Federated Identity Service (FIS)

Product Guide

January 2025

Contents

Document Versioning

Version	Change Overview	Date
IAM 1.0		June 2018
MAG 7.0		February 2021
MAG 7.2	Exostar's KMA™	July 2021
MAG 7.8	KMA™ and Safenet	December 2024

Document Overview

This document provides step-by-step instructions and process information on Federated Identity Service (FIS)-related content for the user and administrator roles, including Basic Level of Assurance (BLOA) and Medium Level of Assurance (MLOA). This includes:

- System and browser requirements
- Installing PKI Client middleware (for MLOA tokens)
- Registration options
- User processes
- Administrator processes
- End-to-end process for obtaining BLOA certificates
- End-to-end process for obtaining MLOA certificates

Federated Identity Service (FIS) Overview

Exostar's **Federated Identity Service (FIS)** is a comprehensive Public Key Infrastructure (PKI) solution, enabling full lifecycle management of certificates, strong authentication practices, and controlled access to applications through Exostar's Managed Access Gateway (MAG). FIS minimizes risk and assures resources and intellectual assets are protected over the extended enterprise. Since it is operationally modeled after and compliant with CertiPath (the PKI cross-certification bridge) security policies and federal best-practice guidelines, FIS is ideal for enabling sensitive online transactions and secure access to information.

To provide this functionality, a client-side software component is required to generate certificate requests and install certificates on the client's machine (PC). This client-side component is delivered to the client machine in the form of Exostar's Key Management Agent (KMA™). To support the certificate issuance functionality, the user must download Exostar's KMA™ and it must be installed on each client's PC used to obtain certificates. To verify authenticity, the KMA™ is signed using the Exostar code-signing certificate.

It is important to note, your organization must be subscribed to FIS before you can successfully request and download certificates.

Purchase Information

You must complete a certificate purchase via Exostar's web store before proceeding with FIS registration. This section describes the end-to-end purchasing process for MLOA Hardware, MLOA Software, and BLOA certificates.

Web Store Access

To access the web store:

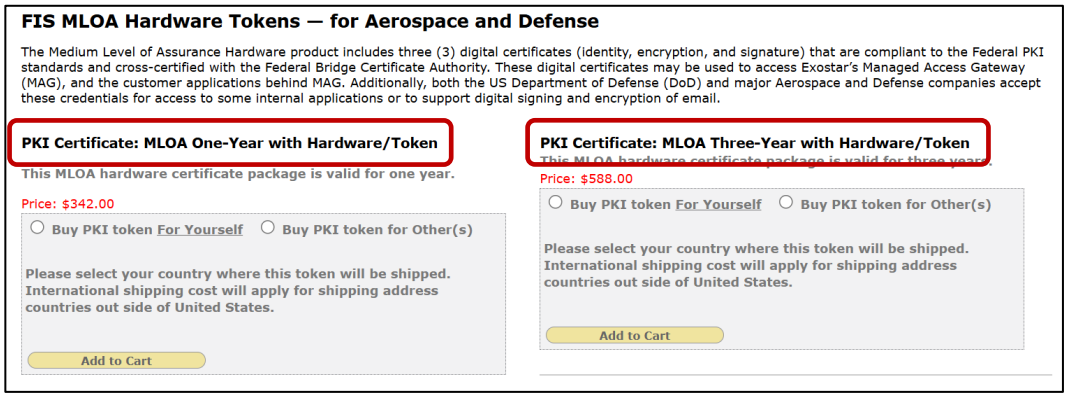
1. Click here to access Exostar's Web Store.
2. Or you can login to your MAG Account, then select **Billing and Support**, located at the bottom of the MAG Dashboard.
3. Next click the **Exostar Web Store – Home Page** tab.

Medium Level of Assurance (MLOA) - Hardware

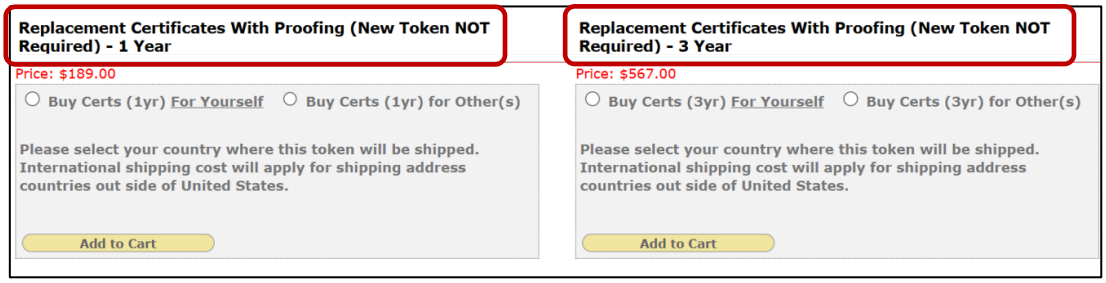
The MLOA Hardware product includes three digital certificates: **identity**, **encryption**, and **signature**. These certificates are compliant to the Federal PKI standards and cross-certified with the Federal Bridge Certificate Authority. You can use these digital certificates to access Exostar's Managed Access Gateway (MAG), and the customer applications behind MAG. Additionally, both the US Department of Defense (DoD) and major Aerospace and Defense companies accept these credentials for access to some internal applications or to support digital signing and encryption of email.

Please follow the steps below to complete an MLOA Hardware-related purchase:

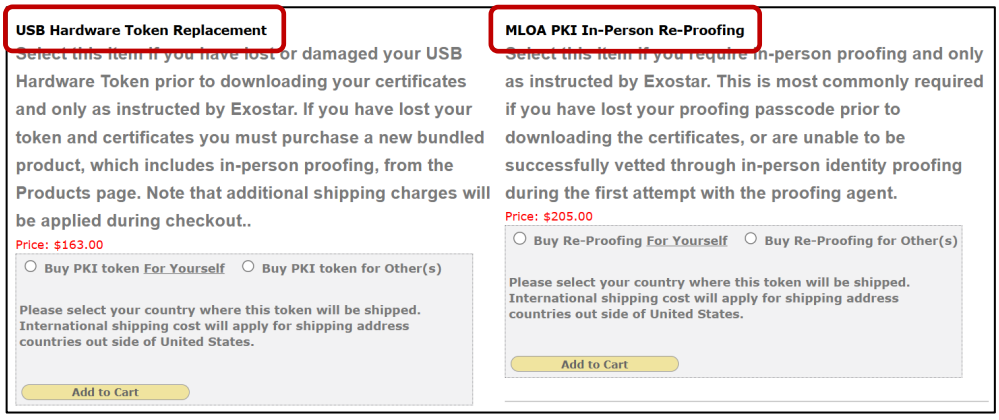
1. Select the **Purchase Now** link located next to **Medium Level of Assurance (MLOA) – Hardware**. Choose one of the following product options:
   - **a.** PKI Certificate: MLOA One-Year with Hardware/Token
   - **b.** PKI Certificate: MLOA Three-Year with Hardware/Token



   - **c.** Replacement Certificates With Proofing (New Token NOT Required) – 1 Year
   - **d.** Replacement Certificates With Proofing (New Token NOT Required) – 3 Year



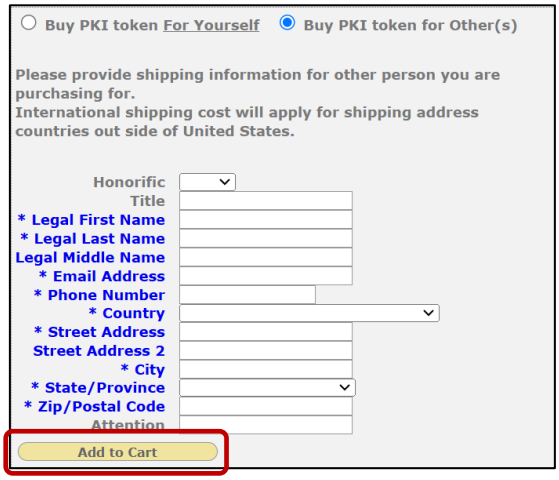
   - **e.** USB Hardware Token Replacement
   - **f.** MLOA PKI In-Person Re-Proofing



NOTE: Please read each product description carefully before completing a purchase.

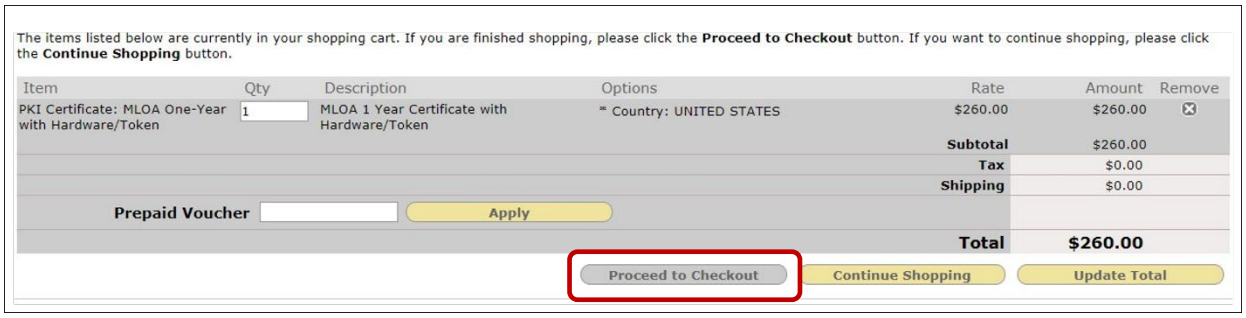
2. Select one of the **Buy** options.

a. **Buy For Yourself**
b. **Buy for Other(s)**: Selecting this option requires you fill in the user's information. Fill out the user's information and click **Add to Cart**.



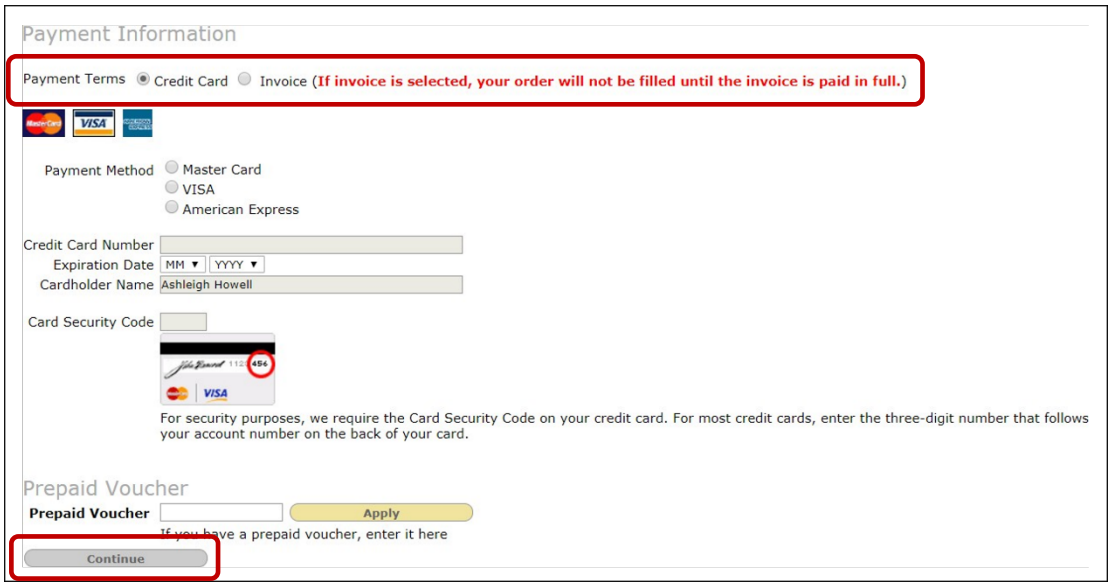
3. Select from the **Country** dropdown and click the **Add to Cart** button.

