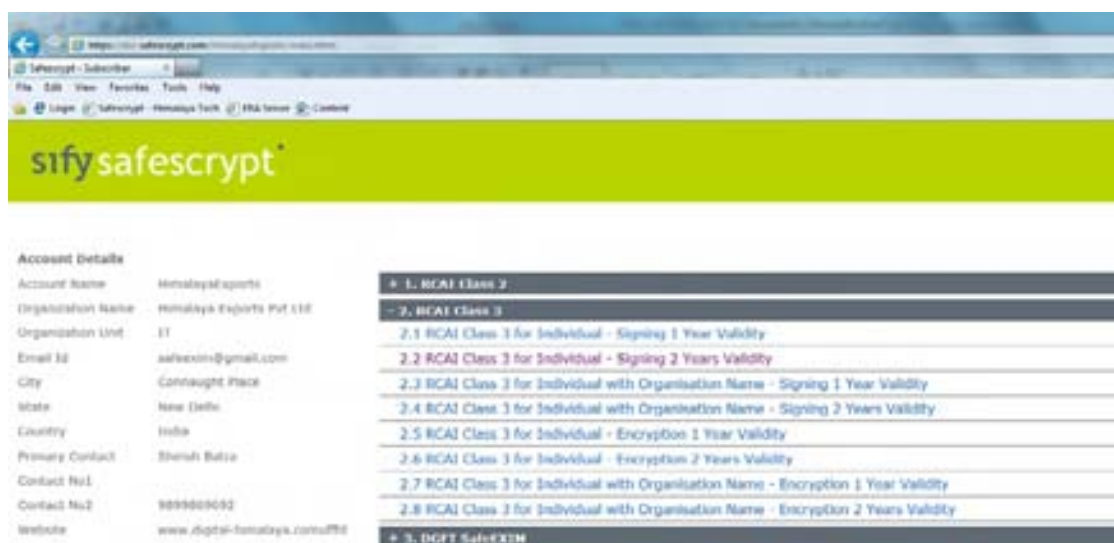


Fig. 1.12: The SifySafescrypt webpage: Selecting the certificate class

Step: 3 Enter registration details as per documents and select CSP as **EnterSafe ePass2003 CSP v1.0** for ePass2003 and click on **Register** button as shown in the figure below:



Fig. 1.13: The Sify Safescrypt webpage: Selecting the CSP

Step: 4 Verify details provided by you shown in the figure below:

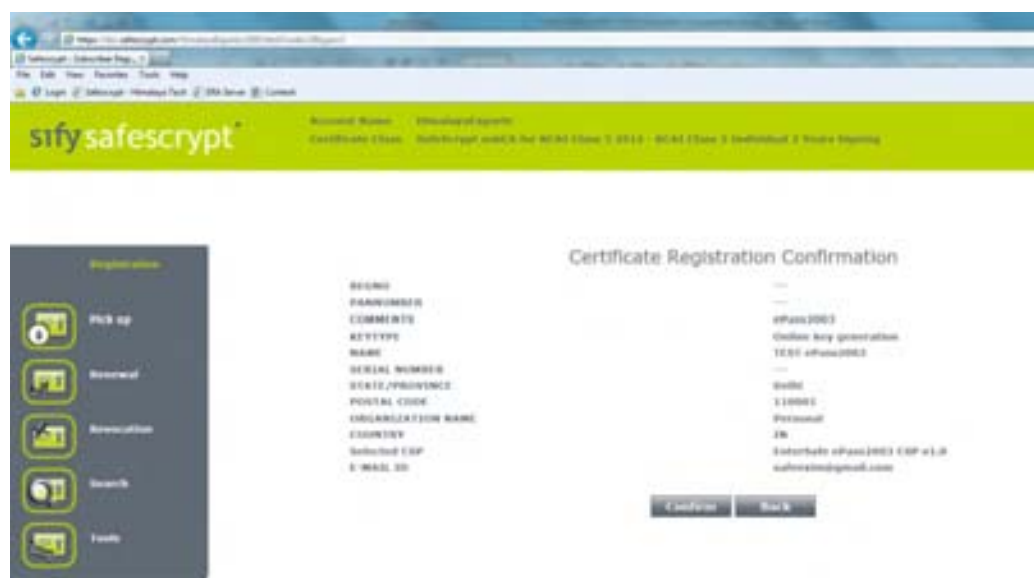


Fig. 1.14: The Sify Safescrypt webpage: Certificate registration confirmation

Step: 5 After confirming the details click on **Confirm** button to enroll the certificate on ePass2003.

Step: 6 The system will prompt for a new password for ePass2003 as shown in the figure below. Type the new PIN and click on **Login** button to proceed further.

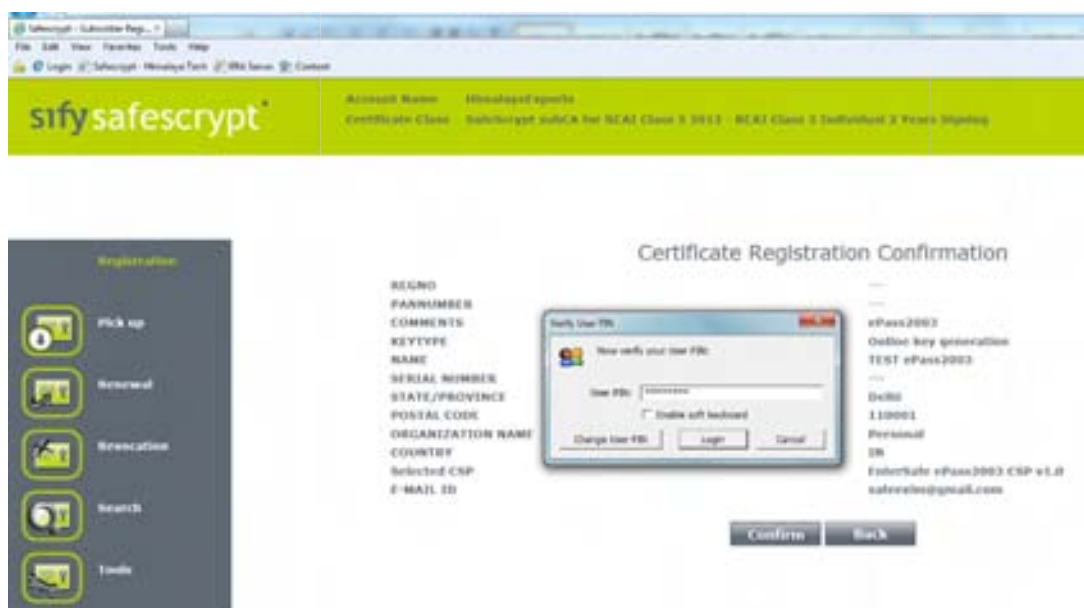


Fig. 1.15: The Sify Safescrypt webpage: Verify User PIN

Step: 7 Click the **Confirm** button and the certificate is enrolled in ePass2003. A message will appear in your screen as shown in the figure below:

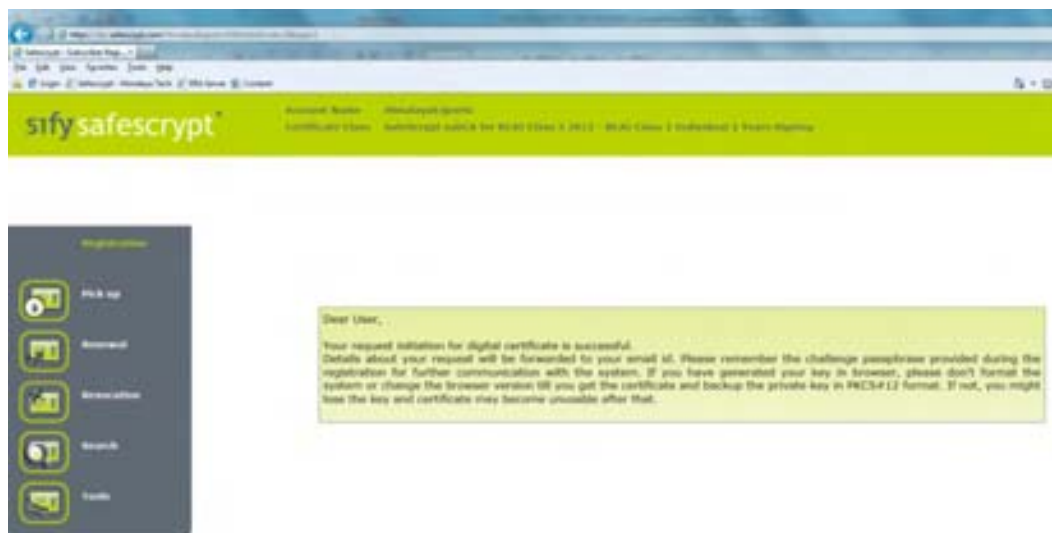


Fig. 1.16: The Sify Safescrypt webpage: Confirmation message

Installing RSA Private Key in the Token

Step: 1 Open the Feitian PKI Manager ePass 2003 as shown below:

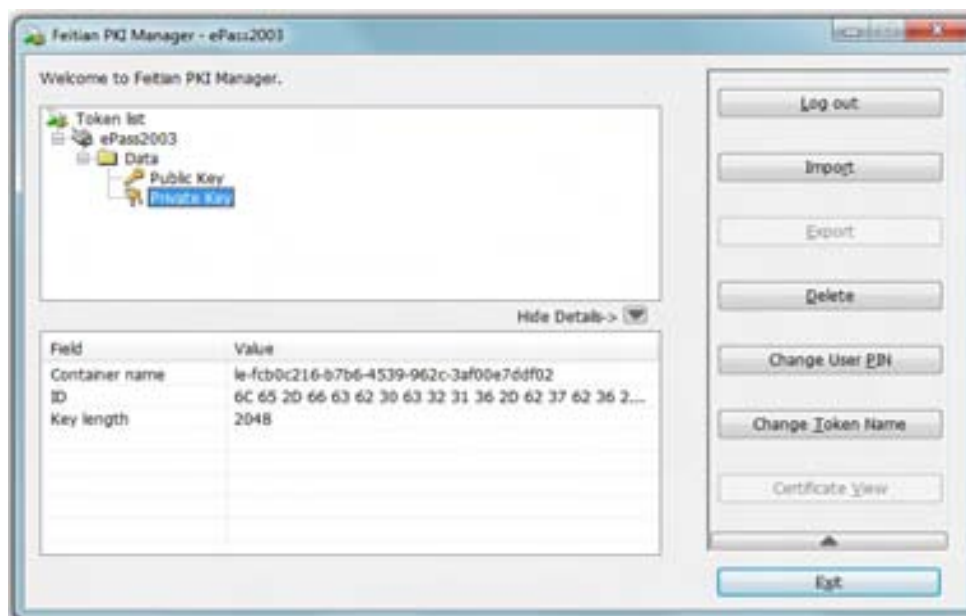


Fig. 1.17: Feitian PKI Manager ePass 2003

Step: 2 Open enrolment link, once the Certificate is issued from the Sify Certifying Authority as shown below:



Fig. 1.18: The SifySafescrypt webpage

Step: 3 Choose the same Class of Certificate as selected while enrolled the certificate as shown in the figure below:



Fig. 1.19: The Sify Safescrypt webpage: Registration details

Step: 4 Click on **Search** on the left frame, type the name in **Common Name** text box and click on **Search** button as shown below:

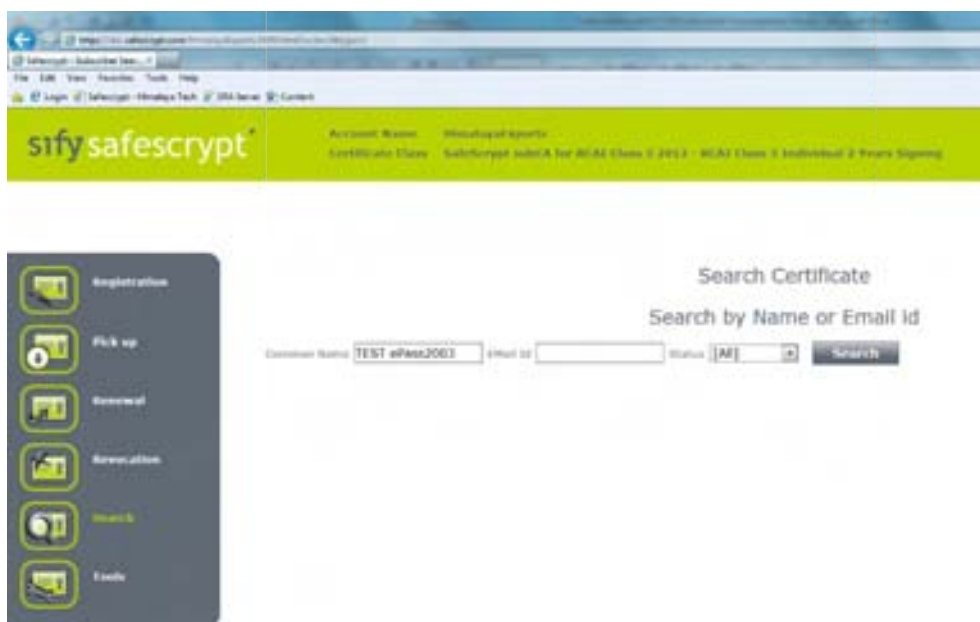


Fig. 1.20: The Sify Safescrypt webpage: Search Certificate option

Step: 5 The search result will appear and insert the Token into the USB Port. Click on **Download** icon in order to download the certificate as shown below:



Fig. 1.21: The Sify Safescrypt webpage: Search results

Step: 6 The system will prompt for PIN. Type the Pin as your password for Token and click on the **Login** button as shown below in order to download the certificate in the Token.

