Medium Certificate Download

Page Contents

- Page Contents
- Jump to...
- Download MLOA Software Certificates
- Download MLOA Hardware Certificates
  - Hardware Token FIPS Mode Review
    - Hardware Token FIPS Mode Initialization
  - Download Certificates to Token

Jump to...

- FIS Overview
- Medium Level of Assurance (MLOA)
- FIS Get Started
- FIS Register
- FIS Self-Help

ɛdium Certificate Download

ˈe

Download MLOA Software Certificates

Pre-requisites for downloading certificates:

- Completed in-person proofing.
- Received 16-digit passcode from the proofer. If you lose this passcode, you are required to complete a reproofing purchase, and go through the in-person proofing process again.
- Reviewed system and certificate download requirements.

To download certificates:

Step 1. Go to the **My Account** tab, and click the **Manage Certificates** tab.

Step 2. Enter the passcode provided to you by your proofing agent during your in-person proofing appointment. This passcode is only valid after you receive an FIS approval email from Exostar.

NOTE: The passcode is a 16-digit number separated by hyphens; for example: 1234-5678-1234-5678. You must enter all characters, including hyphens (or leave hyphens out completely). The passcode is NOT the same as your Managed Access Gateway (MAG) log-in password.

Step 3. Archive the **encryption key**. If your passcode is correct, you will see the list of certificates you can download. The system automatically selects all certificates for download. Click **OK** to archive your encryption key, and enable key recovery.

NOTE: This activity allows Exostar to archive the encryption key for recovery at a later time. Refer to the **Recover Encryption Key** section for more information.

Step 4. Enable **Strong Protection**. Click **Set Security Level**, and then set the security level to **High**.

NOTE: Exostar strongly recommends you enable strong protection for your MLOA certificates, unless there are corporate policies against doing so.

Step 5. By default, the **Medium** option is already selected. Change this to **High** and click **Next**.

Step 6. Provide a password for this certificate. Please note you need to provide this password each time you use your certificate.

Step 7. The system displays the new security level. Click **OK.**

Step 8. Download the certificates. The system prompts you for the password set in step 6, to download the certificates. Once you enter the password, click **OK**.

Step 9. Once the download is complete, a confirmation message displays.

NOTE: Refer to the FAQ page for information on any certificate download errors.

Download MLOA Hardware Certificates

To download the MLOA hardware certificates, complete the following tasks:

- Acquire the appropriate token. Exostar ships your token via FedEx once you schedule your in-person proofing appointment. If you have not received your token, reach out to Customer Support.
- Install the token PKI Client middleware on your machine. Contact your token vendor for appropriate information, or your IT Support for organization specific information.
- Complete a system check to ensure you are able to download the certificates.
- Initialize the token in FIPS 140-2 mode. For more information on how to check for FIPS mode, refer to the **Hardware Token FIPS Mode Review** s ection for details.
- Ensure you have been provided the initial token password to enable you to complete token installation. Contact your vendor to receive the initial password. You are required to enter a password for this token during the certificate download process.
- Complete the in-person proofing process.
- Receive the 16-digit passcode from the proofing agent at the end of your in-person proofing appointment. If you lose this passcode, you are required to complete a reproofing purchase, and go through the in-person proofing process again.

Hardware Token FIPS Mode Review

Exostar's Medium Level of Assurance Hardware (MLOA) digital certificates are 2048 FIPS 140-2 compliant. To ensure the tokens also comply with the FIPS 140-2 compliance, review the token information.

NOTE: You must review this information **BEFORE** downloading the digital certificates.

Step 1. If you completed the initial password change process for your token, plug the token into your USB drive. The **eToken PKI Client Properties** scree n displays for the Aladdin eToken PRO (72K) Java.

Step 2. Click on **View eToken Info** to display the token details.

Step 3. Scroll through the list, and search for **FIPS Mode** and **Supported Key Size** under the Name column. If the token does not display information on **F IPS Mode**, you must follow the steps below to initialize your token in the FIPS Mode.

NOTE: Make sure the **Supported Key** size is 2048. Any certificates on the token are invalid for FIPS 14-compliance. If you already have certificates installed on the tokens, re-initialize the token.

Hardware Token FIPS Mode Initialization

Step 1. Click **eToken Pro Java.**

Step 2. Select the **Initialize eToken** icon to display the initialize screen.

Step 3. Click the **Advance View** icon on the **PKI Client**. If this button is unavailable, contact your **IT Administrator** or **FISA** (FIS Administrator) for additional information on how to set-up the token in the FIPS mode.

Step 4. Check the box for **FIPS mode**, to set-up the FIS mode for the token. Click **OK** to complete.

Step 5. On the **Initialize eToken** screen, click **Start.**

Step 6. Select **OK** to start token initialization.

