

Service Information

Offboard Diagnostic Information System Service (ODIS Service)

Number: AOS-14-13

Subject: ODIS Service Installation Phase 3 - Security Certificate
Request & Installation Instructions

Date: March 20, 2014

Supersedes AOS-14-07 due to revised license & certificate file management.

Table of Contents

Section	Page
1.0 Introduction - MUST READ!	1
2.0 Preparation	2
2.1 Request Resources Checklist	2
2.2 Device & Software Checklist	2
3.0 Certificate Request & File Management	3
3.1 Certificate Request via eCRMS	3
3.2 Certificate File Management	6
4.0 Certificate Installation	7
5.0 Certificate File Backup	11

Notes:

- The following procedures must be performed **by qualified personnel only!**
- Please read these instructions in their entirety before performing these procedures. **If you do not have previous experience loading software or do not understand these instructions, arrange to have a qualified person perform these procedures.**
- Heed all prerequisite requirements and notes, and **follow all instruction steps in the Section order given**, including instructions cross-referenced in documents posted on ServiceNet.
- Perform the procedures in an area that is quiet, clean and without distraction or interruption.
- **Discard all printed copies of this document after use.** Revised versions may be issued at any time. Always check ServiceNet for the latest version.

1.0 – Introduction

An **ODIS Service Security Certificate** is required on each diagnostic device connected to VWAG Group Systems for vehicle immobilizer adaptations, SVM, online software updates and ElsaPro - Infomedia.

The certificate **is associated with the device hardware key and installed license.**

Use this document to request and install a security certificate on VAS diagnostic devices where **a security certificate was not previously installed** or to **request and install a replacement certificate**. ODIS Service installation Phases 1 through 3 must be completed on all new devices and existing devices where the operating system was updated or recovered prior to using ODIS Service for vehicle diagnosis.

2.0 – Preparation

Important preparation prerequisites must be fulfilled prior to proceeding!

2.1 – Request Resources Checklist

✓	Request Resources Checklist
	Person performing certificate request has access permission to the eCRMS application on vwhub*
	Network desktop PC or laptop connected to a printer available
	☐ Fax machine available or ☐ Scanner and network desktop PC or laptop with email program available
*Access is granted by the Dealership Systems Administrator	

2.2 – Device & Software Checklist

✓	Device & Software Checklist
	New Devices – New Request: <ul style="list-style-type: none"> ☐ ODIS Service Installation Phase 1 - Preparation & License Request Instructions (eShop) completed ☐ ODIS Service Installation Phase 2 – Software Installation & Configuration Instructions completed ☐ The latest version of ODIS Service installed
	Existing Devices – Replacement Request: <ul style="list-style-type: none"> ☐ The latest version of ODIS Service installed
	Backup USB flash drive on hand as per installation Phase 2 - Section 5.2. (Backup USB flash drive must contain the device folder with “License” and “Certificate” subfolders, and text document with saved hardware key as per installation Phase 1 - Section 3.5).

ATTENTION!

DO NOT proceed with the certificate request process if...

- You do not have access permission to the eCRMS application on vwhub.
- ODIS Service is not installed.
- The diagnostic device **hardware key** was not recorded in a text document and saved in the backup USB flash drive.

The hardware key must be copied from a text document and pasted into the eCRMS interface. Manual (typed-in) entry of the hardware key is not possible!

☐	Preparation steps completed. Proceed to Section 3.0 – Page 3.
--------------------------	---



3.0 – Certificate Request & File Management

3.1 – Certificate Request via eCRMS

1. Insert the **backup USB flash drive** with **device folder** into available port on a network PC or laptop **connected to a printer**.
2. **Open** the backup USB flash drive directory.
3. **Start Internet Explorer** and **Logon** to **vwhub**.
4. Select the **My Hub** or **Service** category.
5. From the **Related Sites** menu (far left) click on **ODIS Certificate Request Mgmt. System (eCRMS)**.
6. Complete the **eCRMS** logon.
7. Select **Create Certificate**:

The screenshot shows the eCRMS web application. At the top, there's a navigation bar with buttons: 'View Certificate', 'Create Certificate' (highlighted with a red box), 'Advanced Search', 'Go To eShop', and 'User Manual'. Below this is a search section with a 'Search' label, a 'Dealer Number' input field, a 'Status' dropdown menu (showing '-Select-'), and a 'Search' button. At the bottom of the visible area is a 'Certificate Management' section.