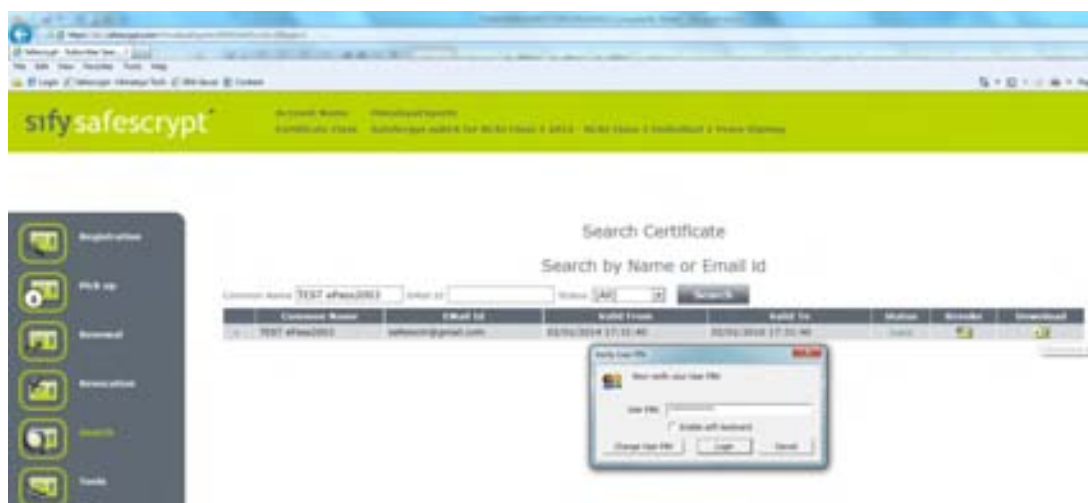


Fig. 1.22: The Sify Safescrypt webpage: Verify User PIN

Step: 7 The system will be prompted with a message that the certificate is successfully installed as shown in the figure below:

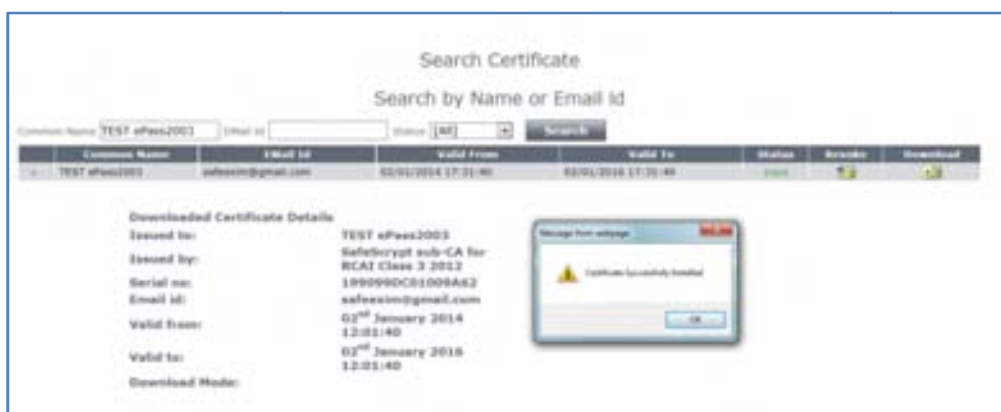


Fig. 1.23: The Sify Safescrypt webpage: Certificate installation message



Fig. 1.24: The Sify Safescrypt webpage: Certificate Details

Step: 8 You can also view the details of the certificate by opening the **Feitian PKI Manager** as shown in the figure below:

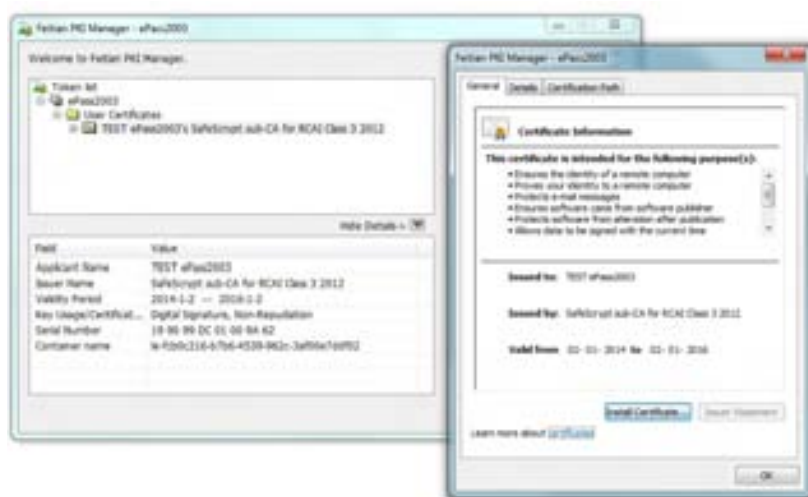


Fig. 1.25: Certificate details from the Feitian PKI Manager ePass 2003

Chapter Summary

- A digital signature is an electronic signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document.
- The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner.



- Digital Signature also ensures that no alterations are made to the data once the document has been digitally signed.
- A DSC is normally valid for 1 or 2 years, after which it can be renewed.
- There are 6 General Classes of Digital Certificate:
 - Class 0: Issue for demonstration/test purpose.
 - Class 1: for individuals, intended for email.
 - Class 2: for organizations, for which proof of identity is required.
 - Class 3: for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority. This class of certificate is used in the e-commerce application wherein high assurance of the certificates is required.
 - Class 4: for online business transactions between companies.
 - Class 5: for private organizations or governmental security.

Exercises

1. What is digital signature?
2. Explain the working of digital signature.
3. What all are the components of a digital signature?
4. Explain the legal validity of digital signatures over IT Act 2000/2008.
5. Explain how to install digital signature in your system.

Guidelines for Usage of Digital Signatures **in e-Governance**

Version 1.0
(December 2010)



Department of Information Technology
Ministry of Communications and Information Technology
Government of India

Contents

1.	INTRODUCTION	4
2.	PURPOSE OF DOCUMENT	4
3.	TARGET AUDIENCE	4
4.	OVERVIEW OF DIGITAL DIGNATURES	5
4.1	DIGITAL SIGNATURES.....	5
4.2	DIGITAL SIGNATURE VERSUS HANDWRITTEN SIGNATURES.....	5
4.3	DIFFERENCE BETWEEN ELECTRONIC SIGNATURES AND DIGITAL SIGNATURES..	6
4.4	OVERVIEW OF HOW DIGITAL SIGNATURES WORK.....	6
4.5	LEGAL VALIDITY OF DIGITAL SIGNATURES	7
5.	PUBLIC KEY INFRASTRUCTURE IN INDIA.....	8
5.1	DIGITAL SIGNATURE CERTIFICATES	10
5.2	CLASSES OF DIGITAL SIGNATURE CERTIFICATES.....	11
5.3	TYPES OF DIGITAL SIGNATURE CERTIFICATES	11
5.4	CERTIFICATE REVOCATION	12
5.5	CERTIFICATE REVOCATION LIST (CRL)	12
5.6	DIGITAL SIGNATURE CERTIFICATE VERIFICATION	12
6.	PROCUREMENT OF DIGITAL SIGNATURE CERTIFICATES	13
6.1	OVERVIEW OF THE PROCESS	13
6.2	PROCEDURE FOR PROCURING DIGITAL SIGNATURE CERTIFICATES.....	14
6.3	MEDIA FOR STORAGE OF DIGITAL SIGNATURE CERTIFICATES	15
6.4	COST	15
6.5	TIME TAKEN.....	16
6.6	PRECAUTIONS WHILE USING DIGITAL SIGNATURE CERTIFICATES.....	16
7.	E-GOVERNANCE APPLICATIONS USING DIGITAL SIGNATURES	16
8.	USAGE SCENARIOS FOR A CITIZEN FOR DIGITAL SIGNATURES	16
8.1	CONTEXT AND OVERVIEW.....	16
8.2	USE CASE SCENARIO FOR APPLICATION FOR A G2C SERVICE.....	16
8.3	USE CASE SCENARIO FOR VERIFICATION OF PRINTED COPY	17
9.	CASE STUDIES OF SUCCESSFUL DIGITAL SIGNATURE IMPLEMENTATIONS	19

9.1	MCA21 APPLICATION	19
9.2	NEMMADI PROJECT IN KARNATAKA	23
9.3	E-DISTRICT APPLICATION OF ASSAM	25
9.4	USAGE OF DIGITAL SIGNATURES IN UP	27
10.	ANNEXURE	30
10.1	ANNEXURE 1 - FREQUENTLY ASKED QUESTIONS	30
10.2	ANNEXURE 2 - DEFINITIONS AND ACRONYMS	37
11.	SOURCES AND REFERENCES	39
12.	LIST OF CONTRIBUTORS	40

1. INTRODUCTION

The vision of National eGovernance Plan (NeGP) of Government of India is to **“make all Government services accessible to the common man in his locality, through Common Service Delivery Outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realise the basic needs of the common man”**. The key objective of this vision is to provide e-services - G2B and G2C - in a ubiquitous manner.

With the implementation of the National eGovernance Plan (NeGP), more and more Departments/Line Ministries in India are automating their operations and business processes and making their Service delivery online. As a result, electronic documentation is slowly permeating every aspect of the business workflow in the Government Departments. However when a signature authorization is required on a document, a hard copy is printed to get a physical routing of signatures. The reintroduction of paper into the workflow increases the Government costs, requires additional time, and prohibits the Government Departments/Line Ministries from realizing the true benefits of a fully electronic workflow.

Digital Signatures provide a viable solution for creating legally enforceable electronic records, closing the gap in going fully paperless by completely eliminating the need to print documents for signing. Digital signatures enable the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones. The purpose of a digital signature is the same as that of a handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptography). Like the pen and paper method, a digital signature attaches the identity of the signer to the document and records a binding commitment to the document. **However, unlike a handwritten signature, it is considered impossible to forge a digital signature the way a written signature might be.** In addition, the digital signature assures that any changes made to the data that has been signed can not go undetected.

2. PURPOSE OF DOCUMENT

This document provides an overview of Digital Signatures, their procurement, authentication mechanism and acceptability in various Governments offices and Courts of Law. The Guidelines also cover case studies of MCA21 application, Nemmadi project in Karnataka, eDistrict application in Assam and Digital Signature Usage in UP. These case studies illustrate how these eGovernance applications have been able to harness the Digital Signatures to deliver G2C services efficiently and with minimum paper work. The Guidelines also have an extensive Frequently Asked Questions (FAQs) section. These Guidelines will serve as a ready reckoner for the State/ Line Ministry officials, Implementing Agencies and citizens.

3. TARGET AUDIENCE

The target audience of this document are the State/ Line Ministry officials, Implementing Agencies and citizens who would like to understand Digital Signatures and how they can be used in various e-Governance applications.

4. OVERVIEW OF DIGITAL DIGNATURES

4.1 Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. **Thus Digital Signatures provide the following three features:-**

Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions (discussed in detail in section 4.4).

Non Repudiation – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

4.2 Digital Signature Versus Handwritten Signatures

A handwritten signature scanned and digitally attached with a document **does not** qualify as a Digital Signature. A Digital Signature is a **combination of 0 & 1s** created using crypto algorithms.

An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Further, paper contracts often have the ink signature block on the last page, allowing previous pages to be replaced after the contract has been signed. Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail. As can be seen in the underlying figure, a Digital Signature is a string of bits appended to a document. The size of a digital signature depends on the Hash function like SHA 1 / SHA2 etc used to create the message digest and the signing key. It is usually a few bytes.

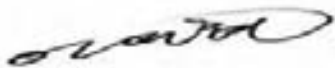
	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 1 3 5 6 8 8 2 1 9 3 1 6 4 8 8 3 7 7 7 5 5 8 3 9 1 9 2 9 3 1 9 3 3 1 9 2 3 9 3 1 9 2 3 1 9 2 3 1 9 4 1 2 5 8 4 1 9 5 1 9 1 3 5 8 3 1 9 4 9 1 3 1 9 5 1 3 1 9 1 9 4 3 4 1 5 1 9 4 5 5 1 3 4 1 9 4 5 1 9 4 4 1 3 1 9 5 2 3 4 1 1 9 1 1 4 1 3 4 1 1 5 1 5 1 1
Problem	Reusable	Impossible to reuse

Figure: Handwritten Versus Digital Signatures

4.3 Difference between Electronic Signatures and Digital signatures

An **electronic signature** means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

4.4 Overview of how Digital Signatures work

The Digital Signatures require a key pair (asymmetric key pairs, mathematically related large numbers) called the **Public** and **Private** Keys. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like crypto smart card or crypto token. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key.

In order to digitally sign an electronic document, the sender uses his/her **Private Key**. In order to verify the digital signature, the recipient uses the sender's **Public Key**.

Let us understand how the Digital Signatures work based on an example. Assume you are going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you had sent and that it is really from you.

1. You copy-and-paste the contract into an e-mail note. Get electronic form of a document (eg : - word or pdf file)
2. Using special software, you obtain a message hash (fixed size bit string) of the contract.
3. You then use your private key to encrypt the hash.
4. The encrypted hash becomes your digital signature of the contract and is appended to the contract.

At the other end, your lawyer receives the message.

1. To make sure the contract is intact and from you, your lawyer generates a hash of the received contract.
2. Your lawyer then uses your public key to decrypt the Digital Signature received with the contract.
3. If the hash generated from the Digital Signature matches the one generated in Step 1, the integrity of the received contract is verified.

