Unlock procedure for SFD (Vehicle Diagnostic Protection)

We wish to inform you that, as of 2020, Volkswagen AG will introduce a new procedure for Vehicle Diagnostic Protection (SFD). In order to utilise the SFD procedure, it is necessary for users to be registered in advance on the SFD back end.

The aim of SFD

Product analyses in the VW Group have shown that there is an increased requirement for protection of data in vehicles. This is also the case for Vehicle Diagnostic Protection. The previous procedure (activation of security access by way of a 5-digit login code) no longer conforms to the state of the art. As of 2020 – beginning with the market entry of the MQB37W (Golf 8) – there will be a cross-brand introduction of the SFD procedure in order to provide Vehicle Diagnostic Protection.

SFD will be introduced in two project stages:

Stage 1 comprises access protection of protected diagnostic objects in control units and the verifiability of this access on an individual level. The protection requirement will be defined for specific control units and diagnostic objects. The protection requirement is limited to specific writing services (codings, adjustments, parametrisations) and routines. Normal reading services (e.g. readout of control unit event memories) will not be SFD-protected. The functions of data string downloading with boot loader data strings, flashing and/or update programming as well as flash data security are also not affected by SFD.

Stage 2 includes, as a supplement to stage 1, tamper protection of diagnostic contents upon integration of the diagnostic contents by end-to-end safeguarding of diagnostic data between VAG IT back end systems and control units.

In order to be able to log access to diagnostic contents requiring protection in future, the IT security organisation requires strong user authentication to be enforced. It is therefore necessary to use two-factor authentication, which can be implemented, for example, by using

- PKI-cards
- SecurID-cards
- Applications that generate one-time passwords (e.g. Google Authenticator or Microsoft Authenticator).

In a first transition phase, however, weak authentication by way of a username and password will initially be introduced when using the Dealer Portal. The transition to strong authentication by means of the Group Retail Portal will be developed in parallel.

The SFD process requires the vehicle diagnostic tester to have an online connection.

Functioning of SFD

Two methods will be offered: online activation and offline activation. The offline activation is a fall-back solution in the event that, for example, the online connection of the vehicle diagnostic tester in the workshop is unavailable at short notice.

1. Online activation (standard case)
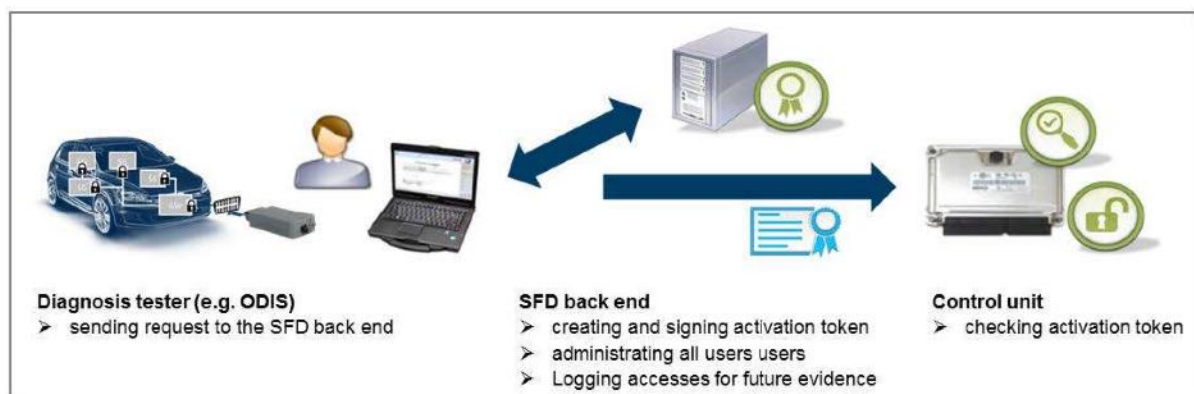
Components involved:

- The control unit in the vehicle contains the diagnostic objects to be protected and grants or refuses access.
- The vehicle diagnostic tester is operated by the user in order to select diagnostic objects in the control unit.
- The SFD back end contains the user database with authorizations and issues activation tokens.

Basic process:

1. It is a prerequisite that the user is registered in the SFD IT back end and in the Dealer Portal (in future, the Group Retail Portal).
2. The user would like to carry out SFD-protected services on one or more SFD-protected control units as part of a vehicle diagnosis.

3. The control unit reports that it is SFD-protected and asks for an activation token.
4. The vehicle diagnostic tester sends an activation request with the ID mark of the control unit and the desired scope to the SFD IT back end.
5. The SFD IT back end checks and authorizes the request and sends a signed activation token to the tester. The SFD IT back end logs the access (user ID, CU ID mark, time etc.).
6. The vehicle diagnostic tester sends the activation token to the control unit. The control unit checks the activation token and grants access to the relevant diagnostic object.

2. Manual SFD activation (offline – fall-back solution)

Process for an offline activation:

1. A direct online token generation with the vehicle diagnostic tester does not work.
2. The workshop employee saves the activation request structure of the control unit that will be necessary for the generation of the token.
3. The user logs into the Dealer Portal (in future, the Group Retail Portal) using a different computer and accesses the token generation website of the SFD back end via the SFD application.
4. The user enters the activation request structure of the control unit, generates an activation token with it, and copies this over to the vehicle diagnostic tester (e.g. using a USB stick).
5. The user executes a function on the tester in order to send the activation token manually to the control unit.
6. The control unit checks the activation token and grants access to the relevant diagnostic object.

Registration of users in the Dealer Portal and in the SFD IT back end

Upon the introduction of SFD in the first half of 2020, diagnostic users must be in a position to authenticate themselves in the SFD IT back end in accordance with the two activation options described above. In order to achieve this, it is necessary to register on the SFD back end in advance.

The local administrators of the Dealer Portal only have to assign the standard role in the "SFD" application to the affected users in the "Local user administration". Synchronisation with the SFD IT back end then takes place overnight, so the users are able to execute SFD-protected functions after no more than **24 hours**.

If there is no local administrator in your company, please contact the respective importer.

Authentication of users during the diagnostic session

1. Working with Guided Fault Finding (recommended)

In a diagnostic start-up via "Guided Fault Finding" (recommended), essentially nothing changes for the user, because upon logging into the Dealer Portal at the start of the diagnostic session, the login details are used automatically to generate the SFD activation tokens.

