

B2B introduction

- The main purpose of B2B Portal is to provide ŠKODA AUTO employees and their business partners (importers, dealers, etc.) important information and access to application of ŠKODA AUTO.
- This interactive guide will help you with the basic operations.

Get access

Security options

Login

Password reset

FAQ

Get access

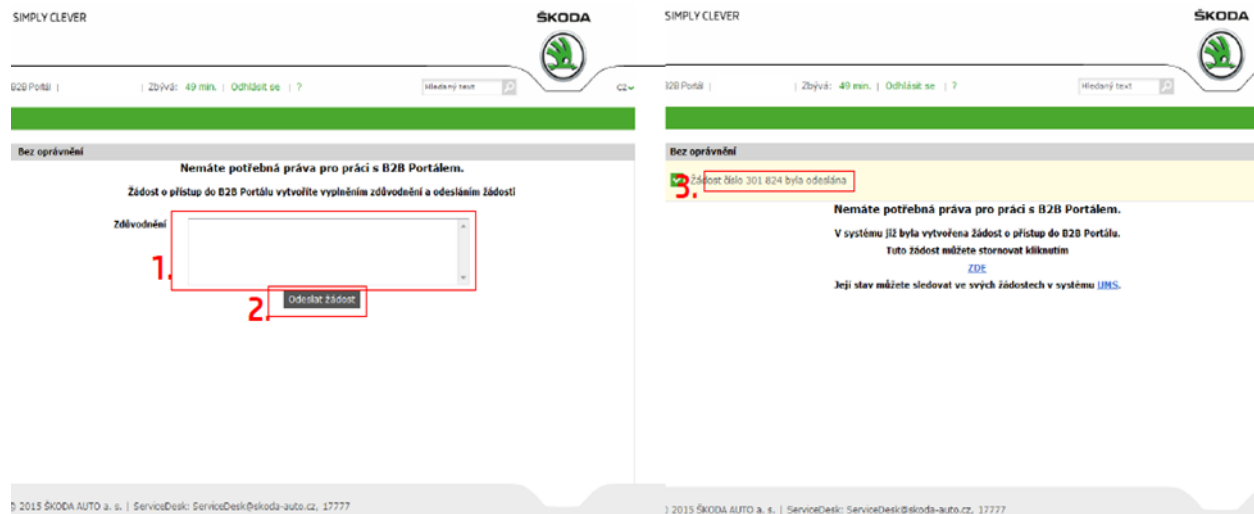
ŠKODA AUTO employees

Other B2B users

ŠKODA AUTO employees

For the first access:

- Open this URL: <https://Bportal.skoda.vwg>
- Fill the reason.
- Choose Send request.
- Your request has been created.



Continue

ŠKODA AUTO employees

- After the new account creation, you will receive instruction for password setting, username (your DZC) and email with certificate. In order to access B2B Portal you will only need the username + password. However, it is also possible to use the certificate to log in, you can find help in this manual.

Password rules

- The password can not be identical to your username.
- The password must be a combination of letters and at least one special character.
- The system remembers the last 6 passwords – those can not be used as a new password.
- The validity of password is 90 days.

Other B2B users

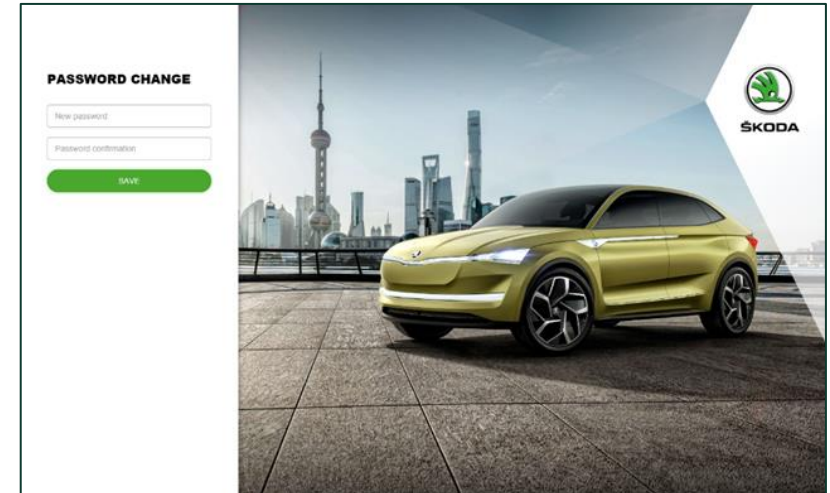
- For the first access to B2B Portal, please contact your OrgAdmin and he will create an electronic request.
- Backup solution is [this paper form](#) (send filled to: b2bhelp@skoda-auto.cz).
- After the new account creation, you will receive instruction for password setting, username and email with certificate. In order to access B2B Portal you will only need the username + password. However, it is also possible to use the certificate to log in, you can find help in [this manual](#).

Password rules

- The password cannot be identical to your username.
- The password must be a combination of letters and at least one special character.
- The system remembers the last 6 passwords – those passwords cannot be used as a new password.
- The validity of password is 90 days.

*extra for users from Poland

- Every password must be a combination of at least one lowercase and uppercase letter, number and a special character.
- The validity of password is 30 days.



Login

Basic

Two-factor

Basic login

Username + password

Certificate + password

Other login methods

Two-factor login

Username + password + one-time password from SMS

Username + password + one-time password from Authenticator

Username + Tokencode

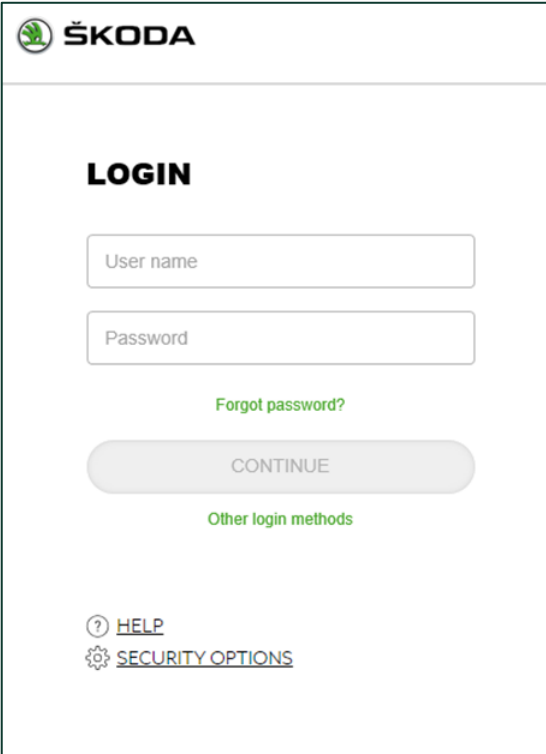
PKI (Employees ID card) + PIN

Only for
ŠKODA AUTO
employees

Username + password

Login instructions:

1. Enter the required URL.
2. Fill in:
 - Username.
 - Password.
3. You are logged in.

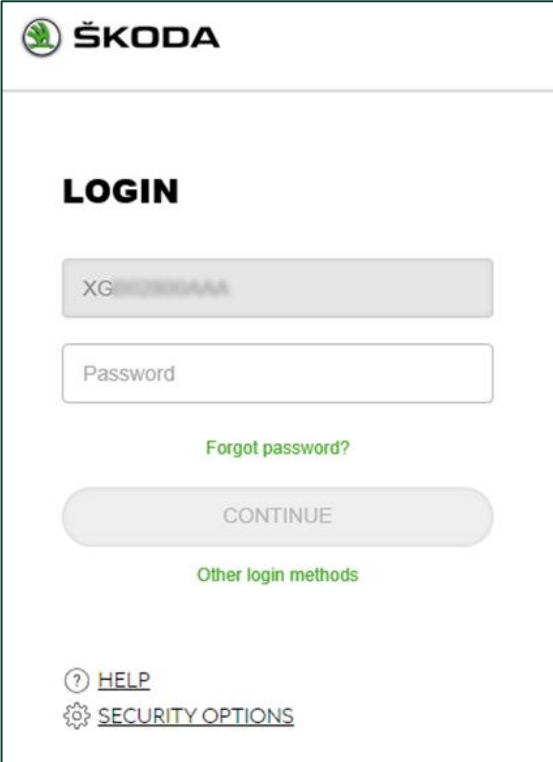


The screenshot shows the ŠKODA login interface. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is displayed in bold. There are two input fields: "User name" and "Password". Below the "Password" field is a link for "Forgot password?". A large, rounded "CONTINUE" button is centered below these elements. Underneath the button is a link for "Other login methods". At the bottom left, there are two links: "HELP" with a question mark icon and "SECURITY OPTIONS" with a gear icon.

Certificate CA Partner + password

Login instructions:

1. Enter the required URL.
2. The available certificates are displayed in the browser. Choose the appropriate one.
3. Fill in:
 - Password.
4. You are logged in.



