Federated Identity Service (FIS)

Product Guide

Contents

Document Versioning....4
Document Overview....5
Federated Identity Service (FIS) Overview....5
Purchase Information....5
  Web Store Access....5
  Medium Level of Assurance (MLOA) - Hardware....6
  Medium Level of Assurance (MLOA) – Software....9
  Basic Level of Assurance (BLOA) – Secure Email and Identity Certificate....12
FIS Registration....14
  Self-Registration....14
  Administrator Registration....16
  Exostar Registration....16
In-Person Proofing....16
Certificate Download Requirements....18
  System Requirements....18
  System Permissions....18
    Certificate Store Permissions....18
  Install Exostar's KMA™....19
Certificate Download....20
  Basic Level of Assurance Identity Certificate Download....20
  Basic Level of Assurance Secure Email Download....21
  Medium Level of Assurance Software Certificates Download....22
  Medium Level of Assurance Hardware Certificates Download....23
    Hardware Token FIPS Mode Review....24
    Download Certificates to Token....25
    Hardware Token Installation....27
Manage Certificates....28
  View Certificates....28
  Revoke Certificates....29
  Recover Encryption Keys....30
    Import Recovered Encryption Keys....34
Certificate Renewal....37
  Download Renewal Certificates....38

Disable/Remove Old Certificates 38
Export/Import Certificates 39
Export Certificates........ 39
Import Certificates 39
Increase Certificate Security Level 40
FIS Administrator Responsibilities........ 40
Approve/Deny FIS Requests........ 41
Request/Prepare Employment Verification Letter 41
View User’s Certificates 42
Revoke User’s Certificates........ 42

Document Versioning

Version	Change Overview	Date	Responsible Party
1.0		06/15/2018	Matt Williams
MAG 7.0		02/19/2021	Beena Nair
MAG 7.2	Exostar's KMA™	07/02/2021	Beena Nair

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
- Exostar's KMA™ installation
- 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 - https://www4.exostar.com/.

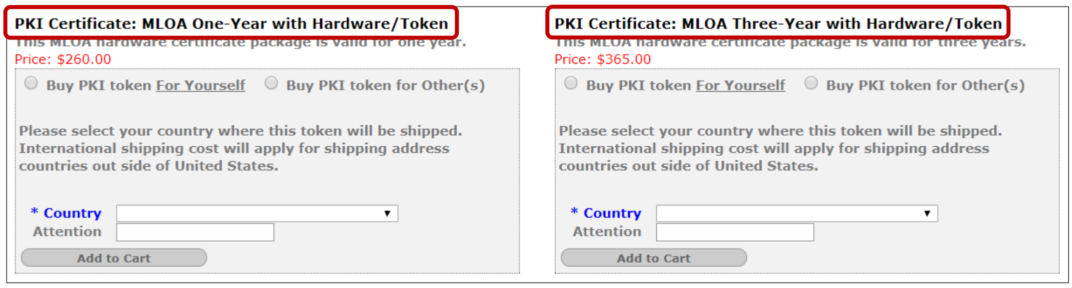
2. Or you can login to your MAG Account, then select **Billing and Support**, located at the bottom of the MAG Dashboard.
3. Next click the **Exostar Web Store – Home Page** tab.

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



PKI Certificate: MLOA One-Year with Hardware/Token
This MLOA hardware certificate package is valid for one year.
Price: $260.00

○ Buy PKI token For Yourself ○ Buy PKI token for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

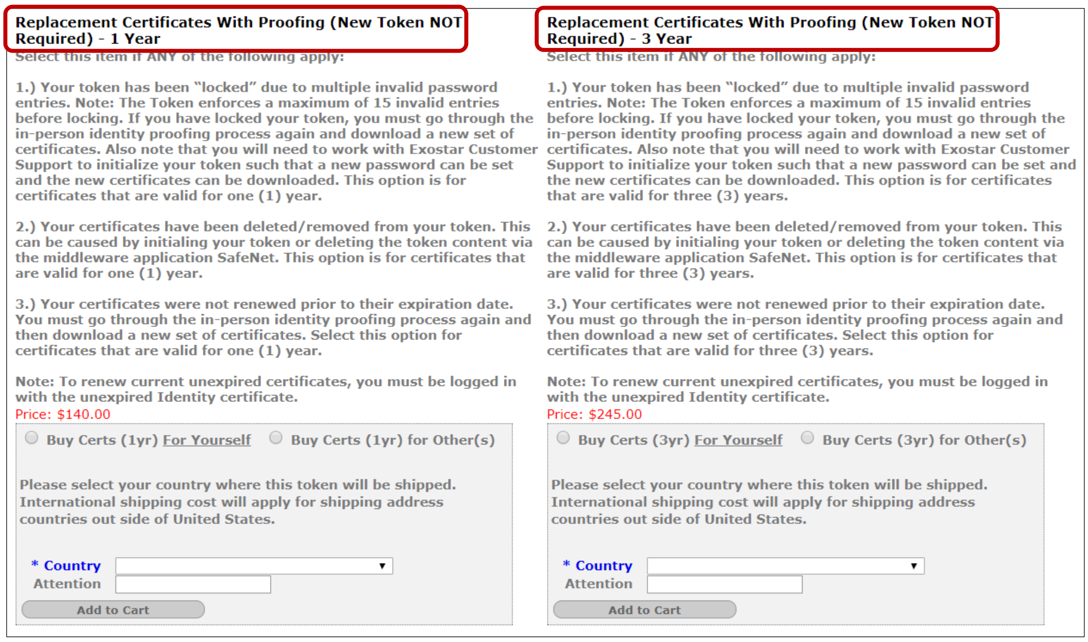
PKI Certificate: MLOA Three-Year with Hardware/Token
This MLOA hardware certificate package is valid for three years.
Price: $365.00

○ Buy PKI token For Yourself ○ Buy PKI token for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

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



Replacement Certificates With Proofing (New Token NOT Required) - 1 Year
Select this item if ANY of the following apply:

1.) Your token has been "locked" due to multiple invalid password entries. Note: The Token enforces a maximum of 15 invalid entries before locking. If you have locked your token, you must go through the in-person identity proofing process again and download a new set of certificates. Also note that you will need to work with Exostar Customer Support to initialize your token such that a new password can be set and the new certificates can be downloaded. This option is for certificates that are valid for one (1) year.

2.) Your certificates have been deleted/removed from your token. This can be caused by initialing your token or deleting the token content via the middleware application SafeNet. This option is for certificates that are valid for one (1) year.

3.) Your certificates were not renewed prior to their expiration date. You must go through the in-person identity proofing process again and then download a new set of certificates. Select this option for certificates that are valid for one (1) year.

Note: To renew current unexpired certificates, you must be logged in with the unexpired Identity certificate.
Price: $140.00

○ Buy Certs (1yr) For Yourself ○ Buy Certs (1yr) for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

Replacement Certificates With Proofing (New Token NOT Required) - 3 Year
Select this item if ANY of the following apply:

1.) Your token has been "locked" due to multiple invalid password entries. Note: The Token enforces a maximum of 15 invalid entries before locking. If you have locked your token, you must go through the in-person identity proofing process again and download a new set of certificates. Also note that you will need to work with Exostar Customer Support to initialize your token such that a new password can be set and the new certificates can be downloaded. This option is for certificates that are valid for three (3) years.

2.) Your certificates have been deleted/removed from your token. This can be caused by initialing your token or deleting the token content via the middleware application SafeNet. This option is for certificates that are valid for three (3) years.

3.) Your certificates were not renewed prior to their expiration date. You must go through the in-person identity proofing process again and then download a new set of certificates. Select this option for certificates that are valid for three (3) years.

Note: To renew current unexpired certificates, you must be logged in with the unexpired Identity certificate.
Price: $245.00

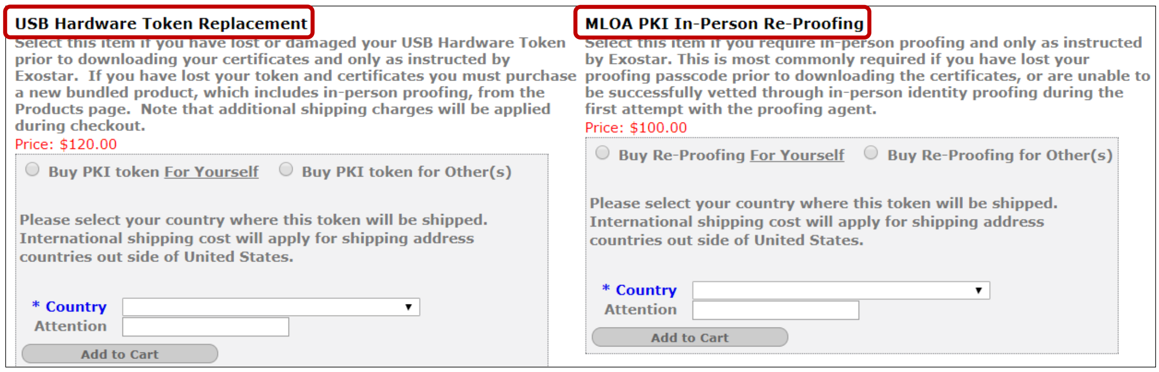
○ Buy Certs (3yr) For Yourself ○ Buy Certs (3yr) for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

e. USB Hardware Token Replacement

f. MLOA PKI In-Person Re-Proofing



USB Hardware Token Replacement

Select this item if you have lost or damaged your USB Hardware Token prior to downloading your certificates and only as instructed by Exostar. If you have lost your token and certificates you must purchase a new bundled product, which includes in-person proofing, from the Products page. Note that additional shipping charges will be applied during checkout.

Price: $120.00

○ Buy PKI token For Yourself ○ Buy PKI token for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country ▾
Attention

Add to Cart

MLOA PKI In-Person Re-Proofing

Select this item if you require in-person proofing and only as instructed by Exostar. This is most commonly required if you have lost your proofing passcode prior to downloading the certificates, or are unable to be successfully vetted through in-person identity proofing during the first attempt with the proofing agent.

Price: $100.00

○ Buy Re-Proofing For Yourself ○ Buy Re-Proofing for Other(s)

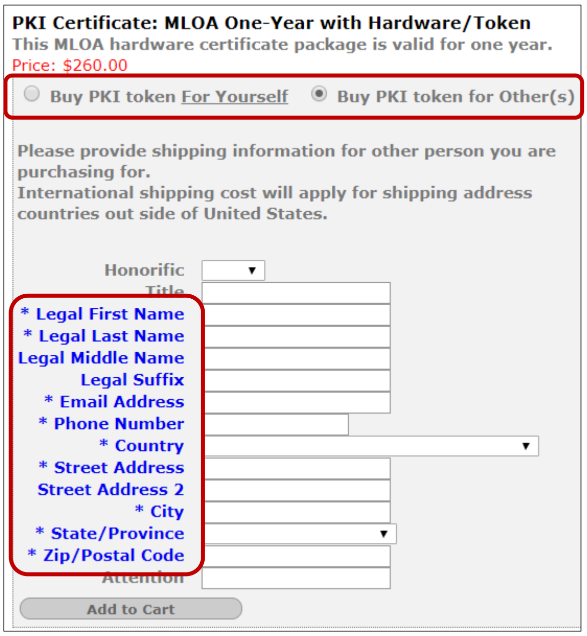
Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country ▾
Attention

Add to Cart

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.



PKI Certificate: MLOA One-Year with Hardware/Token

This MLOA hardware certificate package is valid for one year.

Price: $260.00

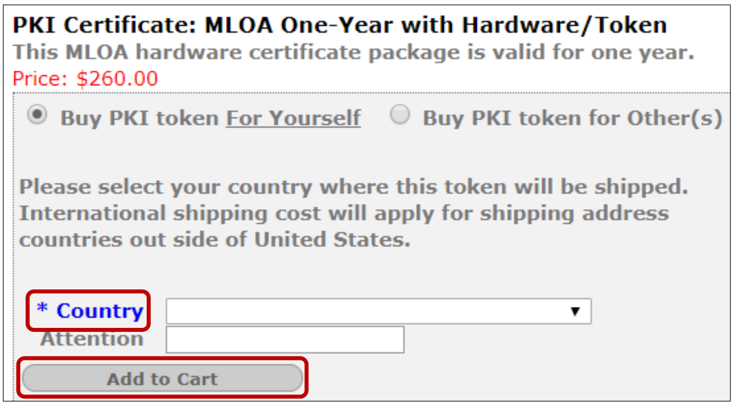
○ Buy PKI token For Yourself ● Buy PKI token for Other(s)

Please provide shipping information for other person you are purchasing for.
International shipping cost will apply for shipping address countries out side of United States.

Honorific ▾
Title
* Legal First Name
* Legal Last Name
Legal Middle Name
Legal Suffix
* Email Address
* Phone Number
* Country ▾
* Street Address
Street Address 2
* City
* State/Province ▾
* Zip/Postal Code
Attention

Add to Cart

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



PKI Certificate: MLOA One-Year with Hardware/Token

This MLOA hardware certificate package is valid for one year.

