Service Information

Audi Truth in Engineering

Offboard Diagnostic Information System Service (ODIS Service) **Number: AOS-17-07**

Subject: Security Certificate Renewal Instructions **Date: Feb. 27, 2017**

Supersedes AOS-17-01 due to updated and additional information.

Table of Contents

1.0 - Introduction

ODIS Service security certificates expire three years after creation. A certificate renewal prompt appears at two months, and then one month etc. before expiration. Use the following procedures to **renew a certificate before its expiration date.**

Notes:

- *Please **read these instructions carefully and in their entirety** before performing the procedures. **If you do not understand these instructions, arrange to have a qualified person perform the procedures.***
- *This document may be revised at any time. Always check ServiceNet for the latest version.*

IMPORTANT:

These instructions are based on the ***Installation Phase 1 – Preparation, License & Certificate Process Instructions*** where the **certificate** and a **text document** with the device **hardware key** are **stored in a folder on the device desktop,** and a back-up copy of the certificate etc. are **stored on a USB flash drive.**

If alternate storage and backup locations were used, determine them NOW.

2.0 – Certificate File Management

2.1 – Preparation – MUST READ!

Effective February 26, 2017, authorized dealership personnel are responsible for requesting **and approving** ODIS Service security certificate requests for new and soon-to-expire certificates.

Security is achieved through **dealership management** approval of certificate requests, and a function where **request "approvers" cannot be the same as the "requestor".**

While anyone with eCRMS access can request a certificate, request **approvers** are restricted to **dealership managers** with the following job titles and **Unified Dealer Extranet (UDE – accessaudi access)** roles:

- Dealer Principal (DLR-PRIN)
- Dealer Principal/General Manager (DLR-PRGM)
- General Manager (GEN-MGR)
- Service Director (SVC-DIR)
- Service Manager (SV-SM)
- Parts & Service Manager (PTSV-MGR)

Access to eCRMS on accessaudi must be granted by the dealership Systems Administrator.

Prerequisites:

- ☐ **The Requestor** *must be aware of a dealership manager that can approve requests.*
- ☐ **The Approver** *must be a* **dealership manager as defined above**, *and have eCRMS access.*
- ☐ *Location of all* ***storage and backup copies*** *of the device's existing certificate are known.*
- ☐ *The diagnostic device's* **hardware key** *and assigned* **device ID** *are known.*
- ☐ *Diagnostic device is plugged in to power adapter and booted to Windows desktop. USB mouse and keyboard connected to tablet.*

2.2 – Delete Existing Certificates

When an active certificate is renewed prior to expiration, it is revoked and no longer valid. Avoid inadvertent re-importation of a revoked certificate by **deleting all stored and backup copies of the certificate before renewal.**

2.2.1 – Delete Stored and Backup Copies

1. Locate and **delete all stored and backup copies** of the device's existing certificate, e.g.: desktop folder, USB flash drive etc.

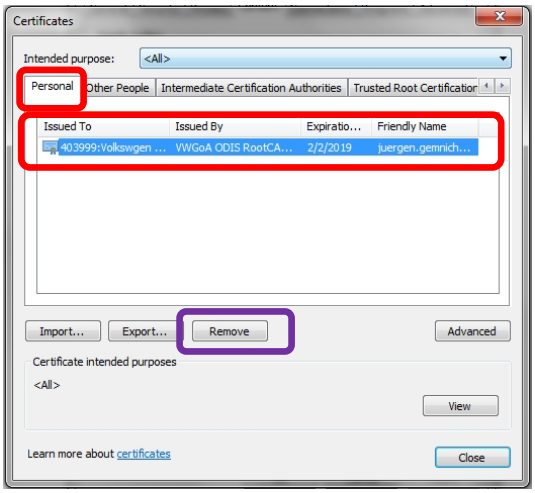
2.2.2 – Delete Certificate from Windows®

1. Launch **Internet Explorer**.
2. Press/hold the **Alt + X** keys, and then select **Internet Options** from the dropdown menu.

(cont.)

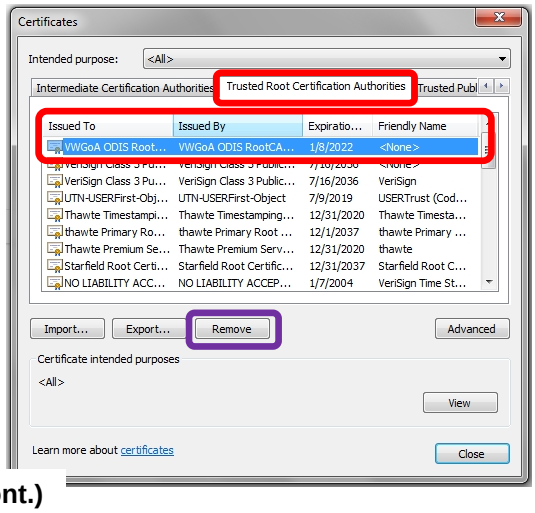
3. Select the **Content** tab, and then select the **Certificates** subcategory:

