USERS' GUIDE

How to acquire an Associate Digital Identity Certificates from the iCA Identity Authority and Configure MAS

Introduction

This guide describes how an authorized Bank of America Associate may acquire a digital certificate (Identity Certificate) from the Enrollment web site. The certificate is used as part of the authentication process for remote access to the Bank of America network (BARONet) via Mobile Access Services (MAS).

The general steps in this process are:

1. Enroll for an Identity Certificate from the Digital Certificates web site (https://certificates.bankofamerica.com)
2. Install the certificate
3. Configure MAS to use the certificate
4. Save the certificate

This process replaces the process previously used to acquire a certificate from the Associate Key Management System (AKMS). Identity Certificates are issued by the Bank of America Internal Certificate Authority (iCA) and are for use by Bank of America Associates only.

Enrollment

The enrollment process is slightly different for the first time enrollee (an Associate with no iCA Identity Certificate) and an enrollee that wishes to replace his/her existing iCA Identity Certificate.

In order to obtain an Identity Certificate, you will need the following pieces of information:

1. Your Simplified Sign On (SSO) credentials
2. Your Person Number

If you do not know your Person Number you may obtain it by selecting the "Get Person Number" link on the Digital Certificates Home page.

To enroll for an Identity Certificate:
* Open Internet Explorer
* Go to https://certificates.bankofamerica.com

Select the "Certificate Enrollment" tab and, under "Internal Certificate Authority (ICA)", select "MAS/VPN Associate Certificates".

This will open an SSO login screen.
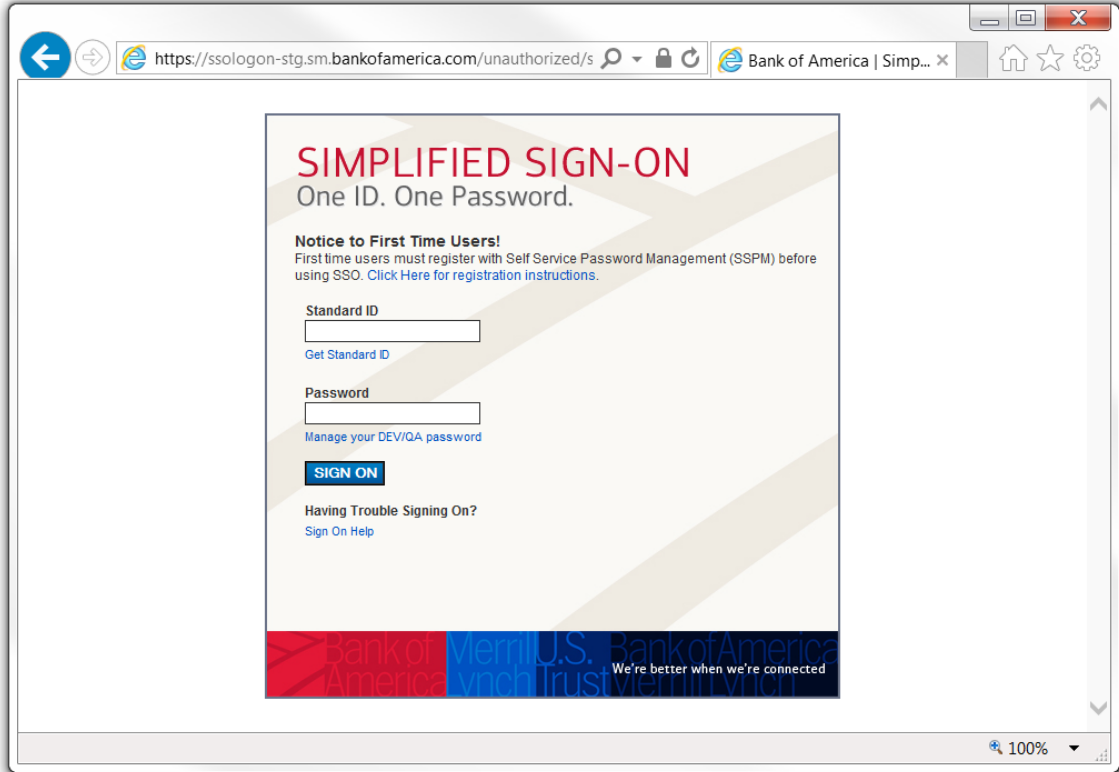
Enter your SSO credentials and click "SIGN ON". This will open the enrollment site.
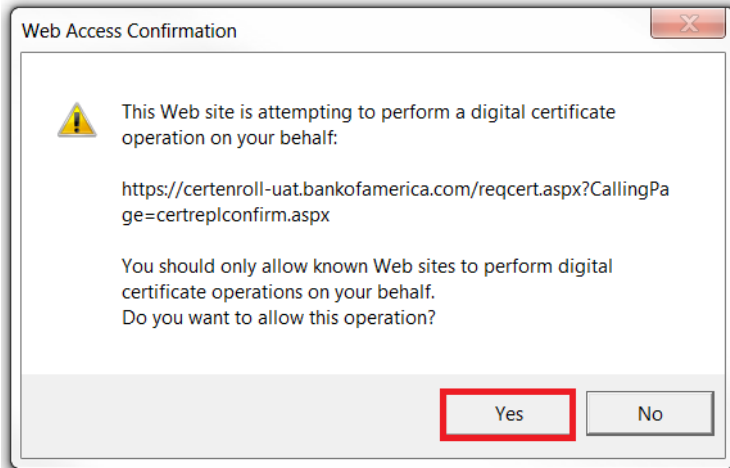
First Time Enrollment