4. Review your **Shopping Cart** for accuracy and click the **Proceed to Checkout** button.



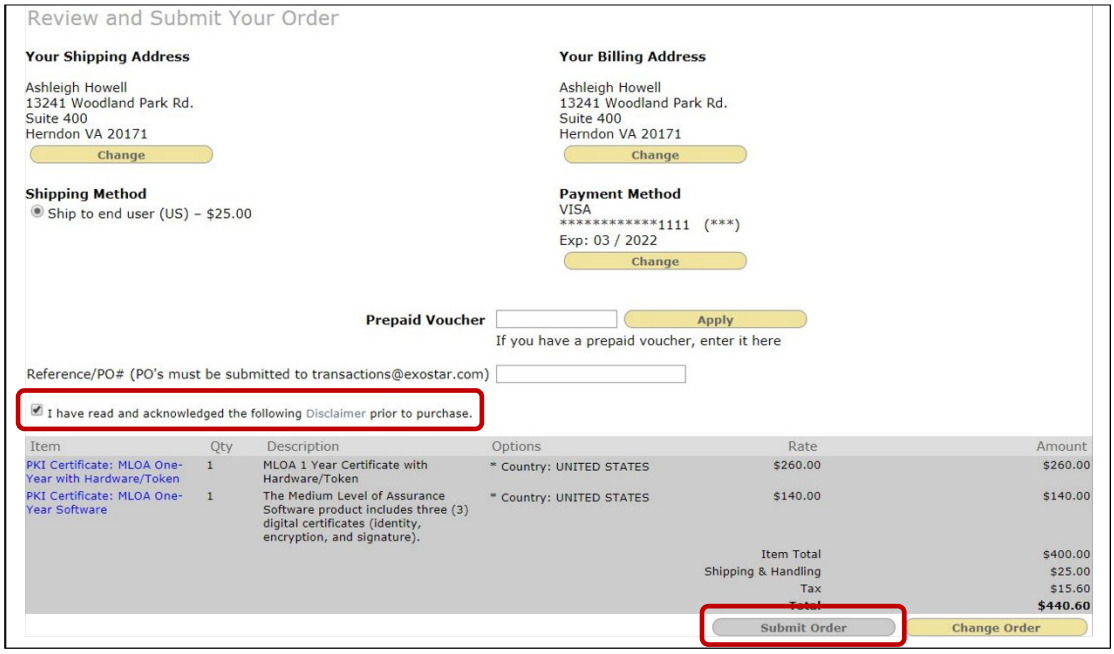
5. You are redirected to the **Shipping Method** page. **Ship to end** user is the only option available and is already selected. Click **Continue**.

6. On the **Payment Information** page, select to pay via credit card or invoice. Fill out all required information. Click **Continue**.



NOTE: If you select the *Invoice* option, you are required to pay in full before you receive any product.

7. On the **Review and Submit Your Order** page, click the **Disclaimer** link and review the information. Once you complete your review, select the checkbox next to **I have read and acknowledged the following Disclaimer prior to purchase**.
8. Click **Submit Order**.



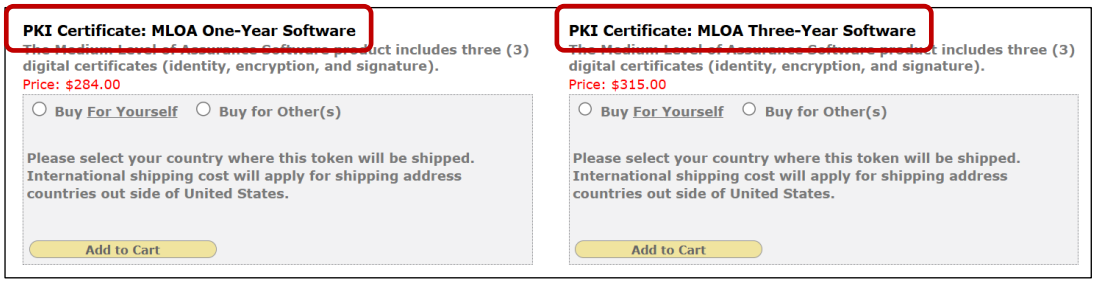
NOTE: A confirmation page displays, providing your **Sales Order Number** (SO#####).

Medium Level of Assurance (MLOA) – Software

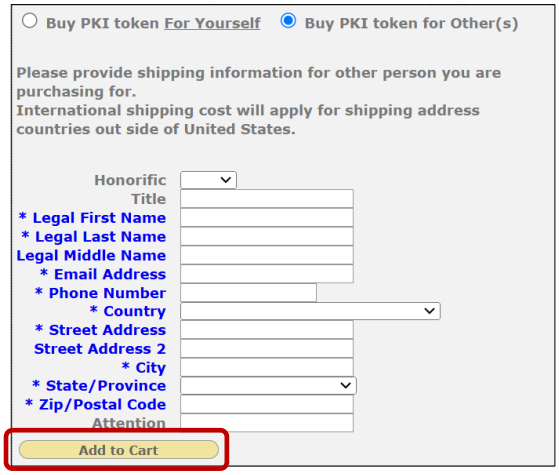
The MLOA Software product includes three digital certificates: **identity**, **encryption**, and **signature**. These certificates are compliant to the Federal PKI standards and cross-certified with the Federal Bridge Certificate Authority. You can use these digital certificates to access Exostar's Managed Access Gateway (MAG), and the customer applications behind MAG. Additionally, major Aerospace and Defense companies accept these credentials for access to some internal applications or to support digital signing and encryption of email.

Please follow the steps below to complete an MLOA Software-related purchase:

1. Select the **purchase now** link located next to **Medium Level of Assurance (MLOA) – Software**. Choose one of the following product options:
   a. PKI Certificate: MLOA One-Year Software
   b. PKI Certificate: MLOA Three-Year Software

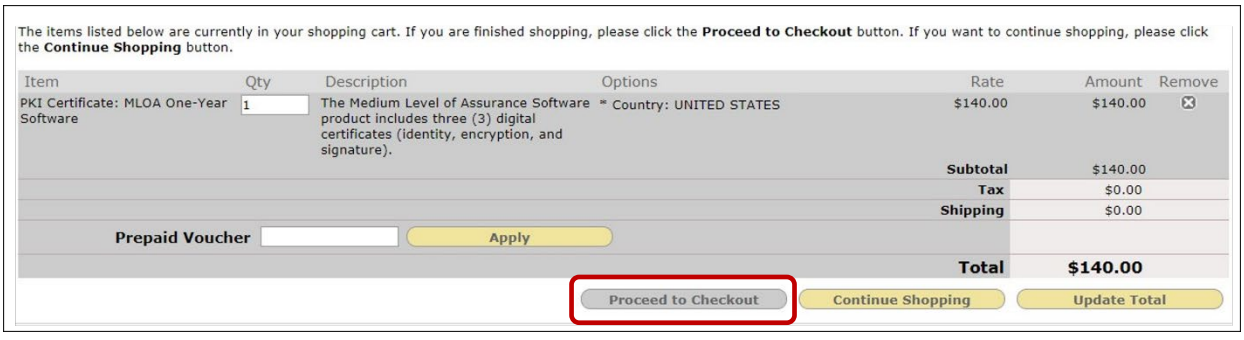


2. Select one of the **Buy** options.
   a. **Buy For Yourself**
   b. **Buy for Other(s)**: Selecting this option requires you fill in the user's information.

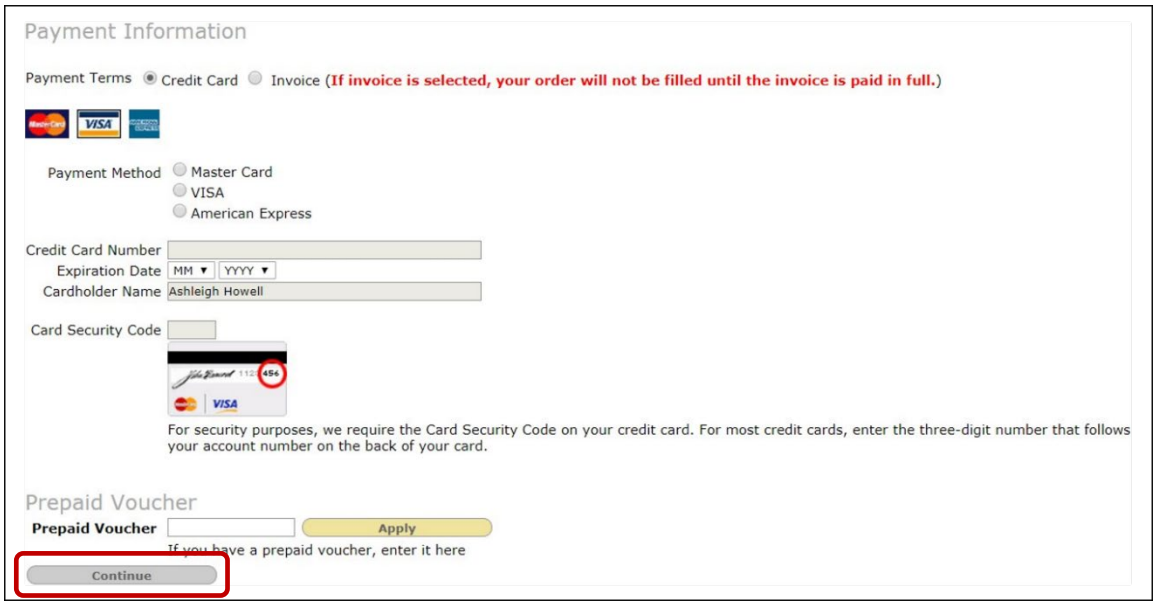


3. Select from the **Country** dropdown and click the **Add to Cart** button.

4. Review your **Shopping Cart** for accuracy and click the **Proceed to Checkout** button.

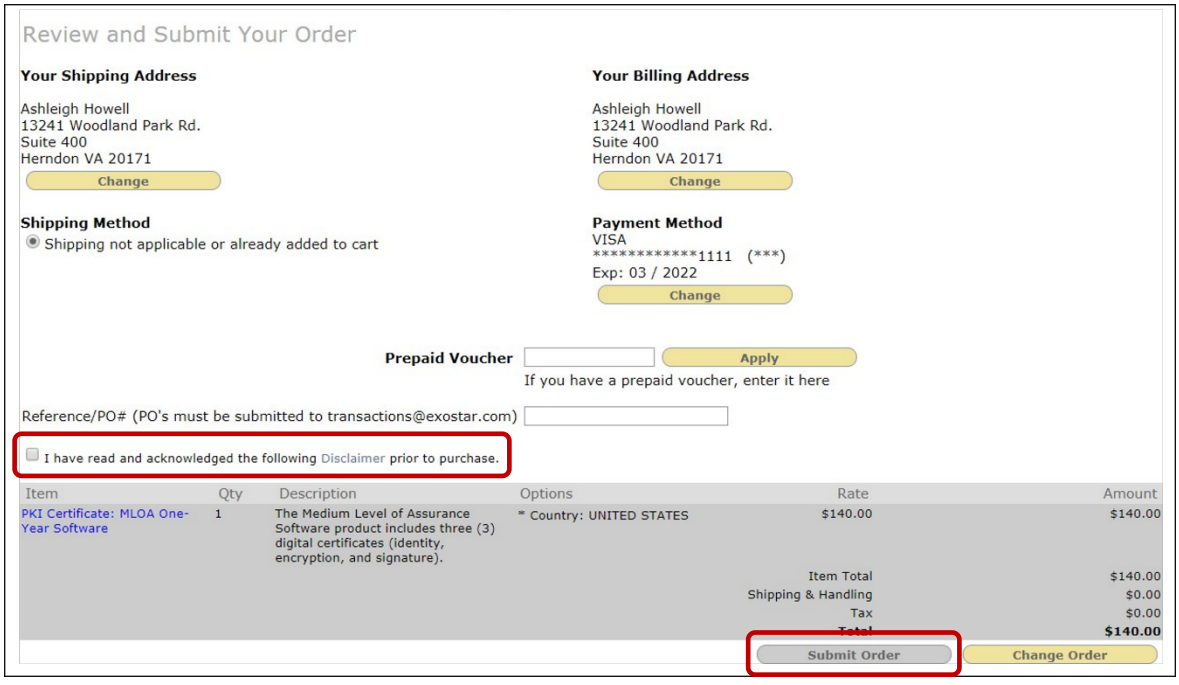


5. On the **Payment Information** page, select to pay via credit card or invoice. Fill out all required information. Click **Continue**.



NOTE: The invoice option requires you to complete payment in full before receiving any product.

6. On the **Review and Submit Your Order** page, click the **Disclaimer** link and review the information. Once you complete your review, select the checkbox next to **I have read and acknowledged the following Disclaimer prior to purchase**.
7. Click **Submit Order**.



NOTE: A confirmation page displays, providing your **Sales Order Number** (SO#####).

