PKI Case Studies

Agenda

- Need for a Digital Signature Certificate
- Getting a Digital certificate
- Procedures for Getting Certificates for Members of Government Agencies
- Case Studies – E-Procurement, E-Shopping
- Some Risks and Precautionary Measures

DSC - Where do you need ?

- Individuals / Members on behalf of Companies
  - E-Filing
    - Individuals, All companies, filing their IT returns online
  - E-Procurement
    - Supplier/Vendors participating in E-procurement process
  - E-Ticketing
    - Accredited agents of IATA, for booking tickets in IRCTC
  - E-Payments
    - E-Transfer – through/between banks;
  - E-Voting
    - Already adopted in some countries!
- Servers / Machines
  - E-Trading / E-Shopping
    - Web Servers hosted by Merchants

Certifying Authorities in India

- 8 CAs licensed under the National Root CA
  - SafeScrypt (www.safescrypt.com)
    - Sify Comm. was formerly known as SafeScrypt Ltd.
    - Sify Comm. is also ***India's first Licensed Certifying Authority (CA)*** under the IT Act 2000

Certifying Authorities in India

- **IDRBT** (**http://idbrtca.org.in**)
  - IDRBT CA issues certificates for Banks and Financial Institutions for RBI's PKI enabled applications
  - To Enroll Go to https://services.idrbtca.org.in/

Certifying Authorities in India

- **National Informatics Centre** (https://nicca.nic.in)
  - Issues and maintains digital certificates for usage within the Government of India domain.

Certifying Authorities in India

- **Tata Consultancy Services** (www.tcs-ca.tcs.co.in)
  - Issues various types of Digital Certificates.
- **Customs and Central Excise** (http://icert.gov.in)
  - Issues Certificates to CBEC's trading community, it's officers and related agencies.
  - iCERT CA functions under the Directorate General of Systems and Data Management (DGSDM), Customs & Central Excise, which is a subordinate office of the CBEC.

Certifying Authorities in India

- **MTNL** (www.mtnltrustline.com)
  - **MTNLTRUSTLINE** provides Digital Certificates to entities including but not limited to Individuals, Organizations, Servers and Network Devices within the framework of IT-Act 2000.

- **nCode** (www.ncodesolutions.com)
  - **(n)Code** provides DSC to individuals, corporates and governments to secure online B2B/B2C applications and other online transactions.
  - It has promoted a portal called www.nprocure.com offering end-to-end electronic procurement services provider. **(n)Code** also designs and builds world class data center infrastructures.

Certifying Authorities in India

- **3i Infotech (e-Mudhra)** – (http://www.e-Mudhra.com)
  - provides digital signatures that guarantee secure and authentic online transactions for the customer.

Approximately 12,00,000 Digital Certificates have been issued by all these CAs combined

Classes of Certificates

- 3 Classes of Certificates
  - Class – I Certificate
    - Assurance Level: Minimum level of assurance; Subscriber identity is proved only with the help of Distinguished Name – DN
    - Suggested Usage: **Signing certificate** primarily be used for signing personal emails and **encryption certificate** is to be used for encrypting digital emails and **SSL certificate** to establish secure communication through SSL

Classes of Certificates

- Class – II Certificate
  - Assurance Level: Conforms the details submitted in the form including photograph and documentary proof
  - Suggested Usage: **Signing certificate** may also be used for digital signing, code signing, authentication for VPN client, Web form signing, user authentication, Smart Card Logon, Single sign-on and signing involved in e-procurement / e-governance applications, in addition to Class-I usage

Classes of Certificates

- Class – III Certificate
  - Assurance Level: Highest level of Assurance; Proves existence of name of the organization, and assures applicant's identity authorized to act on behalf of the organization.
  - Suggested Usage: **Signing certificate** may also be used for digital signing for discharging his/her duties as per official designation and also **encryption certificate** may also be used for encryption requirement as per his/her official capacity

How to get a Digital Signature Certificate?

Getting a Public Key Certificate

- Consists of 2 stages
  - Stage 1: Online Enrollment
  - Stage 2: Validation of Identity
    - Your credentials will be validated before issuing you digital certificate

Stage 1: Online Enrollment

- Visit any of the licensed CA's website and fill in the details
  - Submit your information
  - Some of the mandatory fields include
    - First name and last name
    - Email Address
    - City, State, Country
    - Permanent Address and Pin Code

Stage 1: Online Enrollment Cont…

- Challenge Phrase
  - You will be asked to provide a "challenge phrase"
  - You require this passphrase to renew, replace or revoke your certificate
  - CA does not have access to your challenge phrase
  - Hence it is your responsibility to safeguard it!.
- Your public-private key pair will be generated
  - Private keys will be of 1024 bits in length
  - If you are using IE browser, then you must select the Microsoft Enhanced Cryptographic Provider Option.
    - Remember that, this stores your private key in the IE browser itself

Stage 1: Online Enrollment Cont…

- If you have a smart card or USB token to store your Digital Certificate, you may select the Datakey RSA CSP (Cryptographic Service Provider) from the drop-down list box.
  - The CSP will give you the private keys that are 1024 bits in length
- Your public key will be sent to the CA for creation of the digital certificate
- Make the Payment!, by choosing one of the options.

Stage 2: Validation of Identity

- You need to be present before a trusted third-party who can identify and certify you
  - The third-party could be your banker, performing the authentication function
  - The banker will attest your name, signature and photograph based on the records with the bank
  - Some widely recognized, government-issued Photo-IDs are:
    - Passport, Driving License, PAN card, Voters ID card, Service Identity card issued by any State / Central government to its employee

Stage 2: Validation of Identity

- In short, you must
  - Complete the registration form
  - Have your banker attest the letter
  - Submit all documentation to the CA
- Your name, Email Id, Address that you enter in the form must be exactly as you have provided in the online enrollment

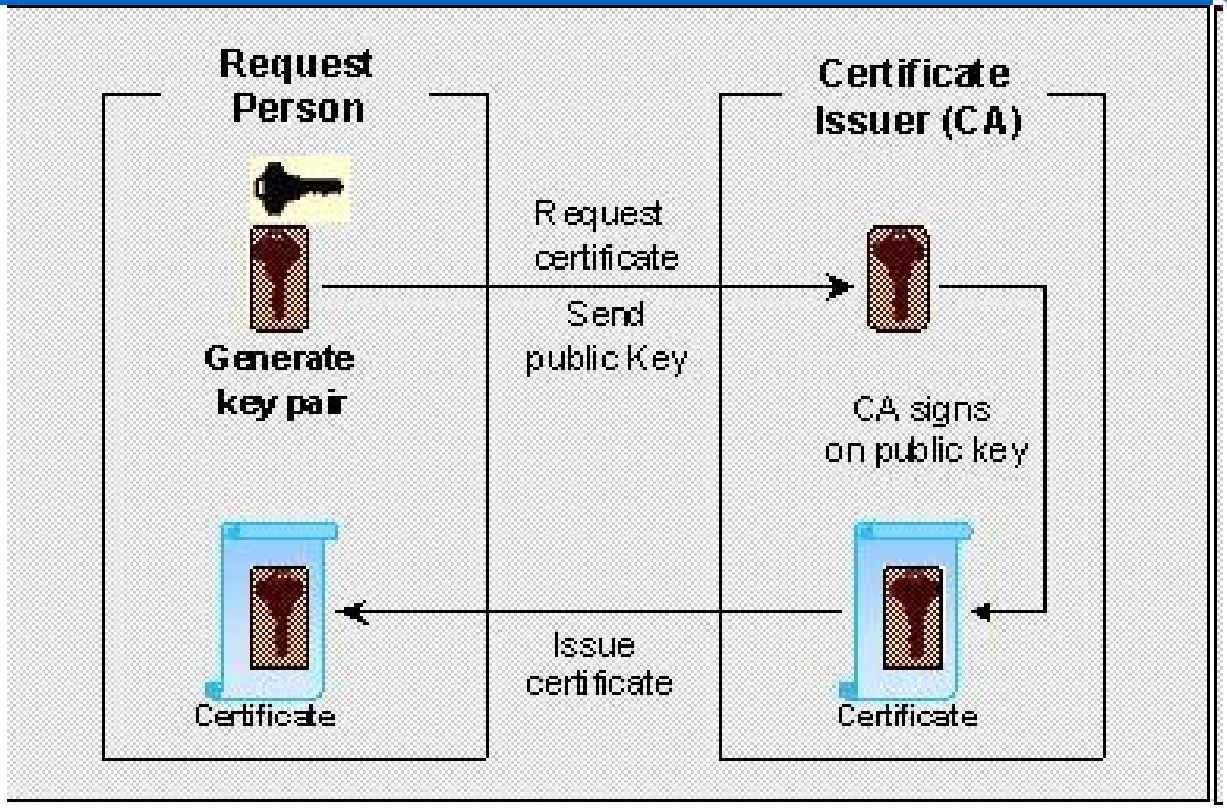
Certificate Issuance

- CA will begin the validation process, after it had received all the duly completed documents
- If there is any discrepancy with the documents submitted, CA will send you an e-mail with the instructions to either re-enroll or to submit corrected documents
- After the validation process is completed, and upon receiving the payment, CA will issue your digital certificate
- You will receive an email with a URL, a PIN number and the instructions to pick your digital certificate

Getting the Certificate

- Visit the URL given in your email, and enter the PIN number into the field on the page, and then 'Submit' it.
- Pick up the Digital certificate using the same computer and browser that you used for enrolling for the digital certificate
- The next option will lead to the installation of the certificate in the browser.

Process - Explained



- Applicant generates his/her own key pair and sends the public key to the CA with some proof of his/her identification
- CA will put the public key in a new certificate, digitally sign the certificate using its private key and then send the certificate to the applicant

Digital Certificate Installation & User Guide

For Class-3 Certificates

TATA CONSULTANCY SERVICES

Stage-1 | Getting Started

Hardware/Software Requirements

Getting Started | Enrollment Prerequisites

System Requirements

Ensure that the following system requirements are met:

- **Operating System:** Windows 98, NT, 2000, XP
- **Browser:** Internet Explorer 5.5 and above
  Click here to download the latest version of Internet Explorer

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
- Click 'Default Settings' and set to 'Medium'

Getting Started | Smart Cards / USB Tokens

- Smart Cards and USB Tokens are portable devices built to provide the highest level of security to the information contained within them. By storing your cryptographic keys and certificates in such devices, you can ensure a much higher level of protection than by simply storing them in your browser.

- In order to use Smart Cards or USB Tokens for storing your digital certificates, you will need to install the required drivers and software before enrolling for your certificate.