Price: $260.00

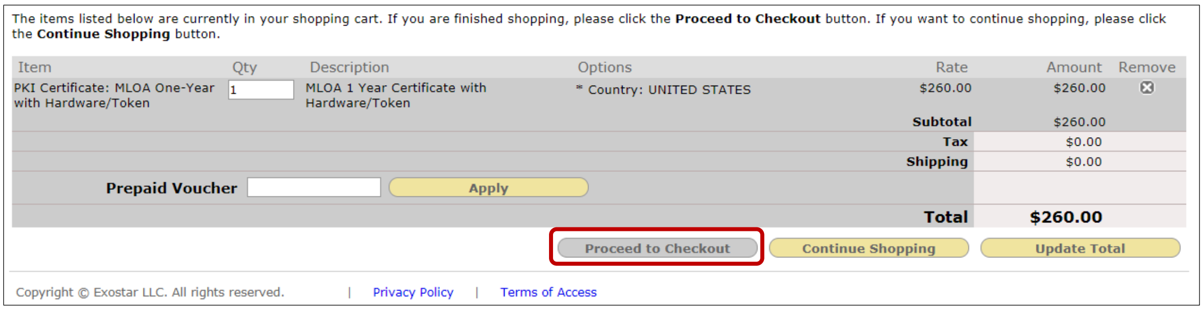
● Buy PKI token For Yourself ○ Buy PKI token for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country ▾
Attention

Add to Cart

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

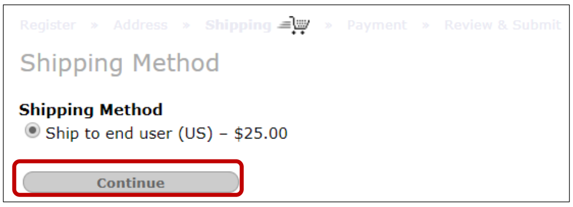


The items listed below are currently in your shopping cart. If you are finished shopping, please click the **Proceed to Checkout** button. If you want to continue shopping, please click the **Continue Shopping** button.

Item	Qty	Description	Options	Rate	Amount	Remove
PKI Certificate: MLOA One-Year with Hardware/Token	1	MLOA 1 Year Certificate with Hardware/Token	* Country: UNITED STATES	$260.00	$260.00	⊗
				Subtotal	$260.00	
				Tax	$0.00	
				Shipping	$0.00	
Prepaid Voucher		Apply				
				Total	**$260.00**	

Copyright © Exostar LLC. All rights reserved. | Privacy Policy | Terms of Access

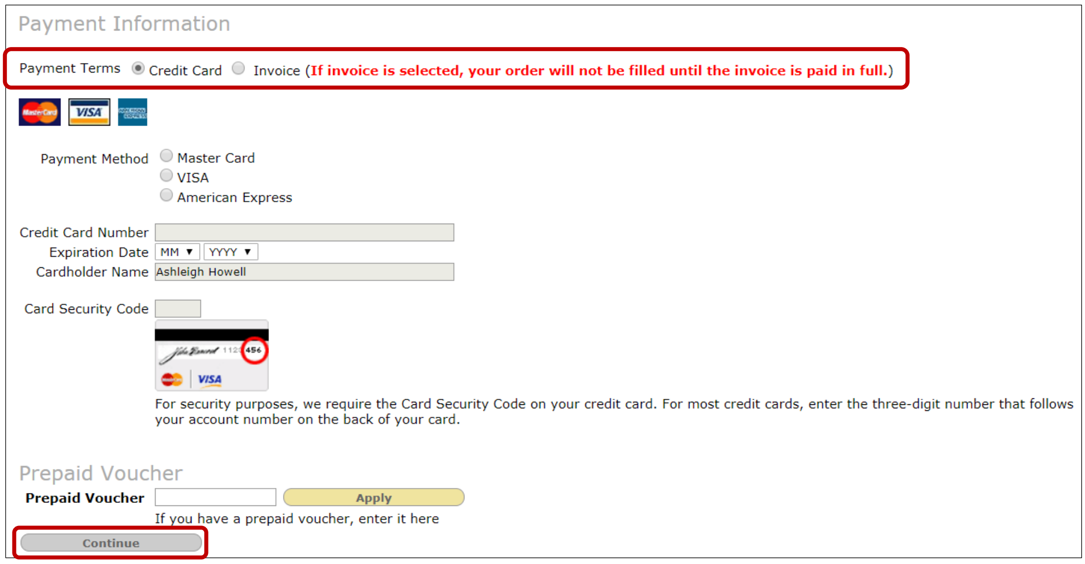
5. You are redirected to the **Shipping Method** page. **Ship to end** user is the only option available and is already selected. Click **Continue**.



Shipping Method

Shipping Method
● Ship to end user (US) – $25.00

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



Payment Information

Payment Terms ● Credit Card ○ Invoice (**If invoice is selected, your order will not be filled until the invoice is paid in full.**)

Payment Method ○ Master Card
○ VISA
○ American Express

Credit Card Number
Expiration Date MM ▾ YYYY ▾
Cardholder Name Ashleigh Howell

Card Security Code

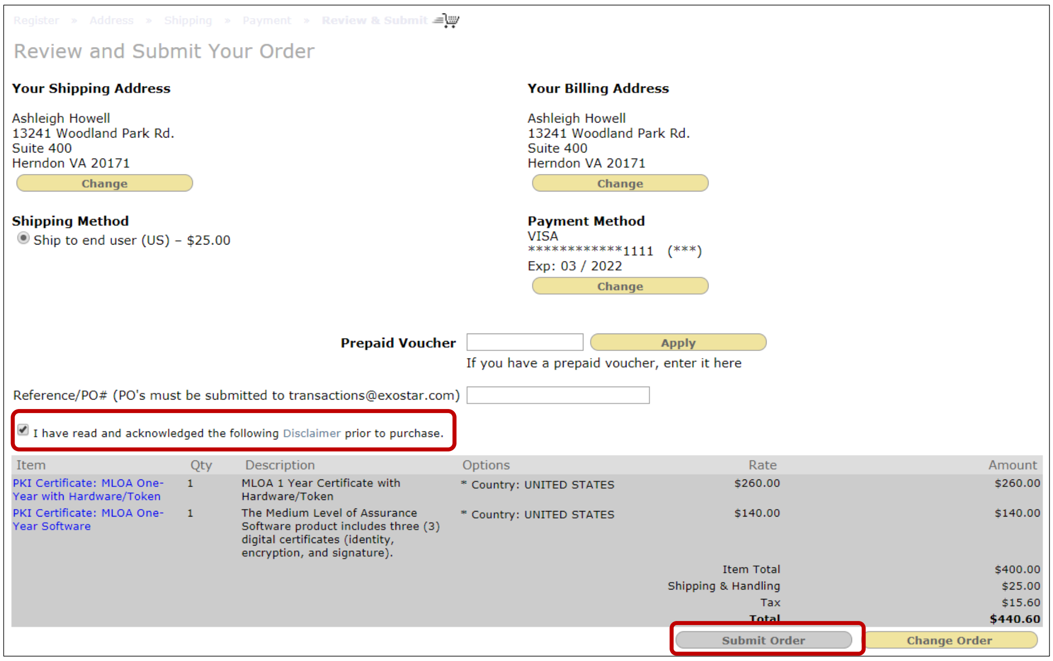
For security purposes, we require the Card Security Code on your credit card. For most credit cards, enter the three-digit number that follows your account number on the back of your card.

Prepaid Voucher
Prepaid Voucher Apply
If you have a prepaid voucher, enter it here

NOTE: The invoice option requires you complete payment before receiving 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**.



Register » Address » Shipping » Payment » Review & Submit

Review and Submit Your Order

Your Shipping Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Your Billing Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Shipping Method

● Ship to end user (US) – $25.00

Payment Method

VISA
************1111 (***)
Exp: 03 / 2022

Prepaid Voucher

If you have a prepaid voucher, enter it here

Reference/PO# (PO's must be submitted to transactions@exostar.com)

☑ I have read and acknowledged the following Disclaimer prior to purchase.

Item	Qty	Description	Options	Rate	Amount
PKI Certificate: MLOA One-Year with Hardware/Token	1	MLOA 1 Year Certificate with Hardware/Token	* Country: UNITED STATES	$260.00	$260.00
PKI Certificate: MLOA One-Year Software	1	The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).	* Country: UNITED STATES	$140.00	$140.00
				Item Total	$400.00
				Shipping & Handling	$25.00
				Tax	$15.60
				Total	**$440.60**

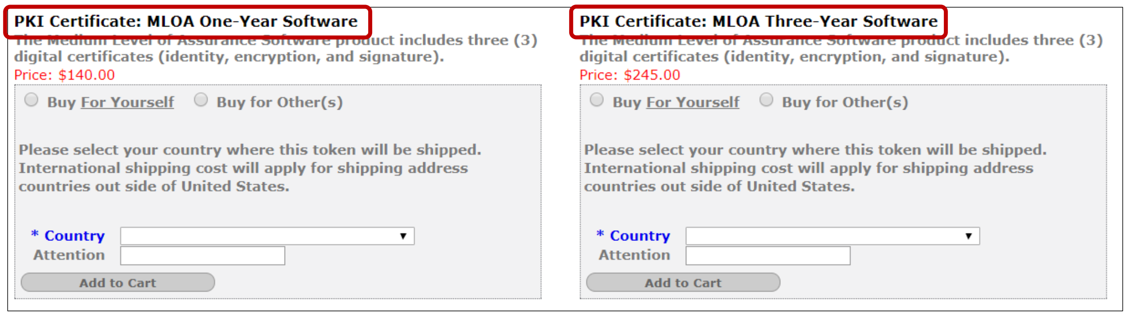
NOTE: A confirmation page displays, providing your **Sales Order Number** (SO#####).

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



PKI Certificate: MLOA One-Year Software

The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).

Price: $140.00

○ Buy For Yourself ○ Buy for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

PKI Certificate: MLOA Three-Year Software

The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).

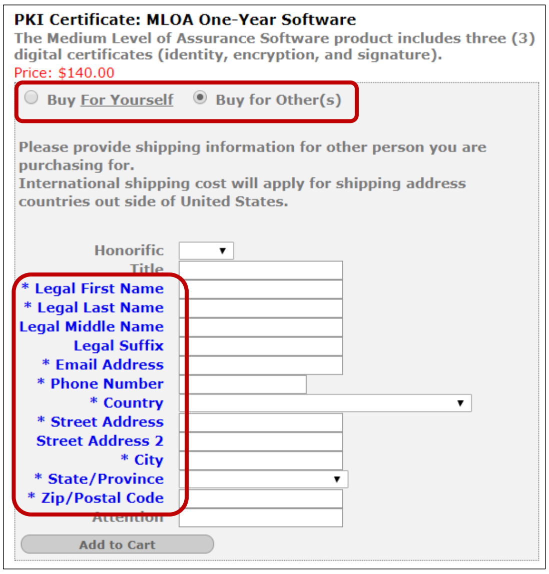
Price: $245.00

○ Buy For Yourself ○ Buy for Other(s)

Please select your country where this token will be shipped. International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

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.



PKI Certificate: MLOA One-Year Software

The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).

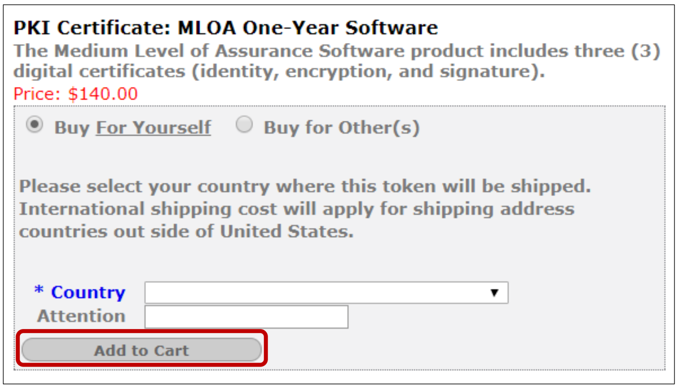
Price: $140.00

○ Buy For Yourself ● Buy for Other(s)

Please provide shipping information for other person you are purchasing for.
International shipping cost will apply for shipping address countries out side of United States.

Honorific
Title
* Legal First Name
* Legal Last Name
Legal Middle Name
Legal Suffix
* Email Address
* Phone Number
* Country
* Street Address
Street Address 2
* City
* State/Province
* Zip/Postal Code
Attention

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



PKI Certificate: MLOA One-Year Software

The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).

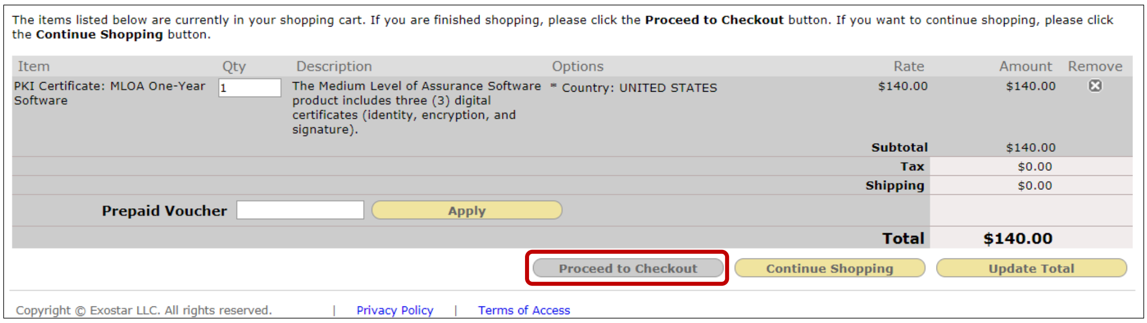
Price: $140.00

● Buy For Yourself ○ Buy for Other(s)

Please select your country where this token will be shipped.
International shipping cost will apply for shipping address countries out side of United States.

