



World-Class Facilities Toolkit Application – User Enrollment Guide



World-Class Facilities *beta*
MHS MILITARY HEALTH SYSTEM | U.S. Department of Defense

[Login]

Home Knowledge Center World-Class Toolkit Executive Dashboard Contact Us



World-Class Facilities

The Portfolio Planning and Management Division of the Office of the Secretary of Defense, Health Affairs is committed to delivering world-class medical facilities that support a care experience that is patient and family-centered, compassionate, convenient, equitable, safe, and always of the highest quality. This site is a place of learning and sharing for everyone involved in making this happen.

Enjoy the use of tools developed specifically for this endeavor. Learn from the vast amount of information compiled here. Post your thoughts and peruse others'.

Become a part of the World-Class movement.

The New Community Hospital, Fort Belvoir, VA. Credit: HDR Architecture, Inc.

WORLD-CLASS UPDATES **NEW!**

There is a new [repository](#) in the [Knowledge Center](#) providing materials related to World-Class Healthcare facilities. It is searchable, sortable, and all materials are accessible. All feedback and suggestions for additional materials are welcome.

NEWS

World AIDS Day Raises Awareness, Highlights Advances
Posted 1 December 2011 | 12:30 pm

Military Medical Panel Promotes Holistic Approach to Healing
Posted 11 October 2011 | 10:25 am

EVENTS

There are no events.

[Full Calendar](#)



QUICK LINKS

- [DMLSS-FM](#)
- [Health.mil](#)
- [High Performance Buildings Database](#)
- [MHS Space Planning Criteria](#)
- [PPMD Website](#)
- [U.S. Green Building Council](#)
- [Whole Building Design Guide References](#)

Categories

- [events](#)
- [Uncategorized](#)

CONNECT *(click a logo to visit connections)*



TAGS *(click a word to see related pages)*

activation Agents Architects army
asset bassett benchmarking best
practices building performance case study
characteristics checklist Clinical collaboration
community domain Engineers
leadership poe world-class

Comment Policy | External Link Disclaimer | FOIA | Site Map | Contact Us

General3
Introduction.....3
User Enrollment.....3
 System Requirements.....3
 User Enrollment Scenarios3
 User Types:5
 Department of Defense – Common Access Card (CAC) Users or5
 Department of Veterans Affairs – Personal Identity Verification (PIV) Card Users5
 Non-CAC/PIV Users.....9
Appendix-A: Obtaining VeriSign Soft-Certificate for 2-factor User Authentication..... 11

General

The World-Class Facilities Toolkit (WC-Toolkit) application implements Department of Defense (DoD) policy to adopt smart card technology department-wide. Smart card technology implementation has been led through guidance and direction of the Deputy Secretary of Defense and Public Law 106-65, National Defense Authorization Act.

The Common Access Card (CAC), Personal Identity Verification (PIV), and VeriSign External Certificate Authority (ECA) certificate will be implemented to provide personnel identification and authentication into the WC-Toolkit web application.

Introduction

On 6 May 1999, the Deputy Secretary of Defense issued a memorandum that encouraged widespread use of public key-enabled applications and provided specific guidelines for applying public key infrastructure (PKI) services throughout the Department. PKI is a set of hardware, software, people, policies, and procedures to create, manage, distribute, use, store, and revoke digital certificates. The strategy to achieve the target DoD PKI is linked to the overall DoD strategy for achieving information assurance (IA). The 12 August 2000 Deputy Secretary of Defense memorandum further defines these guidelines and supersedes the memorandum of 6 May 1999. On 10 November 1999, the Deputy Secretary of Defense directed that the CAC be used as the DoD's primary platform for the PKI authentication token. The smart card is the most feasible, cost effective technology for the authentication mechanism to support the DoD PKI and to protect its critical information.

User Enrollment

System Requirements

- Web Browser, preferably Internet Explorer 7.0 or higher
- For CAC and PIV Users, a smart card reader
- For Soft-Certificate Users, certificates are installed on the web browser
- Windows XP or Windows 7 Operating System (32 or 64-bit)

User Enrollment Scenarios

Figure 1 depicts the flow of events for New Users with CAC/PIV, Registered Users with CAC/PIV, New Users (Non-CAC/PIV), and Registered Users (Non-CAC/PIV). Choose the applicable scenario that best applies to you to help guide you through the WC-Toolkit User Enrollment process.