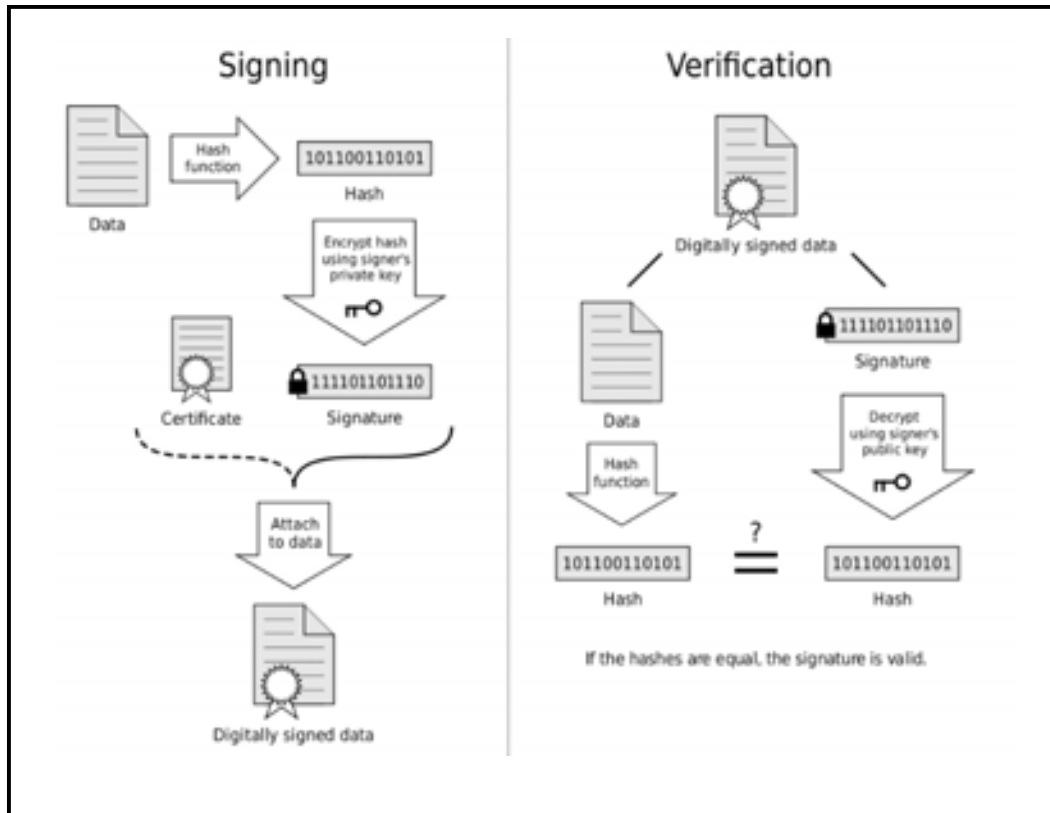


Figure: How Digital Signatures ensure Authenticity, Integrity and Non- Repudiability of the Contract (Source – Wikipedia)

Note: Message digest, also known as the hash of a message, is a small piece of data that results by applying a particular mathematical calculation (hashing function) on the message. Two properties of message digests to note: (i) a small alteration in the original message would cause a big change in the message digest; (ii) derivation of the original message is not possible from the message digest. The hash produced from these functions is a fixed length bit string. For example: - The widely used message digest function SHA -1 generates a 160 bit hash whereas the SHA-2 function generates 256 bit hash as output. The usage of MD5 is to be discontinued by the Certifying Authorities as per the Amendment to the Rules of the IT Act published in 2009. (Link on the CCA website - <http://cca.gov.in/rw/pages/rules.en.do>)

4.5 Legal Validity of Digital Signatures

The Indian Information Technology Act 2000 (<http://www.mit.gov.in/content/information-technology-act>) came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

Section 5 of the Act gives legal recognition to digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.

5. PUBLIC KEY INFRASTRUCTURE IN INDIA

PKI is the acronym for Public Key Infrastructure. The technology is called Public Key cryptography because unlike earlier forms of cryptography it works with a pair of keys one of which is made public and the other is kept secret. One of the two keys may be used to encrypt information which can only be decrypted with the other key. The secret key is usually called the private key. Since anyone may obtain the public key, users may initiate secure communications without having to previously share a secret through some other medium with their correspondent. PKI is thus the underlying system needed to issue keys and certificates and to publish the public information. PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called “digital signatures” to them.

The Office of the Controller of Certifying Authorities (CCA), has been established under the Information Technology (IT) Act 2000 for promoting trust in the electronic environment of India. The current PKI organization structure in India consists of the Controller of Certifying Authority as the apex body and as the Root Certifying Authority of India (RCAI)(as shown in the figure on PKI Hierarchy). The CCA is entrusted with the following responsibilities : -

- ❖ Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- ❖ Controller of Certifying Authorities as the “Root” Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates
- ❖ Certifying the public keys of the CAs, as Public Key Certificates (PKCs).
- ❖ Laying down the standards to be maintained by the CAs.
- ❖ Conflict resolution between the CAs
- ❖ Addressing the issues related to the licensing process including:
 - a) Approving the Certification Practice Statement (CPS);
 - b) Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.

The **RCAI** is responsible for issuing Public Key Certificates to Licensed Certifying Authorities (henceforth referred to as Certifying Authorities or CA). The CAs in turn are responsible for issuing Digital Signature Certificates to the end users. In order to facilitate greater flexibility to Certifying Authorities, the CCA has allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet its business branding requirement. However the sub-CA will be part of the same legal entity as the CA.

The sub-CA model will be based on the following principles:

- ❖ The CAs must not have more than one level of sub-CA
- ❖ A sub-CA certificate issued by the CA is used for issuing end entity certificates
- ❖ A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. The only exception will be for code signing and time stamping certificates, which may directly be issued by the CA.

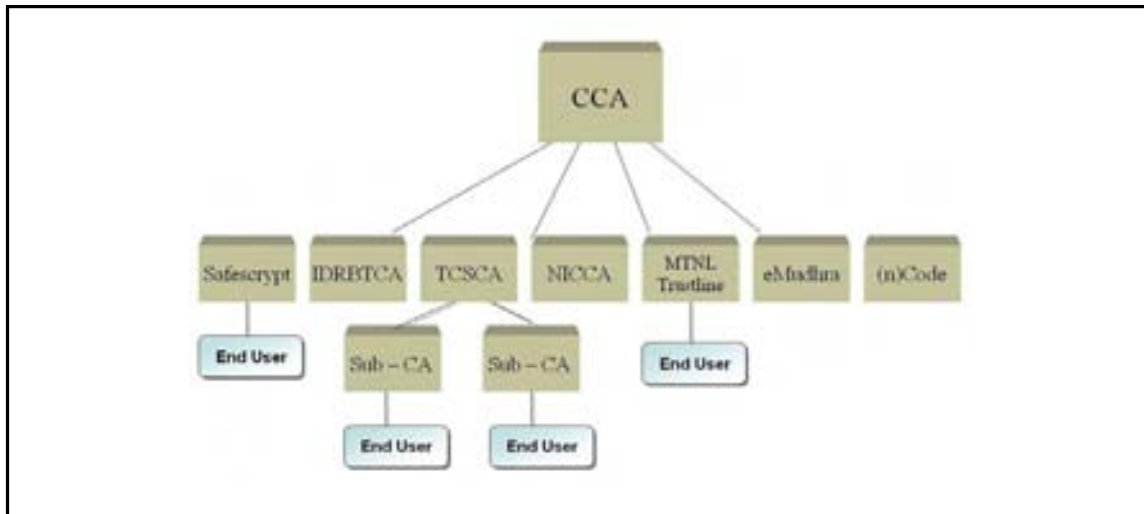


Figure: Overview of PKI Hierarchy in India

A **Registration Authority (RA)** acts as the verifier for the Certifying Authority before a Digital Signature Certificate is issued to a requestor. The Registration Authorities (RAs) process user requests, confirm their identities, and induct them into the user database.

The PKI structure (outlined in the Figure below) in India is the foundation for secure Internet applications which ensure authentic and private transactions that cannot be repudiated at a later time. Thus the CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates as the **Root Certifying Authority of India (RCAI)**. CCA is the Root of the trust chain in India.

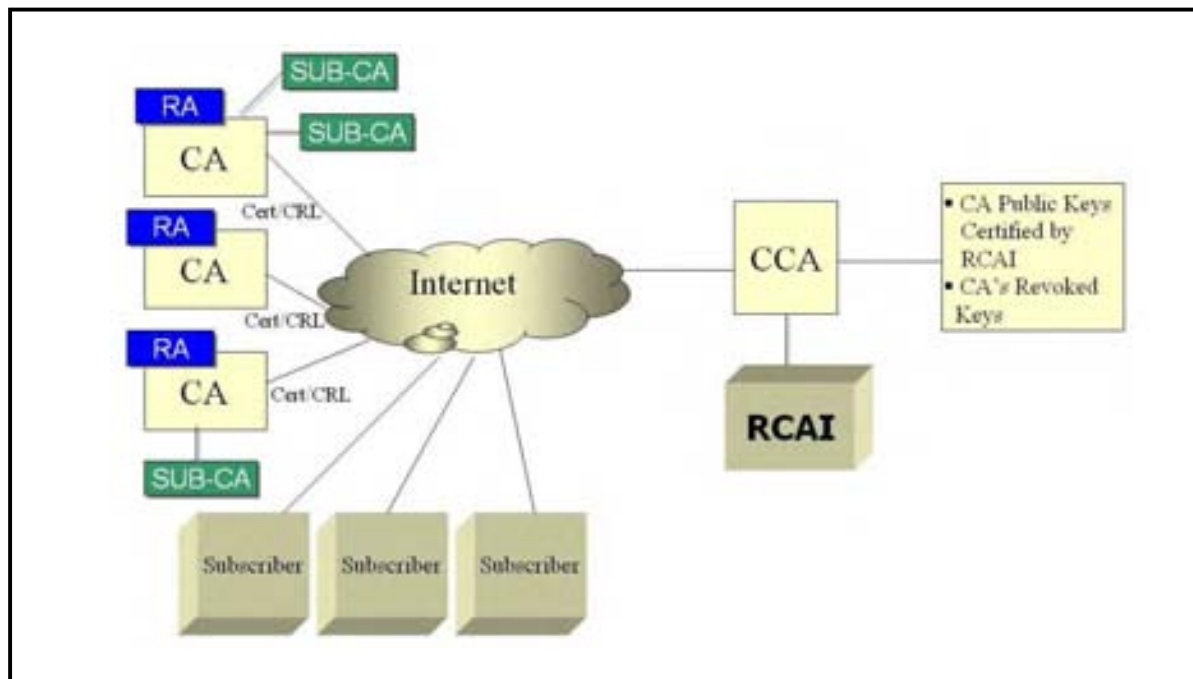


Figure: Overview of CCA Implementation of PKI as per the IT Act

In order to ensure interoperability between the Digital Signature Certificates issued by different CAs' in India, the CCA has come out with the **"Interoperability Guidelines for Digital Signature Certificates issued under the Information Technology Act"** (<http://cca.gov.in/rw/pages/index.en.do>). With these guidelines in place, the Digital Signature Certificate issued by one CA can be used across various e-Governance applications as the Interoperability guidelines have prescribed the formats, field and other aspects that will ensure interoperability. To know more about CCA kindly visit their website <http://cca.gov.in/>.

5.1 Digital Signature Certificates

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet.

A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to the individual. Digital certificates are the digital equivalent (i.e. electronic format) of physical or paper certificates. Examples of physical certificates are driver's licenses, passports or membership cards.

Digital Signature Certificates are endorsed by a trusted authority empowered by law to issue them, known as the Certifying Authority or CA. The CA is responsible for vetting all applications for Digital Signature Certificates, and once satisfied, generates a Digital Certificate by digitally signing the Public key of the individual along with other information using its own Private key.

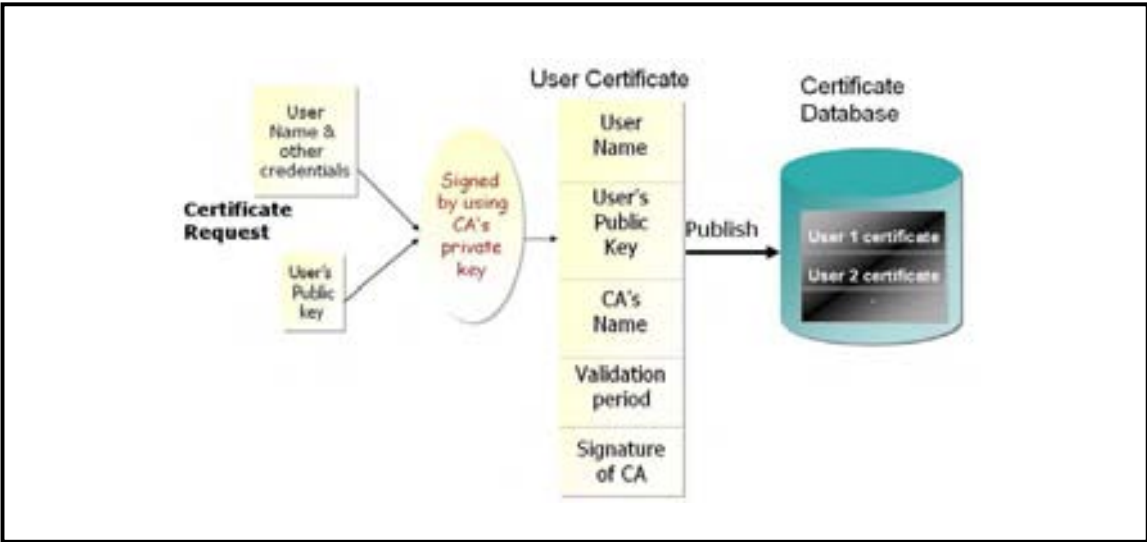


Figure: Overview of Digital Signature Certificate

5.2 Classes of Digital Signature Certificates

Depending upon the requirement of assurance level and usage of DSC the following are the classes of Digital Signature Certificates

Class of DSC	Assurance Level	Applicability
Class 1	Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level users are not likely to be malicious.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
Class 3	These certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

5.3 Types of Digital Signature Certificates

The following table provides an overview of the different types of Digital Signature Certificates.