* Country
Attention

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

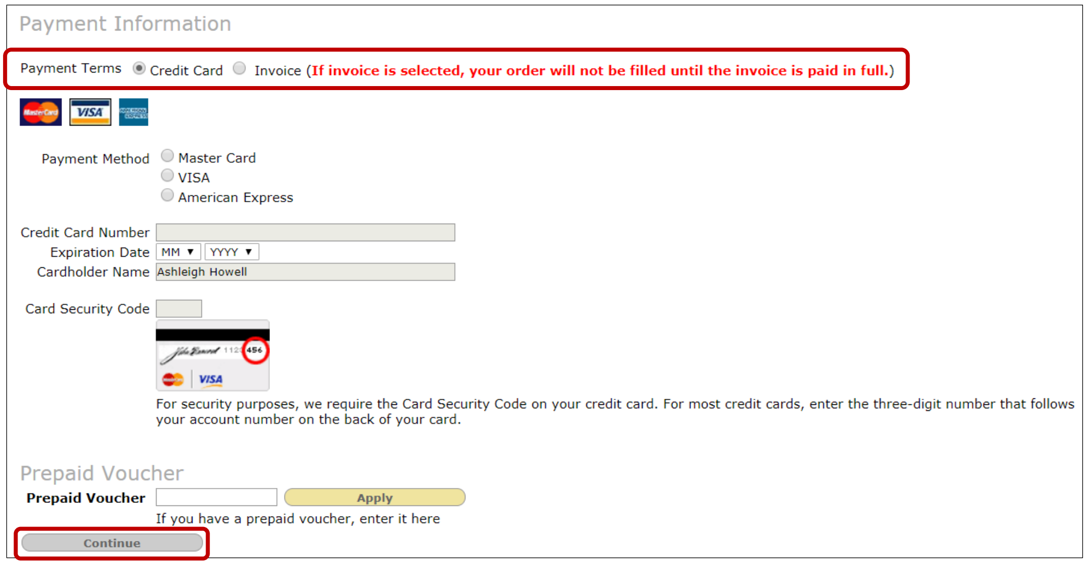


The items listed below are currently in your shopping cart. If you are finished shopping, please click the **Proceed to Checkout** button. If you want to continue shopping, please click the **Continue Shopping** button.

Item	Qty	Description	Options	Rate	Amount	Remove
PKI Certificate: MLOA One-Year Software	1	The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).	* Country: UNITED STATES	$140.00	$140.00	☒
				Subtotal	$140.00	
				Tax	$0.00	
				Shipping	$0.00	
Prepaid Voucher		Apply				
				Total	**$140.00**	

Copyright © Exostar LLC. All rights reserved. | Privacy Policy | Terms of Access

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



Payment Information

Payment Terms ● Credit Card ○ Invoice (**If invoice is selected, your order will not be filled until the invoice is paid in full.**)

Payment Method ○ Master Card
○ VISA
○ American Express

Credit Card Number	
Expiration Date	MM ▾ YYYY ▾
Cardholder Name	Ashleigh Howell
Card Security Code	

For security purposes, we require the Card Security Code on your credit card. For most credit cards, enter the three-digit number that follows your account number on the back of your card.

Prepaid Voucher

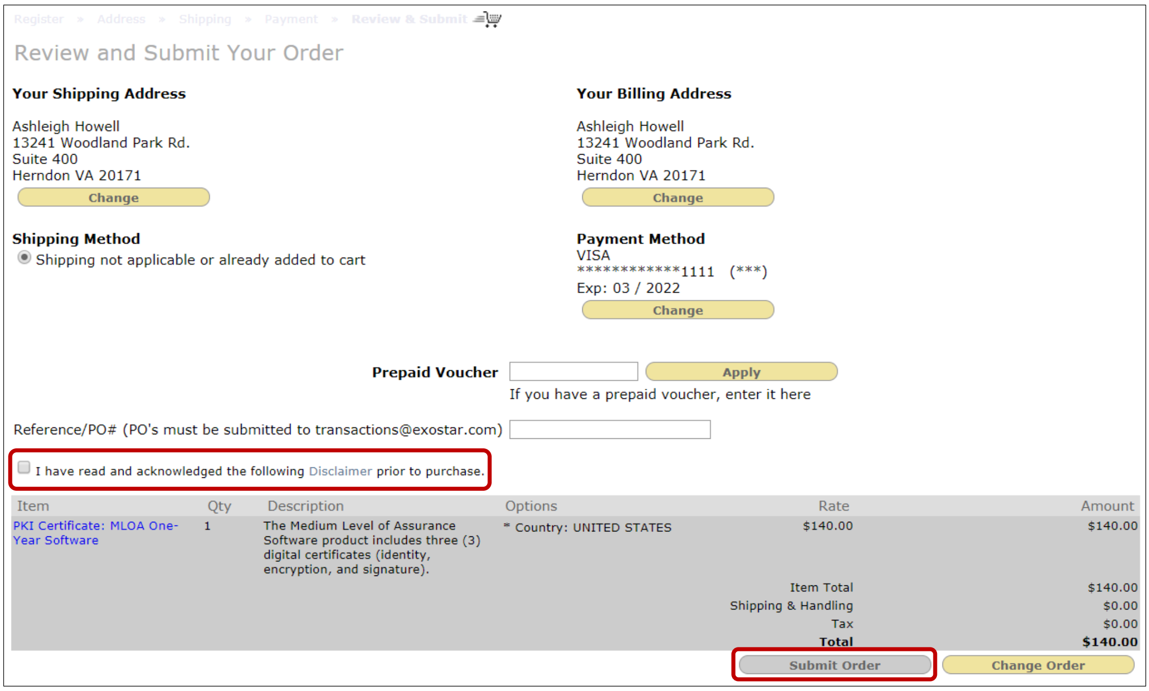
Prepaid Voucher Apply

If you have a prepaid voucher, enter it here

Continue

NOTE: The invoice option requires you complete payment 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**.



Register » Address » Shipping » Payment » Review & Submit

Review and Submit Your Order

Your Shipping Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Change

Shipping Method

● Shipping not applicable or already added to cart

Your Billing Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Change

Payment Method

VISA
************1111 (***)
Exp: 03 / 2022

Change

Prepaid Voucher Apply

If you have a prepaid voucher, enter it here

Reference/PO# (PO's must be submitted to transactions@exostar.com)

□ I have read and acknowledged the following Disclaimer prior to purchase.

Item	Qty	Description	Options	Rate	Amount
PKI Certificate: MLOA One-Year Software	1	The Medium Level of Assurance Software product includes three (3) digital certificates (identity, encryption, and signature).	* Country: UNITED STATES	$140.00	$140.00
				Item Total	$140.00
				Shipping & Handling	$0.00
				Tax	$0.00
				Total	**$140.00**

Submit Order Change Order

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

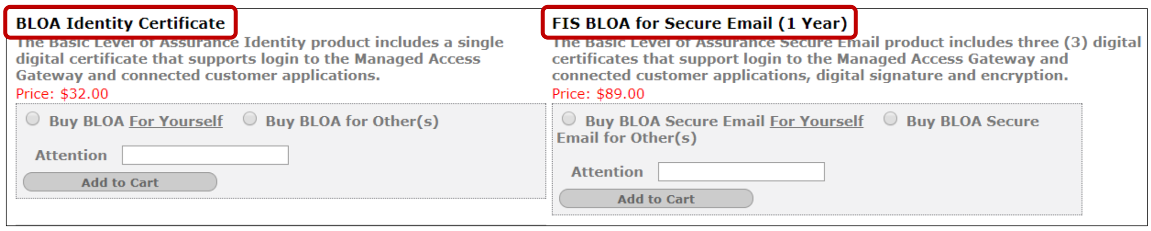
Basic Level of Assurance (BLOA) – Secure Email and Identity Certificate

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:



BLOA Identity Certificate
The Basic Level of Assurance Identity product includes a single digital certificate that supports login to the Managed Access Gateway and connected customer applications.
Price: $32.00

○ Buy BLOA For Yourself ○ Buy BLOA for Other(s)

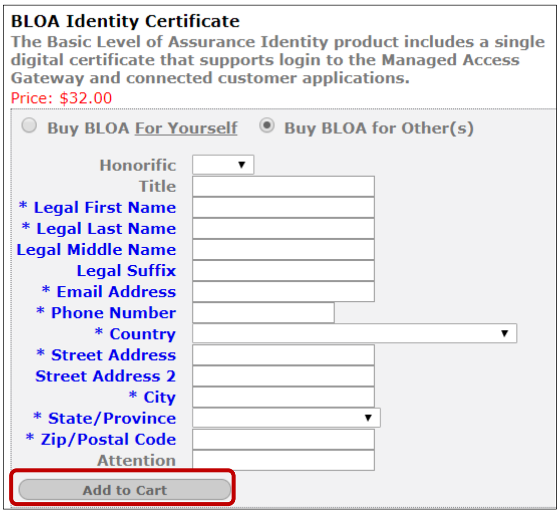
Attention

FIS BLOA for Secure Email (1 Year)
The Basic Level of Assurance Secure Email product includes three (3) digital certificates that support login to the Managed Access Gateway and connected customer applications, digital signature and encryption.
Price: $89.00

○ Buy BLOA Secure Email For Yourself ○ Buy BLOA Secure Email for Other(s)

Attention

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.

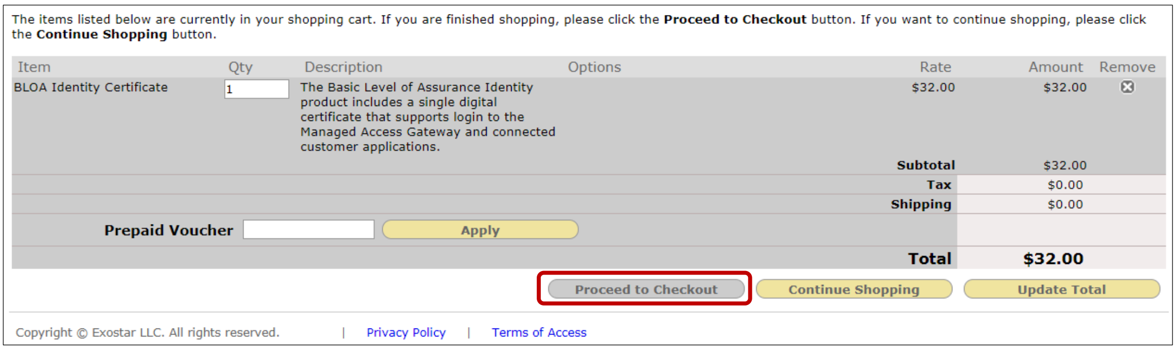


BLOA Identity Certificate
The Basic Level of Assurance Identity product includes a single digital certificate that supports login to the Managed Access Gateway and connected customer applications.
Price: $32.00

○ Buy BLOA For Yourself ● Buy BLOA for Other(s)

Honorific
Title
* Legal First Name
* Legal Last Name
Legal Middle Name
Legal Suffix
* Email Address
* Phone Number
* Country
* Street Address
Street Address 2
* City
* State/Province
* Zip/Postal Code
Attention

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



The items listed below are currently in your shopping cart. If you are finished shopping, please click the **Proceed to Checkout** button. If you want to continue shopping, please click the **Continue Shopping** button.

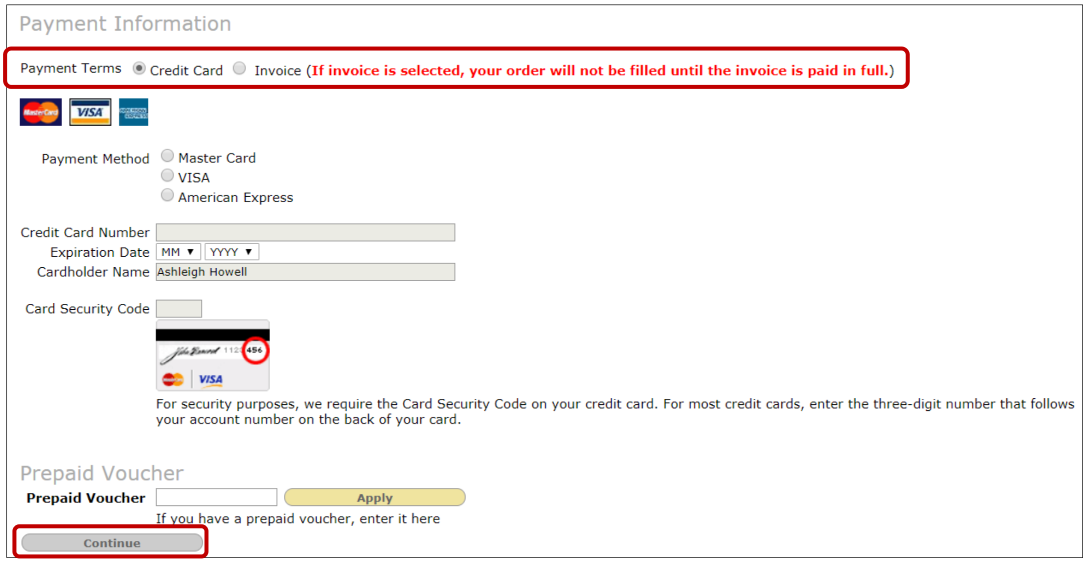
Item	Qty	Description	Options	Rate	Amount	Remove
BLOA Identity Certificate	1	The Basic Level of Assurance Identity product includes a single digital certificate that supports login to the Managed Access Gateway and connected customer applications.		$32.00	$32.00	☒
				Subtotal	$32.00	
				Tax	$0.00	
				Shipping	$0.00	
				Total	**$32.00**	

Prepaid Voucher [ ] Apply

Proceed to Checkout | Continue Shopping | Update Total

Copyright © Exostar LLC. All rights reserved. | Privacy Policy | Terms of Access

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



Payment Information

Payment Terms ● Credit Card ○ Invoice (**If invoice is selected, your order will not be filled until the invoice is paid in full.**)

Payment Method ○ Master Card
○ VISA
○ American Express

Credit Card Number
Expiration Date MM ▾ YYYY ▾
Cardholder Name Ashleigh Howell

Card Security Code

For security purposes, we require the Card Security Code on your credit card. For most credit cards, enter the three-digit number that follows your account number on the back of your card.

