Process for Issuance of DSC

Contents

Documents Required for DSC Application:

1. **Application Form** – Fill the Application form based on Sample form provided in Annex.

Note: Please use the **ONLY** Applicant's (not any group or others) official e-mail ID which the bank proposes to use for IBCART Portal.

2. **Subscriber Agreement – Applicant please** Read and Sign on both pages of the Subscriber Agreement provided in Annex.

3. **Physical Verification** – Video verification during enrolment **"Or"** Physical verification letter (as in the enclosed sample letter in Annex) with Superior's cross-signature **on Applicant's photo**.
4. **Enclosures –**
   i. Applicant's – PAN, Aadhaar, Employee ID card (Self-attested)
   ii. Superior's – PAN, Aadhaar, Employee ID Card (Self-attested) – Annex

5) Please purchase the specified Token (Pen Drive) for the Vendor List as in The Annex or from your listed Suppliers with the **indicated standard specification** by CCA.

The CCA guidelines require tokens to be FIPS 140-2 Level 3 certified, have unique manufacturer-based serial numbers, and enforce strict PIN policies, including mandatory PIN changes at the time of download and no option for PIN resets.

Operational Process

A. Operational process for the bank which <u>has it own</u> Registration Authority (RA):

> a. The RA need to fill up the form on the portal, complete the vKYC (or physical verification letter as in the sample letter) and submit.
>
> b. It will be processed at our end and on verification and authorisation → the bank /entity will get email from us having DSC download link and the required process to be followed.

B. Operational process for the bank which is not a Registration Authority (RA):

  i. Scan the filled in application form along with enclosure documents and save in **one** single file as: **DSC_<Applicant Name>_Prod.pdf**

  ii. Then Superior need to digitally sign the file namely **DSC_<Applicant Name>_Prod.pdf**.

  iii. Scanned the Digitally Signed Application form along with the enclosures which need to be sent to casahyog@idrbt.ac.in

  iv. If the bank/entity is not having any superior authority with DSC, send the filled in application form with enclosures by Courier. The processing of application form will commence after receipt of the hardcopies through courier.

A	v. During processing for the hard copy of application form → → For first time users an email from cahelp@idrbt.ac.in for password generation will be sent. → Thereafter, setup link will also be sent from IDRBT email id cahelp@idrbt.ac.in.
B	User need to generate the password and go to the Setup link. → and fill up the form correctly to attach in the Application Form to be sent by courier as explained above.

After Login, the bank/entity need to fill up the form on the portal, complete the vKYC (or physical verification letter as in the sample letter) and submit.

5. Operational Process

i. The Hard copy of the Form will be assessed and verified with the information submitted digitally on the portal.

ii. After verification the application will be processed for generation of Digital Signing Certificate – Class –3.

iii. The bank /entity will get email from us having DSC download link and the required process to be followed as per Annex

Annex- Application Form

IDRBT CA

APPLICATION FORM FOR DIGITAL CERTIFICATE

Important Notice:
- Subscriber agreement should be submitted along with this application form filled by the applicant.
- All subscribers are advised to read IDRBT CA Certification Practice Statement available at **http://idrbtca.org.in/**
- Copy of identification document of applicant (PAN **or** Aadhaar and Emp.ID card) attested by superior authority with seal should be attached along with the application form.
- Self-attested copy of identification document of superior authority (PAN and Emp. ID) should be attached along with this application form.
- Application form must be submitted to the Registration Authority/IDRBT CA for face-to-face verification in case of Class 3 Certificate.
- Incomplete/Inconsistent application is liable to be rejected.
- Section 71 of IT Act stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with fine up to one lakh rupees or with both.
- * Fields are mandatory. Strike off which are not applicable.

milan

Name of the Organization*	BANK OF ABC
Bank in which subscriber has account	XYZ BANK
New / Renewal ✓	User- ID (in case of Renewal)		Validity: 1 Year ☐ 2 Years ☑

Class *:	Certificate for *:	Application*:	Applicant Type*:	Type of Digital Certificate*:
Class 1 ☐ Class 3 ☑	Individual ☑ Server (System) ☐ Web Server (SSL) ☐	SFMS ☐ NGRTGS CTS Others *(Please specify)* .... *Please Specify*	Bank Employee/Officer (Online) ☑ RA Official (Online) ☐	Signing ☑ Encryption ☐ System ☐ Web Server (SSL) ☐ Code Signing ☐ Document Signer ☐

