NIC Certifying Authority
National Informatics Centre
Ministry of Communications & Information Technology
Government of India

Doc-Id: Form-1

Ref. No. ……

(To be filled by NICCA/RA Office)

DIGITAL SIGNATURE CERTIFICATE REQUEST FORM

NOTE:

1. **All fields are mandatory and validity of the filled form is 90 days**.
2. Please Tick (√) the appropriate option & submit only Page No. 1 & 2 after filling.
3. Subscriber is advised to read Certificate Practice Statement of NICCA.
4. Validity period cannot exceed the date of superannuation of applicant.
5. Asterisk (*) mark entry will be used in Certificate Subject Details.
6. **INCOMPLETE/INCONSISTENT FORMS WILL BE SUMMARILY REJECTED.**

Affix Recent Passport size Photograph **Attested by HO**

1. Category of Applicant : _____ ***[Fill code from Annexure-I]***
2. Project Code : _____ ***[Fill code from Annexure-II]***
3. Class of Certificate Required : Class-1 /Class-2 /Class-3 Device Required: **Token/ Smart Card** only for **signing** certificate
4. Certificate Required (Usage) : Signing /Encryption /SSL/System/Code Signing [**Separate Form for each except Signing/Encryption]**
5. Certificate Validity [Max. 2 Years] : Two Years /Specify Validity [if less than 2 Years] _____
6. Date of Superannuation [DD/MM/YYYY]* : _____
7. Name* (in **BLOCK** letters only) : _____
8. Designation : _____
9. Email-id*[Official email-id preferred] : _____
10. Ministry/Department : _____
    a) Office Address : _____
    _____
    Tel. No.(O)* _____ **Mobile No.*** _____
    b) Residential Address : _____
11. Identification Details* : _____
    [***Attach a photocopy of the same attested by HO***]
    [Departmental / Employment Photo ID No./ Service Verification Certificate with photograph]
12. Certificate Subject Details* : Organisation* _____
    Organisation Unit* _____
    City* _____ Postal Code* _____
    State* _____ Country* **INDIA**
    Only for PAN enabled DSC* : **PAN No.*** _____ [Attach a self attested photo copy of PAN card, for **Company PAN enabled** DSC: provide a company PAN & documentary proof for holding position in the company]
13. SSL/Web Server Certificate Details : Public IP Address_____ Physical Location _____
    [***To be filled only for SSL certificate***] URL/Domain Name _____
    Alternate Domain Name _____
    IP allocation Organisation_____
14. System Certificate Details : IP Address_____MAC Address _____
    [**Any one detail required**] Serial No./Unique Id (CPU/device)_____
15. Payment Details : DD No. _____ Date _____Bank Name_____
    NICSI Project No., if any _____

Place: ……
Date: ……..

(Please do not write below this line) [**Signature of Applicant**]

(For NICCA/RA Office Use Only)

REF	SCAN	UID	SC/SCR	TKN	PRN

Req. No. (S)_____
Req. No. (E)_____

RAA Name …….. **Date** ……..

Declaration by Subscriber

I hereby declare and understand that

1. I have read the subscriber agreement under Resource link available on NICCA website (https://nicca.nic.in).
2. I shall keep the private key safe on **FIPS-140 Level-2 compliant smart card/USB crypto-tokens** (Signing/Code Signing certificate) and will not share with others.
3. I shall verify the contents and the correctness of the certificate before accepting the DSC. I shall send a signed mail to NICCA (casupport@nic.in) to acknowledge the acceptance of the DSC.
4. I shall not use the private key before acceptance of the DSC.
5. I authorize NIC-CA to publish the certificate in the NIC-CA repository after acceptance of the DSC.
6. **If the private key of my DSC is compromised, I shall communicate to NICCA without any delay as per the requirement mentioned in Regulation 6 of Information Technology (Certifying Authority) Regulation 2001.**
7. I understand the terms and conditions of issued DSC and will use the DSC under the terms of issue as in the Certificate Practice Statement.
8. I understand that on cessation of my employment, I shall inform NICCA and my present employer for revocation of my Digital Signature Certificate.
9. I am solely responsible for the usage of these Certificates/Tokens/ Technology. I shall not hold NICCA responsible for any data loss/ damage, arising from the usage of the same.
10. **I am aware that Key Escrow/Archiving of Encryption Keys is not done by NICCA and I shall not hold NICCA responsible or approach NICCA for recovery of my private Encryption Key, in case of its loss or otherwise. I understand that in case of loss of private key of encryption certificate, I will not be able to decrypt the data which was encrypted by corresponding public key of the encryption certificate. I would keep safely backup of p12/pfx encryption key file and recover/restore the same in case its accidental or otherwise loss.**
11. I shall be responsible for compliance to the relevant sections of the IT Act/Indian Telegraphic Act and other Acts/laws of the Indian legal system, pertaining to Encryption/Decryption of any message or document or electronic data, and I shall be liable for associated penal actions, for any breaches thereof.
12. **NICCA shall not be held responsible and no legal proceeding shall be taken against NICCA for any loss and damage that may occur due to any reason whatsoever including technology upgradation, malfunctioning or partial functioning of the software, USB Token/ Smart Card or any other system.**
13. I am aware that the Certificate, issued by NICCA is valid only for the intended usage and for the period mentioned in the certificate. I undertake not to use the Certificate for any other purpose.
14. I am conversant with PKI technology, and understand the underlying risks and obligations involved in usage of Encryption Certificate/DSC.
15. For SSL Server Certificate, I undertake that I have checked the existence of IP/URL/domain name and physical location of the server.
16. For System Certificate, I undertake that MAC/Serial No./IP No. are correct and are in my custody.
17. For Class-3, certificate I shall appear in person at NICCA/RA/ **Physical Appearance Centre (PAC)** any of the NIC Centres, State Units/ District Centres/Cells at various Ministry Cell of NIC along-with a **photograph** and **departmental photo-id card** for **verification** and submit a photo copy of the same.
18. I certify the following: (Tick whichever is applicable)
    - o I have not applied for a DSC with NIC-CA earlier.
    - o I have been issued a DSC by NICCA with User-id _____which is Valid/Revoked/Suspended/Expired.