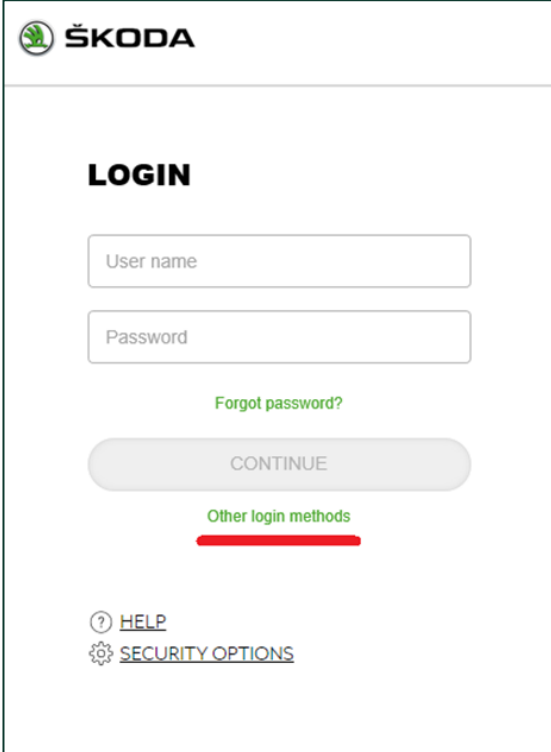
The screenshot shows the ŠKODA login interface. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is displayed in bold. There are two input fields: the first is labeled "XG" and contains a masked value "XXXXXXXXXX"; the second is labeled "Password". Below the password field is a green link "Forgot password?". A large, rounded "CONTINUE" button is centered below the links. At the bottom of the form area is another green link "Other login methods". At the very bottom of the page, there are two links: "? HELP" and "⚙️ SECURITY OPTIONS".

Other login methods

- Link is available in the 'Basic login' screen only.
- User can use higher authentication levels after clicking the link „Other login methods“.

Login instructions:

1. Enter the required URL.
2. Click on 'Other login methods'.
3. Based on chosen method, follow instructions for: [SMS](#), [Authenticator](#), [RSA Tokencode](#).



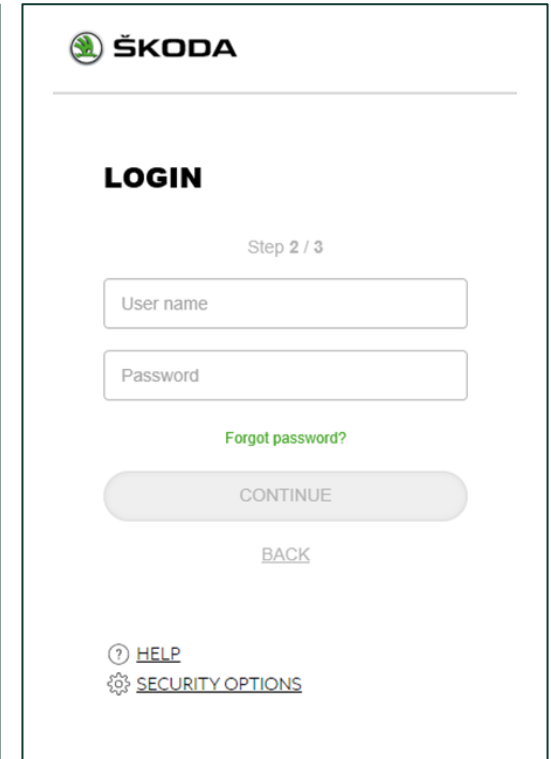
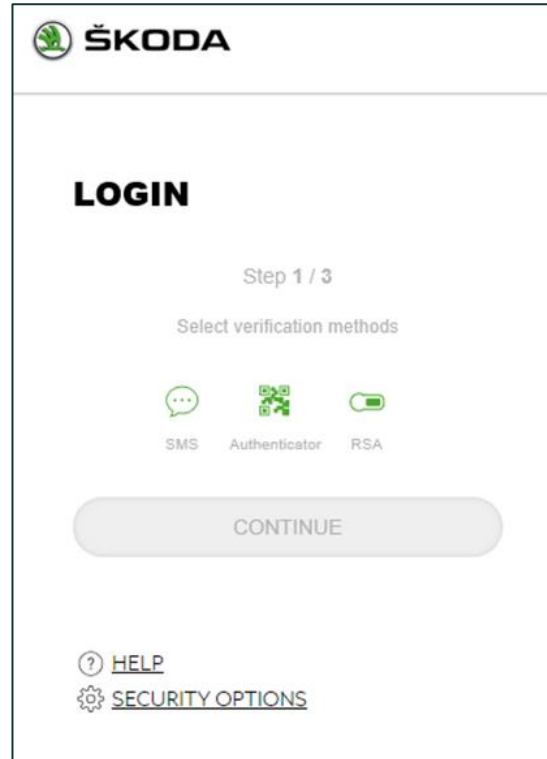
The screenshot shows the ŠKODA login interface. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is displayed in bold. There are two input fields: "User name" and "Password". Below the password field is a link "Forgot password?". A large, rounded "CONTINUE" button is centered below these elements. Underneath the button is the link "Other login methods", which is underlined in red. At the bottom left, there are two links: "HELP" (with a question mark icon) and "SECURITY OPTIONS" (with a gear icon).

Username + one-time password from SMS

– It's necessary to registrate the device first.

Login instructions:

1. Enter the required URL.
2. Choose the method of authentication via SMS and confirm.
3. Enter:
 - Username.
 - Password.



Continue

Username + password + one-time password from SMS

- This step is skipped based on following rules:

In case the user has more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and continues to step 5.

In case the user has only one device registered and activated, the device is chosen automatically, and user is redirected to next step directly.

- Enter the code from SMS.
- You are logged in.

ŠKODA

LOGIN

Step 3 / 3

Select device

TEST 1 (+44123456789)

TEST 2 (+44987744522211)

SMS with authentication code will be send to the chosen phone.

SEND SMS

[BACK](#)

ŠKODA

LOGIN

Step 3 / 3

Selected device

TEST 2 (+44987744522211)

Copy the code in SMS.

Verifying code

VERIFY

[RESEND SMS](#)

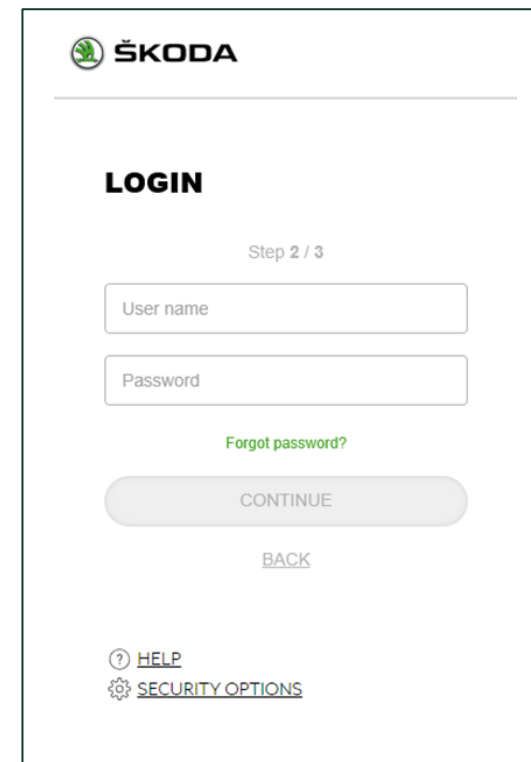
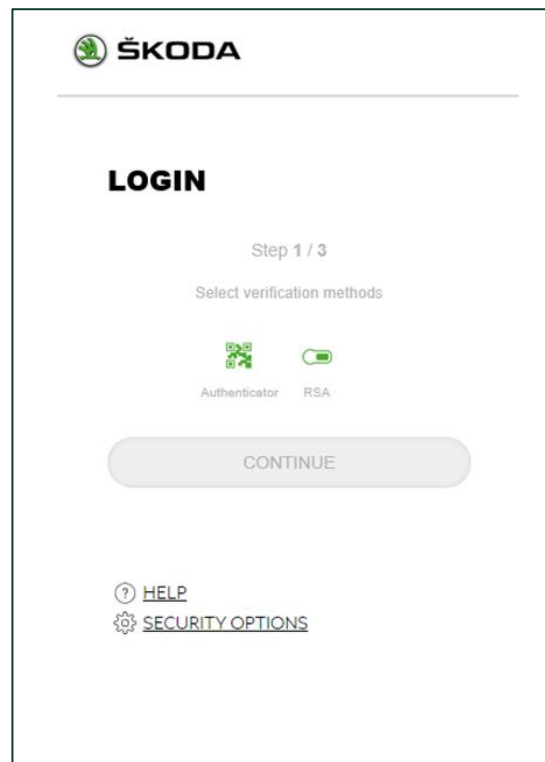
[BACK](#)

Username + password + one-time password from Authenticator

– It's necessary to registrate the device first.

Login instructions:

1. Enter the required URL.
2. Choose the method of authentication via Authenticator and confirm.
3. Enter:
 - Username.
 - Password.