From the iCA Certificate Enrollment site, select "Request Certificate". On the next page you will be asked for your Person Number.
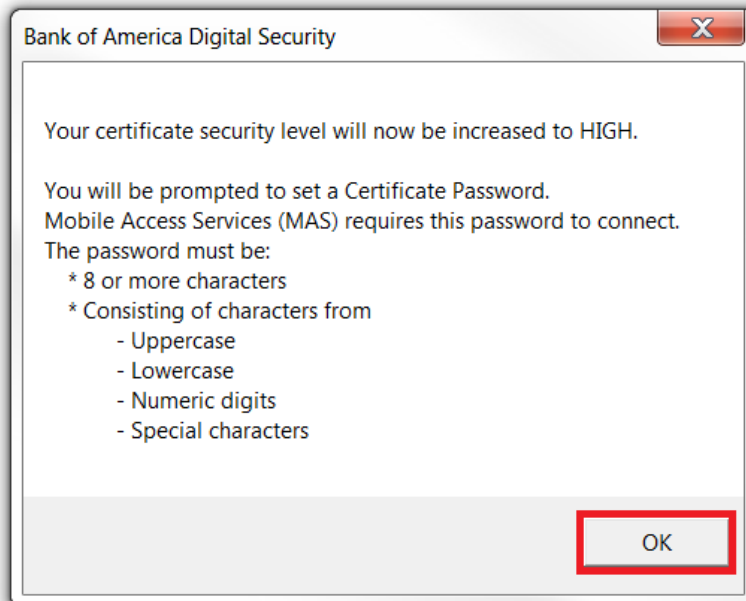
Enter your Person Number and click "submit". The web site will then generate a request for the certificate.

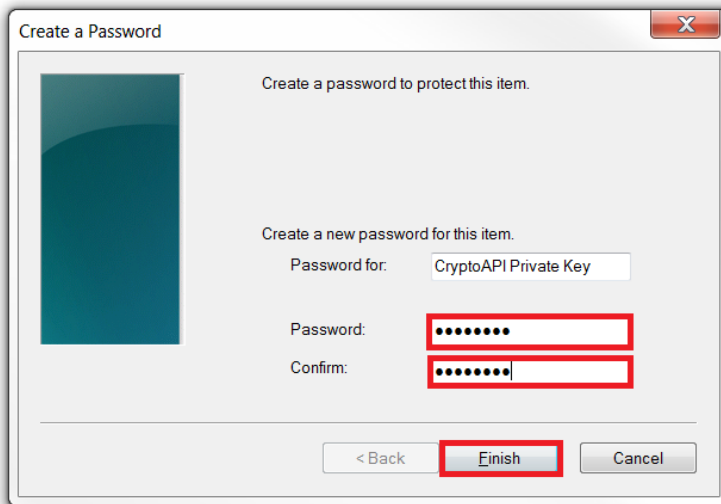If you are prompted for web access confirmation, click "Yes".

Next you will be prompted about increasing your certificate security level to HIGH such that you will be required to create a new password to protect your certificate's private key. The new password must follow the rules as described. Click "OK" to continue.
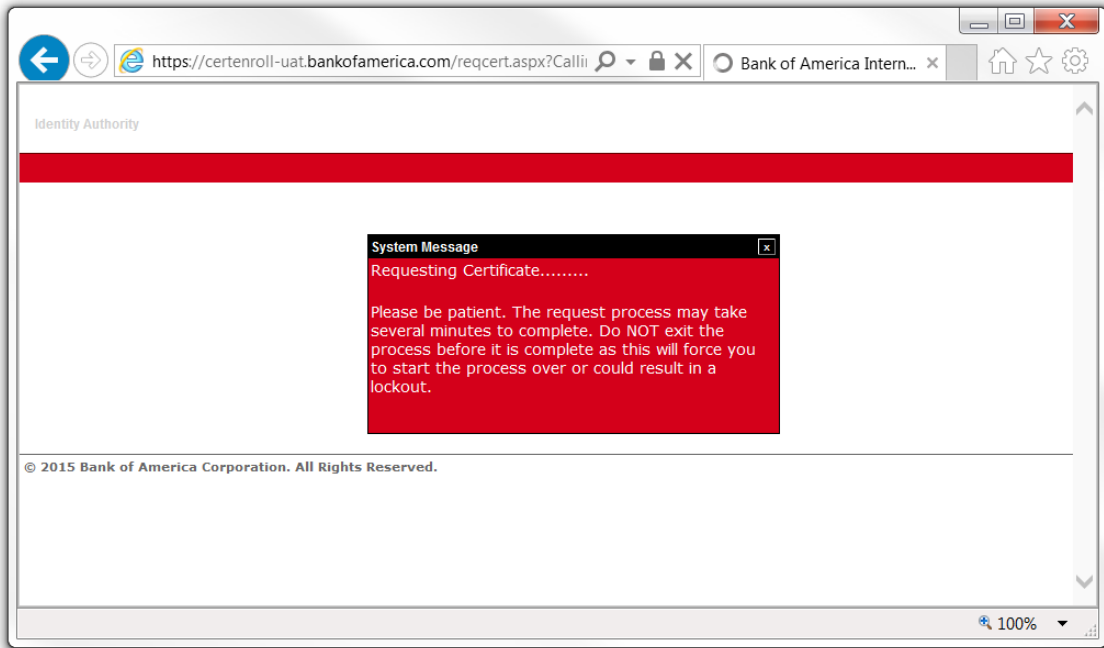
If you see the "Creating a new RSA exchange key" dialog box, click on the "Set Security Level.."


