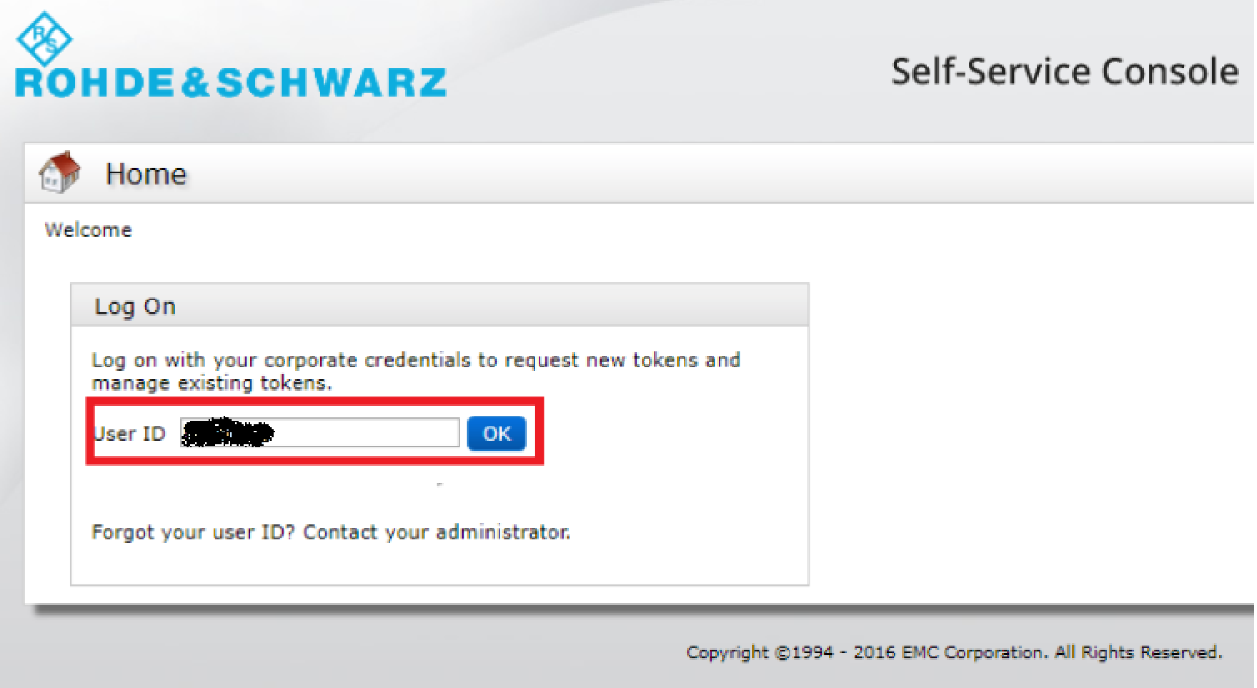
1. What is it?

A hardware token is a physical token device that you can use to generate “one time passwords” (OTP). If you do not have a compatible smartphone for a software token device or there are any other reasons why you would want a dedicated device, this is the right choice.

2. What do I need and how do I get it?

There aren’t any special prerequisites for hardware token devices. You will need physical access to your token device to generate OTPs, so think about a good place to store or attach it to (preferably your key ring or R&S badge**). Please note the activation period is limited to 14 days starting from the day your token got assigned to your user. If the token is not activated during the 14 days, it will be automatically unassigned.**

1. Request your hardware token in our R&S IT-Service Portal. You can find the request under “OTP Token Request”
2. After our Service Desk has assigned the token, you will need to pick it up from the Service Desk (Munich) or from the local admin (outside of Munich).
3. To set your PIN, go to our Self Service Console: https://otptoken.rohde-schwarz.com .
4. Please enter your Windows username in the field “User ID” and press “OK”.