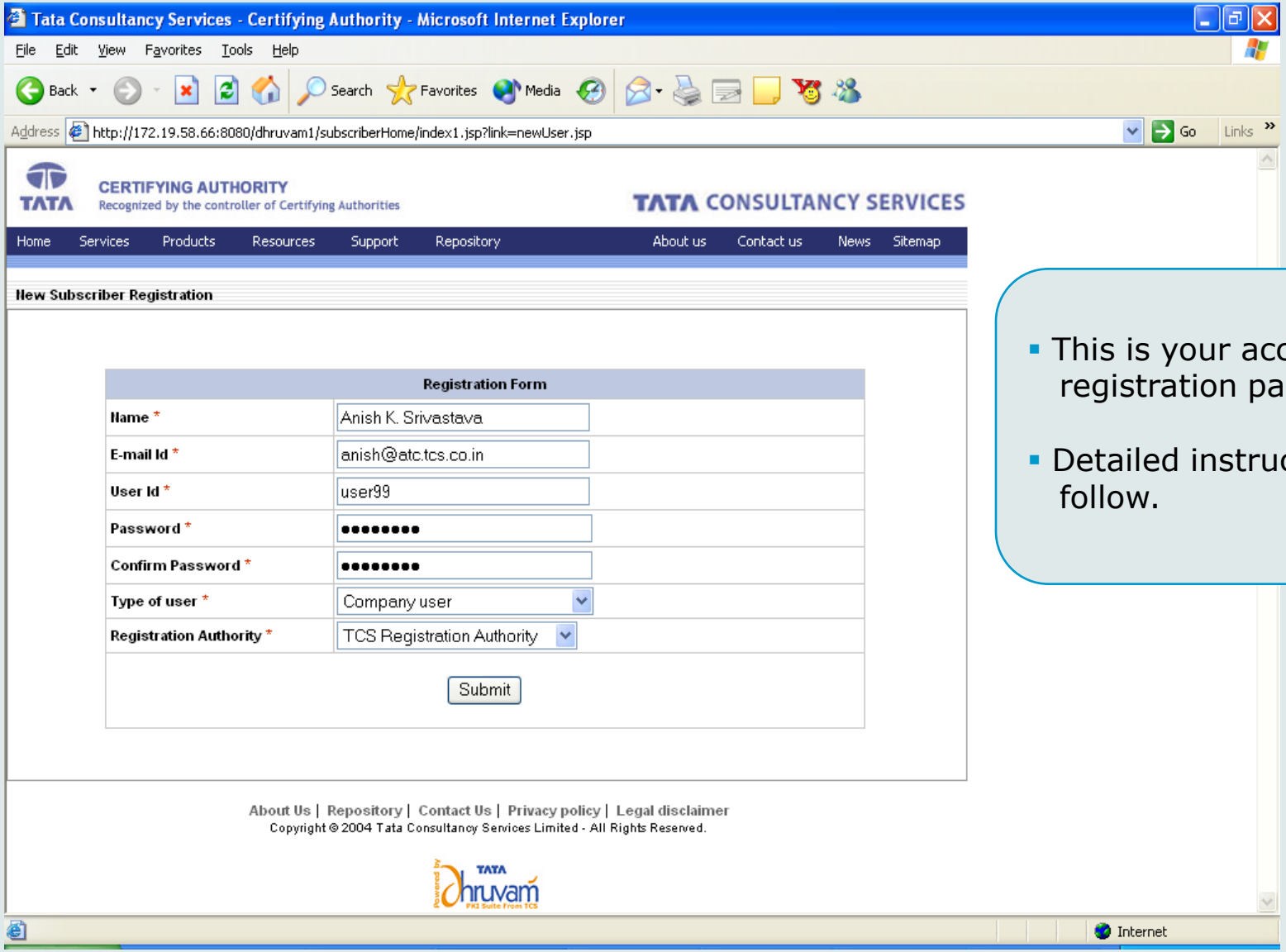
Stage-2 | Registration

Create your user account

Digital Certificates | Account Registration

- In order to enroll for and manage your digital certificates, you will need to register for a user account.
- Click here to go to the TCS-CA Trust Portal
- Click the 'New User? Register' link

Digital Certificates | Account Registration



- This is your account registration page.
- Detailed instructions follow.

Digital Certificates | Account Registration

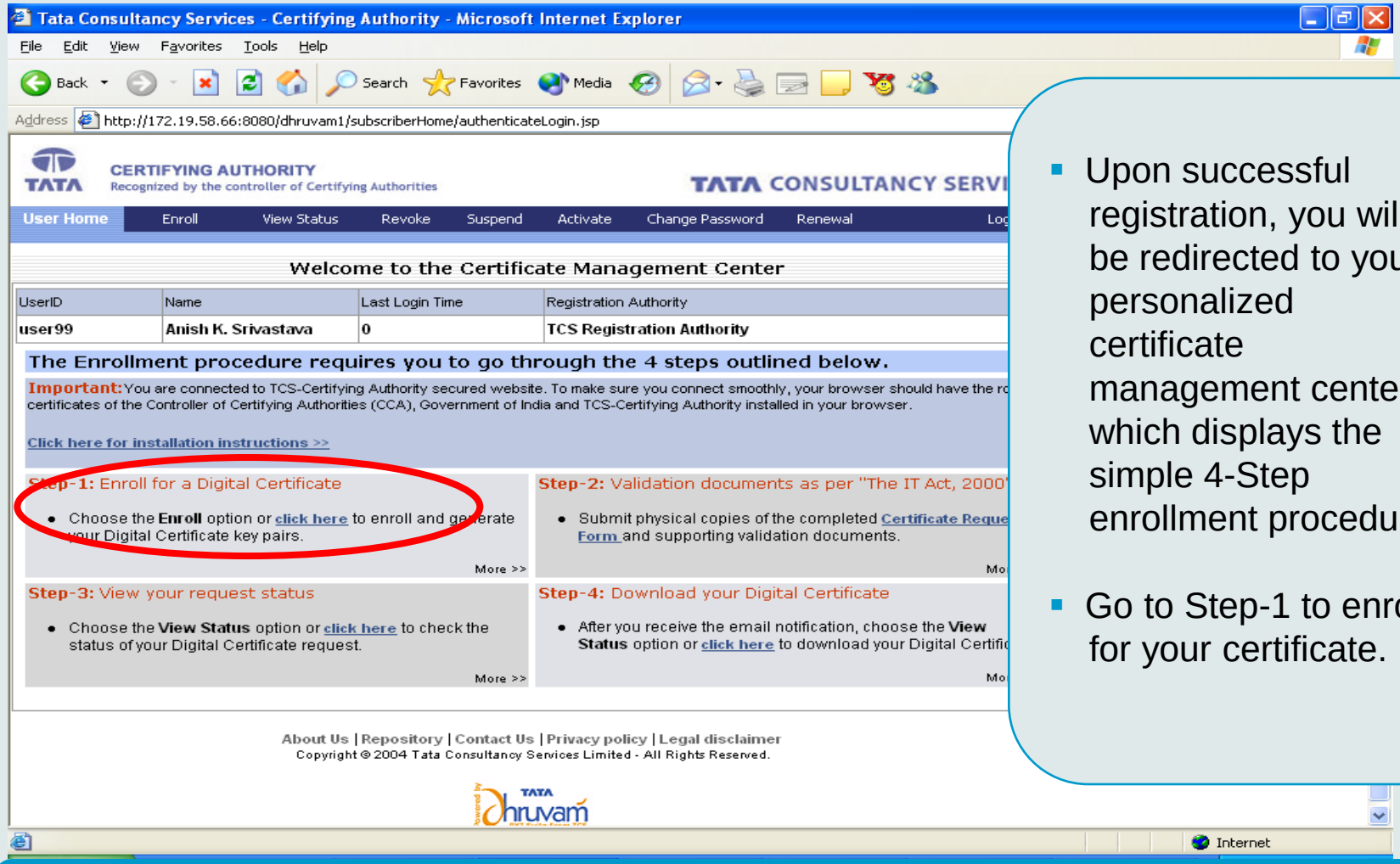
Account Registration Instructions

- Enter your Name, Email, preferred User ID & Password
- Ensure that you remember the User ID & Password as you will need this information to access your account
- Type of User » This maybe Individual, Company or Government, depending on the entity for which a certificate is needed. The verification procedure (and supporting documents required) will be different for each.
- Registration Authority » This is the office through which you are applying for a digital certificate. In your case, it is **TCS Registration Authority**

Stage-3 | Enrollment

Enroll for your Digital Certificate

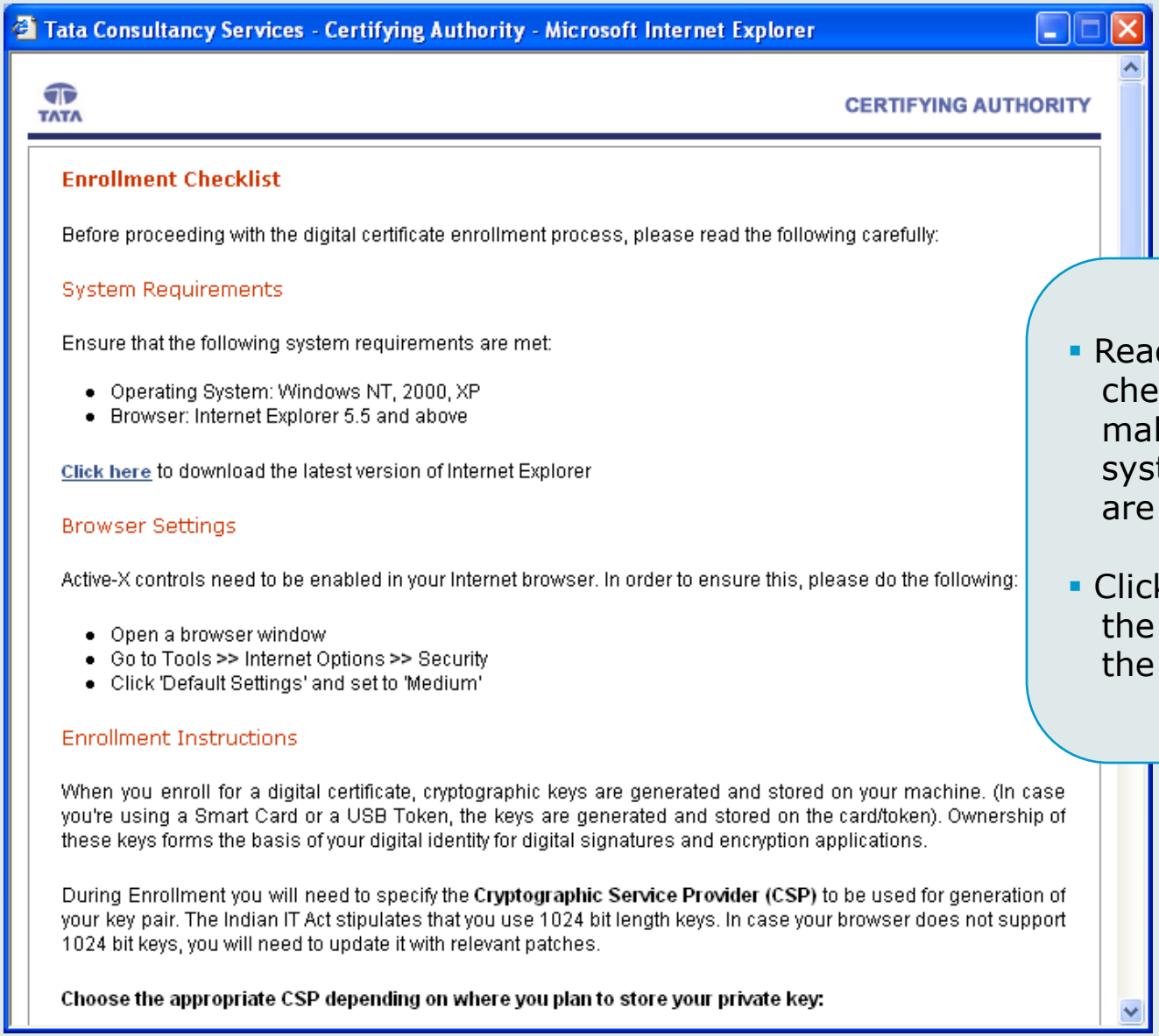
Digital Certificates | Certificate Management Center



- Upon successful registration, you will be redirected to your personalized certificate management center which displays the simple 4-Step enrollment procedure
- Go to Step-1 to enroll for your certificate.