Type of Certificate	Description
Individual Digital Signature Certificates (Signing Certificates)	Individual Certificates serve to identify a person. It follows that the contents of this type of certificate include the full name and personal particulars of an individual. These certificates can be used for signing electronic documents and emails and implementing enhanced access control mechanisms for sensitive or valuable information.
Server Certificates	Server Certificates identify a server (computer). Hence, instead of a name of a person, server certificates contain the host name e.g. " https://nsdq.gov.in/ " or the IP address. Server certificates are used for

	1 way or 2 way SSL to ensure secure communication of data over the network.
Encryption Certificates	Encryption Certificates are used to encrypt the message. The Encryption Certificates use the Public Key of the recipient to encrypt the data so as to ensure data confidentiality during transmission of the message. Separate certificates for signatures and for encryption are available from different CAs.

5.4 Certificate Revocation

Digital Signature Certificates are issued with a planned lifetime, which is defined through a validity start date and an explicit expiration date. A certificate may be issued with a validity of upto two years. Once issued, a Certificate is valid until its expiration date.

However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name (for example, change the subject of a certificate due to an employee's change of name), change of association between subject and CA (for example, when an employee terminates employment with an organization), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to revoke the certificate.

In case a Digital Signature Certificate is compromised, one should immediately contact the respective CA to initiate revocation. The CA will then put the certificate in the Certificate Revocation List. We need to have necessary processes in place defining the roles and responsibility of various government officials for the usage of Digital Signature and their revocation.

5.5 Certificate Revocation List (CRL)

A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point. The CRL has a limited validity period, and updated versions of the CRL are published when the previous CRL's validity period expires. Before relying on a signature the CRL should also be checked to ensure that the corresponding DSC has not been revoked.

5.6 Digital Signature Certificate Verification

Digital Signature Certificates are verified using a Chain of trust. The trust anchor for the Digital Certificate is the Root Certifying Authority (CCA in India). A root certificate is the top-most certificate of the hierarchy, the private key of which is used to "sign" other certificates. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. Certificates further down the tree also depend on the trustworthiness of the intermediates (often known as "subordinate certification authorities").

The Digital Certificate verification process is a recursive process in which the program verifying the end user certificate verifies the validity of the certificate of the issuing authority until it finds a valid certificate of a trusted party. On successful verification of the trusted party Certificate, the Digital Certificate verification stops. In case a trusted party Certificate is not found by the program, the Digital Certificate verification process ends in failure.

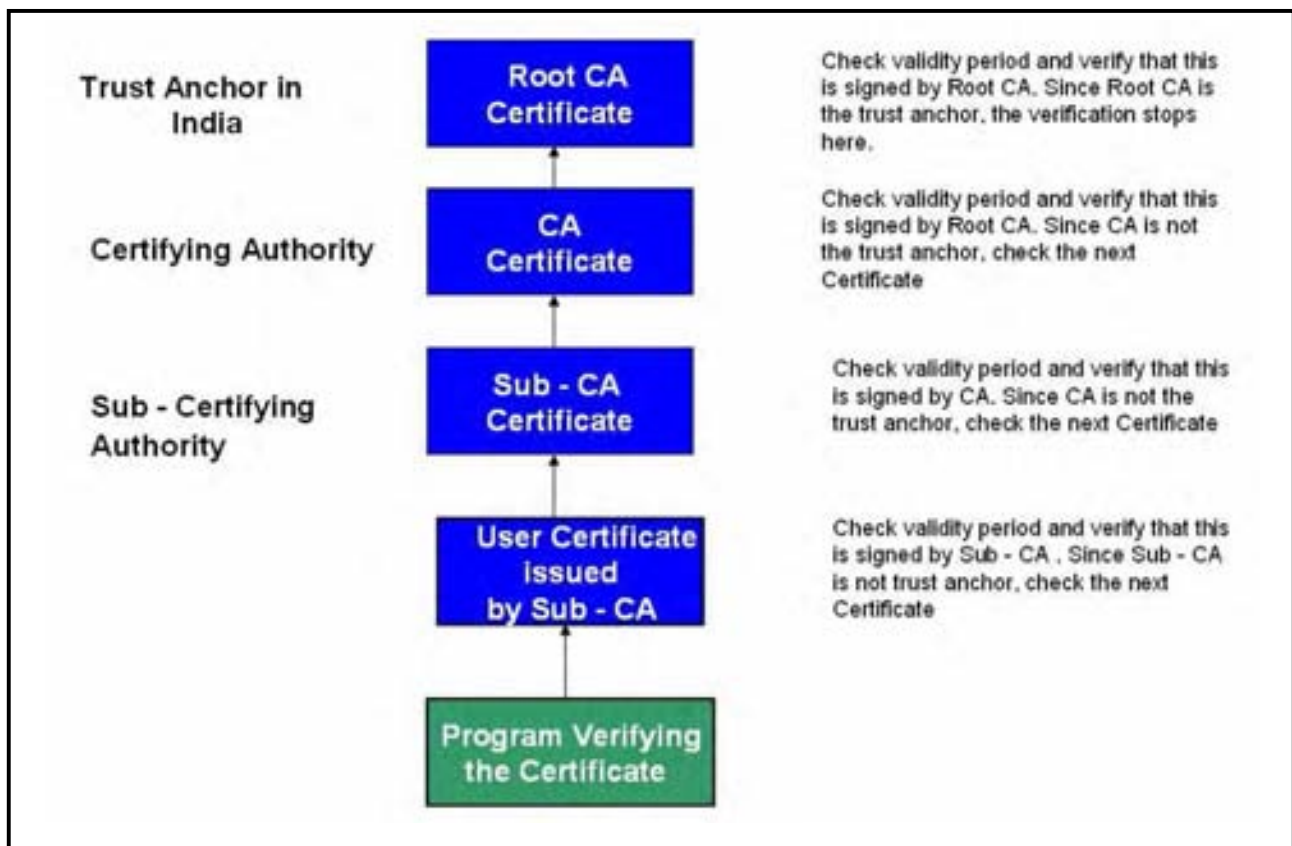


Figure: Overview of Root Chain Verification process for Digital Certificates

The e-Governance applications should also undertake Root chain verification and CRL verification in addition to the Public Key verification while doing the Digital Signature verification.

6. PROCUREMENT OF DIGITAL SIGNATURE CERTIFICATES

6.1 Overview of the Process

The applicant for the Certificate must generate his/her own key pair and send the public key to the CA with some proof of his/her identity.

The CA will issue a Digital Signature Certificate containing the public key. The CA will digitally sign the certificate using its private key and then send the certificate to the applicant. The CA will check the applicant's identification before it generates the certificate and signs the request. Different Certifying Authorities may issue certificates with varying levels of identification requirements. One CA may insist on seeing the Identity card while another may want a signed letter authorizing certification from anyone requesting a certificate.

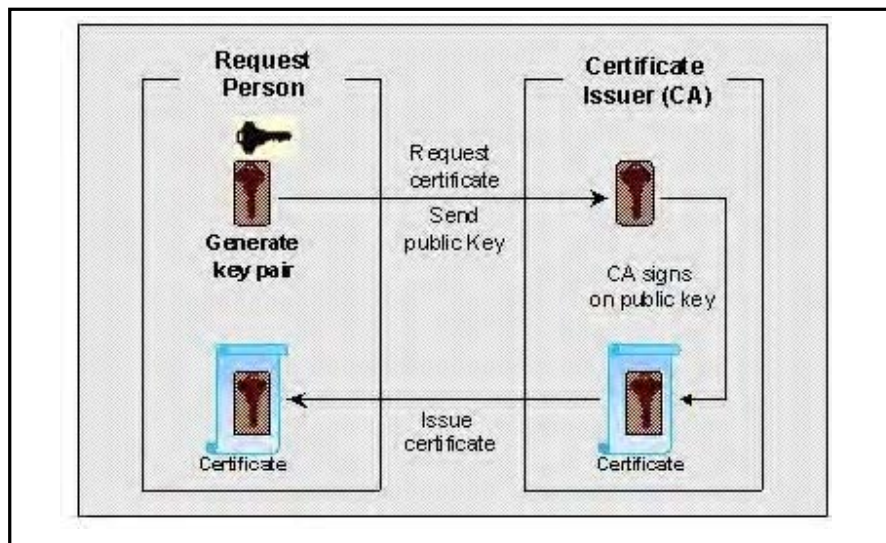


Figure: Certificate Request and Issuance process by a CA (Source NIC-CA)

6.2 Procedure for procuring Digital Signature Certificates

The CCA has licensed seven Certifying Authorities in India to issue Digital Signature Certificates to the end users. The National Informatics Centre issues Digital Signature Certificates primarily to the Government/ PSU's and Statutory bodies. The Institute for Development of Research in Banking Technology (IDRBT) issues Digital Signature Certificates primarily to the banking and financial sector in India. The remaining five CAs - Safescrypt, TCS, MTNL, n(Code) Solutions and eMudhra issue Digital Signature Certificates to all end users across all domains. More than **16 lakh** Digital Signature Certificates have been issued by the different CA's in our country at the time of publication of this document.

6.2.1 Steps for Getting an individual Digital Signature Certificate

- ❖ DSC Form **can be downloaded** from website of the CA
- ❖ For **Class 3 certificate**, the applicant has to submit the **completed forms in person** at the RA
- ❖ On successful processing by the RA, the **Username and password** are sent to applicant mailbox in order for him/her to log onto CA website. The **cryptographic device** is handed over to the user for storing the private key.
- ❖ The **applicant installs the device drivers** for the device (for storing the private key) from CA website. For example:- crypto token, smart card reader
- ❖ User **generates the key pair** and uploads his **Certificate Signing Request (CSR)** request into his/her account on the CA Website
- ❖ CA **generates the DSC** after verification. The user downloads from his/her account on the CA website.

6.2.2 Steps for getting a Web server Digital Signature Certificate

- ❖ **Fill in the application form** for issuance of an SSL certificate and submit the same to your CA along with applicable fee.
- ❖ **Generate a CSR** from the Web Server. Kindly note that the tool used for generating the CSR will generate a keystore and save the private key for the CSR on the key store. The key store will have login-id and password which will be required to import the signed public key later. Note: The details filled for generation of CSR should be the same as filled in the form submitted to the CA.
- ❖ CA will provide a method to **Upload /Submit the CSR**. Upload/Submit the CSR to the CA.
- ❖ On successful processing of the CSR request the CA will generate the SSL Certificate. The same needs to be **downloaded** from the location specified by the CA in an email.

- ❖ After downloading the SSL Certificate, the **Certificate needs to be imported back** into the key store using the same tool. Once imported successfully the same is ready for use now.

6.3 Media for Storage of Digital Signature Certificates

It is recommended to store the private key on secure medium, for example, smart cards/ crypto tokens etc. The crypto token connects to the user computer through the USB interface. For smart cards a compatible smartcard reader needs to be installed on the user computer if not already present. The secure media available for the storing the private key may vary per each Certifying Authority.

6.4 Cost

The cost of the Digital Signature Certificate varies from CA to CA. The Certificates are typically issued with one year to two year validity. These are renewable on expiry of the period of initial issue. Further additional fees for renewal may also be charged. The costs involved in procuring Digital Certificates from NIC- CA are attached as a sample. The costs for the other CAs' can be found on their respective websites.

NIC- CA Certificate Fee Structure (For all classes : Class 1, Class 2 and Class 3)									
Type of Subscriber	Smart Card Individual/ Personal Certificate				USB Token/iKey Individual/Personal Certificate			Soft Token SSL Server/Dev ice Cert. (Proc. Charge)	Renewal (Proc. Charges)
	Smart Card	Smart Card + Reader	Proc. Charge	Total	USB Token	Proc Charge	Total		
Government	227/-	489/-	-	716 /-	555/-	-	555/-		
PSUs & Autonomous / Statutory Bodies	227/-	489/-	200/-	916/-	555/-	200/-	755/-	200/-	200/-
Validity	Two years (Conditions apply)								
Renewal	On expiry of certificate, processing charge shall be applicable as above to renew/create the certificate on the same media. All other formalities shall be same as for a new DSC applicant, including submission of fresh DSC Application form and fees applicable.								
Mode of Payment (Demand Draft/RBI Cheque)									
i) DSC form submitted to NICCA RA Office, Delhi/Chandigarh/Hyderabad: DD in favour of "Accounts Officer, NIC Delhi" payable at New Delhi									
ii) DSC form submitted to NICCA RA Office, Lucknow: DD in favour of "DDO, NIC UP State Centre" payable at Lucknow									
iii) DSC form submitted to NICCA RA Office, Bangalore: DD in favour of "DDO, NIC Karnataka State Centre" payable at Bangalore									
iv) DSC form submitted to NICCA RA Office, Chennai: DD in favour of "DDO, NIC Tamilnadu State Centre" payable at Chennai									
v) DSC form submitted to NICCA RA Office, Bhubaneshwar: DD in favour of "DDO, NIC Orissa State Centre" payable at Bhubaneshwar									
vi) DSC form submitted to NICCA RA Office, Guwahati: DD in favour of "DDO, NIC Assam State Centre" payable at Guwahati									
vii) DSC form submitted to NICCA RA Office, Raipur: DD in favour of "DDO, NIC Chhattisgarh State Centre" payable at Raipur									

Kindly also cross check from the NIC-CA website (<http://nicca.nic.in>) for any further updates.