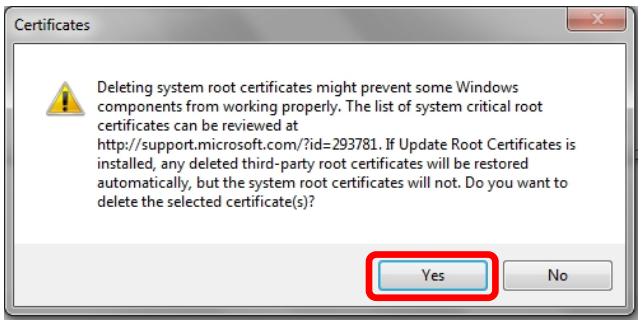
4. From the **Personal** subcategory, confirm the **VWGoA ODIS RootCA…** certificate is automatically highlighted as illustrated, and then select **Remove . . . . Yes**:



5. Select the **Trusted Root Certification Authorities** subcategory tab, and then click the **Issued By** column header to sort the certificates in reverse alphabetical order: (The **VWGoA ODIS RootCA…** certificate is automatically highlighted as illustrated below.)

6. Select **Remove . . . . Yes,** and then close all open windows:

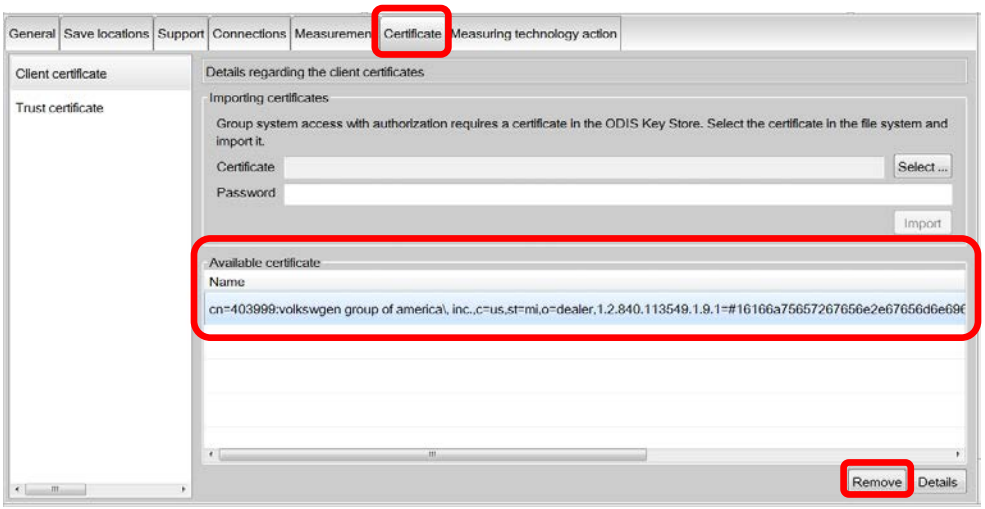


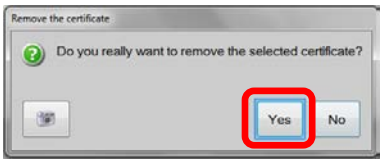


(cont.)

2.2.3 – Delete Certificate from ODIS Service

1. Start ODIS Service, and then select the **Admin** operating mode and **Certificate** subcategory:
2. Select /highlight the **Available certificate** as illustrated, and then select **Remove /Yes:**





3. **Close** ODIS Service.

2.3 – Request Security Certificate (eCRMS)

Prerequisites

- ☐ ***All stored and backup copies of the existing certificate are deleted.***
- ☐ *Text document with the device's **hardware key** must be on hand.*

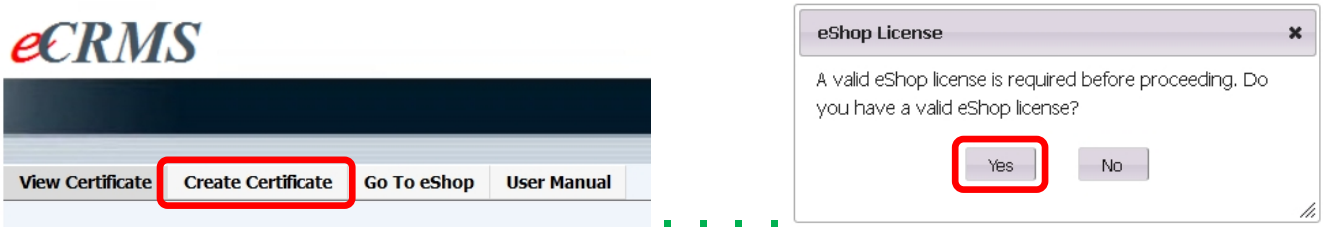
Notes:

- *The diagnostic device's **hardware key** must be **copied electronically** from the text document (not manually-typed) into the request form.*
- *As per the **Phase 1** initial installation instructions, the hardware key should be located in a text document stored in a folder on the device desktop, and backed-up on a USB flash drive.*

1. **Start Internet Explorer**
2. Logon to **accessaudi.**
3. Go to: **App Links > Service**, and select the link to **ODIS Certificate Request Mgmt. System (*eCRMS*).**

(cont.)