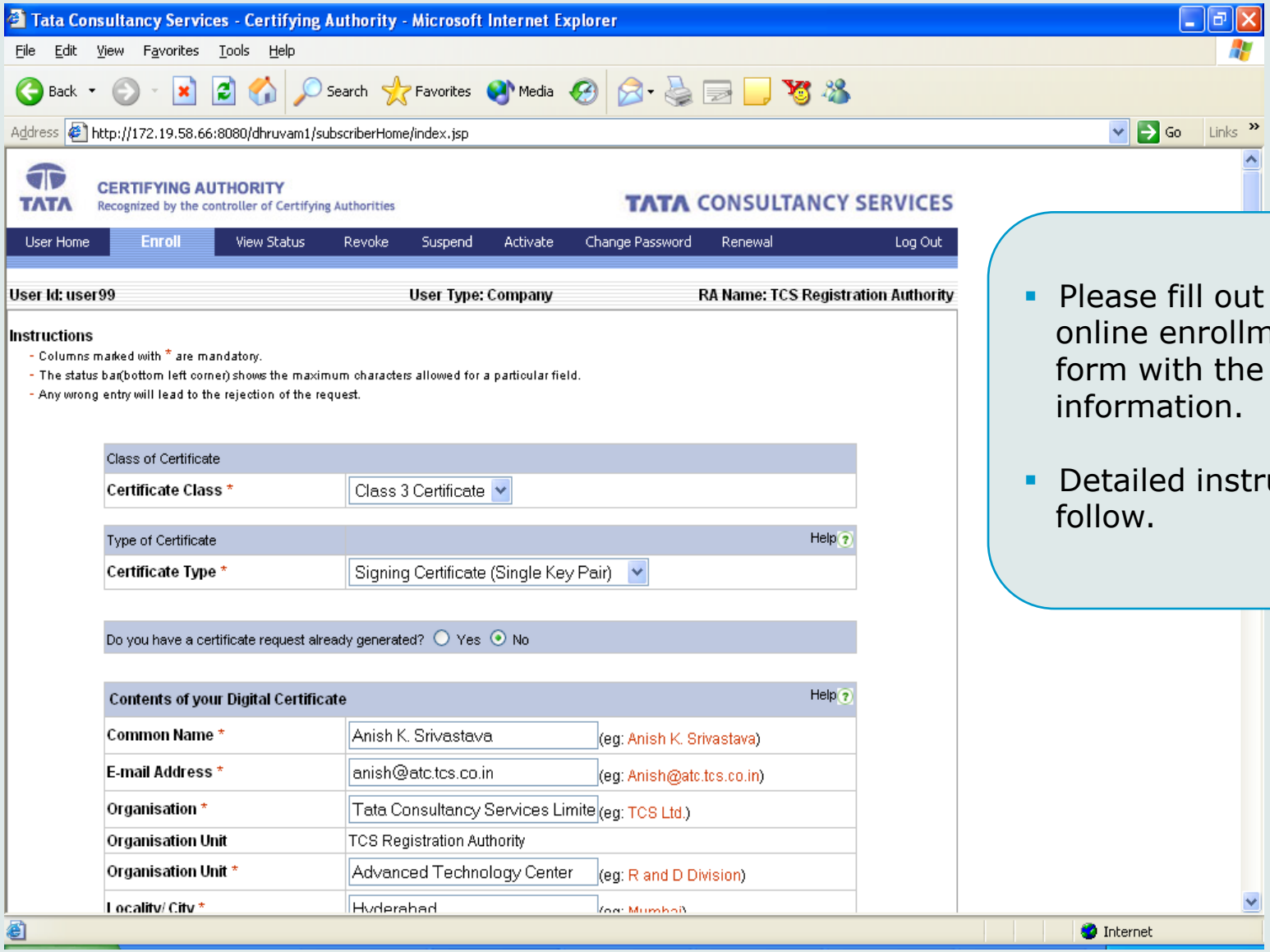
You will need to download your certificate onto the same machine where you perform Step-1 of enrollment.

Digital Certificates | Enrollment Checklist



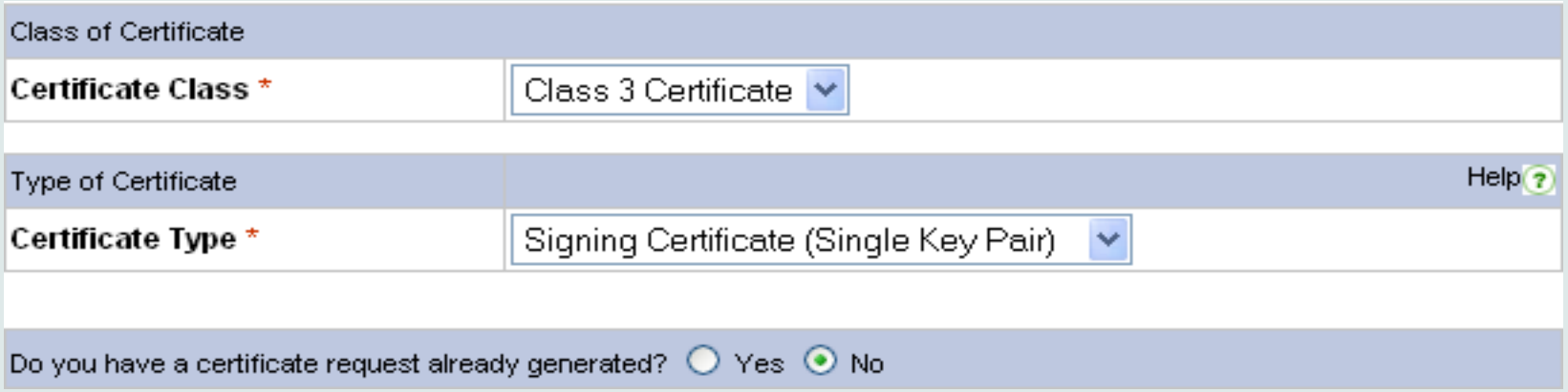
- Read the enrollment checklist carefully and make sure that all system requirements are met.
- Click ‘Close’ to close the checklist and start the online enrollment.

Digital Certificates | Online Enrollment



- Please fill out the online enrollment form with the required information.
- Detailed instructions follow.

Digital Certificates | Online Enrollment



Select the following options:

- **Certificate Class »** Class-3 Certificate
- **Certificate Type »** Signing Certificate (Single Key Pair)
- **Do you have a certificate request already generated? »** No

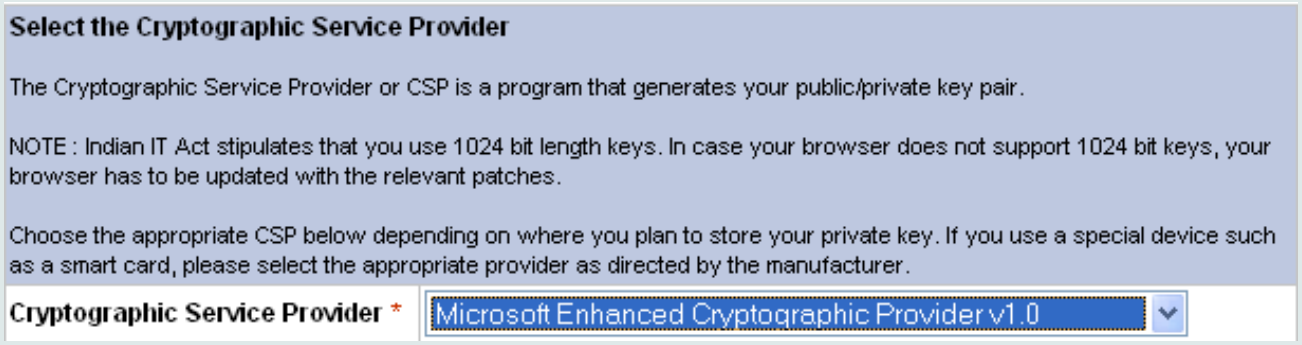
Digital Certificates | Online Enrollment

Contents of your Digital Certificate		Help
Common Name *	Anish K. Srivastava	(eg: Anish K. Srivastava)
E-mail Address *	anish@atc.tcs.co.in	(eg: Anish@atc.tcs.co.in)
Organisation *	Tata Consultancy Services Limite	(eg: TCS Ltd.)
Organisation Unit	TCS Registration Authority	
Organisation Unit *	Advanced Technology Center	(eg: R and D Division)
Locality/ City *	Hyderabad	(eg: Mumbai)
State *	Andhra Pradesh	(eg: Maharashtra)
Country Code	IN	

Contents of your Digital Certificate

- Enter all your personal/organization details exactly as you would like them to appear on your certificate.
  Note: Once your request is generated, these details **cannot** be changed.
- Given the legal significance of digital certificates, please ensure that all information provided is factually correct.
- You Email ID is especially important in the context of digital certificates. Please ensure that you enter it correctly. If an incorrect/invalid Email ID is provided, you will not be able to download/use your certificate.

Digital Certificates | Online Enrollment



Cryptographic Service Provider

- The **Cryptographic Service Provider (CSP)** is the software that generates the cryptographic keys for your digital certificate. These keys form the basis of your digital identity and will be used for digital signing and encryption operations.
- In order to generate the cryptographic keys on your local machine, select the following CSP from the dropdown menu on the enrollment page:
  - **Microsoft Enhanced Cryptographic Provider v1.0**

Digital Certificates | Online Enrollment

Generate Request

- Once you fill out the online enrollment form, review the information provided (paying special attention to the Email ID) and click 'Generate Request' to generate your certificate request.

  Note: Once your certificate request is generated, you cannot change any information. So please ensure that all information is correct before you proceed.