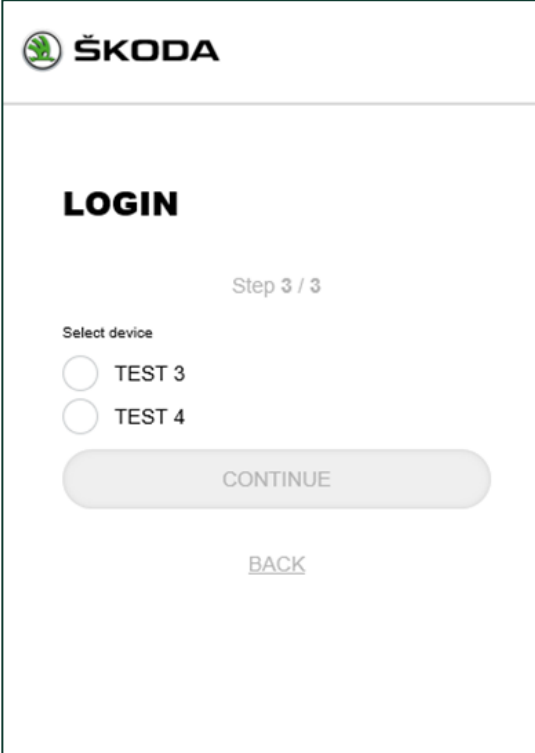
Continue

Username + password + one-time password from Authenticator

4. This step is skipped based on following rules:

In case the user has more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and continues to step 5.

In case the user has only one device registered and activated, the device is chosen automatically, and user is redirected to next step directly.



ŠKODA

LOGIN

Step 3 / 3

Select device

TEST 3

TEST 4

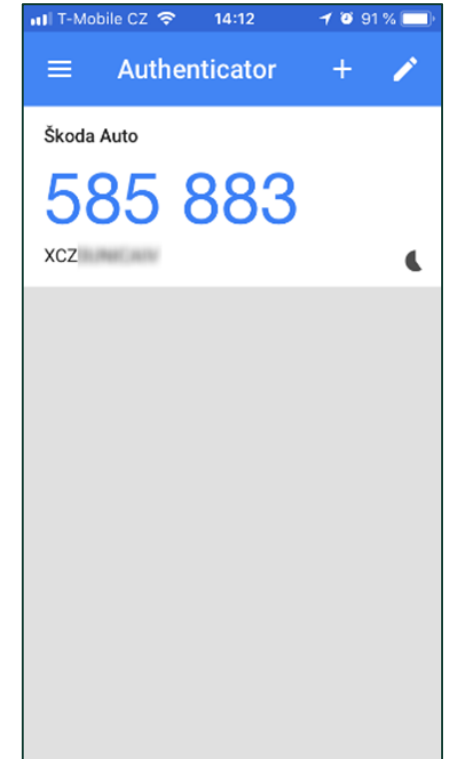
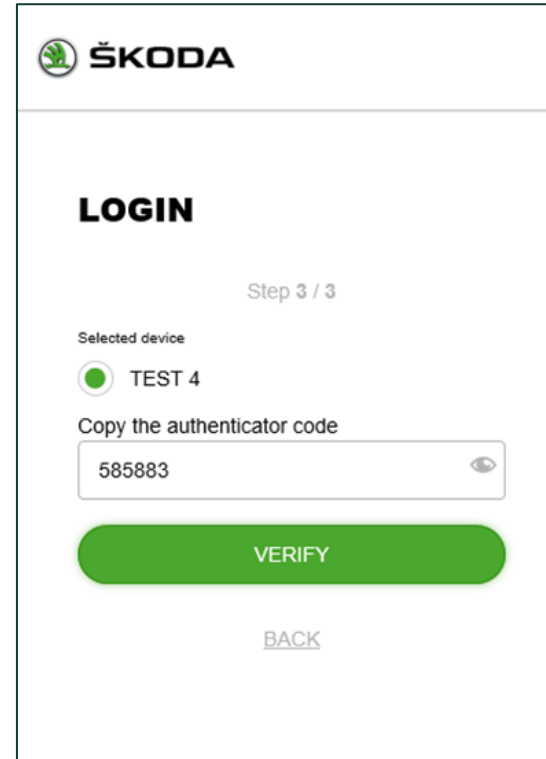
CONTINUE

[BACK](#)

Continue

Username + password + one-time password from Authenticator

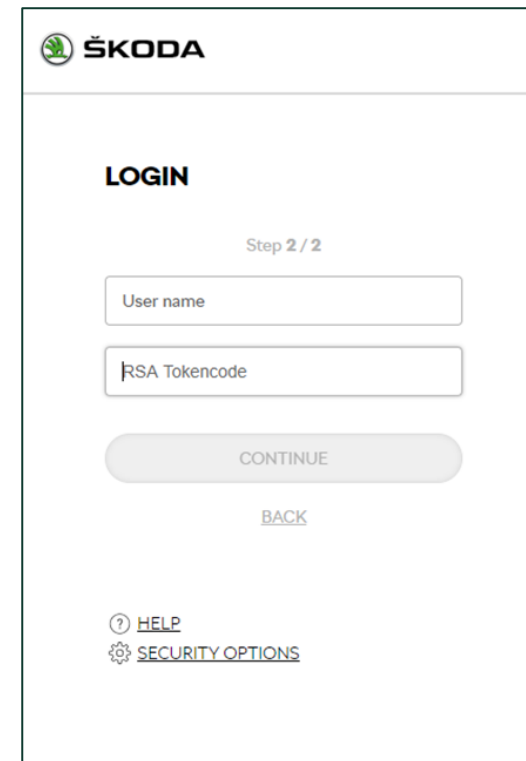
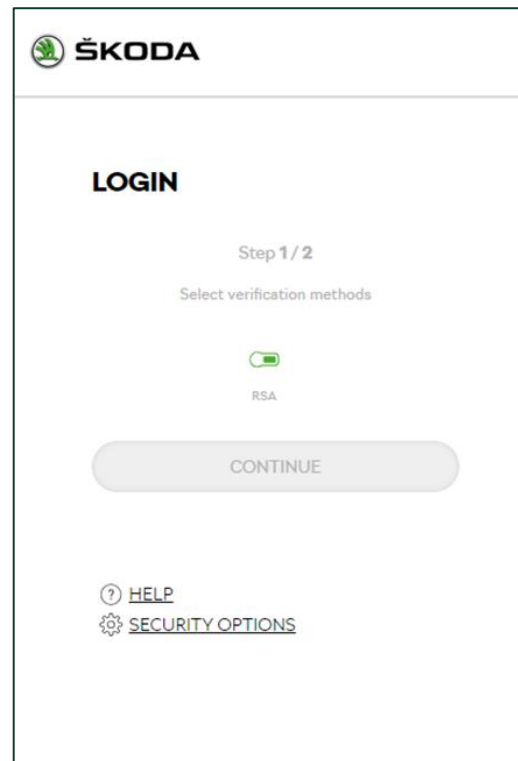
5. You are prompted for one-time password entry from Authenticator (on your mobile device) and confirm
6. You are logged in.



Username + Tokencode

Login instructions:

1. Enter the required URL.
2. Select RSA authentication method and confirm.
3. Enter:
 - Username.
 - PIN + Tokencode.
4. You are logged in.



PKI (Employees ID card) + PIN

Login instructions:

1. Enter the required URL.
2. A certificate (from PKI card) selection window appears, Choose the corresponding one.
3. You are logged in and redirected to required URL.

Security options

Registration

Activation

Registration

Click 'Security options' for adding new device.

- Click the link 'Security options' – new tab will be opened.
- Enter:
 - Username.
 - Password.
- You are logged in.

The screenshot shows the ŠKODA login interface. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is centered. There are two input fields: "User name" and "Password". Below the password field is a green link "Forgot password?". A grey "CONTINUE" button is centered below the links. Underneath the button is another green link "Other login methods". At the bottom left, there are two links: "? HELP" and a gear icon followed by "SECURITY OPTIONS", which is underlined in red.

This screenshot shows the same ŠKODA login interface as the previous one, but without the red underline. It includes the ŠKODA logo, "LOGIN" heading, "User name" and "Password" input fields, "Forgot password?" link, "CONTINUE" button, "Other login methods" link, and "? HELP" link.

Continue

Registration

- Use the ADD button to select the device you want to register.
- It's possible to have more authentication devices. You can also delete the device.

SMS

Authenticator

SECURITY OPTIONS

Below you can see the list of your security devices which allow you to get two-factor authentication within ŠKODA applications. ŠKODA AUTO prefers using **Authenticator**. Its application which provides one-time password generated based on current time. SMS can be used as well. You can start the wizard for device enrolment clicking the button ADD.



Authenticator

Verification with password from application

+ ADD



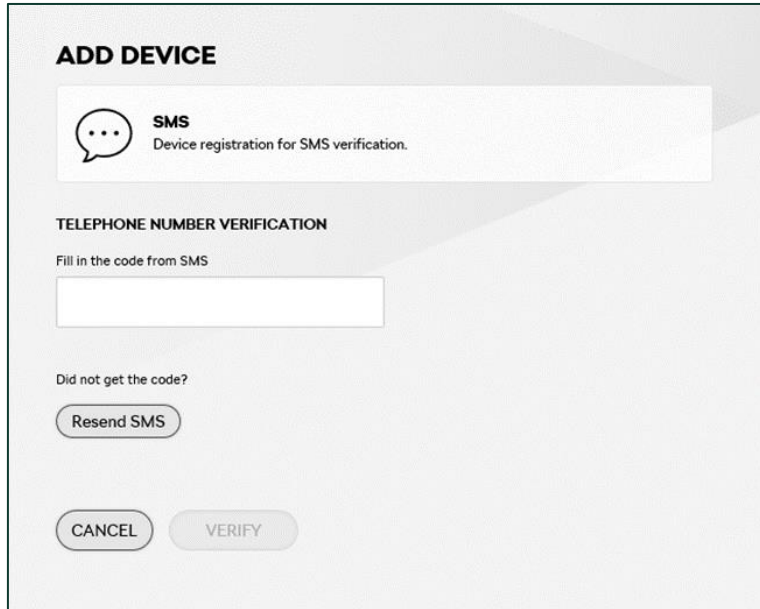
SMS client

Verification with password sent by SMS


+ ADD

SMS

- Enter:
 - Name of your device
 - Telephone number, preselection.