PERSONAL DETAILS

Name*:	Milan damji		Sex*:	Male ✓
Email Address*:	milan.damji@abc.com			Female
Address for communication*:	Corporate Office, Bank of ABC, Bandra-Kurla Complex, Mumbai			
	Pin code*: 400005		Telephone:	Mobile No*: 9999999999
Date of Birth*:			(dd/mm/yyyy) For Ex: 10ᵗʰ May, 1975 is 10051975	
Identification Details* (Valid and not expired)	PAN Card No* ZZZPD1965J	Aadhaar No	6666 8888 4444	
Bank details:	Bank & Branch Name	XYZ BANK, BKC BRANCH		
	Bank Branch Address	BKC, MUMBAI		☑ ☐
	Bank Account No.	00000012345	Type of Bank Account: SB CA	

CERTIFICATE REQUEST DETAILS

The following details will be reflected in the certificate.
Make sure that these details match with those given to generate request using certificate request generation tool or any other PKCS #10 request generation tool.
If necessary, contact your application provider for these details before filling the form.

Common Name* (Name of the person, Server Name, Registered domain name, IFSC Code etc)	Write your name (Only Alphabet- no special characters)
E-Mail* (Valid email address to which the communication be made)	milan.damji@abc.com (official Email)
Organization* (Name of the organization eg: IDRBT)	BANK OF ABC
Organization Unit* (Name of the department eg: Certifying Authority)	Domain Registry
City/Locality* (Name of the city/town eg: Hyderabad)	Mumbai
State/Union Territory* (Name of State/UT eg: Andhra Pradesh)	Maharashtra
Pin Code*	400005
Country*	India

Vidyabagchi
Signature of Superior Authority

milan
Signature of Applicant

-1-

DECLARATION AND UNDERTAKING BY THE APPLICANT*

All the above information provided by me is true to the best of my knowledge and belief. I agree to use only FIPS 140-1/2 Level 2 validated cryptographic modules for key generation and storage. I accept the responsibility for the safety and integrity of the private key by controlling the access to the computer/device containing the same, so that it is not compromised and I will immediately notify my RA/ IDRBT CA in event of key compromise. I agree to publish the Digital Certificate in the IDRBT CA repository and will report IDRBT CA of any error or defect in the certificate and change in the above information.

Date: 18-09-2022

Place: Mumbai

Name of the Applicant: Milan Damji

milan

Signature of the Applicant

FOR SUPERIOR AUTHORITY/BRANCH MANAGER OF APPLICANT*

This is to certify that Mr/Ms ....M.i.l.a.n. .D.a.m.j.i.............. has provided correct information in the "Application Form for Digital Certificate" to

The best of my knowledge and belief. I hereby authorize him/her, to apply for obtaining Digital Certificate from IDRBT CA for the purpose specified above. I have done

physical verification of the subscriber and take responsibility of identification.

Date: 18-09-2022

Place: Mumbai

Name of the Officer: Vidya Bagchi

Official Email: vidya.bagchi@abc.com

Phone No 9999899998

Vidyabagchi

(Signature)

(Official Seal)

FOR RA/ IDRBT CA PURPOSE ONLY

Checklist	Date & Time	Initials
Received the application form for digital certificate?	Only RA	Only RA
Physical Verification(in person/VC/Certified by SA or RA)		
Verified the identification documents(Aadhar card/PAN Card/ Passport /Domain registration)	Only RA	Only RA
Collected the PKCS#10 request for Secure Web Server Certificate		
Creation of user ID		
Request from Subscriber with Request Number.		
Processing		

COST DETAILS

Validity of Test Certificates	Type of Certificate	Amount + GST	Total (Inc. GST*)
6 Months	Class 3 Signing / Encryption	Rupees 1000 + 180	Rupees 1180
6 Months	Class 3 System / SSL	Rupees 5000 + 900	Rupees 5900

Central Goods and Service Tax   18%

CONTACT ADDRESS

IDRBT Certifying Authority,
Road No. 1, Castle Hills, Masab Tank, Hyderabad – 500 057, India.
Phone: +91 40 23294217/19/21/23 /Fax: +91 40 23535157
Email: cahelp@idrbt.ac.in
Website: http://idrbtca.org.in