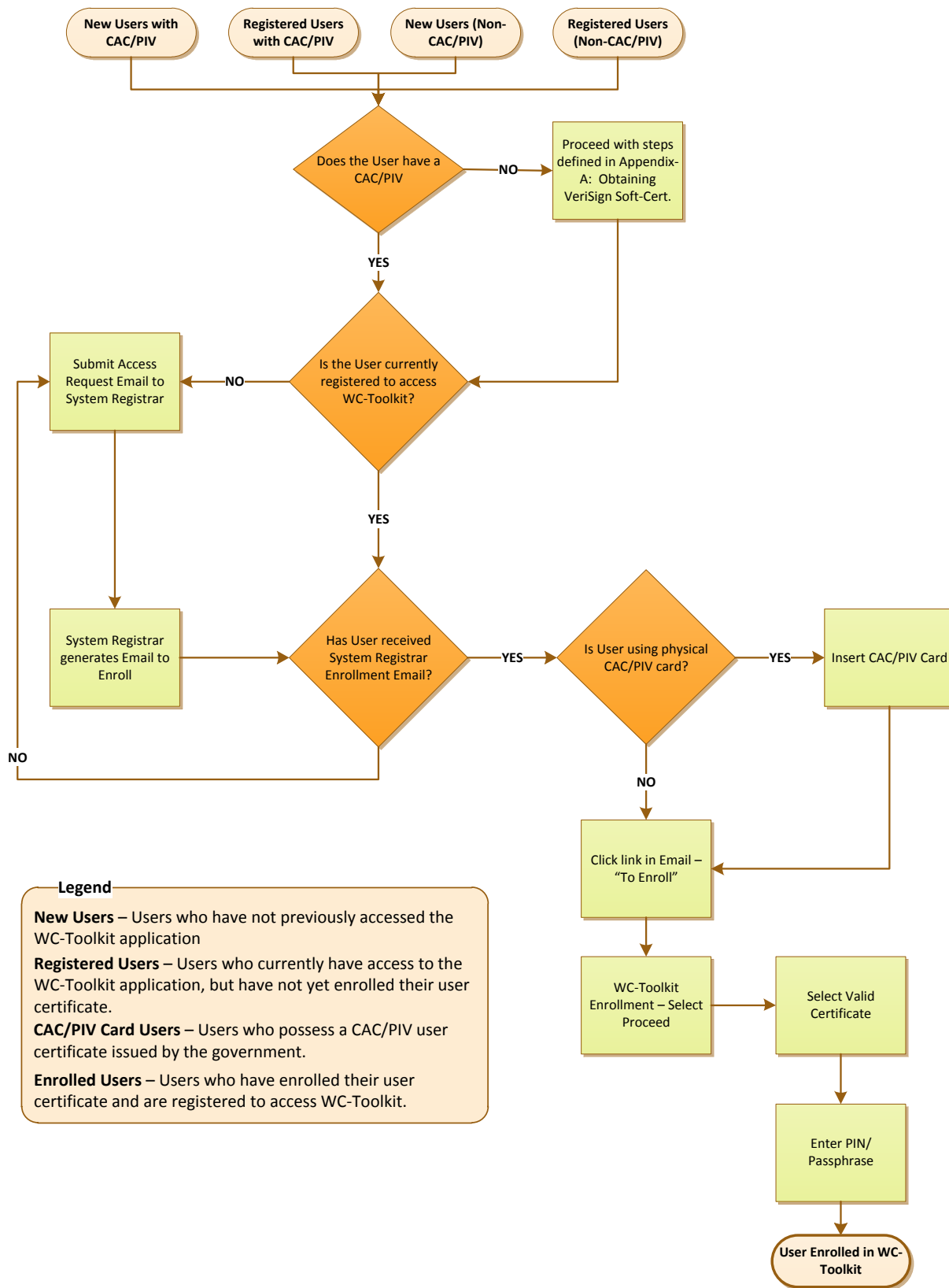


Figure 1 - User Enrollment Flowchart

User Types:

Department of Defense – Common Access Card (CAC) Users or

Department of Veterans Affairs – Personal Identity Verification (PIV) Card Users

This section describes the user enrollment for those users who have either a government issued CAC or PIV Card.

New CAC/PIV Card Users

(Users who are not currently registered to access the WC-Toolkit)

1. If you have a valid CAC or PIV Card, you can request access to this application by submitting an email with the following information to support@mhsworldclassfacilities.org:
 - a) First Name, Last Name
 - b) Email Address
 - c) Organization
 - d) Purpose for Access
2. Once you've submitted the required information, the System Registrar will send you an email with a link requesting you to register your CAC or PIV Card with the system (see Figure 2).