6.5 Time Taken

The time taken by the Certifying Authorities to issue a DSC may vary from three to ten days.

6.6 Precautions while using Digital Signature Certificates

Digital Signatures are legally admissible in the Court of Law, as provided under the provisions of IT Act 2000. Therefore users should ensure that the Private keys are not disclosed to anyone. For example:- Users generally give their crypto tokens to their personal secretaries or subordinates to sign the documents on their behalf. Any illegal electronic transaction undertaken using a person's private key cannot be repudiated by the certificate owner and will be punishable in the Court of Law.

7. e-GOVERNANCE APPLICATIONS USING DIGITAL SIGNATURES

The following are some of the eGovernance applications already using the Digital Signatures:-

- MCA21 – a Mission Mode project under NeGP which is one of the first few e-Governance projects under NeGP to successfully implement Digital Signatures in their project.
- Income Tax e-filing
- IRCTC
- DGFT
- RBI Applications (SFMS)
- NSDG
- eProcurement
- eOffice
- eDistrict applications of UP, Assam etc

8. USAGE SCENARIOS FOR A CITIZEN FOR DIGITAL SIGNATURES

8.1 Context and Overview

A citizen would like to avail various G2C services available at the Common Service Centres(CSC). The following section details the various use case scenarios for a citizen to avail these G2C services.

Please note for the following Use Case scenarios we assume that the digitally signed document that has to be verified is an Income Certificate.

8.2 Use Case Scenario for application for a G2C service

In order to avail a G2C service the user would have to undertake the following steps : -

1. The citizen will visit the nearest Common Service Centre.
2. The citizen will put in the application request for the Income Certificate online at the CSC. He will also submit all the necessary documentary proofs at the CSC. This request will be forwarded to the backend Departmental application.
3. The Department will process the request and after successful verification, the authorized Government Officer will issue the Income Certificate by digitally signing it. The same will be stored in the repository of the Departmental application.

4. The citizen revisits the CSC to check the status of the application request. In case the application request has been completed, the CSC operator will be able to show the citizen the Income Certificate from the application repository. In case the Department wishes, they can provide the citizen with a printed copy of the electronic document to furnish for future use.

8.3 Use Case Scenario for Verification of printed copy

In order to avail the various services and benefits, the citizen will have to show the printed copy of the Income Certificates to various Departments. In order to verify the printed copy of the Income Certificate, the verifier (Department Officer to whom the citizen furnishes the document for availing a service) has the following three options

1) Via Request ID

1.1 The verifier can go to the Department website and search by the Unique Request ID printed on the Income Certificate.

1.2 The electronic version of the Income Certificate will be displayed on the website to the verifier.

1.3 The verifier can compare fields of the Income Certificate displayed in the website with the hardcopy presented by the citizen and thereby verify the authenticity of the document.

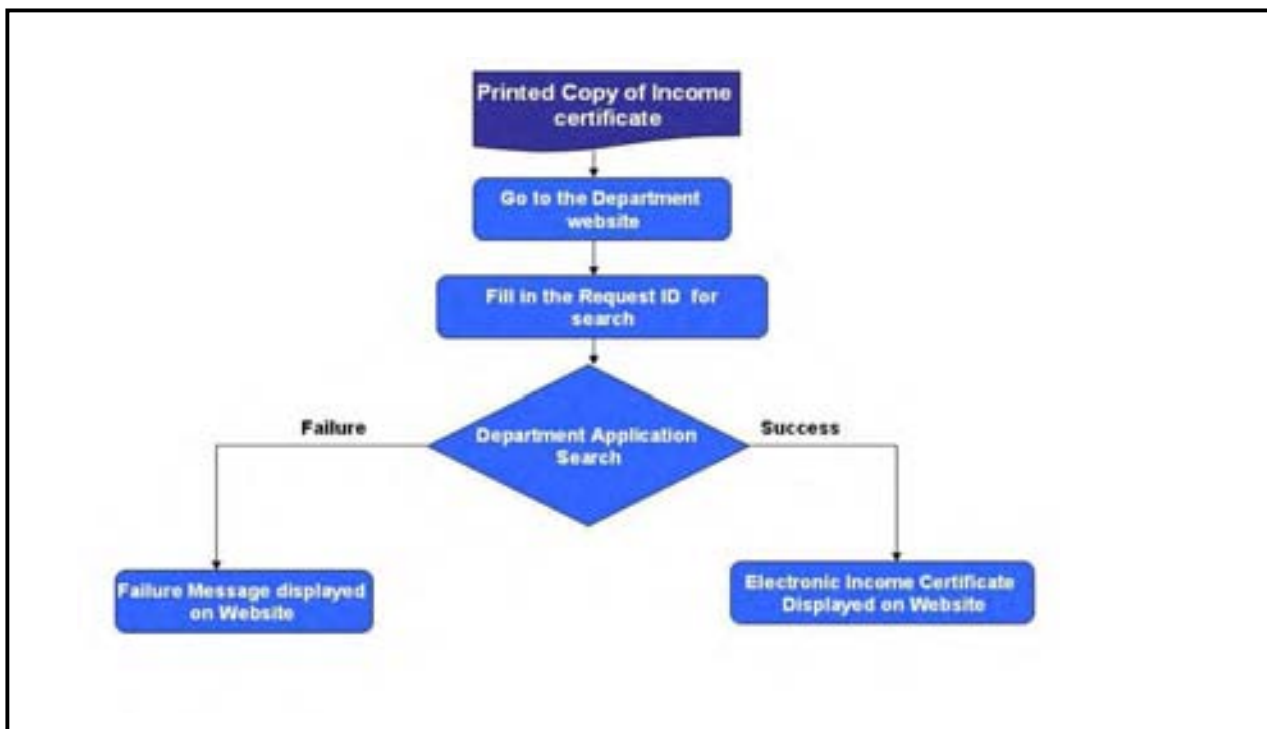


Figure: Verification of Income Certificate by Request ID

2) Via 2D Barcode

The Income Certificate can have a 2D barcode in which the digital signature is embedded. In case a 2D barcode is present on the Income Certificate, the verifier has the following two options to verify the printed copy of the Income Certificate

2.1 Online Verification

The verifier will be required to have an Internet Connection and a 2D barcode reader for this option.

1) The citizen will scan the 2D barcode from the printed copy of the Income Certificate

- 2) The output from the scanner will be fed to the verification utility of the Department (can be downloaded from the Department website)
- 3) The verification utility of the departmental application will verify the digital signature embedded in the barcode with the one stored in the database.
- 4) In case the signatures match, the verification utility will display the electronic version of the Income Certificate on the Department website.
- 5) The verifier can verify the contents of the Income Certificate with that of the Income Certificate displayed on the website.

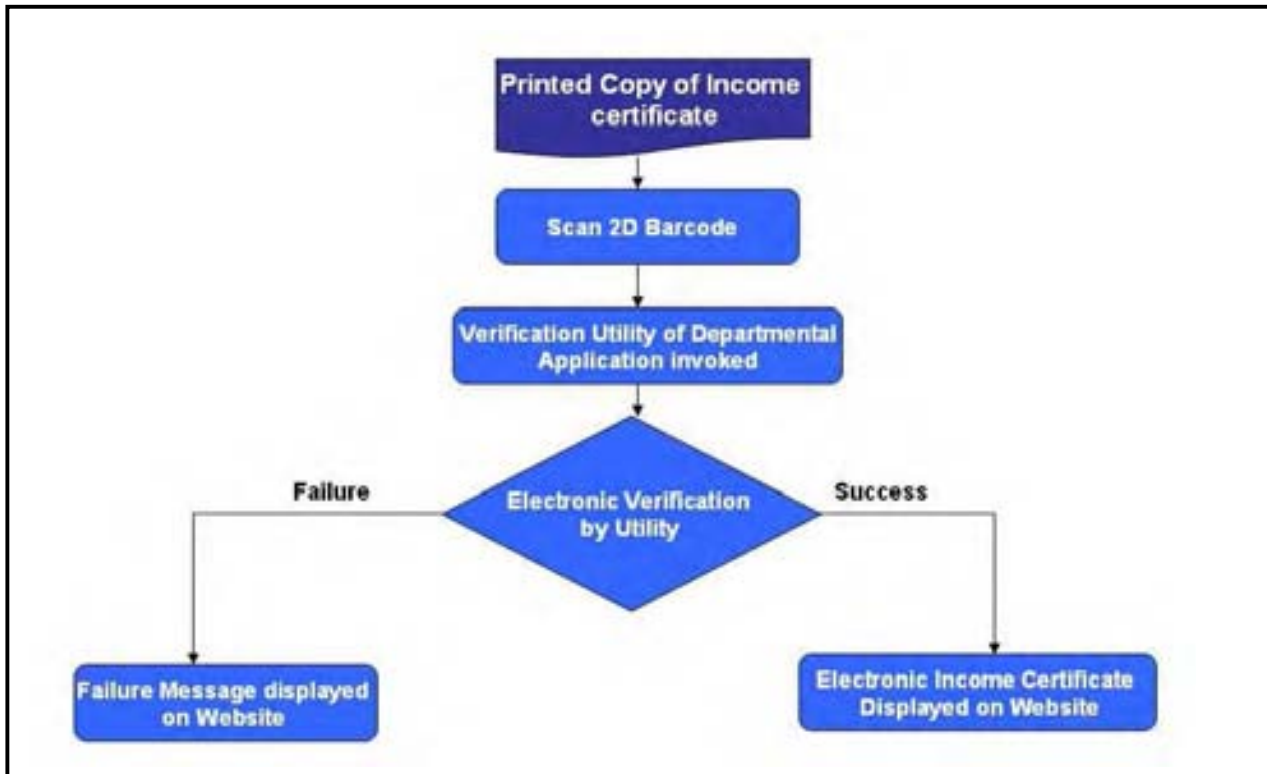


Figure: Online Verification of Income Certificate by citizen

2.2 Offline Verification

The citizen will be required to have a Computer, a 2D barcode reader, Public Key of the Taluka official who signed the Income Certificate, Root Chain Certificate of the CCA and NIC-CA and the verification utility of the departmental application. No connection to internet will be required.

In case the verifier does not have the above softwares installed on the computer, he can follow the underlying steps to install the softwares, This is a one time activity.

- 1) The verifier will download the root chain certificates of CCA from the CCA website (http://cca.gov.in/rw/pages/rcai_root_certificate.en.do) and NIC-CA certificate from the NIC-CA website (<http://nicca.nic.in/index.jsp>).
- 2) The public key of the taluka official can be downloaded from the NIC-CA website by searching for the name of the Taluka official on the website.
- 3) The verifier will install the verification utility of the departmental application by downloading it from the respective department website.

The verifier will have to undertake the following steps to verify the printed copy of the Income Certificate

- 1) The verifier will open the verification utility.
- 2) The verifier will use a barcode reader to scan the 2D barcode from the printed copy of the Income Certificate.
- 3) The verification utility will verify the digital signature scanned from the document.
- 4) The verification utility will accordingly display the appropriate message to the verifier.

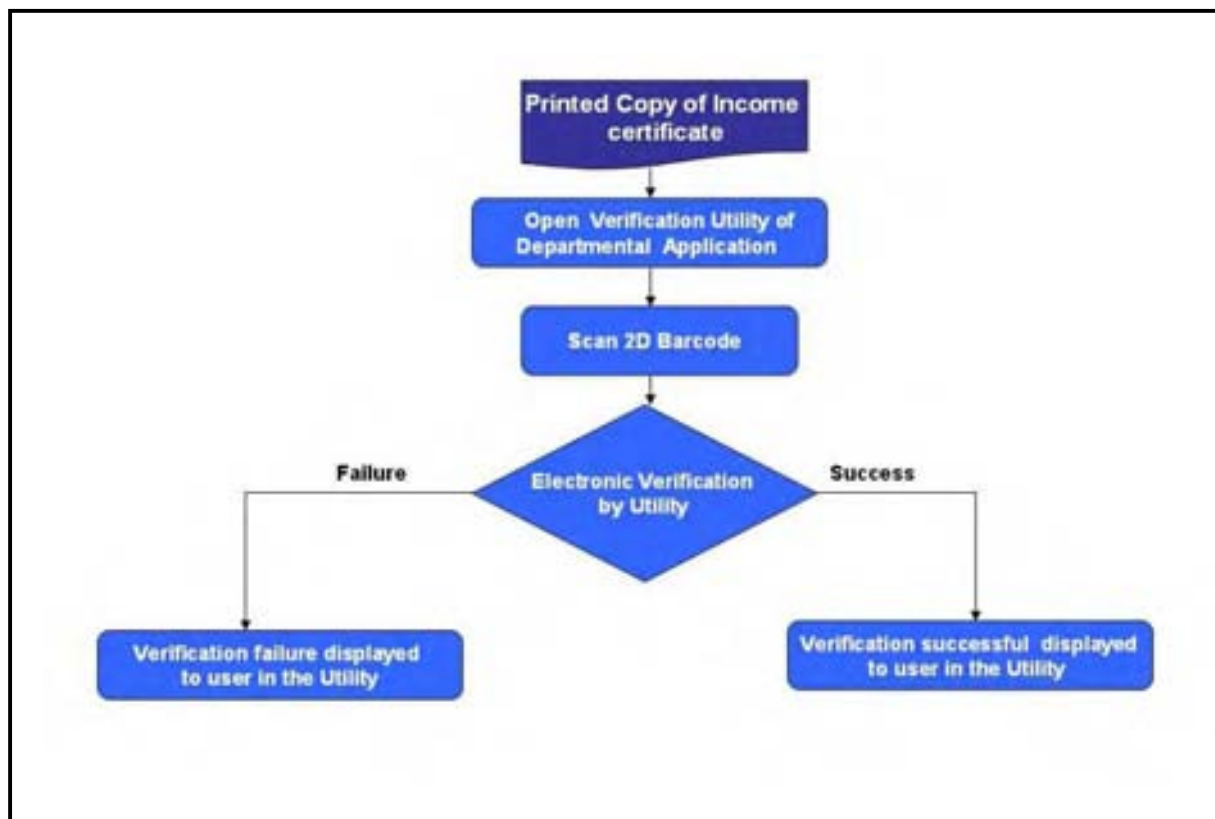


Figure: Offline Verification of Income Certificate by citizen

9. CASE STUDIES OF SUCCESSFUL DIGITAL SIGNATURE IMPLEMENTATIONS

9.1 MCA21 Application

9.1.1 Context and Overview

The Ministry of Company Affairs has undertaken implementation of MCA21 project-an e-Governance initiative that will provide all the Ministry related services online to the businesses through electronic mode. It is a significant step towards an end-to-end paperless delivery of the Government Services. The use of eForms along with Digital Signatures using Digital Signature Certificates (DSCs or just “certificates”) is critical and integral to achieve this goal.