8. The eShop license referred to below is the ODIS Service license file that was installed during the Installation Phase 2 process. Click **Yes**:

The screenshot shows a dialog box titled 'eShop License'. It contains the text: 'A valid eShop license is required before proceeding. Do you have a valid eShop license?'. At the bottom, there are two buttons: 'Yes' (highlighted with a red box) and 'No'.

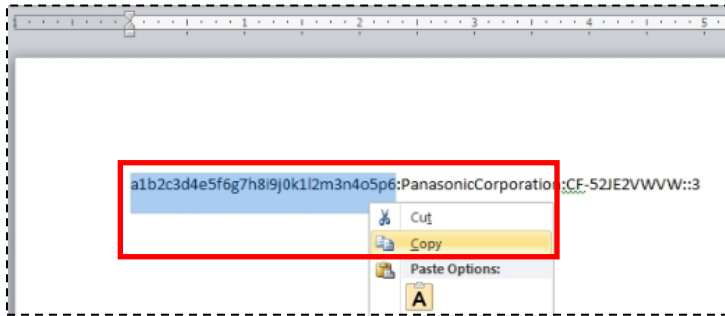
The **eCRMS** request interface appears.

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

9. **Enter all** applicable information as required in the **Dealer/Site Information** and **Contact Information** sections.

Continued ...4/

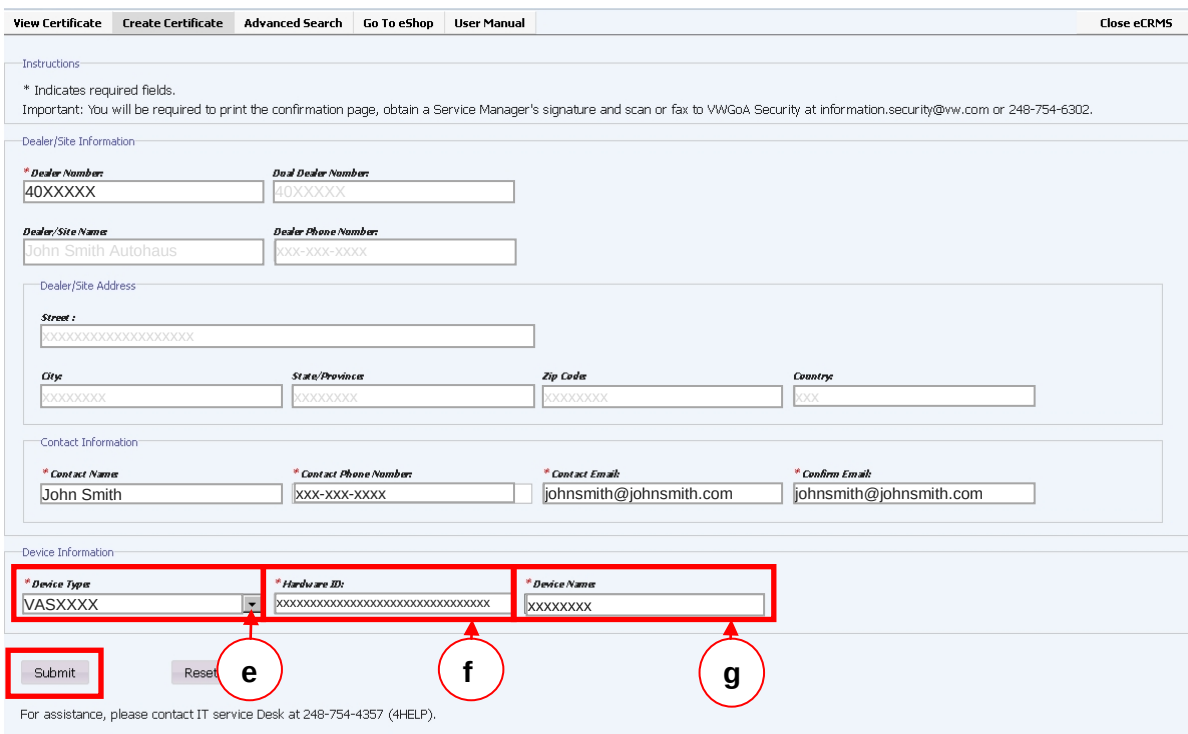
10. Enter the **diagnostic device** information in the **Device Information** section as follows:
 - a. **Minimize** the eCRMS browser session and **navigate to the backup USB flash drive directory** (or other location with the device hardware key saved as text).
 - b. **Open** the applicable **device folder** and **Hardware Key** document (or other document with the recorded **hardware key**).
 - c. **Select and Copy the first 32 characters (only)** of the **hardware key**. Example:



The characters are saved in Windows “clipboard” memory.

- 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**:



View Certificate | Create Certificate | Advanced Search | Go To eShop | User Manual | Close eCRMS

Instructions
* Indicates required fields.
Important: You will be required to print the confirmation page, obtain a Service Manager's signature and scan or fax to VWGoA Security at information.security@vw.com or 248-754-6302.

Dealer/Site Information

* Dealer Number: 40XXXXX | Deal Dealer Number: 40XXXXX

Dealer/Site Name: John Smith Autohaus | Dealer Phone Number: xxx-xxx-xxxx

Dealer/Site Address

Street :
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

City: xxxxxxxx | State/Province: xxxxxxxx | Zip Code: xxxxxxxx | Country: xxx

Contact Information

* Contact Name: John Smith | * Contact Phone Number: xxx-xxx-xxxx | * Contact Email: johnsmith@johnsmith.com | * Confirm Email: johnsmith@johnsmith.com

Device Information

* Device Type: VASXXXX | * Hardware ID: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx | * Device Name: xxxxxxxx

Submit | Reset

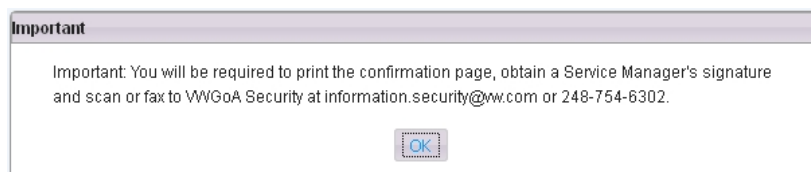
For assistance, please contact IT service Desk at 248-754-4357 (4HELP).

Continued ...5/

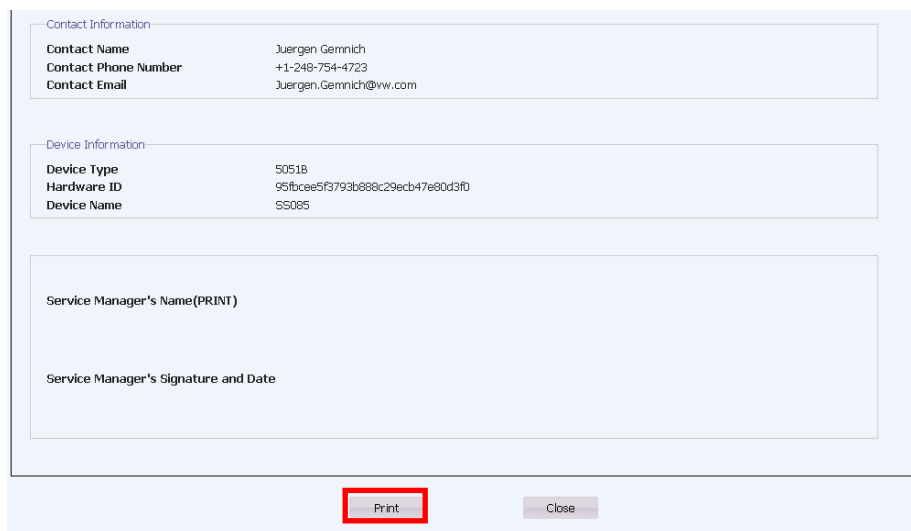
Note:

The **device ID** must be accurately associated with its **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 Management** steps that follow.

11. Note the email address and/or fax number from the **Important** dialog message. Click **OK**:



12. Print the confirmation page (click **Print**):

A confirmation page form with a light blue background. It contains three main sections: "Contact Information" with fields for Contact Name (Juergen Gemnich), Contact Phone Number (+1-248-754-4723), and Contact Email (Juergen.Gemnich@vw.com); "Device Information" with fields for Device Type (50518), Hardware ID (95fbcae5f3793b688c29ecb47e80d3f0), and Device Name (SS085); and a large text area for "Service Manager's Name(PRINT)" and "Service Manager's Signature and Date". At the bottom, there are "Print" and "Close" buttons, with the "Print" button highlighted by a red rectangle.

13. In the **printed copy**, fill in the **Service Manager's name**.

14. Have your Service Manager **sign and date** the printed copy.

15. **Fax** the printed form to **(248) 754-6302** or **scan and email form** to **information.security@vw.com**

16. **Safely remove / eject** the backup USB flash drive.

17. Retain USB flash drive for the Certificate Management steps that follow.

When the certificate request is approved:

- The certificate is created and staged for download in **eCRMS**.
- An email is sent, instructing you to logon to **eCRMS** to locate and download the certificate.

Note: Certificate request confirmation emails can be expected **within one working day** from the time of submission.

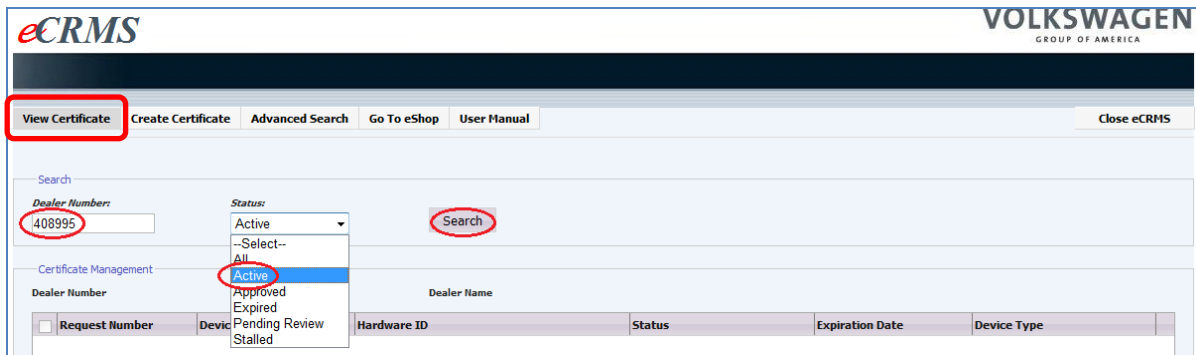
 Certificate Request steps completed. Proceed to [Section 3.2 – Page 6](#).

3.2 – Certificate File Management

Prerequisites:

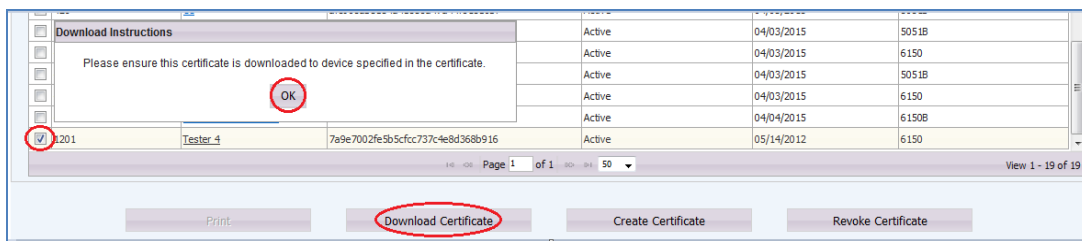
- ☐ **Certificate confirmation email received.**
- ☐ **Backup USB flash drive on hand.**

1. Insert the **backup USB flash drive** with **device folder** into available port on a network PC or laptop.
2. Logon to **vwhub** and navigate through **My Hub** or **Service > Related Sites > ODIS Certificate Request Mgmt. System (eCRMS)**. A new browser window will open.
3. Logon as necessary and then select **View Certificate**:
4. **Enter your Dealer Number**, select **Status: Active**, and click **Search**:

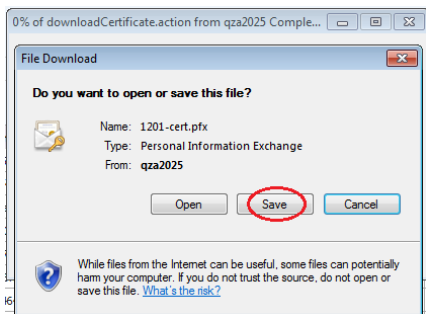


A screen with active certificate(s) for the dealership appears:

1. Note the **Device ID** associated with a posted certificate and place a checkmark (✓) next to the certificate number:
2. Click **Download Certificate**: Note the **Download Instructions** dialog, and click **OK**:



3. **Navigate** to the applicable **device folder** on the backup USB flash drive, and **Save** the certificate in the **Certificate** subfolder:

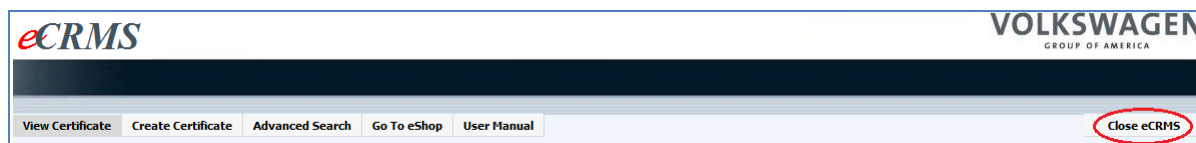


Continued ...7/



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

4. Select **Close eCRMS**:



5. **Safely remove / eject** the backup USB flash drive

6. Retain backup USB flash drive for the certificate installation steps that follow.

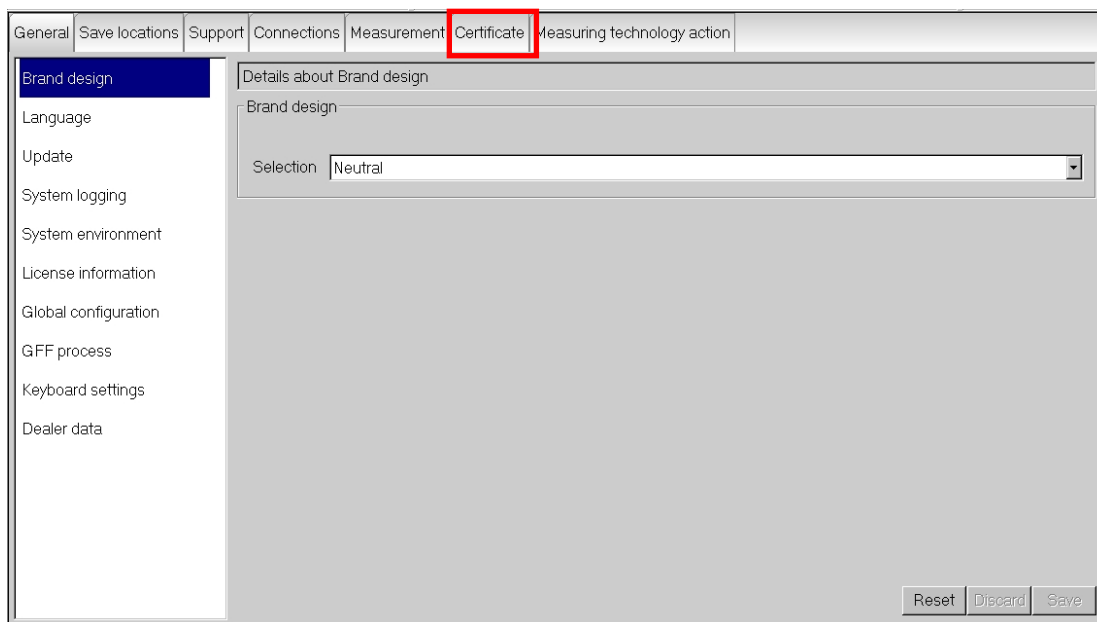
☐ **Certificate Management steps completed. Proceed to Section 4.0 below.**

4.0 – Certificate Installation

Prerequisites:

- ☐ *Diagnostic device plugged in to A/C power adapter and booted to Windows desktop.*
- ☐ *Note the **device ID** of the device on which the certificate installation is being made.*
- ☐ **VAS 5052A:** *Recommend connecting USB mouse and keyboard for easier input.*
- ☐ **Backup USB flash drive with saved certificate file on hand.**

1. Insert the **backup USB flash drive** into the **diagnostic device requiring certificate installation**.
2. From the Windows desktop, click the **DiagStarter** icon.
3. Select **Offboard Diagnostic Information System Service**.
4. From the ODIS Service main screen, select the **Admin** operating mode:
5. Click the **Certificate** tab:



Continued ...8/

6. Click **Select**:

General | Save locations | Support | Connections | Measurement | **Certificate** | Measuring technology action

Client certificate

Trust certificate

Details regarding the client certificates

Importing certificates

Group system access with authorization requires a certificate in the ODIS Key Store. Select the certificate in the file system and import it.

Certificate **Select ...**

Password

Import

Available certificate

Name	Valid from	Valid through

Remove Details

6. Navigate to directory for the **backup USB flash drive**:

General | Save locations | Support | Connections | Measurement | **Certificate** | Measuring technology action

Client certificate

Trust certificate

Details regarding the client certificates

Importing certificates

Group system access with authorization requires a certificate in the ODIS Key Store. Select the certificate in the file system and import it.

Certificate **Select ...**

Password

Import

Available certificate

Name	Valid from	Valid through

Remove Details

Open

Look in: My Computer

Local Disk (C:) | Data (D:) | **Removable (F:)** | Shared Documents | VAS 61508's Documents

File name:

Files of type: *.plx

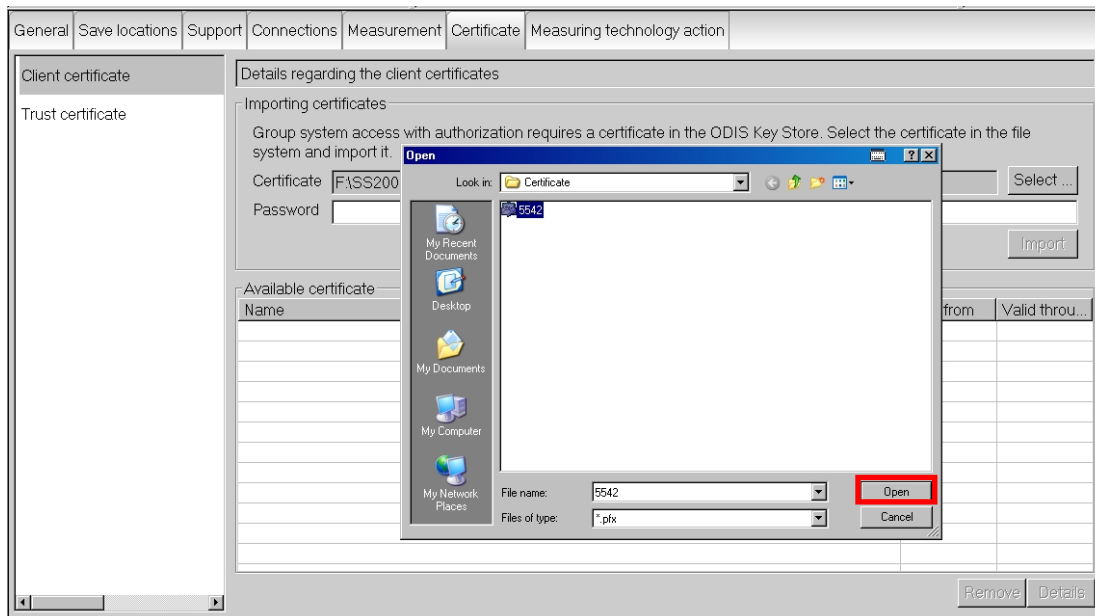
Open Cancel

7. **Open** the backup USB Flash drive directory

8. Locate and **Open** the **device folder** for the device on which the certificate installation is being done.

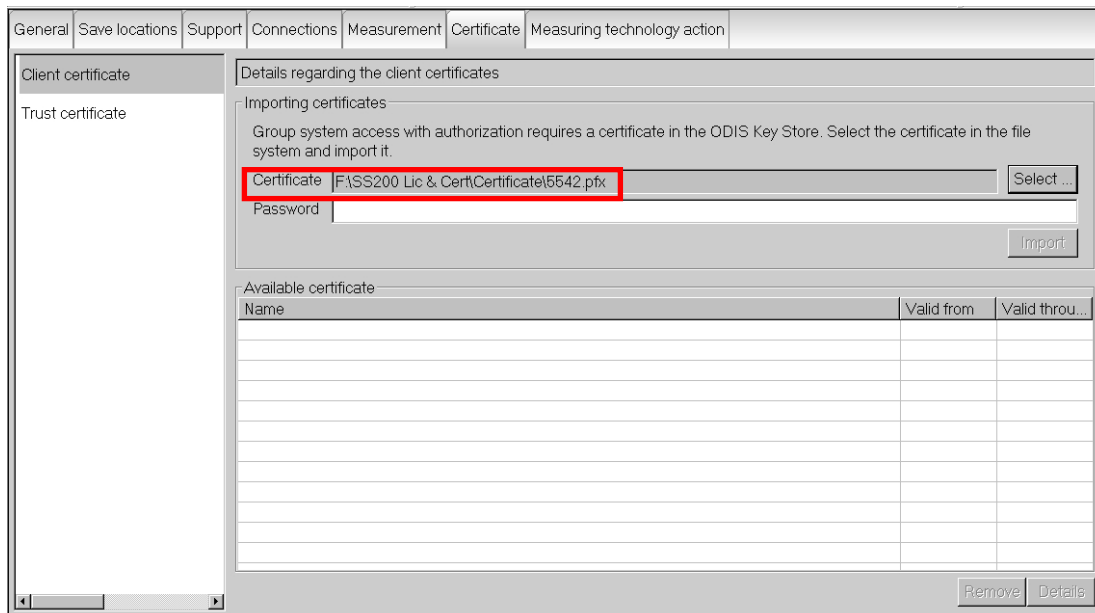
Continued ...9/

9. **Open** the **Certificate** subfolder and **select/highlight** the saved certificate file (xxxx-cert). Then click **Open** to copy the certificate file to the installation window entry:



Note: DO NOT double-click on certificate file in its saved location!