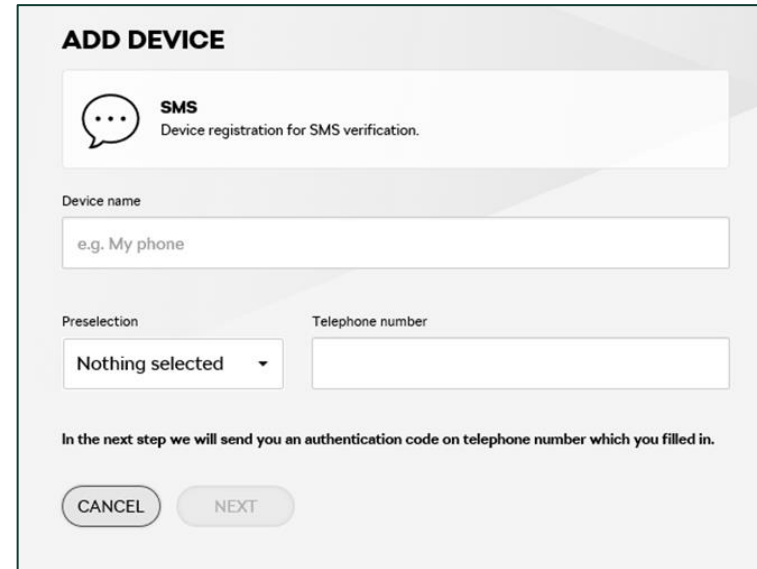
ADD DEVICE

 **SMS**
Device registration for SMS verification.


TELEPHONE NUMBER VERIFICATION

Fill in the code from SMS

Did not get the code?



ADD DEVICE

 **SMS**
Device registration for SMS verification.

Device name

Preselection Telephone number

Nothing selected

In the next step we will send you an authentication code on telephone number which you filled in.

- The user is prompted to enter the code from the SMS and confirm it.

Activation

Authenticator

Web browser application


Mobile application

PC application

Authenticator registration

1. Enter and confirm:
 - Name of your device


ADD DEVICE

 **Authenticator**
Device registration for authentication with application

1. Install application FreeOTP - [Android/iOS](#), or Google Authenticator - [Android/iOS](#).

2. With application scan QR code. If you are unable to scan the QR code, fill in the secret key manually. Make sure your screen is not tracked by anyone - sensitive information will be displayed.


[Hide QR code \(27\)](#)



Secret key
FF6M5Z7FN2ZA542INTRL366T5TRDOH4Q


[Link for authenticator configuration](#)
[Add authenticator](#)

Fill in the code from application.

 **SKODA** Auth

User
Name Surname

ADD DEVICE

 **Authenticator**
Device registration for authentication with application

Device name

2. Click 'Show the QR code' and copy the 'Secret key'. Keep the window opened. Next step is to install the browser addon. Follow 'Firefox addon installation guide'.

Continue

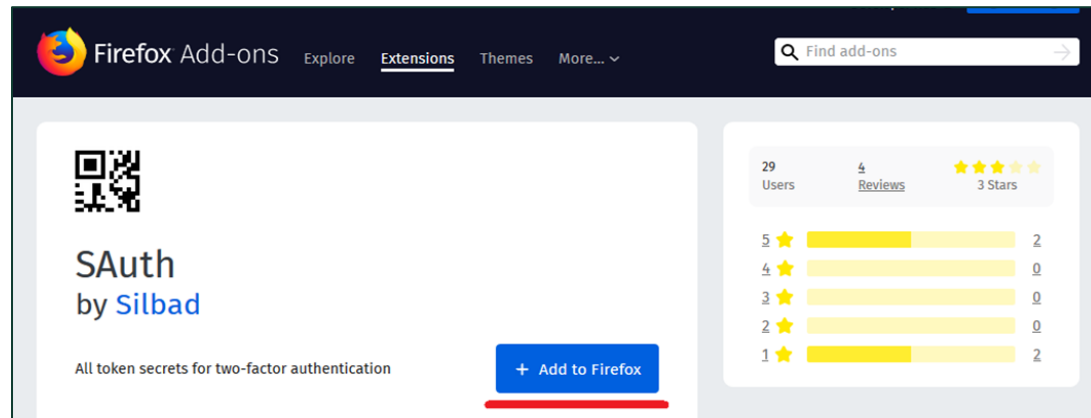
Firefox addon installation guide

This help contains guide for installation the addon SAuth for Firefox („FF“). There are other possibilities for other browsers as well. For example for Internet Explorer, Google Chrome. Such instruction is not a part of this help and can differ.

Warning: This is a third-party product; the information may not correspond to reality. We reserve the right to make changes.

If you do not have the FF browser installed on your PC, you can download it for free here: <https://www.mozilla.org/cs/firefox/new/>

3. Open this URL in FF browser: <https://addons.mozilla.org/firefox/addon/sauth/>
4. Click on 'Add to Firefox' button.

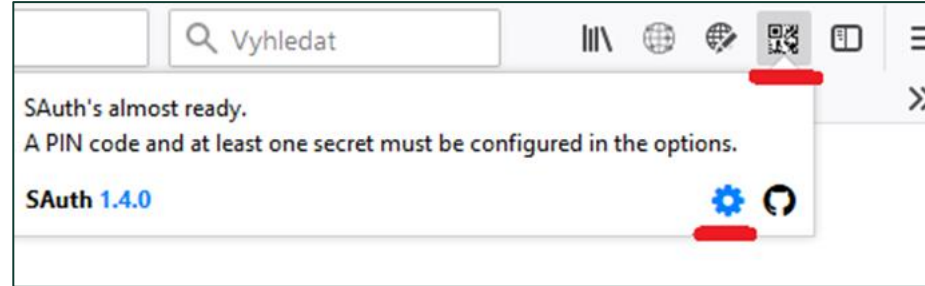


5. A confirmation window will open. Click 'Add'.

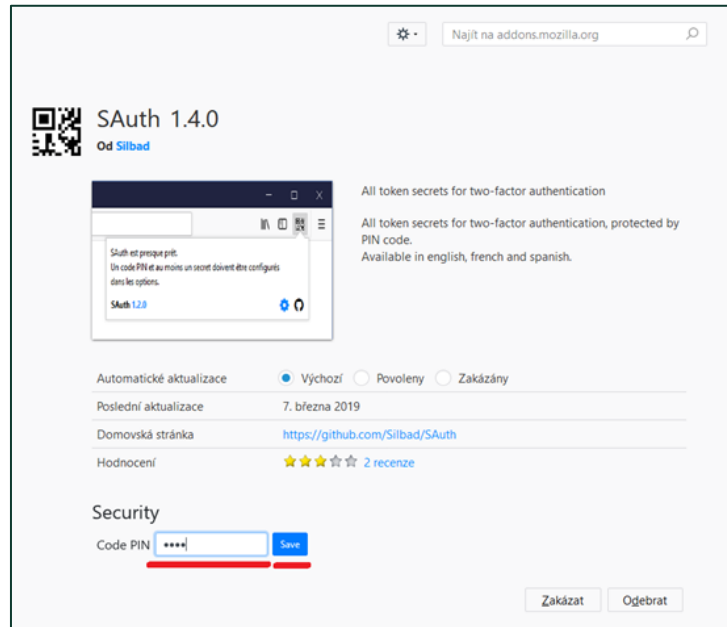
Continue

Firefox addon installation guide

6. Launch the SAuth app.



7. Enter new PIN and click 'Save'.



Continue

Firefox addon installation guide

8. In “Secrets list” enter parameters:

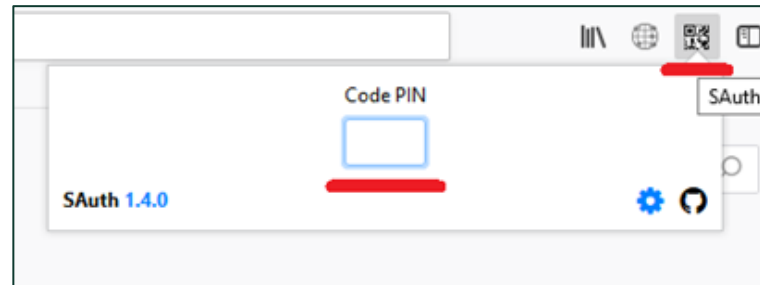
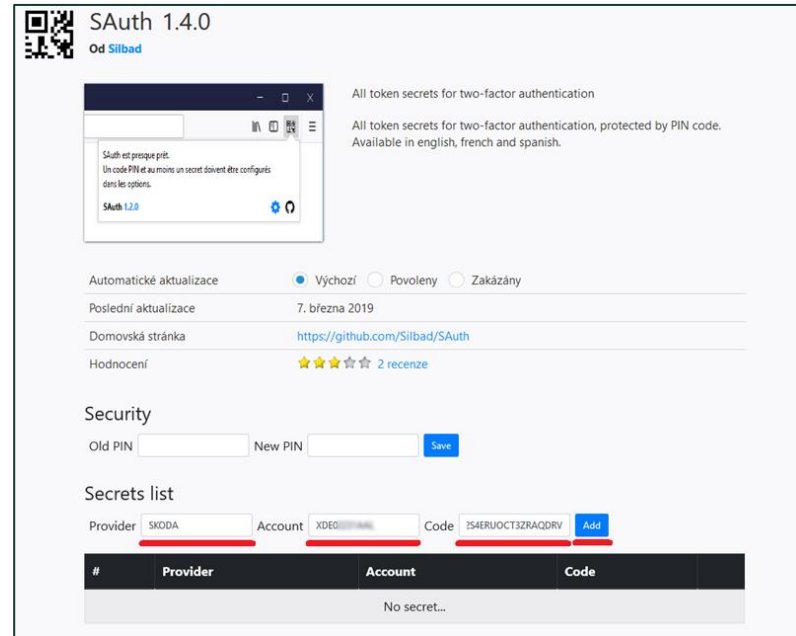
- Provider – SKODA.
- Account – Any value, f.e. your username
- Code – Insert the “Secret key” from the device registration (Security options).

and click on the ‘Add’ button.

9. The device is successfully added to the application and it's ready to use. (You can close the window.)

#	Provider	Account	Code
1	SKODA	XDE[REDACTED]	*****

10. Open the SAuth application in the browser and unlock it using the PIN which was established.



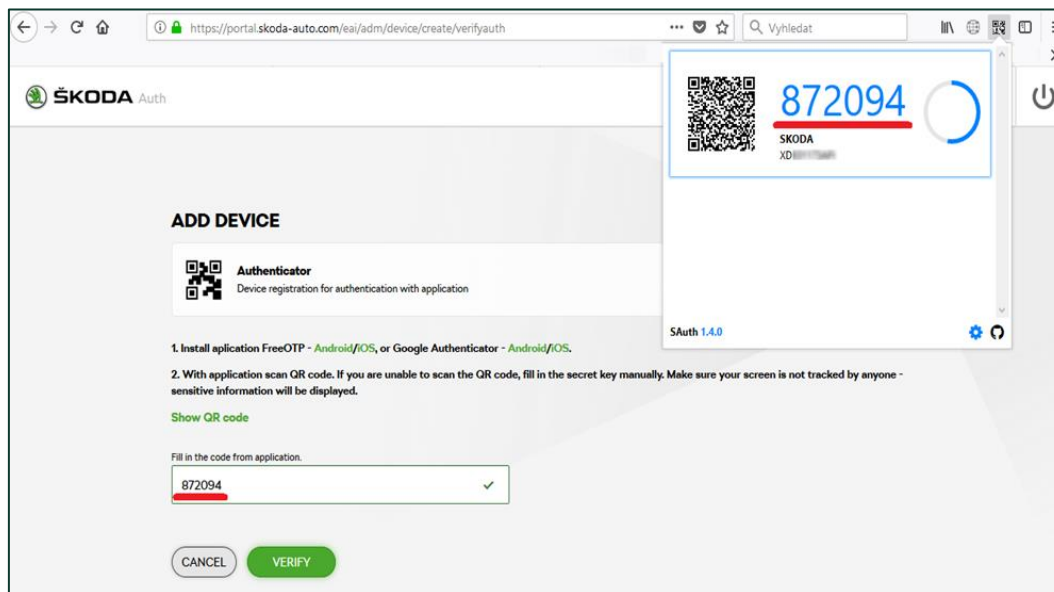
Continue

SKODA

Authenticator registration

Go back to the Security Options:

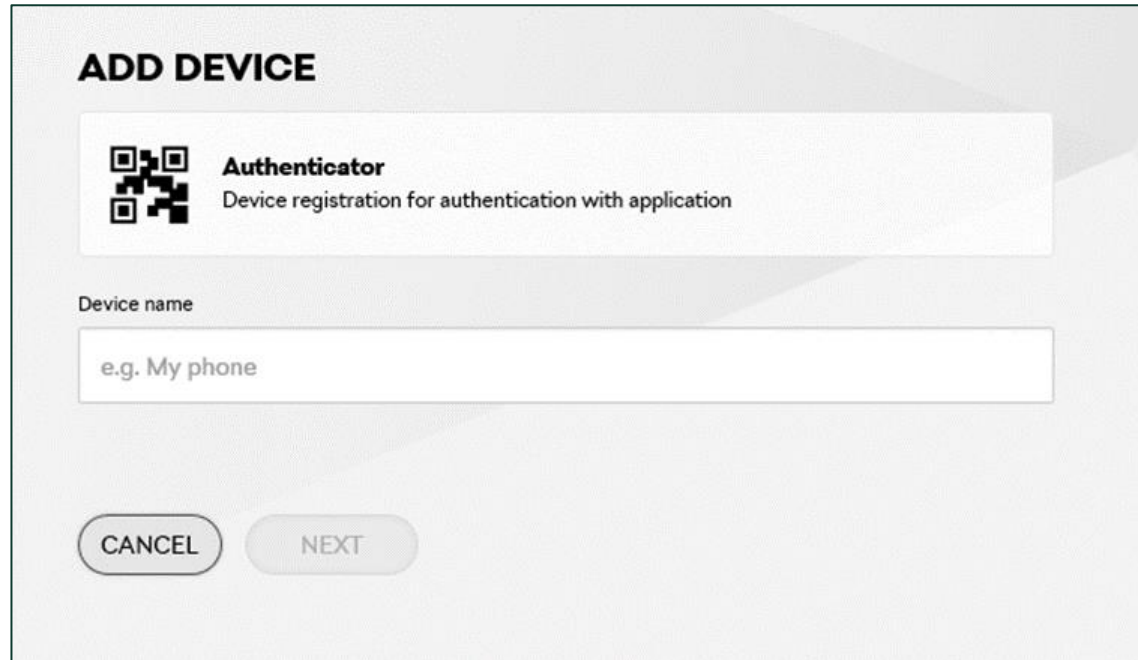
11. Copy the generated code from the SAAuth application to the authentication device registration in the appropriate field. Filling the code must take place within approx. 30 seconds.
12. Click the button 'Verify', the device is created.




Activation

Adding an Authenticator for a mobile phone

1. Enter:
 - Name of your device



ADD DEVICE

 **Authenticator**
Device registration for authentication with application

Device name

e.g. My phone

CANCEL NEXT

Keep the window opened. Next step is to install the mobile application (f.e. FreeOTP / Google Authenticator).


Continue

Adding an Authenticator for a mobile phone

Go back to the Security Options:

2. Click Show the QR code and read it using the mobile application
3. Retype the 6 characters code from mobile app to the Security Options to appropriate field. The code expires after 30 seconds.

ADD DEVICE

 **Authenticator**
Device registration for authentication with application

1. Install application FreeOTP - [Android/iOS](#), or Google Authenticator - [Android/iOS](#).

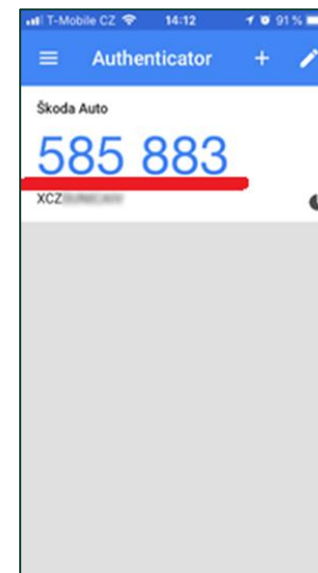
2. With application scan QR code. If you are unable to scan the QR code, fill in the secret key manually. Make sure your screen is not tracked by anyone - sensitive information will be displayed.

[Show QR code](#)

Fill in the code from application.

 ✓

CANCEL VERIFY

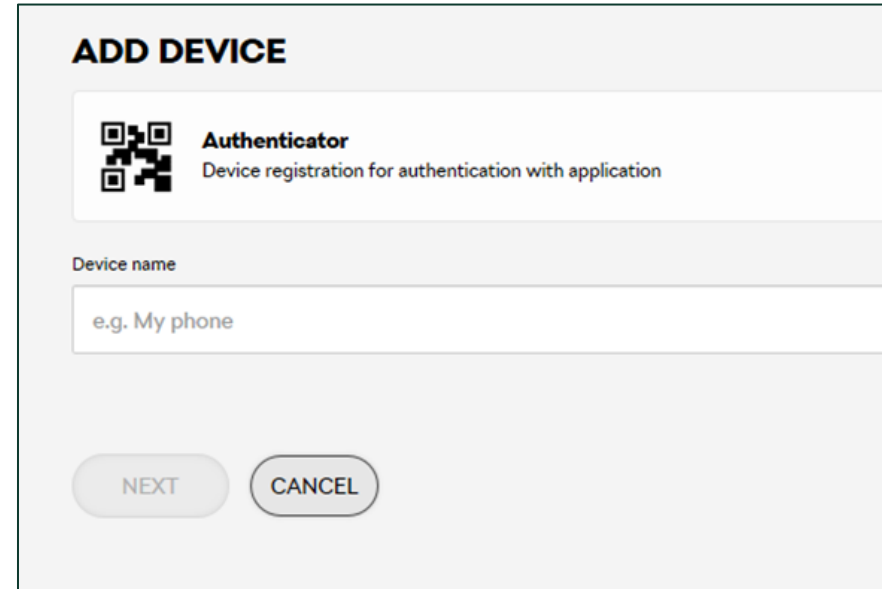
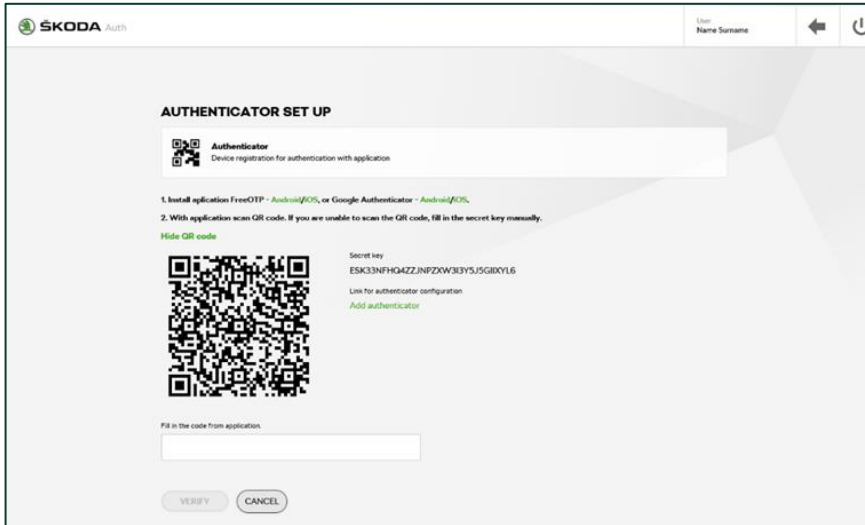


Activation

SKODA

Adding an Authenticator for a PC

1. Enter:
 - Name of your device

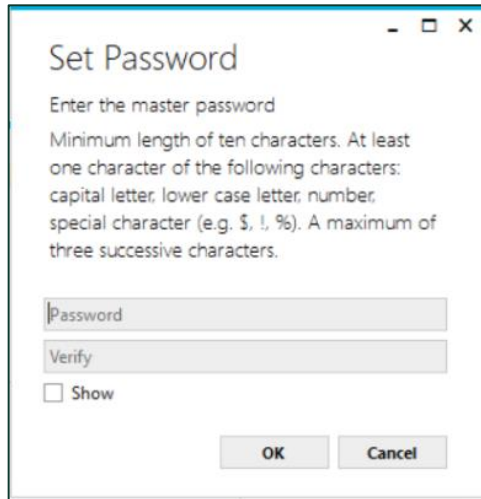


2. Click “Show the QR code “ and copy the “Secret key “. Keep the window opened . Next step is to install the GRPAuth application as shown on the next pages.

Continue

Installing a GRP Auth Authentication for a PC

- This help contains guide for installation of the GRPAuth application. There are other applications that can be used as well, however such instruction is not a part of this help and can differ.
- Attention: The guide is based on 3rd party application. We reserve the right to possible changes.
- You can download the application [HERE](#)
- After launching the application, please set the password you will use for GRPAuth.



Set Password

Enter the master password

Minimum length of ten characters. At least one character of the following characters:
capital letter, lower case letter, number,
special character (e.g. \$, !, %). A maximum of three successive characters.

Password

Verify

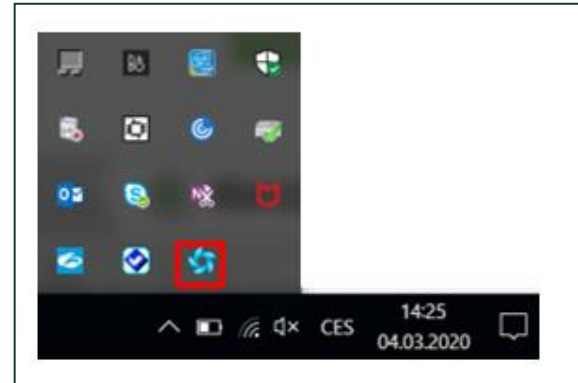
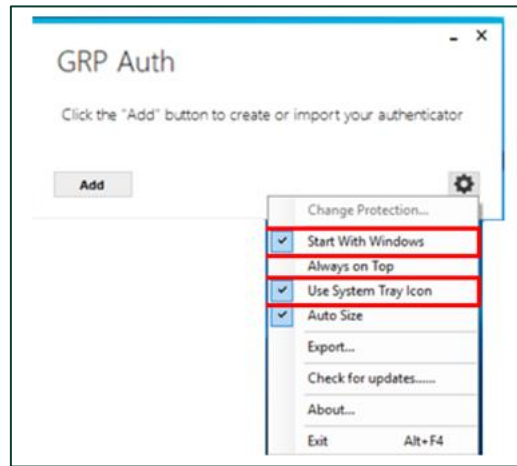
Show

OK Cancel

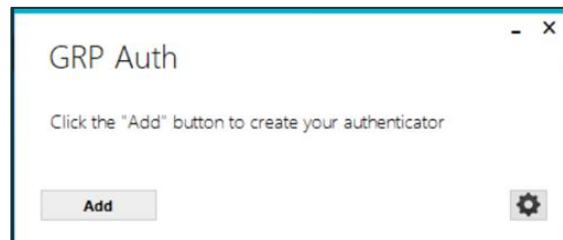
Continue

Installing a GRP Auth Authentication for a PC

- For easier login, when turning on the application, it is possible to add the GRPAuth icon to the bottom bar or launch the application when turning on the PC using the gear icon.



- After you open GRPAuth click on 'Add'.




Continue

Installing a GRP Auth Authentication for a PC

- Enter the name, insert copied 'Secret code' from the device registration (Security options). Then enter your own the password for authentication.

1. Install application FreeOTP - [Android/iOS](#), or Google Authenticator - [Android/iOS](#).
2. With application scan QR code. If you are unable to scan the QR code, fill in the secret key manually.

[Hide QR code](#)



Secret key
ESK33NFHQ4ZZJNPZXW3I3Y5J5GIXYL6

Link for authenticator configuration
[Add authenticator](#)

Fill in the code from application.

VERIFY CANCEL

Add Account

Name

1. Enter the secret code

2. Enter a password. (Minimum length of 10 characters, At least one character of the following characters: capital letter, lower case letter, number, special character e.g. \$, !, %. A maximum of three successive characters.)

Password

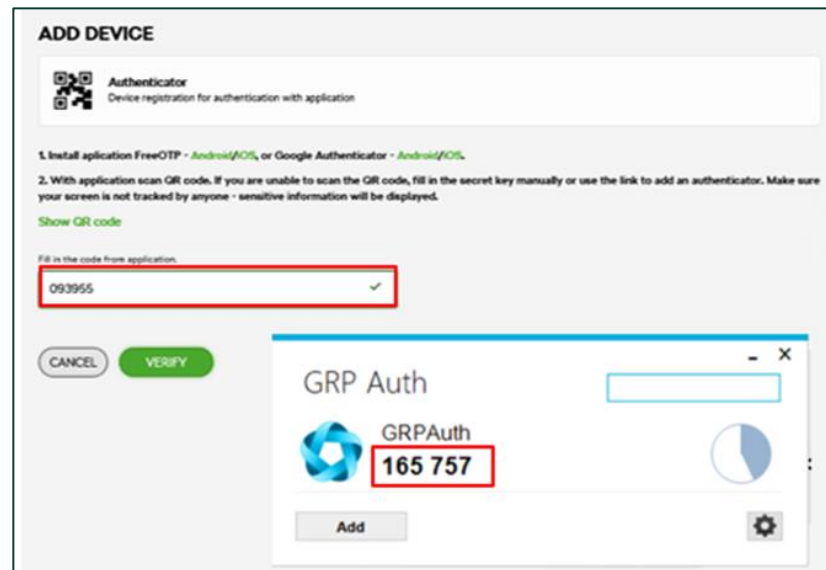
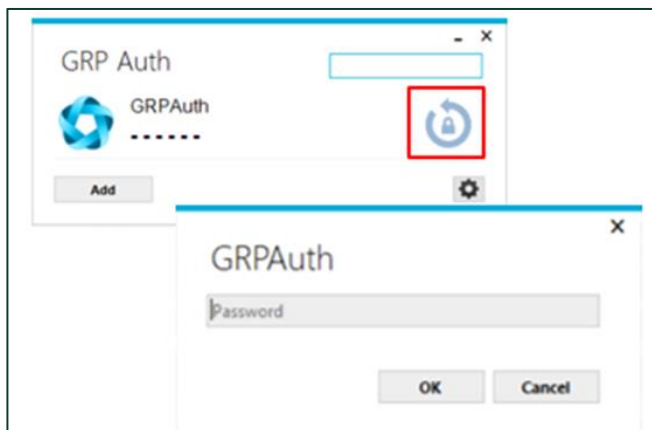
Confirm

OK Cancel

Continue

Adding an Authenticator for a PC

- Click on the marked lock icon and enter your password. A six-digit code will be displayed.
- Go back to the browser on opened device registration, enter the six-digit code in the appropriate field and click on 'Verify'. The code must be entered within a maximum of 30 seconds.