Following are the usage of DSC in MCA21 solution:

a) **Signing of eForms and Documents:** DSC has been used in eForms to ensure the Signatory authentication and data authentication. The eForms and documents shall be digitally signed during submission of requests by the users (Directors, Professionals). Whenever a request for a service is approved and the workflow is completed, the approving officer of the Ministry of Company Affairs (MCA) digitally sign the eform as a proof of having approved the request for delivery of Service.

b) **Role Check:** The MCA21 application requires that the digital signature on the eforms and other documents is done by authorized person. This was difficult to achieve as the DSC issued in India is on Individual category and does not contain any attribute which defines the role. This also brings in the advantage that same DSC can be used by any individual for multiple roles with multiple applications. The role check in MCA21 is achieved through database check.

The Directors and professionals are required to register their DSC with MCA21 portal against their Director Identification Number (DIN) and/or PAN (for professional). Database of professionals has been taken from the professional bodies i.e ICAI, ICSI & ICWA and included within MCA21. The professional users database is updated on regular basis. The DIN database is part of MCA21. Once the DSC is registered a mapping of DSC with DIN and/or PAN is maintained within the MCA21. However, a director or a professional may be linked to multiple companies. Hence, only one DSC is required per individual irrespective of roles he performs and companies with which he is associated.

c) **Secure Login:** MCA Employees, Directors and professionals shall login to the MCA portal using DSC instead of a password. DSC based solution provides a much secure way of login over normal user id / password method. MCA21 system does not permit password based login for its users.

9.1.2 Users of MCA21

For MCA21, five types of users are identified:

1. MCA (government) employees
2. Professionals (Chartered Accountants, Company Secretaries, and others) who interact with MCA & Businesses in the context of the Companies Act.
3. Representatives of Banks & Financial Institutions
4. Authorized Signatories and Directors of Companies
5. Citizens /public user

Each of these users provide specific and different sets of information to the MCA21 applications at the various times – to identify themselves before accessing certain information, performing certain operations, and signing documents they are authorized to sign.

The different category of users as identified above are required to use the digital signatures in discharge of their duties mentioned below:-

i) MCA employees (Government):

Various services required to be delivered by the offices of Registrar of Companies(ROC) under the Ministry of Company Affairs have been re-engineered into e-forms. As such, any client (company/ corporate) seeking to avail of any service would be required to apply for the same in the prescribed e-form. Such e-form would be submitted by the client and processed in the Back Office of each ROC for an appropriate decision thereon. Such decision as a result of processing of the clients' request in the Back Office would be digitally signed in recognition of the approval/

rejection of such request. Thus, the employees of the MCA posted in various ROC offices will be using the DSCs to digitally sign the decision taken by them on various requests. This would constitute one class/ category of users in the MCA21 system.

ii) Professionals:

Professionals are authorised to submit various requests through the prescribed e-forms on behalf of the clients with MCA (companies/ corporates). These professionals, working for their clients under due authorisation, submit various requests/ carry out various statutory compliances on behalf of their clients. As such, they are required to obtain Digital Signature Certificates and use the same for submission of various e-forms on behalf of the companies/ corporate and constitute the second category of users for the purpose of issuance of DSCs.

iii) Directors/ Authorised Signatories:

This class of persons represents the Directors of the companies/ corporates and includes Signatories duly authorised by the companies through Resolutions as permissible under the Company Law. A number of documents required to be filed by the companies in the offices of ROCs, now to be facilitated through e-forms, have to bear the signatures of this class of persons. Hence, they would constitute the third category of the users of DSCs before submission of their filings under the MCA21 system.

iv) Representatives of Banks and Financial Institutions:

Companies/ corporates avail of term loan/ loan against working capital and various other kinds of loans from Banks and Financial Institutions and create a charge of the Financial Institution or the Bank in the process. The document creating a charge or modification thereof at a subsequent stage, is required to be registered with the Registrar of Companies. This service is also to be provided through e-form. The charge creation document bears the signature of the lender as well as the borrower. The FIs/ Banks, being the lenders in this process, would be required to use DSCs under the MCA21 as a token of creation of such charge and the authorised signatory/ Director on behalf of the borrowing company (covered under third category/ class of DSC users) would append their signatures digitally on the e-form before submission thereof to the ROC for registration of this document. Thus, the Banks/ FIs represent the fourth category/ class of DSC users.

v) Citizens/Public user:

Citizens only perform activity of viewing various documents filed by companies as per the Company Act. These users are not required to use DSC as they only perform view operation.

9.1.3 Class of Digital Signature Certificates

Keeping in view of the trust level required and usage model it was decided that all Class 2 or above DSCs will be permitted in MCA21 application.

1. MCA Employee

The application form for the Govt. employees will be followed as notified earlier by Department of Information Technology by Gazette notification dated 23rd April, 2004 (GSR 284(E)). For MCA employee, the Ministry is functioning as Subordinate CA or sub-CA under one of the authorized CA. For this purpose, officer have been assigned the duty of RA and sub-CA for issuance and revocation of the certificate. All MCA employee are issued certificates under the MCA sub-CA and the application only permits certificate under this sub-ca chain to perform duties associated with MCA employees. There are approximately 1000 certificates used under the sub-CA.

2. For Professionals, Directors, Authorised signatories and other category user

Directors/authorized signatories and professionals have to procure "Individual" category DSC from any one of the licensed CA. The DSC issued by the CA should be in accordance with FORM B prescribed by the Department of Information Technology under the Gazette notification dated 23rd April 2004 (GSR 285(E)). A person performing multiple roles of professional, director and authorized signatory for different companies need to procure only one DSC but they are required to register the DSC for each role performed in MCA21 system. The numbers of certificates used are growing every day and have already crossed 5 lakh mark.

9.1.4 Registration Procedure of DSC for Professionals and Directors

Directors/authorized signatories and professionals are required to self register at MCA21 portal. It is mandatory for them to procure DSC before registering. Following steps needs to be performed by the Directors/authorized signatories and professionals for registering the DSC:

- ❖ Provides personal details including individual identifier (DIN for Directors/Authorised signatory and PAN for Professionals.
- ❖ Provide DSC when directed by the MCA21 portal.
- ❖ System checks the name in the DSC as entered in personal details.
- ❖ In case DIN is entered, system validates if DIN is active. System also checks if the name in DIN matches with the name in Personal details.
- ❖ System creates user-id-DSC Serial number-DIN/PAN mapping after all validation are successful.

There may be need to update the DSC already registered with MCA21 due to loss or expiry or renewal of DSC.

There shall be two cases:

Case A: User has existing registered certificate

- i. User logs in with user id – DSC (existing)
- ii. User selects update DSC option.
- iii. User attaches new DSC and necessary validations are performed.
- iv. System shall delete old DSC after successful update,
- v. System creates user id – DSC (new) mapping.

Case B: User has lost certificate or certificate has expired

- i. User selects update DSC option at the MCA21 FO portal.
- ii. User enters user id and attaches new DSC.
- iii. System checks the name in the DSC matches with name entered as personal details.
- iv. System shall delete old DSC after successful update.
- v. System creates user id – DSC (new) mapping.

9.1.5 Verification

The digital signature verification process is same for certificates issued to all categories of users. MCA21 application performs the following before a digital signature is accepted by the system. Normally, when an eform is submitted, the MCA21 application performs the following steps:

1. **Digital signature verification:** The digital signature used in the solution is as defined in IT Rules 2000 as PKCS#7 format. The digital signature is verified using the signer's public key (available in the certificate) to ensure that the signer has signed the document with his private key only and also the data has not been tampered after it has been signed. The class of certificate is also verified.
2. **Role Check:** Role check is performed against the role check database created through the registration process as described above.
3. **Trust Chain Verification:** The signer certificate is verified against the various trust chain under the RCAI. A trust-list of CA certificate is maintained in the MCA21 application. For MCA employees trust till MCA sub-CA is verified.
4. **CRL Verification:** The signer certificate is validated to ensure that the certificate has not expired/revoked and the certificate is valid. The certificate status is checked using the certificate revocation list (CRL) published by the Certifying Authority. CRLs are downloaded from the CAs website on daily basis and maintained within the MCA21 application for verification of DSCs against the CRL.

All documents received are time stamped and maintained in secure repository for future reference.

9.2 Nemmadi Project in Karnataka

9.2.1 Introduction

Under the Nemmadi project, Government of Karnataka (GoK) has set up, through PPP model, a network of 800 telecenters at village level. It has also set up 177 backoffices at the taluka level. These telecenters would deliver range of G2C and B2C services at the citizen's doorsteps. The Government of Karnataka's vision for this project is that IT enabled Government services should be accessible to the common man in his village, through efficient, transparent, reliable and affordable means. The key objectives for this project are

- ❖ To create efficient and smart virtual offices of state government in all the villages.
- ❖ Initially, to provide copies of land records and 38 other citizen centric services of the revenue department in a convenient and efficient manner through 800 village Telecenters across rural Karnataka.
- ❖ To scale up the operations to cover all other G2C services of all the departments.
- ❖ To enhance the accountability, transparency and responsiveness of the government to citizen's needs.
- ❖ To provide government departments and agencies means of efficient and cost effective methods of service delivery to citizens.
- ❖ To manage the delivery of services through PPP model.
- ❖ To enable government departments and agencies to focus on their core functions and responsibilities by freeing them from the routine operations like issuing of certificates, land records, collection of utility bills of citizens and thereby enhancing the overall productivity of the administrative machinery.

9.2.2 Digital Signatures in Nemmadi Application:

The Nemmadi application has been developed by the Karnataka Unit of the National Informatics Centre (NIC). This application serves as the single window system for all government services at the village level. There is no need by the citizen to submit a written application for availing any service. There is a uniform service charge of Rs 15 for every service. The unique feature of this application is that "Signature less" documents are issued after being digitally signed by the appropriate authority.

1. Signatureless RTC

GoK is proceeding towards signature less documents and the Record of Rights, Tenancy and Crop Inspection (RTC) delivered from both the village Telecentre and the Taluka office will not contain any signature. This would therefore considerably reduce the dependency on Village Accountant for signing the RTC document at the village telecentre. This will be achieved by making the Bhoomi application PKI enabled. Each revenue official involved in processing of RTCs will sign any changes to RTC records using his private key.

Additionally the entire lot of pre-existing RTCs will also be signed using the private key of the authorized revenue official. This process which is compliant with the IT Act 2000, will enable issue of RTC with a 2D Barcode printed on the RTC and will remove the need for physical signature by the Village accountant on the RTC form. The 2D barcode will have within it the embedded digital signature of the RTC.

2. Signatureless Rural Digital Services (RDS) Certificate

Rural Digital Services (RDS) involves delivery of services of Revenue department from the Taluka to the citizen. These services include delivery of various types of Caste and Income Certificates, Registration of Birth and Death, Delivery of Birth and Death Certificates and application for Social Security Schemes like Old Age Pension, Widow Pension etc. In future services of other department like Social Welfare, Women and Child development etc. will also be added to the RDS platform.

The government is proceeding towards signature less documents and the RDS certificate delivered from both the village Telecentre and the Taluka office will not contain any signature. The RDS application being PKI enabled will enable the Telecentre operator to issue the certificate at the village itself, after such certificates have been digitally signed by the competent revenue authority, without needing to go to the Taluka office for collecting the physical copy of the signed certificate.

Besides the 2D bar code, the RDS certificate will be printed on a watermark stationary, a certificate id and a hologram to ensure its authenticity.

9.2.3 Verification of Signatureless Certificates

The RDS Certificates are signatureless documents. The certificate is printed on a uniquely numbered and water marked paper supplied by Government of Karnataka and also carries a uniquely numbered hologram. The signed hash of the certificate contents is printed as machine readable 2D barcode at the bottom of the certificate. Each certificate also carries 2 seal impressions and the signature of the Nemmadi operator in accordance with the provisions of IT Act 2000.

The genuineness of these certificates can be verified conclusively by any person or authority as follows:

1. Verification by Request ID

Connect to Nemmadi website (<http://nemmadi.karnataka.gov.in/certificateverification>). Key in the unique Request ID printed on the certificate. This method shows the corresponding record on the Nemmadi website. However, the user needs to compare the contents displayed on computer (of the authentic document stored on SDC) with the content on the print out. This procedure does not require a 2D barcode and therefore also does not tell who has digitally signed the contents of the document. It allows one to compare the authentic document on the government website with the contents on the print out.

