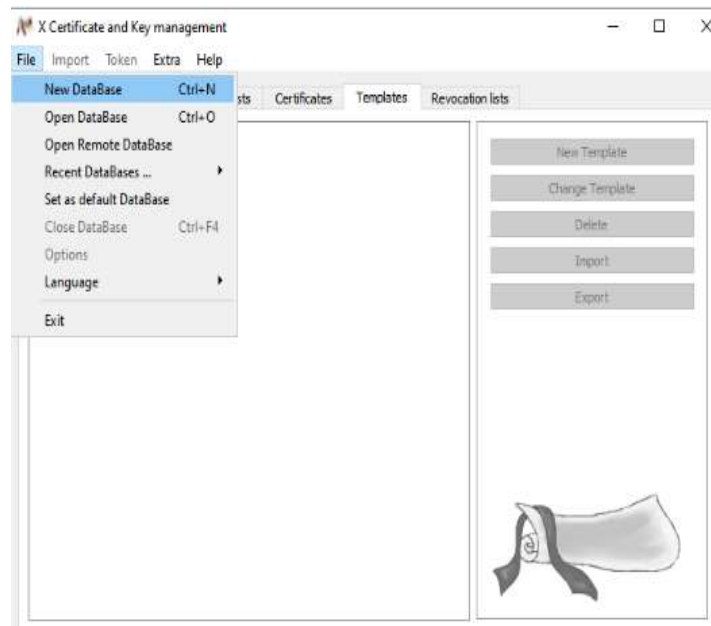


Module:- Public Key Infrastructure Date:- 19/09/2022
Assignment :- 03

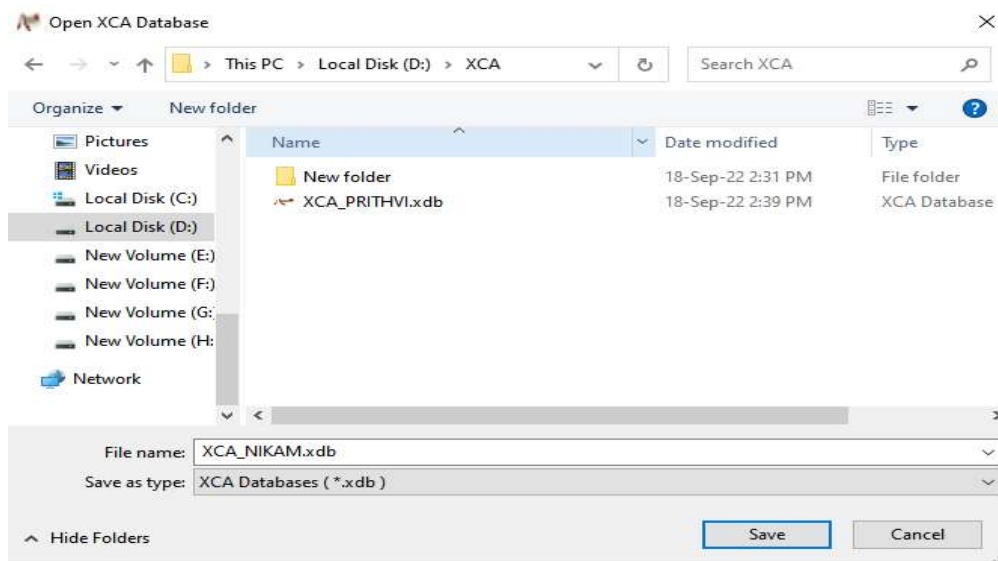
XCA TOOL:-

**PRACTICAL:- Digital Signature Certificate (DSC) validity only one day
19/09/2022 to 20/09/2022.**

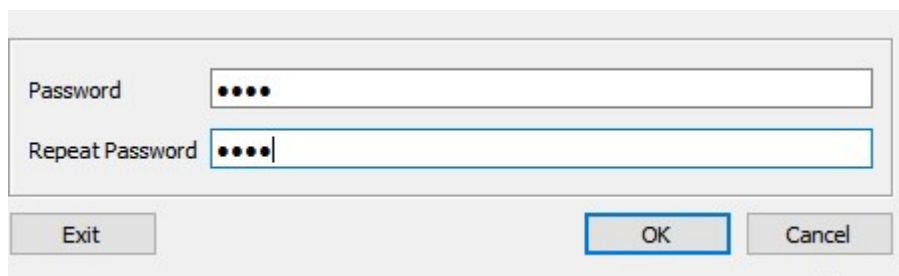
Step – 1:- Open XCA tool and select New Database Option.



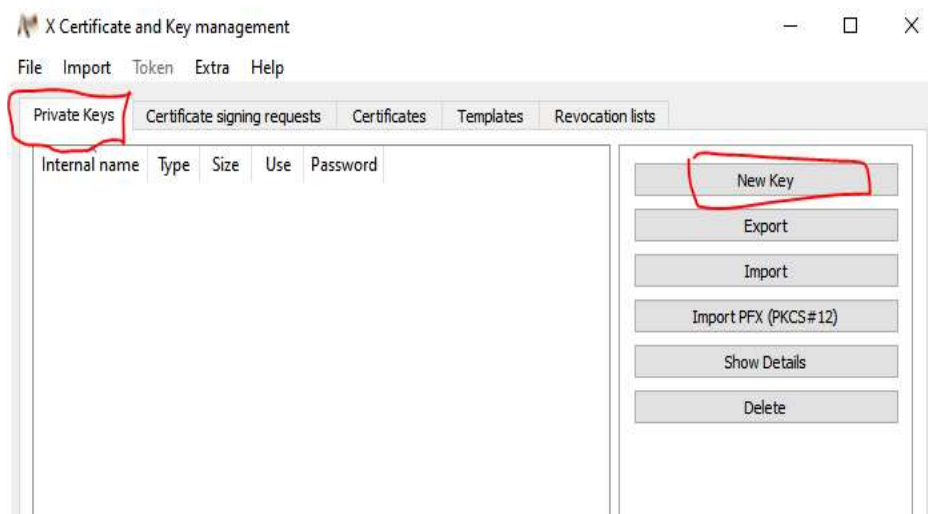
Save New Data Base file into any folder of system.



After Saving Set Password.



Step -2:- Now select Private key option and then select New key option.