The information furnished above is true to the best of my knowledge and belief. I will comply with the terms and conditions of Subscriber (as in section 40-42 of the IT Act 2000) and those of the Certificate Practice Statement of the NIC-CA. If at a later stage any information is found to be incorrect or there is non-compliance of the terms and conditions of use of the DSC, NIC-CA will not be responsible for the consequences/liabilities and will be free to take any action including cancellation of the DSC**.**

Date:…….
Place:……. **[Signature of Applicant]**

Verification and/or Declaration by Head of Office of Applicant for issuance of DSC

1. This is to certify that Mr./Ms _____has provided correct information in the Application form for issue of Digital Signature Certificate for subscriber to the best of my knowledge and belief.
2. I have verified the credentials of the applicant as per the official records/I have got verification letter from the companies/vendors for the contractual employees from where they have been hired/outsourced, as per the **guidelines given at page 4.**
3. I certify that contractual employee Mr/Ms. _____is working in project _____ at _____. His/her contract *is valid from* ..... to …….
4. **I hereby** authorize him/her, on behalf of my organization to apply for obtaining DSC from NICCA for the purpose as in DSC.
5. **In case of issuance of encryption certificate**, it is further certified that a Policy/Procedure is in place, which describes the complete process for Encryption Key Pair Generation, Backup Procedure, safe-keeping of Backups and associated Key Recovery Procedures. The consequences of loss of the key have been explained to the user and he/she has been advised about securing the key and making it available to relevant authorities, in case of emergency. **I shall not approach NICCA for recovery of private Encryption Key, in case of its loss or otherwise**.
6. For SSL server certificate, I have verified the existence of URL/IP, the IP allocation organisation and physical location of web server.
7. For System Certificate, I have verified the MAC/Serial/IP no of the system/device.
8. It is noted that the organization shall inform NICCA for revocation of DSC on the cessation/superannuation of his/her employment.
9. I have attested applicant's photograph and departmental/employment photo-id of the applicant.

Date:
Place: **[Signature of Officer with Office Seal with name and designation]**

Note: Contractual employees will be issued certificate with maximal validity of one year.

Checklist to be ticked [√] by NIC Coordinator before forwarding to NIC RA/CA Office

[ ] All asterisk (*) marked entries are filled
[ ] Attested & self signed copy of Departmental photo-Id attached
[ ] Signature of Applicant done
[ ] In person verification is done for Class-3 applicant as attached **Annexure-III**
[ ] Payment details filled & DD attached (if required)
[ ] Attested & self signed copy of PAN card attached, if any
[ ] Verification by Head of Office (HO) with Signature & Official Seal

Email:……..... Mobile No.:…… **[Signature of NIC Coordinator with name and designation/Office Seal]**

[*This Form is to be forwarded to the respective RA/CA Office of NICCA*]

[DETATCH PAGE NOs. 3 & 4 BEFORE SENDING THE DSC FORM]

Annexure-I
(Applicant Code & Category)

Code	Category	Code	Category
1.	Govt.	6.	Contractual employee in the above category
2.	Judiciary	7.	MP/MLA
3.	PSU	8.	Elected Member of Village Panchayat/Gram Sabha
4.	Statutory/Autonomous Body	...	...
5.	Sec. 25 Company of Govt.	99.	**Others**

Annexure-II
(Project Code & details)

Code	Project	Code	Project
1.	E-Procurement - NIC portal	21.	Integrated Finance Management System
2.	E-Tendering - NIC portal	22.	Professional Courses Counselling, Admissions & Results
3.	E-Tendering - Others	23.	Public Service Management System (Under the Public Service Commission Act, MP)
4.	E-Courts	24.	e-FMS (Facility Management System Under the MGNREGA)
5.	Supply order placing/DGS&D	25.	UP Technical Education Counselling
6.	E-office	26.	UP Polytechnic Counselling
7.	Income Tax Return Filing	27.	UP B.Ed counselling
8.	Email authentication	28.	UP Medical Counselling
9.	Bhoomi Project	29.	UP VAT (Commercial Tax)
10.	E-District	30.	SSDG/EDS
11.	MNREGA	31.	UP Education Department
12.	Election Commission	32.	Instant Money Order of Deptt of Posts
13.	OASYS (Online Answering Information System for Assembly Questions)	33.	Online Police verification for passport
14.	LRC (Land Record Computerization)	34.	Mee Seva – Government of AP portal.
15.	Treasury (for E-Payment)	35.	ERMS Module - Portal for CEO, Tripura (Election Commission)- private portal
16.	Food & Civil Supplies (for Ration Cards)	36.	Vat Soft for Taxes & Excise Organisation, Govt. of Tripura
17.	Nemmadi - Rural Digital Services	37.	IVFRT
18.	eAPAR	38.	
19.	Health department of Bangalore Mahanagara palike	...	
20.	Web HALRIS and Web HARIS	99.	**Others**