2. Verification by 2D BarCode

Connect to Nemmadi website (<http://nemmadi.karnataka.gov.in/certificateverification>). Use a barcode reader to read the 2-D bar code printed at the bottom of the certificate. The verification process would show the corresponding record on the Nemmadi website and also inform whether the signature on the certificate is of a valid authority. However the user needs to compare the contents displayed on computer (of the authentic document stored on SDC) with the contents on the certificate hardcopy. This method requires a computer, an internet connection and a 2D bar code reader.

3. Fully Independent Verification

This method does not require an internet connection for certificate verification. It also does not have dependence on the content on the government website. The verifier can verify the certificate by just using the data printed on the certificate. The user needs to download and install a verification utility custom developed for Nemmadi from the Nemmadi website. The user also needs to download the certificates of CCA and NIC and the public key of the authorised taluka and the taluka official onto the computer. Once these items are installed on the computer, the user can scan the 2D barcode on the Certificate and the verification utility will check the validity of the Digital Signature. The verified message guarantees three things:

1. The document was signed by the competent authority
2. The contents as shown on the document have not been tampered.
3. The issuing authority cannot disown the content of the document.

9.3 e-District Application of Assam

9.3.1 Introduction

The Government of Assam introduced digital signatures in its e-Governance framework under the ambit of NeGP in one of the torch bearer projects called the “e-District Pilot Project” implemented in the districts of Goalpara and Sonitpur. The twin pilot projects were formally launched by Dr. Himanta Biswa Sarmah, Hon'ble Information Technology Minister, Govt. of Assam on the 12th of November, 2009 and 12th of January, 2010 in Goalpara and Sonitpur districts respectively. Digitally signed certificates are being issued in these two districts. Looking at the success of the digitally signed certificates, the Hon'ble Chief Minister of Assam, Sri Tarun Gogoi has already announced his intent to bring digital signatures in the Secretariat itself through the Assam Online Portal/SP/SSDG & Secretariat Less Paper Office Project (SLPO). Due to a very strong commitment of the Government of Assam, digital signatures have now been implemented in two districts, and the project is ready to be rolled out in the balance of 25 districts in a similar fashion. Digital signatures are also poised to make entry into the Assam Secretariat by December, 2010.

The e-District MMP has been implemented in Sonitpur and Goalpara districts of Assam as part of the ambitious National e-Governance Plan for ensuring transparency, efficiency and streamlining various G2C services under the ambit of the District Administration. The e-District project envisages back end computerization of G2C services (Certificates, Pensions, Revenue Courts, Pensions, RTI etc) at the district level and delivery of these services to the citizens electronically leveraging the ASWAN and Common Service Centres. The entire process of application processing and verification of such services would be done electronically and the approval/rejection of the service request by the designated authorities at the District Administration level would be done online. The output of such a service request in the form of a certificate or order, depending on the service would also be system generated with security features like digital signatures, 2D Bar codes etc. Citizens can now collect the print out of such certificates from the CSCs/Public Facilitation Centres by paying a nominal fee.

As part of the e-District Pilot project in Assam, one of the major technological interventions introduced is usage of Digital signatures by various approving authorities. This has brought about a complete change in the way applications are processed and approved. The Case study prepared in this regard, highlights various beneficial aspects of digital signatures, challenges being faced in the implementation and the lessons learnt.

9.3.2 Digital Signatures in e-District Assam

District Level Authorities Using Digital Signatures: The Digital signature has been able to penetrate the district level hierarchy from top to bottom. Despite certain issues, the level of acceptance has been found to be high. To sensitize the officers about digital signatures, several mock demonstrations and actual training sessions were organized at all the levels in the district. The following is the hierarchical list of district officials using digital signatures under the e-District pilots:-

Branches under the DC/SDO Administrative Set up	Authorities using Digital Signatures
Overall	Deputy Commissioner (DC)/Sub Divisional Officer (SDO)
Certificates(Magistracy)	Additional Deputy Commissioners (ADC)
Bakizai	ADC
Revenue Court	ADC
Pensions	ADC
FIC	Deputy Director of Supplies(DDS)
Election	Election Officer
RTI	ADC(APIO)
Below District level:1	Circle Officers(CO)
Below District level:2	Block Development Officers(BDO)

9.3.3 Uniqueness of Assam e-District

The uniqueness of the Assam e-district project has been the use of Digital signatures and the benefits arising out such a usage to the citizens. The following benefits/ features have been highlighted under the project:

1. The certificate / order issued under the project does not carry any physical signatures at all.
2. Each print out of the certificate is treated as original.
3. The certificate carries at least three ways in which it can be verified by any citizen or authority namely-
 1. A unique serial number under the 1-D barcode
 2. Scanning the 2-D barcode and getting the link information downloaded to one's mobile handset using a camera & java enabled mobile phone having barcode readers.
 3. Visiting the e-District Portal and entering the serial number.
 4. Calling up e-District rural call center during office hours at +91-361-2724-555 (This facility is technically ready for launch for the benefit of the citizens)

In case the application is lost or damaged, the citizen can just take another print out from the nearest CSC. So far 7066 number of digitally signed certificates have already been issued in the two districts. An image of an actual digitally signed certificate issued under the e-District project may be seen at the end of this section.

9.3.4 Challenges in Implementation of Digital Signatures

A. Change Management Issues: As the digital signatures are issued in name rather than the designation, transfer of officials requires frequent deactivation and reissue of digital signatures. The administrative effort to manage such issues creates undue delay due to centralized nature of the issuing authority. As the requirement of digital signature is likely to grow after state wide roll out of e-District project, a state level issuing authority is thought to be economically more feasible. Currently, it takes anything from 7 days to a month for a new signature certificate. The State Designated Agency (AMTRON) is likely to become a franchisee of M/S Sify for providing Digital signatures to the officials of the Govt. of Assam in order to keep pace with frequent transfers and to ensure timely delivery of services to the citizens.

B. Issues on Acceptance by certain Authorities: It has been observed some of the authorities such as Courts, some Universities, Passport offices etc. are finding it difficult to accept the digitally signed certificates in the printed form. The Govt. of Assam has already taken up this matter with the Govt. of India and the

authorities concerned. The resistance is slowly melting. If proper awareness is launched in the public, it would help the cause of easy acceptance of digital signatures.

9.3.5 Lessons Learnt and Road Ahead

The following are the lessons learnt and the road ahead suggested for implementation of digital signatures in the e-Governance programmes:-

- The digital signature implementation must be end to end available without any dependency on proprietary OS.
- The verifications must happen on the local application servers, else the implementation model may fail in the remote applications in the rural landscape.
- The State Government needs to develop its own franchisee model for management of digital signatures on a day to day basis, else it may impede decision making.
- No physical signature should be promoted on print outs of any digitally signed certificates/documents
- Awareness campaign should be launched in national and local media (in local languages) regarding what is digital signature and how it benefits the citizens.

GOVERNMENT OF ASSAM
OFFICE OF THE SUB-DIVISIONAL OFFICER
BISWANATH CHARIALI II SONITPUR DISTRICT

PERMANENT RESIDENT CERTIFICATE

Date: 17-06-2010

1706201000004834

This is to certify that the person with the following details :

Name	BABLY KHATUN
Name of Father	MD. ABDUL BAREK BEPARI
Name of Mother	SALEMA KHATUN
Revenue Circle	BISWANATH
Village / Town	AMBARIPAYOH ROAD
Post Office	CHARIALI
Police Station	BISWANATH CHARIALI
Sub - Division	BISWANATH CHARIALI
Purpose of Issue	Admission into higher educational institutions

is Permanent Resident of **SONITPUR**

This certificate shall not be valid for any other purpose other than the purpose stated above.

NOTE :

- This order is digitally signed and therefore needs no physical signature.
- Authenticity of this order can be verified from <http://edistrict.assamgovt.in>. This Order is legally valid as per the Information Technology ACT, 2008 and its subsequent amendments.
- Tampering of this order will attract penal action.

Signature of the Approving Authority

Signature valid

Digitally signed by Anshakar Phukan
Date: 2010.06.17 11:29:42 IST
Reason: e-District Portal
Location: Assam

Figure: Screenshot of a Digitally Signed Residence Certificate

9.4 Usage of Digital Signatures in UP

9.4.1. Introduction

In Uttar Pradesh, Digital Signatures are being extensively used in various projects right from delivery of citizen centric services through eDistrict to online application for tendering system. Many of the manual processes have

been converted to electronic workflow systems and the DSCs are being effectively used by the Government Officials in digitally signing the documents. These processes have made the service delivery faster and have almost brought an end to the physical movement of files and papers which used to cause delays and hold-ups. This has increased the authenticity of documents and reduced the chances of issuance of bogus and fake certificates.

9.4.2. Successful Implementations of Digital Signatures

Some of the successful implementation of Digital Signatures in Uttar Pradesh include -

S.No	Project	Use of Digital Signatures	No of DSC issued
1.	eDistrict – implemented in six pilot districts. More than 18 lakh Digitally Signed Certificates/ Service already delivered to citizens	Digital Signatures are being used for electronically signing the Certificates being issued through eDistrict Centres / CSCs etc. The approving authority puts his Digital Signatures at the time of approving the certificate and the related information is printed on the certificate also. This not only ensures that the details of the signing authority is displayed, even the DSC of the signatory can be verified over the Internet.	500 to various Govt. district functionaries such as DM, SDM, Tehsildar, DSO, DSWO etc for issuance of services
2	Online Counselling for admission to more than 1 lakh seats of Engineering, Medical, Polytechnic & B.Ed. courses.	The Digital Signatures are being used by the Counselling In-charge for document verification, fee submission, registration & for choice locking opted by the candidates which are finally locked by the invigilators using DSC. Class II DSC are being used for these activities In case of any modification in the student record, the same can be carried out only through digital signatures in order to ensure the same is recorded in the database.	1264 B.Ed – 438 UPTU - 433 Medical -433 Polytechnic – 220
3	eProcurement is an online tender processing system for the state government departments. More than 1000 tenders published so far.	The Digital Signatures are being used both by the vendors and government officials for tender submission and processing. The vendors/traders are using it for applying tenders online, while the government officials are using it at time of opening the tenders and during finalizing of the tenders. Class II signatures are being used both for signing and encryption of data.	About 500 to Govt. officials and Around 3000 to bidders
4	Voters List Preparation – The State Election Commission has issued a GO that the field data along with the photo ID will be digitized and the same will be digitally signed assuring the correctness of data.	The DSC will be used to counter verify the digitised data of voters list and the photo ID. This can be used by other applications such as eDistrict for online verification of citizen details.	Under Process
5	Many other departments are using DSC such as 1. CPWD	 1. Class III Signing	

	2. Defence 3. Railways 4. Post	2. Class III Signing & Encryption 3. Class II Signing 4. Class III Signing	
--	--------------------------------------	--	--

10. ANNEXURE

10.1 Annexure 1 - Frequently Asked Questions

- Q1. [What is Cryptography?](#)
- Q2. [How do I get a Digital Signature Certificate?](#)
- Q3. [What is a Certifying Authority \(CA\)?](#)
- Q4. [Who are the CAs licensed by the CCA?](#)
- Q5. [If CA is out of business then if the subscriber is told to move to another CA then the subscriber has to get a new digital certificate. What happens to his/her earlier transactions? Does this not create a legal and financial problem?](#)
- Q6. [Can one authorize someone to use DSC?](#)
- Q7. [Can a person have two digital signatures say one for official use and other one for personal?](#)
- Q8. [In paper world, date and the place where the paper has been signed are recorded and court proceedings are followed on that basis. What mechanism is being followed for dispute settlements in the case of digital signatures?](#)
- Q9. [Is there a "Specimen" Digital Signature like a "Specimen" Paper Signature?](#)
- Q10. [If somebody uses others computer, instead of his own computer, then is there any possibility of threat to the security of the owners/users digital signature?](#)
- Q11. [Is it possible for someone to else to use your digital signature without your knowledge?](#)
- Q12. [When you cancel an earlier communication you can get it back, how does this work in e-environment?](#)
- Q13. [When can a DSC be revoked?](#)
- Q14. [How do digital certificates work in e-mail correspondence?](#)
- Q15. [How do Digital Certificates work in a web site?](#)
- Q16. [What clause an eGov project should have to ensure that the PKI implementation meets the requirement of the IT Act 2000?](#)
- Q17. [Can I use the certificate issued by a CA across eGovernance applications?](#)
- Q18. [What are the key sizes in India?](#)
- Q19. [What is the size of digital signatures?](#)
- Q20. [What is the Key Escrow?](#)
- Q21. [What are the documents accepted by NIC – CA for verification?](#)
- Q22. [How do applications use the CRLs?](#)
- Q23. [How long do the CAs' in India preserve the Public Keys of the end users?](#)
- Q24. [Should e-Governance applications archive the Digital Signature Certificates as well?](#)
- Q25. [Can I have multiple Digital Signatures to a document?](#)
- Q26. [What are the types of applications that should use Digital Signatures?](#)
- Q27. [What are cryptotokens?](#)
- Q28. [What are the different ways of authenticating content of digitally signed documents issued to the citizen?](#)
- Q29. [How can a digitally signed document be verified after the DSC associated with the Public Key has expired?](#)
- Q30. [How can Departments ensure that their Government officers authorized to sign the Certificates do not misuse their Digital Signature Certificates after being transferred from a given place?](#)
- Q31. [How can a citizen be assured that the document has been digitally signed by the appropriate authorized Government officer?](#)

Q1. What is Cryptography?

Cryptography is the science of enabling secure communications between a sender and one or more recipients. This is achieved by the sender scrambling a message (with a computer program and a secret key) and leaving the recipient to unscramble the message (with the same computer program and a key, which may or may not be the same as the sender's key).

There are two types of cryptography: Secret/Symmetric Key Cryptography and Public Key Cryptography.

Secret key (symmetric/conventional) cryptography - is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.