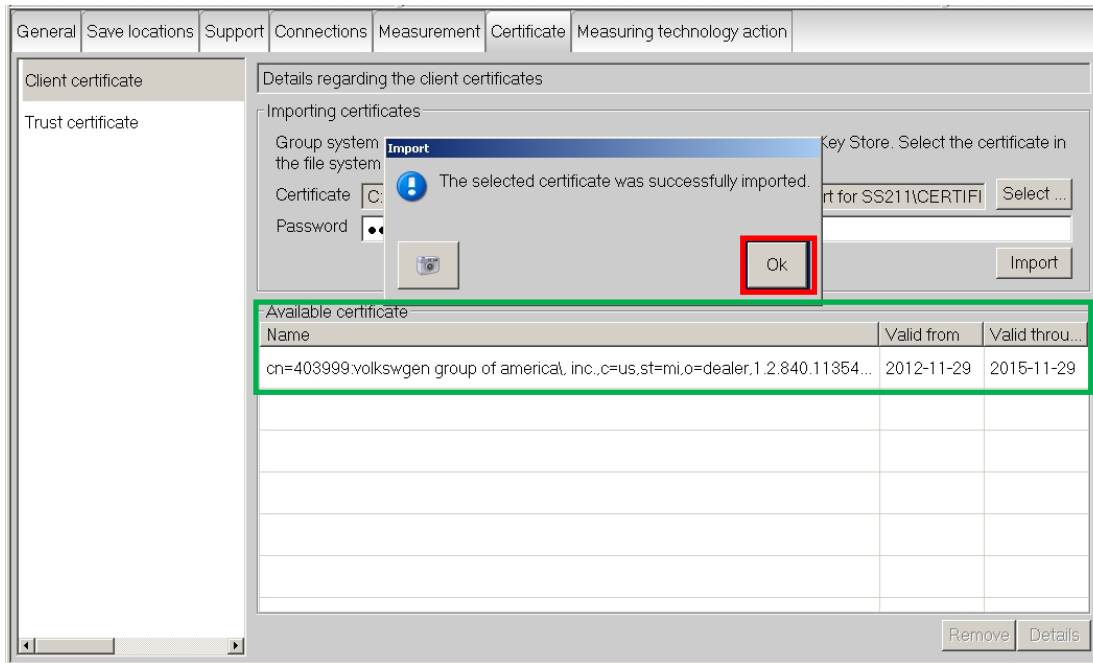
10. Ensure certificate file appears as being copied (directory path illustrated is example only):



11. **Minimize** the ODIS Service window.
12. Navigate to the backup USB flash drive directory (or other location with hardware key saved as text) and open **Hardware Key** document.

Continued ...10/

16. The certificate appears in summary form in the **Available certificate** window. Click **Ok**:



17. Click **Diagnosis** to return to the main screen or **Close** the application.



Security Certificate Installation steps completed. Proceed to Section 5.0 below.

5.0 – Certificate File Backup

The following steps describe how to copy the **certificate file** from the **backup USB flash drive** to the **device folder on the diagnostic device desktop**.

These steps complete the backup of certificate file to facilitate reinstallation of the certificate from the desktop location (in case ODIS Service is removed and reinstalled), or reinstallation of the certificate file from the USB flash drive (in case of Windows system recovery).

1. Navigate to the **device folder** on the **backup USB flash drive**.
2. **Open** the **Certificate subfolder**.
3. **Select** and **Copy** the **certificate file**.
4. Navigate to the Windows desktop and **Open** the original **device folder**.
5. **Open** the **Certificate subfolder** and **Paste** the certificate file in the folder.
6. **Close** all open folders and Windows.
7. **Safely remove/eject** the backup USB flash drive and retain for future use if necessary.



Certificate File Backup steps completed. All Certificate Process steps completed.