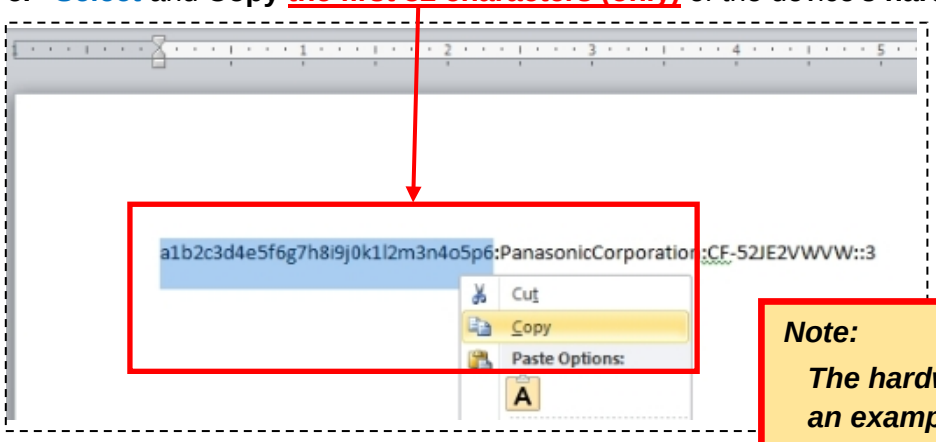
4. Select **Create Certificate . . . . Yes:**



The *eCRMS* request interface appears.

Information must be entered in all request interface fields marked with an asterisk (*)

5. **Enter /confirm all** applicable information required in the **Dealer/Site Information** and **Contact Information** sections.
6. **Enter** the **diagnostic device** information in the **Device Information** section as follows:
   a. **Minimize** the eCRMS browser session.
   b. Navigate to the **device folder** on the Windows desktop (or other location) and **Open** the **Hardware Key** text document:
   c. **Select** and **Copy** **the first 32 characters (only)** of the device's **hardware key.** Example:



Note:

The hardware key illustrated here is an example only. All hardware keys are different!

The characters are saved in Windows "clipboard" memory.

(cont.)

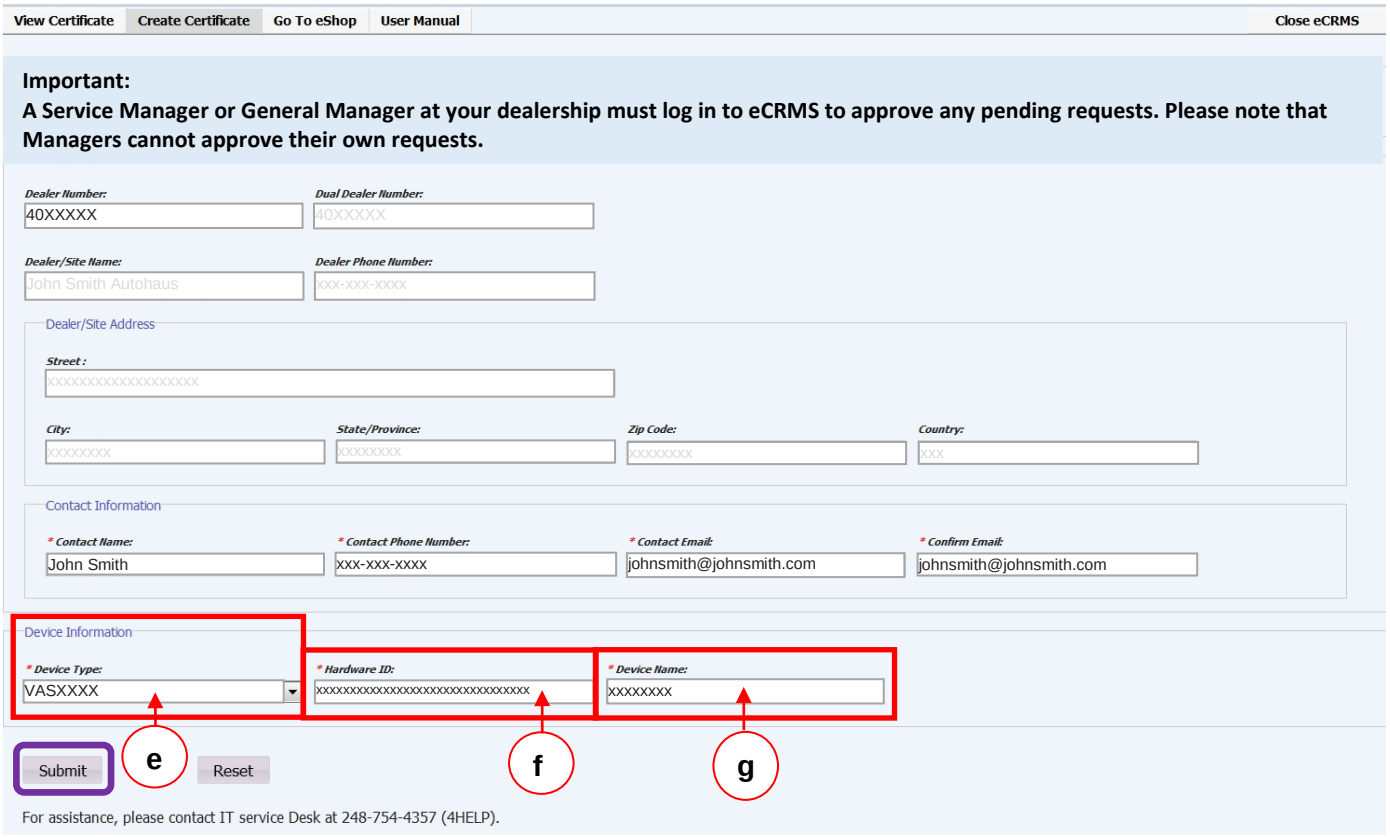
d. **Restore** the ***eCRMS*** browser session.

e. In the ****Device Type*** field, Select the device type from the **dropdown menu.**

f. In the ****Hardware ID*** field, **use Windows keystroke combination Ctrl + V** to **Paste** the **32-character Hardware Key** into the field. (Manual entry is not possible.)

