HYPERSECU®

Windows User Guide for HYP2003

HyperPKI USB Token

09/09/2022

HSTE-NB0064-IND-RV1.2

HYPERSECU INFORMATION SYSTEMS INC

200-6191 Westminster Hwy, Richmond BC, V7C 4V4 Canada
1-604-279-2000 | hypersecu.com

Table of Contents

Document History

Version	Release Date	Description of Changes	Document Owner	Approved By
1.2	2022-09-09	Original document	NB	JL

Software Developer's Agreement

All Products of Hypersecu Information Systems Inc, including, but not limited to, evaluation copies, diskettes,

CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.
2. Prohibited Use – The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Hypersecu provided enhancement or upgrade to the Product.
3. Warranty – Hypersecu warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.
4. Breach of Warranty – In the event of breach of this warranty, Hypersecu's sole obligation is to replace or repair, at the discretion of Hypersecu, any Product free of charge. Any replaced Product becomes the property of Hypersecu.

   Warranty claims must be made in writing to Hypersecu during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Hypersecu. Any Products that you return to Hypersecu, or a Hypersecu authorized distributor, must be sent with freight and insurance prepaid.

   EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
5. Limitation of Hypersecu's Liability – Hypersecu's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Hypersecu be liable for any damages caused by your failure to meet your obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Hypersecu has been advised of the possibility of damages, or for any claim by you based on any third-party claim.
6. Termination – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

Getting Started

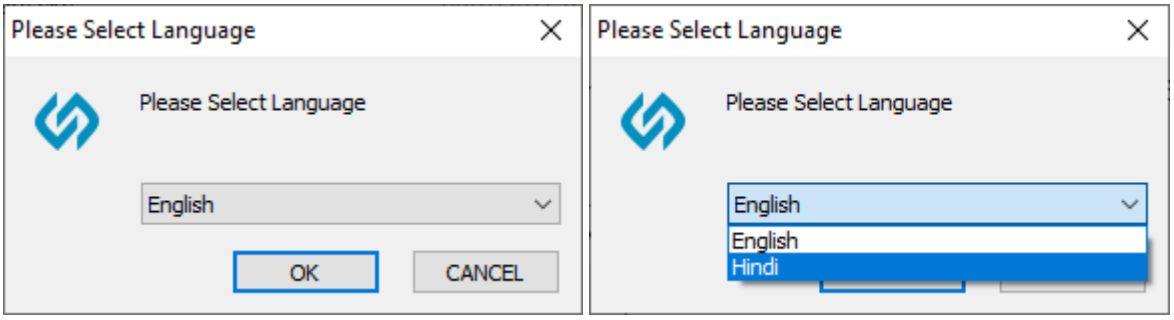
Requirements

Before installing HyperPKI Token Manager for the HYP2003 be sure the following requirements are fulfilled:

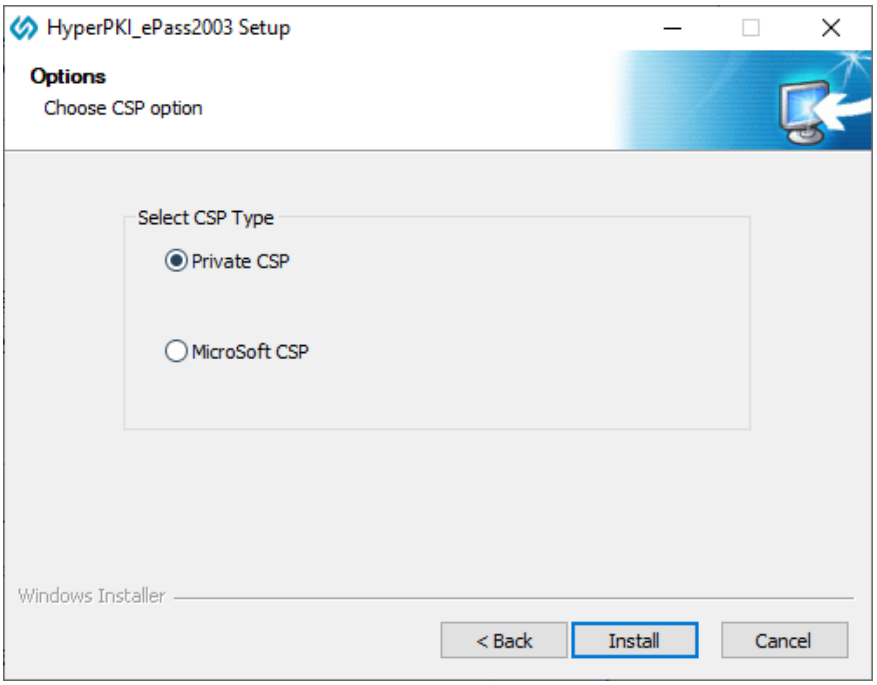
- Windows (2000/XP/2003/Vista/2008/7/8/10) x86/x64
- The latest version of HyperPKI Token Manager for Windows
- At least one available supported USB port
- HyperPKI HYP2003 USB token