Prepaid Voucher

Prepaid Voucher [ ] Apply

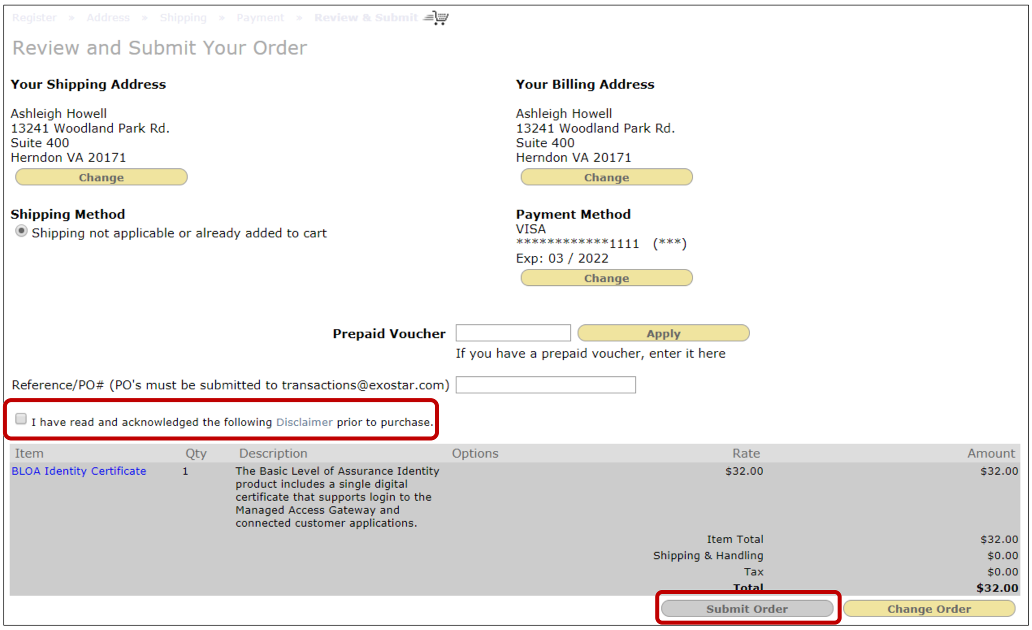
If you have a prepaid voucher, enter it here

Continue

NOTE: The invoice option requires you complete payment 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**.



Register » Address » Shipping » Payment » Review & Submit

Review and Submit Your Order

Your Shipping Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Your Billing Address

Ashleigh Howell
13241 Woodland Park Rd.
Suite 400
Herndon VA 20171

Shipping Method

● Shipping not applicable or already added to cart

Payment Method
VISA
************1111 (***)
Exp: 03 / 2022

Prepaid Voucher
If you have a prepaid voucher, enter it here

Reference/PO# (PO's must be submitted to transactions@exostar.com)

□ I have read and acknowledged the following Disclaimer prior to purchase.

Item	Qty	Description	Options	Rate	Amount
BLOA Identity Certificate	1	The Basic Level of Assurance Identity product includes a single digital certificate that supports login to the Managed Access Gateway and connected customer applications.		$32.00	$32.00
				Item Total	$32.00
				Shipping & Handling	$0.00
				Tax	$0.00
				Total	**$32.00**

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

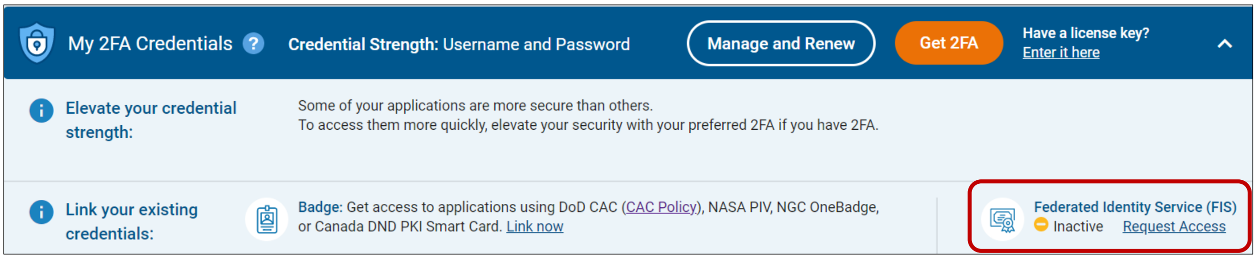
FIS Registration

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.



My 2FA Credentials ? **Credential Strength:** Username and Password

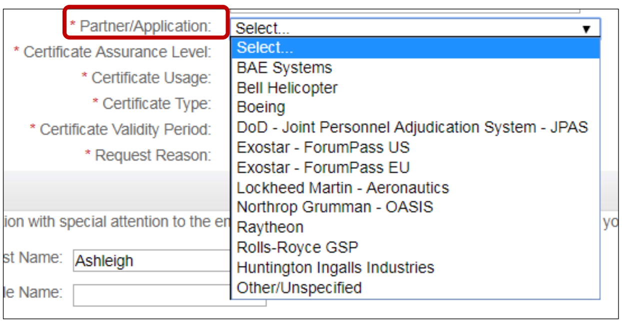
Have a license key? Enter it here

Elevate your credential strength:
Some of your applications are more secure than others.
To access them more quickly, elevate your security with your preferred 2FA if you have 2FA.

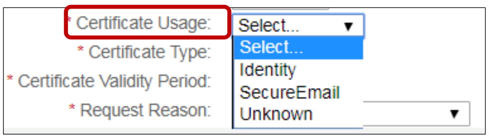
Link your existing credentials:
Badge: Get access to applications using DoD CAC (CAC Policy), NASA PIV, NGC OneBadge, or Canada DND PKI Smart Card. Link now

Federated Identity Service (FIS)
Inactive Request Access

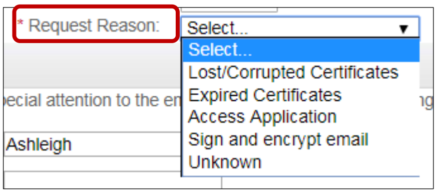
2. Fill out all necessary information under the **FIS Certificate Information** section:
    a. **Partner/Application**



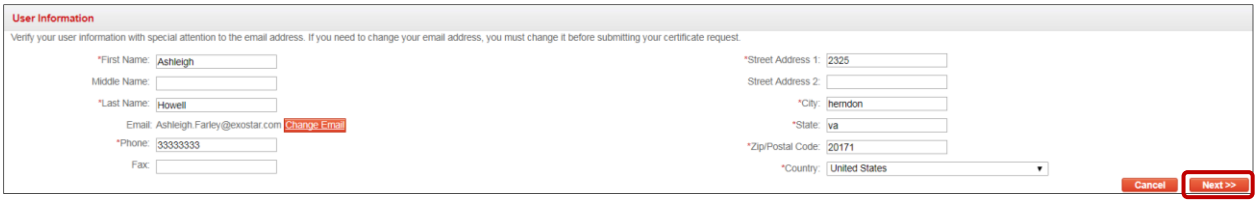
    b. **Certificate Assurance Level**
    c. **Certificate Usage**
        i. If you choose **Basic** assurance level:



        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**.

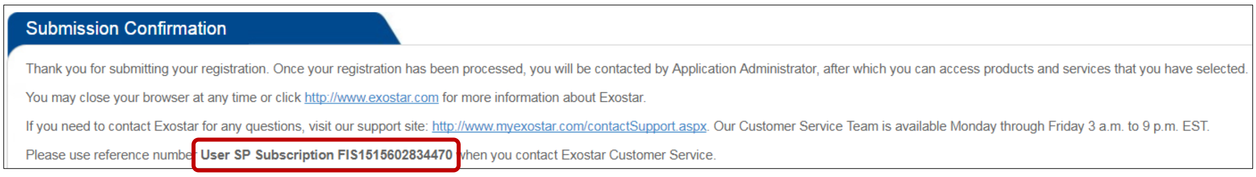


User Information

Verify your user information with special attention to the email address. If you need to change your email address, you must change it before submitting your certificate request.

*First Name:	Ashleigh	*Street Address 1:	2325
Middle Name:		Street Address 2:	
*Last Name:	Howell	*City:	herndon
Email:	Ashleigh.Farley@exostar.com Change Email	*State:	va
*Phone:	33333333	*Zip/Postal Code:	20171
Fax:		*Country:	United States

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



Submission Confirmation

Thank you for submitting your registration. Once your registration has been processed, you will be contacted by Application Administrator, after which you can access products and services that you have selected.

You may close your browser at any time or click http://www.exostar.com for more information about Exostar.

If you need to contact Exostar for any questions, visit our support site: http://www.myexostar.com/contactSupport.aspx. Our Customer Service Team is available Monday through Friday 3 a.m. to 9 p.m. EST.

Please use reference numbe **User SP Subscription FIS1515602834470** when you contact Exostar Customer Service.

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.

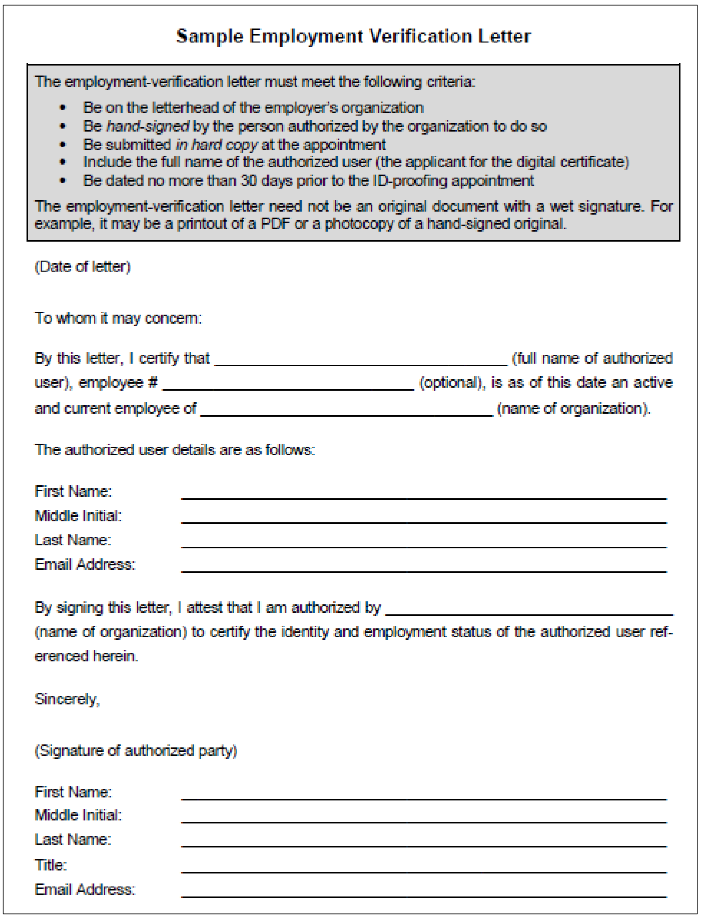
In-Person Proofing

MLOA Hardware and Software require you 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 set-up a proofing appointment with one of their Trusted Agents. For users outside the United States, a Trusted Agent from Verify Europe contacts you to set-up 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.



Sample Employment Verification Letter

The employment-verification letter must meet the following criteria:

- Be on the letterhead of the employer's organization
- Be *hand-signed* by the person authorized by the organization to do so
- Be submitted *in hard copy* at the appointment
- Include the full name of the authorized user (the applicant for the digital certificate)
- Be dated no more than 30 days prior to the ID-proofing appointment

The employment-verification letter need not be an original document with a wet signature. For example, it may be a printout of a PDF or a photocopy of a hand-signed original.

(Date of letter)

To whom it may concern:

By this letter, I certify that ______________________________ (full name of authorized user), employee # __________________________ (optional), is as of this date an active and current employee of ______________________________ (name of organization).

The authorized user details are as follows:

First Name: ____
Middle Initial: ____
Last Name: ____
Email Address: ____

By signing this letter, I attest that I am authorized by ______________________________ (name of organization) to certify the identity and employment status of the authorized user referenced herein.

Sincerely,

(Signature of authorized party)

First Name: ____
Middle Initial: ____
Last Name: ____
Title: ____
Email Address: ____

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 and Windows 10 supported
- Permissions to enable KMA™ controls and plug-ins

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 ActiveX control 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: The confusing 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.

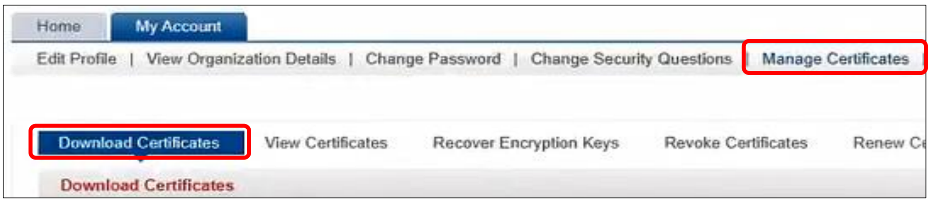
Install Exostar's KMA™

Exostar's Key Management Agent (KMA™) is required to successfully download your hardware certificates. In some organizations, due to IT security policies, individuals may not be allowed to download the KMA™ software to their machine. To install KMA™ software you can download it here or distribute via Group Policy.

NOTE: KMA™ cannot be downloaded using Internet Explorer. You can download KMA™ using Chrome, MS Edge, or Firefox.

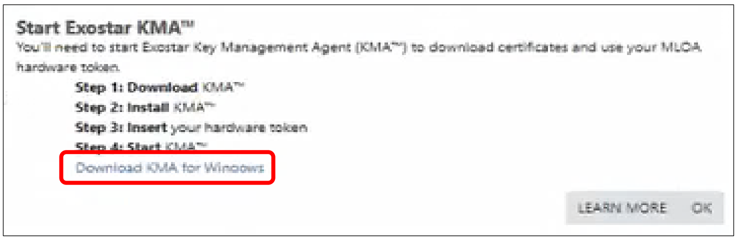
To install the KMA™ software, follow the steps below:

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: KMA™ cannot be downloaded using Internet Explorer. You can download KMA™ using Chrome, MS Edge, or Firefox.



Start Exostar KMA™

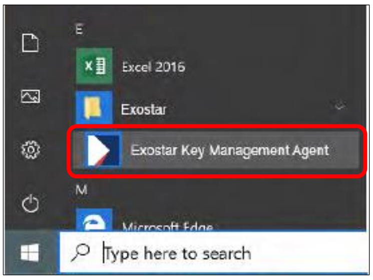
You'll need to start Exostar Key Management Agent (KMA™) to download certificates and use your MLOA hardware token.

Step 1: Download KMA™
Step 2: Install KMA™
Step 3: Insert your hardware token
Step 4: Start KMA™

Download KMA for Windows

LEARN MORE OK

4. After KMA™ has been downloaded and installed, insert your Hardware Token.
5. Next open KMA™ software.



Certificate Download

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

NOTES:

- KMA™ software download is only needed for downloading MLOA Hardware certificates
- 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 certificate store and must be imported from downloads.

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

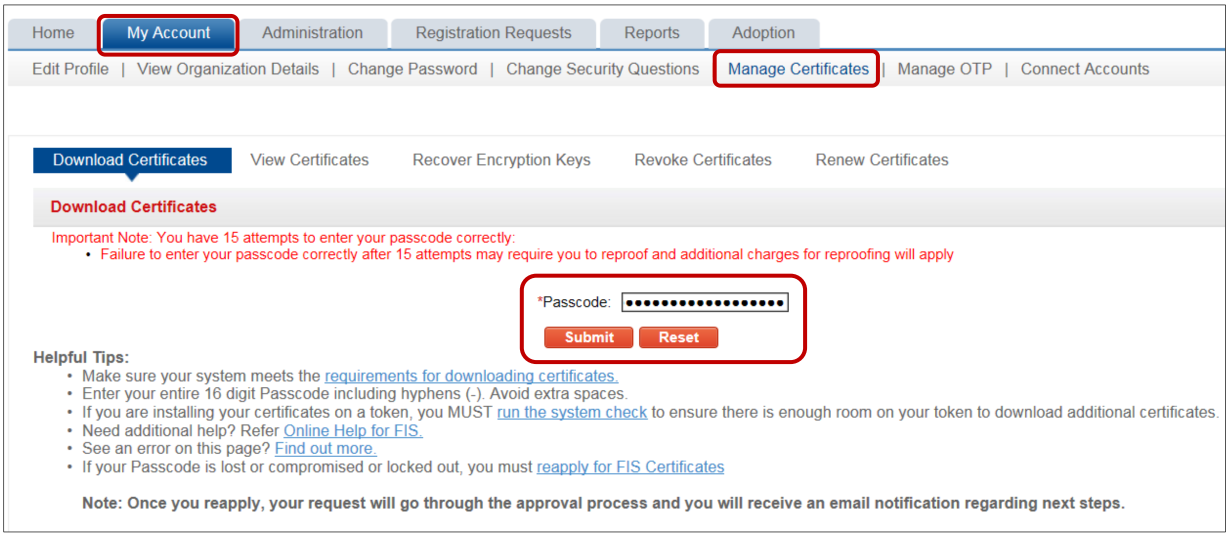
NOTE: Does not require KMA™ software download.

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.



Download Certificates

Important Note: You have 15 attempts to enter your passcode correctly:

- Failure to enter your passcode correctly after 15 attempts may require you to reproof and additional charges for reproofing will apply

*Passcode: ••••••••••••••••••

Helpful Tips:

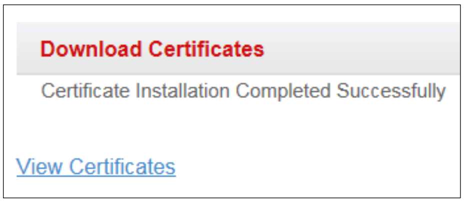
- Make sure your system meets the requirements for downloading certificates.
- Enter your entire 16 digit Passcode including hyphens (-). Avoid extra spaces.
- If you are installing your certificates on a token, you MUST run the system check to ensure there is enough room on your token to download additional certificates.
- Need additional help? Refer Online Help for FIS.
- See an error on this page? Find out more.
- If your Passcode is lost or compromised or locked out, you must reapply for FIS Certificates

Note: Once you reapply, your request will go through the approval process and you will receive an email notification regarding next steps.

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 displays.



Download Certificates

Certificate Installation Completed Successfully

Basic Level of Assurance Secure Email Download

Pre-requisites for downloading identity certificates:

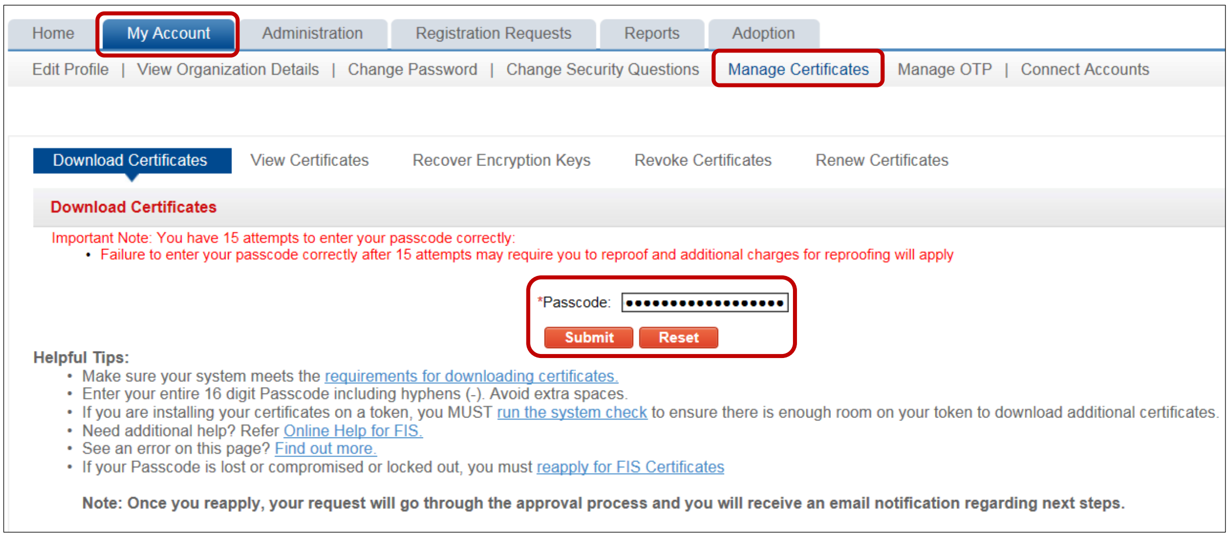
- Received 16-digit passcode from Exostar via email
- Reviewed system and certificate download requirements

NOTE: 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.



Download Certificates

Important Note: You have 15 attempts to enter your passcode correctly:

- Failure to enter your passcode correctly after 15 attempts may require you to reproof and additional charges for reproofing will apply

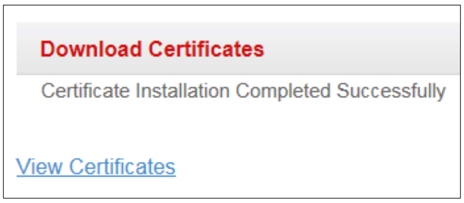
*Passcode: ••••••••••••••••••

Helpful Tips:

- Make sure your system meets the requirements for downloading certificates.
- Enter your entire 16 digit Passcode including hyphens (-). Avoid extra spaces.
- If you are installing your certificates on a token, you MUST run the system check to ensure there is enough room on your token to download additional certificates.
- Need additional help? Refer Online Help for FIS.
- See an error on this page? Find out more.
- If your Passcode is lost or compromised or locked out, you must reapply for FIS Certificates

Note: Once you reapply, your request will go through the approval process and you will receive an email notification regarding next steps.

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.



Download Certificates

Certificate Installation Completed Successfully

Medium Level of Assurance Software Certificates Download

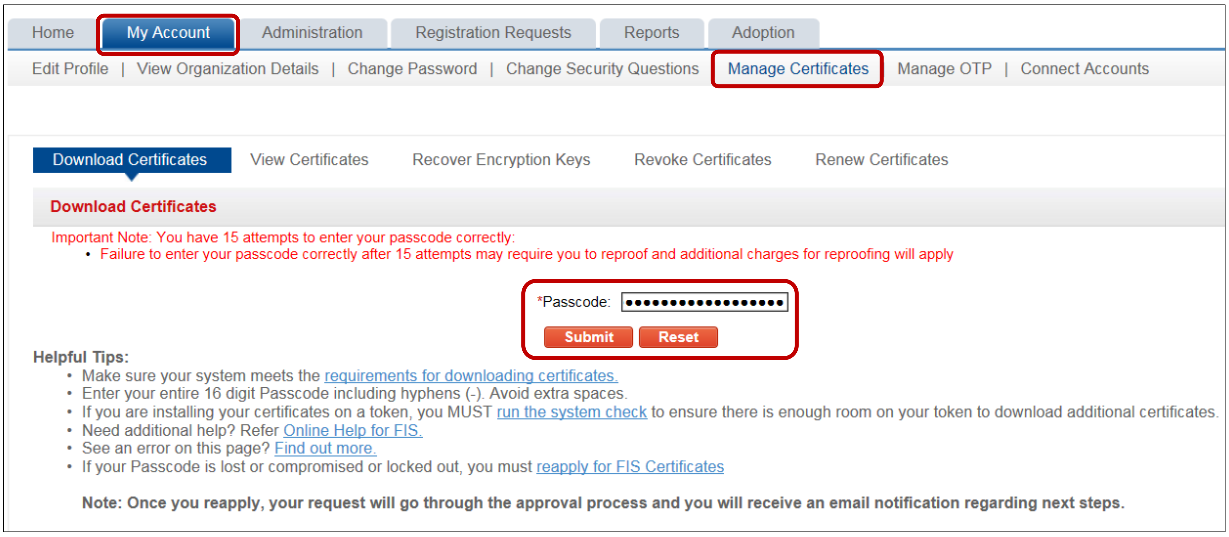
Pre-requisites for downloading certificates:

- 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. 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.



Download Certificates

Important Note: You have 15 attempts to enter your passcode correctly:

- Failure to enter your passcode correctly after 15 attempts may require you to reproof and additional charges for reproofing will apply

*Passcode: ••••••••••••••••••

Helpful Tips:

- Make sure your system meets the requirements for downloading certificates.
- Enter your entire 16 digit Passcode including hyphens (-). Avoid extra spaces.
- If you are installing your certificates on a token, you MUST run the system check to ensure there is enough room on your token to download additional certificates.
- Need additional help? Refer Online Help for FIS.
- See an error on this page? Find out more.
- If your Passcode is lost or compromised or locked out, you must reapply for FIS Certificates

Note: Once you reapply, your request will go through the approval process and you will receive an email notification regarding next steps.

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 Certificates Download

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, contact 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.
- Install the Exostar's Key Management Agent (KMA™) software to download your hardware certificate(s).
- 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 section 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.