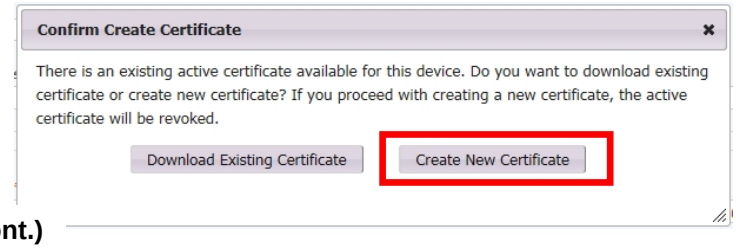
g. In the ****Device Name*** field, **Enter** the corresponding, assigned **device ID.**

When all **required information fields (*)** are filled in, click **Submit:**



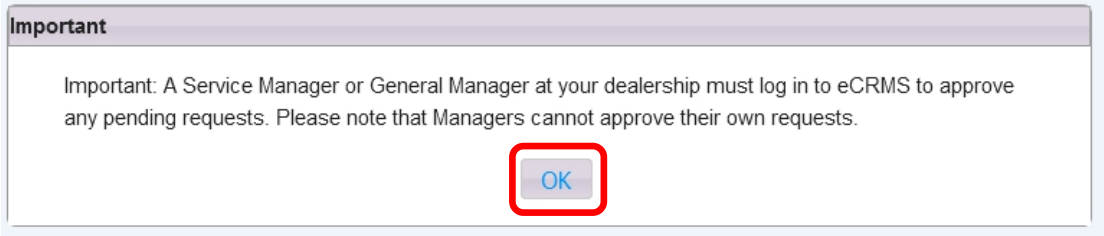
Note: The device ID must be accurately matched with the hardware key in the preceding step*. The* ***device ID*** *and* ***hardware key*** *entered above will appear next to the certificate file* ***staged in eCRMS*** *during the* ***certificate download*** *steps that follow.*

7. Heed the **Confirmation Create** prompt, and then select **Create New Certificate:**



(cont.)

8. Heed the **Important** message, and then click **OK**:



9. **Note the Request Number** from the request summary, and then select **Close.**
10. From the eCRMS header, click **Close eCRMS,** and then **Close** Internet Explorer.

Close eCRMS and Internet Explorer steps are mandatory!

11. Inform a manager authorized to approve certificate requests of the **request number** and diagnostic device details, and ask that the request be approved as per the instructions in **Section 2.4 below.**

2.4 – Approve Certificate Request (eCRMS)

Prerequisites:

- ☐ **The Approver *cannot be the same as* The Requestor.**
- ☐ *The request number is known.*

1. **Start Internet Explorer.**
2. Logon to **accessaudi** and go to: **App Links > Service**.
3. Click the link to **ODIS Certificate Request Mgmt. System (*eCRMS*)** and complete the ***eCRMS*** logon.

The **View Certificate** page displaying all active and pending dealer certificates appears first by default.

4. Locate the pending request by its **Request Number** and **Pending Review** status:
5. Click the **Device Name** for the pending request:

Request Number	Device Name	Hardware ID	Status
42527	352535	72c83b8b8ad040c921c3c6034c205042	Active
42627	gsddsdsdg	72c83b8b8ad040c921c3c6035c205042	Active
42727	Test001	0b12ac04cf979e53af246738b6e5f65e	Active
42728	Test002	382b5410c12eecb71f8c81c470c17b91	Active
42729	6643ef918c699e00c168	6643ef918c699e00c16841d24d03978c	Active
42827	DSS test	0e8ec93100d72ed61905cb3b56a31a0b	Active
42828	59be54acf54e71e99277	59be54acf54e71e9927764fe2a16143e	Active
42829	JG HP Test	34c6af22d4cf1fed0a3b5da8a9f7463a	Pending Review

(cont.)

Note:
The* Request Number, Device ID *and* Hardware ID *information illustrated here are examples only. Each diagnostic device is unique!

6. Confirm the request details from the summary, and then select **Approve:**

7. **Close** the request summary, and then **Close** the eCRMS session.

When the certificate request is approved: A certificate is staged for download in eCRMS and a confirmation email is sent to the requestor.