Installing HyperPKI Token Manager

1. Execute the setup file for HyperPKI Token Manager and select the language you want to use, then click **OK**.



2. Click **Next**, then choose the installation location and click **Next** again.
3. Choose the CSP option you want to use:
    - Choose **Private CSP** to use the CSP provided by Hypersecu. The CSP name is "EnterSafe HYP2003 CSP v2.0".
    - Choose **Microsoft CSP** to use the CSP provided by Microsoft.



IMPORTANT: For Windows Vista and above, Microsoft has integrated a smart card minidriver into Windows and will perform an automatic installation of the Microsoft Base CSP through a system update without a redundant installation package or complicated installation process necessary.

For Windows XP and below, you may need to manually install the base CSP using the system patch KB909520 before you can select the Microsoft CSP option. If you do not have the Microsoft Base CSP installed, the **Microsoft CSP** option will be disabled. For more information or assistance, contact Microsoft Support.

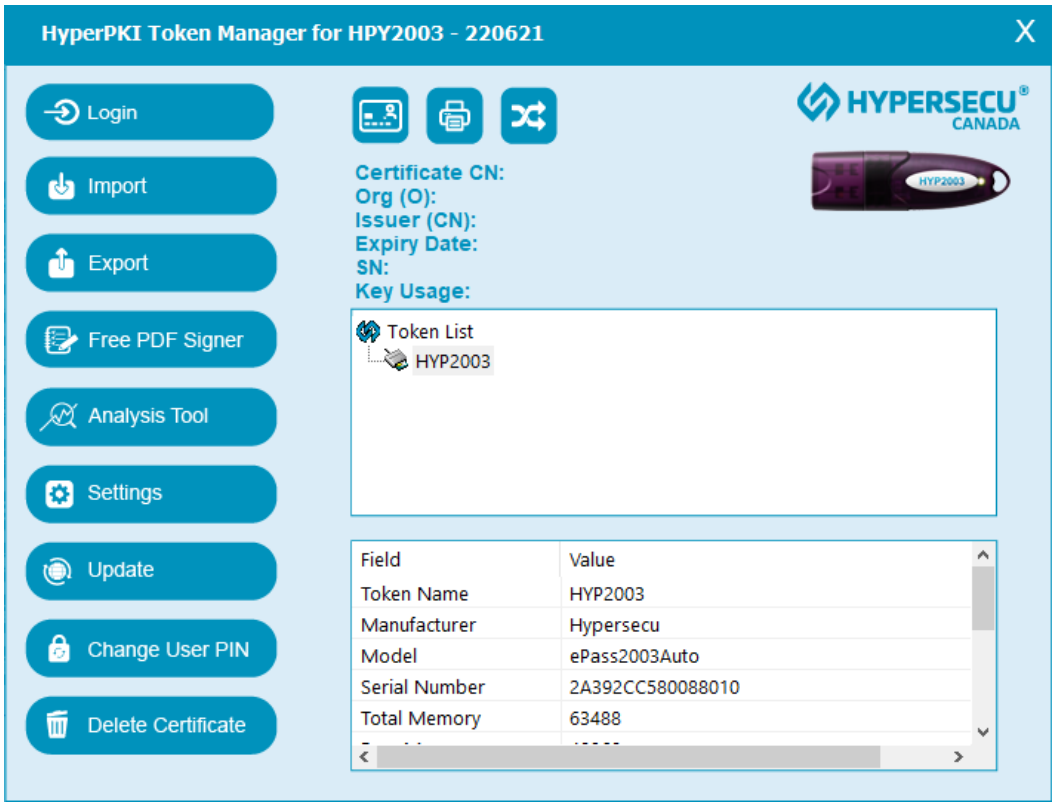
If you do not have access to the Internet, we can provide an installation package.

---

4. Click **Install** to proceed with the installation process, then click **Finish** to complete the installation.

HyperPKI Token Manager Interface

Some features and information will not be available unless a valid HYP2003 token is inserted. After you've inserted an HYP2003 token and logged in, you can view details regarding the token, stored certificates, and more.



Using HyperPKI Token Manager, you can perform the following tasks and more:

- Rename your token
- Change your user PIN
- Import, export, and delete certificates

NOTE: The total private memory space and free private memory space refer to the PIN-protected spaces. Since the private key is highly sensitive and is managed by the COS, the HyperPKI Token Manager interface will not display the total private memory space and the free private memory space.