1. If you completed the initial password change process for your token, plug the token into your USB drive. The **eToken PKI Client Properties** screen displays for the **Aladdin eToken PRO (72K) Java**.
2. Click on **View eToken Info** to display the token details.
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 **FIPS 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

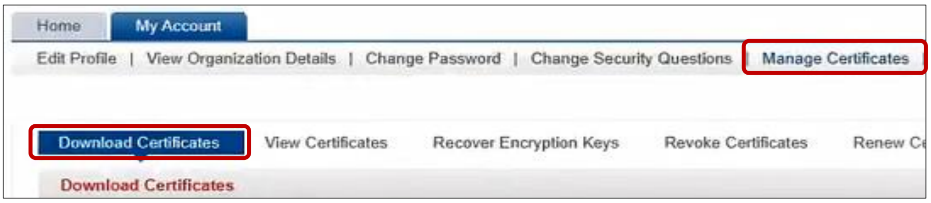
To display on FIPS Mode:

1. Click **eToken Pro Java**.
2. Select the **Initialize eToken** icon to display the initialize screen.
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 setup the token in the FIPS mode.
4. Check the box for **FIPS** mode, to set-up the FIS mode for the token. Click **OK** to complete.
5. On the **Initialize eToken** screen, click **Start**.
6. Select **OK** to start token initialization.
7. Once you successfully initialize your token, a confirmation screens displays. Click **OK**.
8. You are redirected to the **PKI Client** main screen. Select **View eToken Info**.
9. The **FIPS Mode** displays. Click **OK**.

Download Certificates to Token

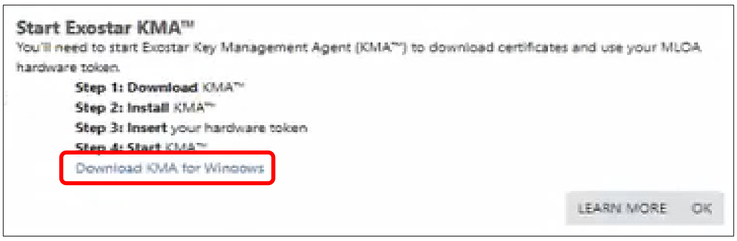
Before you begin downloading your certificates, install KMA™ software on your computer, as well as change the initial password of your token.

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



3. Next click **Download Certificates** tab. A prompt will display to **Download KMA™ for Windows**, then click **OK**.

   NOTE: KMA™ cannot be downloaded using Internet Explorer. You can download KMA™ using Chrome, MS Edge, or Firefox.

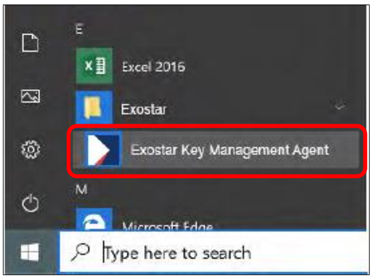


Start Exostar KMA™

You'll need to start Exostar Key Management Agent (KMA™) to download certificates and use your MLOA hardware token.

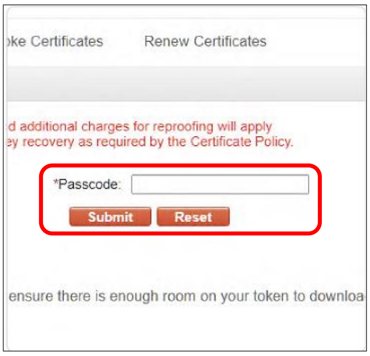
Step 1: Download KMA™
Step 2: Install KMA™
Step 3: Insert your hardware token
Step 4: Start KMA™

4. After KMA™ has been downloaded and installed, insert your Hardware Token.
5. Next **Open** KMA™ software program.



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

6. Enter your 16-digit proofing passcode, then click **Submit**.



d additional charges for reproofing will apply
ey recovery as required by the Certificate Policy.

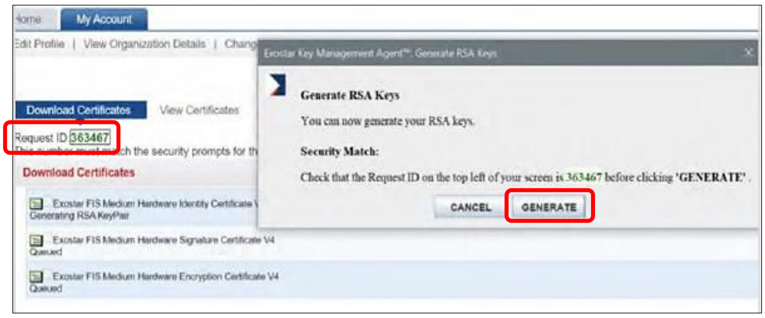
*Passcode:

ensure there is enough room on your token to downloa

NOTES:

- At the time of the in-person proofing appointment, the proofer provided you a passcode. This passcode is only valid after you receive a packet approval email from Exostar.
- 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.
- If you lose the passcode, you are required to complete a reproofing purchase and complete another in-person proofing appointment.

7. Verify the **Request ID** before you click **Generate**.



ome
My Account
Edit Profile | View Organization Details | Chang
Download Certificates
View Certificates
Exostar Key Management Agent™: Generate RSA Keys
CANCEL
GENERATE

Request ID 363467

ch the security prompts for th

Download Certificates

Exostar FIS Medium Hardware Identity Certificate V
Generating RSA KeyPair

Exostar FIS Medium Hardware Signature Certificate V4
Queued

Exostar FIS Medium Hardware Encryption Certificate V4
Queued

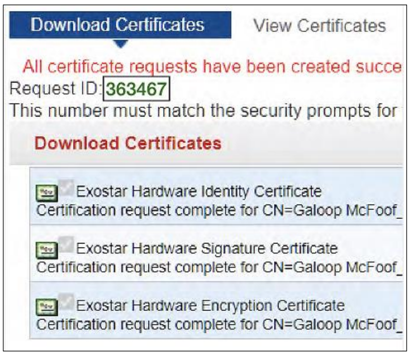
Generate RSA Keys

You can now generate your RSA keys.

Security Match:

Check that the Request ID on the top left of your screen is 363467 before clicking 'GENERATE'.

8. If your passcode is correct, a list of certificates to download will display. The system will automatically selects all of them for download.



All certificate requests have been created succe

Request ID: 363467

This number must match the security prompts for

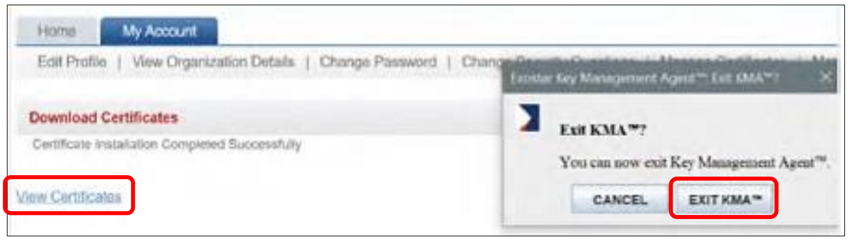
Download Certificates

Exostar Hardware Identity Certificate
Certification request complete for CN=Galoop McFoof_

Exostar Hardware Signature Certificate
Certification request complete for CN=Galoop McFoof_

Exostar Hardware Encryption Certificate
Certification request complete for CN=Galoop McFoof_

9. Once selected, you are prompted to enter the Hardware Token password. Enter the token password and click **OK.**
10. After you have successfully installed the certificates, you can exit KMA™ and view your certificates.



Home
My Account
Edit Profile | View Organization Details | Change Password | Chang
Exostar Key Management Agent™: Exit KMA™?
View Certificates
CANCEL
EXIT KMA™

Download Certificates

Certificate Installation Completed Successfully

Exit KMA™?

You can now exit Key Management Agent™.

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

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 KMA™**.

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

1. Choose one of the links listed below to start the software download process:
    a. For computer environments that support 32Bit: https://portal.exostar.com/safenet/pkianywhere/ExostarSafeNetPKIClientX32v1.exe
    b. For computer environments that support 64Bit: https://portal.exostar.com/safenet/pkianywhere/ExostarSafeNetPKIClientX64v1.exe
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 the small arrow, show hidden icon.
- After the **SafeNet Authentication Client** is installed, the **SafeNet Setup** starts to download.

3. Click **Next** on the **Welcome to the SafeNet Wizard** screen to start the download process.
4. Click **Next** on the **Select Installation Folder** screen. We recommend you keep the pre-selected folder.
5. Click **Next** on the **Confirm Installation** screen and click **Close** on the **Installation Complete** screen.
6. Insert the token into your computer and install software components.

NOTES:

- 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.

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**.

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**.

8. Unplug the token and reinsert. After a few moments, the token is recognized.
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 password you will remember. If you forget this password, you are required to reinitialize your token and reapply for certificates, at your expense.
Default Token Password: **1234567890**

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.

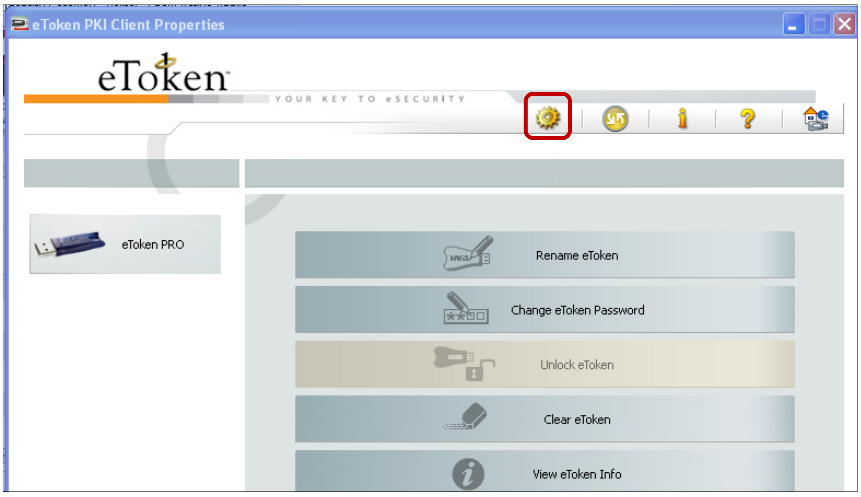
View Certificates

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

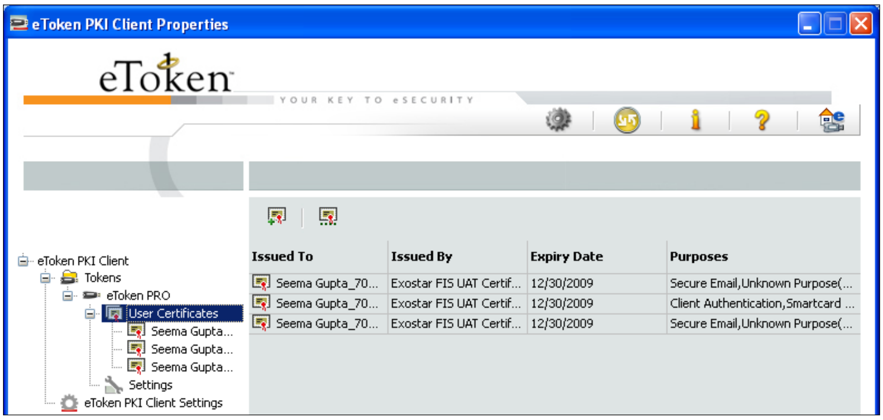
To view your certificates:

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.



Issued To	Issued By	Expiry Date	Purposes
Seema Gupta_70...	Exostar FIS UAT Certif...	12/30/2009	Secure Email,Unknown Purpose(...
Seema Gupta_70...	Exostar FIS UAT Certif...	12/30/2009	Client Authentication,Smartcard ...
Seema Gupta_70...	Exostar FIS UAT Certif...	12/30/2009	Secure Email,Unknown Purpose(...

Revoke Certificates

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

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

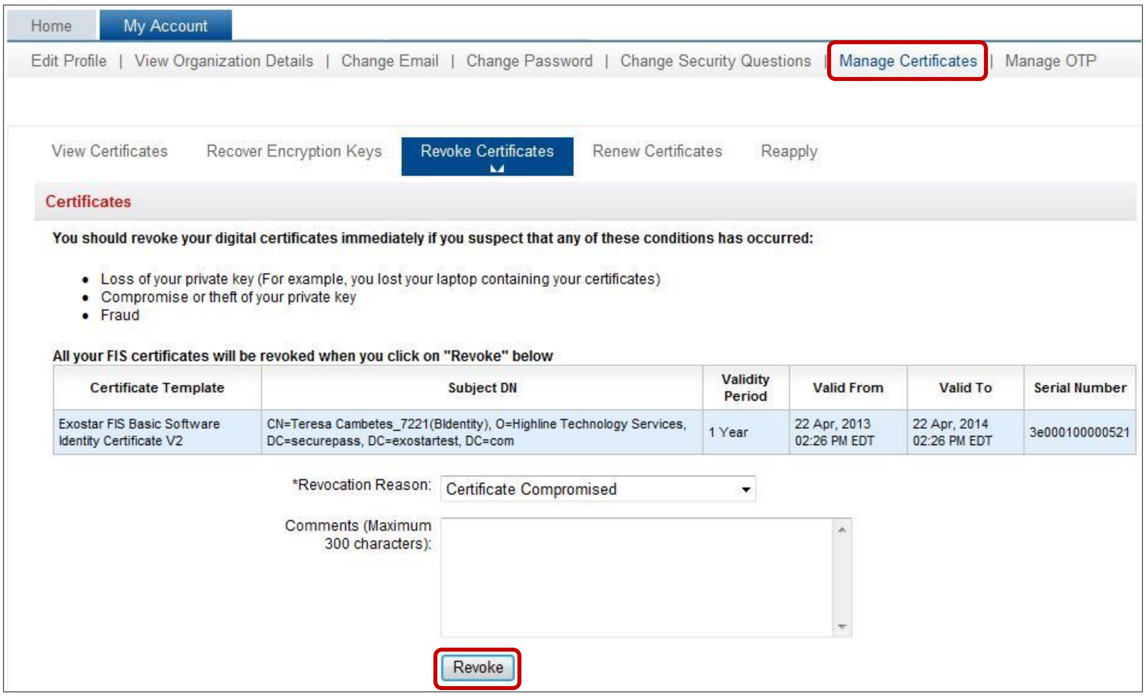
There are four ways to revoke your certificates:

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.