2.5 – Download & Store Security Certificate

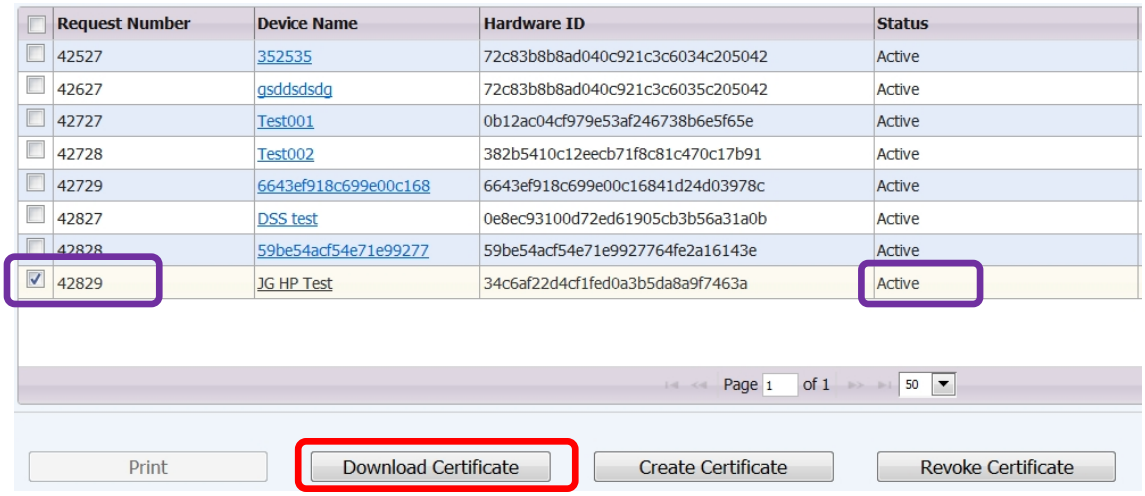
Prerequisite:

- ☐ ***The diagnostic device on which ODIS Service is installed is used to download and store the certificate.***

1. **Start Internet Explorer.**
2. Logon to **accessaudi** and go to: **App Links > Service**.
3. Click the link to **ODIS Certificate Request Mgmt. System (*eCRMS*)** and complete the ***eCRMS*** logon.

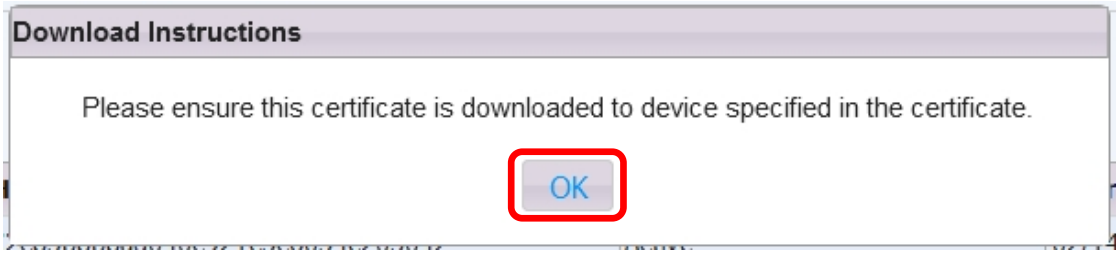
The **View Certificate** page displaying all active and pending dealer certificates appears first by default.

4. Locate the approved certificate by its **Request Number** and **Active** status:
5. **Check** ☑ the certificate and then select **Download Certificate:**

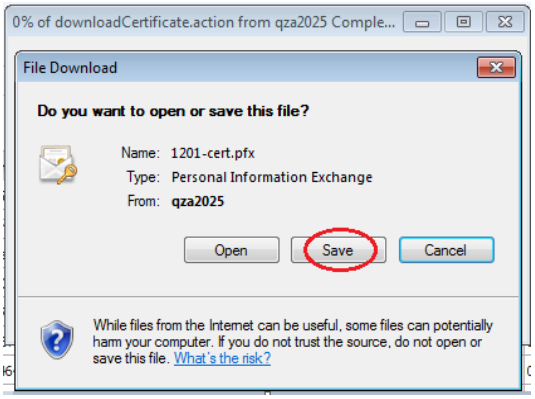


(cont.)

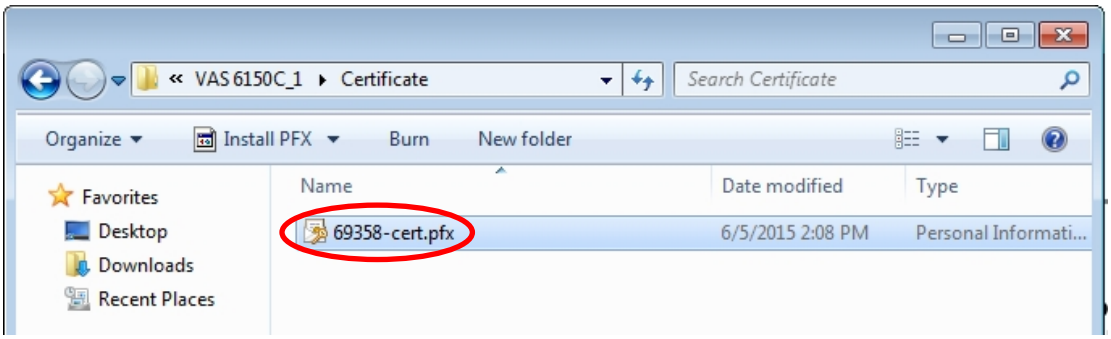
6. **Heed** the **Download Instructions** message, and then click **OK:**



7. Select **Save:**



8. **Navigate** to the **device folder** on the diagnostic device desktop, and **Save** the certificate in the **Certificate** subfolder (or other location on the device):



Ensure the certificate file appears as being saved in the **Certificate** subfolder.

9. From the **eCRMS header**, click **Close eCRMS.**

10. **Close Internet Explorer.**

Note:

Be sure to save a copy of the certificate on the backup USB flash drive as well!