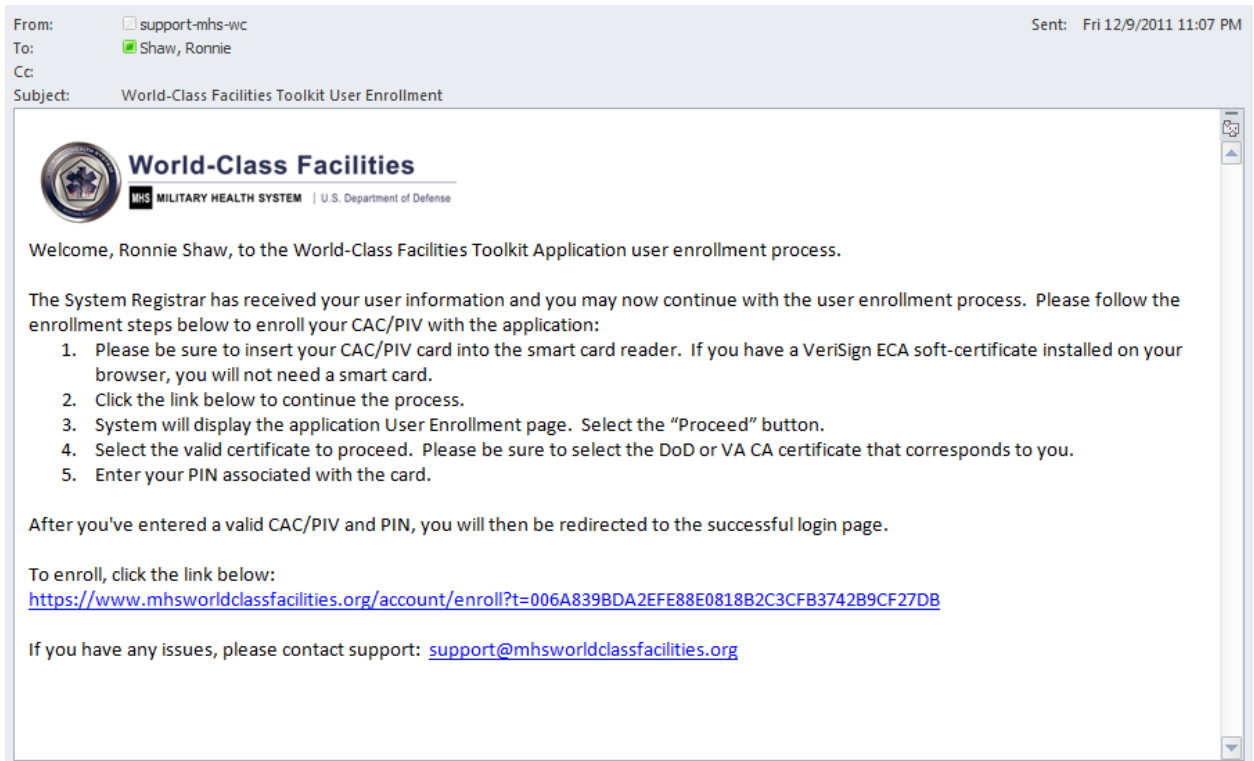


Figure 2 - User Enrollment Email

3. Insert your CAC or PIV Card into your smart card reader.
4. Click on the link in the email below the text: “To enroll, click the link below:”
5. The system will direct you to the application User Enrollment page (see Figure 3)