Basic Level of Assurance (BLOA) – Secure Email and Identity Certificate

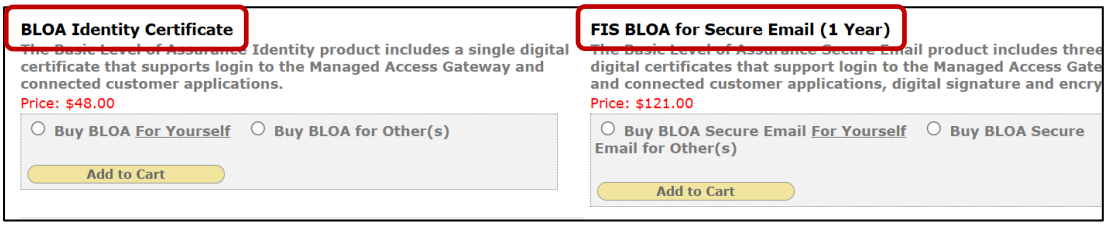
The BLOA Secure Email product includes three digital certificates: **authentication**, **digital signature**, and **encryption**. These certificates support login to Managed Access Gateway (MAG) and connected customer applications, digital signature and encryption.

The BLOA Identity Certificate includes a single digital certificate that supports login to MAG and connected customer applications.

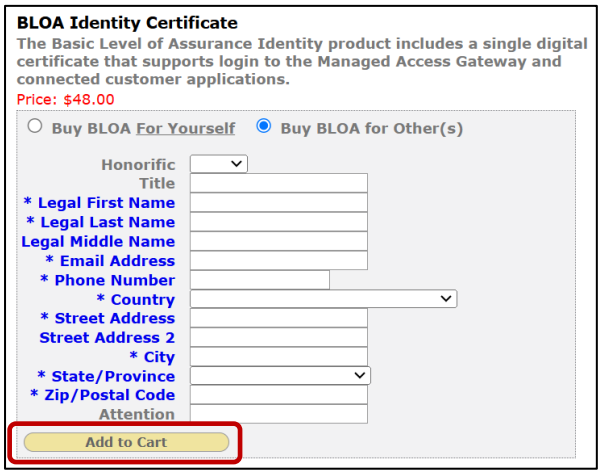
Please follow the steps below to complete a BLOA Secure Email or BLOA Identity Certificate

purchase:

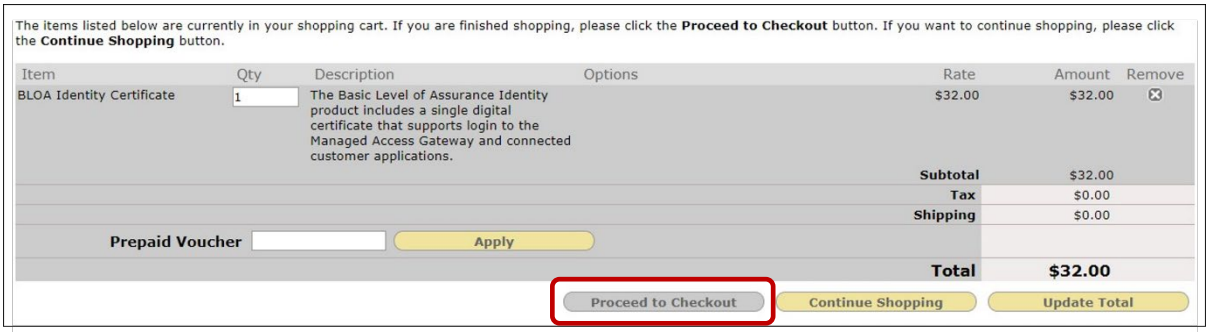
1. Go to http://www4.exostar.com/ and select the **purchase now** link located next to **Basic Level of Assurance (BLOA) – Secure Email** or **Basic Level of Assurance (BLOA) – Identity Certificate**. Both links redirect you to the same page. Choose one of the following product options:



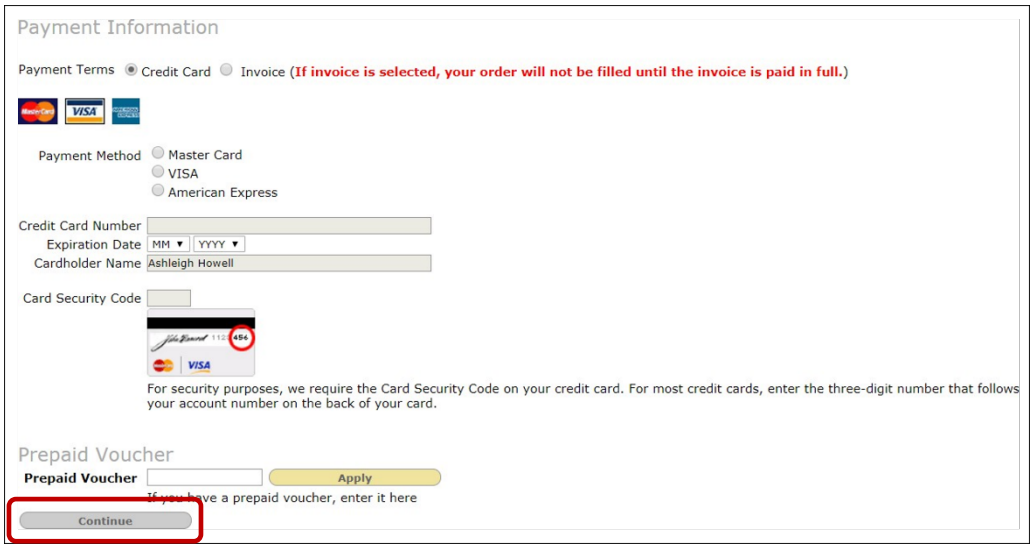
2. Select one of the **Buy** options. Click the **Add to Cart** button.
   a. **Buy For Yourself**
   b. **Buy for Other(s)**: Selecting this option requires you fill in the user's information.



3. Review your **Shopping Cart** for accuracy and click the **Proceed to Checkout** button.

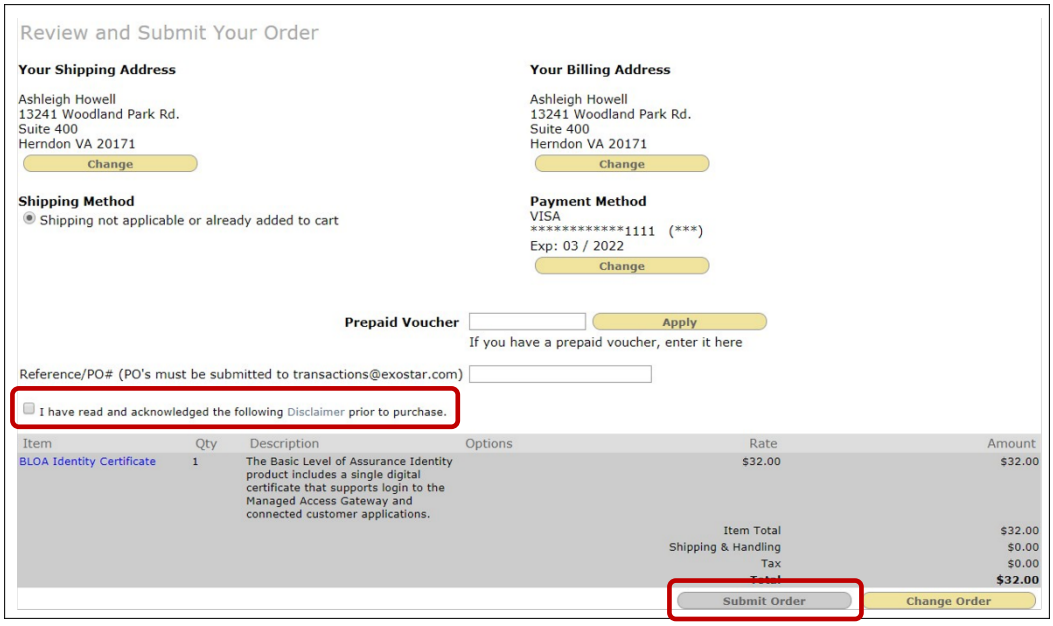


4. On the **Payment Information** page, select to pay via credit card or invoice. Fill out all required information. Click **Continue**.



NOTE: The invoice option requires you complete payment in full before receiving any product.

5. On the **Review and Submit Your Order** page, click the **Disclaimer** link and review the information. Once you complete your review, select the checkbox next to **I have read and acknowledged the following Disclaimer prior to purchase.**
6. Click **Submit Order**.



NOTE: A confirmation page displays, providing your **Sales Order Number** (SO#####).

FIS Registration

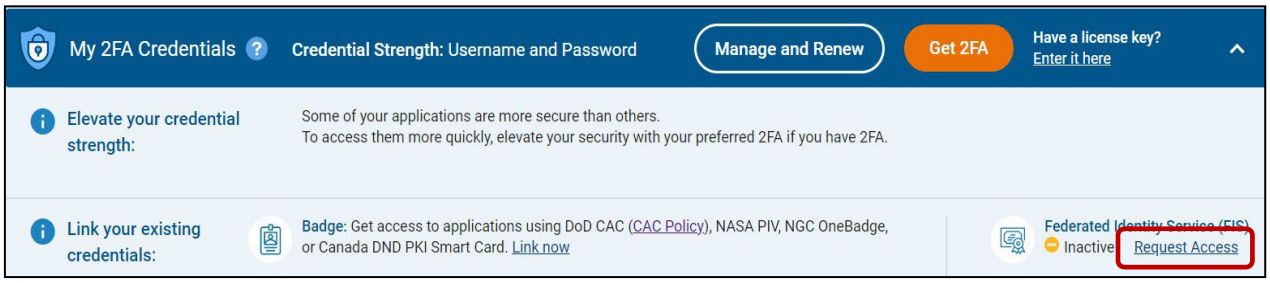
To begin the FIS process after purchase completion, someone must submit a request to Exostar one of three ways: *self-registration*, *administrator registration on your behalf*, or *Exostar can request access on your behalf*. You must have an existing MAG account, and your organization must be subscribed to FIS before you can request FIS access.

Self-Registration

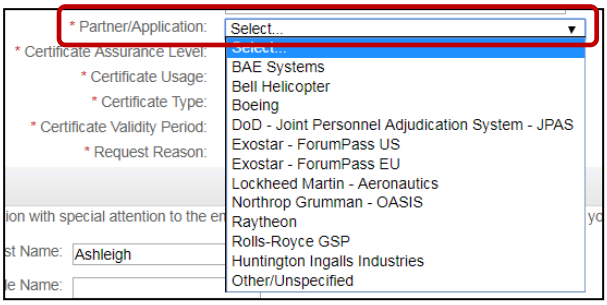
Please follow the steps below to complete the self-registration process:

1. Once you successfully login to MAG, on the MAG Dashboard, locate **Federated Identity Service (FIS)** in the **My 2FA Credentials** section. Select the **Request Access**

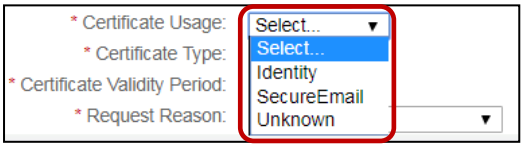
link.



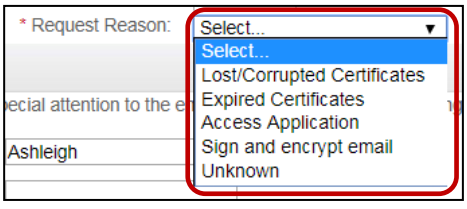
2. Fill out all necessary information under the **FIS Certificate Information** section:
   a. **Partner/Application**



   b. **Certificate Assurance Level**
   c. **Certificate Usage**
      i. If you choose **Basic** assurance level:

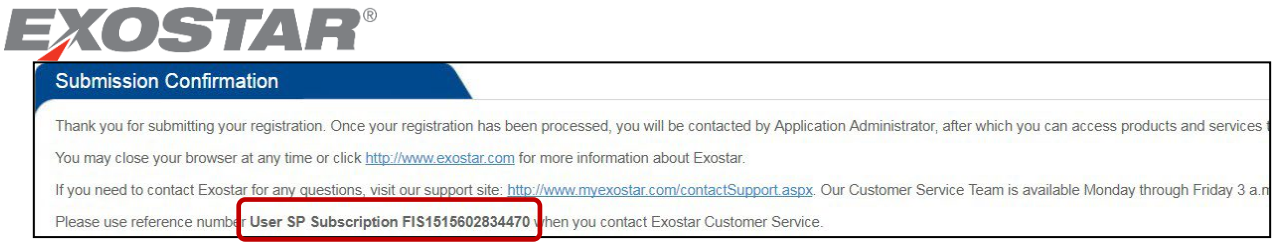


      ii. If you choose **Medium** assurance level:
   d. **Certificate Type**
      i. If you choose **Basic** assurance level, **Software** is the only option.
      ii. If you choose **Medium** assurance level:
   e. **Certificate Validity Period**
      i. If you choose **Basic** assurance level, **1 Year** is the only option.
      ii. If you choose **Medium** assurance level:
   f. **Request Reason**



3. Fill out all necessary information under the **User Information** section. Click **Next**.

NOTE: At this point, you receive a submission confirmation screen with a reference number.