ROHDE&SCHWARZ

Self-Service Console

Home

Welcome

Log On

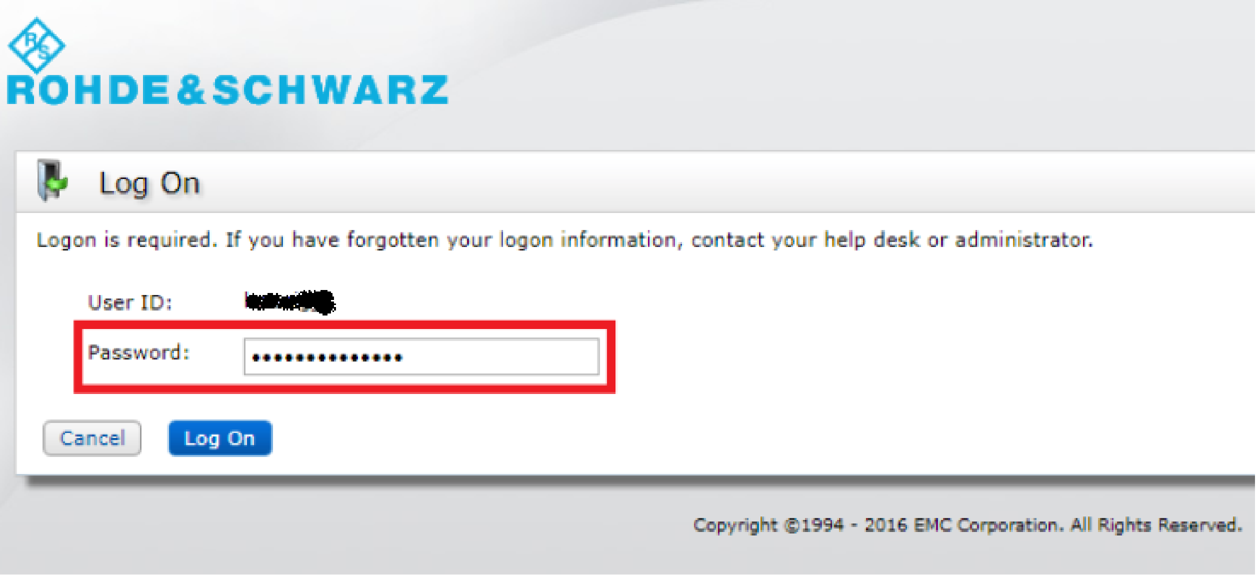
Log on with your corporate credentials to request new tokens and manage existing tokens.

User ID [redacted] OK

Forgot your user ID? Contact your administrator.

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

5. In the next screen, enter your Windows password in the field “Password” and press “Log On”.



ROHDE&SCHWARZ

Log On

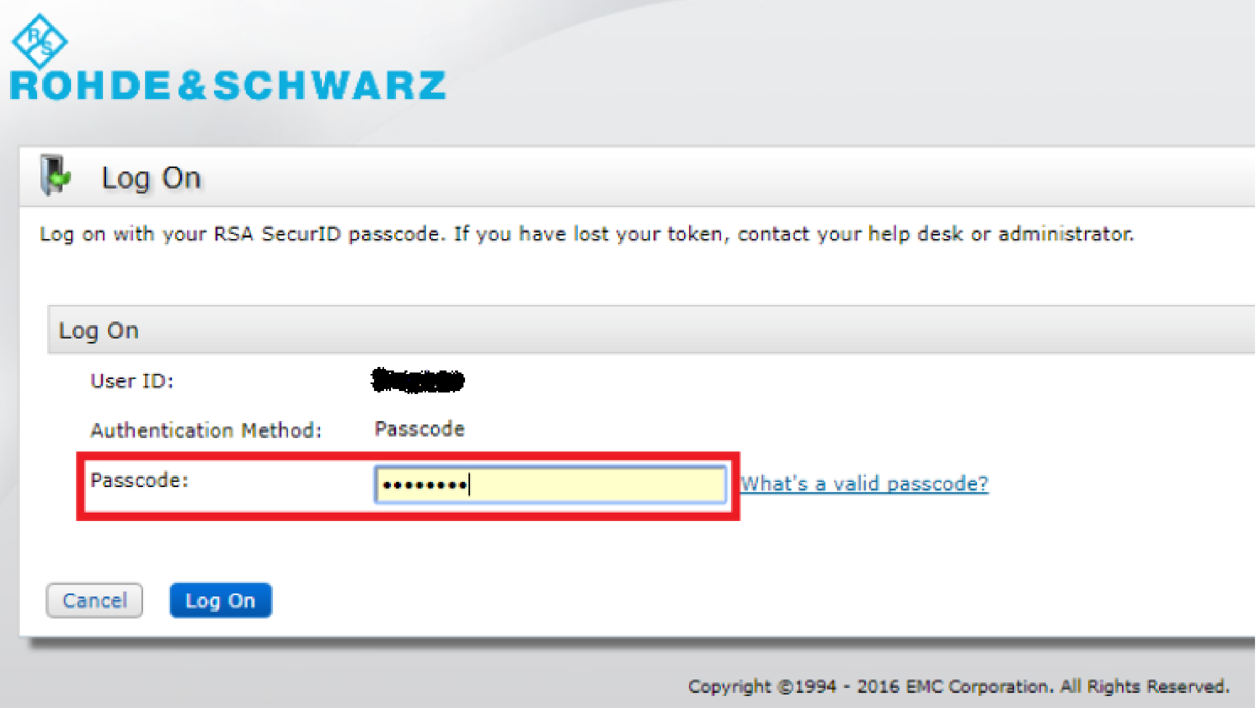
Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID: [redacted]

Password: •••••••••••••••

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

6. Look at your hardware token. Please enter the displayed six-digit number in the field “Passcode” and press “Log On”.



ROHDE&SCHWARZ

Log On

Log on with your RSA SecurID passcode. If you have lost your token, contact your help desk or administrator.

