DB Secure Access Portal
Hardware Token User Guide

DB Systel GmbH

Hardware Token User Guide

Version 1.1

As of February 07, 2019

Contents:

1 Preliminary Note

The ActivIdentity token you have been given enables secure (strong) authentication for remotely accessing applications and other resources of DB AG. You need to activate the token before using it for the first time. This document explains how to do this.

To activate the token, you require:

- Your ActivIdentity token
- The serial number of the token. This can be found on the back of the token underneath the bar code (the ten-digit serial number after "S/N").
- A computer with an Internet connection and Web browser

Notes concerning the token:

- The token can generate eight-digit one-time passwords on demand. To obtain a one-time password, press the button on the token for 2–3 seconds. The number disappears after approximately 45 seconds.
- The token has an expected lifetime of around six years.
- Activating your token is a **one-time** procedure, which is necessary for security reasons.

To activate the token, proceed as follows:

1. Establish an Internet connection.
2. Start the Web browser and call the DB Secure Access Portal:

   https://db.de/token
3. Log in with your DB User and password.
4. Log off from the DB Secure Access Portal and disconnect from the Internet.

2 Token Activation

2.1 Establishing an Internet Connection

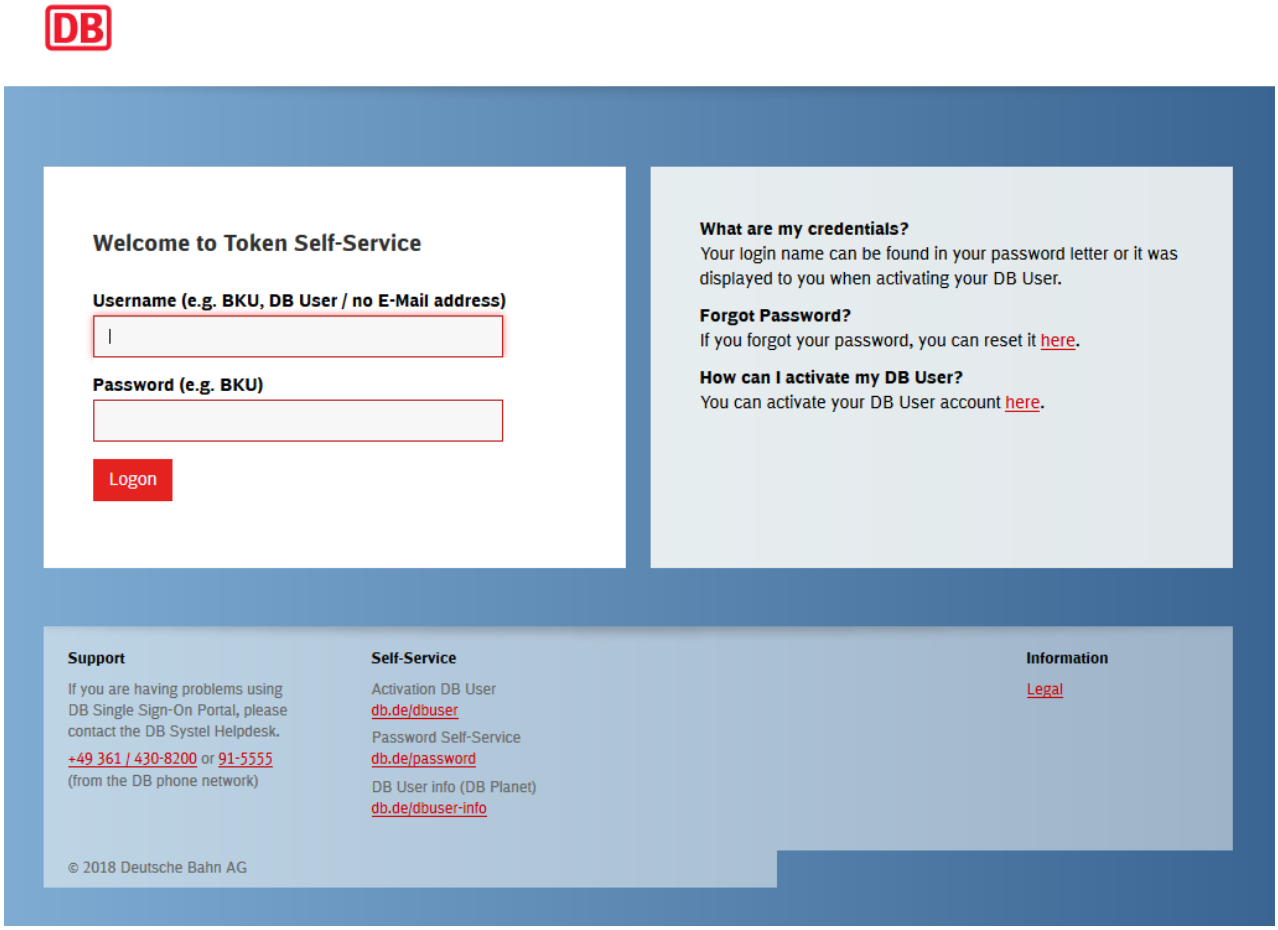
Before you can use the Token Self-Service, an Internet or intranet connection must be established.