X Certificate and Key management

New Key

Please give a name to the new key and select the desired keysize

Key properties


Name:

Keytype:

Keysize:

☐ Remember as default



X Certificate and Key management

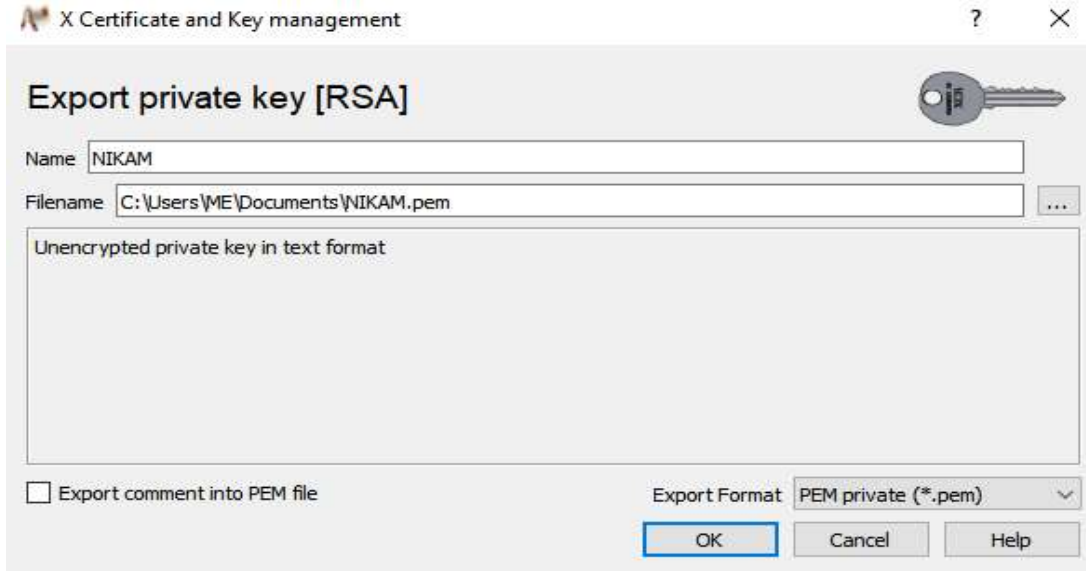
 Successfully created the RSA private key 'NIKAM'

X Certificate and Key management

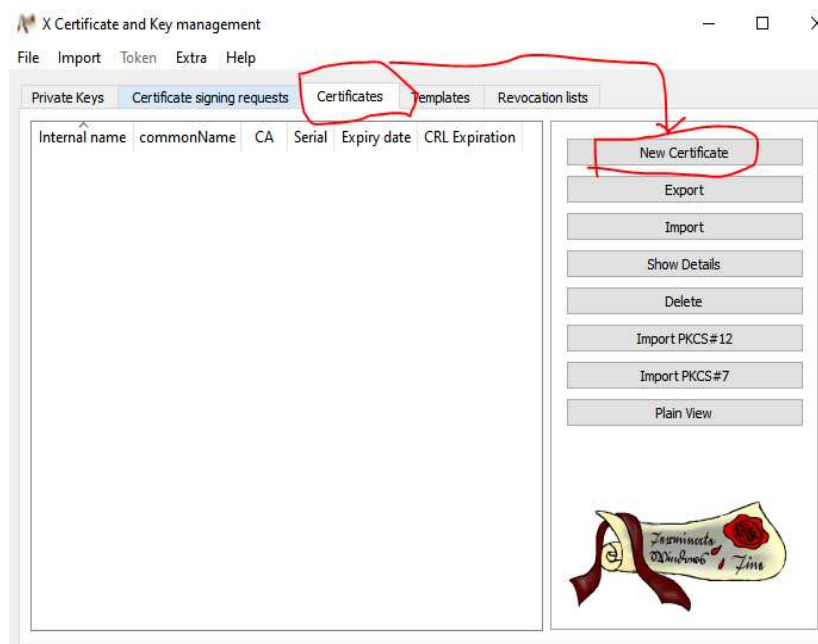
File Import Token Extra Help

Private Keys Certificate signing requests Certificates Templates Revocation lists

Internal name	Type	Size	Use	Password
 NIKAM RSA	RSA	2048 bit	0	Common
 Nikam RSA	RSA	2048 bit	1	Common



Now select Certificate option and then select New certificate option.



Step -3:- Now , after opening new certificate in XCA tool open new window and Create Certificate that have many text box such as.

Internal name:- NIKAM

Country name:- IN

State :- KARNATAKA

Locality :- BANGALURU

Organization name :- CDAC

Organization Unit Nmae :- CDAC

Common Name:- DITISS

Email-ID :- patlnikam813@gmail.com

And then we can select Generate new Key option.

X Certificate and Key management

Create x509 Certificate

Source **Subject** Extensions Key usage Netscape Advanced Comment

Internal Name Nikam

Distinguished name

countryName	IN	organizationalUnitName	CDAC
stateOrProvinceName	Karnataka	commonName	DITISS
localityName	Bangaluru	emailAddress	patlnikam813@gmail.com
organizationName	CDAC		

Type	Content
------	---------

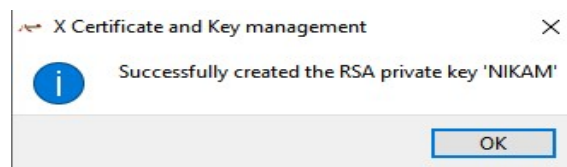
Add
Delete

Private key

NIKAM (RSA:2048 bit) ☒ Used keys too **Generate a new key**

OK Cancel Help

New Key generator generate is following image .



Step -4 :- After we can select Extensions when we can select End Entity and Time Period only one day(19/sep/2022 to 20/sep/2022) .

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced Comment

X509v3 Basic Constraints

Type: **End Entity**

Path length: ☐ Critical

Key identifier

☐ X509v3 Subject Key Identifier

☐ X509v3 Authority Key Identifier

Validity

Not before: 2022-09-19 15:21 GMT

Not after: 2022-09-20 15:21 GMT

Time range

1 Days

☐ Midnight ☐ Local time ☐ No well-defined expiration

X509v3 Subject Alternative Name

X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

Authority Information Access

☐ OCSP Must Staple

Step- 5:- Now we go to Key usage Option when we select Digital signature ,Non Repudiation and Certificate Sign option and last select ok.