You will be shown the "Create a Password" dialog box. If your BAND machine has the latest updates, this dialog box will immediately appear on top of the "Creating a new RSA exchange key" dialog box. Enter the password twice, then click on the "Finish" button.

Once the request is completed the web site will automatically submit the request to the Certification Authority.

As soon as the Certificate Authority issues the certificate, it will be returned to the web site.
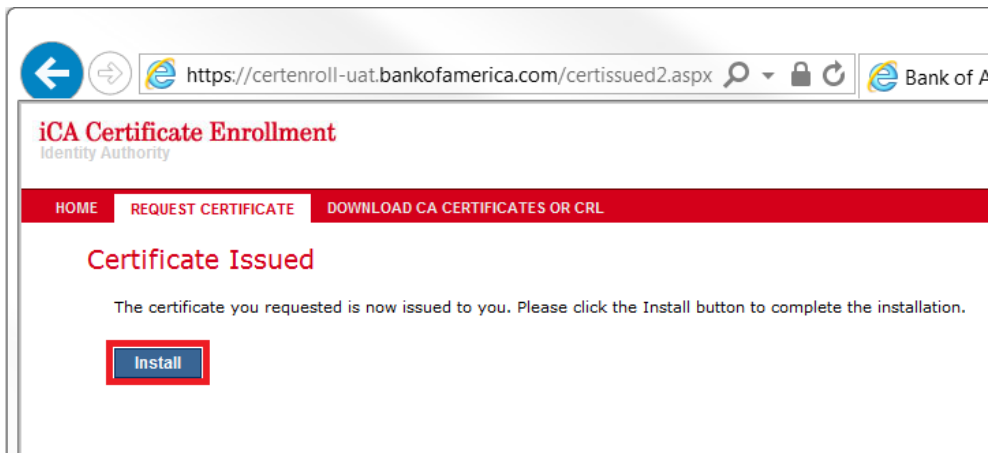
You should then select "Install" and the certificate will be automatically installed on your computer, and you will see the "Certificate successfully installed" dialog box.
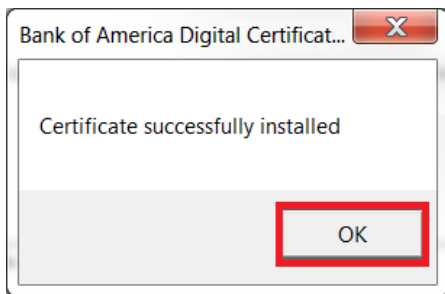
# Using the enrollment site to replace an existing iCA Identity Certificate

There are occasionally situations in which you may need to replace your iCA Identity Certificate. Typically, this will only necessary if you have forgotten the password associated with the certificate or you have lost the certificate due to a system failure.