Proceed to Section 2.6 – Page 10

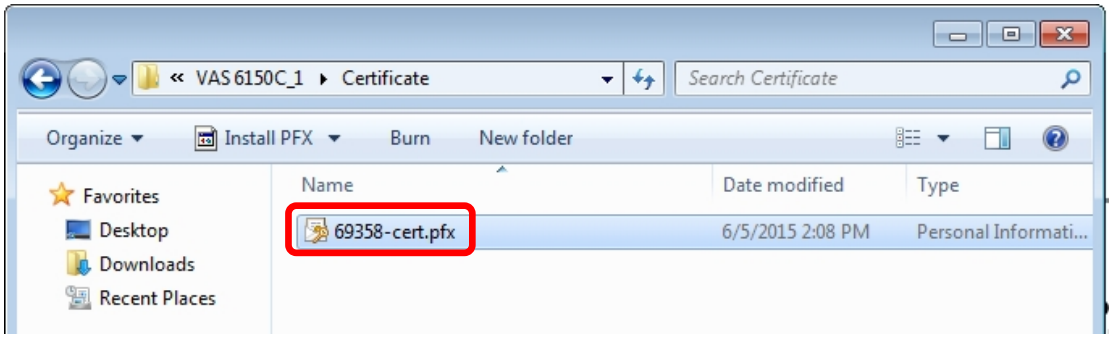
2.6 – Import Security Certificate to Windows

The diagnostic device's **hardware key must be entered as a password** during certificate importation.

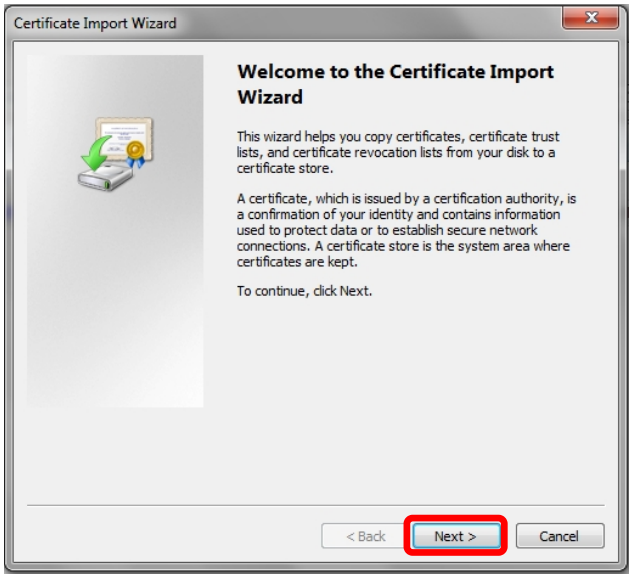
Prerequisites:

- ☐ *Previous certificate deleted from Windows.*
- ☐ *New security certificate saved to folder on device desktop or other location.*
- ☐ *Text document with device's **hardware key** on hand.*

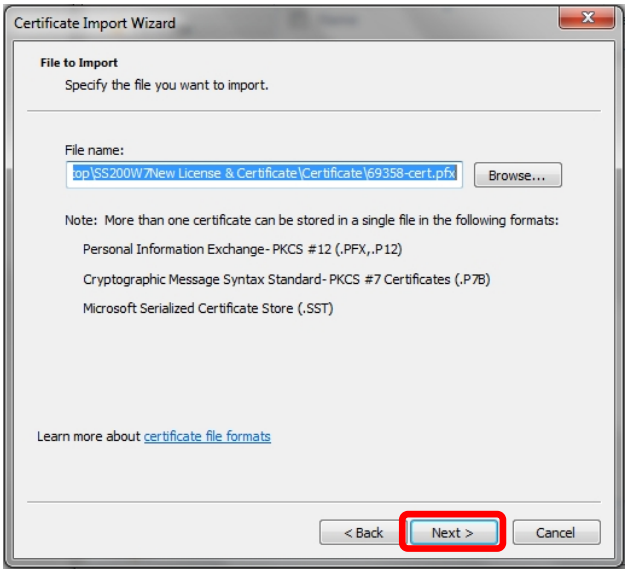
1. From the **device folder** on the Windows desktop (or other location on the device), **Open** the **Certificate** subfolder and **double-click** the **certificate** (.pfx) **file:**



2. Select **Next, . . .** confirm the certificate path is highlighted as illustrated and then select **Next:**



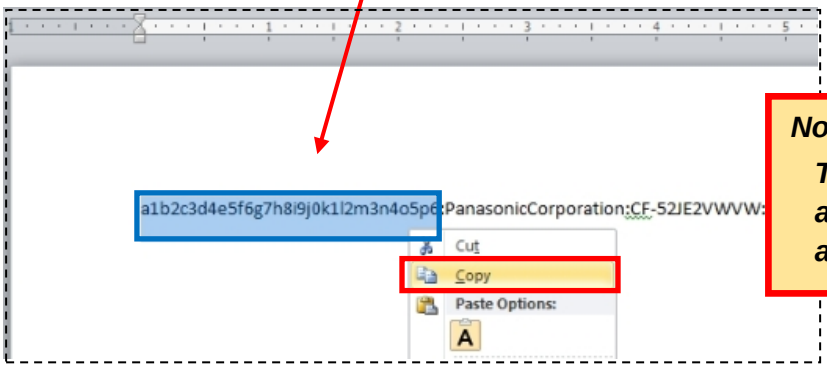
. . .