Administrator Registration

The process for admin registration only varies by the admin filling out the customer's information and approving on their end, which removes the customer's responsibilities for requesting access themselves.

Exostar Registration

Exostar Administrators can issue individual invitations on a customer's behalf. Once Exostar issues an FIS invitation, the user's FIS Administrator must approve the request. If the invite was issued for Medium Level Hardware or Software, Exostar receives the user's FIS request to action accordingly, otherwise, the use can proceed with downloading their Basic Level of Assurance Certificates.

In-Person Proofing

MLOA Hardware and Software requires you to complete an In-Person Proofing verifying your identity.

If you are **located in the United States** and purchased a Medium Level of Assurance (MLOA) Hardware or Software certificate, our vendor NotaryGo, contacts you to setup a proofing appointment with one of their Trusted Agents.

For users **located outside the United States**, a Trusted Agent from Verify Europe contacts you to setup a proofing appointment. Once you successfully complete the proofing appointment, the Trusted Agent provides your 16-digit passcode. This passcode is required for successful certificate download.

You are required to bring originals of the documents listed below for the proofing session. No photocopies are accepted. However, the Employment Verification Letter does not require an original, and Exostar accepts photocopies during the In-Person Proofing session.

Employment Verification Letter: The employment verification letter should be printed on your company's letterhead and duly signed by an authorized executive within your company. You can find a sample of the Employment Verification Letter here.

Identity Verification Documents

Here is a list of acceptable documents for the proofing session:

- **LIST A**: One item from this list fully satisfies the proofing requirement:
  - U.S. Passport or Passport card
  - REAL ID Act compliant Picture Identification, identified by the presence of the DHS REAL ID star
  - Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
  - Employment Authorization Document that contains a photograph (Form I-766)

- Foreign Passport with I-551 stamp
- Foreign Passport with Form I-94 or I-94A
- Certificate of U.S. Citizenship
- Certificate of Naturalization

- **LIST B**: One item from this list PLUS one item from List C, satisfies the proofing requirement.
  - Driver's license or ID Card issued by U.S. government authority, containing personal information and photograph
  - Student ID card with photo
  - U.S. Military ID card or draft record
  - U.S. Military dependent's ID card
  - Voter registration card
  - U.S. Coast Guard Merchant Mariner Card
  - Driver's license issued by Canadian government authority
  - Native American tribal document

- **LIST C**: One item from this list PLUS one item from list B, satisfies the proofing requirement.
  - U.S. Social Security card issued by the Social Security Administration
  - Original or certified copy of birth certificate issued by U.S. government authority
  - Certification of Birth Abroad issued by U.S. Dept. of State (Form FS-545)
  - Native American tribal document
  - U.S. Citizen ID card (Form I-197)
  - ID card for Use of Resident Citizen in the United States (Form I-179)
  - Employment authorization document issued by DHS

Certificate Download Requirements

System Requirements

- Windows 8.1, 10, and 11 supported
- Download Exostar's SafeNet Client software (you will **need Administrator** access)
- Permissions to enable Exostar's KMA™ software and plug-ins (you will not need Administrator access)

System Permissions

This section describes the system permissions that must be granted (typically by a network or security administrator) to the logged-on user's account. Please reach out to your network or security administrator to review these permissions.

Certificate Store Permissions

A Microsoft-generated dialog box may display during FIS certificate installation if the logged-on user does not have permissions to write a trusted root certificate to the system's trusted root certificate store. The user must click **Yes** on this dialog for FIS certificates to install correctly. This section provides detailed information concerning this issue. As part the certificate acquisition process for an FIS user, an attempt is made by the Exostar KMA™ to download and install one or more digital certificates in the certificate store of the user's system. Each

certificate downloaded can be one of two general types:

- Certificates issued to the FIS user (FIS end user certificates) that are installed in the user's personal certificate store.
- Certificates that may be used to trace the user certificate to a trusted root authority (trusted root authority certificates) installed in the systems Trusted Root Certification Authorities certificate store (or Trusted Root Store for short).

Scenarios:

- If the logged in user (i.e., the FIS user attempting to obtain an FIS certificate does have permissions to store the trusted root authority certificates in the Trusted Root Store), the certificate installation process completes successfully.
- If the logged in user (i.e., the FIS user attempting to obtain an FIS certificate does not have the permissions to store the trusted root authority certificates in the Trusted Root Store), the FIS certificate download and install process can still proceed successfully, however due to a known Microsoft issue, the process may require an additional interactive step by the user.
- If the logged in user (i.e., the FIS user does not have the permissions to store the trusted root authority certificates in the Trusted Root Store), an informational dialog box may be generated by the Microsoft operating system during the certificate installation process. The Microsoft dialog box is intended to alert the user an attempt to install a certificate in the Trusted Root Store is being made and allows the user to proceed with the operation or cancel it.

Due to a known Microsoft issue (documented in the Microsoft Knowledge Base article #940275) the dialog displays and does not contain the intended informational message. Instead of a blank, not so informational message, the message should display as follows:
You are about to install a certificate from a certification authority (CA) claiming to represent:
"CANameCertificate_Information Do you want to install this certificate?"
The missing message text makes the dialog very confusing to the end user. For FIS certificate installation to complete successfully, the FIS user must click the **Yes** button on the Microsoft dialog box.

IMPORTANT: This dialog box only displays under the following conditions:

1. The logged-on user does not have permissions to store a trusted root certificate in the system's trusted root certificate store.
2. The trusted root certificate does not already exist in the trusted root store. If the certificate already exists, then no attempt to install is made and therefore the Microsoft dialog will not display.

Certificate Download

Once your certificates are approved, you can begin the download process. This section explains each certificate download.

NOTES:

- BLOA and MLOA Software certificate download does not require KMA™.
- If the BLOA and MLOA Software certificates are downloaded in MS Edge, they will not

be available in the Certificate Store and must be imported from downloads.

- Install Exostar's SafeNet Client is only needed for downloading MLOA Hardware certificates.
- Install Exostar's KMA™ software is only needed for downloading MLOA Hardware certificates.

Basic Level of Assurance Identity Certificate Download

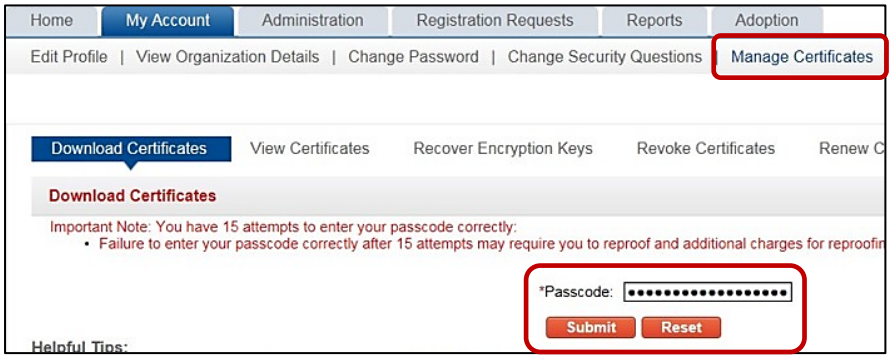
Pre-requisites for downloading identity certificates:

- Received 16-digit passcode from Exostar via email
- Reviewed system and certificate download requirements
- Does not require KMA™ software download.

To download certificates:

1. Go to the **My Account** tab. Click the **Manage Certificates** sub-tab.
2. Enter the passcode you received via email from Exostar. Click **Submit**.

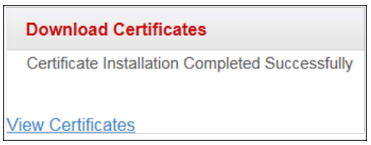
NOTE: The passcode is a 16-digit number separated by hyphens; for example: 1234-5678-1234-5678. The passcode is NOT the same as your MAG account login password.



3. If your passcode is correct, the certificate displays with a status. The system automatically selects the certificate to download.

NOTE: You are only able to see the **Download Certificates** sub-tab under **Manage Certificates** when you have an approved FIS request pending certificate download. If no certificates are available for download, you cannot view this sub-tab.

After the certificate successfully downloads, a confirmation message will display.



Basic Level of Assurance Secure Email Download

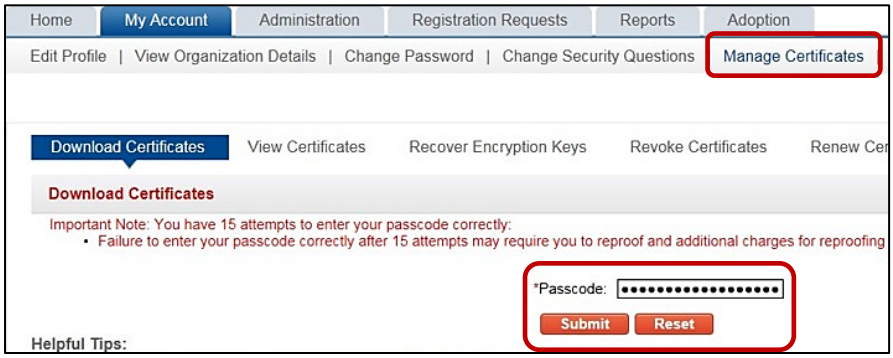
Pre-requisites for downloading identity certificates:

- Received 16-digit passcode from Exostar via email
- Reviewed system and certificate download requirements
- Does not require KMA™ software download.

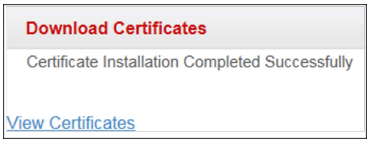
To download certificates you are approved for:

1. Go to the **My Account** tab. Click the **Manage Certificates** sub-tab.
2. Enter the passcode you received via email from Exostar. Click **Submit**.

NOTE: The passcode is a 16-digit number separated by hyphens; for example: 1234-5678-1234- 5678. The passcode is NOT the same as your MAG account login password.



3. If your passcode is correct, the list of certificates you can download displays. The system automatically selects all certificates for download.
4. Click the **OK** button to archive your encryption key and enable key recovery.
5. Complete the certificate download. The system presents the download status at each step.
6. Once the download is complete, a confirmation message displays.



Medium Level of Assurance Software Certificates Download

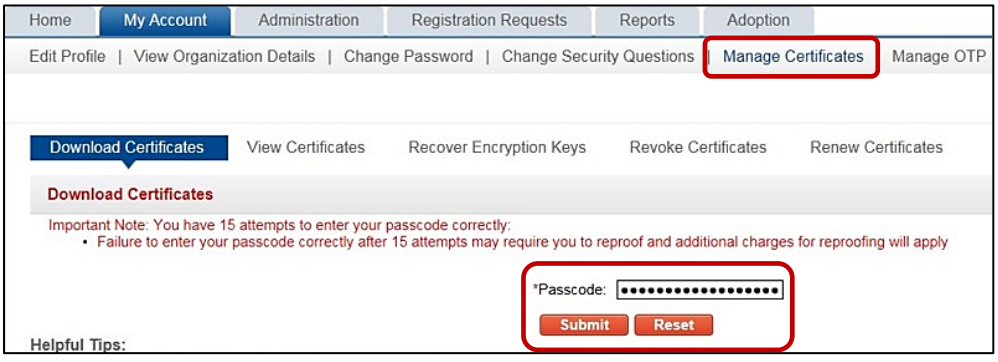
Pre-requisites for downloading certificates:

- Completed In-Person Proofing.
- Receive 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.
- Does not require KMA™ software download.

To download certificates:

1. Go to the **My Account** tab, and click the **Manage Certificates** sub-tab.
2. Enter the passcode provided to you by your Proofing Agent during your In-Person Proofing appointment, then click **Submit**. (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. The passcode is **NOT** the same as your MAG account login password.



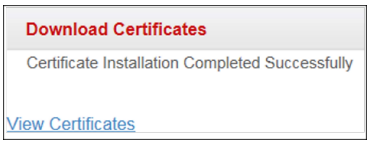
3. If your passcode is correct, a list of certificates you can download displays. The system

automatically selects all certificates for download. Click **OK** to archive your encryption key and enable key recovery.

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.

5. By default, the **Medium** option is already selected. Change this to **High** and click **Next**.
6. Provide a password for this certificate. Please note you need to provide this password each time you use your certificate.
7. The system displays the new security level. Click **OK**.
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**.
9. Once the download is complete, a confirmation message displays.



Medium Level of Assurance Hardware Token

This section provides instructions on how to install the required software in order for your computer to properly communicate with the MLOA Hardware token you purchased. This token is used to download/access Medium Level of Assurance (MLOA) hardware digital certificates.

Before you download your MLOA hardware certificates, complete the following tasks first:

1. Purchase the appropriate token. Exostar ships your token via FedEx once you schedule your In-Person Proofing appointment. If you have not received your token, please contact Customer Support.
2. Request access to FIS (see FIS Access section above).
3. 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).*
4. Install the token PKI Client middleware on your machine. Contact your token vendor for appropriate information, or your IT Support for organization specific information.
   - Install Exostar's SafeNet Client software. (***NOTE:*** *You will need* ***Administrator access*** *to download software to your computer).*
   - Install the Exostar's Key Management Agent (KMA™) to download your hardware certificate. (***NOTE:*** *You do not need Administrator access to download KMA software to your computer).*
5. Change Default Password. Please make sure you have been provided the initial token password prior to installing your token on your computer. (***NOTE:*** *If you have not received your initial password, contact your vendor to obtain this. You are required to enter a password for this token during the certificate download process).*

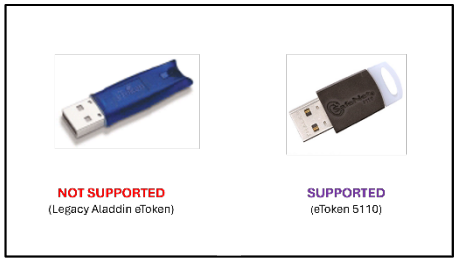
Supported Tokens

Exostar's Medium Level of Assurance Hardware (MLOA) digital certificates currently support the following PKI hardware tokens:

- Thales eToken 5110 Series

- Thales eToken 5110+FIPS (FedRAMP and FIPS 140-2 Certified) – *[Note that the eToken 5110 and the eToken 5110+FIPS look physically identical]*

NOTE: Legacy PKI hardware tokens such as the Aladdin eToken PRO are *no longer supported* and must be updated* (see image below).



The Properties of an eToken 5110+ should have the following parameters (obtained from the Exostar SafeNet Client tool (see token information below).

Change Token Default Password

To change your token's default password:

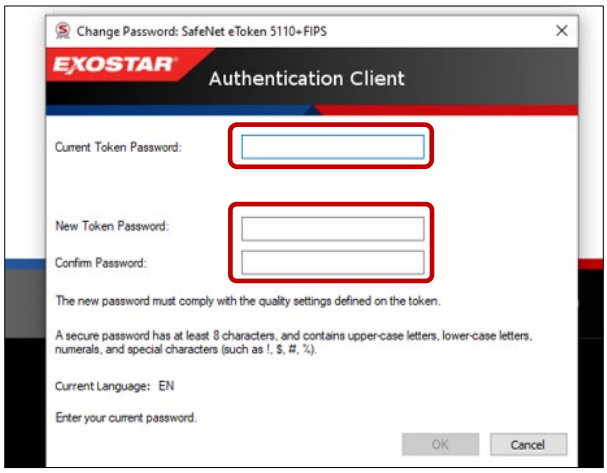
1. Insert your new Token in your computer's USB drive.
2. Launch Exostar SafeNet client tool.
3. A screen will display to change the token password. (If you are not automatically prompted, choose the "Change Token Password" option).
4. Enter the default token password, **1234567890**. Enter a **new password** and then enter it again to confirm your new password. Then click **OK**. (Please make sure you remember your password).

IMPORTANT! If you forget this Token Password, you will be required to: 1. Reinitialize your Token, 2. Reapply for certificates, and 3. Complete the identity proofing process again at your expense.

Additional 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 MAG login password.
- If you lose the passcode, you are required to complete a reproofing purchase and complete another in-person proofing appointment.

- The passcode is only valid for 30 days from the time of Exostar proofer approval.
- The proofing approval process may take up to 1 business week.



Install Exostar's SafeNet Client

Exostar's SafeNet Client is required to successfully download your hardware certificates. You will need Administrator rights (access) to install the software on your computer.

The latest version of the Exostar SafeNet Client application is packaged in the following Microsoft Installer (MSI) which will guide you through the setup process. Download and install the latest version of SafeNet Client here. After you have successfully downloaded SafeNet, please install Exostar's KMA™ next.

System Compatibility

Operating System	Chrome (132.0.6834.15)	MS Edge (131.0.2903.63)	Firefox (132.0.2)	Safari (17.4.1)
Windows 11	Yes	Yes	Yes	N/A
Windows 10	Yes	Yes	Yes	N/A
MAC OSX	No	No	No	No

Install Exostar's KMA™

Exostar's Key Management Agent (KMA™) software is required to successfully download your MLOA Hardware Certificates. You do not need Administrator rights (access) to download KMA™. However, some organizations may require Administrator permissions before you install KMA™ software on your computer.

To install KMA™ software, you can download it here or distribute via Group Policy.

NOTE: You can download KMA™ using Chrome, MS Edge, or Firefox.

System Compatibility

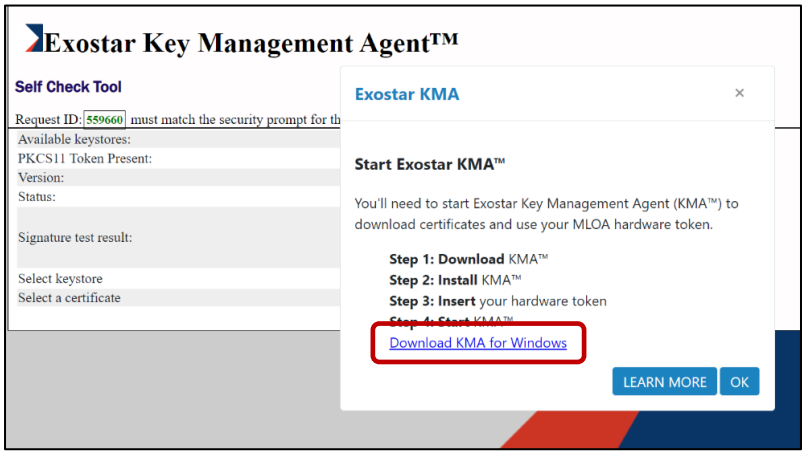
Operating System	Chrome (132.0.6834.15)	MS Edge (131.0.2903.63)	Firefox (132.0.2)
Windows 11	Yes	Yes	Yes
Windows 10	Yes	Yes	Yes
Windows 8	No	No	No

To download and install KMA™ software, follow the steps below:

1. Login to your MAG Account - https://portal.exostar.com.
2. Select the **My Account** tab, then click **Manage Certificates** sub-tab.

3. You will be prompted to download and install KMA™. Click **Download KMA™ for Windows**.

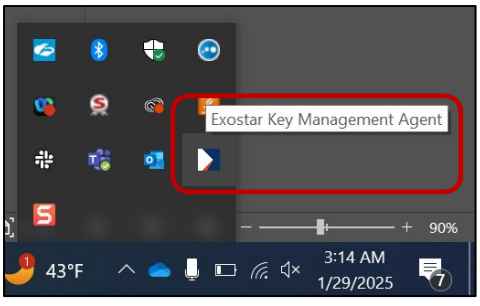
NOTE: You can download KMA™ using Chrome, MS Edge, or Firefox*.
*(*If you use Firefox to download KMA™ for software certificates, the certificates will be imported into OS key store. Users will have to manually import the certificates into Firefox for 2FA into MAG).*



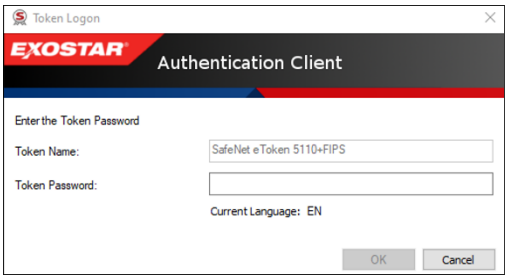
4. Follow the prompts to download and install KMA™ on your computer.
5. Next follow the steps to authenticate your Hardware Token with KMA™.

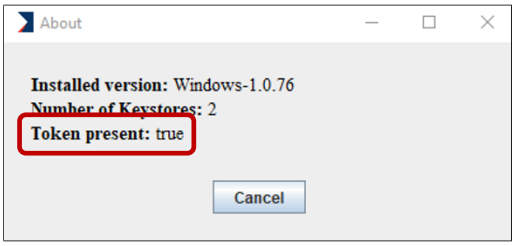
Authenticate your Token to KMA™

1. Make sure Exostar KMA™ is not running (you can look at the System Tray on the far right side of your Desktop Taskbar).



2. Insert your token in your computer's USB drive.
3. Then launch KMA™. You will be prompted to enter your token password, then click OK.
4. To verify your token is authenticated, click the **About** tab in KMA™. Your token will display as "**true**" if its authenticated.



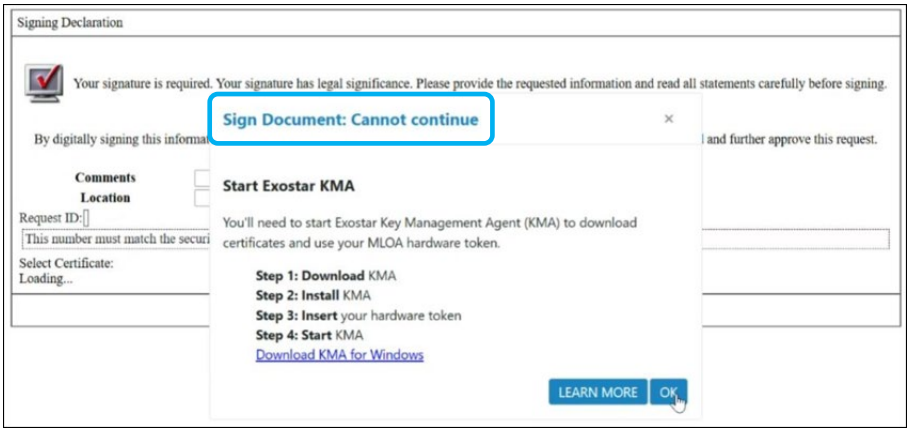


5. Next install your MAG PKI Certificates on your token.

Download Certificates to Token

Before you can download your certificates please complete the following tasks outlined below.

1. First launch Exostar SafeNet client.
2. Plug your token into your computer's USB drive and make sure you are logged into your MAG user account.
3. Next launch Exostar KMA™.
4. Make sure your token is authenticated to KMA™. (If you are logged into MAG and your token is not authenticated to KMA™, this will result in a looping failure to sign certificates and you will receive an error).



Install Certificates on Token

After you have authenticated your token to KMA™, you can download your MAG PKI Certificates to your MLOA Hardware Token.

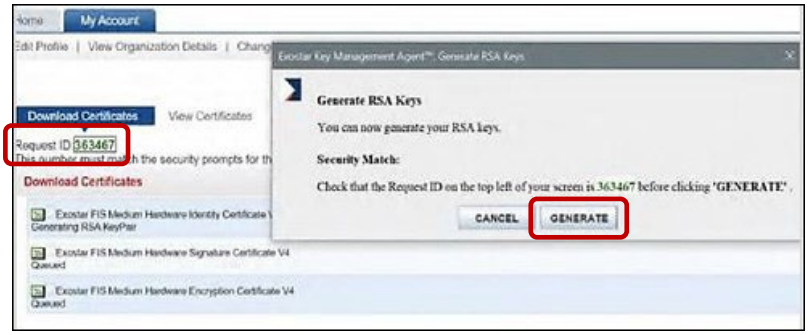
1. Login to your MAG user account. In the upper right corner under FIS, you will see a **Download** link. You can click this link or go to **My Accounts**, then **Manage Certificates** sub-tab to download your certificates. (**NOTE:** The Download Certificates link is only visible under the Manage Certificates tab when you have an approved FIS request pending certificate download. If no certificates are available for download, this sub-tab does not display).
2. Enter the 16-digit passcode, the Proofing Agent provided you with during your in-person proofing appointment.

   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 MAG login password.*

- *If you lose the passcode, you are required to complete a reproofing purchase and complete another in-person proofing appointment.*
- *The passcode is only valid for 30 days from the time of Exostar proofer approval.*
- *The proofing approval process may take up to 1 business week.*

3. If your passcode is correct, a list will display of certificates to download. (The system will automatically select all the certificates to download). Once selected, you are prompted to enter the Hardware Token Password that you previously created. Enter the Token Password and click **OK.**
4. Verify the Request ID, ensuring both numbers match before generating the RSA keys. Then click **GENERATE**.



5. Next your certificates will be created and archived. This process may take a few minutes (once the process is complete, a **View Certificates** link will display).
6. Click **Exit KMA** to complete the process.

Manage Certificates

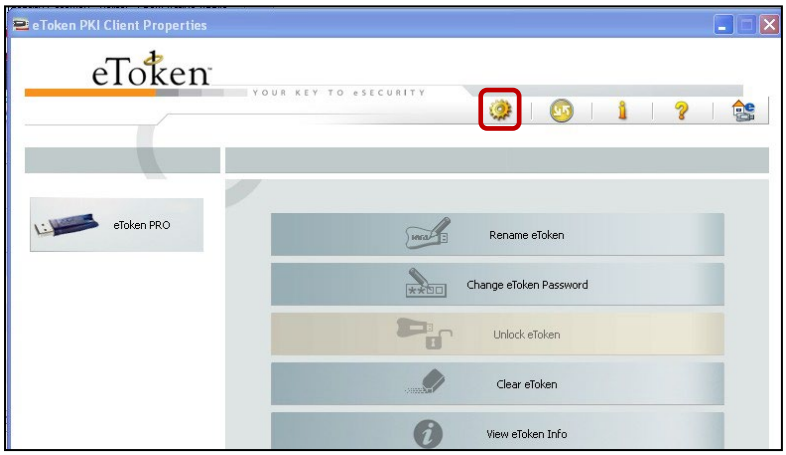
Once you successfully download your certificates, go to the **Manage Certificates** tab in your Exostar's Managed Access Gateway (MAG) account to manage your certificates.

View Certificates

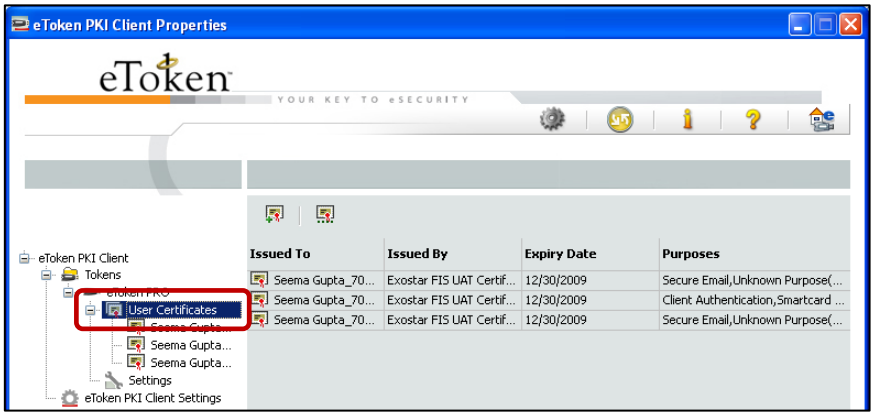
After you successfully download your FIS certificates, you can view the certificates, and their details, under the **View Certificates** sub-tab.

To view your certificates:

1. After installing the certificates, open the token client. The following screenshots depict the information specific to **Aladdin eToken Pro 72 K** token.
2. Click **Advanced** view.



3. Expand the **User Certificates** by clicking the plus sign (**+**). You should view the list of all installed certificates. Click each certificate to view details.



Revoke Certificates

If you suspect one of the following, you should revoke your certificates:

- Loss, compromise, or theft of your private key
- Fraud

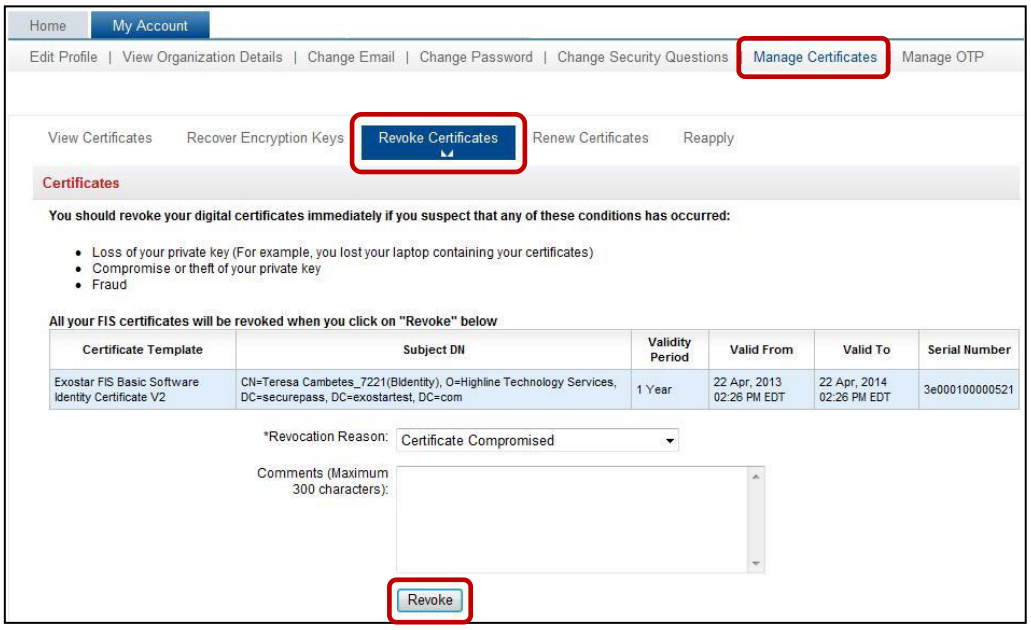
There are four ways to revoke your certificates:

1. **Yourself**: Login to your MAG Account using your User ID and password, then follow the steps below.
2. **Organization Administrator**: Your Organization Administrator can revoke your certificates at any time.
3. **FIS Administrator**: Your organization's designated FIS Administrator can revoke your certificates on your behalf.
4. **Exostar Customer Support**: If your certificates have been compromised, contact Exostar Customer Support and request certificate revocation.

To Revoke your Certificates:

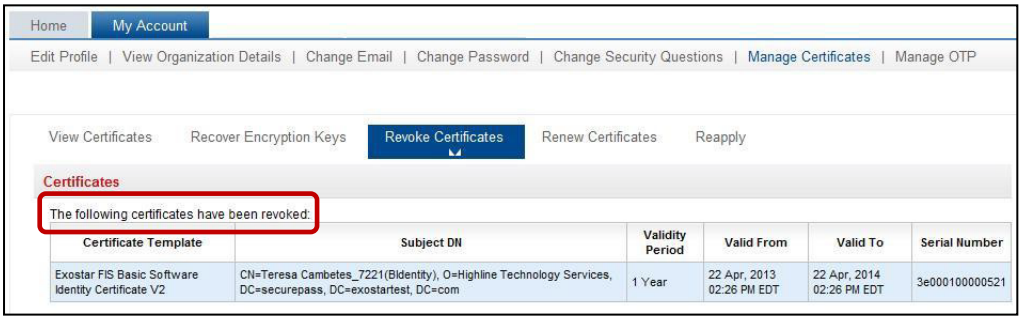
- Go to the **My Account** tab, click the **Manage Certificates** sub-tab, and then click the **Revoke Certificates** tab.

NOTE: You cannot selectively revoke certificates. This activity revokes all of your downloaded certificates.



1. Click the **Revoke** button to revoke **ALL** FIS certificates. You will receive a confirmation notification.

2. Select **OK** to revoke all certificates. The **Certificate Revocation Confirmation** displays.



Recover Encryption Keys

This section is only pertinent to users with:

- BLOA SecureEmail
- MLOA Software
- MLOA Hardware

A user receives three certificates for FIS BLOA SecureEmail, MLOA Software, and Hardware:

1. Identity
2. Authentication
3. Encryption

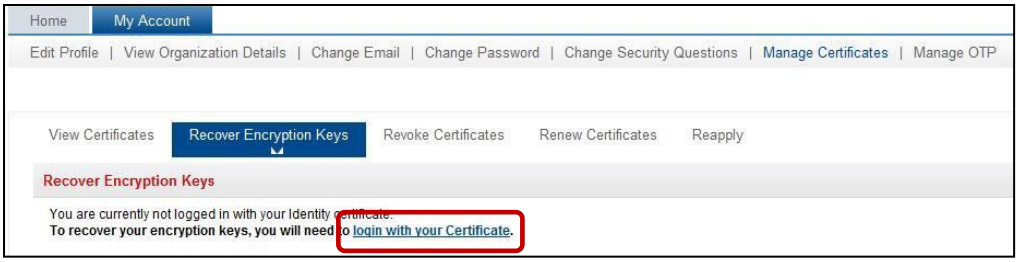
Once a user revokes or loses their MLOA certificates, they will need to re-apply for certificates and go through the In-Person Proofing process again. This may also require an additional purchase. To enable users to access data encrypted using the revoked/lost certificates, Exostar offers the self-key recovery functionality.

IMPORTANT:

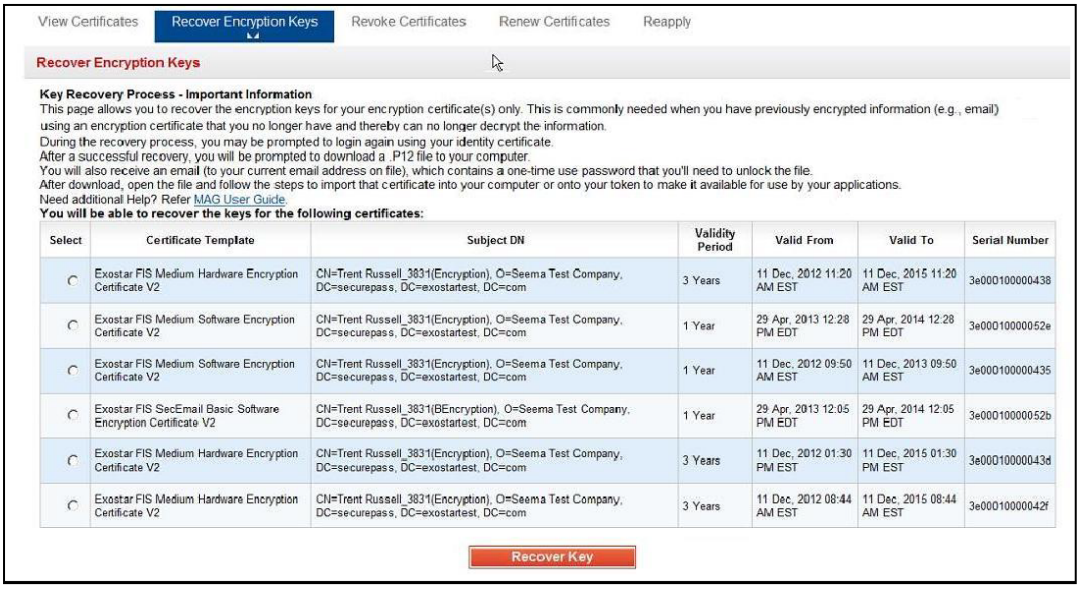
- If you are approved for and downloaded FIS **BLOA SecureEmail** certificates, you can recover encryption keys for all active, revoked, or expired certificates.
- If you are approved for and downloaded FIS **MLOA Software** certificates, you can recover both BLOA SecureEmail and MLOA Software encryption keys for all active, revoked, or expired certificates.
- If you are approved for and downloaded FIS **MLOA Hardware** certificates, you can recover encryption keys for all certificates – BLOA SecureEmail, MLOA Software, and MLOA Hardware. However, for hardware certificates, you can only recover expired or revoked encryption keys. Current keys cannot be recovered.
- If you are recovering hardware encryption keys, you need to login using your hardware token.
- You can use the keys only to access the data which was encrypted using the revoked or lost certificates.

To recover the keys:

1. Login to MAG account using your new MLOA certificates. If you have not reapplied for certificates, complete all activities related to requesting access, In-Person Proofing, and downloading your certificates, prior to attempting to recover encryption keys.
2. The following screen displays if you have not logged-in using your new certificates. Click the link "**login with your Certificate**" and select the certificate associated with your login credentials.