Please note – there is a limit on the number of replacement certificate you can request within a 24 hour period. If you exceed the limit you will receive a notice instructing you to contact the Help Desk.
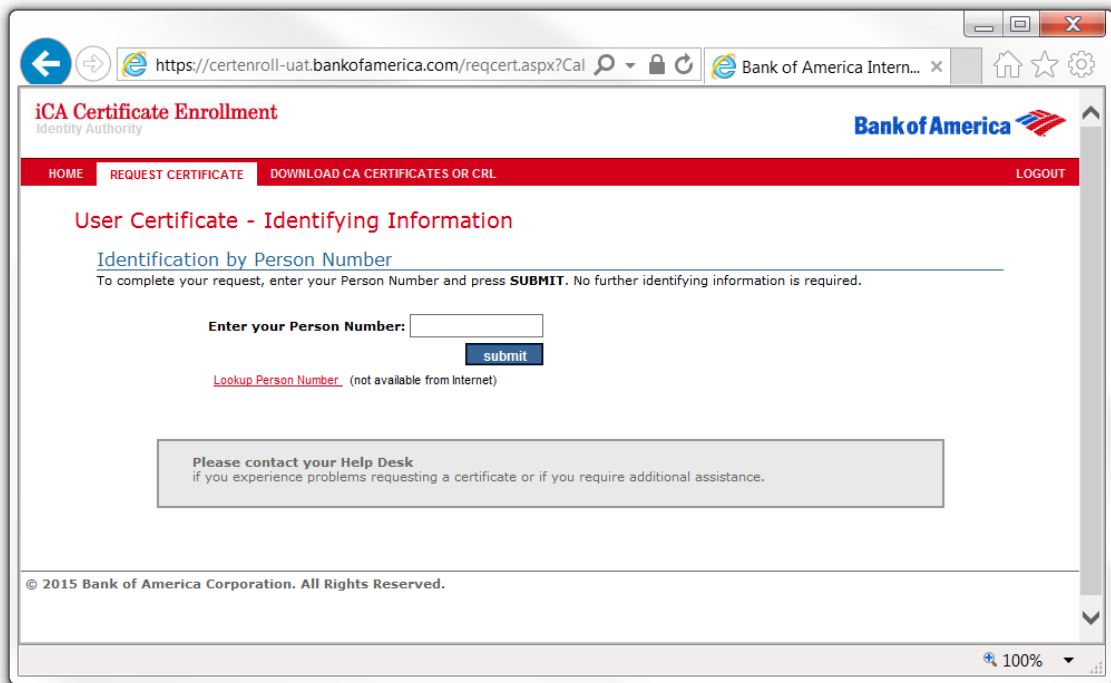
The process of obtaining a replacement certificate is almost the same as getting a certificate the first time. From the Digital Certificates Home page, select "Certificate Enrollment", then, under "Internal Certificate Authority (ICA), choose "MAS/VPN Associate Certificates", and login using your SSO credentials.
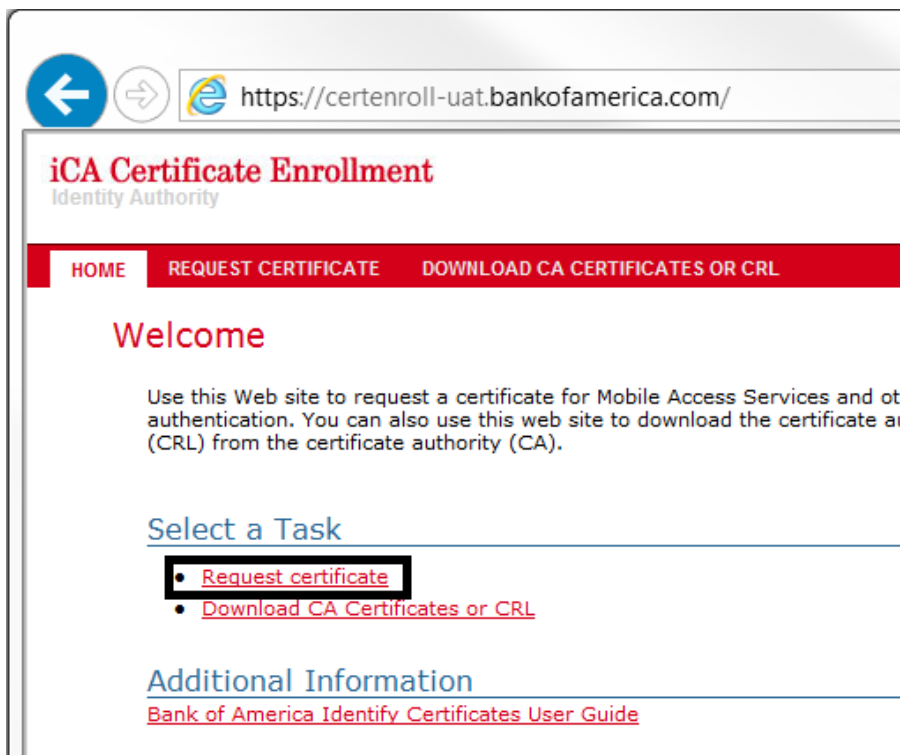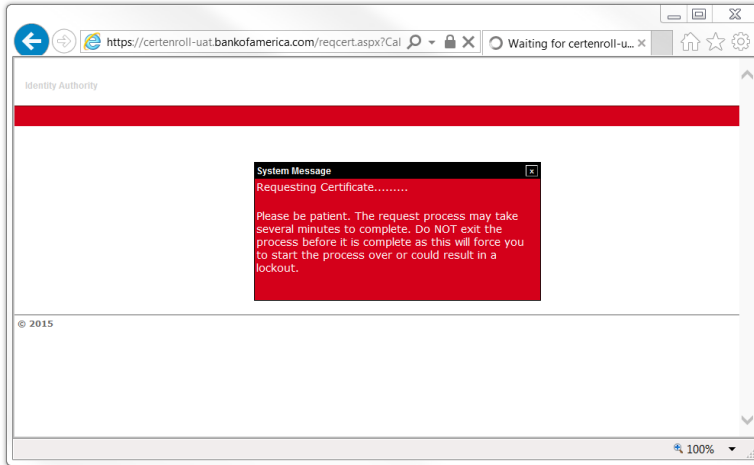