Home
My Account
Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP
View Certificates
Recover Encryption Keys
Revoke Certificates
Renew Certificates
Reapply
Revoke

Certificates

You should revoke your digital certificates immediately if you suspect that any of these conditions has occurred:

- Loss of your private key (For example, you lost your laptop containing your certificates)
- Compromise or theft of your private key
- Fraud

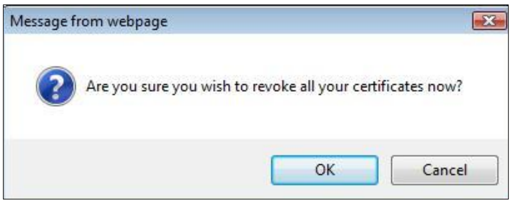
All your FIS certificates will be revoked when you click on "Revoke" below

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

*Revocation Reason: Certificate Compromised

Comments (Maximum 300 characters):

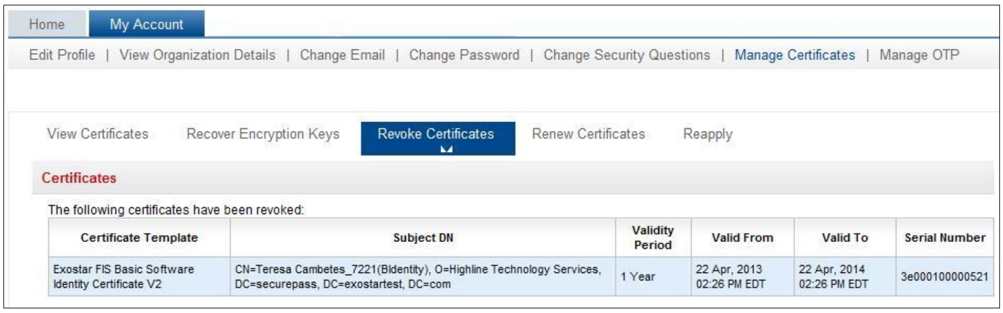
1. Click the **Revoke** button to revoke **ALL_**FIS certificates. You will receive a confirmation notification.



Message from webpage

Are you sure you wish to revoke all your certificates now?

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


Home
My Account
Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP
View Certificates
Recover Encryption Keys
Revoke Certificates
Renew Certificates
Reapply

Certificates

The following certificates have been revoked:

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

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

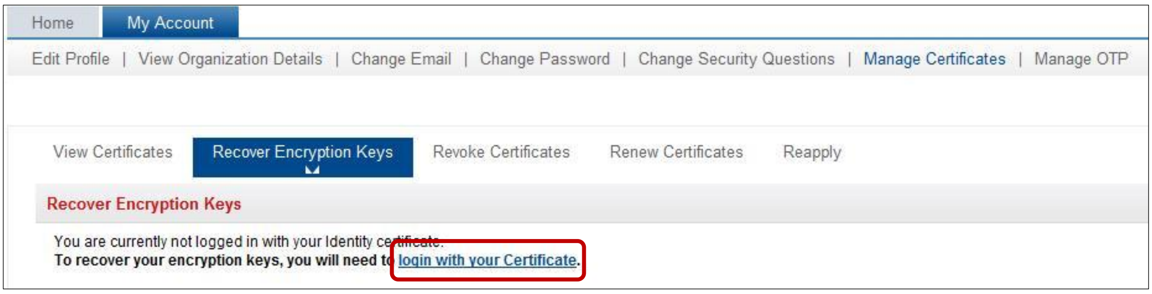
Once a user revokes or loses their MLOA certificates, they will need to re-apply for certificates, and go through the in-person proofing process again. This may also require an additional purchase. To enable users to access data encrypted using the revoked/lost certificates, Exostar offers the self-key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

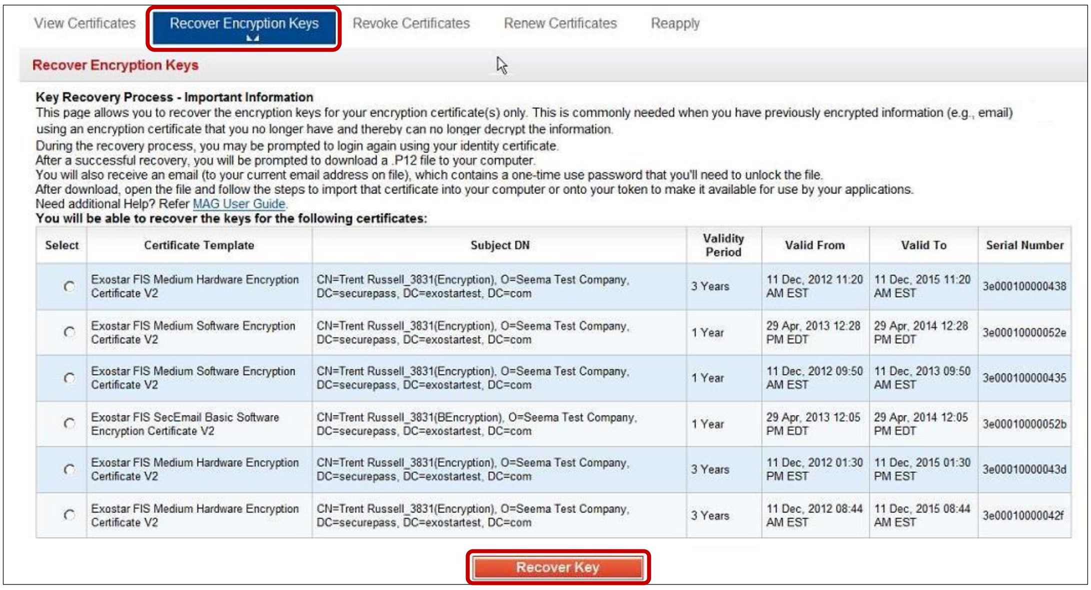
1. Login to MAG account using your new MLOA certificates. If you have not reapplied for certificates, complete all activities related to requesting access, in-person proofing, and downloading your certificates, prior to attempting to recover encryption keys.
2. The following screen displays if you have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


Home
My Account
Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP
View Certificates
Recover Encryption Keys
Revoke Certificates
Renew Certificates
Reapply

Recover Encryption Keys

You are currently not logged in with your Identity certificate.
To recover your encryption keys, you will need to login with your Certificate.

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

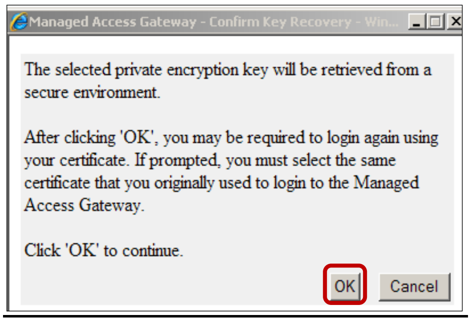


Recover Encryption Keys

Key Recovery Process - Important Information
This page allows you to recover the encryption keys for your encryption certificate(s) only. This is commonly needed when you have previously encrypted information (e.g., email) using an encryption certificate that you no longer have and thereby can no longer decrypt the information.
During the recovery process, you may be prompted to login again using your identity certificate.
After a successful recovery, you will be prompted to download a .P12 file to your computer.
You will also receive an email (to your current email address on file), which contains a one-time use password that you'll need to unlock the file.
After download, open the file and follow the steps to import that certificate into your computer or onto your token to make it available for use by your applications.
Need additional Help? Refer MAG User Guide.
You will be able to recover the keys for the following certificates:

Select	Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
○	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	3 Years	11 Dec, 2012 11:20 AM EST	11 Dec, 2015 11:20 AM EST	3e000100000438
○	Exostar FIS Medium Software Encryption Certificate V2	CN=Trent Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	1 Year	29 Apr, 2013 12:28 PM EDT	29 Apr, 2014 12:28 PM EDT	3e00010000052e
○	Exostar FIS Medium Software Encryption Certificate V2	CN=Trent Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	1 Year	11 Dec, 2012 09:50 AM EST	11 Dec, 2013 09:50 AM EST	3e000100000435
○	Exostar FIS SecEmail Basic Software Encryption Certificate V2	CN=Trent Russell_3831(BEncryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	1 Year	29 Apr, 2013 12:05 PM EDT	29 Apr, 2014 12:05 PM EDT	3e00010000052b
○	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	3 Years	11 Dec, 2012 01:30 PM EST	11 Dec, 2015 01:30 PM EST	3e00010000043d
○	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostartest, DC=com	3 Years	11 Dec, 2012 08:44 AM EST	11 Dec, 2015 08:44 AM EST	3e00010000042f

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.

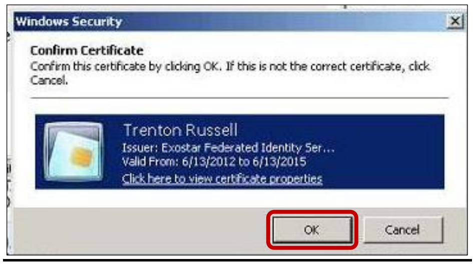


The selected private encryption key will be retrieved from a secure environment.

After clicking 'OK', you may be required to login again using your certificate. If prompted, you must select the same certificate that you originally used to login to the Managed Access Gateway.

Click 'OK' to continue.

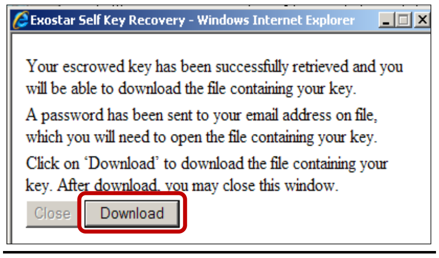
5. From the **Choose a digital certificate** pop-up screen, select the certificate you used to login.



Confirm Certificate
Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

Trenton Russell
Issuer: Exostar Federated Identity Ser...
Valid From: 6/13/2012 to 6/13/2015
Click here to view certificate properties

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**.

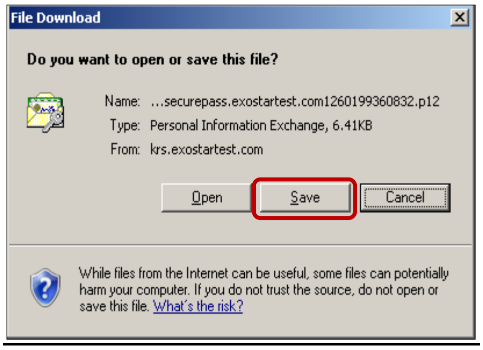


Your escrowed key has been successfully retrieved and you will be able to download the file containing your key.

A password has been sent to your email address on file, which you will need to open the file containing your key.

Click on 'Download' to download the file containing your key. After download, you may close this window.

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

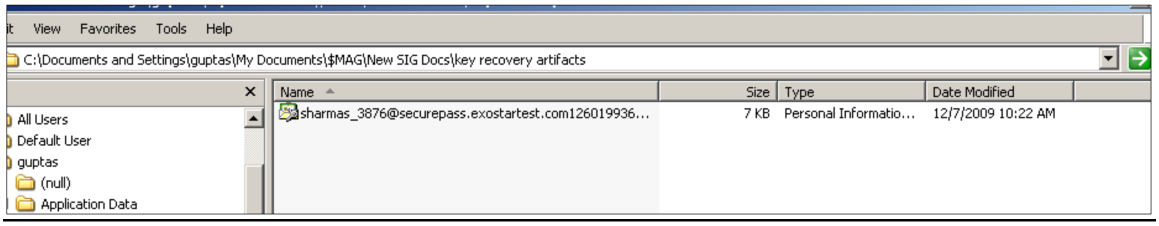


Do you want to open or save this file?

