

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

Section		Page
1.0	Introduction	1
2.0	Certificate File Management	<u>2</u>
2.1	Preparation – MUST READ!	<u>2</u>
2.2	Delete Existing Certificates	<u>2</u>
2.3	Request Security Certificate (eCRMS)	<u>4</u>
2.4	Approve Security Certificate (eCRMS)	<u>7</u>
2.5	Download & Store Security Certificate	<u>8</u>
2.6	Import Security Certificate to Windows®	<u>10</u>
2.7	Import Security Certificate to ODIS Service	<u>13</u>

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 <u>before its expiration date.</u>

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.

All rights reserved. Information contained in this document is based on the latest information available at the time of printing and is subject to the copyright and other intellectual property rights of Volkswagen Group of America, Inc., its affiliated companies and its licensors. All rights are reserved to make changes at any time without notice. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, nor may these materials be modified or reposted to other sites, without the prior expressed written permission of the publisher.



2.0 – Certificate File Management

2.1 – Preparation – MUST READ!

Effective February 26, 2017, authorized dealership personnel are responsible for requesting <u>and</u> <u>approving</u> 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)

- Service Director (SVC-DIR)
- Dealer Principal/General Manager (DLR-PRGM)
- General Manager (GEN-MGR)

- 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* <u>dealership manager as defined above</u>, 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 <u>deleting all stored and backup copies of the</u> <u>certificate before renewal.</u>

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.)

^{© 2017} Audi of America, Inc.

All rights reserved. Information contained in this document is based on the latest information available at the time of printing and is subject to the copyright and other intellectual property rights of Volkswagen Group of America, Inc., its affiliated companies and its licensors. All rights are reserved to make changes at any time without notice. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, nor may these materials be modified or reposted to other sites, without the prior expressed written permission of the publisher.



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

Internet Options		? ×			
General Security Privacy	Content Connection	s Programs Advanced			
Family Safety					
Control the Internet content that can Family Safety be viewed.					
Certificates	Certificates				
Use certificates for encrypted connections and identification.					
Clear SSL state	Certificates	Publishers			

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

Certificates	
Intended purpose: <all></all>	
Personal Other People Intermediate Certification Authorities Trusted Root Certification	
Issued To Issued By Expiratio Friendly Name	
Import Export Remove Advanced Certificate intended purposes	Certificates You cannot decrypt data encrypted using the certificates. Do you want to delete the certificates?
<al> View Learn more about <u>certificates Close </u></al>	Yes No

- 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:

© 2017 Audi of America, Inc.

Travia Ta	Torough Bus	Evaluatio	Evinethy Name	
Issued To	Issued By	1/8/2022		
Egivenaign class a ru	 venaign class a Public 	7/10/2000		
VeriSign Class 3 Pu	. VeriSign Class 3 Public	7/16/2036	VeriSign	Certificates
UIN-USERFirst-Obj.	UIN-USERFirst-Object	//9/2019	USERTrust (Cod	
Thawte Timestampi.	Thawte Timestamping	12/31/2020	thawte timesta	
The under Printer y Ko	There is a contract of the con	12/1/2037	thawte Frindi y	
inawte Premium se.	Thawte Premium Serv	12/31/2020	thawte	Deleting system root certificates might prevent some Windows
Starneid Root Certi.	Starneid Root Certific	12/31/203/	Starfield Root C	components from working properly. The list of system critical root
LABILITY ACC	. NO LIABILITY ACCEP	1/7/2004	verisign time st	certificates can be reviewed at
				http://support.microsoft.com/?id=293781. If Update Root Certificate
Import Export.	Remove		Advanced	installed, any deleted third-party root certificates will be restored
				automatically, but the system root certificates will not. Do you want
Certificate intended purpo	oses			automatically, but the system root certificates will not. Do you want
<all></all>				delete the selected certificate(s)?
NAIL2				
			View	
				N

Page 3 of 14



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:

Client certificate	Details regarding the client certificates	
Trust certificate	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	
	cn=403999:volkswgen group of america inc.,c=us,st=mi,o=dealer,1.2.840.113549.1.9.1=#16166a75657267656e2e67656d6e69€	
	cn=403999:volkswgen group of america inc.,c=us,st=mi,o=dealer,1.2.840.113549.1.9.1=#16166a75657267656e2e67656d6e69£	Remove the certificate
	cn=403999:volkswgen group of america inc.,c=us,st=mi,o=dealer,1.2.840.113549.1.9.1=#16166a76657267656e2e67656d6e699	Remove the certificate Do you really want to remove the selected certificate

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.)

^{© 2017} Audi of America, Inc.

All rights reserved. Information contained in this document is based on the latest information available at the time of printing and is subject to the copyright and other intellectual property rights of Volkswagen Group of America, Inc., its affiliated companies and its licensors. All rights are reserved to make changes at any time without notice. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, nor may these materials be modified or reposted to other sites, without the prior expressed written permission of the publisher.

4. Select Create Certificate Yes:

ecrms	eShop License 🗙
	A valid eShop license is required before proceeding. Do you have a valid eShop license?
View Certificate Create Certificate Go To eShop User Manual	Yes No

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.
 - 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:

·····	· · · 2 · · · · 1 · · · 3 · · · 1 · · · 4	* * * 1 * * * 5 * *
a1b2c3d4e5f6g7h8i9j0k1l	2m3n4o5p6:PanasonicCorporation :CE-5	2JE2VWVW::3
	Copy Paste Options:	Note: The hardware key illustrated here is
		an example only. All hardware keys

The characters are saved in Windows "clipboard" memory.

(cont.)

© 2017 Audi of America, Inc.



 In the *Device Ty In the *Hardware 	pe field, Select the de	ovice type from the drep	
. In the *Hardware		evice type from the drop	down menu.
character Hardw.	<i>ID</i> field, use Windov are Key into the field ame field, Enter the c	vs keystroke combinati . (Manual entry is not po orresponding, assigned o	on Ctrl + V to Paste the 32- ssible.) device ID.
When all required in	formation fields (*) are filled in, click Subm	lit: Close e
Important: A Service Manager or Gen Managers cannot approve	eral Manager at your deale their own requests.	rship must log in to eCRMS to a	pprove any pending requests. Please note tha
Dealer Number:	Dual Dealer Number:		
40XXXXX	40XXXXX		
Danlay (Cita Nama)	Destas Oberes Numbers		
John Smith Autohaus			
Street: >00000000000000000000000000000000000	State/Province:	Zip Code:	Country:
Contact Information			
* Contact Name:	* Contact Phone Number:	* Contact Email:	* Confirm Fmail:
John Smith	xxx-xxx-xxxx	johnsmith@johnsmith.com	johnsmith@johnsmith.com
Device Information * Device Type: VASXXXX Submit Evaluation • Device Type: • Constant II condition • Constant II condition • Conditio	Hardware ID: X000000000000000000000000000000000	Device Name: XXXXXXX	
For assistance, predse contact IT service	e Desk dl 240-704-4307 (4HELP).		

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:

There is an certificate o certificate w	existing active certificate available fo r create new certificate? If you proce vill be revoked.	r this device. Do you want to downlo ed with creating a new certificate, th	ad exist e active
	Devertee d Existing Contificate	Create New Certificate	

© 2017 Audi of America, Inc.



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



- 9. Note the <u>Request Number</u> 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	<u>gsddsdsdg</u>	72c83b8b8ad040c921c3c6035c205042	Active
42727	<u>Test001</u>	0b12ac04cf979e53af246738b6e5f65e	Active
42728	Test002	382b5410c12eecb71f8c81c470c17b91	Active
42729	6643ef918c699e00c168	6643ef918c699e00c16841d24d03978c	Active
42827	DSS test	0e8ec93100d72ed61905cb3b56a31a0b	Active
42828	59bc54acf54e71e99277	59be54acf54e71e9927764fe2a16143e	Active
42829	JG HP Test	34c6af22d4cf1fed0a3b5da8a9f7463a	Pending Review

Note:

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

© 2017 Audi of America, Inc.

(cont.)

Page 7 of 14

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

Device Information			
Device Type:	Hardware ID:	Device Name:	
6150B	34c6af22d4cf1fed0a3b5da8a9f7463a	JG HP Test	
Approve Revok	e service Desk at 248-754-4357 (4HELP).		