After this log in, necessary SFD activation tokens for work on the control units are generated automatically in the background.

After vehicle identification and reading DTCs you select an SFD-protected function (in the example, online coding) on an SFD-protected control unit (in example 15, Airbag):

Afterwards you have to log in again for online coding (Service 42 / SVM), as was also the case previously:
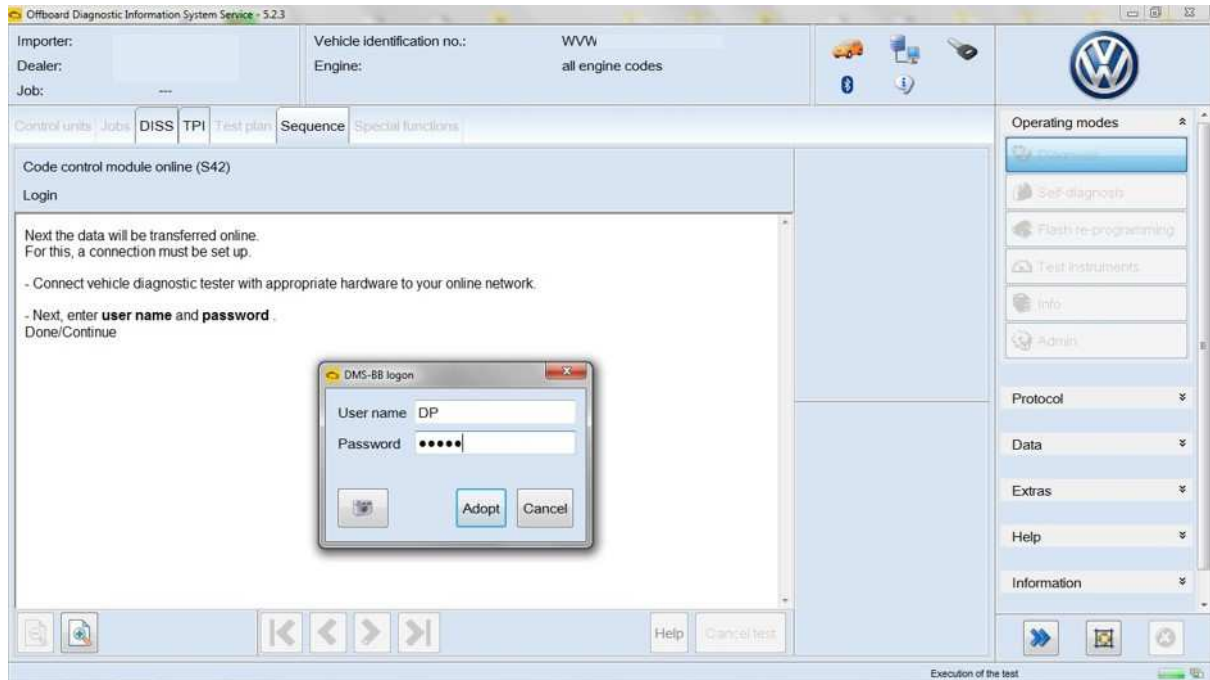
The SFD-protected airbag control unit has been automatically opened for the write operation and the coding has been carried out successfully:
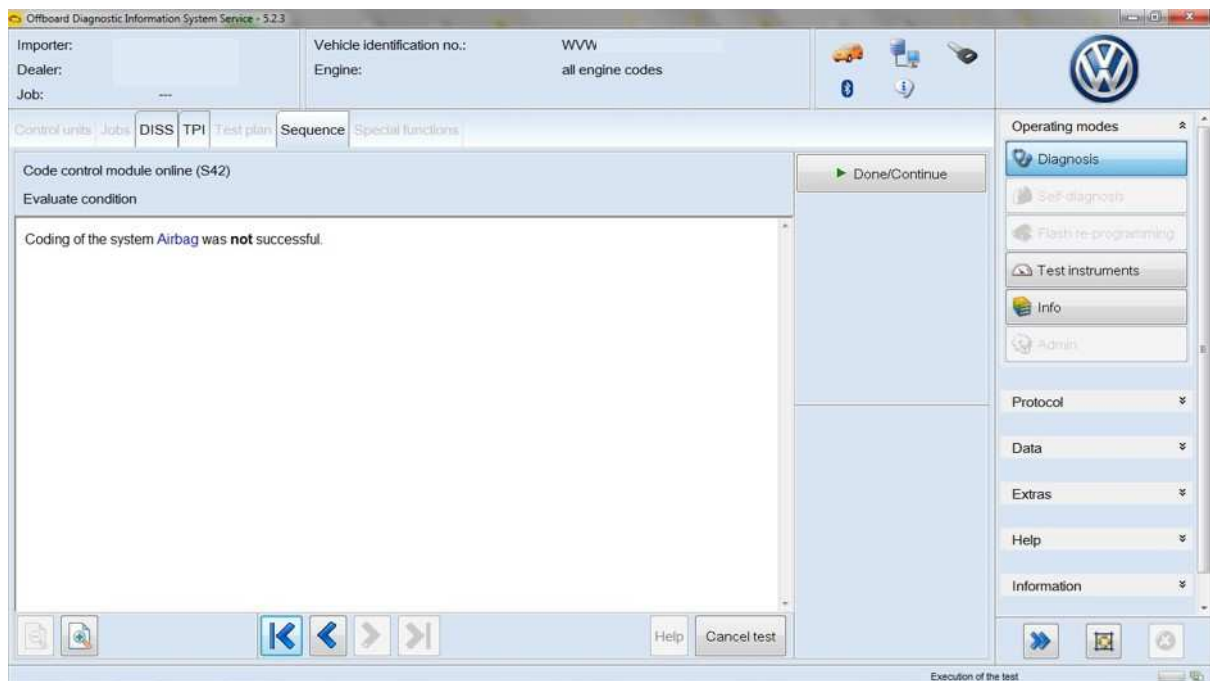
When using Guided Fault Finding SFD-protected control units are automatically locked at the end of the diagnostic session.