A. Instructions for DSC Applicants

1. NIC-CA abides by the Information Technology Act, 2000, laid down by the Govt. of India. The applicant must read the IT Act 2000 under Resources (https://nicca.nic.in).
2. Subscriber is required to send one copy of DSC request form, duly signed and forwarded by Head of Office to respective RA/NIC-CA. Applicant is advised to retain a copy of the same, which would be required while generating DSC request on line from https://nicca.nic.in
3. The RA/NIC-CA scrutinizes the DSC form, for issue of DSC. If all particulars are in order, a User-Id, password and the profile for the applicant is created using the details submitted. The form will be valid for 90 days only (applicant has to generate key pair request and download certificate within 90 days) failing which, user is required to submit fresh DSC application.
4. It is very important & legally binding to keep the private key securely, for which the applicant must generate key pairs/request using FIPS-140 Level-2 compliant smart card/USB crypto-tokens, which guarantees that private key never leaves the card/token once generated.
5. In case of loss/compromise of DSC, applicant should immediately inform NIC-CA office either by phone 011-24366176 or e-mail at casupport@nic.in or send online revocation request through Member Login from https://nicca.nic.in.
6. For viewing all valid DSCs and CRLs, the user can access the website (https://nicca.nic.in/) under Repository.
7. Smart card/USB crypto-tokens, **allow only maximum 4-10 numbers of incorrect attempts for entering pass phrase/pin**. It is advisable to be careful while entering the pass phrase as repeated incorrect entries shall block the same. On exceeding this limit, special efforts may be required to unblock the device.
8. It is important to note that email-id given by the **applicant is functional** and applicant accesses the same on regular basis as all communication related to DSC like generation, revocation, renewal, expiry details are communicated through the given email-id.
9. SSL Server certificates are not issued for Private IPs; it is issued only for Public IPs. The applicant has to fill the information about IP address allocating Authority.

10. **CERTIFICATE CLASSES, OID & ASSURANCE LEVEL**

Sr. No.	Class of Certificate	OID	Assurance Level/Verification Process
1.	Class-0	2.16.356.100.2.0	It carries no assurance, as it is created with general distinguished name not for an individual
2.	Class-1	2.16.356.100.2.1	Provides minimum level of assurance. Subscriber's identity is proved only with help of Distinguished Name- DN and hence provides limited assurance of the identity.
3.	Class-2	2.16.356.100.2.2	Provides higher level of assurance confirming the details submitted in the DSC Request Form, including photograph and documentary proof in respect of at least one of the identification details.
4.	Class-3	2.16.356.100.2.3	Provides highest level of assurances, as verification process as in addition to the verification process required for the class-2 certificates, the applicants are required to be personally present at Physical Appearance Centre (PAC) for completion of in-person verification process.

11. The DSC applicant with category Govt/PSU/Judiciary/Statutory/Autonomous Bodies/Sector 25 Govt Company has to get his credentials verified from his/her **Head of the office of organisation,** contractual employee has to verify his credentials from his/her employer, the Elected Member (MP/MLA/Village Panchayat/Gram Sabha) has to verify his/her credentials from head secretariat/Panchayat.
12. For any further clarification, user can write to casupport@nic.in or visit the NIC-CA website (https://nicca.nic.in).
13. Issued certificates not downloaded within **2 weeks** shall be revoked without intimation to the applicant and a fresh form would be required for new certificate.
14. Media provided by NICCA is with a warranty of six months against manufacturing defects from the date of issuance. In case of manufacturing defect, the same shall be replaced, but for issuance of DSC, subscriber has to apply with a fresh form.
15. On loss/physical damage of USB Token/Smart Card, new media shall be issued after payment only. Also for issuance of new DSC, the subscriber has to revoke the previous issued (lost) DSC and submit a new form for DSC issuance.
16. The media provided by NICCA shall provide support for platforms as mentioned at NICCA website (https://nicca.nic.in) Also for platform which has become obsolete due to technology advancement, support shall be discontinued.
17. The applicant is responsible for preparation of his/her machine with all relevant software downloads from NICCA website or otherwise for certificate request creation and download from web interface of NICCA at (https://nicca.nic.in).
18. Authentication pin for downloading the certificate shall be sent ONLY to the email specified in the DSC request Form. Request for auth-pin from any other person will not be entertained. In case of accidental deletion/non-delivery of email containing the pin the DSC applicant has to send a mail from email id quoted in the application to casupport@nic.in for resending the authentication pin.
19. **Department photo-id card is essential for completion of physical verification for Class-3 DSC applicant**.
20. **Contractual employees** will be issued **only Class-1/Class-2 Signing** certificates.
21. NICCA IS NOT RESPONSIBLE FOR ANY POSTAL DELAYS OR LOSS OCCURING DURING THE TRANSIT OF THE MEDIA. NICCA CANNOT BE HELD LIABLE FOR THE SAME.