Log On

User ID: [redacted]

Authentication Method: Passcode

Passcode: •••••••••

What's a valid passcode?

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

7. Think about a PIN you want to use each time you generate an OTP.

   A valid PIN consists of four to eight numbers.

   Please do not use a PIN with a leading zero!

8. Enter your PIN in the fields “New PIN” and “Confirm New PIN”.

9. For the field “Next Tokencode” you have to construct an OTP with your new PIN. Look at your hardware token again and wait for the code to change (new 6-digit number). The bars on the left side of the display indicate how long this will take. Append the displayed code to your PIN and you will get a valid OTP.

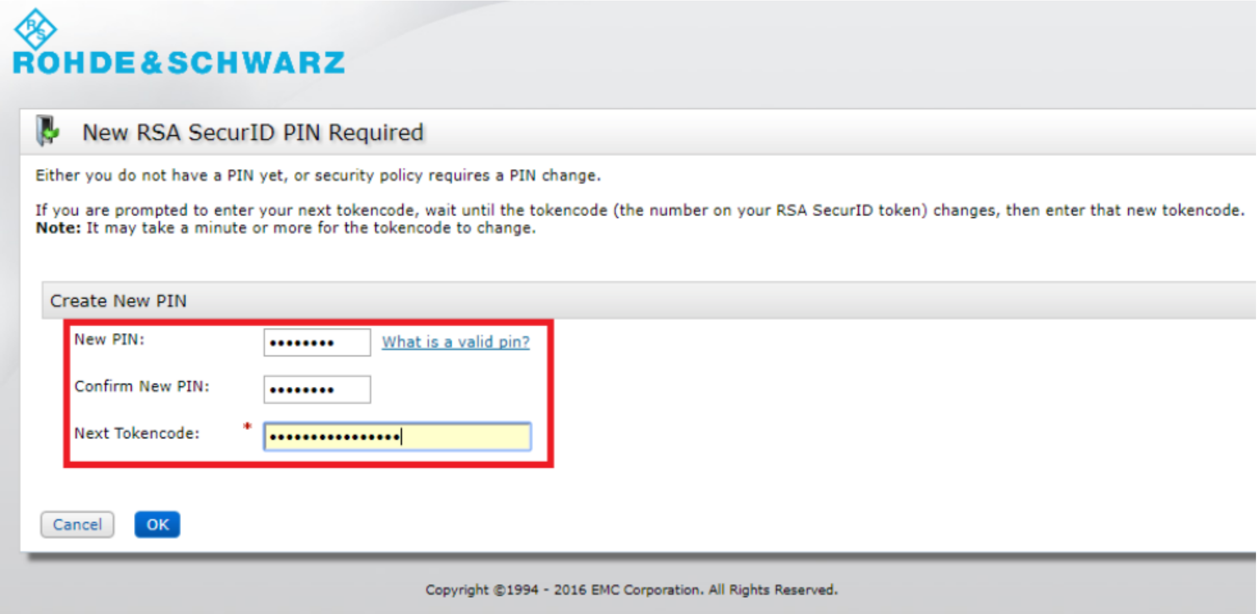
   Here is an example:

   Let us say your PIN is: 12345678

   The currently displayed code is: 159759

   Your currently valid OTP is: 12345678159759

10. Enter the so constructed OTP in the field “Next Tokencode” and press “OK”.



New RSA SecurID PIN Required

Either you do not have a PIN yet, or security policy requires a PIN change.

If you are prompted to enter your next tokencode, wait until the tokencode (the number on your RSA SecurID token) changes, then enter that new tokencode.
Note: It may take a minute or more for the tokencode to change.

Create New PIN

New PIN: •••••••• What is a valid pin?

Confirm New PIN: ••••••••

Next Tokencode: * ••••••••••••••••

Copyright ©1994 - 2016 EMC Corporation. All Rights Reserved.

11. You should now see all your currently assigned token devices. Congratulations, your PIN is now set and your token device is fully operational.

3. How to generate an OTP?

To construct an OTP please append the currently displayed code to your PIN – that’s it!

Here is an example:

Let us say your PIN is: 12345678

The currently displayed code is: 159759

Your currently valid OTP is: 12345678159759

Please take note of the following:

- The bars on the left side of the display indicate how long the currently displayed code (and so your constructed OTP) is valid. After all bars disappeared, you will get the next code to construct your OTP.

- If authentication fails, it’s a good practice to go back to the start screen, enter your PIN again and wait for the OTP to change before the next authentication attempt.