2. Working with Self-diagnosis: online activation

In a diagnostic start-up via "Self-diagnosis", after selecting a control unit you can establish whether the control unit is SFD-protected using the "Display measured values" function (Measured value [MAS 18157]_SFD activated status). In order to activate it, select the "Access authorization" option:
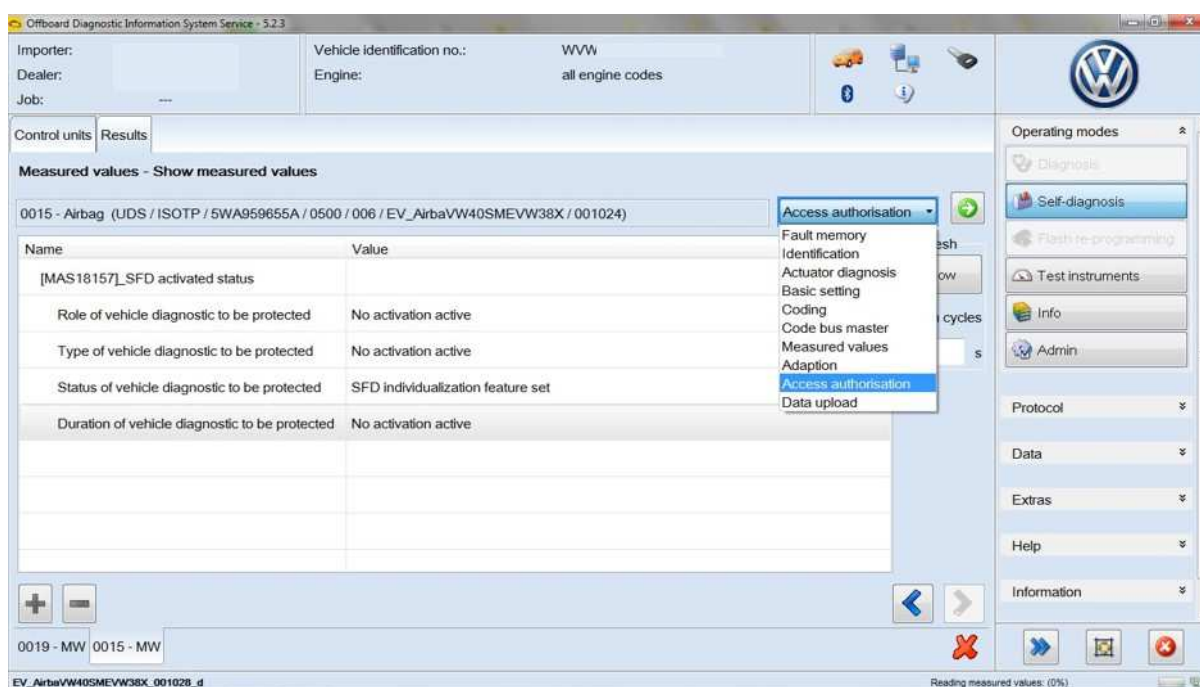