<mark>SUBSCRIBER AGREEMENT</mark>

The purpose of this agreement is to establish the contractual relationship between the IDRBT CA and the Applicant/Subscriber. The issue and subsequent use of public keys and Certificates issued, constitutes acceptance of this agreement, the terms and conditions of the IDRBT CA Certification Practice Statement ("IDRBT CA CPS") associated with the keys and Certificates issued to the Subscriber. The IDRBT CA CPS is amended from time to time, and is published on the INFINET in IDRBT CA's repository at http://idrbtca.org.in/repository.htm and http://idrbtca.org.in/cps.html and is available via E-mail from: cahelp@idrbt.ac.in .

Important Notice:

THE SUBSCRIBER MUST READ THIS SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGITAL CERTIFICATE FROM IDRBT CA. IF THE SUBSCRIBER DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE DIGITAL CERTIFICATE.

THE SUBSCRIBER AGREES TO USE THE DIGITAL CERTIFICATE AND ANY RELATED IDRBT CA CERTIFICATION SERVICES ONLY IN ACCORDANCE WITH THE IDRBT CA CPS.

Indemnity

The Subscriber agrees to:

1. accept responsibility for the safety and integrity of private keys, if keys or Certificates are compromised the Subscriber will immediately notify the IDRBT CA, as well as any other users with whom you exchange information;
2. indemnify IDRBT CA for any loss to any person or Organization arising from the failure to ensure the safety and integrity of your private keys and Digital Certificates;
3. indemnify and hold harmless IDRBT CA from any and all damages and losses arising out of
   a) use of an IDRBT CA issued Digital Certificate in a manner not authorized by IDRBT CA;
   b) tampering with the Digital Certificate; or
   c) any misrepresentations made during the application and use of the Digital Certificate.
4. assure and hold harmless IDRBT CA from and against any and all damages (including legal fees) of lawsuits, claims or actions by third-parties relying on or otherwise using a Certificate relating to:
   a) Subscriber's breach of its obligations under this agreement;
   b) Subscriber's failure to protect his/her Private Keys;
   c) Claims arising from content or other information or data supplied by Subscriber; or

Use of Keys and Certificates

The subscriber agrees:

1. that true complete and accurate information has been provided in applying for these keys and Certificates, and further undertakes to promptly notify IDRBT CA in the event that this information changes;
2. to immediately inform IDRBT CA if it is known or suspected that a private key has or may have been compromised;
3. that use of the Digital Certificates are at their sole risk;
4. to use Digital Certificates strictly for lawful purposes and will not infringe a third party's rights; and
5. that use of the private key and/or its associated Digital Certificate constitutes acceptance of the terms of the IDRBT CA CPS.
6. that Erroneous utilization of the Digital Certificates or violation to the practices specified in

IDRBT CA CPS shall be liable to be proceeded against, both under the relevant civil and criminal laws, and shall be subject to punishment under the Information Technology Act, 2000 or/and any other relevant law/s of the land. The duties of the subscribers to be followed are described in the Chapter VIII of The Information Technology Act, 2000.

7. that IDRBT CA disclaims all warranties, except as expressly provided in the IDRBT CA CPS.IDRBT CA makes no representations or warranties, express, implied or otherwise relating to IDRBT CA Digital Certificate or any services provided by IDRBT CA in connection therewith, including without limitation any warranty of non-infringement, merchantability or fitness for a particular purpose.

The Subscriber demonstrates his/her knowledge and acceptance of the terms of this subscriber agreement by either (i) submitting an application for a Digital Certificate to IDRBT CA, or (ii) using the Digital Certificate issued by IDRBT CA, whichever occurs first.

Declaration by the Subscriber

I, hereby declare that I have read and understood the IDRBT CA CPS and the terms and conditions of this Subscriber Agreement. I shall abide with IDRBT CA CPS and the terms and conditions of this Subscriber Agreement.