Digital Certificates | Online Enrollment

Confirm your E-Mail ID

- Before your request is generated, you will be prompted to check your E-Mail ID. It is extremely important to ensure that you provide a valid E-Mail ID.
- In case your E-Mail ID is invalid/incorrect, you will not be able to download your certificate and will have to repeat the entire enrollment process.

Digital Certificates | Online Enrollment

Setting the Security Level of your Private Key

- You will be prompted to set the security level of the private key that will be generated.
- Click 'Set Security Level' to set the desired security level.

Digital Certificates | Online Enrollment

Setting the Security Level of your Private Key

- It is extremely important to protect your private key from unauthorized access.
- Hence, set the security level to 'High'. This way, your private key will be password protected. Click 'High' to choose this level.

Digital Certificates | Online Enrollment

- Set the password to be used for accessing your private key in future.

Setting the Security Level of your Private Key

Please ensure that you remember this password. If you lose the password to your private key, you will not be able to use your Digital Certificate.

Digital Certificates | Online Enrollment

Setting the Security Level of your Private Key

- You will see the above confirmation screen once the security level is changed to 'High'.
- Click 'OK' to proceed.

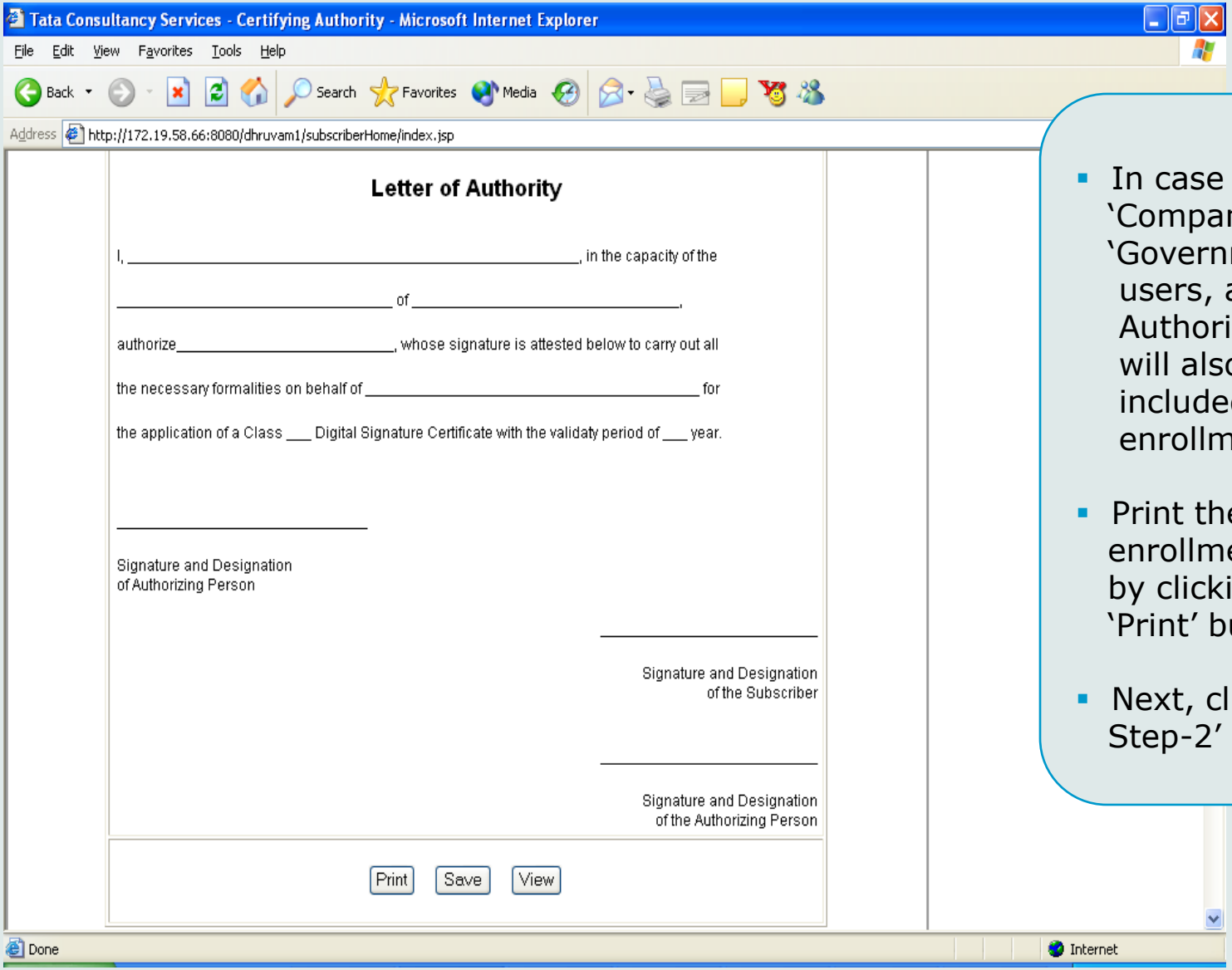
Digital Certificates | Online Enrollment

Certificate **Enrollment Form** for Request Number - **2898**	
Certificate Class	CLASS3
Certificate Type	Signing Certificate (Single Key Pair)
Contents of your Digital Certificate Request	
Name	Anish K. Srivastava
Organization	Tata Consultancy Services Limited
Organization Unit	Advanced Technology Center
E-mail Address	anish@atc.tcs.co.in
City	Hyderabad
State	Andhra Pradesh

Important:
1. Print this **Enrollment Form** by clicking **[Print]** button.
2. The printed copy should be physically signed by the Subscriber and the Authorizing person and sent to Registration Authority.

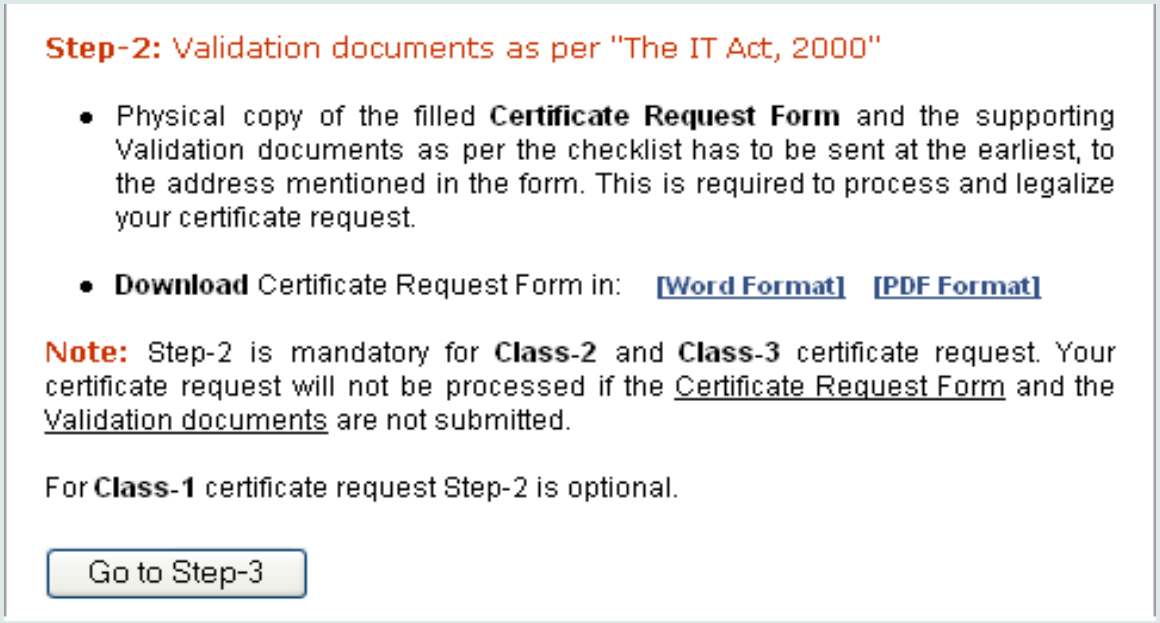
- On successful enrollment, you will see this confirmation screen.
- Verify the information displayed. If you find any mistakes, please contact your RA Administrator immediately.

Digital Certificates | Online Enrollment



- In case of 'Company' and 'Government' type users, a 'Letter of Authority' form will also be included in the enrollment form.
- Print the enrollment form by clicking the 'Print' button.
- Next, click 'Go to Step-2'

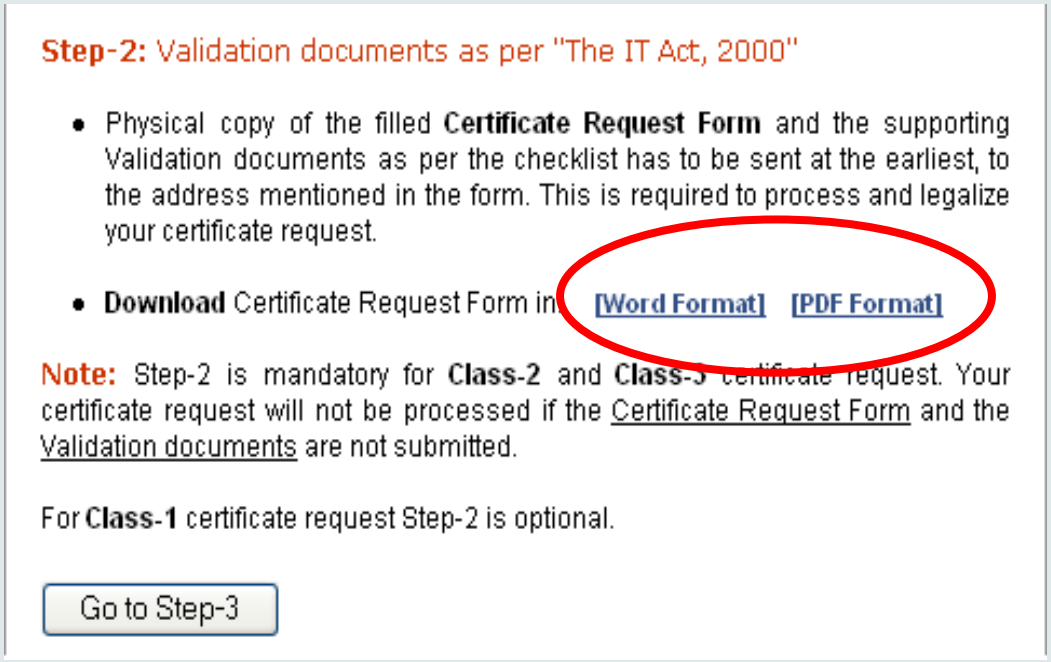
Digital Certificates | Submission of Documents



Documents for Verification

For a Class-3 certificate, you will need to submit supporting documents required for verification of your personal and/or organization credentials. This is an extremely important part of the enrollment procedure and your certificate will only be issued upon successful receipt and verification of these documents.

Digital Certificates | Submission of Documents



Documents for Verification

- Download the Certificate Request Form by clicking the relevant link.
- The Certificate Request Form contains a detailed checklist of the documents that are to be submitted. Please fill out this form and send all required documents as to the address specified in the form.