Then select the "Online activation" use case (standard case):
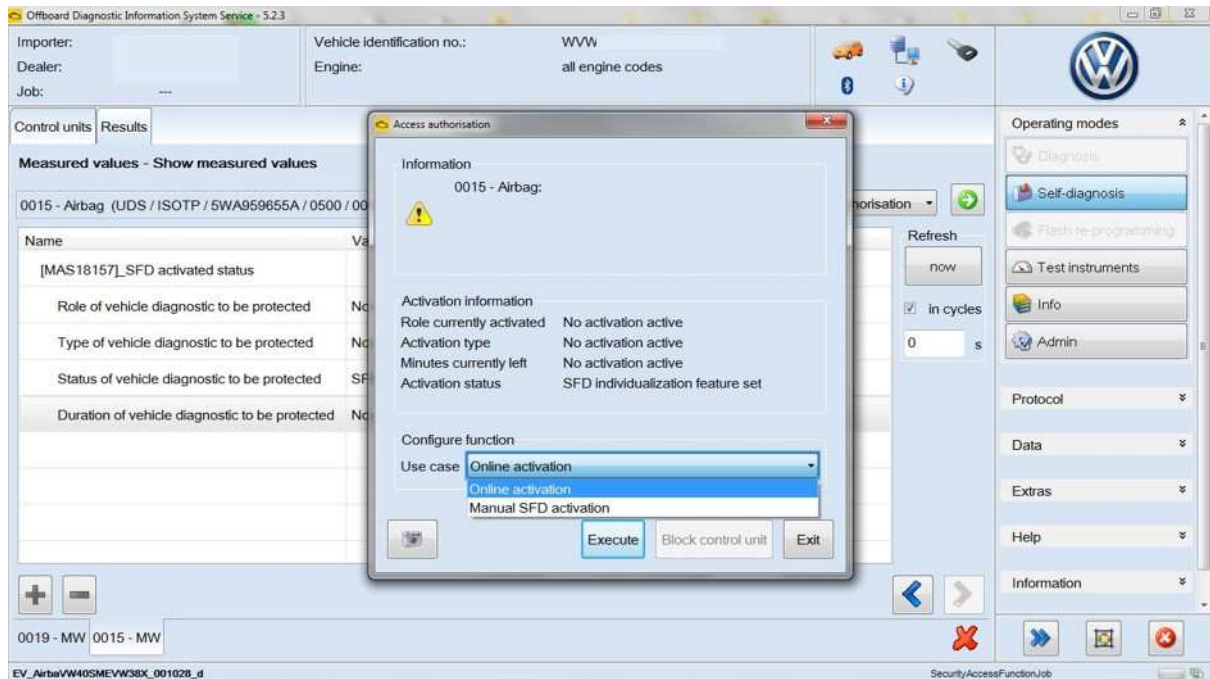
Then log in with your Dealer Portal login details:
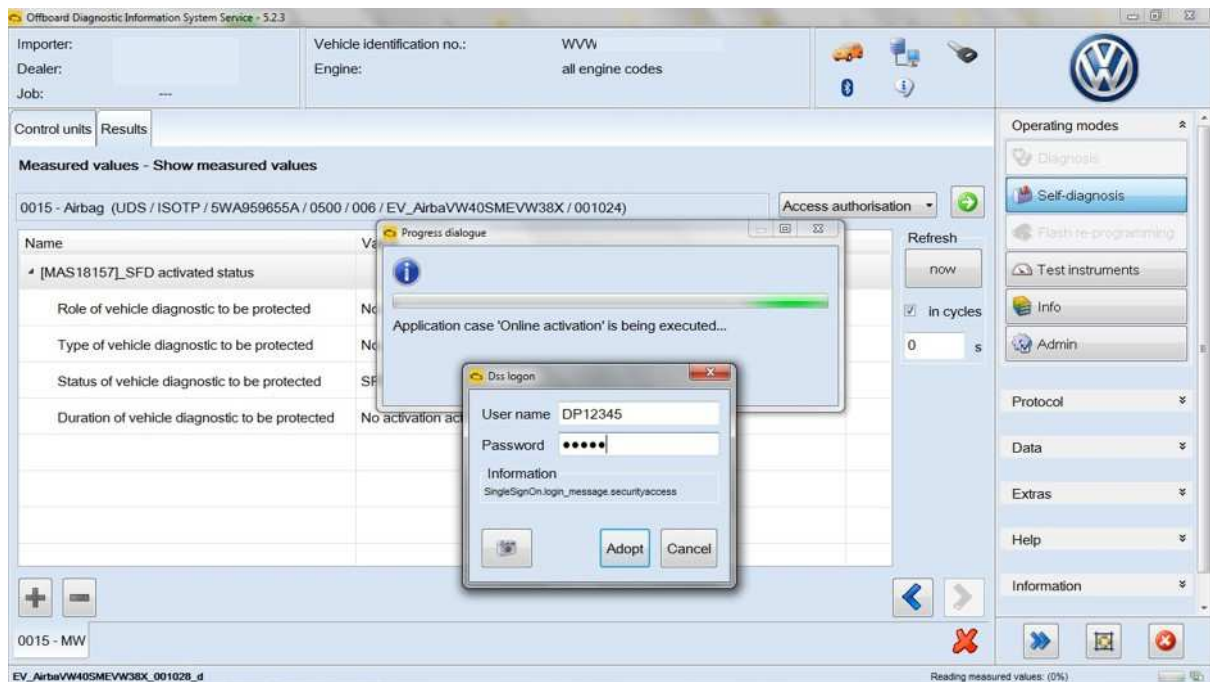
The activation status displays the activated role and the remaining activation period:
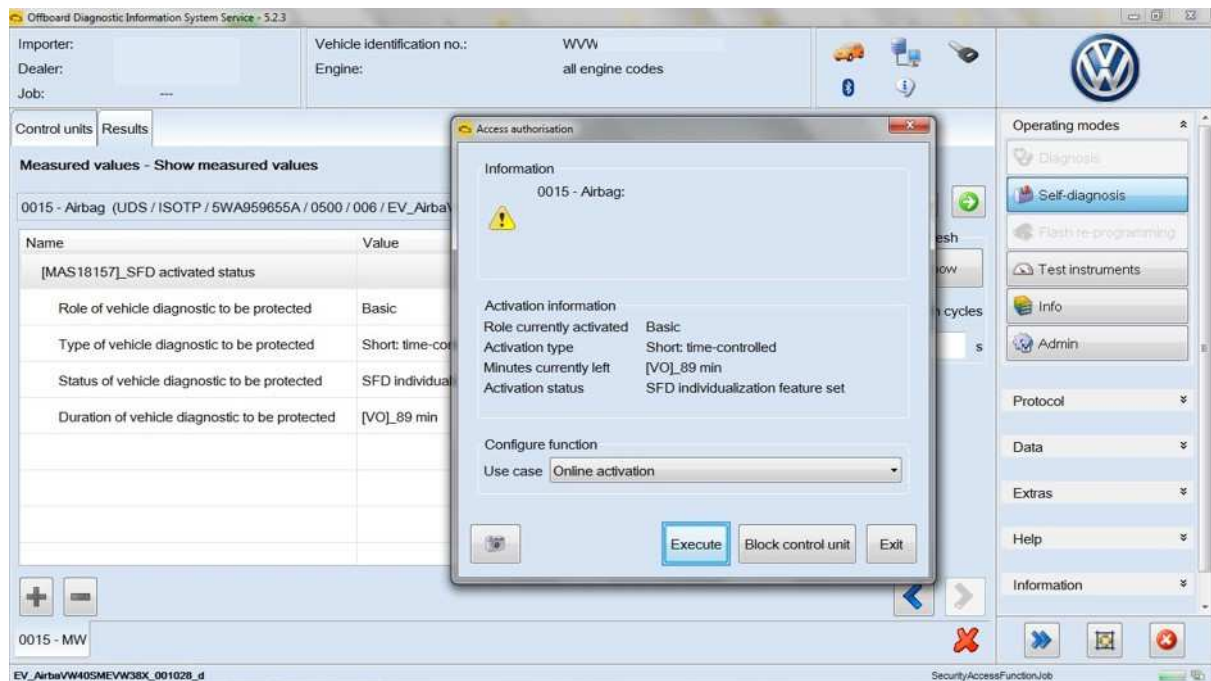
3. Working with Self-diagnosis: manual SFD activation (offline)