Date:

Place:

Name of the Subscriber: **Subscriber's (Applicant)**
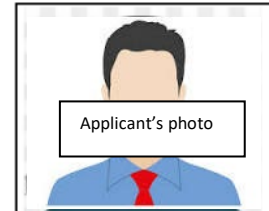**Signature**

Annex-Physical Verification

(On Bank Letter Head)

Date:

Applicant's photo

Superior's Signature across the photo

To

The Director
IDRBT Certifying Authority
Road no. 1, Castle Hills
Masab Tank,
Hyderabad – 500057

Dear Sir,

Physical Verification for issue of Class 3 Digital Signature Certificate (DSC)

This is to certify that I have done physical verification of the applicant Sri/Smt_Milan Damji_ who has applied for a Class 3 Digital Signature Certificate from IDRBT-CA, who's PAN Number is _____ZZZPD1985J_____, Aadhar Number is __9999 7777 8888__ and Employee/ Employee ID Number is _____1234Z____ on Date ___dd/mm/y. I have satisfied myself with applicant's identification and also taking responsibility of authenticity of the same. This certificate is in accordance with the requirement of the guidelines issued by the Controller of Certifying Authorities (CCA), Government of India.

A Copy of the PAN/Aadhaar & Employee ID of the applicant, attested by me is also attached herewith.

This certificate is given in-lieu of the applicant's physical presence at the Registration Authority (RA) of the bank or identification through Video Verification service provided by IDRBT-CA, which I declare could not be performed in the applicant's case because __Reason___.

Hence, I request you to accept the application for the DSC and issue the Digital Certificate to the above mentioned applicant, based on this certificate of physical verification.

Yours faithfully,

Superior Authority's Signature

(Superior Authority)

Name   :
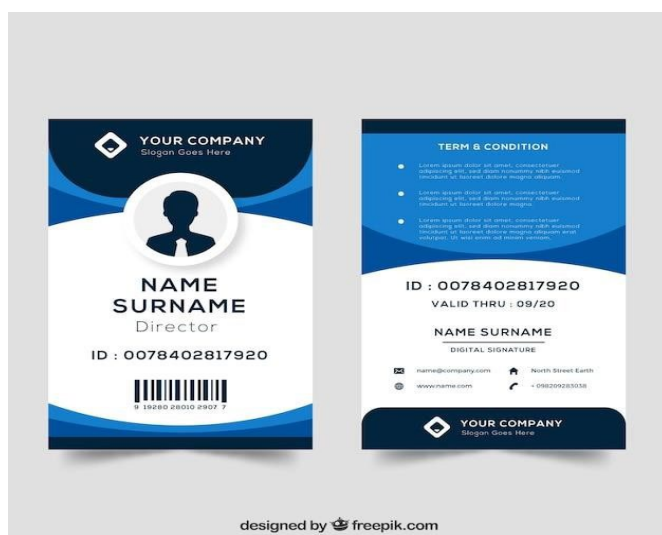
Designation   :

Mobile Number:

Seal   :

Applicant ID Proofs

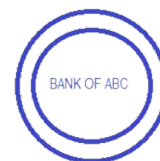Pan Card

Bank Employee ID

Aadhar Card

Applicant's Signature

milan

Superior's Signature

Vidyabagchi

BANK OF ABC

Note: All the respective ID proofs must be scanned in one page together.

Superior ID Proofs

Pan Card

Bank Employee ID

Aadhar Card

Superior's Signature

Vidyabagchi

Note: All the respective ID proofs must be scanned in one page together.

emBridge Installation Procedure

Download appropriate emBridge.exe from the Link depending on your operating system – Windows/Linux/etc.

https://embridge.emudhra.com/index.jsp#

Figure 1

1. *Install emBridge with admin rights. (If you do not have system admin rights, please contact your system admin department to install it.)*

2. Click on the **emBridge.exe** file and follow the below-mentioned steps.

3. After clicking the **emBridge.exe** file, Browse to the location where emBridge should be installed on your system. Specify the path, or it will default to a common folder. After selecting the location, click the "Next" button, as shown in Figure 1.

4. Click the "Next" button, as shown in Figure 2.
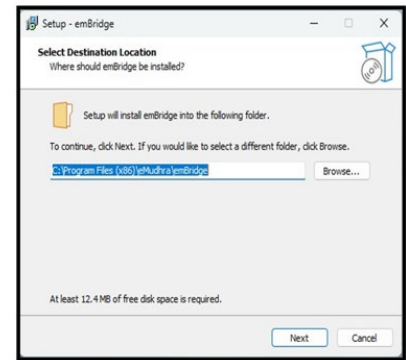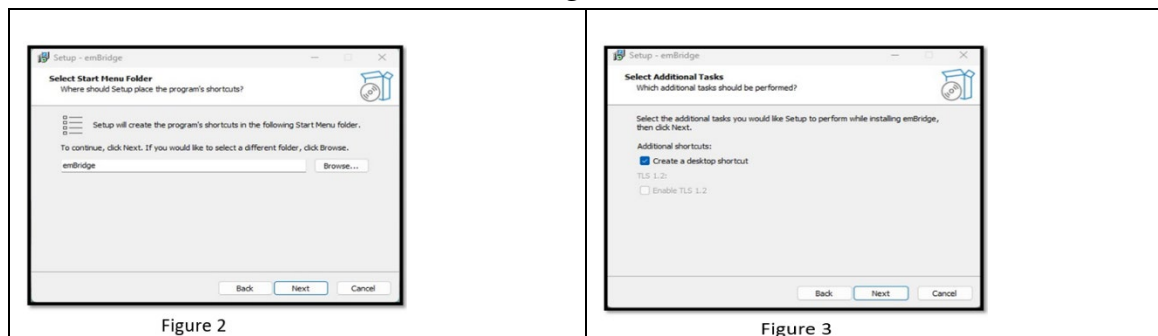
Figure 2

Figure 3

5. Click on "Check box" to add desktop shortcut as in Figure 3.
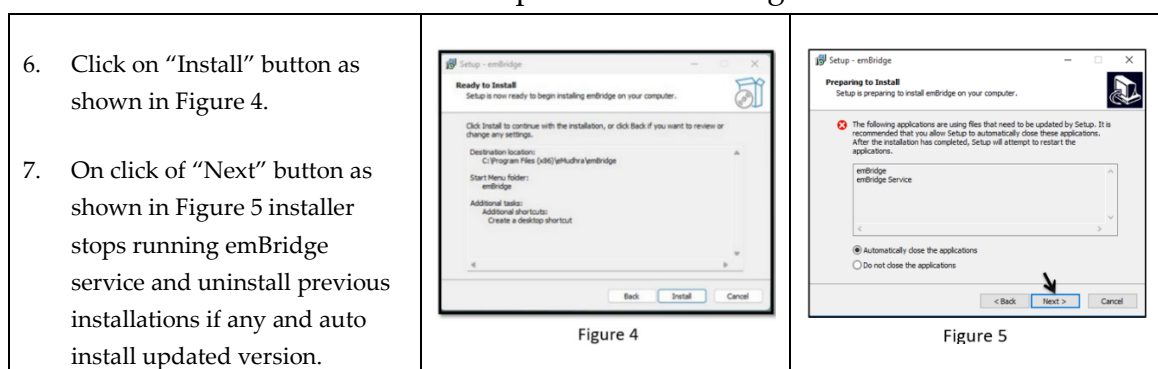
6. Click on "Install" button as shown in Figure 4.

7. On click of "Next" button as shown in Figure 5 installer stops running emBridge service and uninstall previous installations if any and auto install updated version.

Figure 4

Figure 5

8. emBridge is successfully installed in your PC click "Finish" button to complete the installation as shown in Figure 6. 9. Launch the application "emBridge" by clicking on the icon in desktop as shown in the Figure 7, to check running status.	 Figure 6	
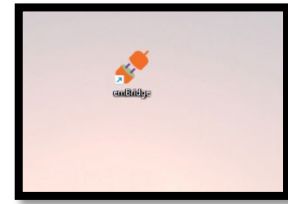
PKI Token Installation Guide

Step 1: Preparing for installing PKI Token

Before installing PKI Token Runtime, make sure the following requirements are satisfied:
Your computer has at least one functional USB port available.

- Your BIOS supports the USB device, and USB support has been enabled in CMOS settings.
- USB extension or hub available (optional).
- **HYP2003 Token (HYPERPKI - FIPS 140-2 Level 3 Certified) available. The bank may purchase these Tokens from their suppliers.**
- Administration Credentials will be required, if the token has to be installed within LAN.

Step 2: Installing PKI Token Runtime

1. Insert the **HYP2003** PKI Token.

1st. In explorer → Locate the file **"HyperPKI_HYP2003_Setup.exe"** and double-click to open it. 2nd. After clicking the **setup.exe** file, the following welcome interface will appear	
	If you do not have system admin rights, you will be prompted for a username and password. In that case, please contact your system admin department to install it.
 Figure 3: Welcome Interface	 Figure 4:Select Install Path
Choose CSP interface will appear. 2. After selecting the Private CSP, click "Install" to continue. Once the installation process is complete, the following interface appears.	
3. Click "Finish" to complete the installation process	
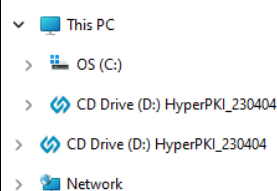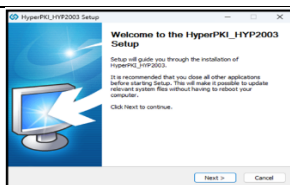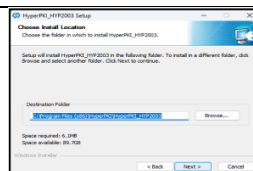
Annex- Download DSC in PKI Token

1. Once you receive the approval email with your **Application Number** and **Download PIN**, log in to the Subscriber Portal using your email ID and password.

2. The banks/entities may get the specified USB Dongle from the indicative list of suppliers' available on the following Link :
   https://idrbtca.org.in/Download/VendorsListforsupplyofUSBTokens.pdf

3. After logging in, click on the **Download** option to proceed.
4. Enter the Application ID and Download PIN received in the email into the respective fields.
5. Insert the USB token, select it from the dropdown, enter the token password, agree to the terms, and click Download.

USB Token Suppliers List (Indicative List)

The CCA guidelines require USB tokens to be FIPS 140-2 Level 3 certified, have unique manufacturer-based serial numbers, and enforce strict PIN policies, including mandatory PIN changes at the time of download and no option for PIN resets.

S No	Name Of the Vendor	Product with Product series
1	**WATCHDATA TECHNOLOGIES (India) PVT. LTD** #2370, 19th Cross, Banashankari 2 Th Stage, KR. Road, Bangalore 560070. Contact Person: Jagadish Sales Manager Tel/Fax: +91-080-26762012 Mobile: +91-9900191968 / 9964269100 E-Mail: jagdish.rohit@watchdata.com.sg Website: www.watchdata.com/	PROXKey - WD
2	**PAGARIA ADVISORY PRIVATE LIMITED** 901-902, Mayuresh Square, Plot - 17, Sector -15, CBD Belapur, Navi Mumbai, Maharashtra – 400614 Email: ankush@pagariagroup.com Mob: +91 9323251252 Knowledge Portal : www.knowledge.cryptoplanet.in Ticket Support : www.support.cryptoplanet.in IVR: +91 93336 93336	PROXKey - WD

3	**CHARTERED INFORMATION SYSTEMS PVT LTD** #222-223, Durga Chambers, 1334/35, Desh Bandhu Gupta Road, Karolbagh, NEW DELHI – 110 005 INDIA #110, Hari-Om Plaza, Building No 3, Opp. National Park,M G Road, Borivali (E), Mumbai - 400 066 INDIA "Chartered House", Near Lata Mangeshkar Musical Park, Bhandara Road, NAGPUR – 440 008 INDIA #207-B, Wing A, Brigade Majestic, 1st Main (Kalidas) Road, Above AirTel Gallery, Gandhi Nagar, Bengaluru – 560 009 INDIA Contact Person: Navneet Vasant Mobile: +91 9860 561871 Email: navneet@charteredinfo.com	HYP2003 - HS
4	Thales DIS India Private Limited M/s Thales DIS India Private Limited Plot no C-001A/2,3-8 Floor Berger Tower Section-16B, Gautam Buddha Nagar, Noida, UP, IN, 201301 Contact details: Pratik Sangoi E-Mail: pratik.sangoi@thalesgroup.com Mobile : +91 96198 61691 Santhosh Raju E-Mail: Santhosh.raju@thalesgroup.com Mobile : +91 90366 37033 Website: https://cpl.thalesgroup.com/access-management/authenticators/pki-usb-authentication	Thales safenet etoken 5110 - TH