Note: You can logoff once you download the Certificate Request Form.

Digital Certificates | Check your application status

Check/View the status of your application

Your application will be considered complete once you submit the online request **and** the request form and all supporting documents required for verification of your request.

While your application is under review, you will receive automated e-mail updates on the status of your application. Notifications will be sent informing you of the following:

- **Receipt of your Online Request:** This is sent immediately upon successful online enrollment
- **Generation of your Certificate:** This is sent once your request and documents are verified and your certificate is generated.
- **Rejection of your Certificate Request:** If your request is rejected for any reason, you will be intimated of the same.

Note: You can always login to your user account and perform **Step-3** in the Certificate Management Center to know the status of your application.

Digital Certificates | Download your Certificate

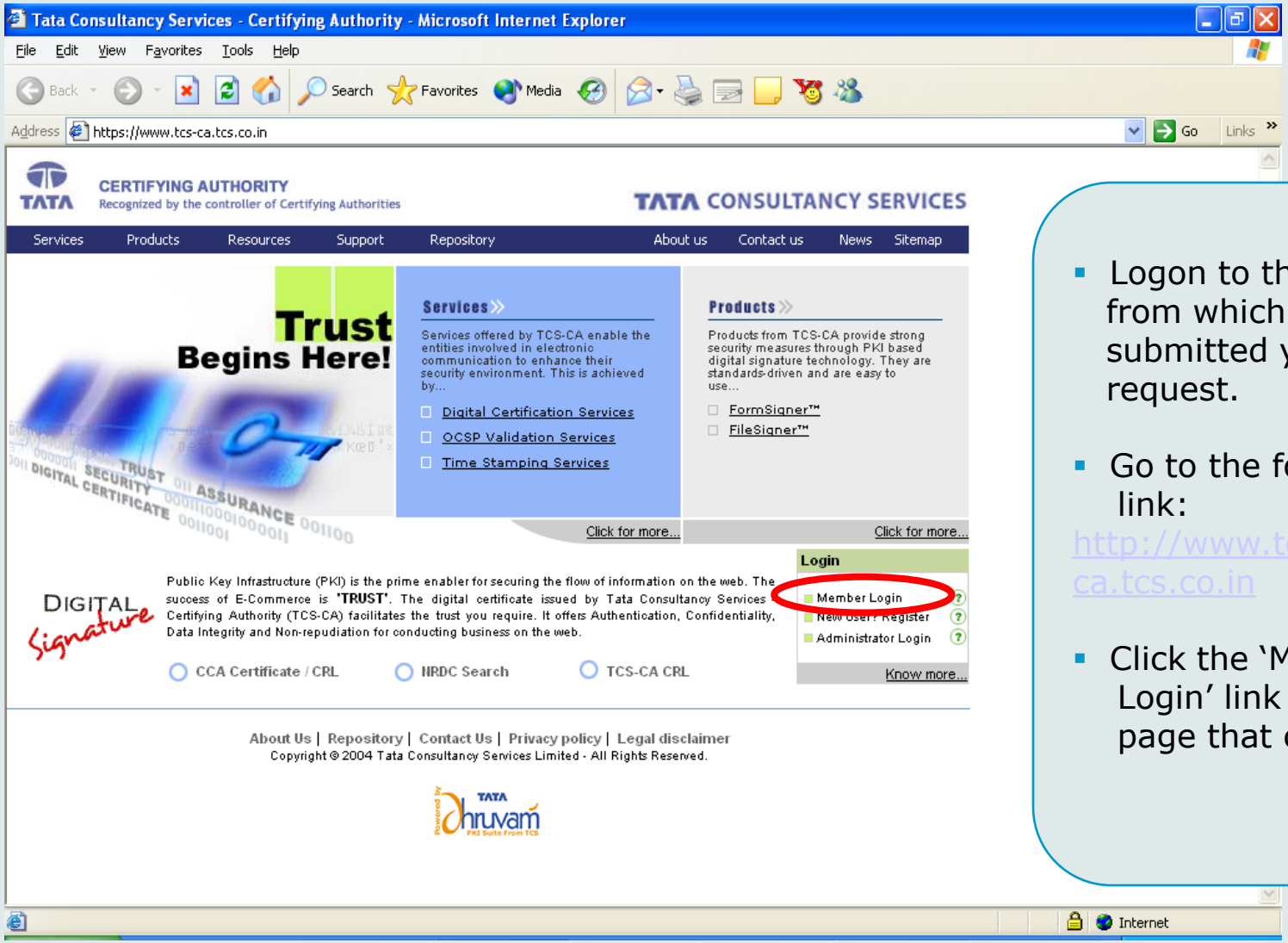
Certificate Download Instructions

- Once your certificate is generated, you will receive an email notification informing you of the same. This notification is sent to the email address entered during the enrollment process **(Step-1).**
- The email will include detailed instructions and an **Authentication PIN** that needs to be entered at the time of certificate download.
- Instructions follow on how to download your certificate.

Note:

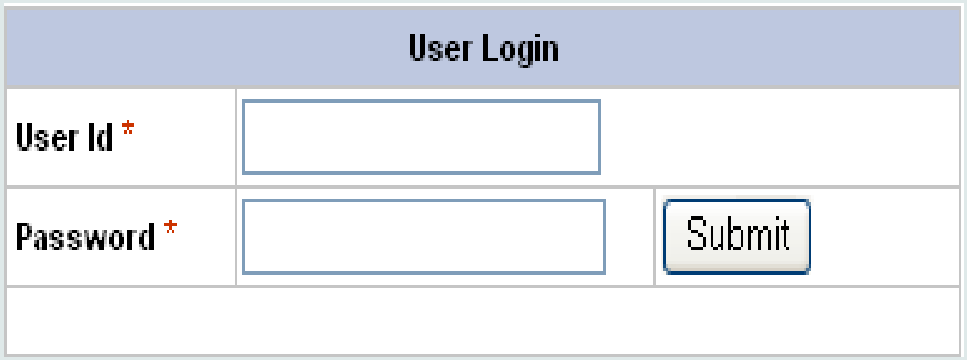
- The certificate should be downloaded on the same iKey token where the Key Pair was generated.
- It is very important that you provide a valid e-mail address at the time of enrollment. If you submit an invalid e-mail address, you will not receive the Authentication PIN and hence will not be able to download your certificate.

Digital Certificates | Download your Certificate



- Logon to the machine from which you submitted your online request.
- Go to the following link: http://www.tcs-ca.tcs.co.in
- Click the 'Member Login' link on the page that comes up.

Digital Certificates | Download your Certificate

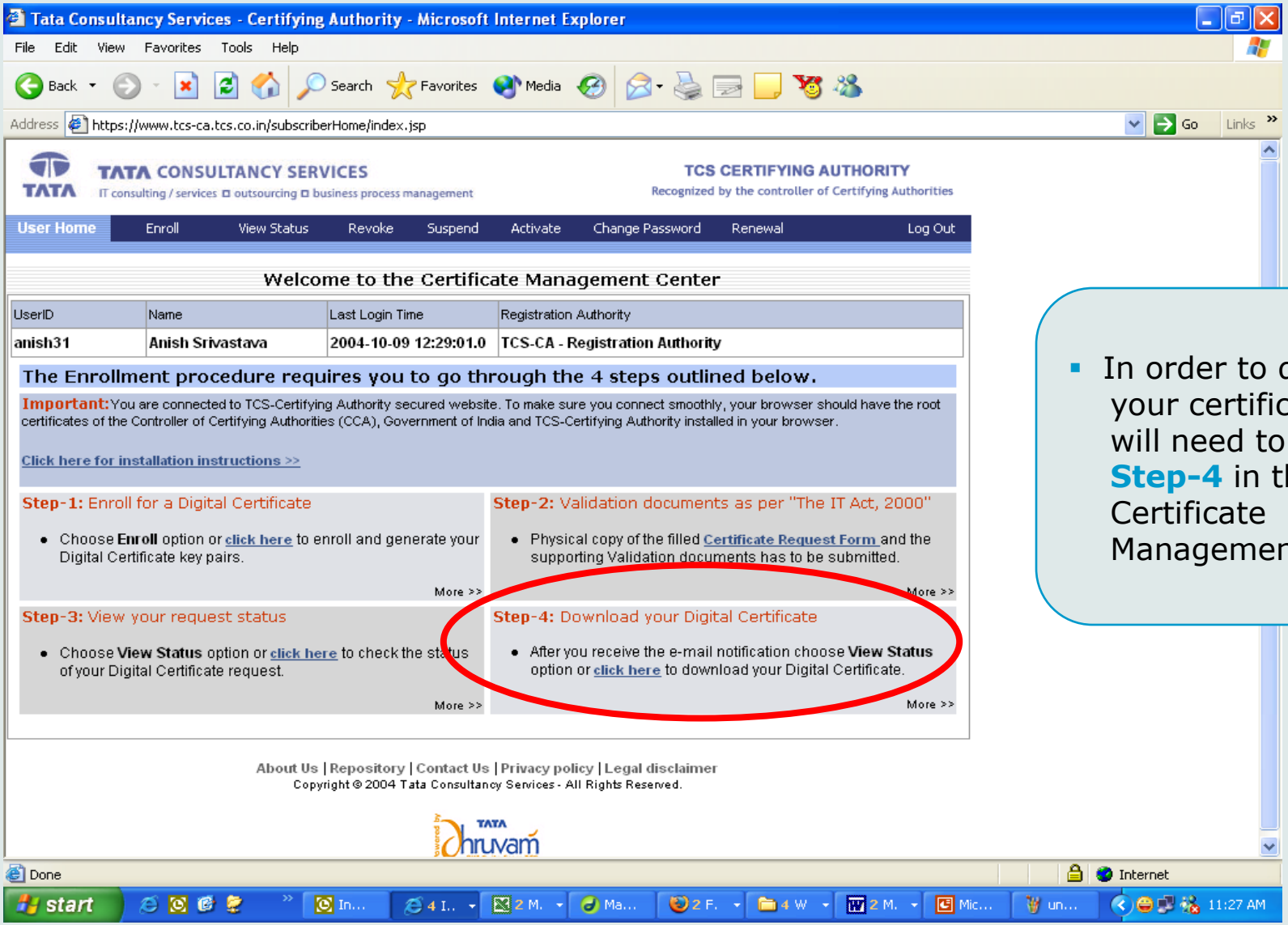


Login to your User Account

- Enter your User ID and Password to login to your account for certificate download.