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions **Key usage** Netscape Advanced Comment

X509v3 Key Usage

☐ Critical

Digital Signature

Non Repudiation

Key Encipherment

Data Encipherment

Key Agreement

Certificate Sign

CRL Sign

Encipher Only

Decipher Only

X509v3 Extended Key Usage

☐ Critical

TLS Web Server Authentication

TLS Web Client Authentication

Code Signing

E-mail Protection

Time Stamping

Microsoft Individual Code Signing

Microsoft Commercial Code Signing

Microsoft Trust List Signing

Microsoft Server Gated Crypto

Microsoft Encrypted File System

Netscape Server Gated Crypto

Microsoft EFS File Recovery

IPSec End System

IPSec Tunnel

IPSec User

IP security end entity

Microsoft Smartcard Login

OCSP Signing

EAP over PPP

EAP over Lan

Signing KDC Response

PKINIT Client Auth

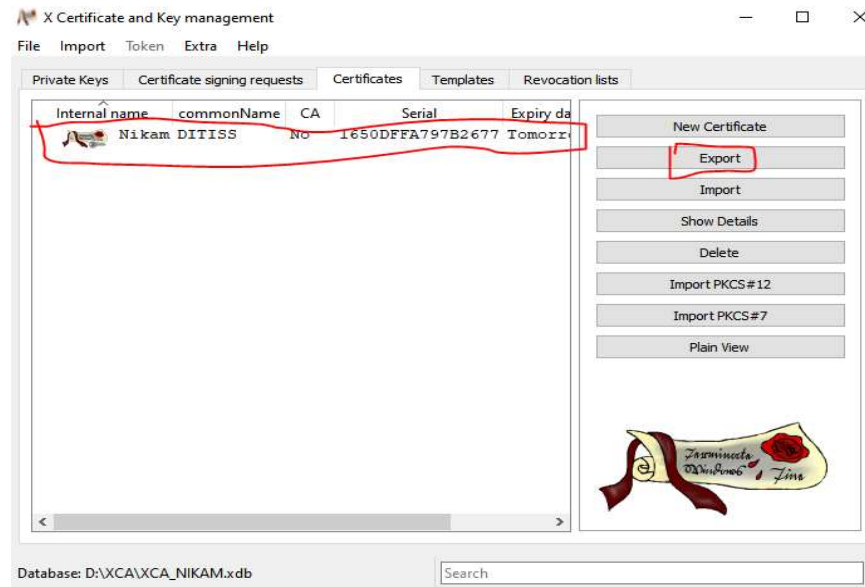
SSH Client

Adobe PDF Signing

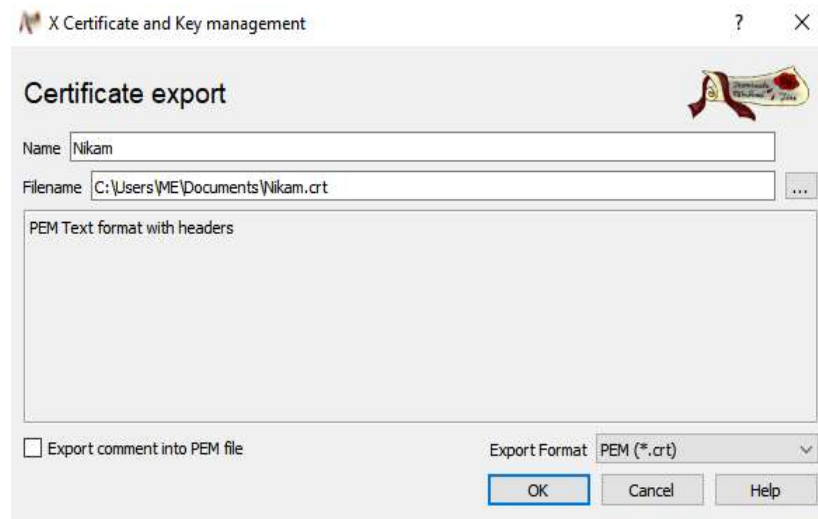
Microsoft Office Signing

Microsoft BitLocker Drive Encryption

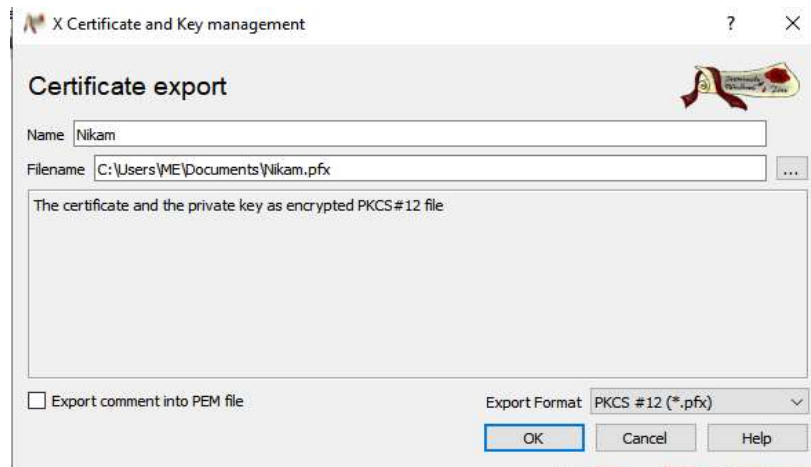
Step -6 :- Click Certificate and Export it.



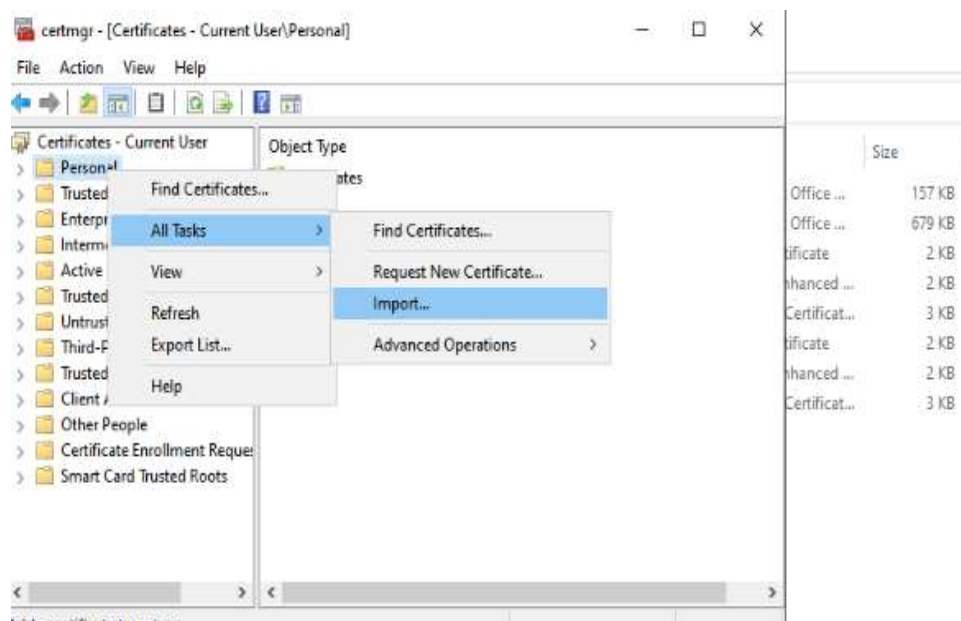
Export certificate in directory



Export pfx file in Directory.