B. Guidelines for verification by Head of Office (HO)

The head of the office is appointed in the Govt. Department/Organisation. The Superior officer not necessarily be the Head of the Office (HO).

a. The **Head of Office (HO) of respective organizations/departments of** DSC requestor has to verify the identity /credentials of applicants. They will be solely responsible for authentication and validation of each subscriber/applicant within the organisation. **The onus of verification lies with Head of office (HO) of the Applicant.**

b. For the DSC applicant with category Govt/PSU/Judiciary/Statutory/Autonomous Bodies/Sector 25 Govt Company the credentials have to be verified by **Head of the office of organisation, for t**he contractual employee credentials have to be verified by his/her employer, for the Elected Member (MP/MLA/Village Panchayat/Gram Sabha) credentials have to be verified by secretary/ Panchayat Head.

c. The **HO of respective organizations/departments** must utilize various procedures to obtain evidence in respect of employment in Government Sector/contractual persons deployed for e-governance project by way of documentary evidence and cross examination of the same with available official records in their office.

d. For contractual employees, the HO has to get verified the credentials from the companies/vendors from where these contractual employees have been hired/outsourced by way of getting a letter on letter head from the company/vendor.

e. **Registration Authorities of NIC (NICRA) are not responsible for verification of credentials of the applicant**.

f. For SSL server certificate the **HO** has to ensure the correctness of URL/IP address and must verify the physical location of web server.

g. For System Certificate the HO has to ensure the correctness of MAC/Serial No./IP address of the system.

h. The HO has to put his signature and official seal.

C. Guidelines for NIC-Coordinator

On receipt of DSC application form, NIC-Co-ordinator must check & tick the Checklist based on information/documents available with the DSC form before forwarding to NIC RA/CA Office. He/She has to put his signature along with official seal. In case of Class-3 DSC applicant, **Annexure-III** has to be dully filled & submitted.

~oOo~

Ref. No.: …… *(To be filled by NICCA/RA Office)*

Annexure-III

Physical Appearance Verification Details

(To be filled by NIC Verifying Officer for **Class-3** DSC applicant)

- ✓ In-person verification of Shri/Smt/Ms……..…….....Class-3 DSC applicant has been carried out on …… (dd/mm/yyyy) at .....(hh:mm).
- ✓ He/she has shown his/her departmental-id bearing No. ……..…….
- ✓ His/her signature & photograph have been matched with signature & photograph available on his/her departmental-id card as well as DSC application form.
- ✓ His/her signature & photograph have been attested by the undersigned as shown below.
- ✓ His/her mobile No. is ……..……..
- ✓ His/her self attested photocopy of departmental-id card is attached herewith.

Paste passport size latest Photograph of Applicant (For class-3 certificate only) **Attested by NIC Verifying Officer**	**Applicant's Signature** (To be signed in the presence of verifying officer) ……..

Attested/verified by:-

Signature of NIC Verifying Officer: …….…….
Name/Designation/Emp. Code
Official Seal/Stamp:
Email:
Telephone/Mob No.:
NIC Centre/Location:

[For Class-3 certificate only - ***This Annexure is to be attached with DSC form & forwarded to the respective NICCA/RA Office***]

Updated on: 31-Mar-2014

Certificate Fee Structure (in Rs.) (For all classes: Class-I, Class-II & Class-III)									
Type of Subscribers	Smart Card Individual/ personal Certificate				USB Token/iKey Individual/ personal Certificate			SSL/Device Cert. (Proc. charge)	Renewal (Proc. charge)
	Smart Card	S.Card Reader	Proc. Charge	Total	# USB eToken	Proc. Charge	Total		
Central & State Government, Judiciary, Attached & Subordinate Offices	227/-	489/-	Nil	716/-	555/-	Nil	555/-	Nil	Nil
Autonomous Bodies, Boards & Corporations, PSUs & Joint Ventures, Statutory Bodies, Commissions & Councils	227/-	489/-	200/-	916/-	555/-	200/-	755/-	200/-	200/-
Note	1. Issuing authority of Office I. Card may be used to ascertain type of Organisation of the applicant. 2. GOI directory website may be used for further reference.								

	3. For ascertaining type of organisation for purpose of applicable fees, discretion of NICCA will be final.
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 as applicable.

Mode of Payment (Demand Draft/RBI Cheque)

i) **DSC form submitted to NICCA RA Office, Delhi/Mumbai/Meghalaya/Tripura**:
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, Bhubaneswar:**
DD in favour of " **DDO, NIC Bhubaneswar**" payable at **Bhubaneswar**

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**

viii) DSC form submitted to NICCA RA Office, Thiruvananthapuram:
DD in favour of "**DDO, NIC Kerala State Centre**" payable at **Thiruvananthapuram**

ix) DSC form submitted to NICCA RA Office, Bhopal:
DD in favour of "**DDO, NIC MP State Centre**" payable at **Bhopal**

x) DSC form submitted to NICCA RA Office, Rajasthan:
DD in favour of "**DDO, NIC** " payable at **Jaipur**

xi) DSC form submitted to NICCA RA Office, Goa:
DD in favour of "**DDO, NIC Pune** " payable at **Pune**

---

xii) DSC form submitted to NICCA RA Office, Hyderabad:
DD in favour of "**DDO, NIC Hyderabad** " payable at **Hyderabad**

---

xiii) DSC form submitted to NICCA RA Office, Jharkhand:
DD in favour of "**DDO, NIC Jharkhand State Centre** " payable at **Ranchi**

---

xiv) DSC form submitted to NICCA RA Office, Uttarakhand:
DD in favour of "**DDO, National Informatics Centre Dehradun** " payable at **Dehradun**

---

xv) DSC form submitted to NICCA RA Office, Chandigarh:
DD in favour of "**National Informatics Centre Chandigarh** " payable at **Chandigarh**

---

xvi) DSC form submitted to NICCA RA Office, Shimla:
DD in favour of "**National Informatics Centre Shimla** " payable at **Shimla**

---

xvii) DSC form submitted to NICCA RA Office, West Bengal:
DD in favour of "**National Informatics Centre** " payable at **Kolkata**

---

xviii) DSC form submitted to NICCA RA Office, Jammu & Kashmir:
DD in favour of "**DDO, NIC State Centre, Jammu** " payable at **Jammu**

Digital Signature (ഡിജിറ്റൽ സിഗ്നേച്ചർ)

ഡിജിറ്റൽ സിഗ്നേച്ചർ എന്തിനു?