Step 7. Once you successfully initialize your token, a confirmation screens displays. Click **OK.**

Step 8. You are redirected to the **PKI Client** main screen. Select **View eToken Info.**

Step 9. The **FIPS Mode** displays. Click **OK**.

Download Certificates to Token

Before you begin downloading your certificates, install the PKI Client on your computer, as well as change the initial password of your token. Once you complete this, please follow the steps below:

Step 1. Plug the token into your USB drive, and make sure you are logged into your Managed Access Gateway (MAG) user account.

Step 2. Go to your **My Account** tab and then click the **Manage Certificates** sub-tab.

NOTE: The **Download Certificates** sub-tab is only visible under the **Manage Certificates** tab when you have an approved FIS request pending certificate download. If no certificates are available for download, this sub-tab does not display.

Step 3. Enter your 16-digit passcode. At the time of in-person proofing appointment, the proofer provided you a passcode. This passcode is only valid after you receive a packet approval email from Exostar.

NOTES:

- The passcode is a 16-digit number separated by hyphens, for example: **1234-5678-1234-5678**. You must enter all characters, including the hyphens, OR leave the hyphens out completely. The passcode is NOT the same as your Managed Access Gateway (MAG) log-in password.
- If you lose the passcode, you are required to complete a reproofing purchase and complete another in-person proofing appointment.

Step 4. If your passcode is correct, a list of certificates to download displays. The system automatically selects all of them for download. Once selected, you are prompted to enter the hardware token password. Enter the token password and click **OK.**

Step 5. Click **OK**. Certificates are created and archived.

NOTE: This activity allows Exostar to archive the encryption key for recovery at a later time. Refer to the Recover Encryption Keys section for details.

Step 6. Once the archiving process is complete, click **OK** to complete the installation process.

Step 7. You are prompted again for your token password. Enter your password, and click **OK** to import the certificates to your token.

Step 8. Click **OK** to complete the process.

Hardware Token Installation

This section provides instructions on how to install the required software in order for your computer to properly communicate with the Aladdin token you purchased. This token is used to download/access Medium Level of Assurance (MLOA) hardware digital certificates. The software can be loaded by either clicking the links provided below, or by inserting the token into your computer which downloads the middleware automatically. The software required for download is the following: **SafeNet Authentication Client and Exostar Certificate Issuance Software**.

NOTE: Please close all open programs before starting the hardware token installation.

Step 1. Choose one of the links listed below to start the software download process:

- **For computer environments that support 32Bit:** https://portal.exostar.com/safenet/pkianywhere/ExostarSafeNetPKIClientX32v1.exe
- **For computer environments that support 64Bit**: https://portal.exostar.com/safenet/pkianywhere/ExostarSafeNetPKIClientX64v1.exe

Step 2. Please click Yes when the SafeNet Authentication Client Download screen displays to start the download process.

NOTES:

- The **Loading eToken PRO Anywhere** dialog box displays when software files are being installed.
- While Windows configures the SafeNet Authentication Client, a dialog box displays the remaining time.
- After installation, note the SafeNet Icon in the bottom right corner of your desktop. You may need to click on the small arrow, **show hidden icon**.
- After the SafeNet Authentication Client is installed, the **Exostar Certificate Issuance Software Setup** starts to download.

Step 3. Click **Next** on the **Welcome to the Exostar Certificate Issuance Software Setup Wizard** screen to start the download process.

Step 4. Click **Next** on the **Select Installation Folder** screen. We recommend you keep the pre-selected folder.

Step 5. Click **Next** on the **Confirm Installation** screen and click **Close** on the **Installation Complete** screen.

Step 6. Insert the token into your computer and install software components.

NOTES:

- In order for your computer to properly communicate with the token, you must first install the token software, which is provided by the token manufacturer, **SafeNet-Aladdin**.
- When you insert your token for the first time, it may install USB-related software, and request you restart your computer. In such cases, please proceed with a restart.

Step 7. You are prompted to download and install required components (internet connection required). Click **Run Launcher.exe** and follow the prompts.

NOTE: If you are not automatically prompted, open Windows Explorer (right click on the **Start** menu, select **Explorer**), the token displays as a **CD Drive** . Double click on **Launcher.exe**.

Step 8. Unplug the token and reinsert. After a few moments, the token is recognized.

Step 9. You are prompted to change the **Token Password**.

Important: When you use the token going forward, you are required to enter this password. Choose a Token Password you will remember. If you forget this Token Password, you are required to reinitialize your Token and reapply for certificates, **at your expense**.

Default Token Password: 1234567890

Important During installation:

- You must have Administrative rights to your computer.
- You may be prompted by Windows to allow changes to your computer. Select **Yes** or **Allow**.
- Click **Next** when prompted by the installer to accept default options.
- Click **Close** when you see **Installation Complete**.

How useful was this content?

Your Rating: Results: 21 rates