Step -7:- We can go to and search, Manage user certificate when store Certificate and select personal → All task → Import → Nikam.crt and Nikam.pfx .



Now Popup Open it is Certificate vizard

←  Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location


- ☒ Current User
☐ Local Machine

To continue, click Next.

Next

Cancel

Now Import PFX File from Directory

←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\ME\Documents\Nikam.pfx

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel

Put password and click to next

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

Select Personal

← Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:
 Browse...

Next Cancel

Completing the import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\ME\Documents\Nikam.pfx

Finish

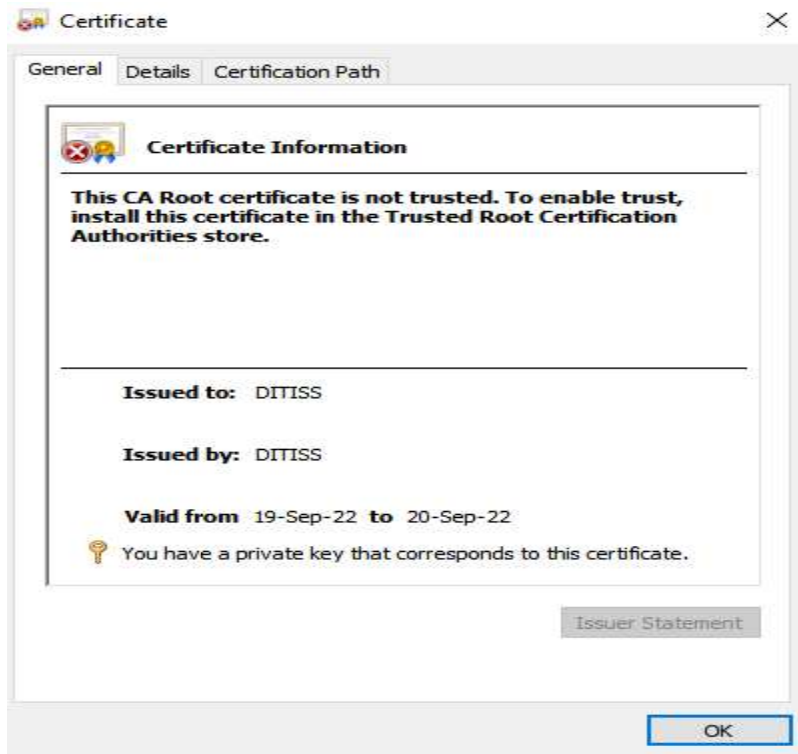
Cancel

Select the certificate and open it.

certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help

Certificates - Current User		Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Personal	Certificates	DITISS	DITISS	20-Sep-22	<All>	Nikam		
		DITISS	DITISS	19-Sep-23	<All>	Mohammad Misba...		

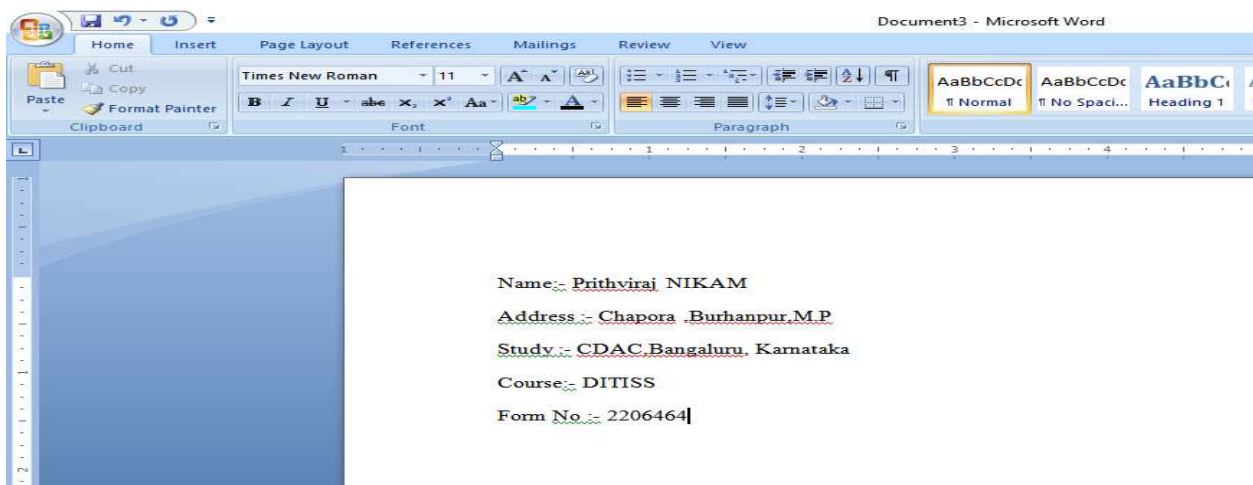


SIGN A DOCUMENT DIGITALY

A) PDF:-

PRACTIAL :-

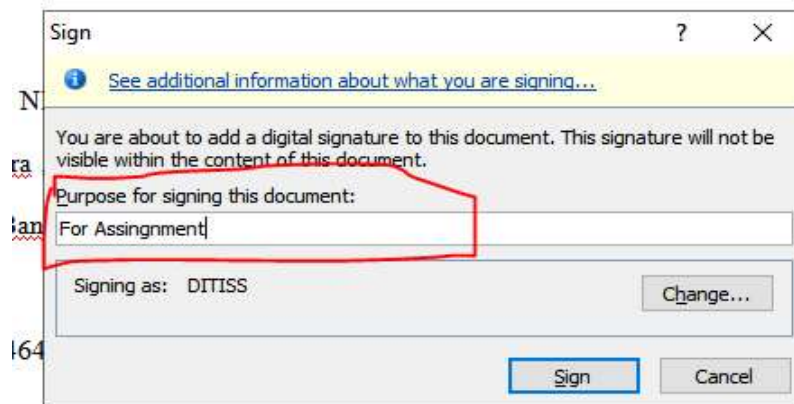
Step-1:- Open the new word file and fill some information save it.