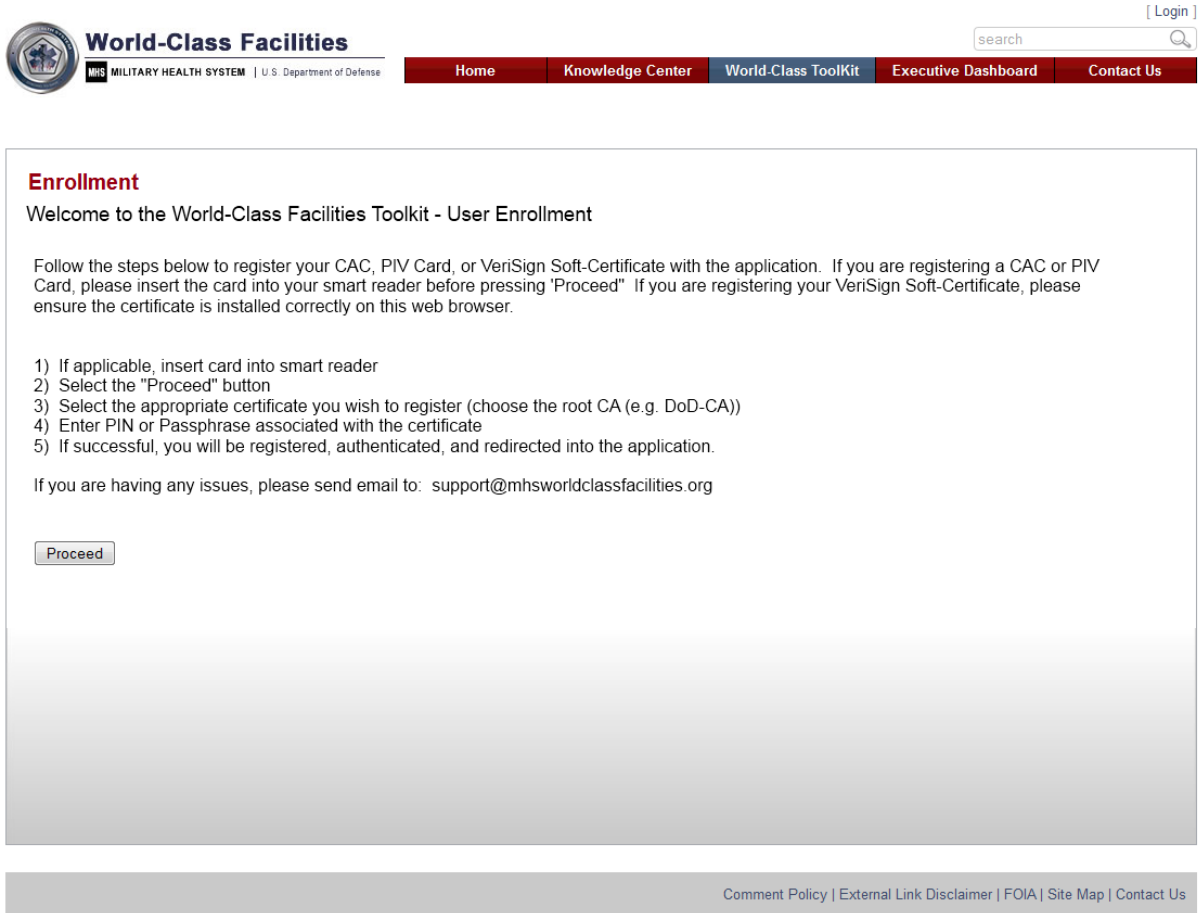


Figure 3 - User Enrollment

6. Follow the instructions on the User Enrollment page and select the “Proceed” button.
7. The system will search for valid certificates on the CAC or PIV Card and prompt you to select a valid certificate (see Figure 4)