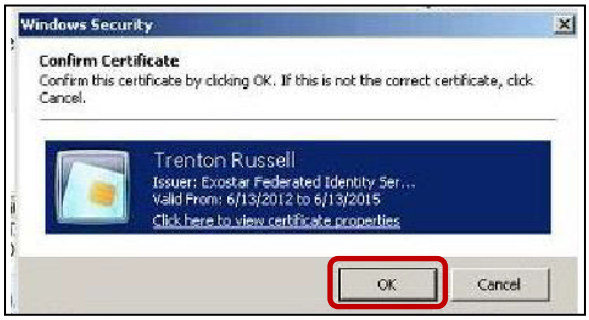


3. Select the **Recover Encryption Keys** sub-tab under the **Manage Certificates** tab.

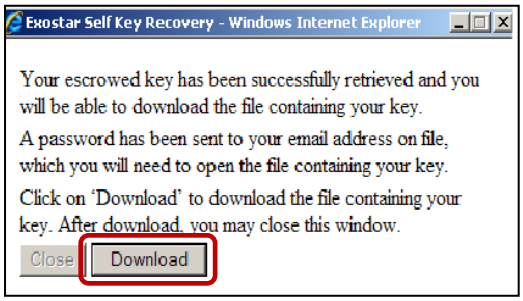


4. Select the certificate for which you need to recover the encryption key. If multiple certificates are available, repeat the process to recover each key. Click **OK** to proceed.

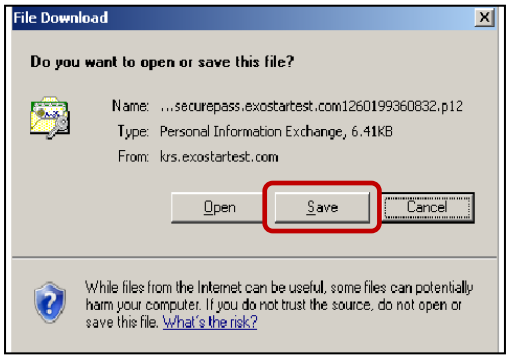
5. From the **Choose a digital certificate** pop-up screen, select the certificate you used to login.



6. You may be prompted to login again using your MLOA certificate. Complete the login with the MLOA certificate used to login in step 1 and click **OK**. The following screen displays. Click **Download**.

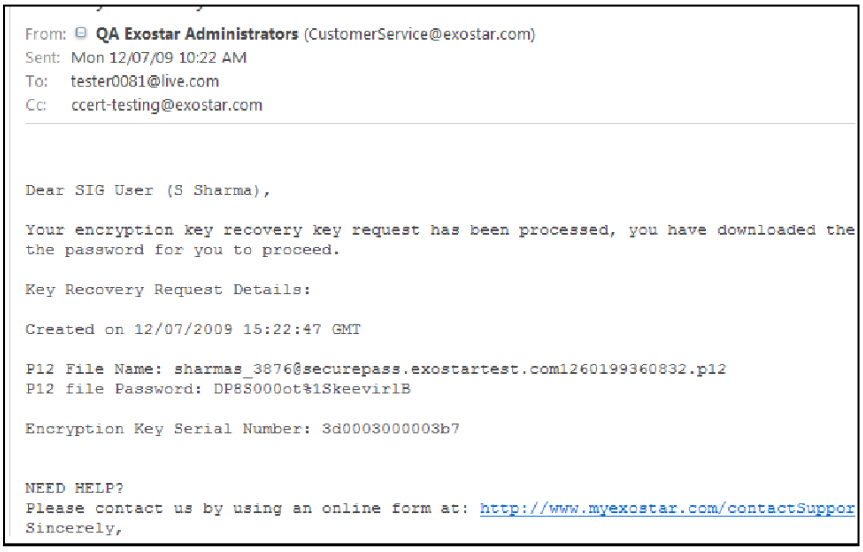


7. You are prompted to either **Open** or **Save** the file. Click **Save**.



8. Save the certificate file (.p12 format) at a location of your choice. Click **Close** on the **Exostar Self Key Recovery** screen.

9. You will receive an email with a one-time password, which is required to unlock the file you just downloaded. Follow the instructions under the **Importing Recovered Encryption Keys** section for the next steps.



Import Recovered Encryption Keys

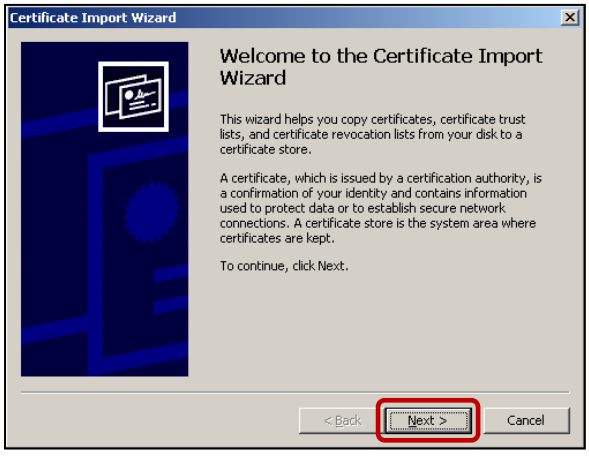
To import the encryption keys recovered in the **Recover Encryption Keys** section, you need the following:

- Access to the location where you saved the .p12 file.
- Email with the one-time password, to unlock the key for importing.

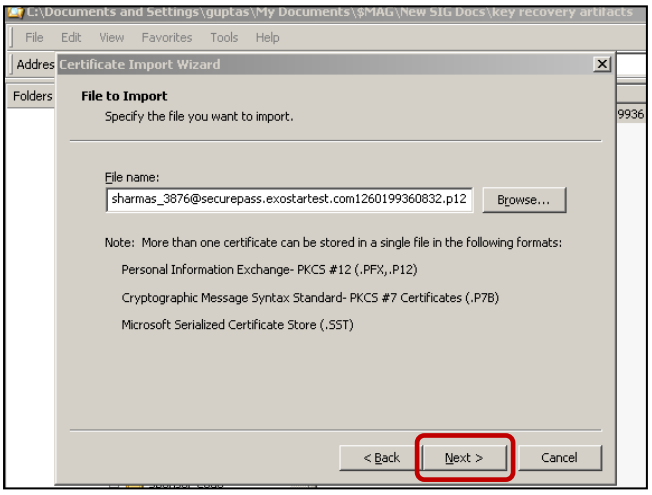
Follow the steps below to import your encryption key:

1. Double click the saved .p12 file.

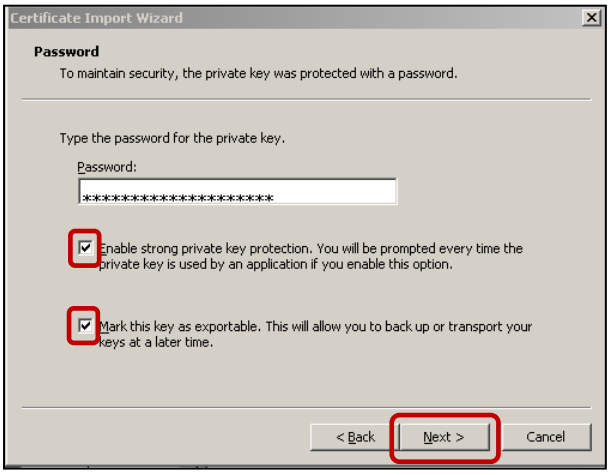
2. You are presented with the **Certificate Import Wizard**. Click **Next**.



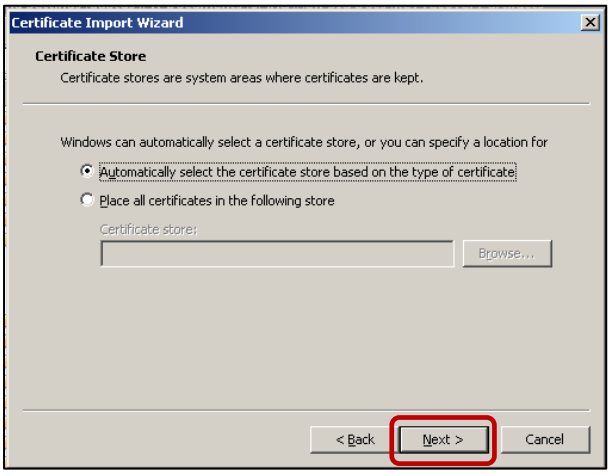
3. Confirm the file name and click **Next**.



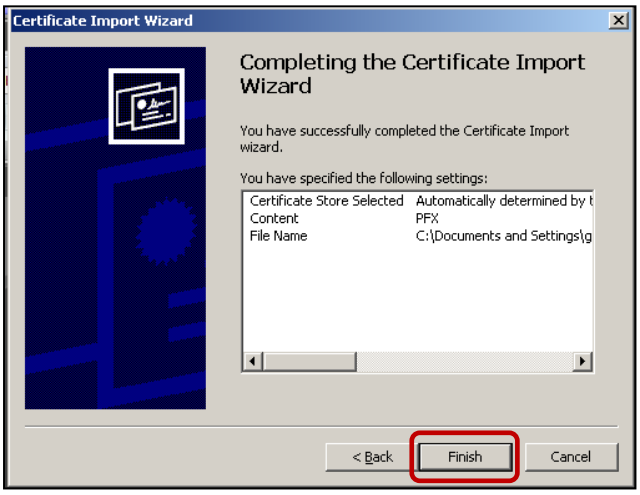
4. Copy or enter the one-time password from the email you received, and make sure no trailing spaces are entered. In addition, it is strongly suggested you enable **strong key protection**, and setup a password to access the encryption key. To enable further export of the key, you may also select the **Mark this key as exportable** option.



5. Click **Next**. You are prompted to select a location to store the certificate. Click **Next**.



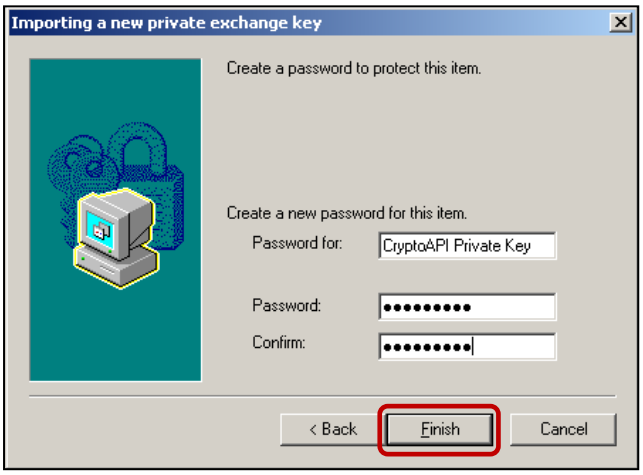
6. Click **Next** again to complete the import process, then click **Finish**.



7. If you selected to **Enable strong protection** in step four, you are presented with the below screen. Click **Set Security Level** to set a password for the encryption key.

8. Select **High** to ensure you are prompted for a password each time and click **Next**.

9. Enter a password. Click **Finish**.



10. Click **OK**, and the following screen displays:

NOTE: When you attempt to open an encrypted document or email, which was encrypted using this key, you are automatically prompted for the key password you setup. Enter the password to access your document or email.

Certificate Renewal

You may renew your certificates 90 days *prior* to expiration. If you have expiring certificates, you only need to renew not reapply for certificates. You only replay for certificate if you are attempting to upgrade the certificate assurance level.

For FIS MLOA Software and Hardware certificates, you must download your renewed certificates using your existing unexpired certificates.

To renew your certificates:

1. Use your unexpired certificates to log into MAG.
2. Click your **My Account** tab, the **Manage Certificates** sub-tab.
3. Next select **Renew Certificates** tab. Then click the **Renew** button.
4. Optionally, provide a sponsor code if one is available to you. Click **Next**.
5. A confirmation screen will display.

Next Steps:
Once you submit your certificate renewal request, the following actions will happen:

- You receive two confirmation emails your request for renewal has been submitted to the FIS Administrator (FISA) for approval.
- The FISA receives a notification to approve your request.
- If the FISA approves your request, you receive an approval email with a passcode to download your certificates.

Download Renewal Certificates

Prerequisites to download renewed certificates:

- Login to your MAG account with your User ID & password AND the certificates you renewed.
- The passcode you received in the **Certificate Renewal Approval** email.

To download your renewed certificates:

1. Log into MAG and select the **My Account** tab, then select **Manage Certificates** sub-tab.

NOTE: Skip to Step 3 if you are downloading renewal certificates other than FIS MLOA hardware.