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 I the certificate and then select Download Certificate:

Request Nu	mber Device Name	Hardware ID	Status			
42527	352535	72c83b8b8ad040c921c3c6034c205042	Active			
42627	gsddsdsdg	72c83b8b8ad040c921c3c6035c205042	Active			
42727	Test001	0b12ac04cf979e53af246738b6e5f65e	Active			
42728	Test002	382b5410c12eecb71f8c81c470c17b91	Active			
42729	6643ef918c699e00c	168 6643ef918c699e00c16841d24d03978c	Active			
42827	DSS test	0e8ec93100d72ed61905cb3b56a31a0b	Active			
47878	59be54acf54e71e99	277 59be54acf54e71e9927764fe2a16143e	Active			
42829	JG HP Test	34c6af22d4cf1fed0a3b5da8a9f7463a	Active			
		Page 1	of 1 50 💌			
Page 1 of 1 50 V						

© 2017 Audi of America, Inc.

Page 8 of 14



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):

	i0C_1 ▶ Certificate	• •j	Search Certificate		• <mark>*</mark>
Organize 🔻 📷 Insta	all PFX 🔻 Burn New folder				0
☆ Favorites	Name		Date modified	Туре	
🧮 Desktop	69358-cert.pfx		6/5/2015 2:08 PM	Personal Ir	nformati
🐌 Downloads					
Recent Places					

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

- 9. From the eCRMS header, click Close eCRMS.
- 10. Close Internet Explorer.



Proceed to Section 2.6 - Page 10

© 2017 Audi of America, Inc.

Page 9 of 14

All rights reserved. Information contained in this document is based on the latest information available at the time of printing and is subject to the copyright and other intellectual property rights of Volkswagen Group of America, Inc., its affiliated companies and its licensors. All rights are reserved to make changes at any time without notice. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, nor may these materials be modified or reposted to other sites, without the prior expressed written permission of the publisher.



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:

Certificate Import Wizard			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.		File to Import Specify the file you want to import. File name: [op\SS200W7New License & Certificate\Certificate\69358-cert.pfx] Browse Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange-PKCS #12 (.PFX,.P12)		
	To continue, dick Next.		Learn more about <u>certificate file formats</u>		

(cont.)

© 2017 Audi of America, Inc.

Page 10 of 14

All rights reserved. Information contained in this document is based on the latest information available at the time of printing and is subject to the copyright and other intellectual property rights of Volkswagen Group of America, Inc., its affiliated companies and its licensors. All rights are reserved to make changes at any time without notice. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, nor may these materials be modified or reposted to other sites, without the prior expressed written permission of the publisher.

- 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:



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:



© 2017 Audi of America, Inc.

Page 11 of 14



7. Select Finish:



8. Select Yes:



9. Click OK:



Proceed to Section 2.7 - Page 13

© 2017 Audi of America, Inc.

Page 12 of 14



2.7 – Import Security Certificate to ODIS Service

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

Prerequisites:



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:

General	Save locations	Support Connec	ions Measureme	Certificate	easuring technology a	action			
Client ce	ertificate	Details re Importing Group s import i	garding the client of certificates ystem access with	ertificates authorization r	equires a certificate in th	he ODIS I	Key Store. Select	the certificate in the file	e system and
		Certifica	rd						Select
		Available Name	certificate					Valid from	Valid throu
<		,						Ren	nove Details

- 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:



Page 13 of 14

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

Details regarding the client certificates						
Importing ce	Importing certificates					
Group syste import it.	em access with authorization requires a certificate in the ODIS Key Store. Select the certi	ificate in the file sys	stem and			
Certificate	C:\Users\VAS6150D\Desktop\SS240 License & Certificate\Certificate\77642-cert.pfx		Select			
Password						
		[Import			

- 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:

1 • • • • • • • • • • • • • • • • • • •	5
a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6:PanasonicCorporation:CE-52JE2VW	Note: The hardware key illustrated here is an example only. All hardware keys are different!
Paste Options:	

The characters are saved in Windows "clipboard" memory.

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

Details regarding the client certificates							
Importing ce	Importing certificates						
Group syste import it.	Group system access with authorization requires a certificate in the ODIS Key Store. Select the certificate in the file system and import it.						
Certificate	C:\Users\VAS6150D\Desktop\SS240 License & Certificate\Certificate\77642-cert.pfx Select						
Password	•••••••						
	Impo	ort					

8. Click OK:



© 2017 Audi of America, Inc.

Page 14 of 14