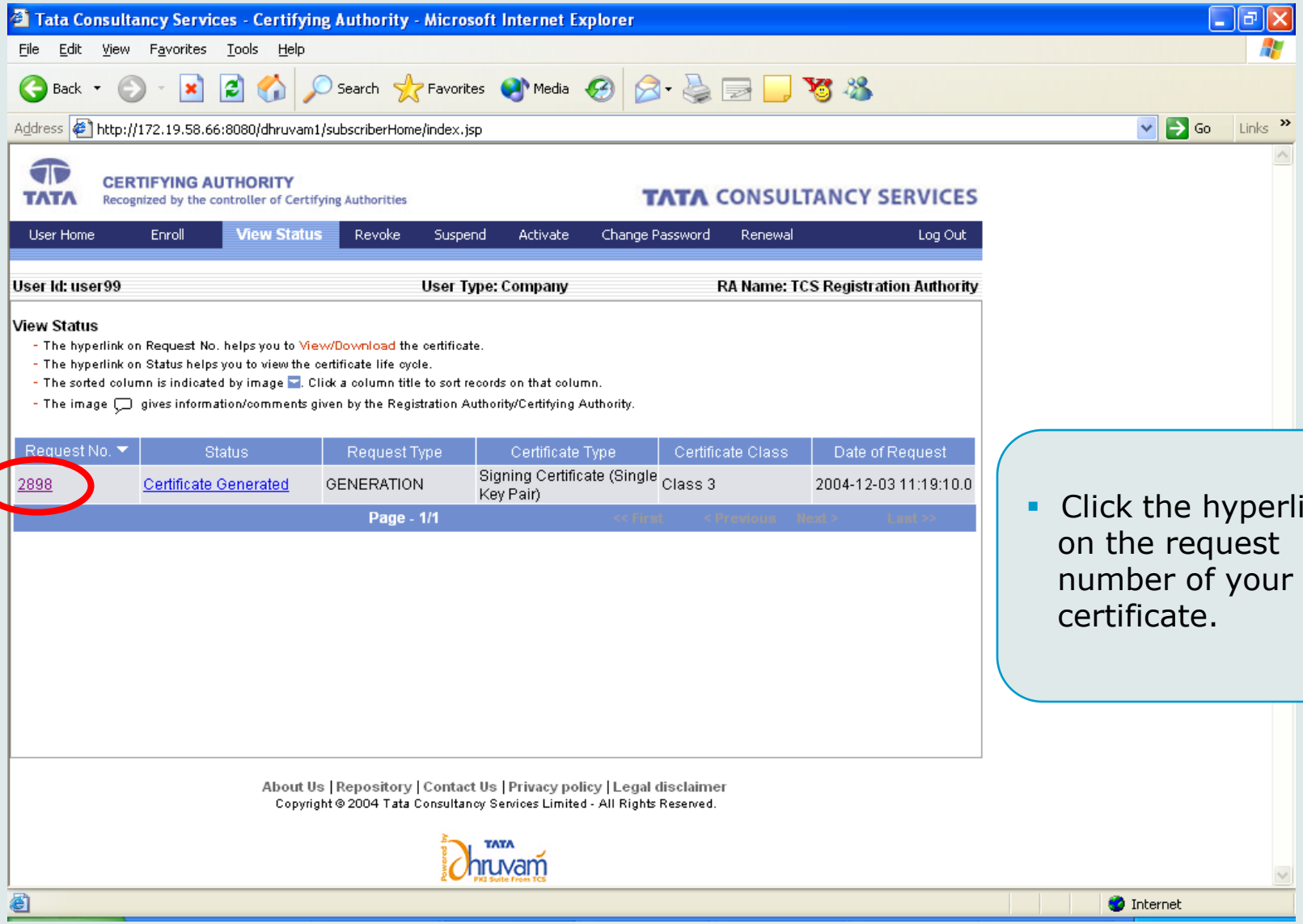
Note: If you do not remember your User ID and/or Password, please contact your RA Administrator.

Digital Certificates | Download your Certificate



- In order to download your certificate, you will need to perform **Step-4** in the Certificate Management Center

Digital Certificates | Download your Certificate



- Click the hyperlink on the request number of your certificate.

Digital Certificates | Download your Certificate

Your Digital Certificate Information	
E-mail Address	anish@atc.tcs.co.in
Country	IN
State	Andhra Pradesh
Locality/ City	Hyderabad
Organisation	Tata Consultancy Services Limited
Organisation Unit	Class 3 Certificate
Organisation Unit	Advanced Technology Center
Organisation Unit	TCS Registration Authority
Common Name	Anish K. Srivastava
Serial Number	5DDE

Please enter the Authentication PIN sent to anish@atc.tcs.co.in, the E-mail ID provided in the certificate request.

Authentication PIN

Back | Download | Reject

You will <u>not</u> be able to download your certificate without the Authentication PIN.

Digital Certificates | Download your Certificate

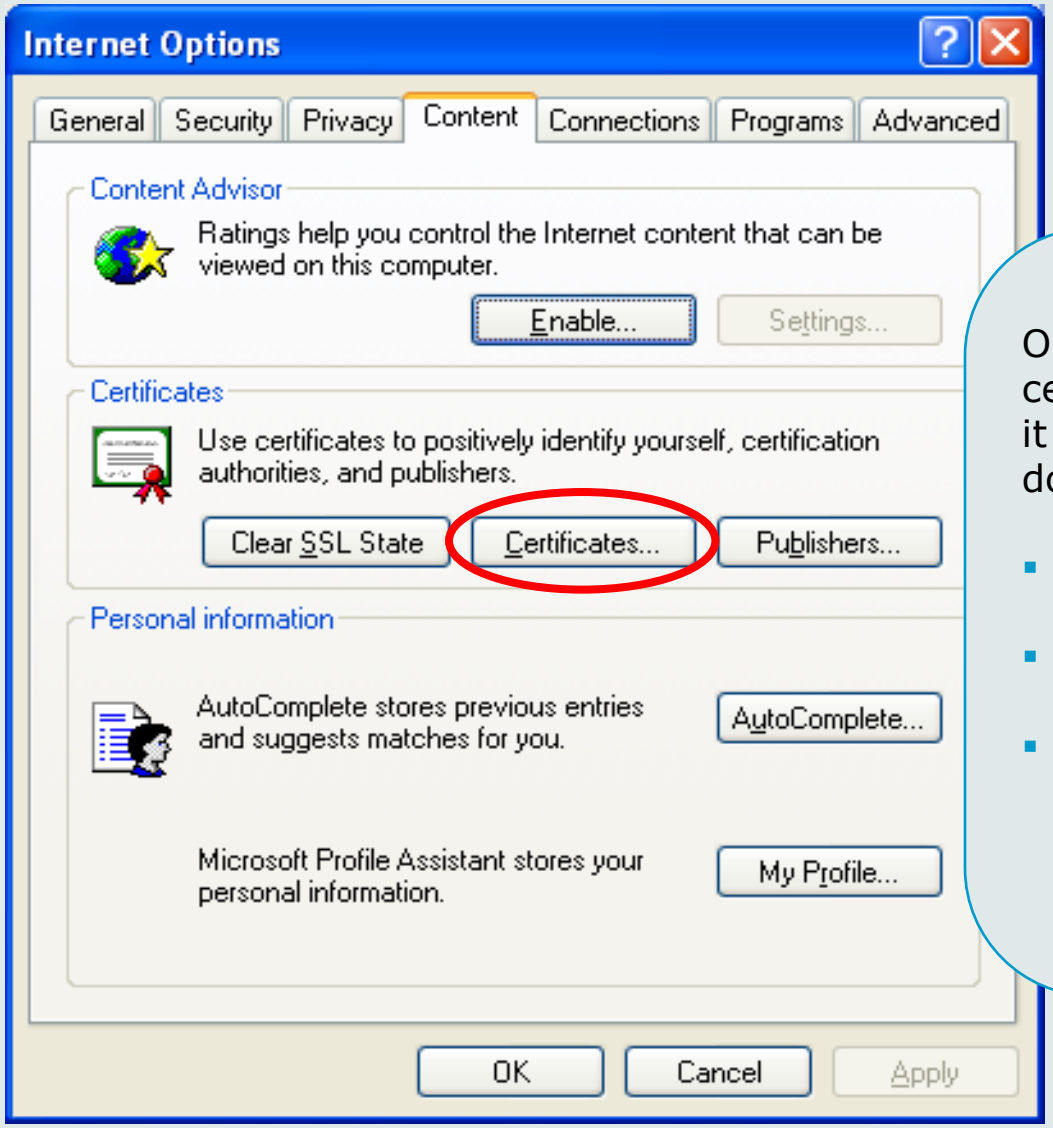
Certificate Download Instructions

- Verify the details of your certificate. If there is any problem, please contact your RA Administrator.
- Enter the Authentication PIN that was emailed to you earlier.
- Click ‘Download’ to complete the certificate download.

Stage-4 I Usage

Use your Digital Certificate

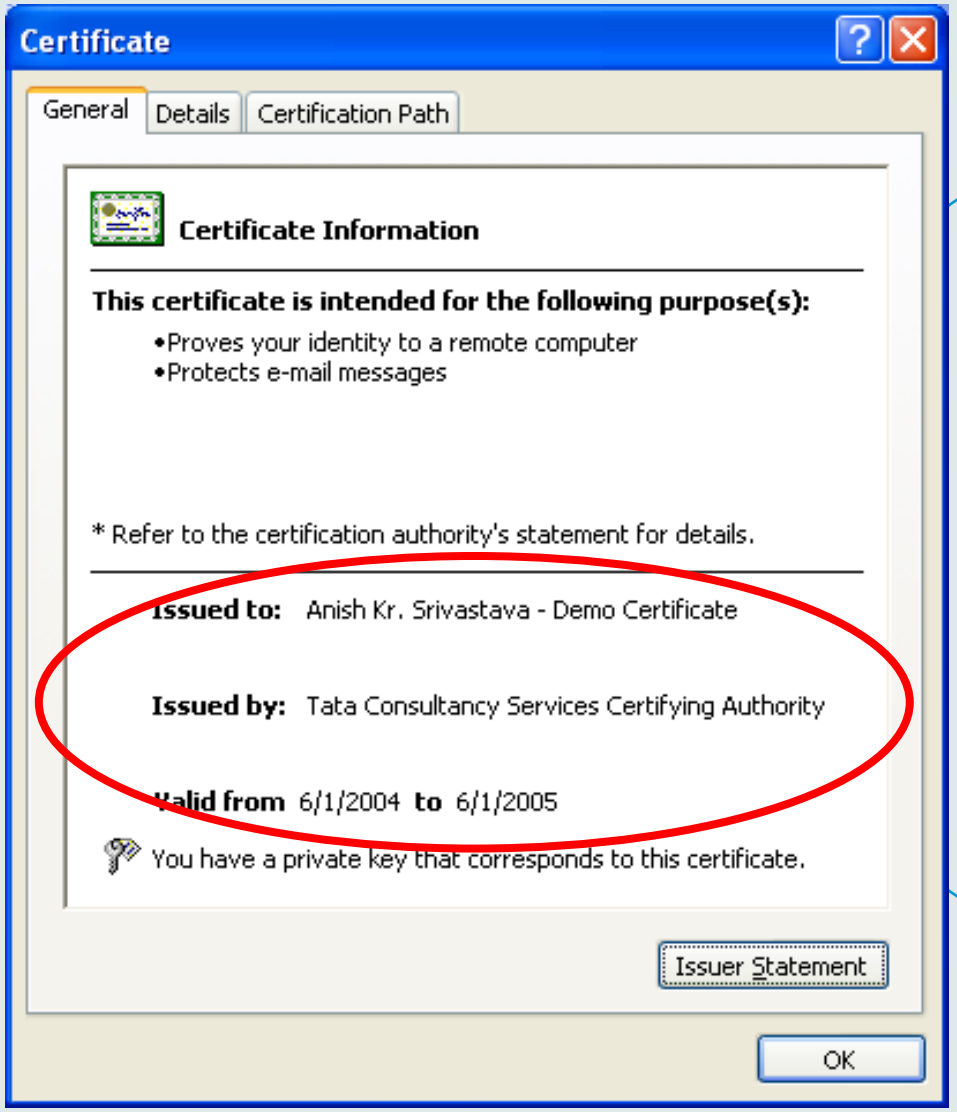
Digital Certificates | Verification



Once you download your certificate, you can verify whether it has been successfully downloaded by doing the following:

- Open an Internet Explorer window
- Go to Tools → Internet Options → Content → Certificates
- View the list of certificates – you should be able to see a certificate containing your name on it.