2.2 Logging In with Your DB User

Launch the browser (preferably Chrome or Microsoft Internet Explorer) and enter the following link:

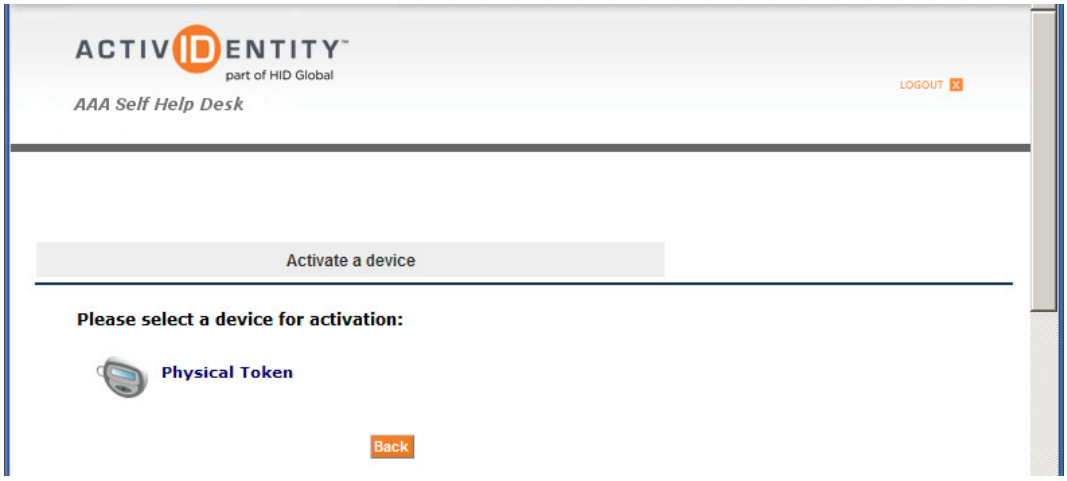
https://db.de/token

You are taken to the Token Self-Service and must first authenticate using your DB User and password:



2.3 Activation Steps

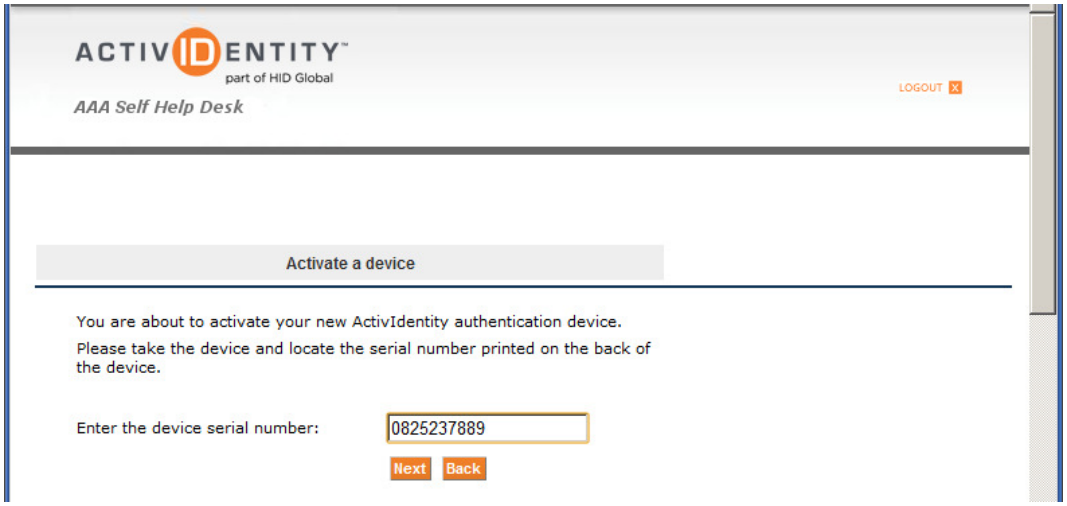
The system detects that your DB User has not yet been assigned a token and prompts you to choose the appropriate option:



Select "Physical Token" followed by "OK". The page is then displayed on which you need to enter the token serial number.

The ten-digit serial number can be found at the bottom of the label on the back of the token:

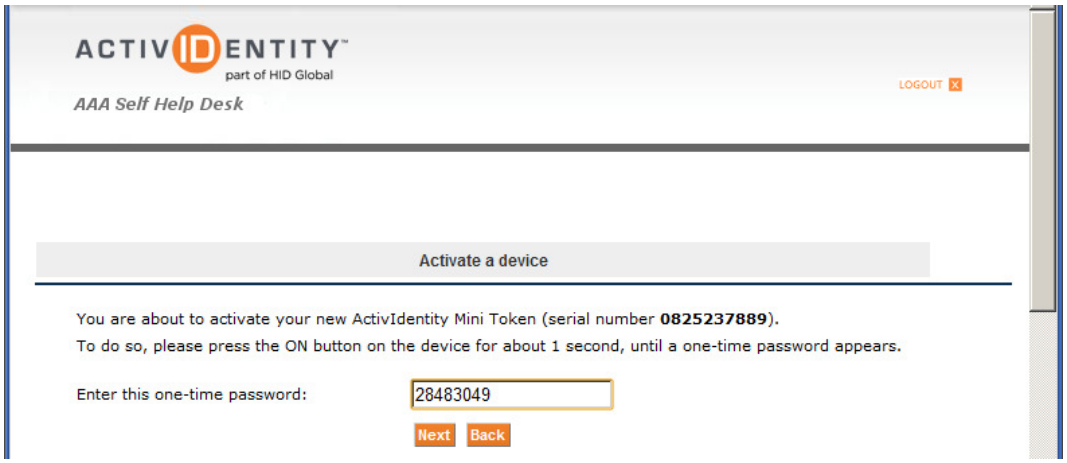
The ten-digit serial number can be found at the bottom of the label on the back of the token:



Then click "Next".

This takes you to the next page, on which the authentication check takes place for activating the token. To enable this, you first need to generate a one-time password using the token. Press the button for 2–3 seconds until an eight-digit number appears.

Note: The number disappears automatically after approximately 45 seconds.



Enter the one-time password displayed by the token in the corresponding field and click "Next". A page is now displayed on which you need to enter the PIN.

Whenever you dial in by means of strong authentication in the future, you will require both a PIN known only to you and the one-time password generated dynamically using the token (as is the case with the current RAS VPN solution).

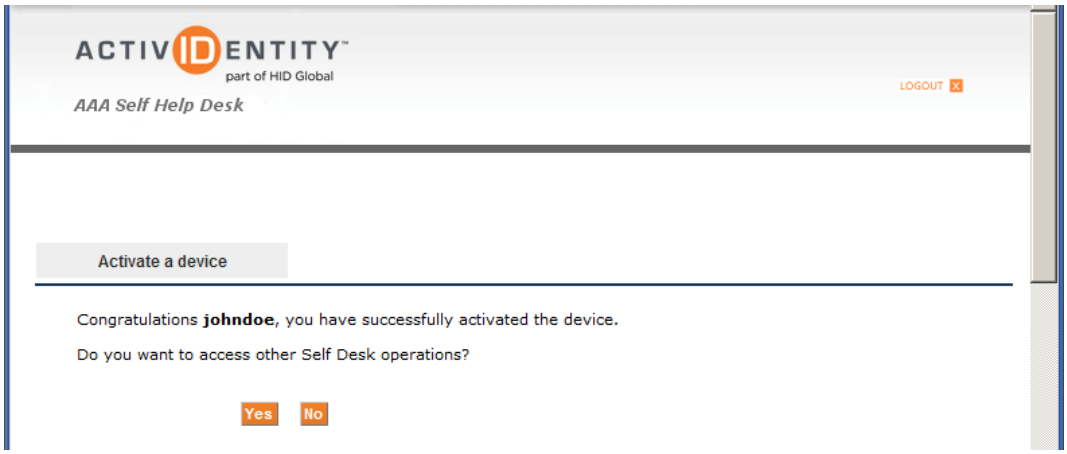
The DB AG security policy stipulates that this PIN must comprise between four and eight alphanumeric characters. Trivial PINs such as 1234 are rejected by the system. Do not use number combinations that can easily be guessed by others, such as your date of birth.

For security reasons, you should not disclose your PIN to anyone else. It is not recommended to write down your PIN. If you forget it, you can assign a new PIN at any time via the DB Secure Access Portal and Token User Self Service.

The PIN is disguised on the screen. For this reason, you need to enter it a second time in the "Confirm PIN" field for verification purposes. This prevents typing errors.

Then click "Set PIN" to assign the new PIN to the token.

Finally, a message appears stating that the token has been activated successfully.



To complete the token activation procedure, simply click "No" followed by the close icon (the X at the top right of the screen).

You have now activated your new token and can use it for authentication purposes with immediate effect.

3 Token Handling

3.1 Generate Token Code

This section explains how to generate a one-time password (token code) with the ActivIdentity Mini Token to log in to the DB Secure Access Portal.

1. Hold down the button until the token shows an eight-digit number.
2. On the login page, enter your DB User in the first field and your secret token PIN in the second field ("PIN + token code") followed by the token code generated in step 1.
3. Press the button again to turn off the token. Otherwise, the token will automatically switch itself off after about 30 seconds.

The generated token code will be validated after successful login and cannot be used again (one-time password functionality). Furthermore, it should be noted that the generated token code is limited and has a life span of 2 minutes. If it is not used within that time, it expires.

3.2 Defective Token

Please return defective tokens (due to an empty battery or a key that does not function properly) to DB Systel GmbH. Use the returns form on the last page of these instructions for this purpose.

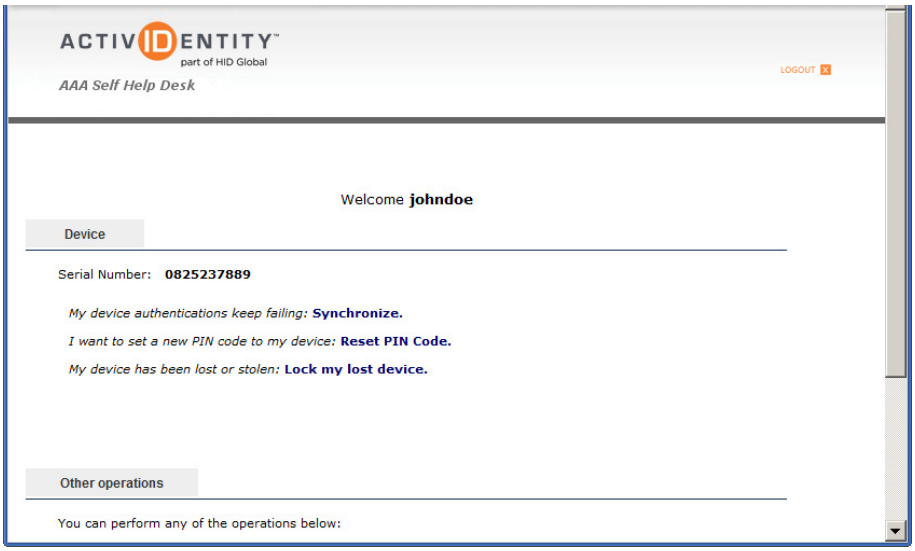
You are also advised to contact the Helpdesk DB Systel to arrange for a replacement token to be sent. In urgent cases, the Helpdesk DB Systel can set up emergency access, which temporarily allows you to use the RAS VPN solution without a mini token.

Important: If your token functions but you cannot log into the DB Secure Access Portal, refer to sections 3.3.1 Synchronize and 3.3.2 Reset PIN code and follow the instructions provided.

3.3 Token User Self Service

The Token User Self Service is a Web-based service that allows you to carry out various actions for your token. You can access the Token User Self Service by https://db.de/token

Once you have logged in, the following screen appears:



The following options are available:

1. Synchronize
2. Reset PIN Code
3. Lock my lost device

Further information about these options is provided in the following sections.

3.3.1 Synchronize

In rare cases, your ActivIdentity mini token may no longer be synchronized with the settings of the authentication server. This means that any authentication request will be unsuccessful. You will not be able to log

into the Portal although you seem to have entered all of your credentials correctly. This can be due to various reasons. First of all, make sure that you have entered your DB User and PIN correctly. If you are unsure, reassign your PIN as described in the previous section. If you still cannot log in successfully, the token must be resynchronized. This may be necessary for two reasons:

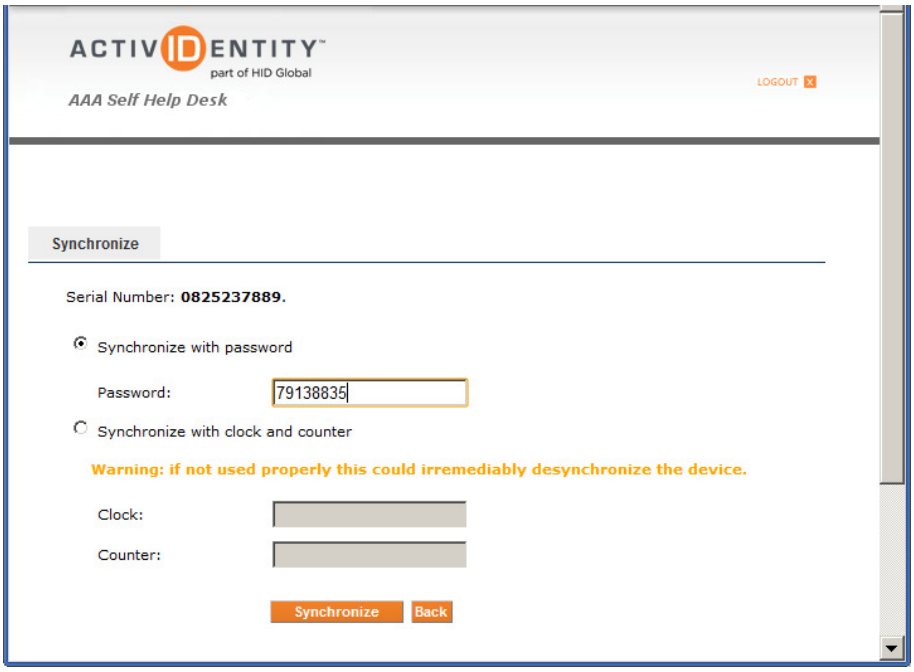
1. The internal clock is not within the permitted tolerances (in older tokens with weak batteries, the clock is usually slow).
2. The count is not within the expected window (this occurs when a token code is generated repeatedly (more than 30 times) and is not used for authentication).

Two options are available for resynchronizing your token. The first of these (which is the more straightforward option) involves using a one-time password, while the second resynchronizes the token using the internal counter and time. We recommend that you try variant 1 first. If this is unsuccessful, you can use variant 2.

3.3.1.1 Variant 1 – Synchronize with Password

On the AAA Web Help Desk, click "Synchronize". The first option ("Synchronize with password") is selected by default.

Create a one-time password with your token in the usual way and enter it in the field provided. In the example, the 8-digit password is 79138835:



Then click the "Synchronize" button. If synchronization was successful, the message "Successful resynchronization" appears in blue. If resynchronization was unsuccessful, the message "Resynchronization by password failed" appears in red.

In this case, carry out the steps described in the following section.

3.3.1.2 Variant 2 – Synchronize with Clock and Counter

To resynchronize your token, determine the time and counter on your token as follows:

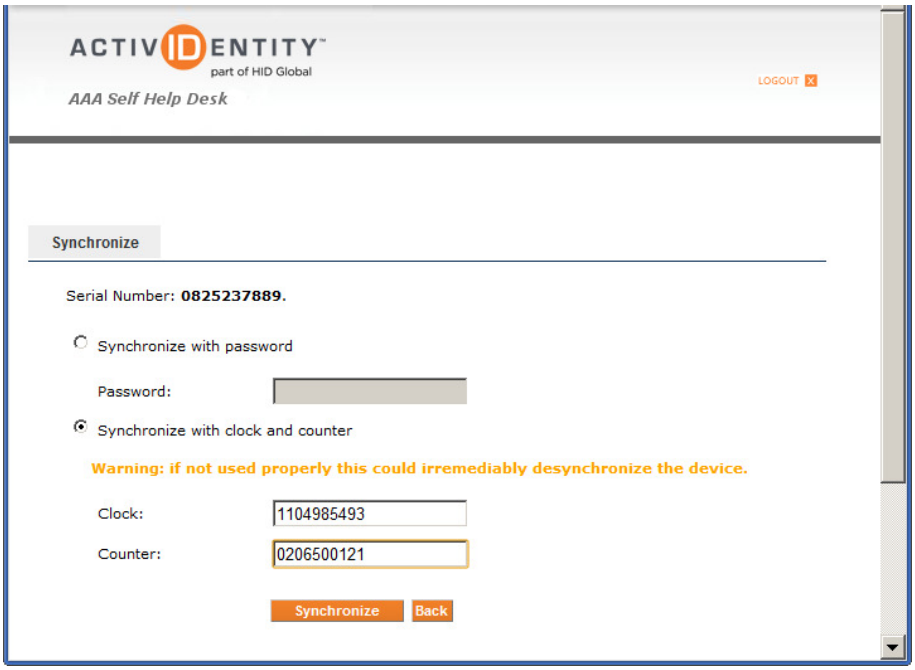
1. Press the button for 2 to 3 seconds until a one-time password is displayed.
2. Press the button again for 2 to 3 seconds until the token serial number is displayed. Two parts of a 10-digit serial number are displayed alternately:
   1. V Sn (abbreviation for **V**iew **S**erial **n**umber)
   2. 1 08252 (part 1 of the serial number)
   3. 2 37889 (part 2 of the serial number)

   The sequence is repeated three times. In this example, the 10-digit serial number is 0761134561 and is displayed for verification purposes only.

3. Press the button again for 2 to 3 seconds until the encoded time is displayed:
   1. V Clock (abbreviation for View Clock)
   2. 1 11049 (part 1 of the encoded time)
   3. 2 50083 (part 2 of the encoded time)

   The sequence is repeated three times. In this example, the 10-digit encoded time is 1004650083.
4. Press the button again for 2 to 3 seconds until the encoded count is displayed (in this example, 0546747638):
   1. V Count (abbreviation for View Count)
   2. 1 02065 (part 1 of the count)
   3. 2 00121 (part 2 of the count)

On the AAA Web Help Desk, choose "Synchronize with clock and counter" and enter the values as shown in the example:



Then click the "Synchronize" button. If resynchronization was successful, the message "Successful resynchronization" appears in blue. If resynchronization was unsuccessful, the message "Invalid clock" appears in red.

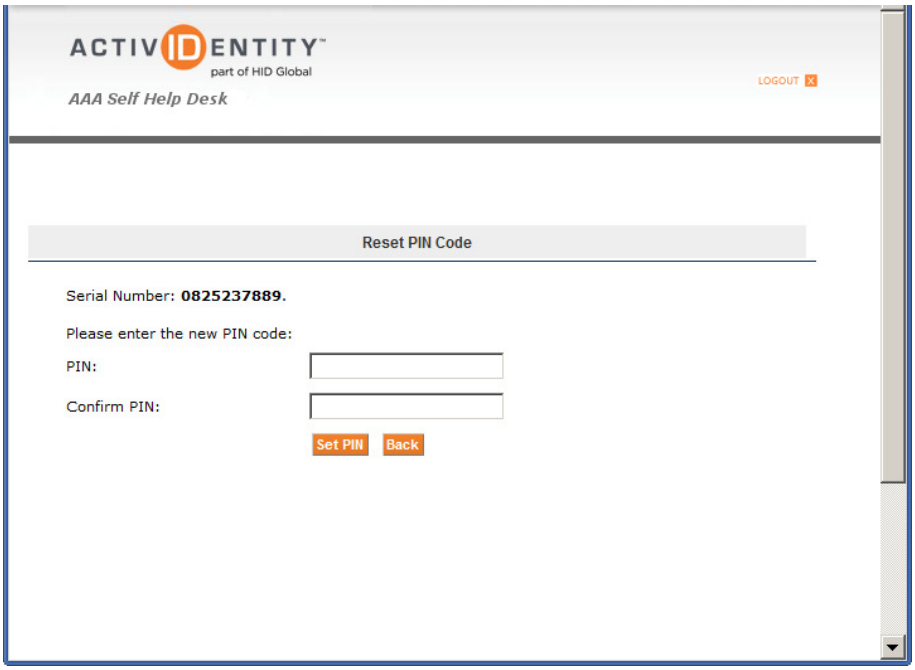
Experience has shown that the success rate of resynchronizing tokens with the clock and count is very high. Unsuccessful resynchronization is very often due to data being read or entered incorrectly. It is, therefore, advisable to carry out a test run with the token and to note the count readings. You will see that the values only change in the second part when this is repeated directly.

In extremely rare cases, the token cannot be resynchronized and must, therefore, be replaced. Please contact the staff of the Helpdesk DB Systel (see section 4.1) for this purpose, who will arrange for a replacement token to be sent.

3.3.2 Reset PIN code

You can change the PIN assigned to your token at any time. In the interests of security, you should do this if there is a risk of your PIN being disclosed to a third party, for example, through "shoulder sniffing". This function is also useful should you forget your token PIN.

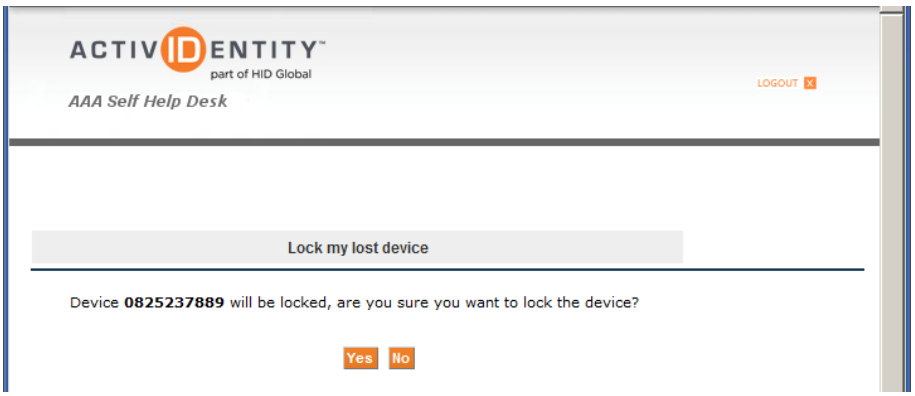
Once you have logged into the Token User Self Service, click "Change token PIN". The following dialog box appears:



Enter your new PIN, which must contain between four and eight alphanumeric characters (letters and numbers), in the fields provided and click "Set PIN"‘. Then click "LOGOUT" to close the session.

3.3.3 Lock My Lost Device

If you have lost your token or it has been stolen, you should report it as being lost and click the relevant option in the Token User Self Service to prevent it from being used further. Confirm the question shown below by clicking the "Yes" button:



The token will then be locked and cannot be used for the time being to log into the DB Secure Access Portal. If you find your token again, you can have it reactivated by contacting the Helpdesk DB Systel.

Please also report a lost or stolen token to the staff of the Helpdesk DB Systel (see section 4.1 Helpdesk DB Systel Contact Information on page 12), who will arrange for a replacement token to be sent. In urgent cases, the Helpdesk DB Systel can set up emergency access, which temporarily allows you to use the RAS VPN solution without a mini token.

4 Support Services of DB Systel

4.1 Helpdesk DB Systel Contact Information

If you have any further questions or problems, please contact the Helpdesk DB Systel on +49 (0)361-4308200 or 915555 (internal).

You can also contact the Helpdesk DB Systel by e-mail at Helpdesk.IT@deutschebahn.com.

DB Systel GmbH
Helpdesk DB Systel (RAS-VPN)
Weimarische Straße 42-44

D-99099 Erfurt

RAS VPN token return

Dear Sir/Madam,

Please find enclosed the following token(s):

Serial number:_____ (see reverse)

Reason for returning token:

☐ **Token is defective**

☐ **User account for RAS VPN cancelled**

Sender information (must be completed):

Company: _____

First/last name: _____

DB User: _____

Street: _____

Postal code, city: _____ _____