Activation

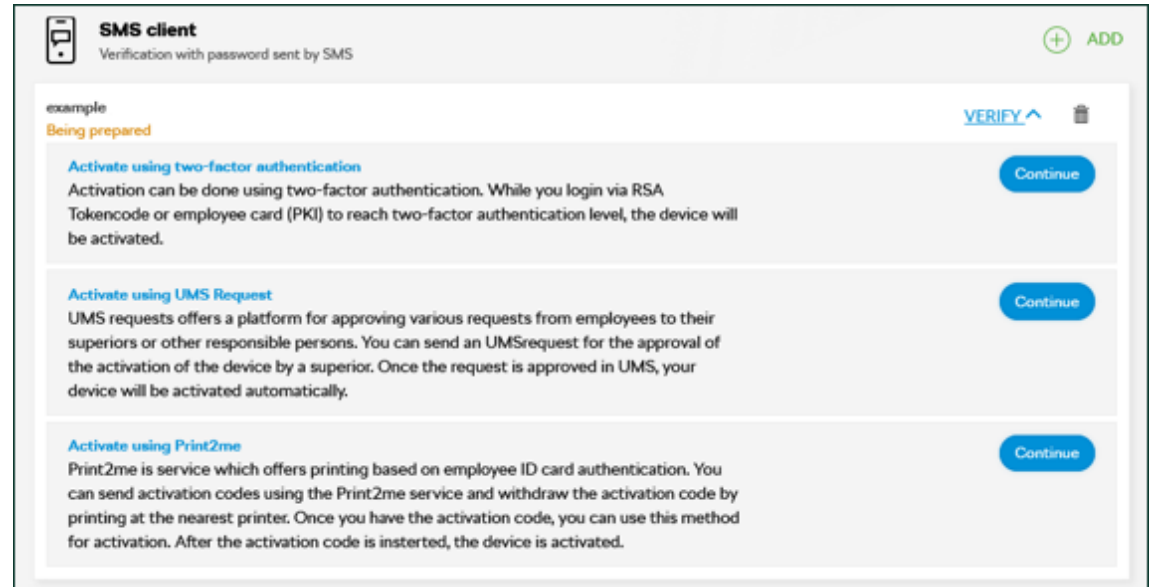
Device activation

ŠKODA AUTO employees

Other B2B users

Device activation for ŠKODA AUTO employees

- List of available activation methods is displayed:
 - Activation using two-factor authentication.
 - Activate using UMS Request
 - Activation using Print2me.
- User chooses the wanted method by clicking the appropriate button 'Continue'.



Continue

Device activation for ŠKODA AUTO employees

Activation using Print2me

- The code is sent to the printer, where user can print it using employee card.
- User enters the code from document and confirms.
- The device is activated.

DEVICE ACTIVATION

Activation code was sent to the printer. The code has got limited expiration. After the expiration its necessary to resend the code again.

Insert the code from the document.

CANCEL VERIFY

Did not get the code?
Send the activation code to the printer (Print2me). Resend

Continue

Device activation for ŠKODA AUTO employees

Activate using UMS Request

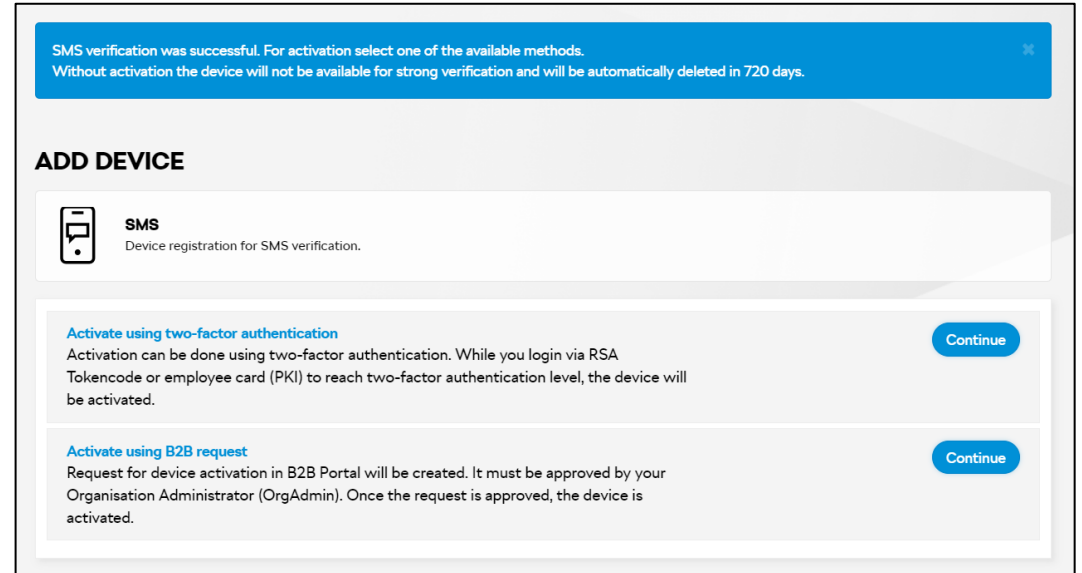
- The request has been sent to UMS.
- Once the request is approved in UMS, the device is automatically activated.

Activation using two-factor authentication

- User is redirected to Login page where two-factor methods are available - SMS, Authenticator, RSA Tokencode.
- Once user is logged in the device is activated within Security options.

Device activation for other B2B users

- List of available activation methods is displayed:
 - Activation using two-factor authentication.
 - Activation using B2B request.
- User chooses the wanted method by clicking the appropriate 'Continue' button.



Continue

Device activation for other B2B users

Activation using B2B request

- User is redirected to the initial page within 'Security Options'.
- The request is automatically created and sent to the B2B Portal application.
- Request approver is user's Organization Administrator or the Organization Administrator of parent organization.
- Once the request is approved, the device is activated, and the user is notified by e-mail.

Activation using two-factor authentication

- User is redirected to Login page where are two-factor methods available - [SMS](#), [Authenticator](#), [RSA](#).
- Once user is logged in the device is activated within Security Options. The device is activated.

Password reset

- It is possible to reset your password on the login page of B2B Portal.
- The link is available from basic login and two-factor login using SMS, and Authenticator.

Instructions:

1. Click the link 'Forgot password?'
 2. User enters and confirms:
 - Username.
 - Re-captcha security code.
- User can use the method which does not require the password using the link 'Alternative login methods'. The process is described in appropriate chapter [HERE](#).

SKODA

LOGIN

[Forgot password?](#)

CONTINUE

[Other login methods](#)

[HELP](#)

[SECURITY OPTIONS](#)

SKODA

NEW PASSWORD SETTING

P E W F H

Copy the code

RECOVERY

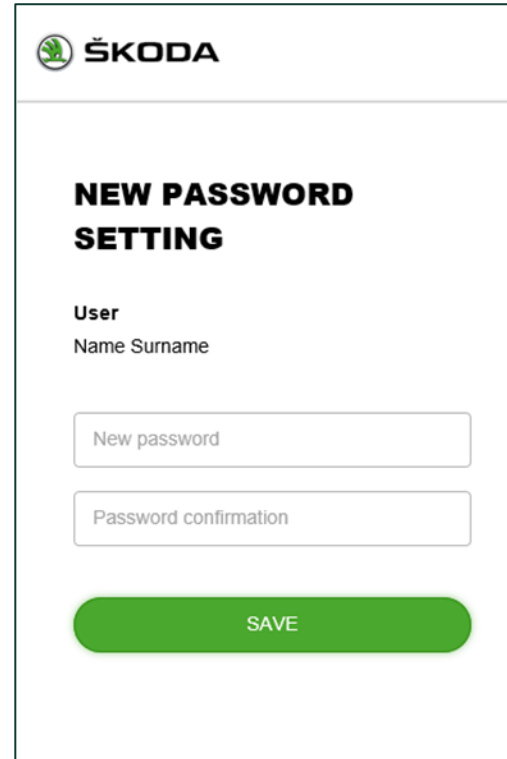
[BACK](#)

[Alternative login methods](#)

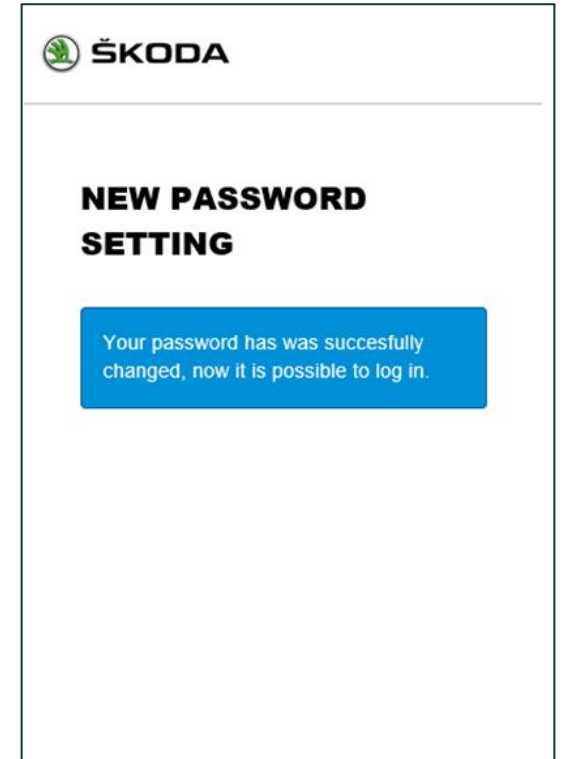
Continue

Password reset

3. E-mail which contains the link for password reset is sent and user is redirected back to the login page.
4. After clicking the link in the e-mail, user is redirected to the page for setting new password.
5. Notification about successful password change is displayed.