Digital Certificates | Verification



- Double-click your certificate in the list displayed.
- Your certificate details will be displayed.
- Verify the following details:
  - Issued To
  - Issued By
  - Valid from __ to __
- If there's any problem, please contact your RA Administrator.

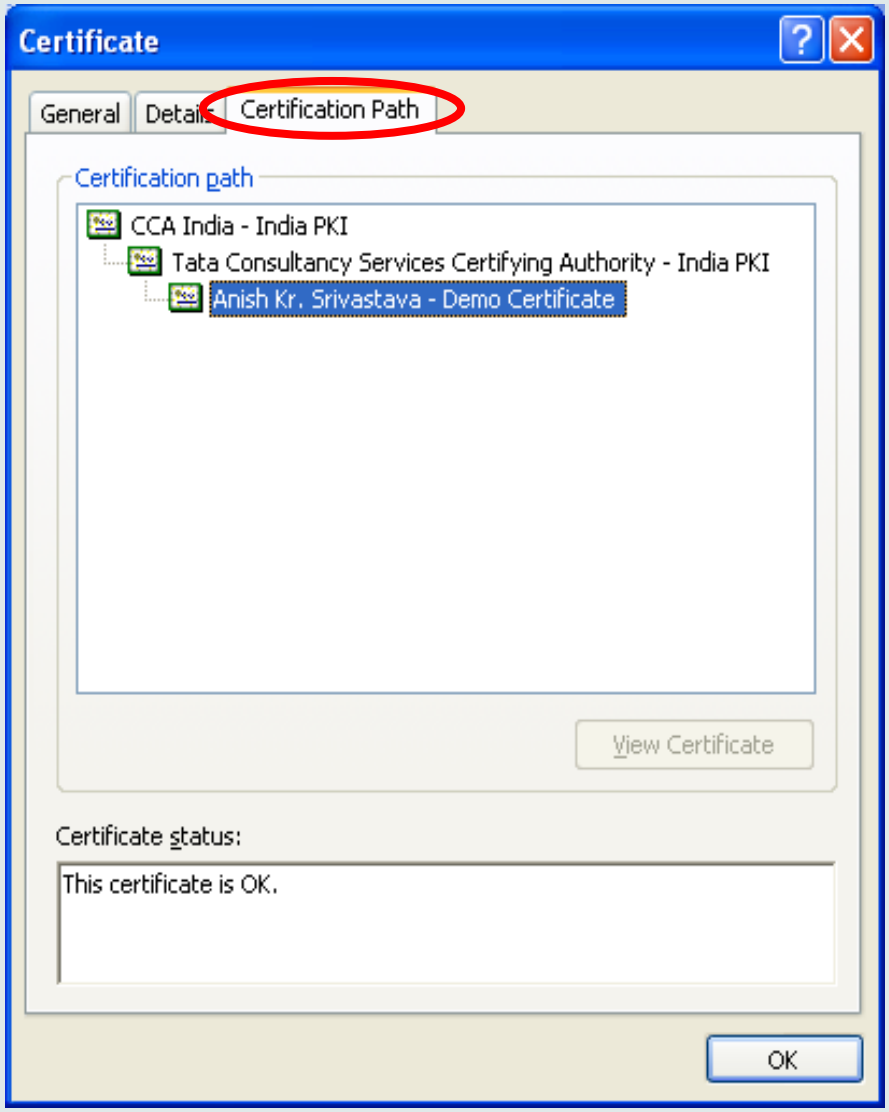
Digital Certificates | Installation of the Trust Chain

Installation of the Trust Chain

Before you can use your Digital Certificate, you need to install the TCS-CA trust chain. Following is the procedure for installation:

- Download the TCS-CA trust chain by clicking here: https://www.tcs-ca.tcs.co.in/cert/chain.p7b
- Save the **chain.p7b** file on the machine where you plan to use your digital certificate.
- Right-click the **chain.p7b** file and select 'Install'. This will install the certificate trust chain on your machine.

Digital Certificates | Installation of the Trust Chain



To verify whether the installation is successful, please do the following:

- Open an Internet Explorer window
- Go to Tools → Internet Options → Content → Certificates
- Double-click your certificate and select the Certification Path.

You should be able to see the following:

- CCA India – India PKI
- Tata Consultancy Services Certifying Authority – India PKI
- 'Your Name'

Case Studies

Case 1: E-Procurement

Digital Signature Certificates used by Vendors and Issuers of a Tender

E-Procurement

- Benefits
  - Cartel formation, rigging, information leakages, modifications etc… can be avoided
  - Provide privacy and confidentiality to the documents within the tenders
  - Keep the information regarding vendors confidential

E-Procurement - Process

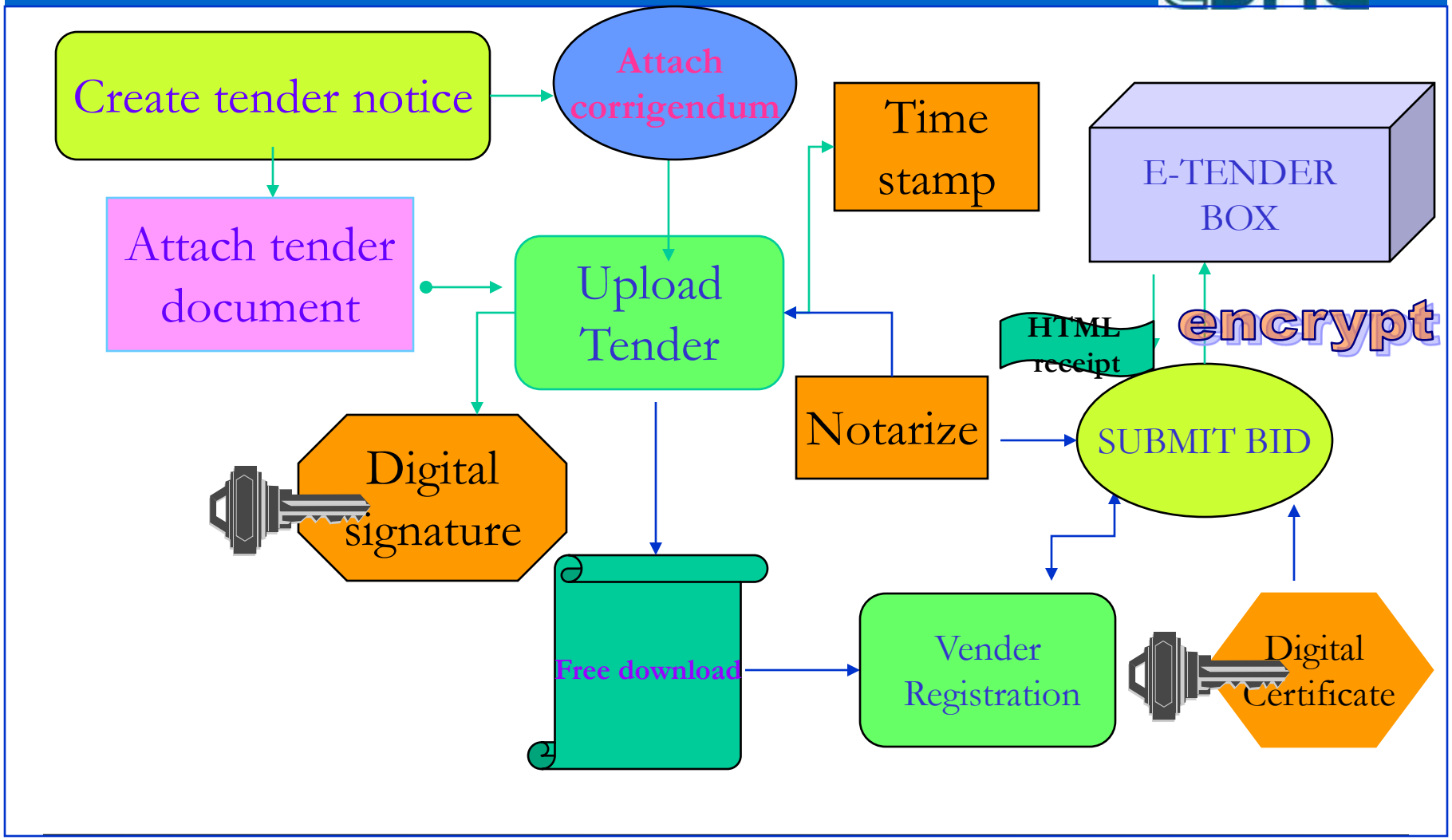
- Issuer of the Tender needs to have a Digital Signature Certificate
  - The public key of the issuer of the tender is required for the vendors
- Each vendor logs on to a online system and provides his digital certificate
- A vendor prepares and digitally signs his document
  - Vendor uses his private key to sign it
- A vendor then uploads his document
  - A vendor uses the public key of the issuer of the tender to encrypt data
  - Now, only the issuer of the tender can decrypt it, using his private key
  - At the server side, the digital signature and data is verified before storing it for further processing