If there is no online connection from the vehicle diagnostic tester to the workshop network, after selecting "Access authorisation" select "Manual SFD activation":
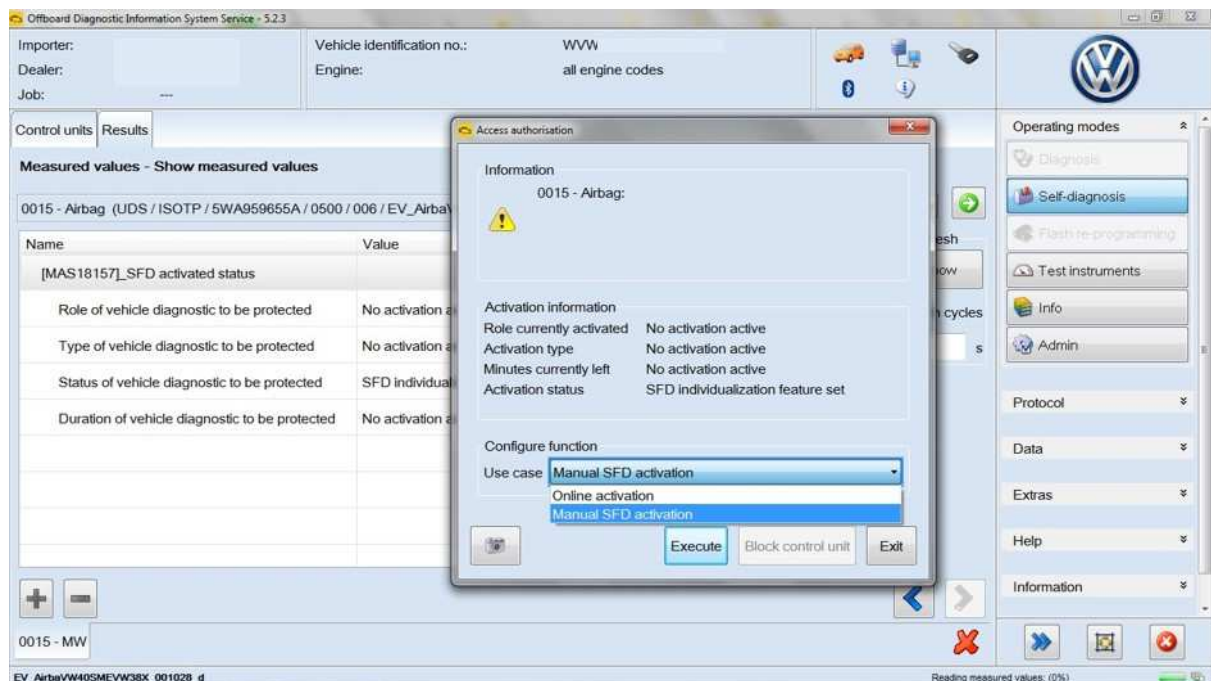
If an activation token has not yet been generated, answer "No" to the following question:
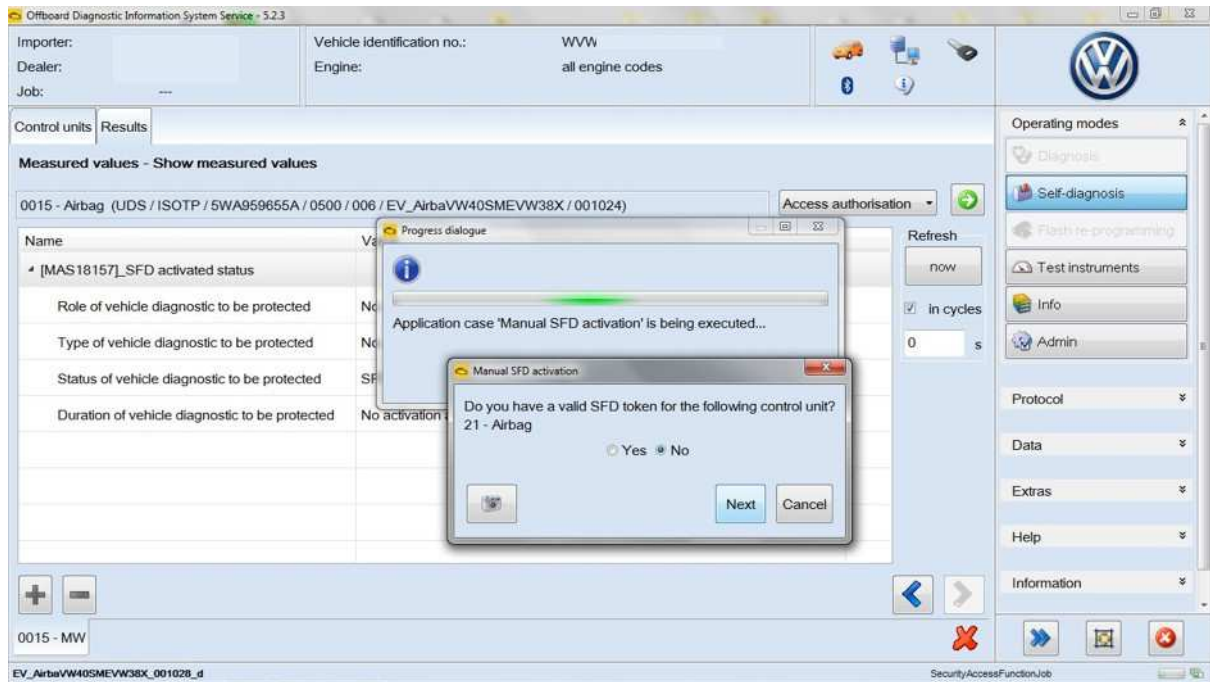
The activation request structure generated by the control unit is required so that the SFD back end can generate an activation token. You can now either copy the structure to the clipboard or save it in a file:
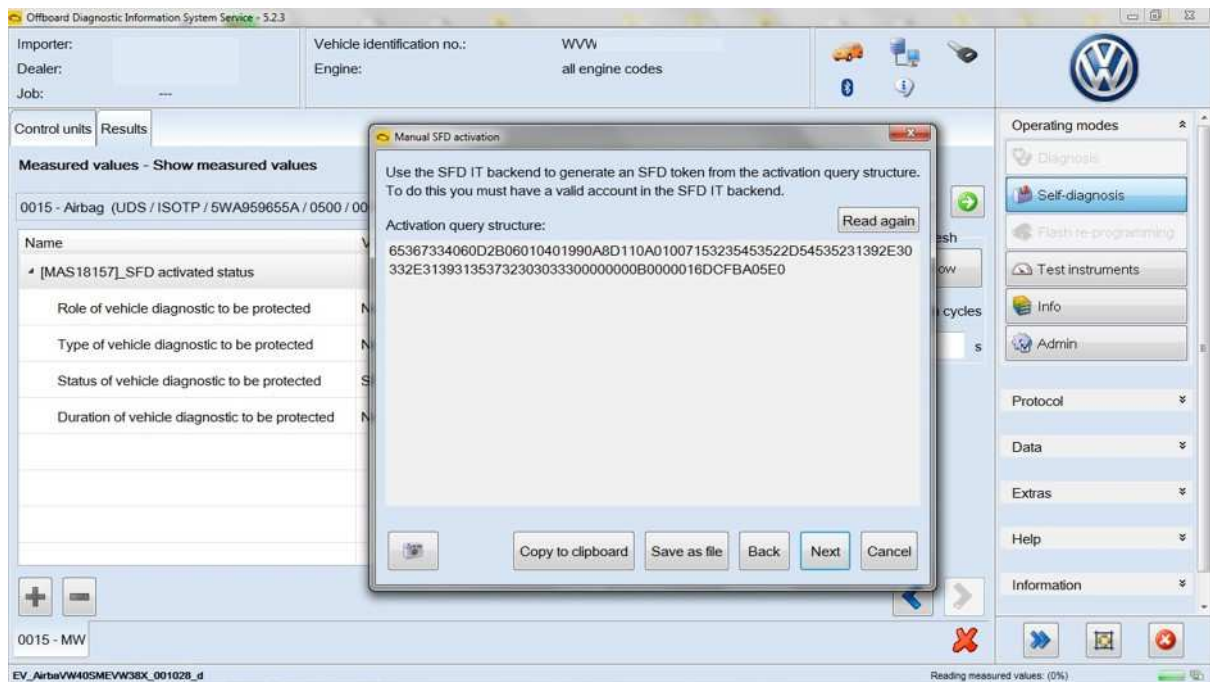
Then open the "SFD" application in the Dealer Portal:

Then you can access the token generation website of the SFD back end. There you enter the previously determined activation request structure and the vehicle identification number and select the brand:

The required activation token is generated by clicking on "Request a token":

Back in ODIS, once you have the required activation token, answer "Yes" to the following question:

Then enter the activation token, either via the clipboard or from a file:
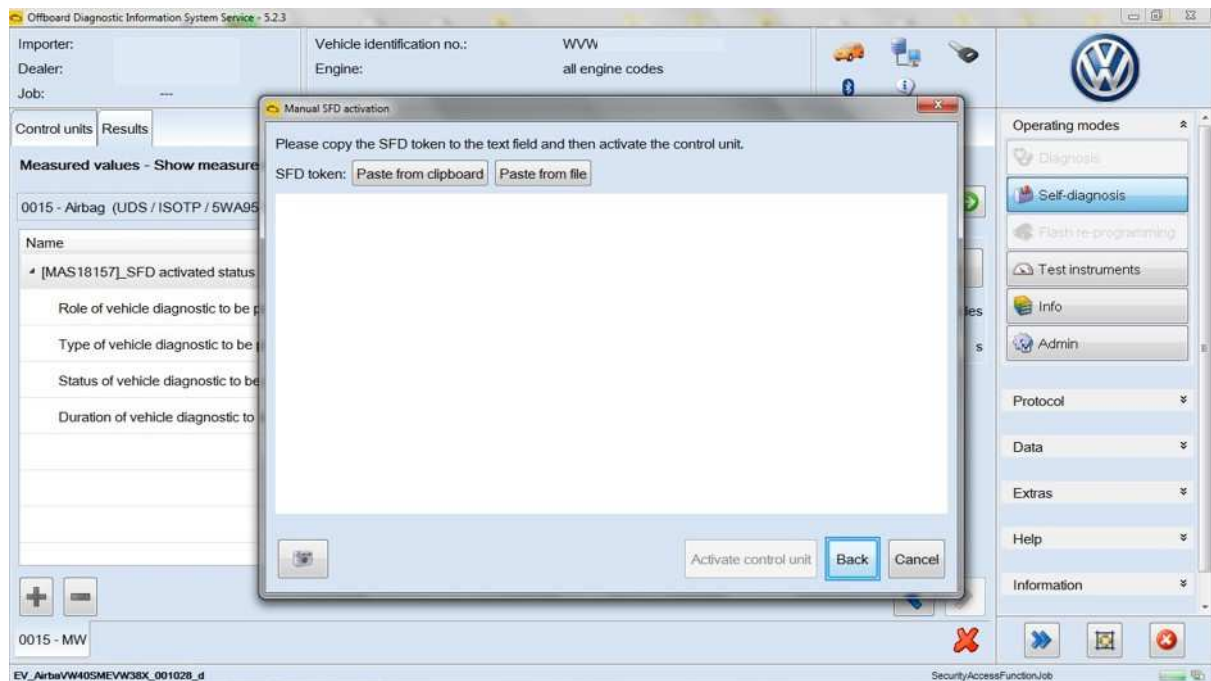
Please note:

Each activation token is specific to the control unit and usable only one time!!

4. Locking the control units again

When using Guided Fault Finding SFD-protected control units are automatically locked at the end of the diagnostic session. Otherwise they are also automatically locked again 90 minutes after activation.