The screenshot shows the 'NEW PASSWORD SETTING' page. At the top left is the ŠKODA logo. Below it, the title 'NEW PASSWORD SETTING' is displayed in bold. Underneath, the text 'User' is followed by 'Name Surname'. There are two input fields: 'New password' and 'Password confirmation'. At the bottom, there is a green rounded button labeled 'SAVE'.

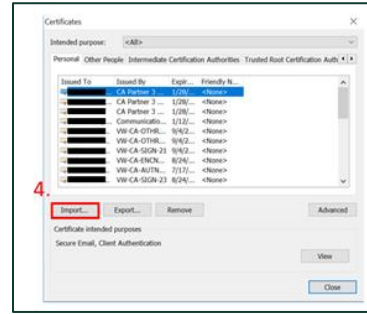
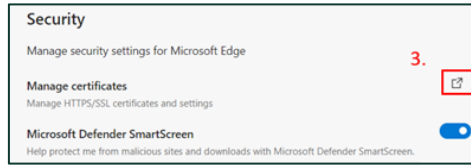
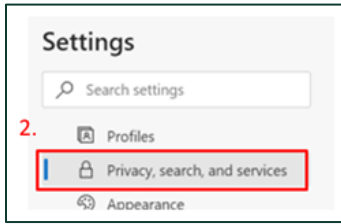
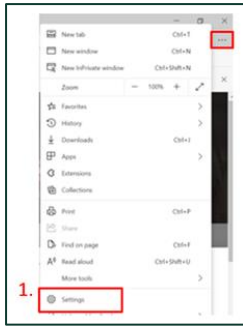


Certificate installation

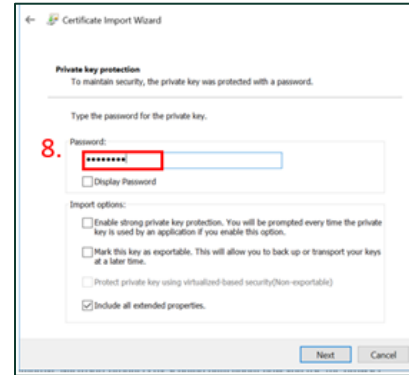
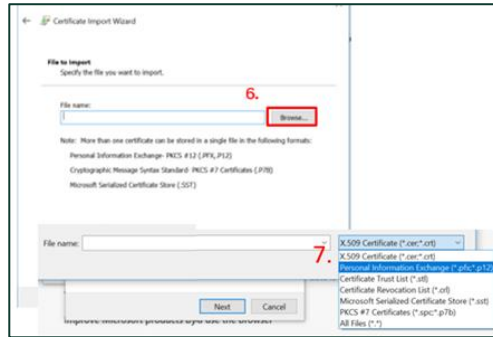
Microsoft Edge

Firefox

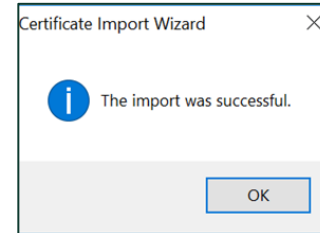
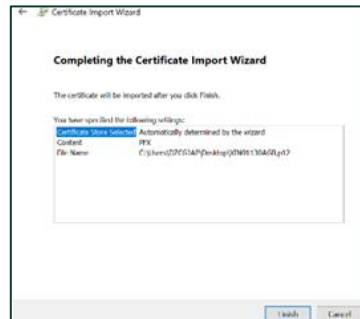
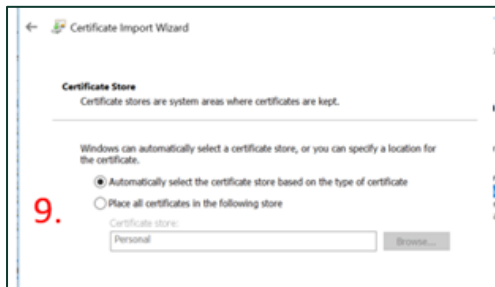
Microsoft Edge – certificate installation



1. Settings
2. Privacy, search and services
3. Scroll down to security and click on 'manage certificates'
4. Import

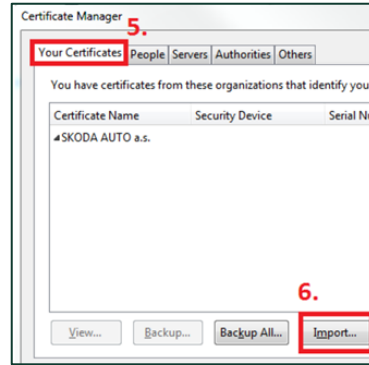
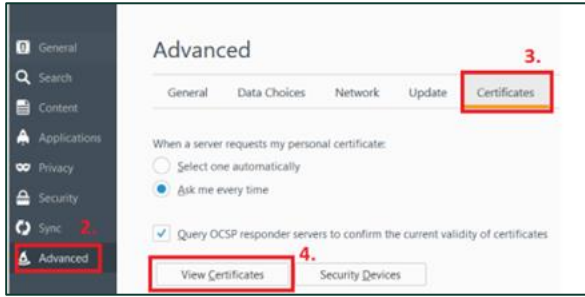
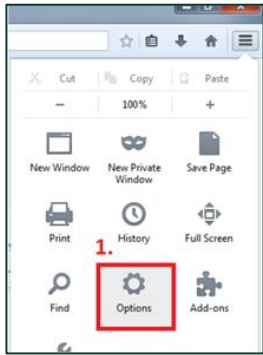


5. Next
6. Browse
7. Choose*.pfx*.p12 and choose your certificate
8. Enter the password from PDF file




9. Choose certificate store and finish

Firefox – certificate installation



1. Options
2. Extended
3. Certificates
4. Certificates
5. Personal
6. Import
7. Find your certificate
8. Open
9. Enter password from PDF file
10. OK

Get access



**Request for establishment,
modification or cancellation of
access to B2B**

Access establishment
 Access modification
 Access cancellation

Required access to:

Information about user	
Surname:	First name:
User ID:	
Business number:	
Company name:	
Address:	
Phone:	
e-mail:	
Reason:	
Description of required type of permission (role):	

User	<i>Classified information</i>
Date	yes <input type="checkbox"/> no <input type="checkbox"/>
signature	
Control of user's integrity*	Approved by (superior of user)
yes <input type="checkbox"/> no <input type="checkbox"/> signature, name stamp, stamp

For employees of external companies

User of external company confirmed preservation of confidential information	Head of OU (submitter)
 signature, name stamp, stamp
	Date:

Establisher	name	signature
-------------	------	-----------

* => Checks a file in the superior of user, in case of confidential information
 ** -> in only in unusual cases

**Please send fully filled form via email (B2Bhelp@skoda-auto.cz)
or with internal mail to VVM department**

User is obliged to care about safety of data according to regulations "Protection and safety of data" "Sustaining a confidential information".

In case of any questions or special requests, please contact User Help Desk - tel. 19100.

SKODA AUTO s.r.o. | SKODA AUTO s.r.o., Tl. Václava Klementa 858, 251 69 Mladá Boleslav, Česká republika

FAQ - Login

Rules for code from SMS

- Max. number of attempts is 8.
- The interval for checking number of attempts is 1 hour.
- Sending SMS is possible max. 3-times a day
- Password is valid for 15 minutes (if you don't login with this password within 15 minutes of receiving the message, password will expire, and you will have to send your SMS with a one-time password again)
- After using this one-time password from SMS, You won't be verified by this password again within one day (24 hours), however you must be verifying on the same device. For another login you will use only Login + your password to B2B Portal.

Rules for code from Authenticator

- Max. number of attempts is 8.
- The interval for checking number of attempts is 1 hour.
- After using this one-time password from Authenticator, You won't be verified by this password again within one day (24 hours), however you must be verifying on the same device. For another login you will use only Login + your password to B2B Portal.
- For user verification is necessary to have exact time on mobile device.

Continue

FAQ - Přihlášení

Login 24 hours

- The validity of the code from the SMS, Authenticator is 24 hours. Within one day, you are no longer authenticated with the code from the device (just enter the username + password). The condition is that you authenticate a second time at the same station.

Validity of Password Reset link

- It is valid for 24 hours. If the link has already been used or has expired, a corresponding message will be displayed, and you will have to repeat the password recovery process.

Fingerprint2

- If you have Adblock installed in your browser and Fingerprint2 library blocking is enabled in the settings, you lose the convenience of logging in with a higher authentication method and the "24-hour login" functionality. You will always have to re-authenticate with the code from the SMS, the Authenticator.

Continue

FAQ – Device registration

Rules for code from SMS

- SMS can be sent max. 3 times per day.
- The password is valid for 15 minutes.

Code rules from Print2me

- Lasts 24 hours on the printer. After this time, it is necessary to send the key to the printer again.
- Validity 2 days.
- If the user has multiple devices registered, all keys with a validity period of more than 2 days will be sent. It is not defined which key belongs to which device. The key can only be used once for any one device.