(cont.)

3. From the **device folder** on the Windows desktop (or other location), **Open** the **Hardware Key** text document:

4. **Select** and **Copy** **the first 32 characters (only)** of the **hardware key.** Example:

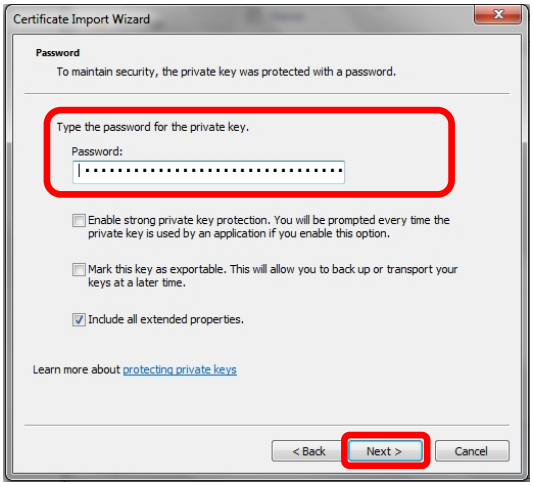


Note:

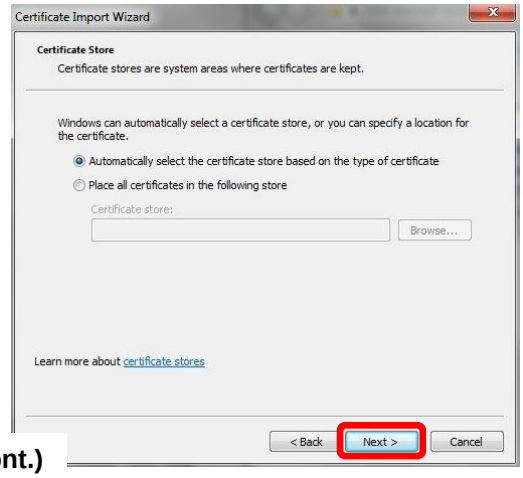
The hardware key illustrated here is an example only. All hardware keys are different!

The characters are saved in Windows "clipboard" memory.

5. **Paste** the 32-characters copied above into the **Password:** entry field, and then select **Next:**

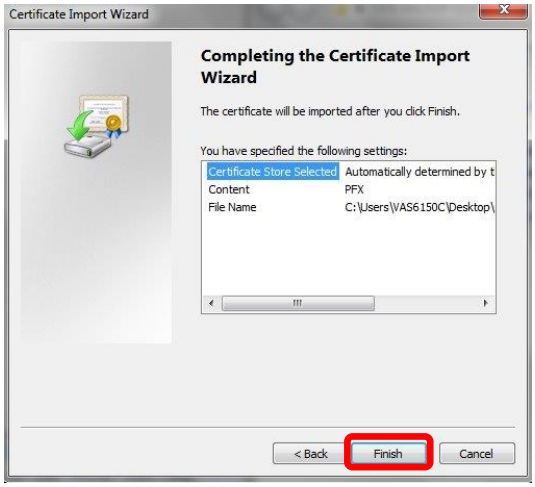


6. No action needed. **Select Next:**

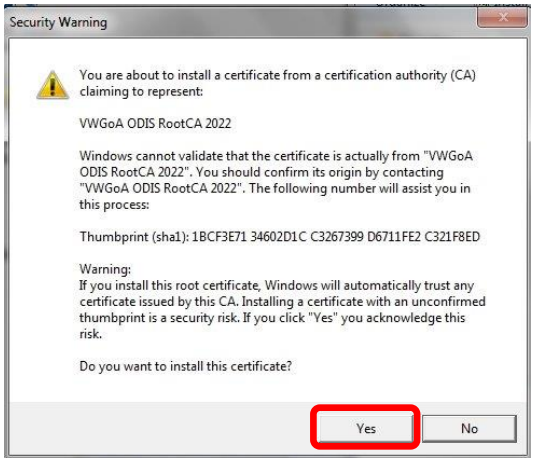


(cont.)