2. Complete system check for FIS MLOA Hardware certificates.

NOTE: Your renewal confirmation email provides a link to the system check. Follow the instructions provided in the email to complete the system check and clearing of encryption and signature certificates from your FIS MLOA Hardware token.

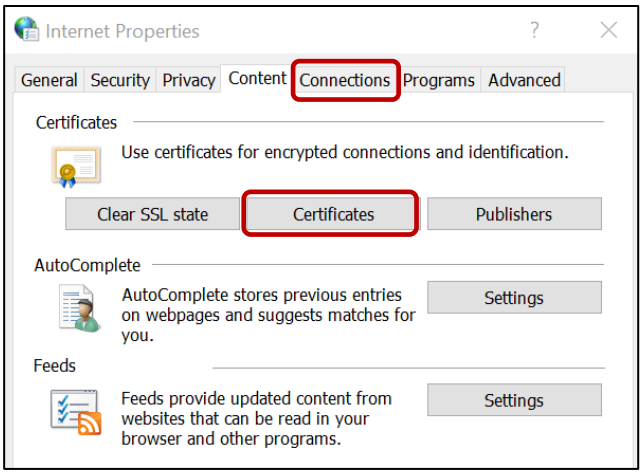
3. Click the **Download** button to proceed. The remainder of the process follows the basic download. Please see previous download sections for more information.

Disable/Remove Old Certificates

Exostar recommends removing expired certificates to ensure the user is not presented with multiple certificates at the time of accessing the ForumPass application.

To start the process:

1. Go to your Windows Start menu.
2. Search for **Internet Options** and open it.
3. Click the **Content** tab and select the **Certificates** sub-tab.



4. In the Certificates pop-up screen, select the certificate you wish to remove.
5. Check the Expiration date. Then click **Remove**.
6. A confirmation message displays. Click **Yes** to proceed or **No** to cancel.

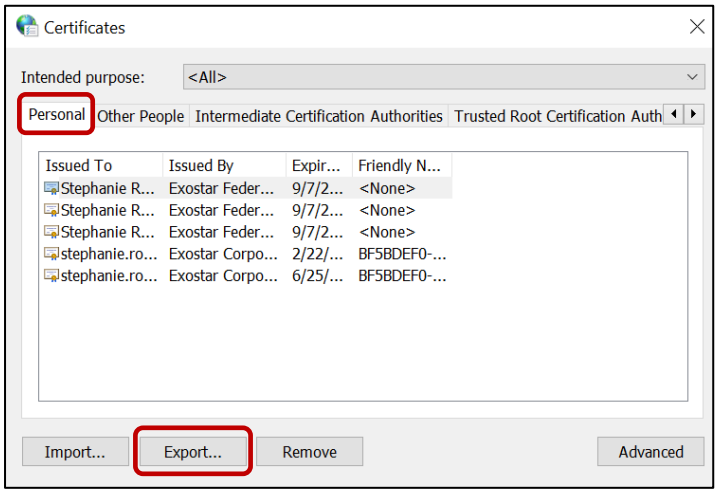
Export/Import Certificates

The instructions for exporting and importing your digital certificate are intended for **certificate backup purposes only**. Users should maintain control of their digital certificates at all times, and it is recommended users apply strong passwords to their certificates during export process. For additional information on your organization's policies regarding certificate usage and storage, please contact your organization's IT or Security department.

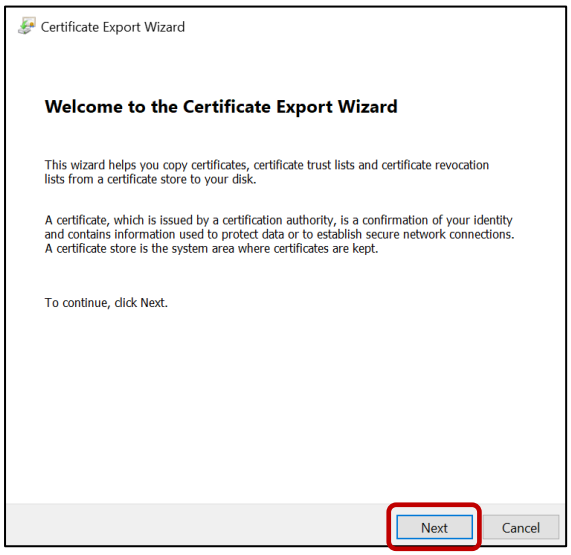
Export Certificates

Follow the steps below to export certificates:

1. Go to your Windows Start menu.
2. Search for **Internet Options** and open it.
3. Select the **Content** tab and click the **Certificates** sub-tab.
4. On the **Certificates** dialog box, select the **Personal** tab.
5. Highlight the **Identity** certificate and click **Export**.



6. The **Certificate Export Wizard** opens, click **Next**.



7. Choose "**Yes, export the private key**" option and click **Next**.
8. Select the "**Include all certificates in the certification patch if possible**" option and click **Next**.
9. Apply a password to the certificate. Click **Next**.

NOTE: You must remember this password. It will be used during the certificate import process.

10. Browse for a location to store your certificate. Click **Browse…** For security reasons, it is important you always maintain control of your digital certificate.
11. Enter your first and last name as the file name. The **Save as Type** should be *.pfx. Click **Save**.

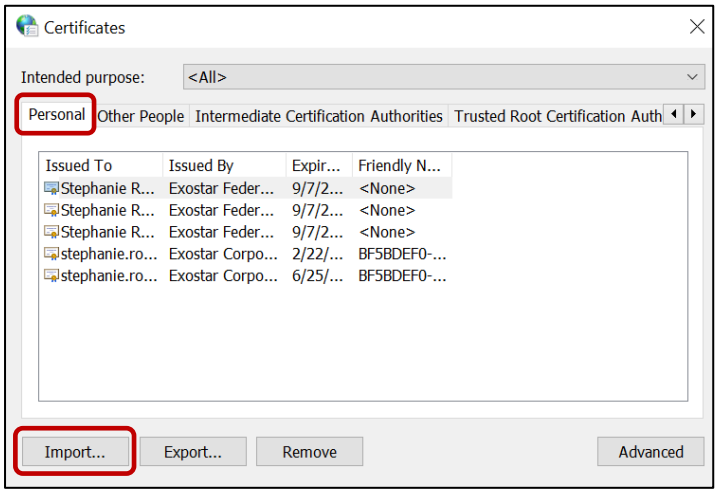
NOTE: To label this as your **Identity** certificate, enter **last name (Identity)**. This enables you to identify your certificates correctly.

12. The file path is created. Click **Next**, then click **Finish**.
13. Click **OK** on the confirmation screen.
14. You have successfully exported your digital certificate. If you have multiple certificates, back-up each certificate by following this process.

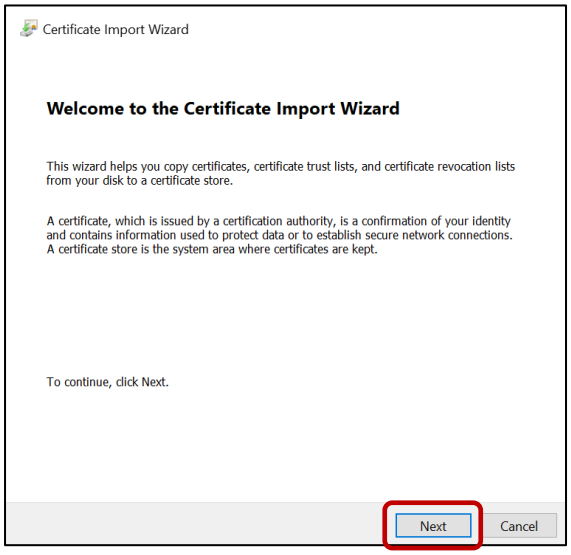
Import Certificates

Follow the steps below to import the certificates you previously backed up:

1. Go to your Windows Start menu.
2. Search for **Internet Options** and open it.
3. Select the **Content** tab and click the **Certificates** sub-tab.
4. From the **Personal** tab, click **Import**.



5. The **Certificate Import Wizard** opens, click **Next.**



6. Browse for the .pfx file (certificate) you saved during the export process. Click "**Browse…**"
7. Make sure you are browsing for file type .pfx and choose the certificate labeled **Identity** and click **Open.**
8. The certificate file path populates. Click **Next**.
9. Enter the password you applied to the certificate during the export process.
10. Optionally, check the box to **Enable Strong Key** protection to be prompted for this password each time this certificate is leveraged.
11. Choose the "**Automatically select…**" option and click **Next**.
12. Click **Finish**.

13. The **Importing new private exchange key** window displays. At this point, you have the option to increase the security level of the certificate.

NOTE: If you wish to increase the security level, click **Set Security Level** and follow the steps provided in the Increasing Certificate Security Level section for next steps.

14. To leave your security level at **Medium**, click **OK.**
15. Click **OK** on the confirmation screen.

You have completed the certificate import process. If you need to import additional certificates, follow the process until you import all certificates.

Increase Certificate Security Level

In the previous section, we covered the Import of Digital certificates. As a corporate policy, you may also be required to add additional Security levels for your certificate. At Exostar, we encourage you to set the security level for your Medium Level of Assurance Certificates to **High**.

1. Starting from Step 13 above, click the **Set Security Level** button.
2. Choose the **High** option and click **Next**.
3. Enter a **CryptoAPI Private Key Password**, confirm the password and click **Finish**.

NOTE: Please remember this password. When using your certificate to access ForumPass, you are prompted for this CryptoAPI password after selecting your certificate.

4. Security level is now set to **High**. Click **OK**.
5. Click **OK** on the confirmation screen.

FIS Administrator Responsibilities

FIS Administrators are individuals of an organization who are designated within MAG to perform administrative activities for an application. A FISA performs the following functions:

- Approves all user requests for access to FIS
- Prepares employment authorization letters for users
- Revokes user's Digital Certificates

The FISA is not required to have digital certificates to perform all the roles above.

Approve/Deny FIS Requests

1. Log into MAG.
2. Click the **Registration Requests** tab.
3. Click **Authorize FIS** to redirect to the **FIS Requests** queue.
4. Filter/sort the requests by clicking the drop-down menus and column headers.
5. Click the hyperlinked **Request ID** for the request you want to process.
6. Review user information and modify if required. Review the certificate attributes and if any fields have **Unknown**, review, and select appropriate option. Add any comments you may want to add. If denying the request, you are required to enter the denial comments.
7. Click **Approve** or **Deny**.
8. A confirmation screen displays.

NOTES:

- Selecting **Deny** prompts you to enter deny comments.

- Depending on your Organization's subscriptions, you may be prompted to approve a user for Basic Level of Assurance (BLOA) or Medium Level of Assurance (MLOA). Please note MLOA certificates require the user to appear for in-person identity vetting.

Request/Prepare Employment Verification Letter

The employment verification letter must be signed by the FIS Administrator or an authorized signatory within the organization and provided to the user for their In-Person Proofing appointment.

To prepare an employment verification letter:

1. Log into MAG and follow the steps above to approve the user's FIS registration request.
2. Request or prepare an employment verification letter.
3. Sign the employment verification letter (the FIS Administrator's signature must be on the letter).
4. Provide the letter to the user prior to the scheduled identity vetting appointment.
5. Inform the user they must present this letter to the authorized individual facilitating the identity proofing.

NOTES:

- The employment verification letter is a crucial component to the successful completion of the identity proofing of the user. Failure on the part of the user to provide this letter results in failed identity vetting. Users are required to re-appear for their identity vetting appointment. This could incur an additional cost.
- The employment verification letter should be printed on corporate letterhead, provide the applicant's full name, employee number, assert the applicant's affiliation with the organization, and be duly signed by the FIS Administrator/authorized signatory.

View User's Certificates

To view a user's certificates:

1. Log into MAG.
2. Click the **Administration** tab.
3. Enter search criteria, or leave blank for all, and click **Search**.
4. Review search results and change the number of results per page using the drop-down.
5. Sort by a column (ascending or descending) by clicking the column header.

NOTE: As an FIS Administrator, you can only view and not change a user's profile information.

Revoke User's Certificates

To revoke a user's certificates:

1. Log into MAG and locate the desired user's profile.
2. View the user's certificates at the bottom of their profile.
3. Click the **Revoke** button.
4. A revocation email is sent to you and the user.

NOTES:

- Users can revoke their own certificates at any time.
- You should revoke a user's certificates if you believe the security of those certificates have been compromised in any way.

- You should revoke a user's certificates if they are no longer employed with your organization.
- Revocation of certificates is a permanent action (i.e., there is no way to recover those certificates and the user must reapply should they need those certificates).