Select "Request Certificate". The web site will recognize that you already have a certificate and ask you to confirm your intention to replace it.
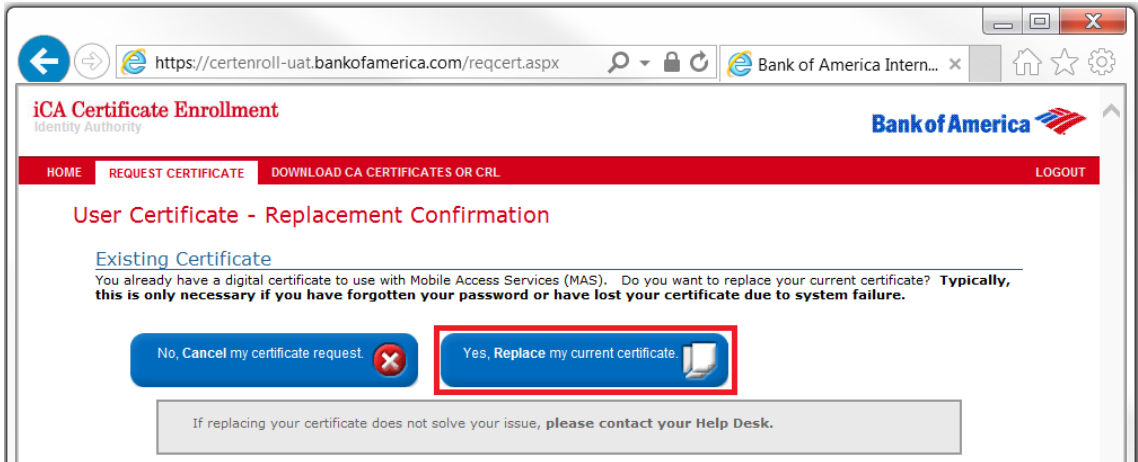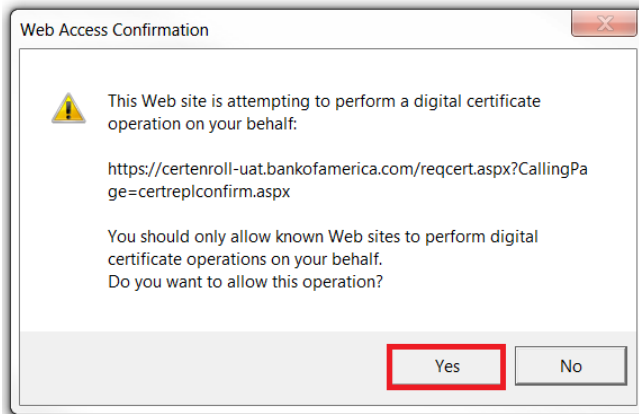
To replace your certificate, select "Yes, replace my current certificate". From this point on the process is identical to the process of obtaining a certificate the first time. On the next page you will be asked for your Person Number.
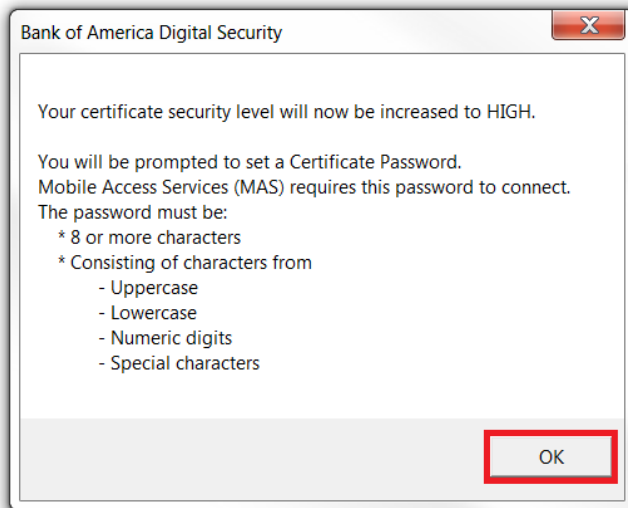

Enter your Person Number and click "submit". The web site will then generate a request for the certificate.
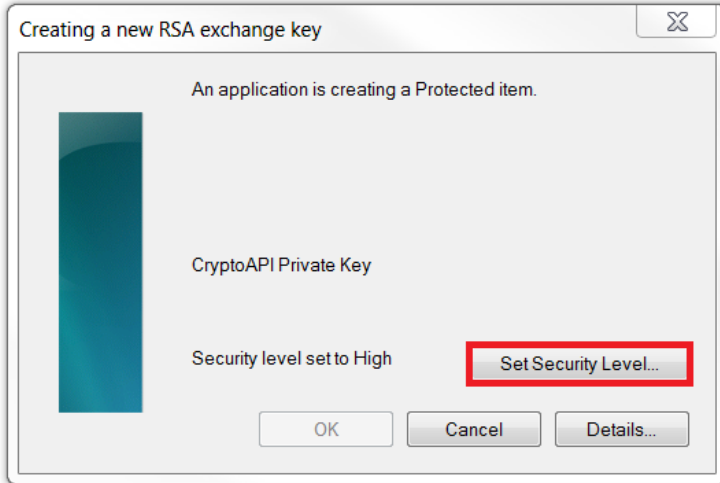
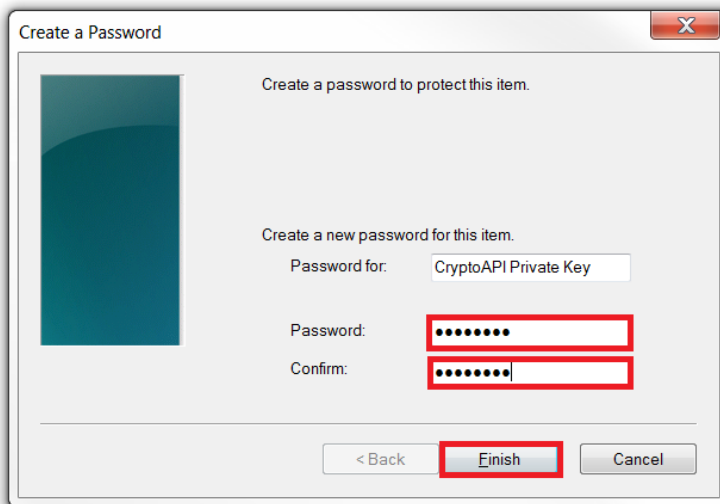If you are prompted for web access confirmation, click "Yes".

Next you will be prompted about increasing your certificate security level to HIGH such that you will be required to create a new password to protect your certificate's private key. The new password must follow the rules as described. Click "OK" to continue.
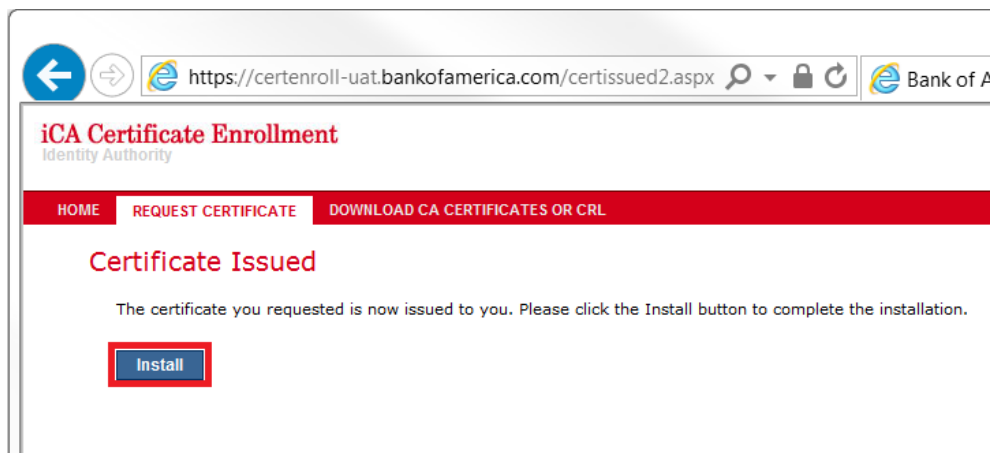
If you see the "Creating a new RSA exchange key" dialog box, click on the "Set Security Level.."

