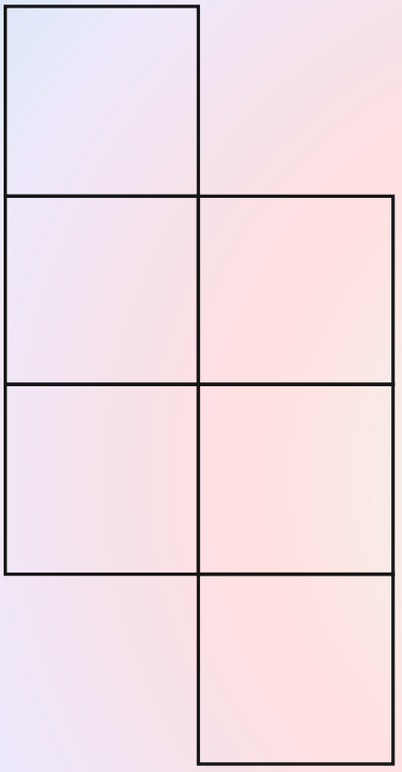
2011

E-Tendering Guideline (For RWD Officers)



This is a guidance note. It provides advice to RWD officials and others on aspects of e-procurement/tendering process. Where procedures are recommended for e-procurement tasks, it is stressed that this guidance note is not intended to replace or supersede guidance on procurement. Changes adopted in e-tendering will not alter any basic principal of procurement process adopted in department or in SBD.

RWD
http://rwd.bih.nic.in
28/08/11

Table of Contents

1. Introduction

This is a guidance note. It provides advice to RWD officials and others on aspects of e-procurement/ tendering process. Where procedures are recommended for e-procurement tasks, these are intended to embody 'best practice', i.e. procedures which in the opinion of RWD meet a high standard of professional competence. This guidance note is in response to the growth in the preparation of tender documents in electronic format. Whether issuing and receiving of all tender documents in electronic format, it is essential that there is a clear understanding amongst all parties concerned as to the nature and intent. By adopting standard practice (both in terms of presentation and content), all parties will benefit from consistency of approach, avoiding ambiguity and reducing frustrations over technical incompatibility. There are many benefits that can flow from the introduction of e-tendering, ranging from simplifying the process, reducing tendering costs, greater transparency, minimizing human errors, to ultimately enabling a fairer assessment between tenders.

It is stressed that this guidance note is not intended to replace or supersede guidance on procurement. It is entirely concerned with the tender process and procedure, and assumes that the most appropriate procurement route has already been selected. ***Changes adopted in e-tendering will not alter any basic principal of procurement process adopted in department or in SBD.*** Only procedural changes will be adopted to implement e-tendering (Example- Digital signature will be used instead of physical signature and digital document will be accepted in place of physical documents)

2. What is e-tendering?

e-tendering is the carrying out of the tendering process using electronic means, such as the internet and specialist e-tendering software applications.

3. Why does e-tendering matter and why should RWD be interested?

E-tendering enables bidders in different geographic location to be notified of an

opportunity, to express an interest, to pre-qualify, to download tender documents and to submit a response. This promotes competition for the tender, and provides a process that is efficient for both the department and bidder and a selection process that is transparent to bidders. Example of good procurement practices that is supported by e-tendering process

- Cost efficient tendering process – e-tendering can deliver savings and benefits to department by enhancing efficiency, competition and control of tendering process. Savings are both cashable (direct) and non cashable (indirect). Cashable benefits result in reduction in expenditure and
- Reduction in overhead costs incurred during the tendering process. Non-cashable benefits include improved management information, better audit trail/ records and increased compliance with process or legislation.
- Greater Transparency – It is important for the tendering process in the department to be fair and for that fairness to be documented. E-Tendering provides a secure history from advertising the tender to awarding a contract. This history is a full audit trail that encourages openness and integrity in all contractual decisions.

  A full audit trail can help department if they face request for information from the public, but can also support the department if they face legal action over the award of a contract.
- Standardize the tender process – e-tendering can ensure that a standard process is applied to all tenders. This enables the department to devolve the tender process to officers, whilst maintaining control over the award of contract.
- To have detailed knowledge of departmental tenders – e-tendering provides detailed information on all past and present tenders. Officers can observe and manage response to the tender through the department e-procurement website.

4. E-tendering system adopted by RWD

- Initially Department had adopted e-tendering for procurement of PMGSY works with the support of NRRDA and NIC and first tender was floated in June 2010.
- E-procurement/ tendering software GePNIC developed by NIC was made available for this purpose.
- Overall project management is being carried out by NIC & NICSI and they will be responsible for project infrastructure management.
- The MoRD/ NRRDA have provided approvals, directions and funds for the project.