1. ഡിജിറ്റൽ ഡാറ്റയുടെ പ്രാമാണ്യം തെളിയിക്കാൻ
2. ഉത്തരവാദിത്തം തള്ളിക്കളയാൻസാധിക്കില്ല
3. ഡിജിറ്റൽ രേഖകൾക്ക് അംഗീകാരം നൽകുന്നതിന്
4. സോഫ്റ്റ്വെയർ ഉപയോഗിക്കുന്നതിന് പ്രവേശനാനുമതി നല്കാൻ (ലോഗിൻ ചെയ്യുന്നതിന്)
5. കമ്പ്യൂട്ടർ ഉപയോഗിച്ചുള്ള സാമ്പത്തിക ഇടപാടുകൾ, മറ്റു പ്രമുഖ നടപടികൾ നിർവഹിക്കുന്ന സ്ഥലങ്ങളിൽ കള്ളയാധാരമുണ്ടാക്കൽ, ഡാറ്റ ഹാനീവരുത്തൽ തുടങ്ങിയവ തടയാൻ ഈ സഗേതിക വിദ്യ സഹായിക്കുന്നു.
6. ഇന്ത്യ തുടങ്ങിയ നിരവധി രാജ്യങ്ങളിൽ നിയമാനുസൃതമായി പ്രാധാന്യം നൽകിയിട്ടുണ്ട്.

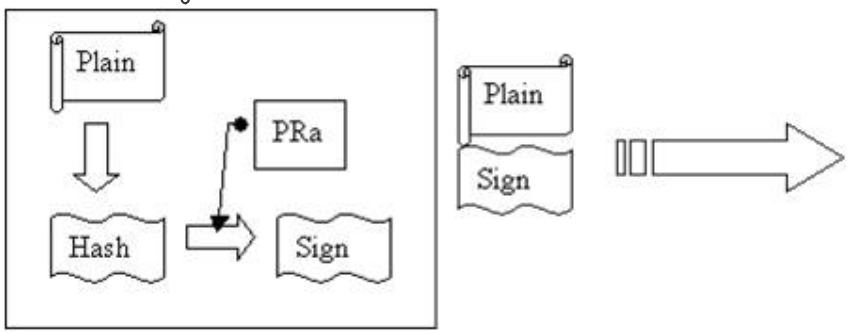
ഡിജിറ്റൽ സിഗ്നേച്ചർ എന്നാൽ എന്ത്?

1. ഗണിതശാസ്ത്രപരമായ ഒരു സമ്പ്രദായം ഉപയോഗിച്ചാണ് “ഡിജിറ്റൽ സിഗ്നേച്ചർ ” പ്രാവർത്തിക മാക്കുന്നത്
2. ഡിജിറ്റൽ രേഖകളുടെ ഗൂഢാക്ഷര ലേഖകൾ (Encrypted data) അസുരക്ഷിതമായ കമ്പ്യൂട്ടർ ശൃംഖലകളിലൂടെ അയച്ചാലും അവ ലഭിക്കുന്ന വ്യക്തിക്ക് അയച്ച വ്യക്തിയുടെ തിരിച്ചറിയൽ സാധ്യമാകുന്നതും പ്രാമാണ്യം ഉറപ്പിക്കുന്നതിനും സാധിക്കുന്നു.
3. Asymmetric Cryptography എന്ന രീതിയിലാണ് പ്രധാനമായി “ഡിജിറ്റൽ സിഗ്നേച്ചർ ” സമ്പ്രദായത്തിനായി ഉപയോഗിച്ച് പോരുന്നത്. അതായത് ഉടമസ്ഥന്റെ കൈവശം സുരക്ഷിതമായി സൂക്ഷിച്ചിട്ടുള്ള ഒരു “Private Key” യും മറ്റുള്ളവർക്ക് നൽകുന്ന ഒരു “Public Key” യും.
4. ഉദാഹരണത്തിന് : സുരക്ഷിതമാക്കേണ്ട ഡാറ്റ ഒരു “Private Key” ഉപയോഗിച്ച് മറ്റുള്ളവർക്ക് മനസ്സിലാകാത്ത വിധത്തിൽ രഹസ്യ കോഡിൽ എഴുതുന്നു. അവ ഉടമസ്ഥന്റെ തന്നെ “Public Key” ഉപയോഗിച്ച് തിരികെ പൂർവ സ്ഥിതിയിലേക്ക് കൊണ്ടുവരാൻ സാധിക്കുന്നു.

സാങ്കേതികമായി ഡിജിറ്റൽ സിഗ്നേച്ചർ ഉപയോഗിക്കുന്ന രീതി.

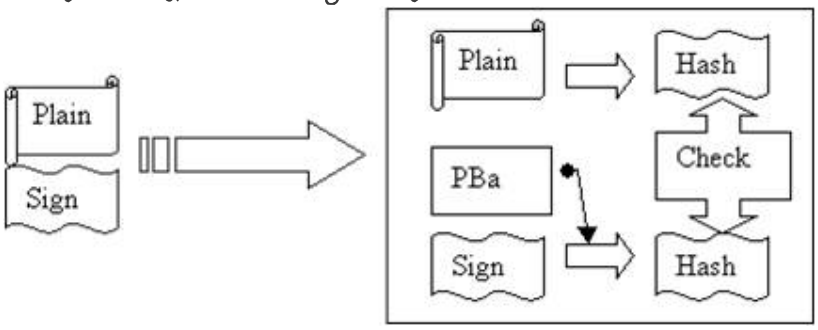
1. ഇതിനായി നാം ഇവിടെ ഉപയോഗിക്കുന്നത് RSA encryption algorithm (Rivest, Shamir, Adleman) മാണ്.
2. സാങ്കേതികമായി സൈൻ ചെയ്യുന്ന പ്രക്രിയ:
3. സുരക്ഷിതമാക്കേണ്ട ഒരു ഡാറ്റ യുടെ ഒരു “Hash” ഉണ്ടാക്കുന്നു.

4. “ഹാഷ്” എന്നാൽ ഇതൊരു ഡാറ്റ യുടെയും ഒരു സാരാംശം അഥവാ സത്ത്. പ്രസ്തുത സത്തിന്റെ വലിപ്പം ഇപ്പോഴും ഒന്നുതന്നെ ആയിരിക്കും. വ്യത്യസ്തമായ ഡാറ്റ കൾക്ക് വ്യത്യസ്തമായ “ഹാഷ്” ആയിരിക്കും ലഭിക്കുക. അതുപോലെ തന്നെ, ഒരേ ഡാറ്റ പലതവണയായി “ഹാഷ്” ചെയ്താലും ഒരേ “ഹാഷ്” തന്നെ ലഭിക്കുകയുള്ളൂ. എന്നാൽ ഒരു ഹാഷ് ഏതു രീതിയിൽ ശ്രമിച്ചാലും തിരികെ അതിന്റെ പൂർവ രൂപത്തിൽ എത്തിക്കുവാൻ സാധിക്കില്ല.
5. ശേഷം പ്രസ്തുത ഹാഷിനെ സൈൻ ചെയ്യുന്ന വ്യക്തിയുടെ “Private Key” ഉപയോഗിച്ച് ഗൂഢാക്ഷരലേഖ ഉണ്ടാക്കുന്നു. ഇവയെയാണ് “Signature” എന്ന് പറയുക.
6. ഇങ്ങനെ ലഭിക്കുന്ന “Signature” റും, യഥാർത്ഥ ഡാറ്റയും സൈൻ ചെയ്ത വ്യക്തിയുടെ “Public Key” യും മറ്റുള്ളവർക്ക് കൈമാറാവുന്നതാണ്.



സൈൻ ചെയ്ത വിവരം സാങ്കേതികമായി ശരിയാണോ എന്ന് പരിശോധിക്കുന്ന പ്രക്രിയ:

1. ആദ്യമായി, ലഭിക്കുന്ന ഡാറ്റ യുടെ ഒരു ഹാഷ് തയ്യാറാക്കുക.
2. ശേഷം “Signature”-നെ സൈൻ ചെയ്ത വ്യതിയുടെ “Public Key” ഉപയോഗിച്ച് തിരികെ പൂർവ്വസ്ഥിതിയിൽ എത്തിക്കുക. ഇന്ങ്ങനെ ലഭിക്കുന്ന ഹാഷും യഥാർത്ഥ ഡാറ്റയുടെ ഹഷും ഒന്നാണെങ്കിൽ അവ ഉപയോഗിക്കാവുന്നതാണ്. ഇല്ലെങ്ങിൽ പ്രസ്തുത ഡാറ്റ ആരോ തിരുത്തി എന്ന് ബോത്യമാകും.



ഡിജിറ്റൽ സിഗ്നേച്ചർ ലഭിക്കാൻ ..

പ്രധാനമായും ഇവയെ ക്ലാസ്സ് 2 എന്നും ക്ലാസ്സ് 3 എന്നും രണ്ടായി തരം തിരിക്കാം. സാധാരണ ആവശ്യങ്ങൾക്ക് ക്ലാസ്സ് 2 എന്ന തരവും, കൂടുതൽ സുരക്ഷിതമായ ആവശ്യങ്ങൾക്ക് ക്ലാസ്സ് 3 യും ഉപയോഗിക്കാം. ഡാറ്റ സൈൻ ചെയ്യുന്നതിനായി ക്ലാസ്സ് 2 തരത്തിലുള്ള സിഗ്നേച്ചർ മതിയാകും

ഡിജിറ്റൽ സിഗ്നേച്ചർ ലഭിക്കാൻ ..

1. ഡിജിറ്റൽ സിഗ്നേച്ചർ ലഭിക്കുന്നതിനുള്ള അപേക്ഷ https://nicca.nic.in എന്ന വെബ്സൈറ്റിൽ നിന്നും ഡൗൺലോഡ് ചെയ്യാവുന്നതാണ്
2. അപേക്ഷ പ്രസ്തുത ഫോർമാറ്റിൽ ഉയർന്ന ഉദ്യോഗസ്ഥന്റെ സാക്ഷ്യപെടുത്തലോട്കൂടി NIC യുടെ സംസ്ഥാന ഓഫീസിൽ നൽകുക. (ആവശ്യമായ തുകയുടെ DD യോടുകൂടി, നിലവിൽ Rs. 555/- ആണ്)
3. വെബ്സൈറ്റിൽ പ്രവേശിക്കുന്നതിനുള്ള ലോഗിൻ അപേക്ഷകന്റെ ഇ-മെയിലിൽ ലഭിക്കും
4. അപേക്ഷയുടെ അവസ്ഥ ഇ-മെയിലിൽ യഥാസമയം അറിയിക്കും.
5. അപേക്ഷ അന്ഗീകരിച്ചാൽ NIC യുടെ വെബ്സൈറ്റിലെ അപേക്ഷകന്റെ ഇ-മെയിലിൽ ലഭിച്ച ലോഗിൻ ഉപയോഗിച്ച് ഡിജിറ്റൽ സിഗ്നേച്ചർ ഡൗൺലോഡ് ചെയ്യാവുന്നതാണ്.
6. പ്രസ്തുത ഡിജിറ്റൽ സിഗ്നേച്ചർ സൂക്ഷിക്കുന്നതിനായുള്ള പ്രത്യേക ടോക്കൻ ഇതോടൊപ്പം ലഭിക്കും
   ടോക്കൻ : USB ഡ്രൈവിൽ ഉപയോഗിക്കാവുന്ന തരത്തിലുള്ള ഒരു സുരക്ഷിതമായ ഉപകരണമാണ് ടോക്കൻ

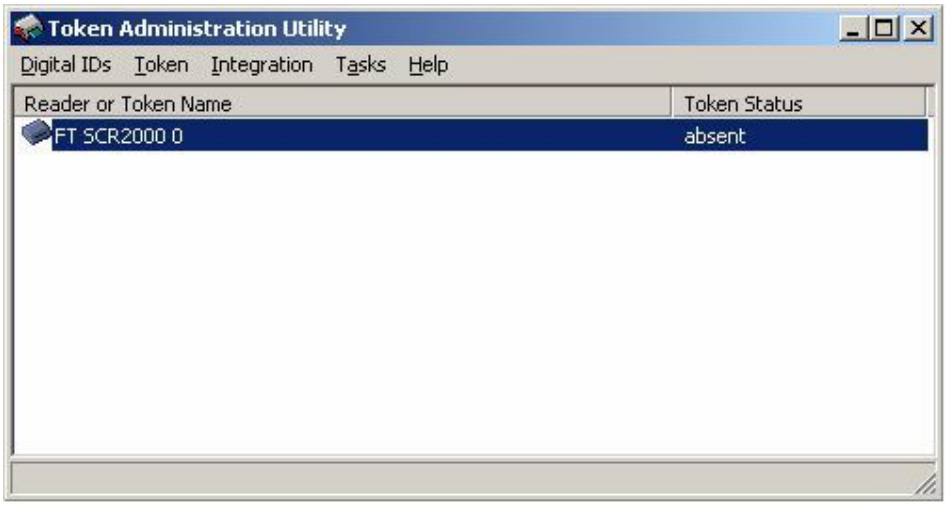
7. Token വിന്യസിക്കുന്നതിനുള്ള സെറ്റപ്പ് ഫയൽ , വിന്യസിക്കുന്നതിനുള്ള സഹായങ്ങൾ തുടങ്ങിയവയും ഈ വെബ്സൈറ്റിലൂടെ ലഭിക്കും
8. അവ സുരക്ഷിതമായ ഒരു ഫോൾഡറിൽ സൂക്ഷിക്കുക

Installation of Digital Signature in USB Token

Token ഉപയോഗിക്കേണ്ട രീതി

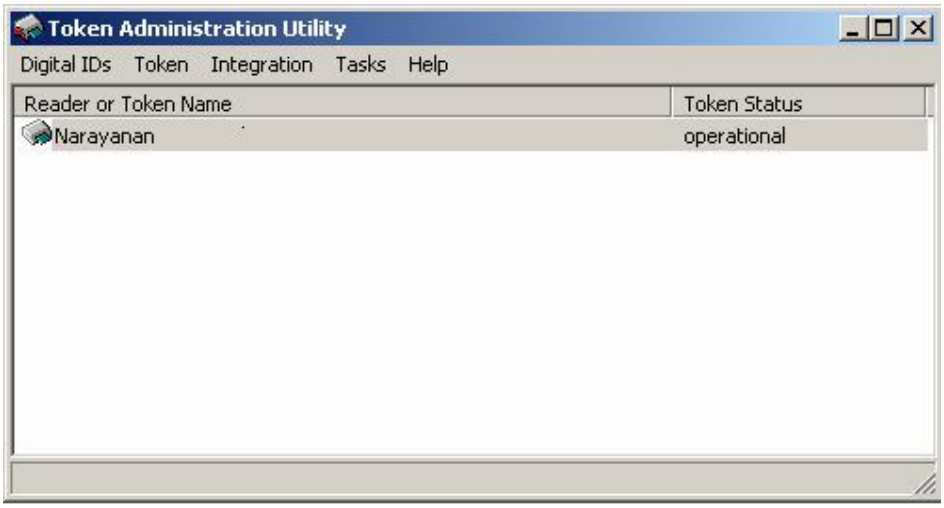
നേരത്തെ പറഞ്ഞിട്ടുള്ളതുപോലെ NIC വെബ്സൈറ്റിൽ നിന്നും (http://nicca.nic.in/html/datakey.html) ഡൌൺലോഡ് ചെയ്ത ഫയലുകൾ (Token വിനിയസിക്കുന്നതിനുള്ള സെറ്റപ്പ് ഫയൽ (Token Driver file) , വിനിയസിക്കുന്നതിനുള്ള സഹായങ്ങൾ, എന്നിവ ഒരു ഫോൾഡറിൽ സൂക്ഷിചിട്ടുണ്ടല്ലോ..അതിനായി ആദ്യം Token ഉപയോഗിക്കേണ്ട രീതി പഠിക്കേണ്ടതായിട്ടുണ്ട് ആദ്യം കമ്പ്യൂട്ടറിന്റെ USB port ൽ Token കണക്ട് ചെയ്യുക