7. Select **Finish:**



8. Select **Yes:**



9. Click **OK:**

Proceed to Section 2.7 – Page 13

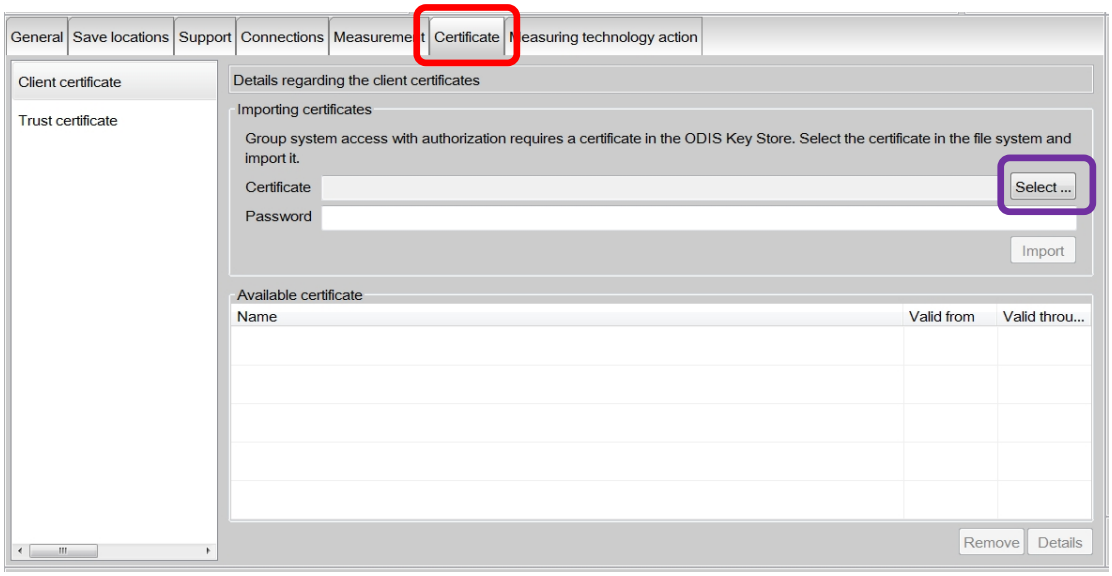
2.7 – Import Security Certificate to ODIS Service

The diagnostic device's **hardware key must be entered as a password** during certificate importation.

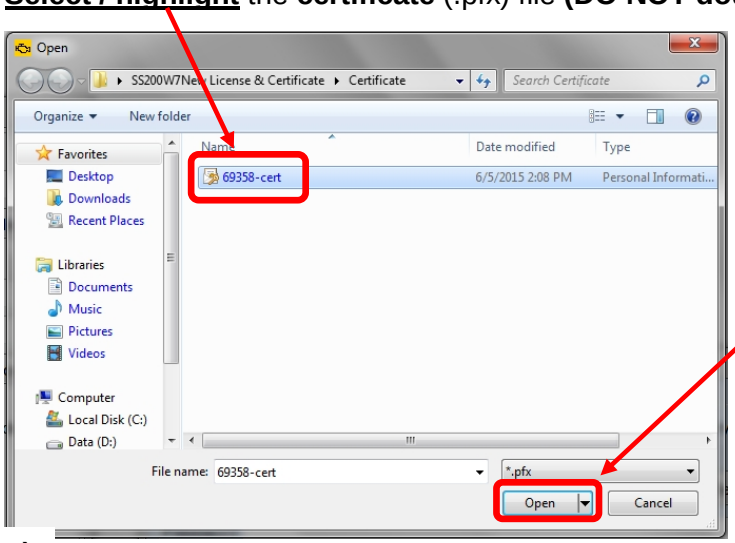
Prerequisites:

- ☐ *Previous certificate deleted from ODIS Service.*
- ☐ *Text document with device's **hardware key** on hand.*

1. **Start ODIS Service**, and then select the **Admin** operating mode and **Certificate** subcategory:
2. Click **Select:**



4. From the **device folder** on the Windows desktop (or other location on the device), **Open** the **Certificate** subfolder:
5. **<u>Select / highlight</u>** the **certificate** (.pfx) file **(DO NOT double-click)**, and then click **Open:**



Note:

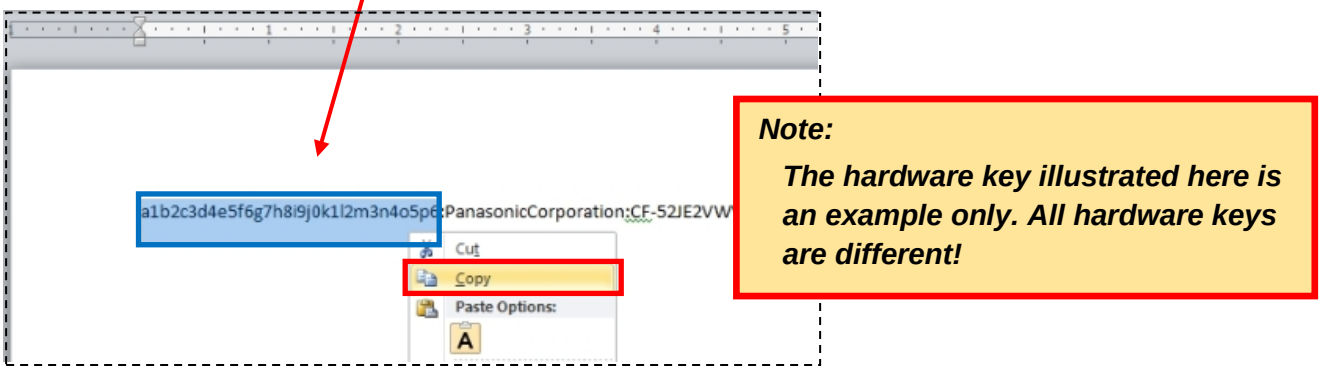
DO NOT *double-click the certificate file in its saved location!*

(cont.)

6. Ensure the **certificate file directory path** appears in the **Certificate** import window:

7. From the **device folder** on the Windows desktop (or other location), **Open** the **Hardware Key** text document:

8. **Select** and **Copy** **the first 32 characters (only)** of the **hardware key.** Example:



The characters are saved in Windows “clipboard” memory.

9. **Paste** the 32-characters copied above into the **Password:** entry field, and then select **Import:**

8. Click **OK:**