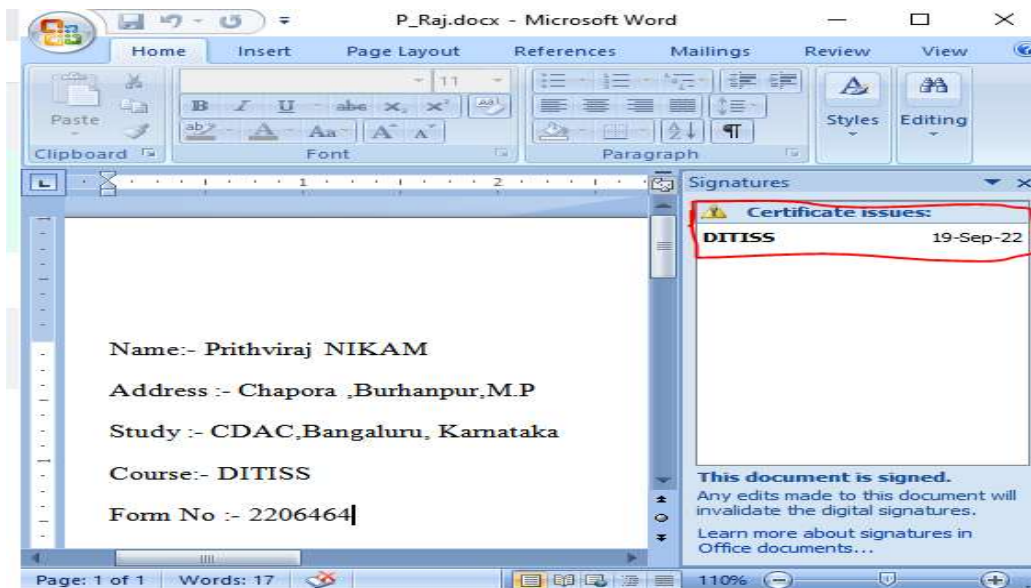
Step – 2:- Now open the new popup and select ok.



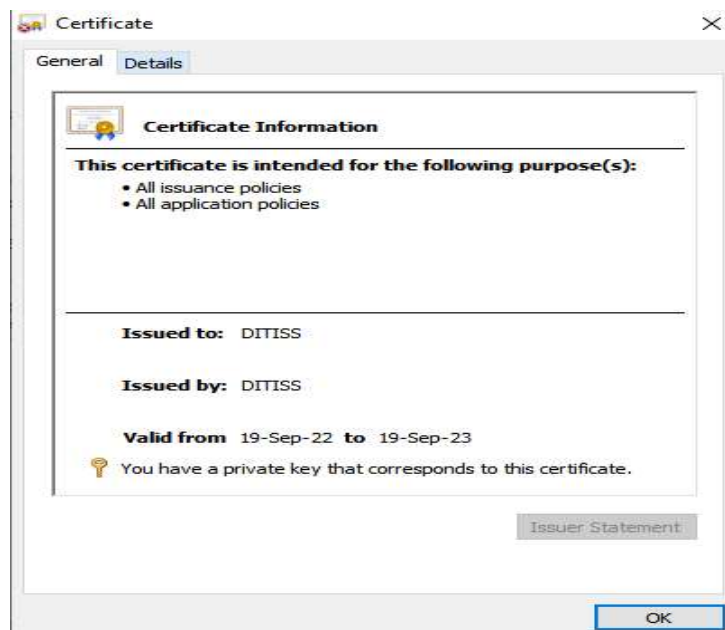
Step- 3:-opening the new window that can be show the purpose of document.



Step- 4:- Then word file right side showing the certificate DITISS.Now we can select DITISS → Signature Detail



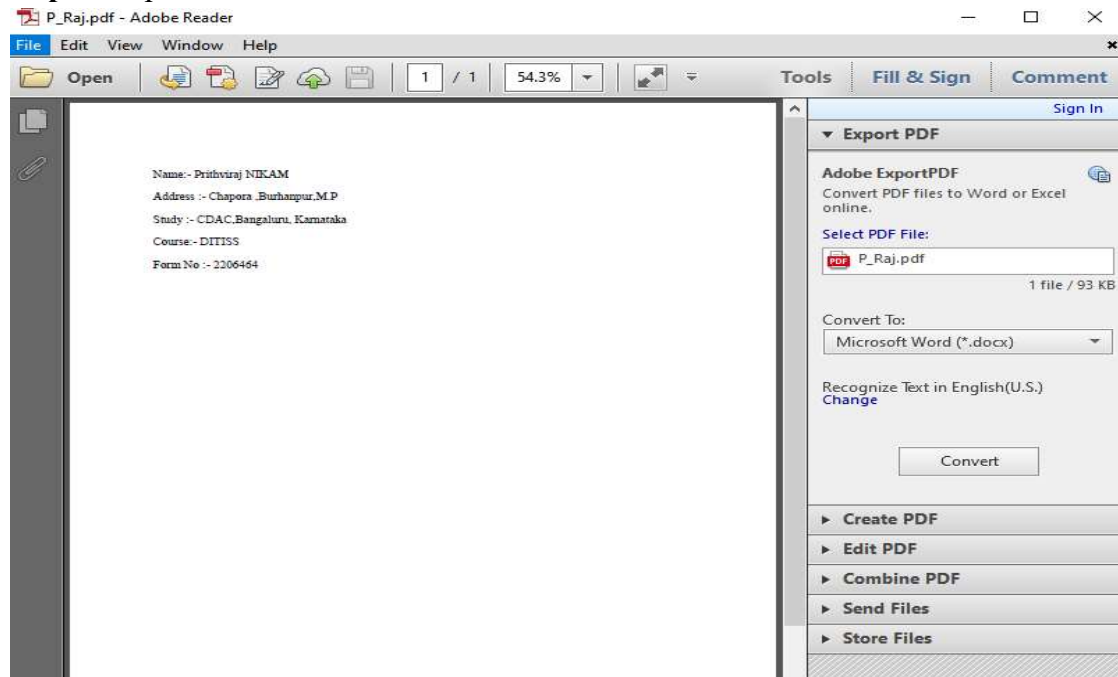
Step-5 :- Now we can view the certificate.



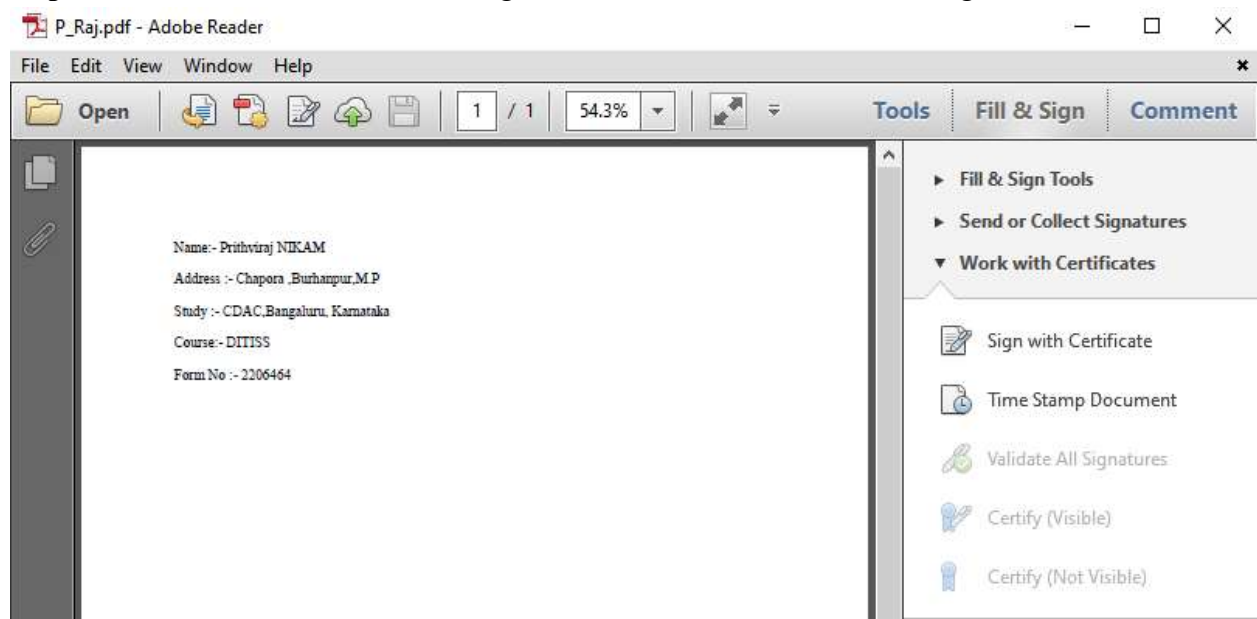
B) PDF :-

PRACTICAL :-

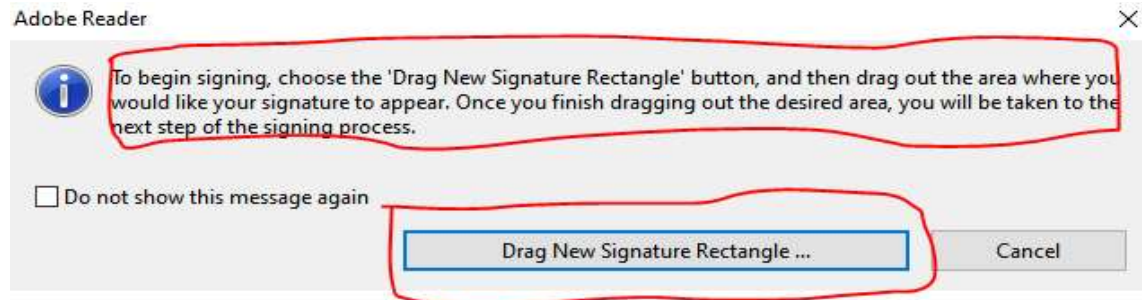
Step-1:- Open the new PDF file.



Step-2:- Now we can select Fill & Sign → Work with certificate → Sign with certificate.

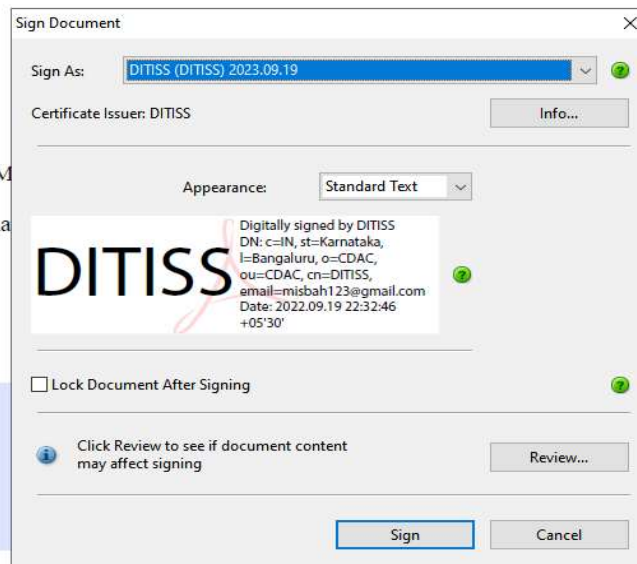


Now open the new popup that can be shown by drag and create a space on pdf page .



After Selection Drag New Signature Rectangle then click sign option.

Name:- Prithviraj NIKAM
Address :- Chapora ,Burhanpur,M
Study :- CDAC,Bangaluru, Karna
Course:- DITISS
Form No :- 2206464



Step – 3:- Now The signature is created.

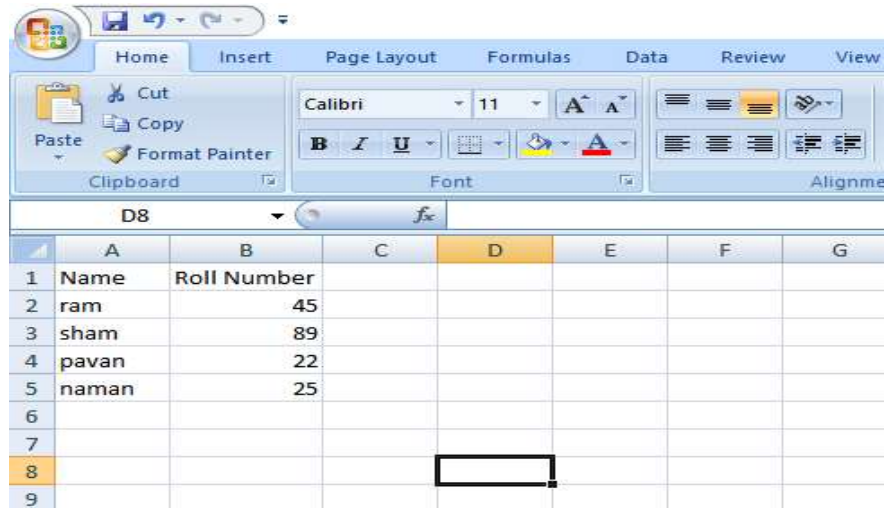
Name:- Prithviraj NIKAM
Address :- Chapora ,Burhanpur,M.P
Study :- CDAC,Bangaluru, Karnataka
Course:- DITISS
Form No :- 2206464

DITISS Digitally signed by DITISS
DN: c=IN, st=Karnataka, l=Bangaluru,
o=CDAC, ou=CDAC, cn=DITISS,
email=misbah123@gmail.com
Date: 2022.09.19 22:33:40 +05'30'

C) XCEL :-

PRACTICAL:-

Step-1:- Open the new Xcel file and fill some information save it.