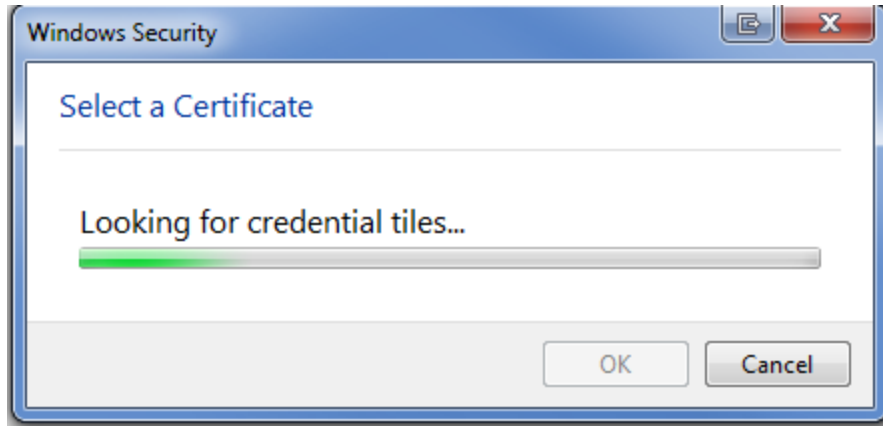


Figure 4 - Web Browser Reading Smart Card or Loading Browser Certificates

8. Select the valid CAC or PIV certificate (labeled DOD-CA) (see Figure 5)

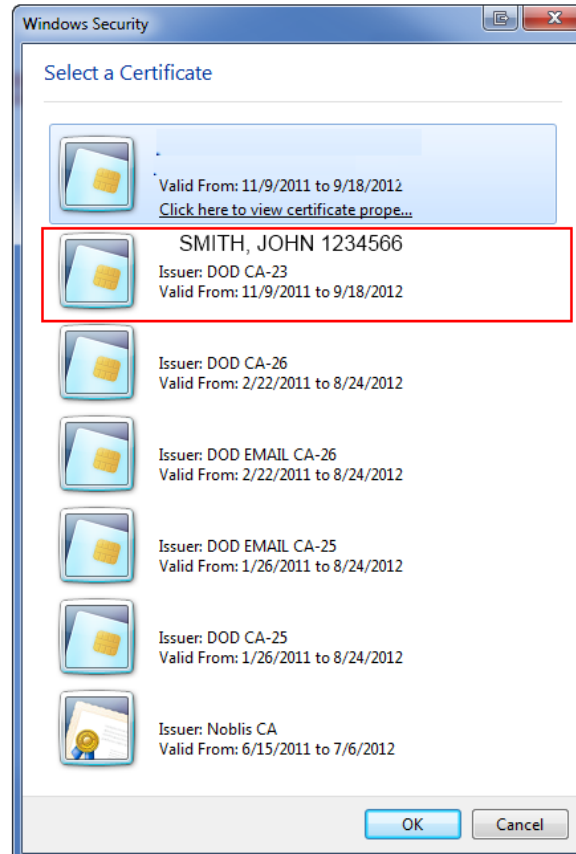


Figure 5 - User Certificate Selection

9. The system will prompt you to enter your CAC or PIV Card PIN (see Figure 6). After you've submitted valid credentials, you will be registered, authenticated, and redirected into the application.

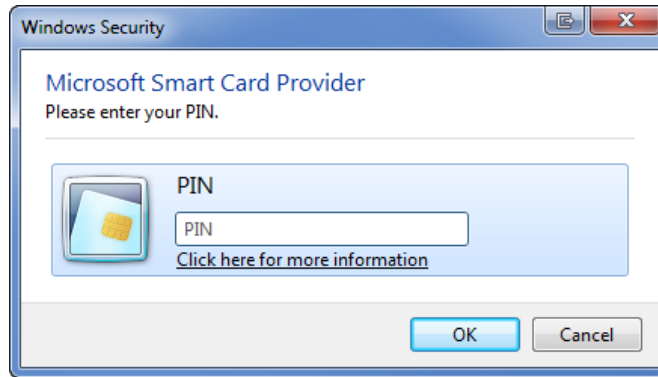


Figure 6 - User CAC/PIV Card PIN

Currently Registered Users

(Users who are currently registered but have not enrolled their CAC/PIV Card)

If you have a valid CAC or PIV Card and are already an active user in the application, you should have received an email containing a registration email from the System Registrar. If you did not, you may request another CAC or PIV Card registration email by submitting an email request to support@mhsworldclassfacilities.org.

To enroll into the WC-Toolkit, follow the instructions below:

1. After submitting an email request, the System Registrar will send you a new email containing a link requesting you register your CAC or PIV Card with the system (see Figure 2).
2. Insert your CAC/PIV Card into the smart reader
3. After selecting the link, the system will direct you to the User Enrollment page. (see Figure 3)
4. Follow the instructions on the User Enrollment Page and select "Proceed."
5. The system will then prompt you to select the valid CAC certificate and enter your CAC or PIV Card PIN (see Figures 4 & 5).
6. After you've submitted valid credentials (see Figure 5), you will be authenticated and redirected into the application.
7. You have now successfully registered your CAC/PIV Card with the application.

Non-CAC/PIV Users

This section describes the user enrollment for those users who do not have either a government issued CAC or PIV Card.

New Users

(Users who do not have CAC or PIV Card issued by the government)

If you have neither CAC nor PIV card, you will need to purchase a VeriSign soft-certificate to access this application. See Appendix-A for instructions on purchasing this soft-certificate.

Once you've received and installed the VeriSign soft-certificate, you can request access to this application by submitting an email with the following information to support@mhsworldclassfacilities.org:

1. First Name, Last Name
2. Email Address
3. Organization
4. Purpose for Access

To enroll into the WC-Toolkit, follow the instructions below:

1. After submitting an email request, the System Registrar will send you a new email containing a link requesting you register your VeriSign soft-certificate with the system (see Figure 2).
2. After selecting the link, the system will direct you to the User Enrollment page. (see Figure 3)
3. Follow the instructions on the User Enrollment Page and select "Proceed."
4. The system will then prompt you to select the valid soft-certificate (see Figures 4 & 5 as examples).
5. After you've submitted the valid passphrase, you will be authenticated and redirected into the application.
6. You have now successfully registered your soft-certificate with the application.

Currently Registered Users

(Users who are currently registered but have not enrolled their VeriSign Soft-Certificate)

If you have neither CAC nor PIV card, you will need to purchase a VeriSign soft-certificate to access this application. See Appendix-A for instructions on purchasing this soft-certificate.

If you are already an active user in the application, you should have received an email containing a user registration email from the System Registrar. If you did not, you may request another VeriSign soft-certificate registration email by submitting an email request to support@mhsworldclassfacilities.org.

To enroll into the WC-Toolkit, follow the instructions below:

1. After submitting an email request, the System Registrar will send you a new email containing a link requesting you register your VeriSign soft-certificate with the system (see Figure 2).
2. After selecting the link, the system will direct you to the User Enrollment page. (see Figure 3)
3. Follow the instructions on the User Enrollment Page and select "Proceed."
4. The system will then prompt you to select the valid soft-certificate (see Figures 4 &5 as examples).
5. After you've submitted the valid passphrase, you will be authenticated and redirected into the application.
6. You have now successfully registered your soft-certificate with the application.

Appendix-A: Obtaining VeriSign Soft-Certificate for 2-factor User Authentication

- 1) Using a web-browser, go to VeriSign External Certificate Authority (ECA)
<https://eca.verisign.com>
- 2) Select ECA Certificate Enrollment (<https://eca.verisign.com/enrollintro.htm>)
- 3) Review the ECA Certificate steps and print the page.
- 4) Select Continue
- 5) Enter your information and preferred Enrollment Method (Notary or Trusted Agent)
 - a. If you know your Organization's Trusted Agent, select that enrollment method
 - b. Otherwise, choose Notary
- 6) Select Certificate Validity (1-year \$119, 2-year \$218, 3-year \$299)
- 7) Enter Payment Type
- 8) Enter Challenge Password
- 9) Select Accept & Purchase
- 10) Follow Instructions for Printing Notarize Form
- 11) Follow the instructions to install the VeriSign CA Root and Intermediate Certificates on the machine you wish to access the World-Class Facilities Toolkit Application
- 12) Bring the Subscriber Enrollment Form to your notary or Trusted Agent
 - a. **Provide all the following forms of identification** to the notary, Trusted Agent, U.S. consular officer, or authorized DoD employee:
 - i. One government-issued photo ID for proof of identity, such as a driver's license, passport, or military ID.
 - ii. One document for proof of citizenship, such as a passport, certified birth certificate, or certificate of naturalization or citizenship.
 - iii. One document for proof of organizational affiliation (if any), such as a valid employee ID that must include a photograph and identify organizational affiliation.
 - b. In the presence of the notary, Trusted Agent, U.S. consular officer, or authorized DOD employee, sign your name in the "Subscriber Information" section.
 - i. Note: You are responsible for any fees that may be charged by the notary.
 - c. Ask the notary to read the instructions and complete the acknowledgement.
- 13) Bring the Subscriber Enrollment Form to your organizational representative (e.g. Human Resources Department) to complete and sign the "Subscriber's Organizational Contact" section to provide the **organization's DUNS number** (Dun and Bradstreet number). If your organizational representative has not provided a DUNS number or your company does not have a DUNS number, you must provide other appropriate proof of organization information to VeriSign along with your Subscriber Enrollment Form.

- 14) Once you have completed the original notarized copy of the Subscriber Enrollment Form, mail the documentation to VeriSign.
 - a. If enrollment method was Subscriber Enrollment Form using Notary
 - i. Mail documentation to:
Symantec Corporation
Attention: Enterprise Authentication Team
350 Ellis Street
Mountain View, California 94043
 - b. If enrollment method was Subscriber Enrollment Form using Trusted Agent
 - i. Trusted Agent or authorized DoD employee will verify your enrollment request and forward it to VeriSign.
- 15) Await your ECA Certificate approval email (5-8 business days)
 - a. When VeriSign completes authenticating and processing your ECA Certificate request, you will receive an email with instructions for picking up your ECA Identity and Encryption Certificates. If your ECA Certificate request is not approved, VeriSign will notify you, and you will not be billed.