1. അതിനുശേഷം ഡൌൺലോഡ് ചെയ്ത സെറ്റപ്പ് ഫയൽ (Token Driver file) ഇൻസ്റ്റാൾ ചെയ്യുക.
2. ഇൻസ്റ്റാൾ ചെയ്തു കഴിഞ്ഞാൽ കമ്പ്യൂട്ടറിന്റെ പ്രോഗ്രാം മെനുവിൽ നിന്നും ഇൻസ്റ്റാൾ ചെയ്ത സോഫ്റ്റ്വെയർ എടുക്കാവുന്നതാണ്.താഴെ കാണുന്ന സ്ക്രീൻ ഷോട്ട് നോക്കുകToken USB port ൽ കണക്ട് ചെയ്തിട്ടില്ല എങ്കിൽ absent എന്ന് കാണിക്കുന്നതാണ്



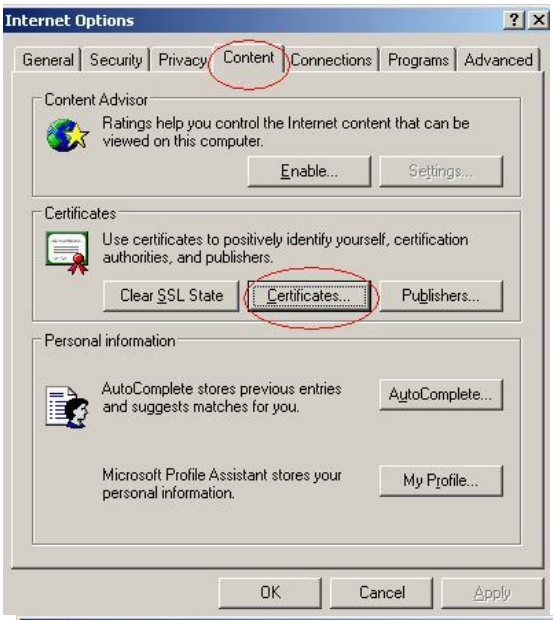
ടോക്കൻ കണക്ട് ചെയ്തു കഴിഞ്ഞാൽ Token Status " operational എന്ന് കാണിക്കും.

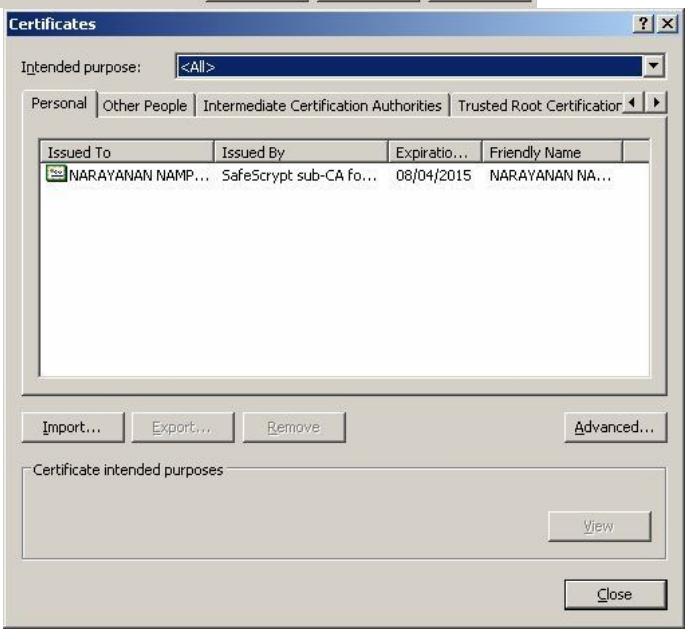
താഴെ കാണുന്ന സ്ക്രീൻ ഷോട്ട് നോക്കുക.



മുകളിൽ കാണിച്ചിട്ടുള്ള സ്ക്രീനിൽ Token Status " operational" എന്നാണ് കാണിക്കുന്നതെങ്കിൽ താങ്കളുടെ Token വിജയകരമായി initialise ചെയ്തു കഴിഞ്ഞു എന്ന് മനസിലാക്കാം

.അതുപോലെ തന്നെ ഇങ്ങനെ Token
ൽ ഇൻസ്റ്റാൾ ചെയ്തിട്ടുള്ള Certificate Token കണക്ട് ചെയ്ത കമ്പ്യൂട്ടറിൽ കാണാവുന്നതാണ്.ഇതിനായി internet Explorer ഓപ്പൺ ചെയ്ത് അതിന്റെ മെനു ബാറിൽ നിന്നും tools മെനുവിലുള്ള internet options സെലക്ട് ചെയ്യുക. താഴെ കാണുന്ന സ്ക്രീൻ ഷോട്ടുകൾ (സ്ക്രീൻ ഷോട്ട് (1), സ്ക്രീൻ ഷോട്ട് (2)) എന്നിവ നോക്കുക.





സ്ക്രീൻ ഷോട്ട് (1)

സ്ക്രീൻ ഷോട്ട് (2)