Public key (asymmetric) cryptography - is a system based on pairs of keys called public key and private key. The public key is published to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

The Digital Signatures created using the private key ensure data integrity, data authentication and non-repudiation. However, to ensure confidentiality, encryption of the data has to be done with the recipient's public key.

Q2. How do I get a Digital Signature Certificate?

The Office of Controller of Certifying Authorities (CCA), issues Certificate only to Certifying Authorities. The CAs in turn issue Digital Signature Certificates to the end-users. You can approach any of the CAs for getting the Digital Signature Certificate. For more information about the respective CAs kindly visit their websites (provided below)

Name of CA	Website
Safescript	www.safescript.com
National Informatics Centre	www.nic.in
Institute for Development and Research in Banking Technology (IDRBT)	www.idrbtca.org.in
TCS CA services	www.tcs-ca.tcs.co.in
MTNL CA services	www.mtnltrustline.com
(n) Code Solutions	www.ncodesolutions.com
eMudhra	www.e-Mudhra.com

Q3. What is a Certifying Authority (CA)?

A CA is a trusted third party willing to verify the ID of entities and their association with a given key, and later issue certificates attesting to that identity. In the passport analogy, the CA is similar to the Ministry of External Affairs, which verifies your identification, creates a recognized and trusted document which certifies who you are, and issues the document to you.

Q4. Who are the CAs licensed by the CCA?

- a. Safescrypt
- b. NIC
- c. IDRBT
- d. TCS
- e. MtnTrustline
- f. GNFC
- g. e-MudhraCA

Q5. If CA is out of business then if the subscriber is told to move to another CA then the subscriber has to get a new digital certificate. What happens to his/her earlier transactions? Does this not create a legal and financial problem?

Prior to cessation of operations the CA has to follow procedures as laid down under the IT Act. Such problems should not therefore exist.

Q6. Can one authorize someone to use DSC?

Incase a person wants to authorize someone else to sign on his/her behalf, than the person being authorized should use their own PKI credentials to sign the respective documents.

Q7. Can a person have two digital signatures say one for official use and other one for personal use?

Yes.

Q8. In paper world, date and the place where the paper has been signed is recorded and court proceedings are followed on that basis. What mechanism is being followed for dispute settlements in the case of digital signatures?

Under the IT Act, 2000 Digital Signatures are at par with hand written signatures. Therefore, similar court proceedings will be followed.

Q9. Is there a "Specimen Digital Signature" like Paper Signature?

No. The Digital signature changes with content of the message.

Q10. If somebody uses others computer, instead of his own computer, then is there any possibility of threat to the security of the owners/users digital signature?

No, there is no threat to the security of the owner / users digital signature, if the private key lies on the smartcard /crypto token and does not leave the SmartCard/crypto token.

Q11. Is it possible for someone to use your Digital Signature without your knowledge?

It depends upon the how the signer has kept his private key. If private key is not stored securely, then it can be misused without the knowledge of the owner. As per the IT Act 2000, the owner of the private key will be held responsible in the Court of Law for any electronic transactions undertaken using his/her PKI credentials(public/private keys).

Q12. When you cancel an earlier communication you can get it back, how does this work in e-environment?

A new message saying that the current message supersedes the earlier one can be sent to the recipient(s). This assumes that all messages are time stamped.

Q13. When can a DSC be revoked?

The DSC can be revoked when an officer is transferred, suspended or his/her key is compromised.

Q14. How do digital certificates work in e-mail correspondence?

Suppose Sender wants to send a signed data/message to the recipient. He creates a message digest (which serves as a "digital fingerprint") by using a hash function on the message. Sender then encrypts the data/message digest with his own private key. This encrypted message digest is called a Digital Signature and is attached to sender's original message, resulting in a signed data/message. The sender sends his signed data/message to the recipient.

When the recipient receives the signed data/message, he detaches sender's digital signature from the data/message and decrypts the signature with the sender's public key, thus revealing the message digest.

The data/message part will have to be re-hashed by the recipient to get the message digest. The recipient then compares this result to the message digest he receives from the sender. If they are exactly equal, the recipient can be confident that the message has come from the sender and has not changed since he signed it. If the message digests are not equal, the message may not have come from the sender of the data/message, or was altered by someone, or was accidentally corrupted after it was signed.

Q15. How do Digital Certificates work in a web site?

When a Certificate is installed in a web server, it allows users to check the server's authenticity (server authentication), ensures that the server is operated by an organization with the right to use the name associated with the server's digital certificate. This safeguard's the users from trusting unauthorized sites.

A secure web server can control access and check the identity of a client by referring to the client certificate (client authentication), this eliminates the use of password dialogs that restrict access to particular users.

The phenomenon that allows the identities of both the server and client to be authenticated through exchange and verification of their digital certificate is called mutual server-client authentication. The technology to ensure mutual server-client authentication is Secure Sockets Layer (SSL) encryption scheme.

Q16. What clause an eGovernance project should have to ensure that the PKI implementation meets the requirement of the IT Act 2000?

The eGovernance applications have to be developed in compliance with RFC5280 certificate profile. A number of commercial and open source PKI toolkits are available which can be used to develop a standard validation process. Eg : - Microsoft CNG, Sun Java Toolkit. Please refer to Annexure IV of the Digital Signature Certificate Interoperability Guidelines (<http://cca.gov.in/rw/pages/index.en.do>) for further details.

Q17. Can I use the certificate issued by a CA across eGovernance applications ?

Yes.

Q18. What are the key sizes in India?

CA Key is 2048 bits and the end user keys are 1024 bits. However from 1 Jan 2011, the end user keys will be 2048 bits as well as per the notification by CCA.

Q19. What is the size of digital signatures?

The size of the Digital Signatures varies with the size of the keys used for generation of the message digest or hash. It can be a few bytes.

Q20. What is the Key Escrow?

Key escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

Q21. What are the documents accepted by NIC – CA for verification?

Any of the following id's are accepted by NIC-CA for verification of CSR

- Employee ID
- Passport Number
- Pan Card Number
- Driving License Number
- PF Number
- Bank Account Details
- Ration Card No

Q22. How do applications use the CRLs?

The applications download the CRLs from the respective CA sites at a specified frequency. The applications then verify the public keys against this CRL at the time of Digital Signature verification. The CCA is in the process of implementation of the OCVS (Online Certificate Verification Service) . This will ensure online verifications of the CRLs by the applications.

Q23. How long do the CAs' in India preserve the Public Keys of the end users?

As per the IT Act 2000, each CA stores the Public Key in their repository for a period of 7 years from the date of expiration of the Certificate.

Q24. Should e-Governance applications archive the Digital Signature Certificates as well?

In view of the fact that the CAs have a mandate to save the DSCs for a period of 7 years, it may be advisable for the e-governance applications which would need to verify the records for authenticity for periods beyond 7 years.

Q25. Can I have multiple Digital Signatures to a document?

Yes one can have multiple Digital Signatures to a document. For eg: - in the MCA21 application the forms are signed by different Directors as part of the application workflow.

Q26. What are the types of applications that should use Digital Signatures?

The eGovernance applications mainly provide:

1. Information Services
2. Interactive Services (downloading of forms etc)
3. Transaction Services with or without payments like issuance of various Certificates etc

The category 3 services (transaction based) can benefit from the use of digital signatures. In general wherever a eGovernance application requires handwritten signatures during the workflow of a document in the approval process, we should replace them with Digital Signatures.

Q27. What are cryptotokens?

They are hardware security tokens used to store cryptographic keys and certificates. Eg :- USB etc

Q28. What are the different ways of authenticating content of digitally signed documents issued to the citizen?

There are different ways of verifying the content and the digital signatures of the document. Some of the mechanism are enlisted below:-

1. Via Unique Request ID (manual content verification only) - In this process the user can verify the validity of his/her document by logging onto the Department website and providing the unique request number printed on the document. The Department application will display the electronic version of the document stored in the application repository. However in this process since the digital signature on the document is not verified, the contents have to be verified manually by the user by comparing the online document from the website with the hardcopy of the document. This process thus provides content verification only. The verification of the Digital Signature does not take place in this process.

2. Verification by the 2D Barcode – In this process, the barcode printed at the bottom of the document is used for the digital signature verification. The barcode has the Digital Signature embedded in it. The two verification mechanisms enlisted below verify the Digital Signature only. Since the complete content of the document is not being scanned, the content verification has to be done manually.

a) Online Verification

In this process, a barcode reader is used to scan the 2-D bar code printed at the bottom of the certificate. The verification utility of the Departmental application would verify the digital signature embedded in the document and after successful verification, show the corresponding electronic record on their website. However the user needs to compare the contents of the electronic record and the hardcopy. This method requires a computer, an internet connection and a 2D bar code reader.

b) Offline Verification

In this process, the user can verify the digital signature embedded in the barcode without connecting to the Department website. Thereby this process is called as “offline” verification. The user needs to download and install the verification utility custom developed by the Department (downloadable from their website). The user also needs to download the root chain certificates of CCA and NIC and the public key of the authorised taluka and the taluka official onto the computer. Once these items are installed on the computer, the user can scan the 2D barcode on the document and the verification utility will check the validity of the digital signature embedded in the document thereby proving the authenticity of the document. However, the content of the hardcopy of the document will have to be manually verified by the comparing with the electronic version available at the Department website as the content of the hardcopy is not being scanned in this process.

Q29. How can a digitally signed document be verified after the DSC associated with the Public Key has expired?

The digital signature verification process for a document requires the public key, root chains and the CRL. The eGovernance application should therefore have a repository of public key certificates, root chains and the CRL's of the time the document was digitally signed. The CA's as of now are mandated to store the Digital Signature

Certificates, root chains and the CRLs for a period of 7 years as per the Rules of the IT Act. Therefore the Digital Signature Certificates can be downloaded from the CAs for a period of 7 years. However, if the digital signature on the document needs to be verified after this period, the eGovernance applications will have to have a provision to store the DSCs, root chains and the CRLs in a repository and undertaking the verification of digitally signed document against this repository. However, it may be a cumbersome process to get the CRLs' from the respective CAs for a specific period (in the past).

Q30. How can Departments ensure that their Government officers authorized to sign the Certificates do not misuse their Digital Signature Certificates after being transferred from a given place?

It is recommended that as part of the handing over of charge of a given officer, the DSC issued to the officer be revoked. Further his user credentials in the respective eGovernance applications should be deactivated so that he can no longer access the application while the Certificate revocation is under process with the CA. Once the DSC is successfully revoked, the officer will be no longer able to sign the documents.

Q31. How can a citizen be assured that the document has been digitally signed by the appropriate authorized Government officer?

In order to ensure that the documents are signed by authorized individuals only, the Departments should maintain a repository having a mapping between the DSC and the respective roles assigned to the officers of the Departments. The eGovernance application should check against this repository for the various documents before allowing an officer to digitally sign the document. This mechanism has been implemented in MCA21 application wherein multiple directors sign the eforms for the application. The key challenge with this approach is to be able to maintain an updated repository at all times.

The Government of India is currently looking into the proposal for creation of a central repository of Digital Signature Certificates and CRLs' in order to ensure that digitally signed documents can be verified at a later date (greater than 7 years).

10.2 Annexure 2 - Definitions and Acronyms

Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Cryptography systems can be broadly classified into **symmetric-key systems** and **public-key systems**.

Secret key (Symmetric/Conventional) cryptography

This is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.

Public – Key (Asymmetric Key) Cryptography

This system is based on pairs of keys called public key and private key. The public key is published and known to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

Hash Function

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or digest or hash.

Cryptotoken

Cryptotoken is a security token used to store cryptographic keys for digitally signing the documents. They are typically small enough to be carried in a pocket or purse or keychain. For example : - USB

Digital Signature Certificates (DSC)

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet.

Certificate Revocation List (CRL)

A CRL is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon. A CRL is generated and published periodically, often at a defined interval. The CRL is always issued by the CA which issues the corresponding certificates. All CRLs have a lifetime during which they are valid. During a CRL's validity period, it may be consulted by a PKI-enabled application to verify a certificate prior to use.

Public Key Infrastructure (PKI)

PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called “digital signatures” to them.

Certifying Authority (CA)

This is an entity that issues Digital Signature Certificate to the end users. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

Registration Authority (RA)

This is an entity within the CA that acts as the verifier for the Certifying Authority before a Digital Signature Certificate is issued to a requestor. The Registration Authority (RA) processes user requests, confirm their identities, and induct them into the user database.

Root Certifying Authority of India (RCAI)

This entity is created under CCA and is responsible for issuing Public Key Certificates to Licensed Certifying Authorities. This serves as the root of the trust chain in India. The requirements fulfilled by the RCAI include the following:

- The licence issued to the CA is digitally signed by the CCA.
- All public keys corresponding to the signing private keys of a CA are digitally signed by the CCA.
- That these keys are signed by the CCA can be verified by a relying party through the CCA's website or CA's own website.

11. SOURCES AND REFERENCES

CCA website: <http://cca.gov.in>

NIC- CA website: <http://nicca.nic.in>

Interoperability Guidelines for Digital Signature Certificates:
<http://cca.gov.in/rw/pages/index.en.do>

IT ACT 2000 <http://www.mit.gov.in/content/information-technology-act>

Wikipedia <http://www.wikipedia.org>

Nemmadi <http://nemmadi.karnataka.gov.in/>



Assam Electronics Development Corporation Ltd.

(A Government of Assam Undertaking)

Industrial Estate, Bamunimaidan, Guwahati-781 021, Assam
www.amtron.in



Head Office : G-4, H.No.2-2-647/125A, Sagarika Apartments
Central Colony, Bagh Amberpet
Hyderabad - 500 013

Guwahati Office : Zoo-Narengi Road, Near Geetanagar Police Station
Guwahati -781 024, Assam
www.medhassu.in