You will be shown the "Create a Password" dialog box. If your BAND machine has the latest updates, this dialog box will immediately appear on top of the "Creating a new RSA exchange key" dialog box. Enter the password twice, then click on the "Finish" button.

Once the request is completed the web site will automatically submit the request to the Certification Authority.

You should then select "Install" and the certificate will be automatically installed on your computer, and you will see the "Certificate successfully installed" dialog box.
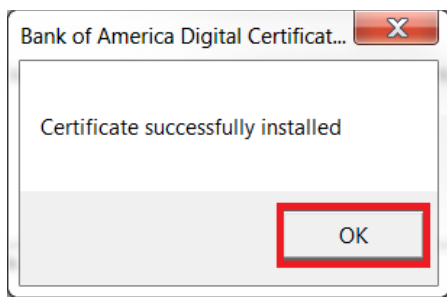
What happens if the number of replacement requests exceeds the 24 hour limit?

If your request for a replacement certificate exceeds the limit on the number of requests allowed within a 24 hour period, you will receive the following notice.
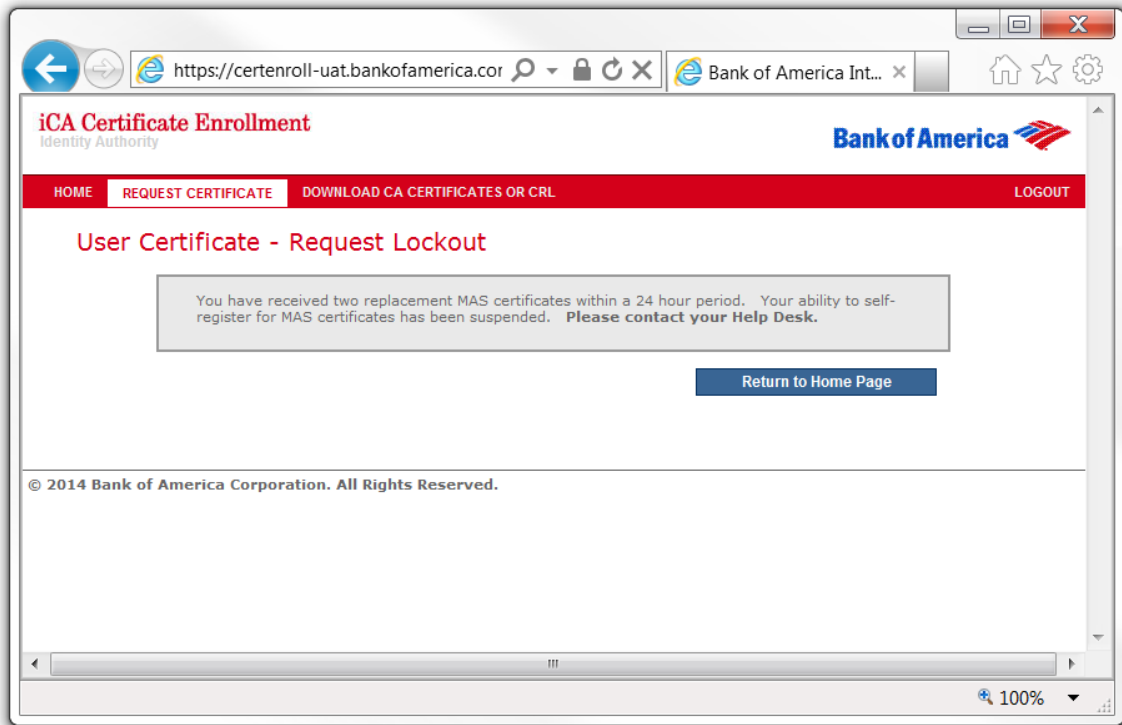
Simply follow the instruction contained in the notice.

Saving your new certificate

Note that it is recommended that you save your certificate.
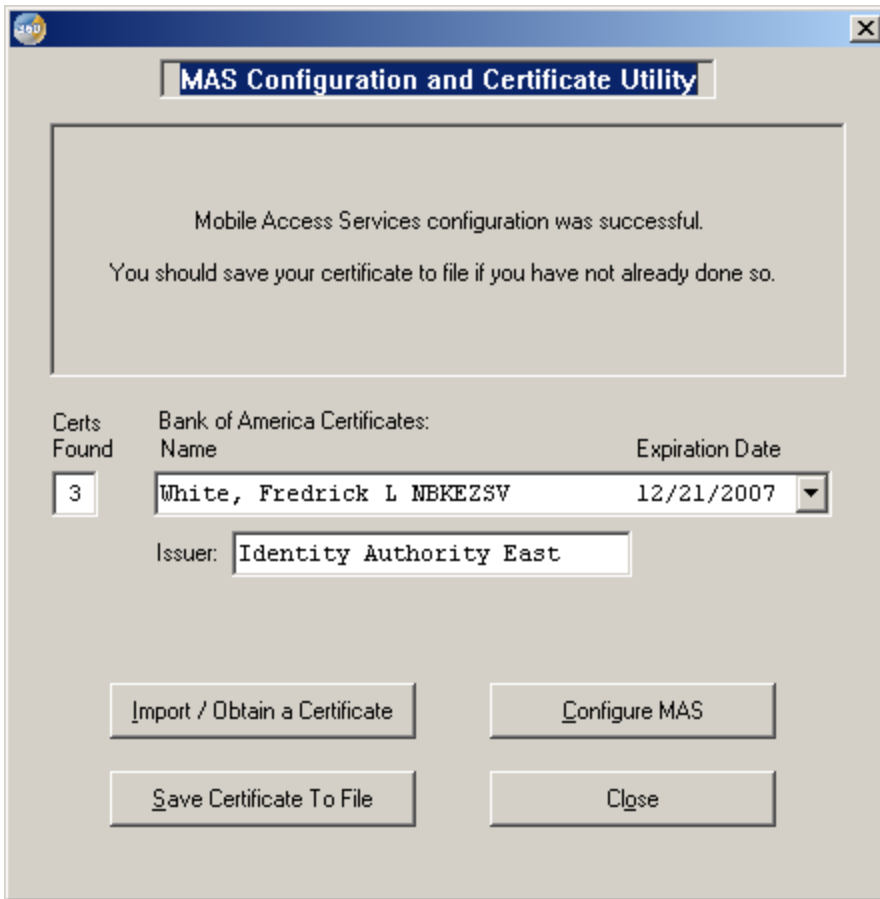
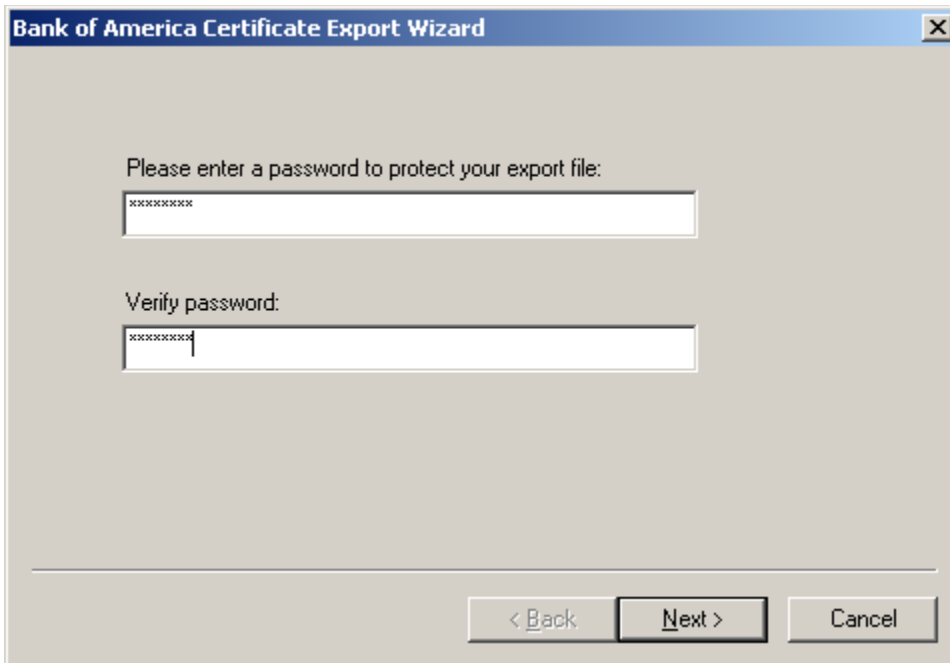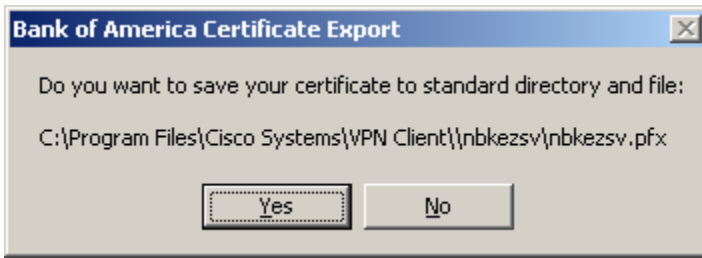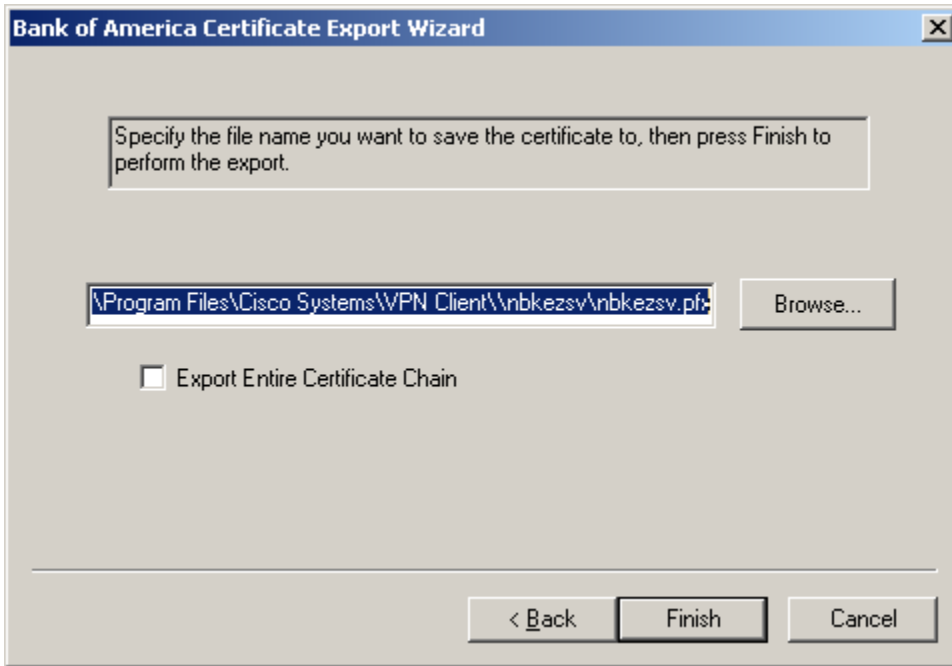To do so, select "Save Certificate to File." This will open the Export Wizard.