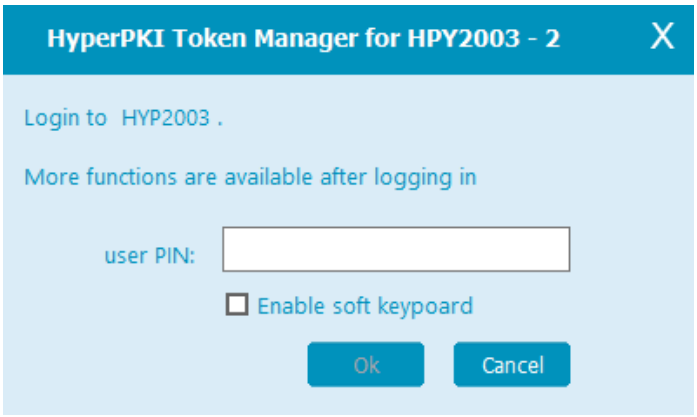
Logging In

Before you can log in, make sure your HYP2003 token is inserted into a valid USB port.

IMPORTANT: Each token has a set number of log in attempts. If you attempt to log in with the incorrect PIN too many times, your token may be locked from further login attempts and you will not be able to perform any operations with the token until it is unlocked. If your token is locked, contact your system administrator to unlock the token and reset your PIN.

---

1. If you have more than one HYP2003 token inserted, select the one you want to log in to from the token list.
2. Click **Login**, then enter your PIN and click **OK**.



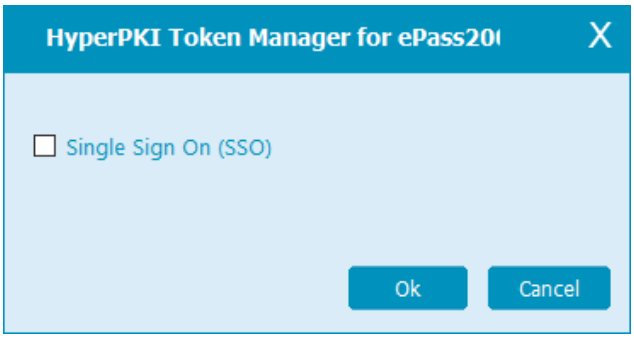
NOTE: When the PIN input dialogue box is displayed, the HyperPKI Token Manager will enable safe desktop. In this mode, only the PIN input dialogue box is highlighted, and most other operations are disabled. The default PIN is **12345678**.

TIP: To enable soft keyboard for extra security, check the **Enable soft keyboard** box. The physical keyboard will be disabled while the soft keyboard is enabled.

Enabling Single Sign-On (SSO)

You can enable Single Sign-On when logging in to HyperPKI Token Manager

1. Click **Settings.**
2. Check the **Single Sign On (SSO)** box.



3. Click **OK.**

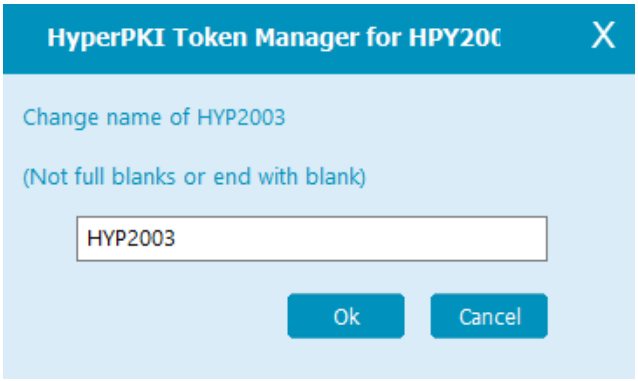
Token Management

You can only log in to and manage one token at a time. To manage another token, you must log out and log in to another token.

Renaming Your Token

You can rename your token at any time. Giving your token a unique name will help differentiate it if you have more than one token.