- RWD has registered domain ID http://pmgsytendersbih.gov.in for e-tendering process and this was used for all procurement of PMGSY works.
- Later Department decided to adopt this for all procurement works of department. Department circular notified that all tender value above 25 lakhs will compulsorily be procured through e-tendering system.

5. System requirement for e-tendering

- Computer system with Linux/ Windows 2000, XP or higher Operating System with Antivirus.
- Web Browser Internet Explorer version 7.0 or higher.
- Legally valid Digital Signature Certificate (DSC) certified by CCA, India.
- Broadband Internet Connection.
- Printer.
- UPS.

6. Pre-requisites

- Broadband Internet connection should be available.
- One should have administrative rights to install the DSC software.
- When the system is switched on, the DSC must be attached with the USB port.
- DSC driver should be installed from the resource CD.
- JRE 1.6 should be installed.
- One should be a Registered Department User/ Bidder to access the Web application.

7. Digital Signature Certificate (DSC) and Digital Encryption

A Digital Signature Certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender cannot revoke or deny. Accordingly, Digital Signature Certificate is a digital equivalent of a hand written signature which has an extra data attached electronically to any message or a document.

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. 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.

- To work on the system all users will require to have Class II or Class III e-token based Digital Signature Certificate (DSC). Department official will have to use DSC with encryption facility.
- Data Encrypted with Public Key, can only be decoded by corresponding Private Key. No one can access decrypted data without private key.
- It is advisable to department officers to obtain DSC from NICCA.
- Department officers are required to send one copy of DSC request form, duly signed and forwarded by Head of Office through State Informatics Officer, NIC Bihar Sate Centre, along with required amount of DD in the name of "Accounts officer, NIC" payable at New Delhi.
- Details of management procedure of NICCA, DSC are available on http://nicca.nic.in/ .
- In case, during the process of a particular Tender, the Authorized User loses his/ her Digital Signature Certificate, he/ she may not be able to work on tender. Hence the Authorized user is advised to keep DSC safely under proper security.
- Bidders can get DSC through Indian Government recognized CA (such as n-code, TCS, siffy etc) and department has no role in this regard, NICCA issues DSC only to Government officials.

8. Creation of Department User and role base access

- Access to website is on the basis of rights allocated to a User or Group of Users.
- For department user no need to get enrolls in the system. The department users are created by the Nodal officers of the department and different roles are assigned to them. Following are the list of roles and functions assigned to a department user. One or more roles assigned to a department user.

	Role	-	Functions
○	Procurement Officer Admin	-	Creates a New Tender/ Corrigendum
○	Procurement Officer Publisher	-	Publishes the Tender/ Corrigendum created
○	Procurement Officer Opener	-	Conducts the Bid opening process
○	Procurement Officer Evaluator	-	Updates the Bid Evaluation details in the AOC
○	Auditor	-	Auditing of Tendering activities

- Depending on the roles assigned, the department users will carry out the relevant activities which are briefed in detail in the User Manual available on web site.

9. Steps of e-tendering to be followed by Departmental Officers

There are seven major steps needed to be adopted in procurement process

i. Online Tender Creation: The department users who have access level of new tender/ corrigendum creation will be able to create tender/ corrigendum on line and it will be available to publishing authority to view and publish the same on portal. Tender/ corrigendum will not be visible to the contractor/ Bidders till it is published at due date and time.

Soft copy of approved tender documents NIT, SBD, BOQ is to be uploaded during the tender creation level. NIT and SBD should reflect all the e-tendering process and critical dates and times. NIT will have two version one short NIT required to be published in newspaper and other detail NIT mentioning all the term and conditions. Both versions will be uploaded on the website. Changes in SBD will simply reflect the required procedure to be adopted for e-tendering and ***will not alter any basic principal of procurement process mentioned in SBD.***

BOQ has to be created in excel format provided in the website. BOQ thus created should be protected by password. Participating bidders will only be able to fill unlocked cell of name, rate and less or excess values in the protected sheet.

Before uploading the tender documents ex- NIT, SBD and BOQ it should be approved on file and hard copy from competent authority. Tender creating and publishing officers whose DSC is attached with tender document will be responsible for any discrepancies.

Minimum Two officers from the online list of officers will be assigned for bid opening.

ii. Online Tender/ Corrigendum Publishing: The Department users who have access level of tender/ corrigendum publishing will view the tender / corrigendum created and if it is proper then he/ she will publish the same using his/her digital signature certificate. Publisher will be responsible for publishing all tender documents and corrigendum. The use of e-tendering should not affect

the standard procedure dealing with the tender period.

iii. **Bid Opening:** The Department users who have access level of Bid opening will able to open (by decrypting) the bid as per the time schedule. She/he will have to use their digital Signature Certificate. Two officers assigned for the bid opening at the stage of tender creation will only be able to decrypt and open the bid. When both of them have decrypted with their DSC then only tender will be available for further processing. Bid opener will accept or reject the bid at first place as per EMD and tender amount received by the department or not before the bid opening time.

iv. **Technical evaluation:** Technical evaluation will be done by the bid committee as per the existing procurement process of the department. Bid committee report is to be uploaded by the bid opener and date and time will be fixed for financial bid opening. Any dispute by the bidders regarding file uploaded by the bidder in the tender should be entertained only with the copy of acknowledgement (received by the bidder after submitting online tender) and application mentioning the problem.

v. **Financial bid opening:** Same officers who were assigned for bid opening at the time of tender creation will be able to decrypt the technically accepted bids. Bid opener will have to verify each BOQ received by the bidder and only those BOQ should be accepted which has been submitted in the BOQ uploaded by the departmental officers with their DSC. Any changes in protected BOQ by the bidder should be out rightly rejected. Comparative chart is automatically generated by the system and this should be used for financial evaluation.

vi. **Financial evaluation:** Financial evaluation should be done as per existing procurement process of the department. Negotiation with L1 can be done at this stage and final agreed rate and amount should be uploaded along with the scanned copy of committee decision report.

vii. **AOC:** Award of Contract (AOC) is the final stage of e-tendering process. The Department users who have access level of Bid evaluation will be able to update the bid evaluation details in AOC.

The entire tender should be processed till AOC and it should not be left in between. Details of AOC will complete all stages of tendering process and will be available for online public viewing.

viii **Auditor:** The Department users who have access level of Auditor will be able to Audit all tendering activities of department in e-tendering.

10. Security features- role base access, time base access, time stamping

- **Role Base Access:** Access to website is on the basis of rights allocated to a User

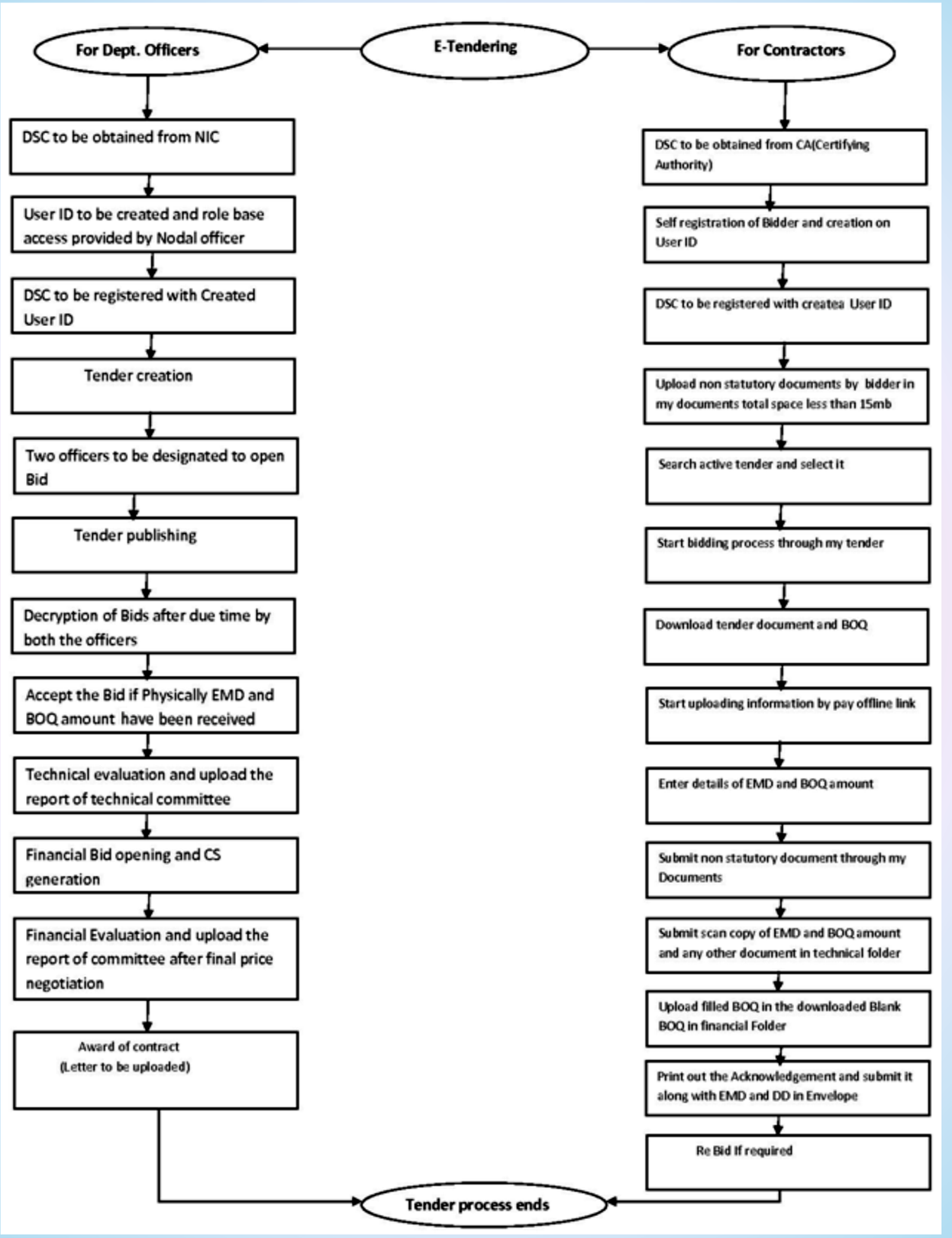
or Group of Users. This ensures that Tampering by unauthorized person is not possible.

- **Time Based Access:** No activity can be carried out before due date & Time for e.g. Tender cannot be opened even by authorized User before due date. Tenders cannot be submitted after due date and time. Tender cannot be opened before due date and time. Server Time cannot be tampered as it is mapped to National Standard Time Server.
- **Time Stamping:** All processes are time stamped and IP address of computers are noted down that participate in the tendering process for additional security features.

11. Future projection

- ❖ More training session will be organized at Circle level for Departmental Officers and Contractors. Sufficient Infrastructure and Trainers will be deputed to achieve this target.
- ❖ Presently e-tendering is being adopted at the level of Nodal officers of different schemes afterward it is expected that Works Division will become capable through proper training to use e-tendering process.
- ❖ Software **up-gradation** and **new features addition** is continuous process and it will be adopted by the department when and where they are included in the e-tendering software.
- ❖ Currently offline payment mode is only the option available for the bidders and this dilutes some benefit of e-tendering process. Department is in consultation with NIC, NICSI, NRRDA and other departments in this regard and it is expected that **online payment mode** will soon be adopted by the Department with the help of Banks and other financial institute.
- ❖ Department expects that e-tendering software and other online reporting software are **linked and synchronized** so that duplication of online work may not happen. Department is also working in this regard so that it will help to improve management and monitoring system of works in department.
- ❖ Department is also hopeful that all file movement will be digitized. For electronic file movement software Currently **IWDMS** (Integrated Work Flow Management System) is in the process of being adopted in selected department of Bihar Government. RWD is also hopeful to adopt this system. This will help online file movement and decision making which are currently being done offline in e-tendering software.

12. Flow Chart of E-tendering



13. Do's and Don'ts

Do's

i. NICCA provides blank token and Digital Signature should be installed in the token so that it may be used as DSC token.
ii. All the relevant software should be installed in the computer, such as DSC software, Java, Pdf reader etc.
iii. Model BOQ format available in the website should be used for preparation of BOQ.
iv. Check all tender documents created in website before publishing it.
v. Authorized officers should decrypt the tender at designated time.
vi. Online tender acceptance of bid should be done only if BOQ amount and EMD has been physically received.
vii. Name of the member of technical Bid Committee and their decision should be uploaded at the time of online Technical Evaluation.
viii. Online Comparative Chart should be generated at the time of financial bid opening.
ix. Rate negotiation may be performed with L1 if required and agreed rate should be uploaded at the time of Financial Bid evaluation.
x. AOC (Award of Contract) should be necessarily uploaded on the website.

Don'ts

i. Don't try to create User ID and Password to use website, for Departmental officers it is provided by Administrative Officer.
ii. Don't use BOQ format other than provided in website.
iii. Don't upload unlocked excel sheet of BOQ.
iv. Don't accept online bid without comparing the received EMD and BOQ amount physically.
v. Don't accept BOQ at the time of online financial bid opening if it has not been provided in the format uploaded at the time of tender creation.

14. Glossary / Abbreviations

AOC

Award of Contract.

APPLICATION SYSTEM

A family of products designed to offer solutions for commercial data processing, office, and communications environments, as well as to provide simple, consistent programmer and end user interfaces for businesses of all sizes.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (See also verify (a digital signature))

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

BOQ

Bill of Quantity.

CCA

Certificate Certifying Authority.

CD

Compact Disk (Storage media).

CERTIFICATE

A Digital Signature Certificate issued by Certifying Authority.

CERTIFYING AUTHORITY (CA)

A person who has been granted a license to issue a Digital Signature Certificate under section 24 of Information Technology Act, 2000.

CERTIFICATE CLASS

A Digital Signature Certificate of a specified level of trust.

DIGITAL SIGNATURE

Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.

DSC, DIGITAL SIGNATURE CERTIFICATE

Means a Digital Signature Certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000.

EMD

Earnest Money Deposit.

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

GENERATE A KEY PAIR

A trustworthy process of creating private keys during Digital Signature Certificate application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital Signature Certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HARD COPY

A copy of computer output that is printed on paper in a visually readable form; e.g. printed reports, listing, and documents.

ID, IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

JRE

Java Run Time Environment.

KEY

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation,

signature generation, or signature verification).

KEY GENERATION

The trustworthy process of creating a private key/public key pair.

KEY PAIR

In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

NIC

National Informatics Centre.

NICCA

NIC Certifying Authority

NIT

Notice Inviting Tender.

NRRDA

National Rural Road Development Agency.

ON-LINE

Communications that provide a real-time connection.

PASSWORD (PIN NUMBER)

Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.

SBD

Standard Bidding Document.

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative.

SERVER

A computer system that responds to requests from client systems.

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

TOKEN

A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

USB

Universal Serial Bus (Port provided in computer to attach other hardware).

VIRUS

Means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

WEB BROWSER

A software application used to locate and display web pages.

ZIP

To Digitally compress file.

15. Appendix

- NICCA website http://nicca.nic.in for DSC related information
- E-tendering website http://pmgsytendersbih.gov.in for e-tendering information.
- Departmental website http://rwd.bih.nic.in for departmental information.
- PMGSY Home page http://pmgsy.nic.in
- Bihar Government Website http://gov.bih.nic.in
- Information and Public Relation Department of Bihar Government http://prdbihar.gov.in

Steps to install Digital Signature Certificate and encryption Certificate in the blank token / Card provided by NICCA

Hardware/ Software requirements for certificate installation

Hardware: Computer, Internet Connection and Card Reader (For Card type token)

Software: Windows Operating System, Java, Internet Explorer and Browser Setting (Enable Active X Control)

STEP1: Installation of e-token driver

For Star key token

- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Go to Support and click Download-Datakey Reader S/W
- Click on option Starkey e-Token SDK Download) and save it on desktop or any desired folder.
- Unzip this file with Winzip. There are two folders in it (i) - SafeSign-Identity-Client-2.3.6.SCI- admin and (ii) - StarKey100V30_2Readers)
- Double click to install SafeSign-Identity-Client-2.3.6.SCI-admin and StarKey100V30_2Readers
- Reboot your system.

For Card Reader Drivers

- Plug in Card reader in to USB port of your system
- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Go to Support and click Download-Datakey Reader S/W
- Click on option 7 Starkey e-Token SDK Download) and save it on desktop or any desired folder.
- Unzip this file with Winzip. (There are two folders namely – 32 and 64 in the folder eToken G&D StarKey)
- Depending on the machine (32 bit or 64 bit) install SafeSign-Identity-client-3.0.33.SCI-Admin.exe from the directory.
- Reboot your system.

STEP2: Initialize your e-Token.

- Insert e-Token in USB Port.

- Click Start Programs Safe Sign Standard Token Administration.
  Token Administration Utility window will open. In this window under 'Reader or Token Name' and 'Token Status' a number of items will be displayed. When you insert your card in to reader the token status for FT SCR2000 0 will change from absent to Uninitialized. This means Token drivers are installed properly.
- Right Click on Blank Token and click Initialize. A new window will open. Here enter the following details.
  1. Token Label: Your Name,
  2. Enter PUK: 0000 and confirm the same.
  3. Enter PIN: 1234 or as desire and confirm the same and click OK.

This will initialize your Token and your Token is ready for certificate generation.

NOTE: Please remember / memorize the Token Password as this will be required at the time of certificate generation and whenever you are going to use it in your application

STEP3: Browser Settings

Active-X controls need to be enabled in your Internet browser. In order to ensure this, please do the following:

- Open a browser window
- Go to Tools **>>** Internet Options **>>** Security **>>** Custom level
- Click 'Custom Level' and set security level as 'Medium' and enable all Active-X controls

STEP4: Enrollment Instructions - Generating Key Pair

When you enroll for a digital certificate, cryptographic keys are generated and stored on your USB Token. For generating the Key Pair on USB Token select the appropriate CSP – (SafeSign Standard Cryptographic Service Provider)

- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Click Member Login and login with User-id / Password issued by NIC Certifying Authority
- Insert your e-Token in the USB port
- Click Enroll for generating your Digital Certificate key pairs. (An Electronic Form will appear which is self-explanatory. You are required to fill in Your details as mentioned in Digital Signature Certificate Request Form and submitted to NICCA)
- Certificate Class: It is fixed at the time of User-id creation.
- Certificate Type: Select Signing Certificate.
- Do you have a certificate request already generated? Click No

- Fill in the seven mandatory fields under "Contents of your Digital Certificate"
- Cryptographic Service Provider: Select SafeSign Standard Cryptographic Service Provider (for safe sign token). Do not Scroll down the page with mouse wheel; it changes the selected option. To avoid this move arrow away from selected option and click left mouse-button once.
- Check all entries once again and Click Generate Request.

(A confirmatory message will be displayed on your computer screen. Read it and Click OK). At this time you will be prompted to enter Passphrase/PIN of the eToken.

- Enter Passphrase / PIN of the e-Token.

Your Digital Certificate key pair will be generated on eToken.

A request Number will also be generated and displayed on your computer screen. Please note it down for further follow up.

No need to go to Step-2. Go to Step-3 or Step-4 (mentioned on website) to view the status of your DSC Request or simply click View Status on the top of the page.

Once RA administrator and CA Administrators process the certificate request, your Digital certificate will be generated and authentication PIN will be sent to you on your email address.

STEP5: Downloading Digital Certificate on E-Token

- Insert your e-Token in the USB port
- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Click Member Login and login with User-id / Password issued by NIC Certifying Authority
- Click on View Status - This will show the status of your DSC request. If the certificate has been generated a link will be provided on the DSC request number.
- Click on DSC Request Number
- Enter Authentication PIN (Ten Digit Alphanumeric code - all CAPITAL LETTERS) and click on Download. First Certificates of CCA and NICCA will be downloaded on your system and then your certificate will be downloaded on the e-Token.

STEP6: Request for encryption Certificate

- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Click Member Login and login with User-id / Password issued by NIC Certifying Authority
- Click Enroll for requesting of encryption certificate. Requesting for encryption certificate should be done only after installation of signature certificate. An Electronic Form will appear which is self-explanatory. Officers are required to fill

in their details as mentioned in Digital Signature Certificate Request Form and submitted to NICCA.

- A request Number will also be generated and displayed on your computer screen. Please note it down.
- To view the status of your encryption certificate request simply click View Status on the top of the page it will show pending against your request number.

STEP7: Downloading encryption Certificate on E-Token

- Once NICCA process the encryption certificate request, your Digital certificate will be generated and authentication PIN will be sent to you on your email address.
- Login on nicca site with your user ID and Password.
- Click on View Status on the top of the page and proceed if request number shows certificate generated.
- Click encryption certificate request Number.
- Enter Authentication PIN (Ten Digit Alphanumeric code - all CAPITAL LETTERS) and click on Download.
- Install encryption certificate by importing the certificate in the token.

STEP8: Download and Install Certificate Chain

When you download your certificate on e-Token, the certificate chain is also downloaded and installed in your browser. In case you are using your certificate (e-Token) on some other system, make sure certificate chain is also installed on that system. To download and install certificate chain follow these steps.

- Open the Browser and go to https://nicca.nic.in or http://164.100.20.212.
- Click Certificate Chain (CCA & NICCA Certs)
- Click on Download (Left Hand Side Window pane) and Click Download Certificate Chain (,zip format). Save this file on Desktop or your desired location.
- Unzip this file with Winzip. This will display a number of files.
- Right click on chain2 (Including nicca2 & cca2 certs). p7b and click install certificate. This will install the certificate chain (nicca & cca certificates).

View the certificate details through token software and confirm that both Signature certificate and Encryption certificate have been installed in the token/ Card.