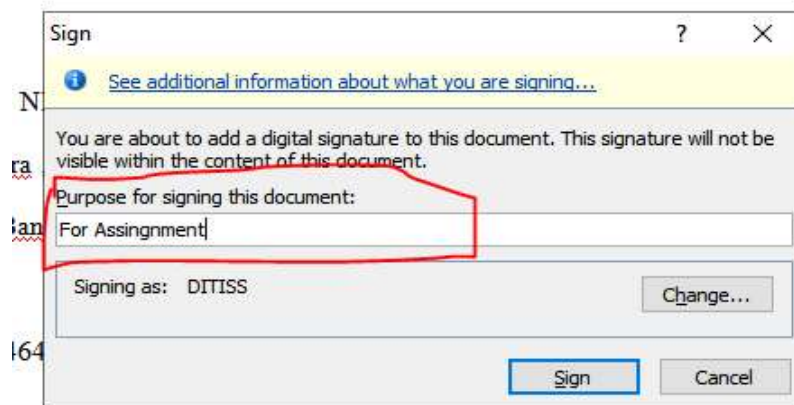
The screenshot shows the Microsoft Excel interface. The 'Home' tab is selected. The ribbon shows 'Clipboard' (Paste, Cut, Copy, Format Painter) and 'Font' (Calibri, 11, Bold, Italic, Underline, Text Color, Background Color). The 'Align' group is also visible. The spreadsheet has columns A through G and rows 1 through 9. A table is entered with the following data:

	A	B	C	D	E	F	G
1	Name	Roll Number					
2	ram	45					
3	sham	89					
4	pavan	22					
5	naman	25					
6							
7							
8							
9							

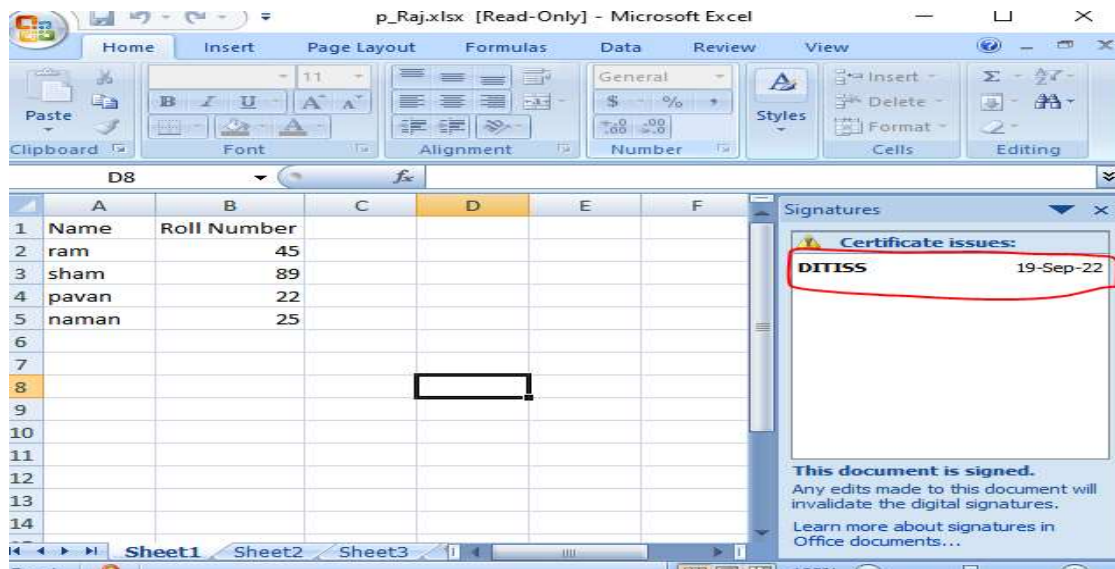
Step – 2:- Now open the new popup and select ok.



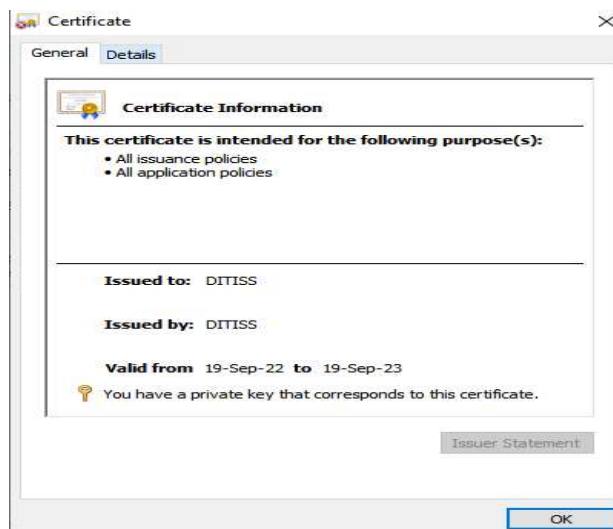
Step- 3:-opening the new window that can be show the purpose of document.



Step- 4:- Then word file right side showing the certificate DITISS.Now we can select DITISS → Signature Detail



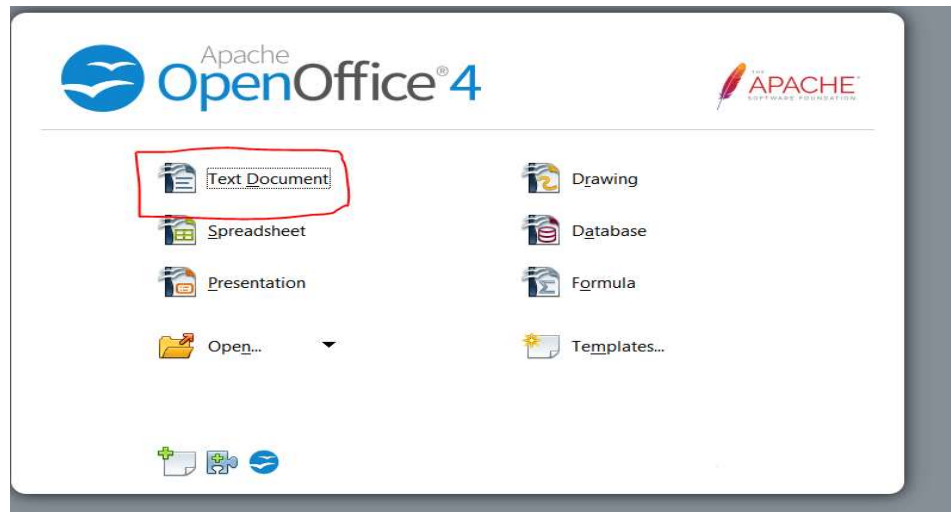
Step-5 :- Now we can view the certificate.