1. Click the **Change Token Name** button 
2. Enter a name for your token. Names cannot contain a space.



3. Click **OK**.

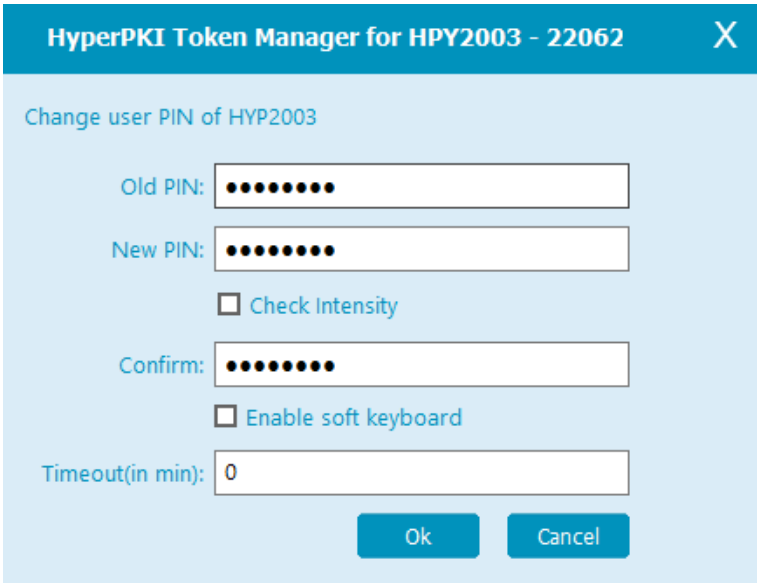
Changing Your User PIN

You can change your HYP2003 token's user PIN at any time. The PIN can't be changed if the token has been blocked. If your token is blocked, you must contact a system administrator to unblock your token.

NOTE: All PINs must contain 4 or more characters.

To change your token's user PIN:

1. Click Change User PIN.



2. In the Old PIN field, enter your current PIN.
3. In the New PIN field, enter the new PIN you want to use.
4. In the Confirm field, enter the new PIN again to confirm.
5. Click **OK** to finish.

TIP:
To enable soft keyboard for extra security, check the **Enable soft keyboard** box. The physical keyboard will be disabled while the soft keyboard is enabled.

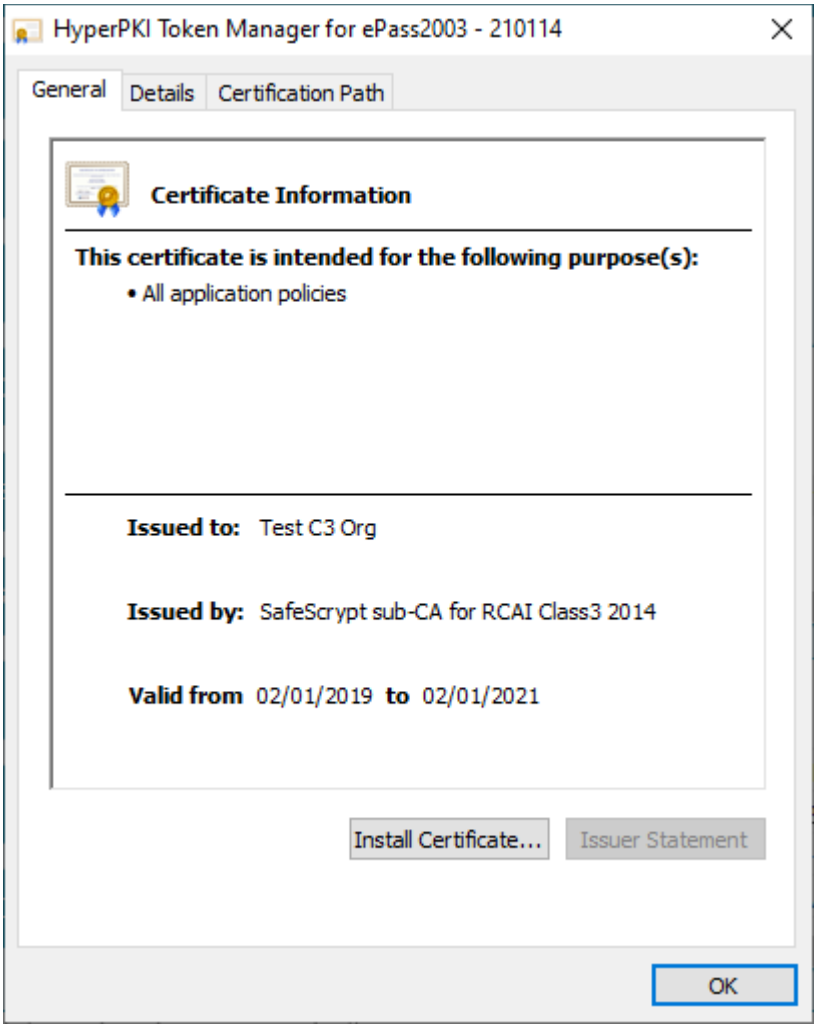
To check the security of your chosen PIN, check the **Check intensity** box. Your PIN will be ranked from Low security (red) to High security (green).

Certificate Management

Each HYP2003 token can store multiple digital certificates and key-pairs. They are used for encryption, decryption, authentication, and digital signing.