Name: ...securepass.exostartest.com1260199360832.p12
Type: Personal Information Exchange, 6.41KB
From: krs.exostartest.com

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

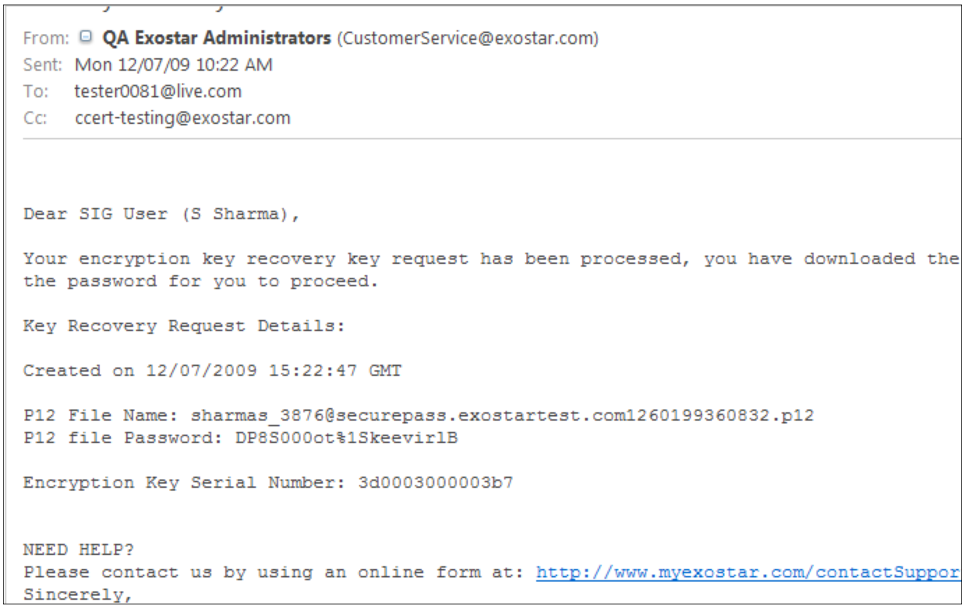
8. Save the certificate file (.p12 format) at a location of your choice. Click **Close** on the **Exostar Self Key Recovery** screen.



C:\Documents and Settings\guptas\My Documents\$MAG\New SIG Docs\key recovery artifacts

Name	Size	Type	Date Modified
sharmas_3876@securepass.exostartest.com126019936...	7 KB	Personal Informatio...	12/7/2009 10:22 AM

9. You 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.



From: QA Exostar Administrators (CustomerService@exostar.com)
Sent: Mon 12/07/09 10:22 AM
To: tester0081@live.com
Cc: ccert-testing@exostar.com

```
Dear SIG User (S Sharma),

Your encryption key recovery key request has been processed, you have downloaded the
the password for you to proceed.

Key Recovery Request Details:

Created on 12/07/2009 15:22:47 GMT

P12 File Name: sharmas_3876@securepass.exostartest.com1260199360832.p12
P12 file Password: DP8S000ot%1SkeevirlB

Encryption Key Serial Number: 3d0003000003b7


NEED HELP?
Please contact us by using an online form at: http://www.myexostar.com/contactSuppor
Sincerely,
```

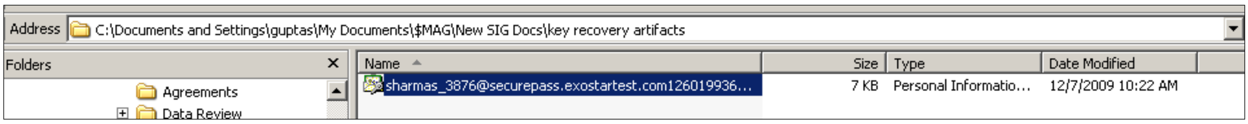
Import Recovered Encryption Keys

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:

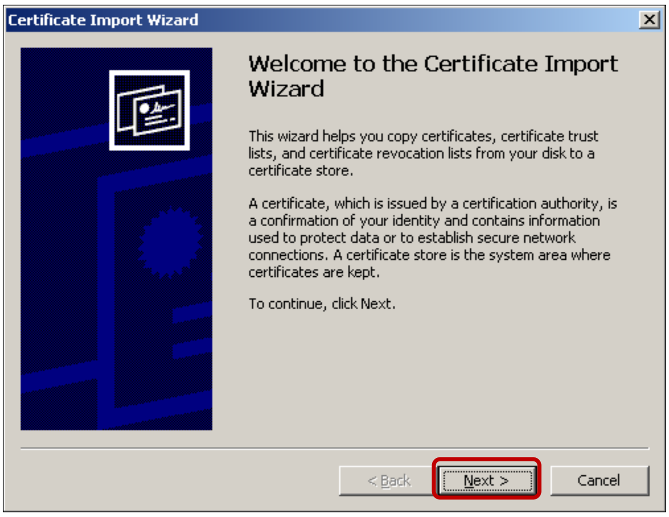
1. Double click the saved .p12 file.



Address: C:\Documents and Settings\guptas\My Documents\$MAG\New SIG Docs\key recovery artifacts

Name	Size	Type	Date Modified
sharmas_3876@securepass.exostartest.com126019936...	7 KB	Personal Informatio...	12/7/2009 10:22 AM

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



Certificate Import Wizard

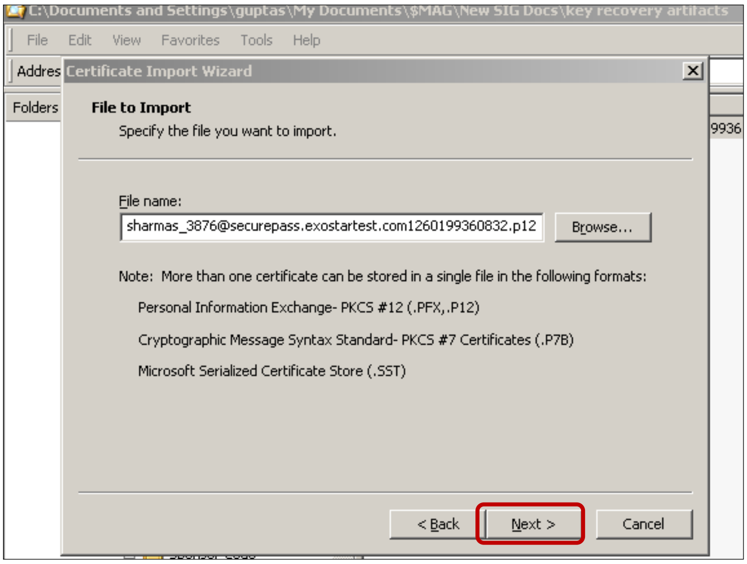
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



C:\Documents and Settings\guptas\My Documents\$MAG\New SIG Docs\key recovery artifacts

Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

sharmas_3876@securepass.exostartest.com1260199360832.p12

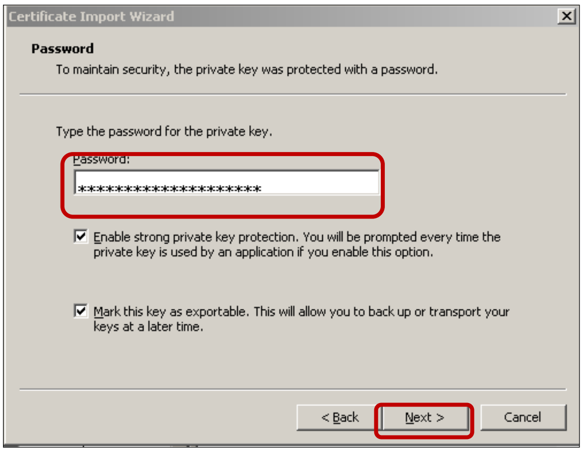
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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 set-up 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.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

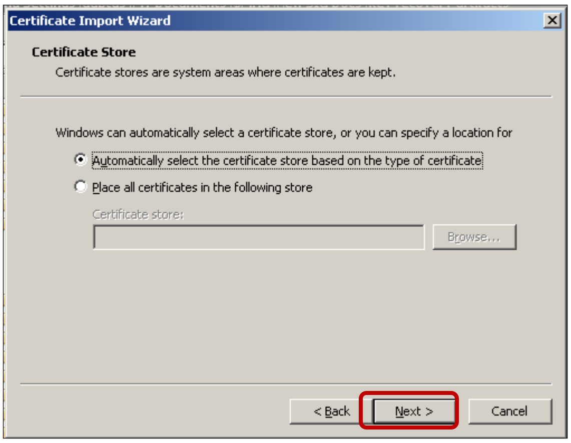
Password:

****

☑ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

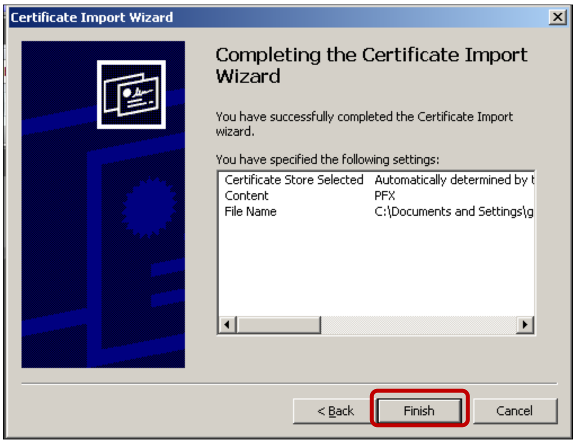
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

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



Certificate Import Wizard

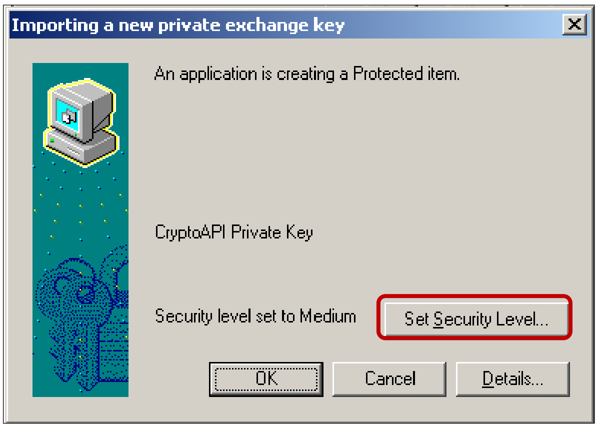
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

```
Certificate Store Selected   Automatically determined by t
Content                      PFX
File Name                    C:\Documents and Settings\g
```

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.



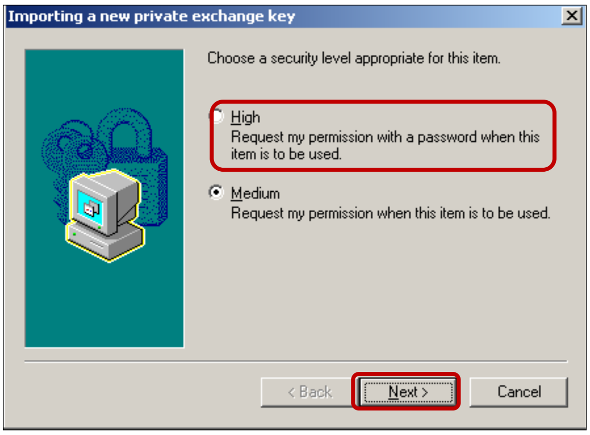
Importing a new private exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

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



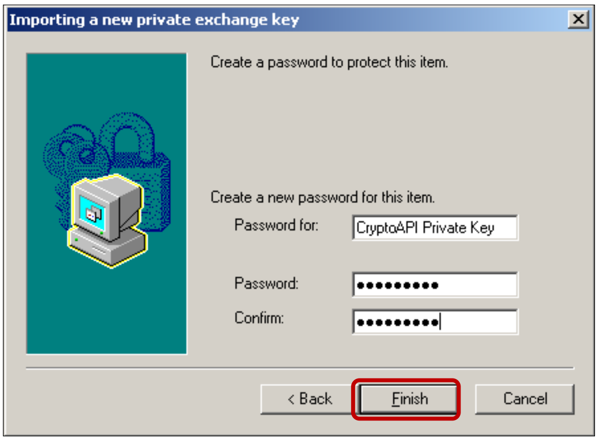
Importing a new private exchange key

Choose a security level appropriate for this item.

○ High
Request my permission with a password when this item is to be used.

● Medium
Request my permission when this item is to be used.

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



Importing a new private exchange key

Create a password to protect this item.

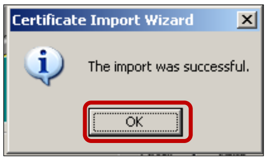
Create a new password for this item.

Password for: CryptoAPI Private Key

Password: ●●●●●●●●●

Confirm: ●●●●●●●●●

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



Certificate Import Wizard

The import was successful.

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 set-up. 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 must not reapply for certificates, unless 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, then the **Renew Certificates** tab.
3. 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. Once you are logged in, go to the **My Account** tab, **Manage Certificates/Download 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. Open an Internet Explorer browser window.
2. Click **Tools**, then **Internet Options**.
3. Click the **Content** tab and select the **Certificates** button.
4. In the Certificates pop-up screen, select the certificate you wish to remove.

5. Check the Expiration date. 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. For additional information on your organization's policies regarding certificate usage and storage, please contact your organization's IT or Security Office.

Export Certificates

Follow the steps below to export certificates:

1. Open an Internet Explorer browser window.
2. Click **Tools** and select **Internet Options.**
3. Select the **Content** tab and click the **Certificates** button.
4. On the **Certificates** dialog box, select the **Personal** tab.
5. Highlight the **Identity** certificate and click **Export**.
6. Select the **Yes, export the private key** option and click **Next**.
7. Select the **Include all certificates in the certification patch if possible,** option and click **Next**.
8. Apply a password to the certificate. Click **Next**.

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

9. Browse for a location to store your certificate. Click **Browse…** For security reasons, it is important you always maintain control of your digital certificate.
10. 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.

11. The file path is created. Click **Next**, then click **Finish**.
12. Click **OK** on the confirmation screen.

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. Open an Internet Explorer browser window.
2. Click **Tools** and select **Internet Options.**
3. Select the **Content** tab and click the **Certificates** button.
4. From the **Personal** tab, click **Import**.

5. The 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).