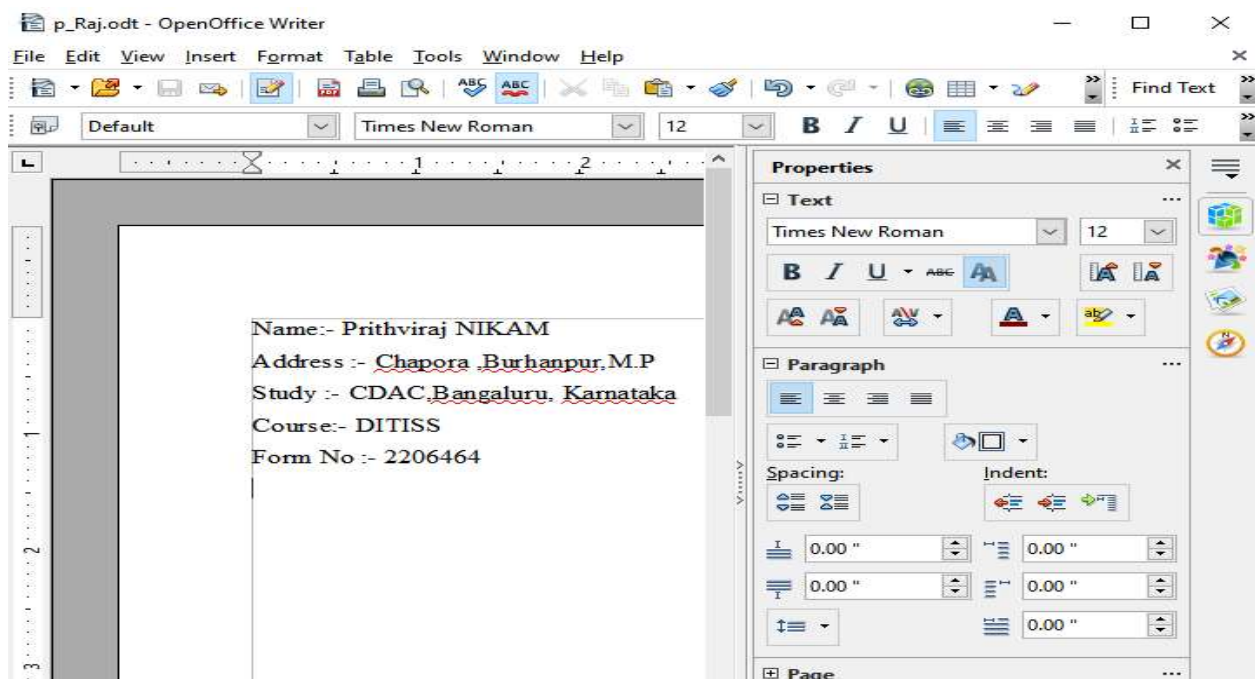
D) OPEN OFFICE :-

PRACTICAL :- Using Apache Open Office

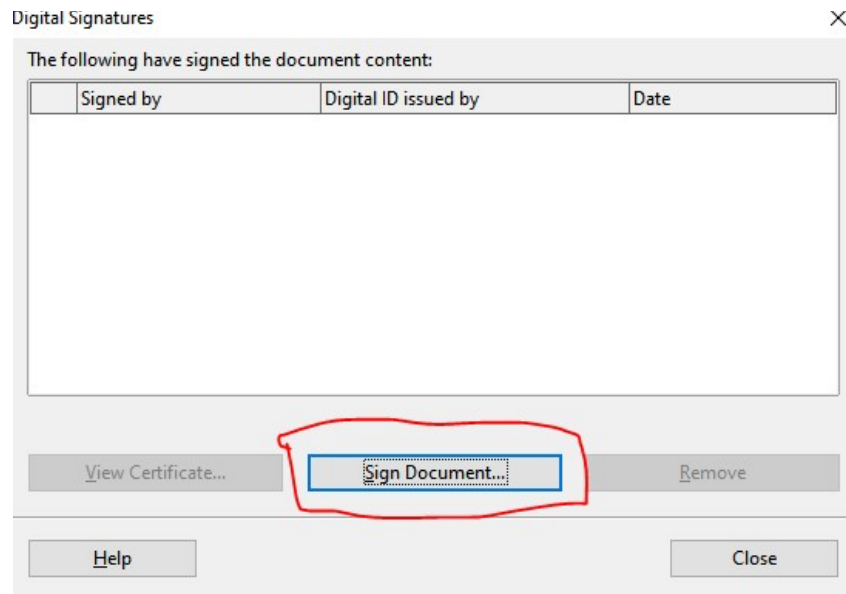
Step-1:- Now we can open the Apache Open Office and select text document.



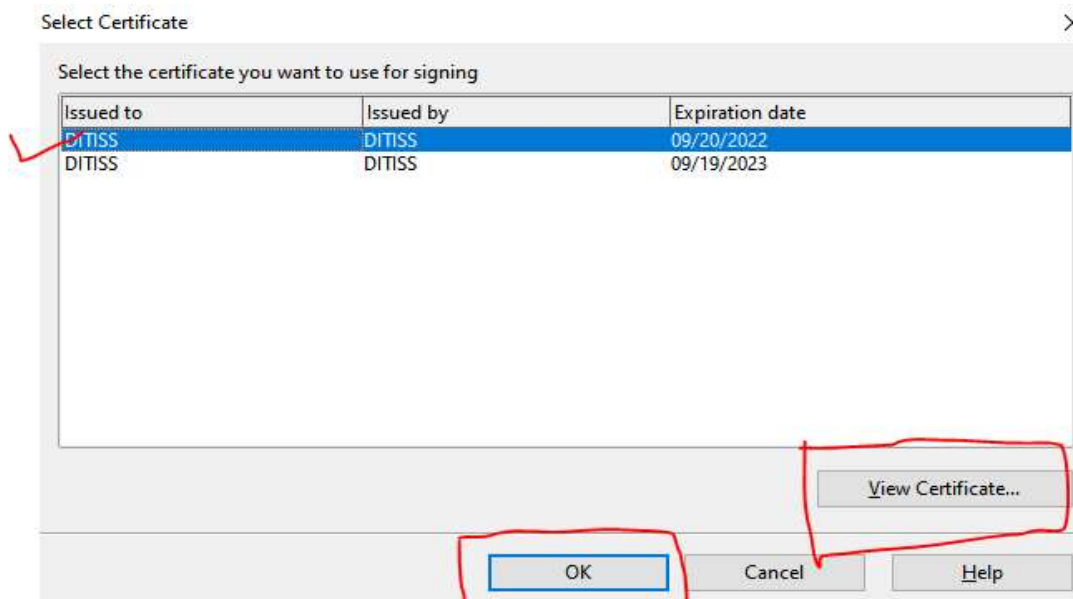
Step- 2:- Fill some information and save the file with .odt extension. Then go to File → Digital signature and Click it.



Step -3:- Then show the new window option Sign Certificate and click it



After clicking again new window will be open and select any one certificate and view it.



New screen will be open that can be show the certificate detail.