Viewing Certificate Information

1. Select the container with the certificate you want to view and expand the content by clicking "+" or double clicking the container.
2. Double click the certificate or click the **View Certificate** button to see details such as:
    - The validity of the certificate
    - The certificate's issuer
    - The certificate's expiry date



3. Click **OK** when you're finished viewing.

Importing a Digital Certificate

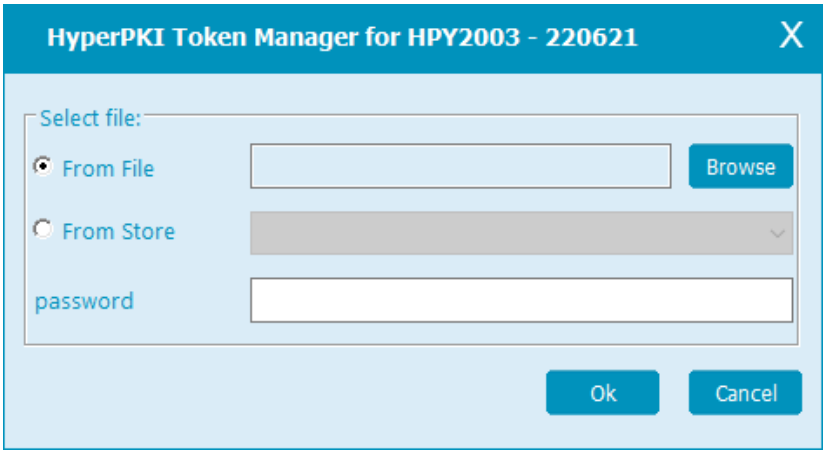
The HYP2003 supports the following types of digital certificates:

- P12
- PFX
- CER

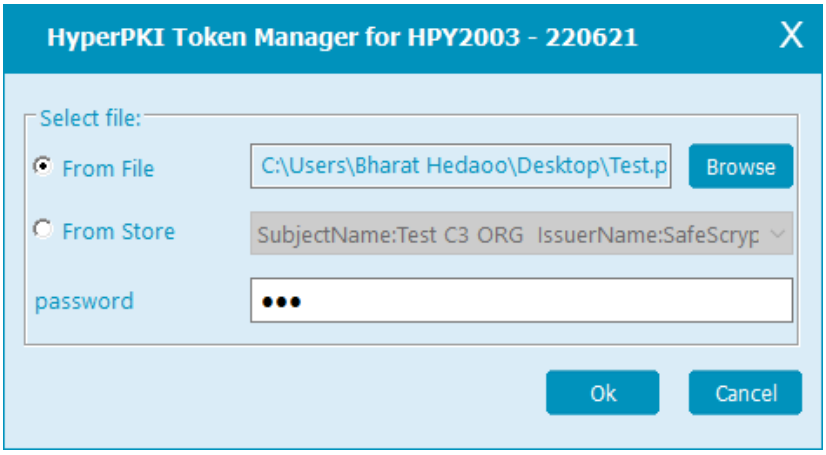
P12 and PFX type certificates contain a key-pair (a public key and a private key). CER type certificates do not.

Certificates can be imported from a file or from the certificate store.

1. Click **Import**
    - Choose **From File** to import from a file, then click **Browse** to choose the certificate file you want to import. Enter a password if necessary.



    - Choose **From Store** to import from the certificate store, then select a certificate from a list of available certificates.



2. Click **OK** to complete the import.

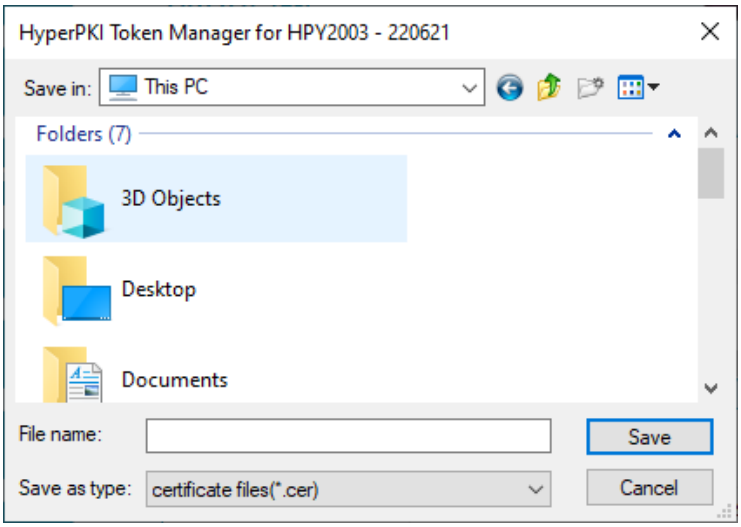
Exporting a Digital Certificate

You can export a digital certificate from the HYP2003 token as a file.

NOTE: If the digital certificate contains a key-pair, the private/public key cannot be exported.

To export a digital certificate:

1. Select the certificate you want to export.
2. Click **Export**, then choose the file location you want to save the exported certificate in.



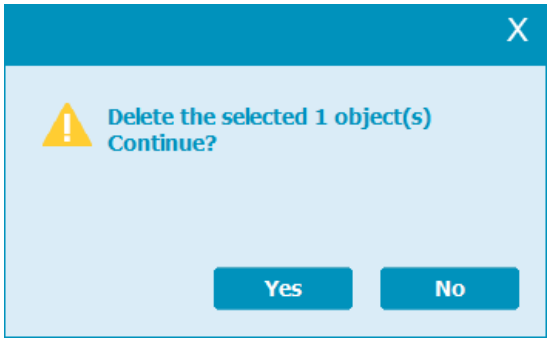
3. Click **Save** to complete the export.

Deleting a Certificate

You can delete any digital certificate or container. This process cannot be reversed. Be sure you want to delete the certificate or container before doing so.

NOTE: You can also select the token and delete all its contents. This includes all certificates and keys in the token.

1. Select the container or certificate you want to delete.
2. Click **Delete** and confirm you want to proceed.



IMPORTANT: Do not remove the token until the deletion process has been completed.

Free PDF Signer

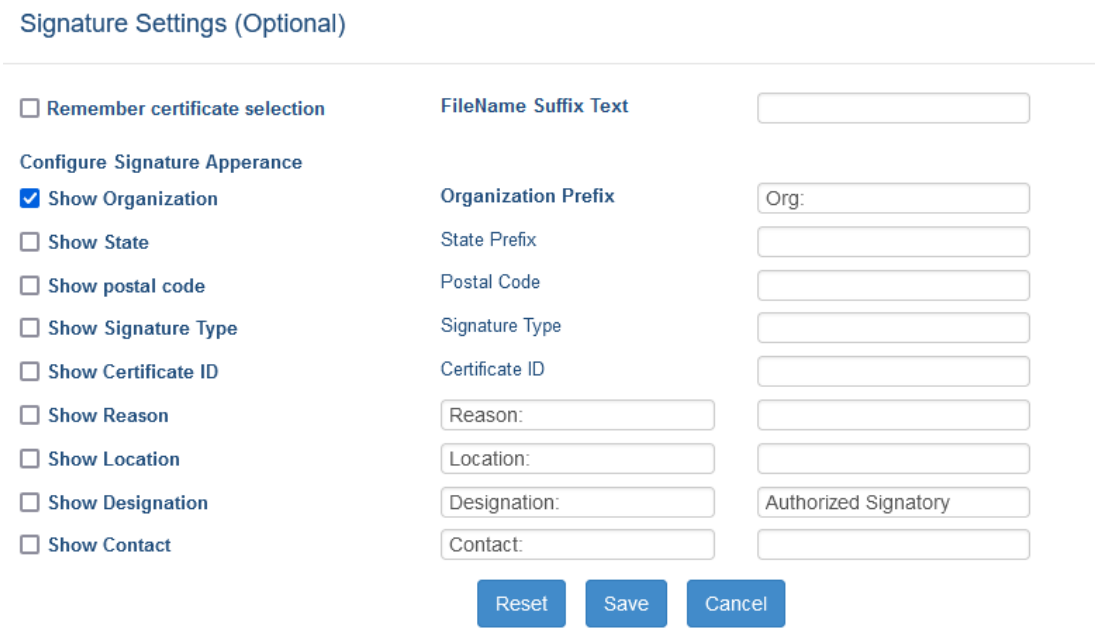
Upon installation of HyperPKI Token Manager, the Signer.Digital extension will be added to your Chrome browser.

NOTE: Make sure that the Signer.Digital extension is enabled in your Chrome browser. If you are using Firefox or Microsoft Edge, the extension must be installed manually.

Firefox:
https://addons.mozilla.org/en-US/firefox/addon/signer-digital

Microsoft Edge:
https://chrome.google.com/webstore/detail/signerdigital/glghokcicpikglmflbbelbgeafpijkkf

1. In the HyperPKI Token Manager, click **Free PDF Signer** to open a web address (https://web.signer.digital/InteractiveSigning) in your default browser. You can bookmark this address in your browser to directly open it.
2. Click the **Sign Setting (Optional)** button.
3. Configure the settings you want, then click **Save**.



4. Enter the required CAPTCHA, then click the **Browse** button.

5. To add text to the PDF, click the **Add Text Annotation (Optional)** button.
6. Once the PDF is ready to sign, click the **Sign PDF** button and draw the signature box where a signature is required.
7. Release the mouse to finish drawing the box and select the certificate you want to use to sign the PDF.
8. Enter the PIN to sign the PDF and save the file.

NOTE: All signing processes are performed in the system memory cache. No information is shared over the Internet for security purposes.

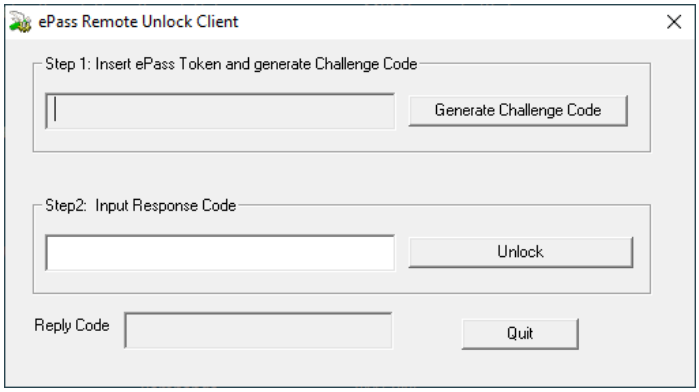
Troubleshooting

Unlock or Reset User PIN

A token may be locked due to a variety of security reasons, including if a user has exceeded the number of allowable user PIN attempts. Once a token has been locked, it must be unlocked before it can be used again.

NOTE: Make sure you have the latest HYP2003 drivers installed before beginning. Remote Unlock Client only works on driver versions 180929 and above. Click **Update** if your driver version is a previous version.

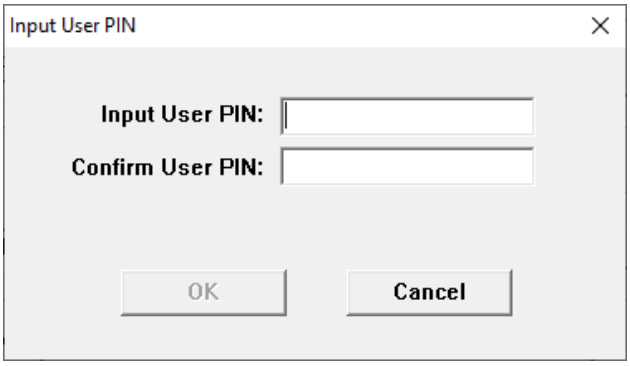
1. Download Remote Unlock Client from `https://taxpro.co.in/DSC/TokenDrivers/RemoteUnlockClient.zip` and extract the file.
2. Run `RemoteUnlockClient.exe` and insert the HYP2003 token you want to unlock.



3. Click **Generate Challenge Code.**
4. If you receive the Reply Code `SN¡¢Cert Transmit Success`, check the email address given in the DSC present in the token for the activation/response code.

NOTE: The activation/response code is sent from the email address `tokenunblock@charteredinfo.com`. If you are not sure how to access the registered email address present in the token's digital certificate, see *Identifying Your Token's Registered Email*.

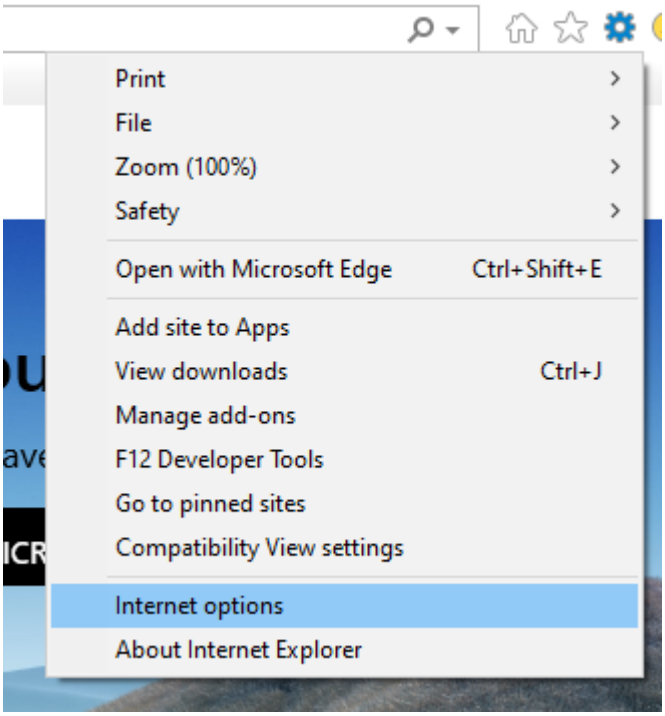
5. Enter the received activation code in the Input Response Code field, then click **Unlock**.
6. Enter the new User PIN and confirm the User PIN, then click **OK**.



Identifying Your Token's Registered Email

To identify the registered email attached to your token's certificate:

1. Make sure your HYP2003 token is plugged in, then open Internet Explorer.
2. Click on the Tools menu and select **Internet options**.



3. Navigate to the Content tab, then click **Certificates**.

4. Select the certificate that is on the token and click **View**.
5. Navigate to the Details tab, then scroll to find the field **Subject Alternative Name**. This field will list the email registered to the Digital Signature Certificate.

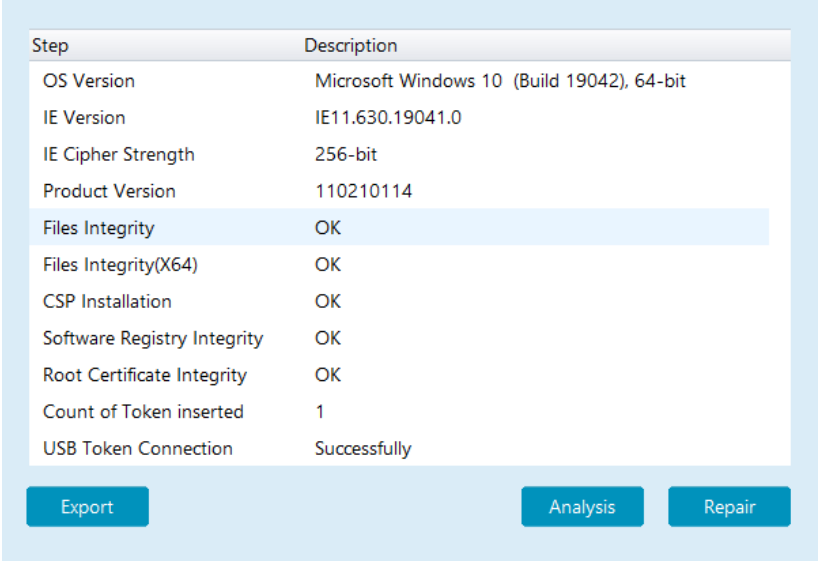
Analysis Tool for Analysis and Repair

In cases where analysis and repair are required, you can run the Analysis Tool to do so. The following enhancements and features have been added to the tool:

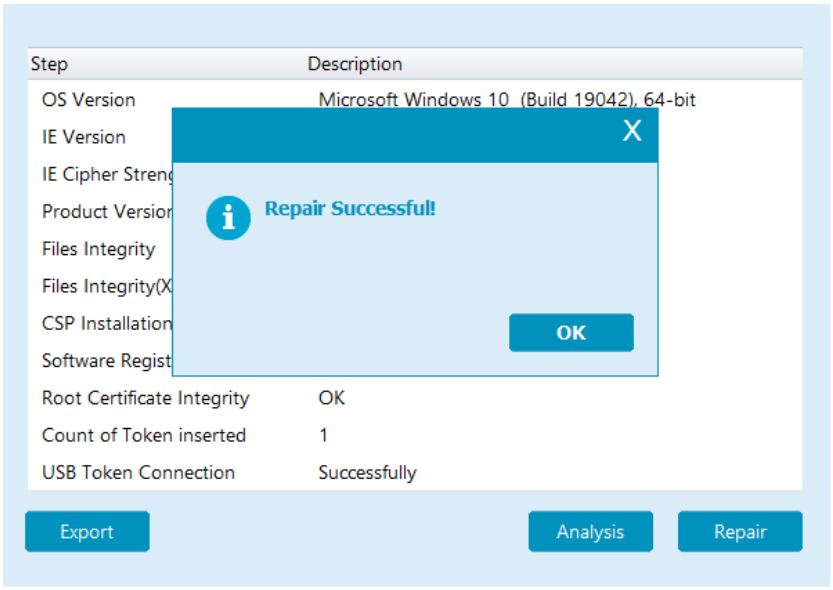
- Check and repair ActiveX settings in Windows
- Check the Java version installed. If the system does not have Java installed, a link to install Java will open
- Check and repair Java plug-in settings in Windows
- Check and install necessary DLL files for using digital certificates in Windows

To run the Analysis Tool:

1. Click **Analysis Tool**, then click **Analysis**



2. Once analysis has completed, click **Repair**.



Uninstalling HyperPKI Token Manager

1. In the start menu, perform one of the following operations:
    - Navigate to **Add or Remove Programs** in the Control Panel, then choose **HYP2003 (Remove only)** and click **Change/Remove**.
    - Navigate to **Hypersecu > HYP2003** in All Programs, then select **Uninstall HYP2003**.
2. In the Uninstall Wizard, click **Uninstall**.
3. Click **Finish** to complete the uninstallation.