Enter and confirm your password. Then select "Next".

Bank of America Certificate Export

Do you want to save your certificate to standard directory and file:

C:\Program Files\Cisco Systems\VPN Client\\nbkezsv\nbkezsv.pfx

[Yes]   [No]

Please select "Yes" to save the certificate to the default location. This location has been chosen to simplify support.

Bank of America Certificate Export Wizard

Specify the file name you want to save the certificate to, then press Finish to perform the export.

\Program Files\Cisco Systems\VPN Client\\nbkezsv\nbkezsv.pfx   [Browse...]

☐ Export Entire Certificate Chain

[< Back] [Finish] [Cancel]

When you select "Finish", you will be prompted for your certificate password. Enter the password and select "OK".
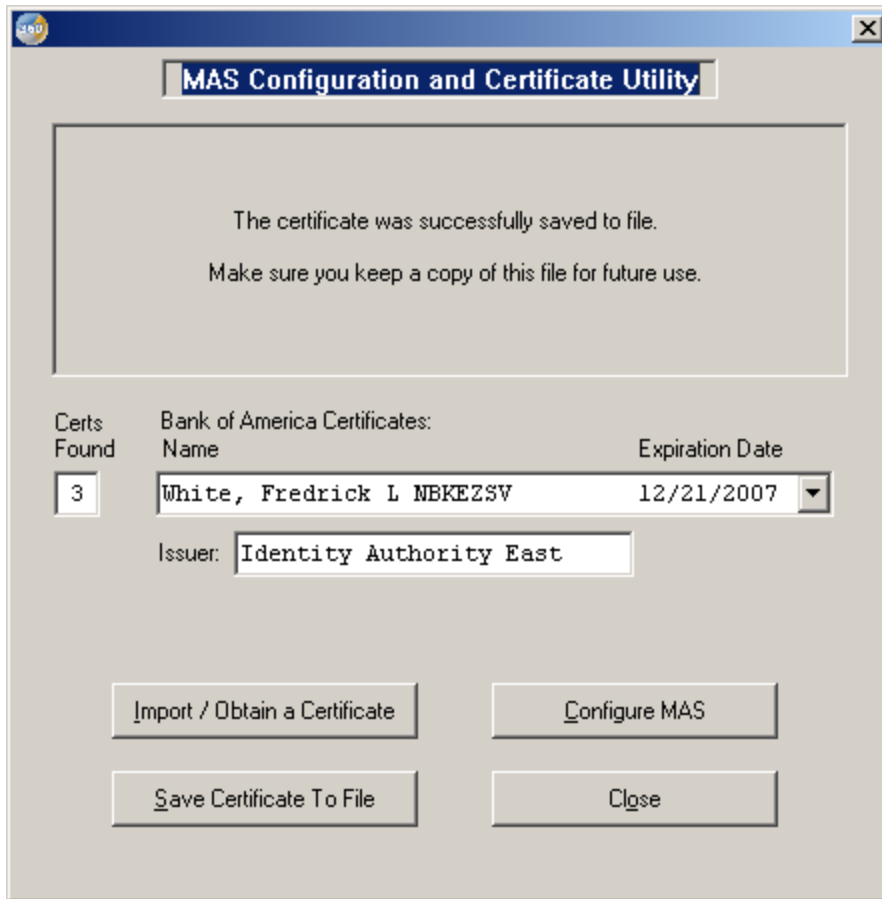
The MAS Configuration and Certificate Utility confirms that the certificate was successfully saved.

Summary

This concludes the process using the enrollment web site to acquire an iCA Identity Certificate for use with MAS. The following topics have been covered:

Enrollment – Begins at the Digital Certificates Home page. To enroll, you will need your SSO credentials and Person Number.

First Time Enrollment and using the enrollment site to replace an existing iCA Identity Certificate – These two processes are only slightly different. You should only need to replace your certificate if you have forgotten your password or if the certificate has been lost.

What happens if the number of replacement requests exceeds the 24 hour limit? – When you reach the limit on the number of replacement certificates you will be referred to the Help Desk.

Configuring MAS to use a new iCA Identity Certificate – Whenever you receive a new certificate you must use the BA Certificate Setup and Repair Wizard to configure MAS to use the certificate.

Saving your new certificate – It is recommended that you save your new certificate at the time you receive it, using the Export Wizard from the BA Certificate Setup and Repair Wizard.