E-Procurement - Process

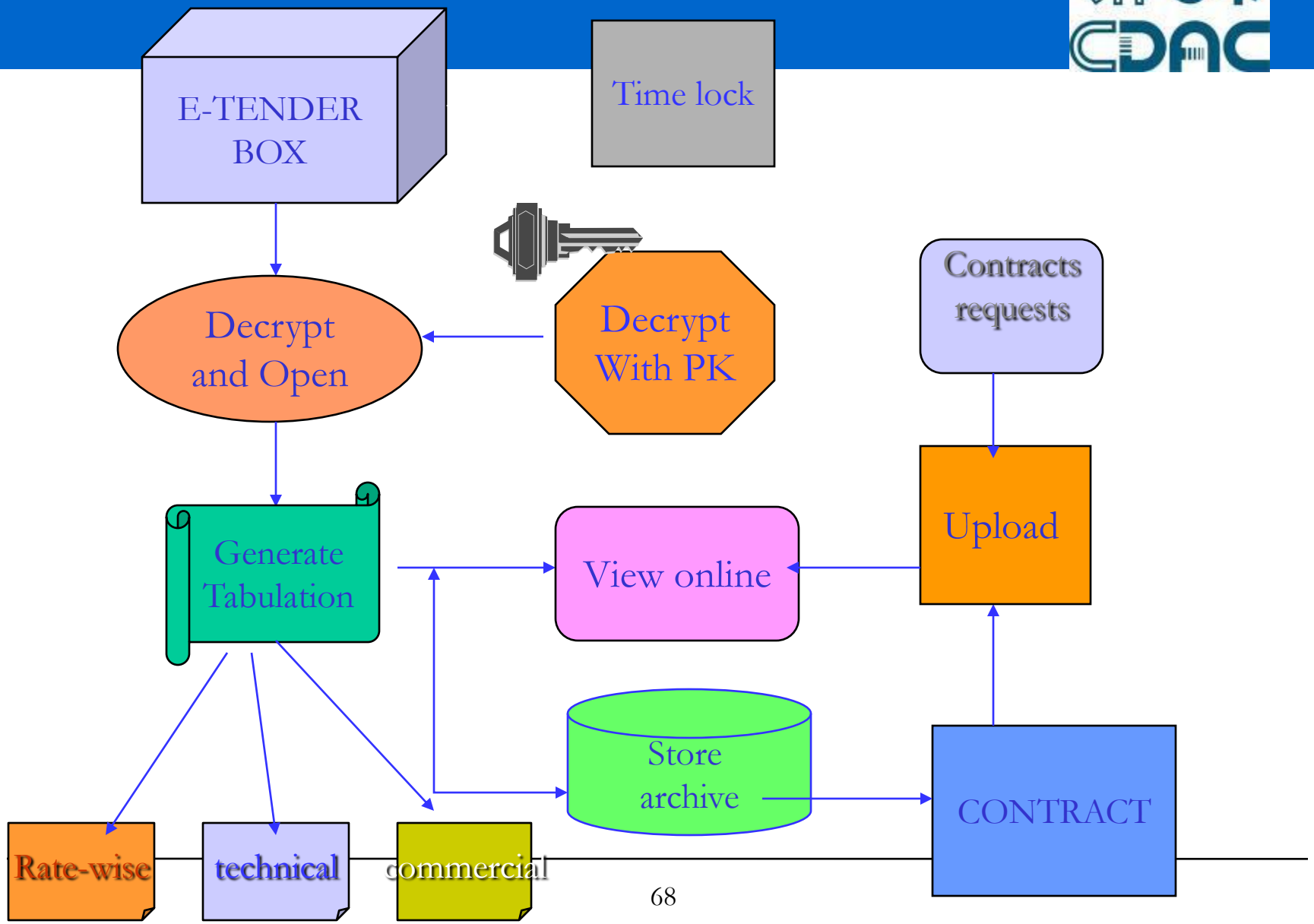
- Vendor can be sure that:
  - Except for the issuer of the tender, none can open his quote document
- Issuer of the tender can be sure that:
  - That the quote that has been received from a given vendor, has indeed come from the same vendor
  - That the quote given by the vendor has not been tampered on the way

Process of e-Procurement for Indian Railways

Process flow chart



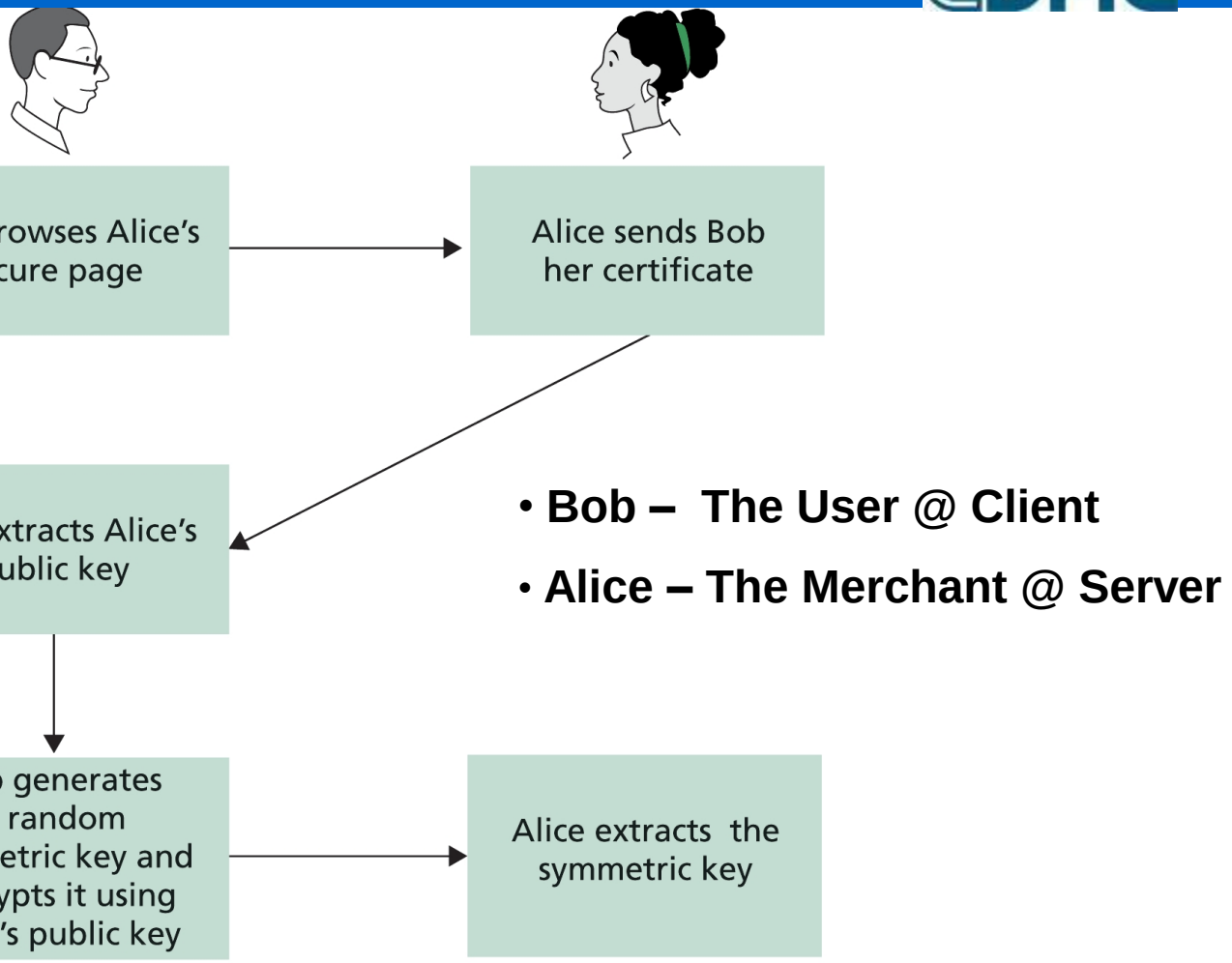
Post tender opening work flow



Case 2: e-Shopping & e-Payment

Digital Signature Certificate used by an Online Merchant's Web server

SSL - Explained



- **Bob – The User @ Client**
- **Alice – The Merchant @ Server**

Courtesy: James F Kurose, Keith W Ross, Computer Networking: A Top-Down approach featuring the Internet

E-Shopping Process

- Traditional E-Shopping
  - Machine (Server) – Machine (Client) Authentication
  - You are @ Client side; Merchant is @ Server side;
  - Client (Browser) will receive a digital certificate from the Server (Web Server), signed by a CA
  - If the CA is not in the list of 'Trusted CAs', Client will ask you, whether to trust this CA, and go forward
  - On trusting the CA, Client will then extract the Public Key, associated with the Domain Name of that Web Server

E-Shopping Process

- Client will then generate a random symmetric key and encrypts the key with the server's public key and sends it to the server
- Server will decrypt the message using its private key, and will find the key to be used for encrypting and decrypting messages, thus establishing a secure communication channel
- This is how **SSL** Works!

Case 3: e-filing of IT Returns

e-filing of IT Returns

Below is the step by step procedure of filing Income Tax Return with your digital Signature:

- Prepare your Income Tax Return and Generate XML.
- Save XML file in your favourite location [Say Desktop].
- Connect your digital Signature Certificate - USB Token to your System.
- If not registered, Register Assessee PAN at http://incometaxindiaefiling.gov.in
- Login to Income Tax eFiling website.
- Click on" Submit your Return" for Respective ITR Form..

e-filing of IT Returns

- Select the XML file saved on your computer.
- Click on "Digitally Sign" button and select respective digital signature from USB Token.
- Click on "Submit" button". It will verify the return and signature, then will show ITR-V with Acknowledgement number.
- Take the printout of ITR-V and keep it for future reference along with Paper printout of complete return form.
- **Digital Signature should be a valid certificate and should be on the name of "Authorised Signatory" of the Return.

- Income tax website
  - https://incometaxindiaefiling.gov.in/
- Enter your credentials
  - https://incometaxindiaefiling.gov.in/portal/uploadXML.do
- Upload the .xml file and then click the check box for digitally signing
  - https://incometaxindiaefiling.gov.in/portal/uploadXML.do?SIGNIT=%27sign%27

Case 4: e-booking of Railway Tickets (IRCTC)

e-ticketing using Dig. Cert.

First Flight Tours & Travels Case Study

- · Download Class 3 Digital Certificate or Software from software CD.
- · Insert e-token in the USB port of the system and wait for 1 Min. (In case if you have taken Digital Signature in USB Token Format.
- · Go on homepage of IRCTC www.irctc.co.in and click on Agent Login.
- · A window will appear stating your name. Highlight the name and click ok to continue.

- Insert the USER ID and password given by IRCTC. Click login to Continue.
- · The "Plan my travel and Book tickets" page appears.
- · Use help option for any help required to book tickets.
- · Select your train from the list that appears on the screen.
- · If the From/To station selected by you are correctly in the route of the train then:
- · Select e-Ticket option.
- · The list of e-ticket trains will be highlighted.

Some Risks …

Risks & Precautions

- You have to protect your private (secret) key!
  - You prove your ***identity*** by proving that you "control" the private key corresponding to the public key in the certificate
  - As a signer cannot credibly deny having made the signature
  - Hence, the passwords that you use to operate PKI software for signing has to be protected!
  - You may have to also protect the computer system that stores your private key!
    - Go for USB tokens instead of simply using browsers

References

- http://nicca.nic.in – CA website of NIC
- http://www.cca.gov.in/LicencedCer.jsp - List of CA Certificates
- Online Demo for getting Digital Certificate – www.tcs-ca.tcs.co.in
- ONGC e-Procurement online guide
- e-Procurement in Indian Railway – Presentation by A.K. Goel

Thank You