Each control unit can also be locked again manually, however, by clicking the "Block control unit" button for an open control unit:
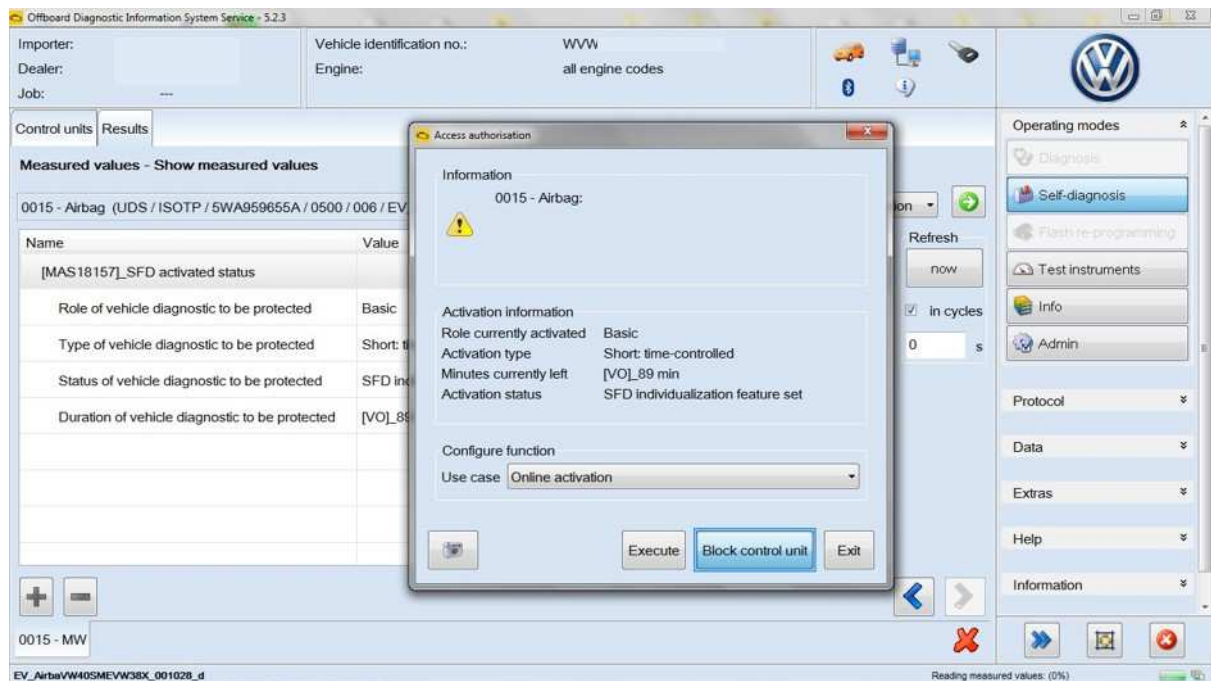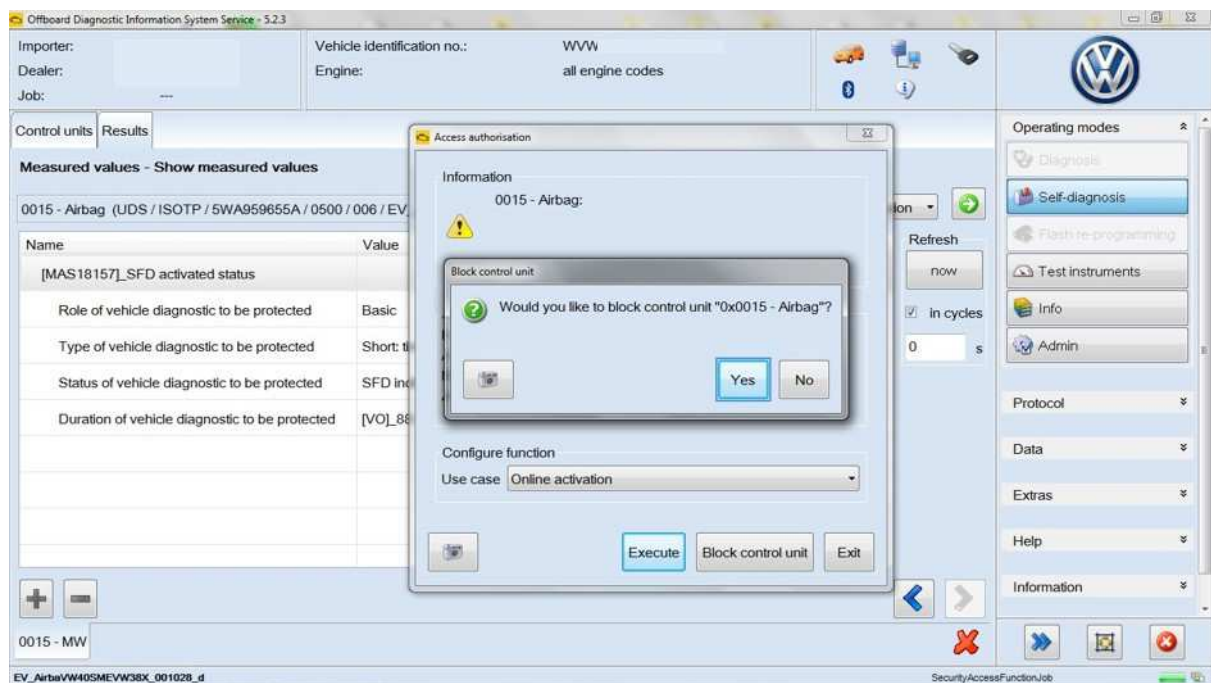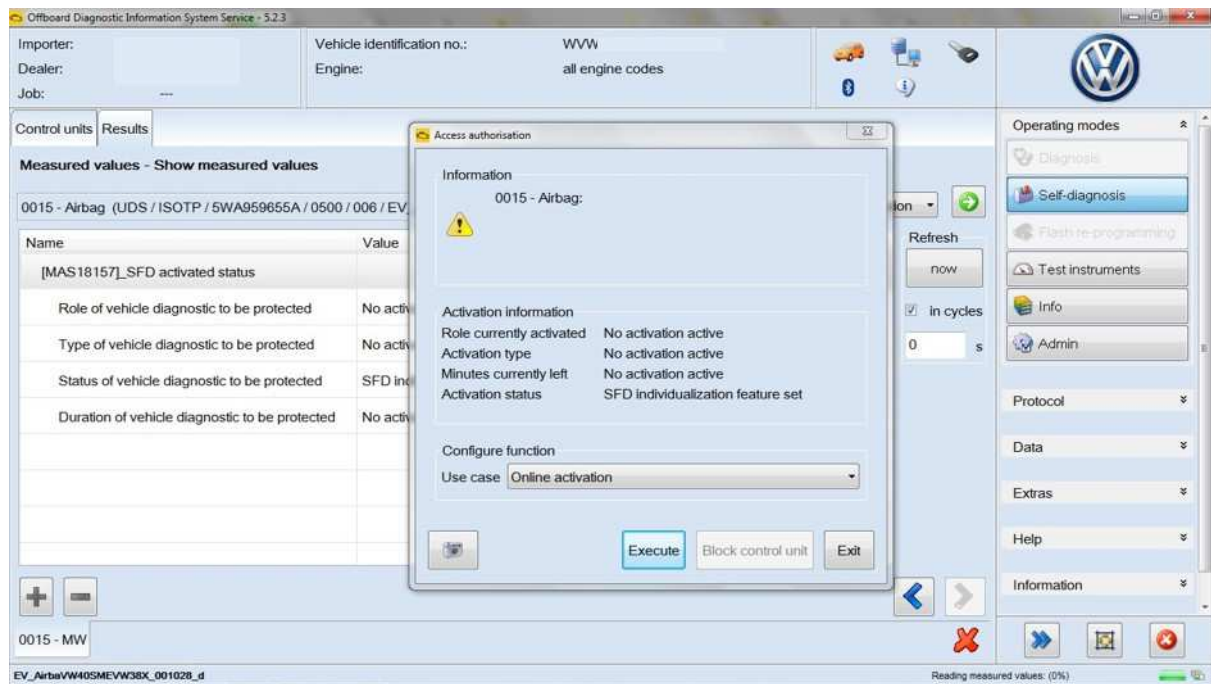
Answer "Yes" to the corresponding enquiry:

The activation status now shows that the control unit is locked. You can then activate it again:

Alternatively, all of the control units can also be locked at once by selecting "Block vehicle":
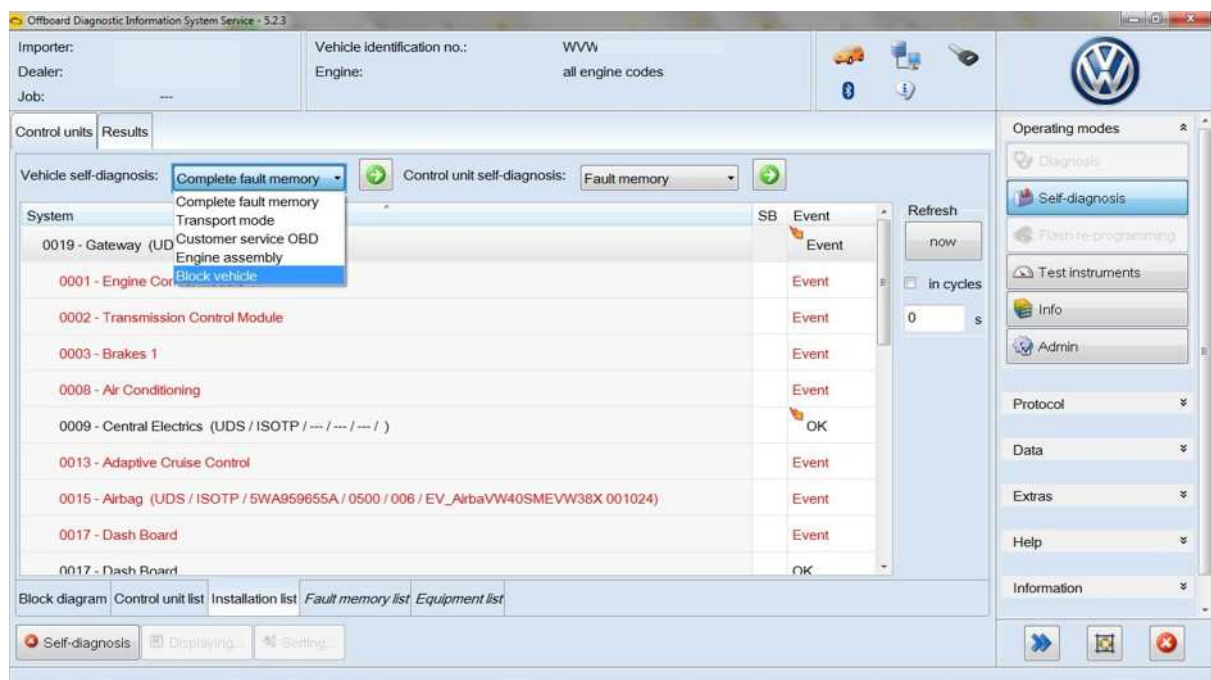
Then the locking of the vehicle is confirmed by clicking on "Yes".
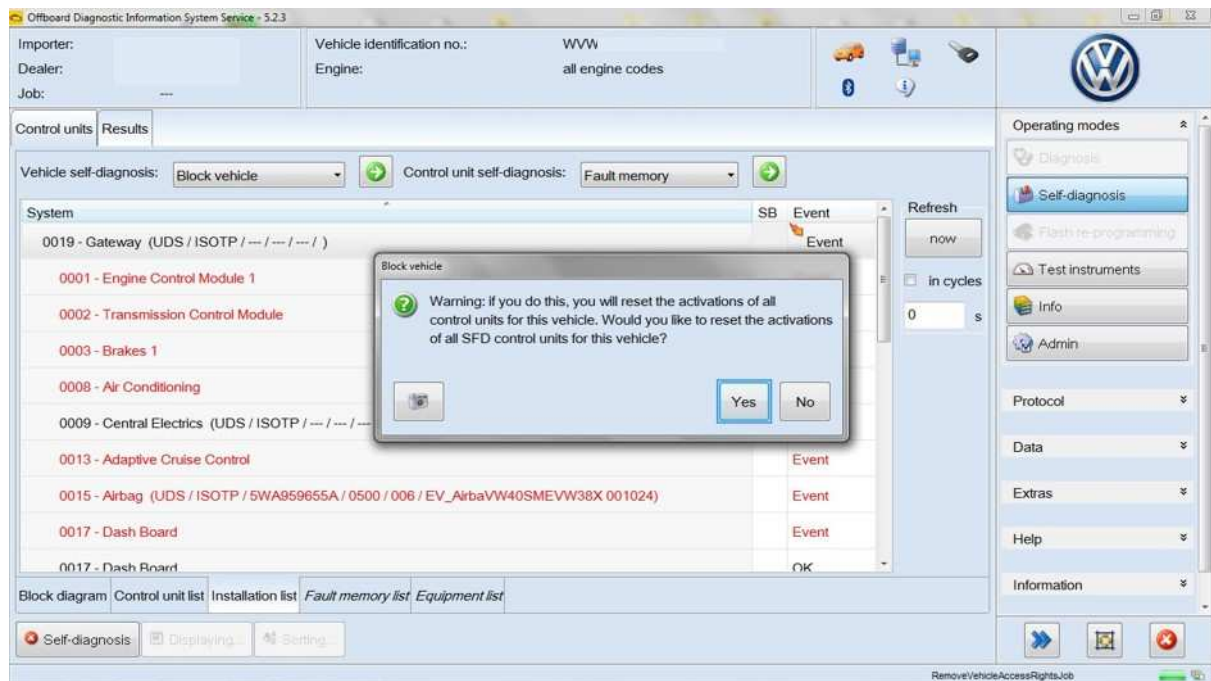
You will receive a response as to which control units have successfully been locked: