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.

Get access

Security options

Login

Password reset

FAQ

Get access

ŠKODA AUTO employee

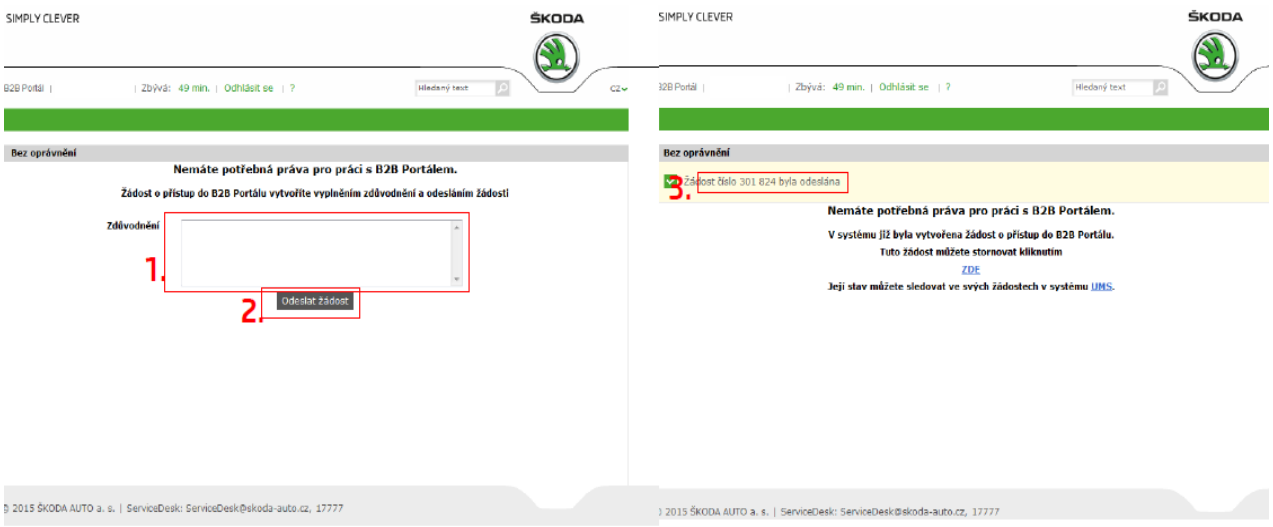
Other B2B users

Please choose one option and click

ŠKODA AUTO employee

For the first access:

- Open this URL: https://Bportal.skoda.vwg.
- Fill the reason.
- Choose Send request.
- Your request has been created , B2B team is going to contact you with the certificate.



Continue

ŠKODA AUTO employee

- After receiving the certificate and a password from B2B team to you e-mail, please install the certificate according this manual.
- During the first login it is necessary to set a new password.

Password rules

- The password cannot be identical to your user name.
- The password must be a combination of letters and at least one special character.
- The system remembers tle last 6 passwords – those passwords cannot 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 (filled send to address: b2bhelp@skoda-auto.cz).
- After receiving the certificate to your e-mail and installation password from your OrgAdmin, please install your certificate according to this manual.
- After installation of your certificate, during the first login it is necessary to set a new password.

Password rules

- The password cannot be identical to your user name.
- The password must be a combination of letters and at least one special character.
- The system remembers tle last 6 passwords – those passwords cannot be used as a new password.

*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

User name + password

Certificate + password

Other login methods

Two-factor login

User name + password + One-time password from SMS

User name + password + One-time password from Authenticator

User name + Tokencode

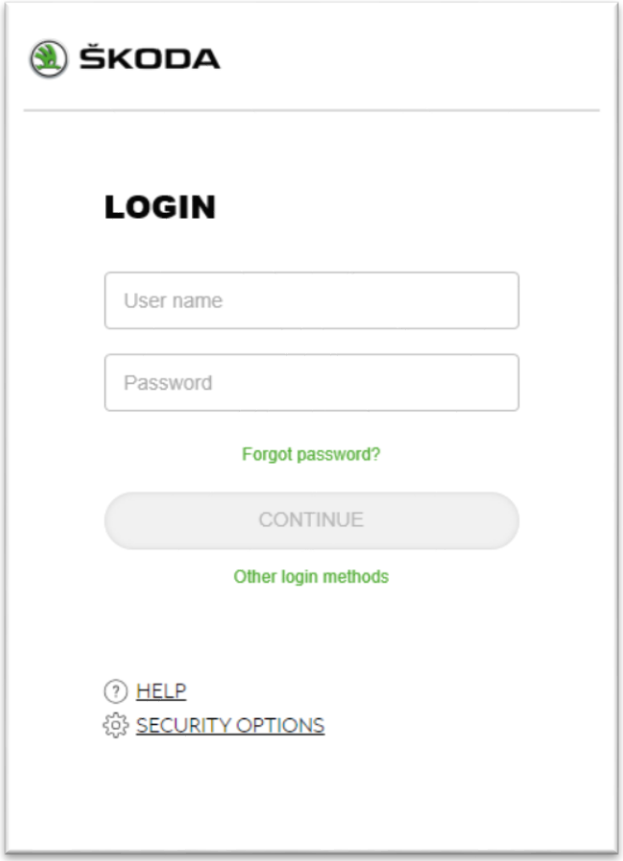
PKI (Employee ID card) + PIN

Only for ŠKODA AUTO employees

User name + password

Login instructions:

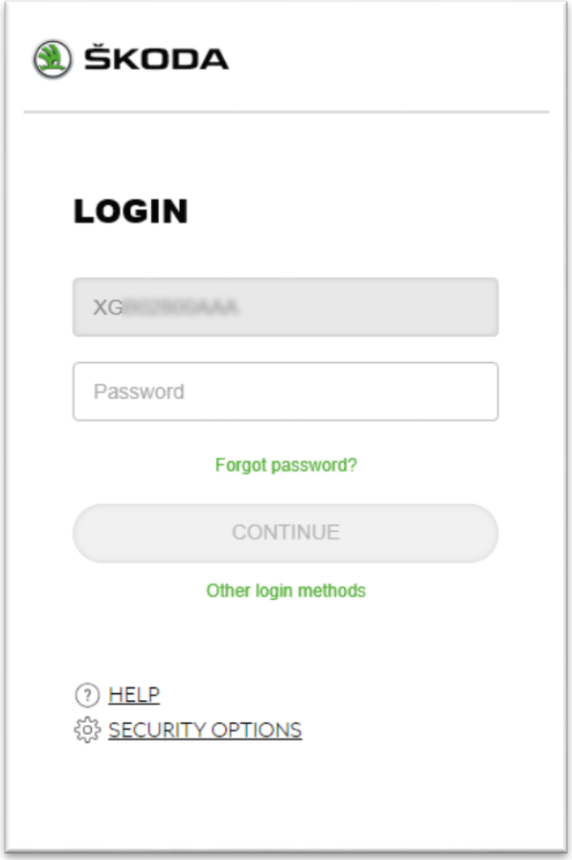
1. Enter the required URL.
2. Enter:
    - User name.
    - Password.
3. You are logged in.



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. Enter:
    - Password.
4. You are logged in.

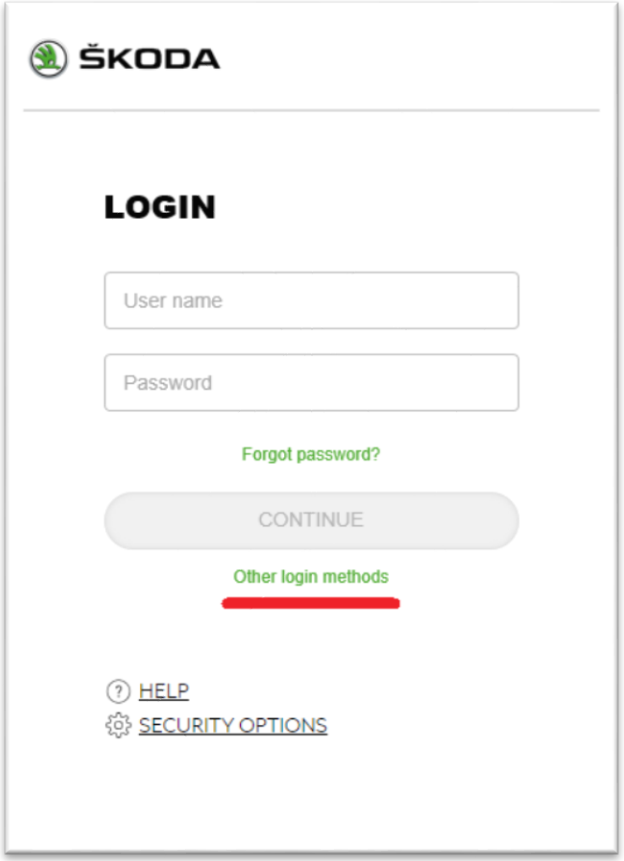


Other login methods

- 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 „Other login methods“.
3. Based on chosen method, follow instructions for SMS, Authenticator, RSA Tokencode.

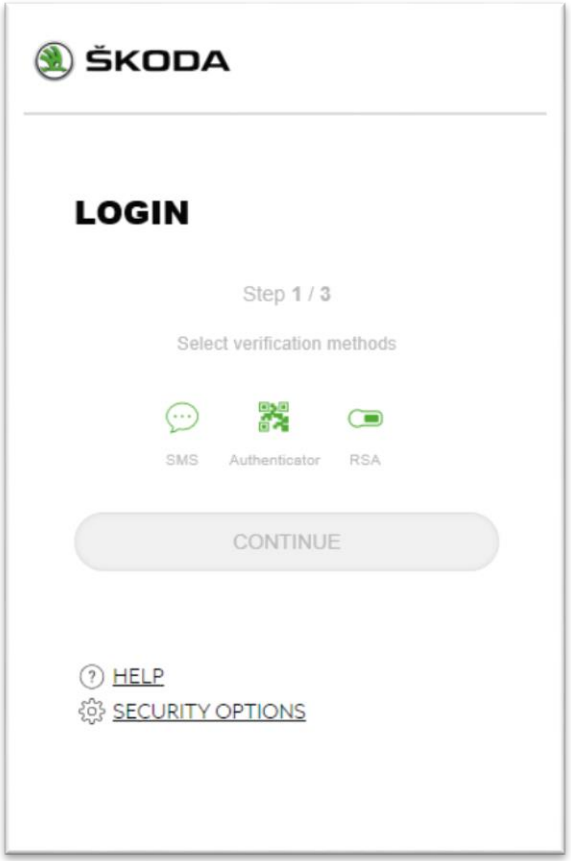


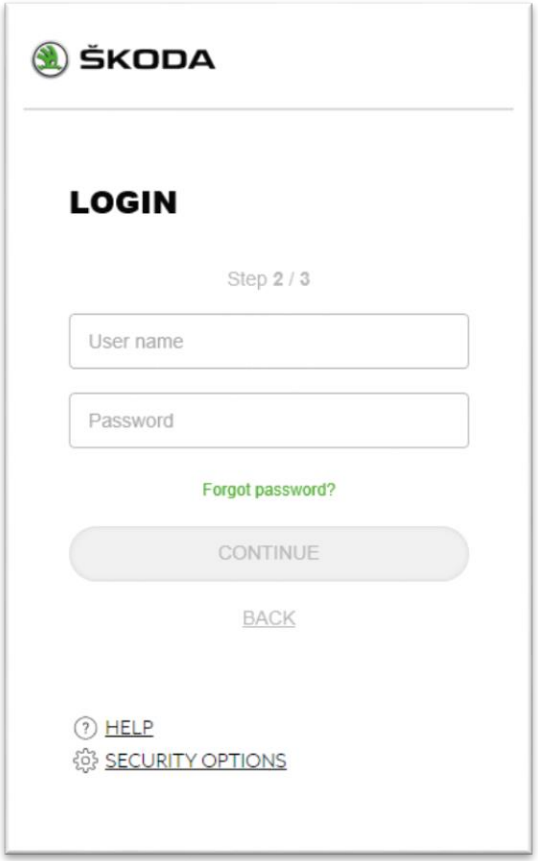
User name + password + One-time password from SMS

First it is necessary to registrate the device.

Login instructions:

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





Continue

User name + password + One-time password from SMS

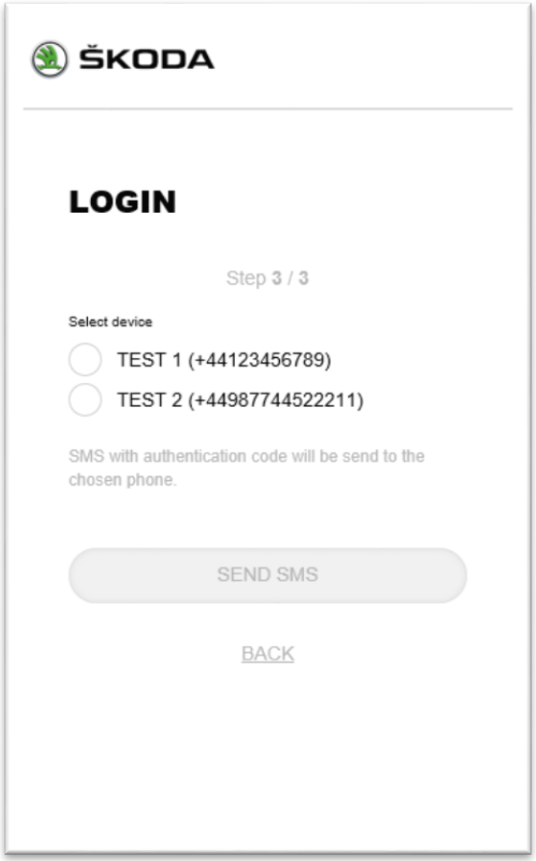
4. This step is skipped based on following rules:

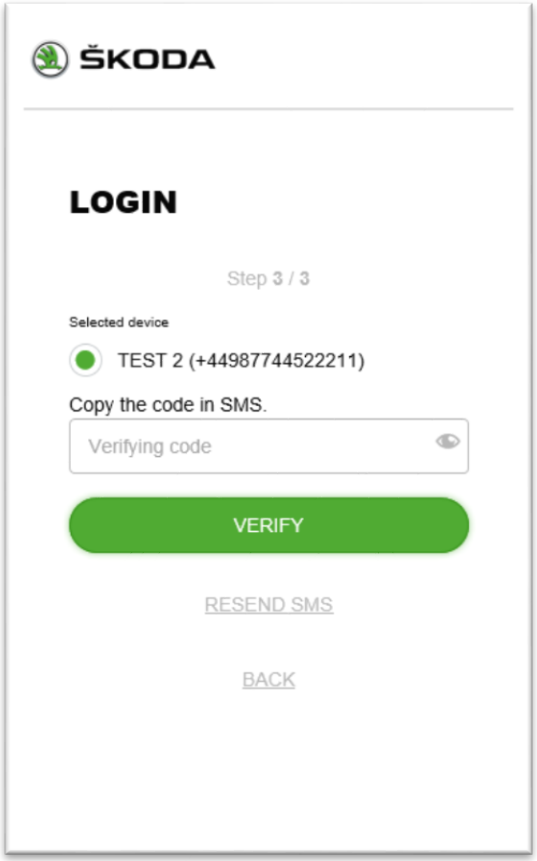
In case user has got more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and confirms the form.

In case user has got only one device registered and activated, the device is chosen automatically and user is redirected to step 5 directly.

5. Enter the code from SMS.

6. You are logged in.



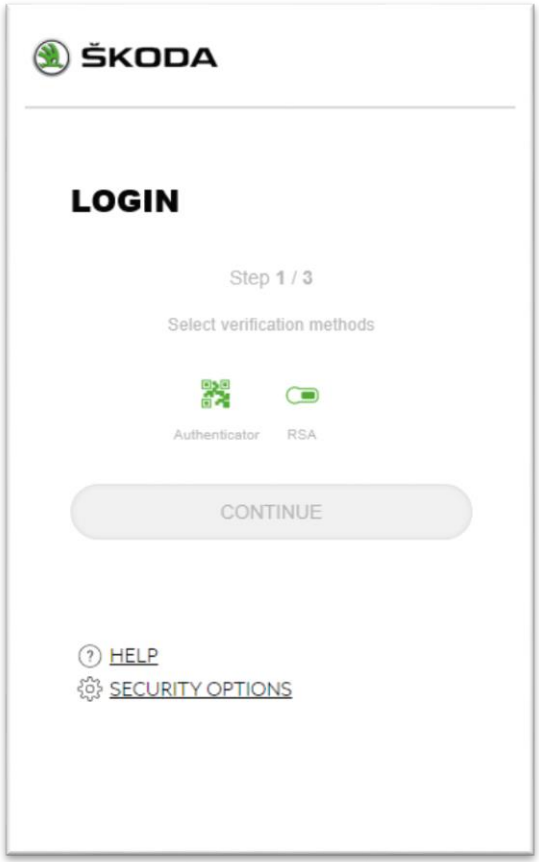


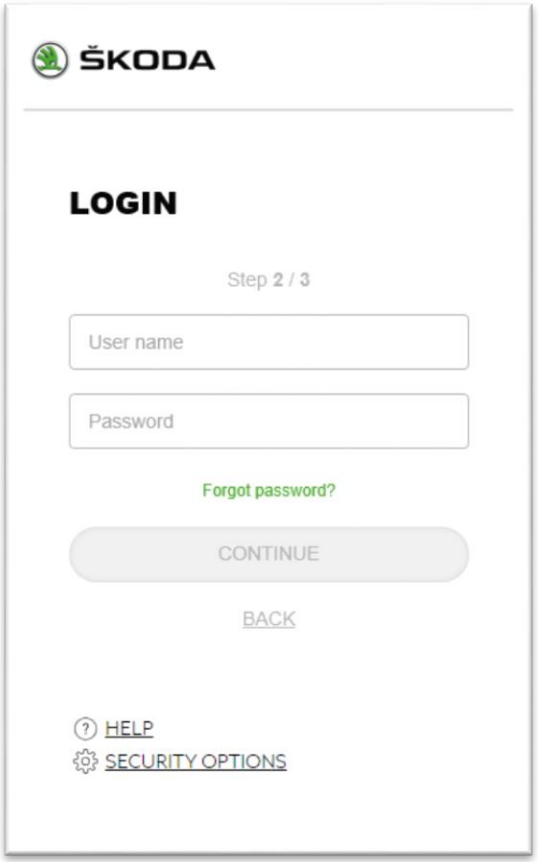
User name + password + One-time password from Authenticator

First it is necessary to registrate.

Login instructions:

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





Continue

User name + password + One-time password from Authenticator

4. This step is skipped based on following rules:

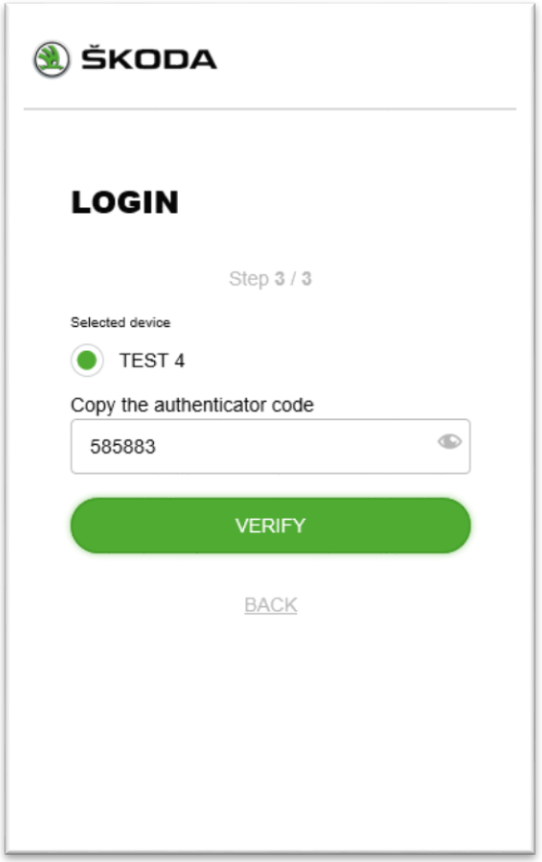
In case user has got more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and confirms the form.

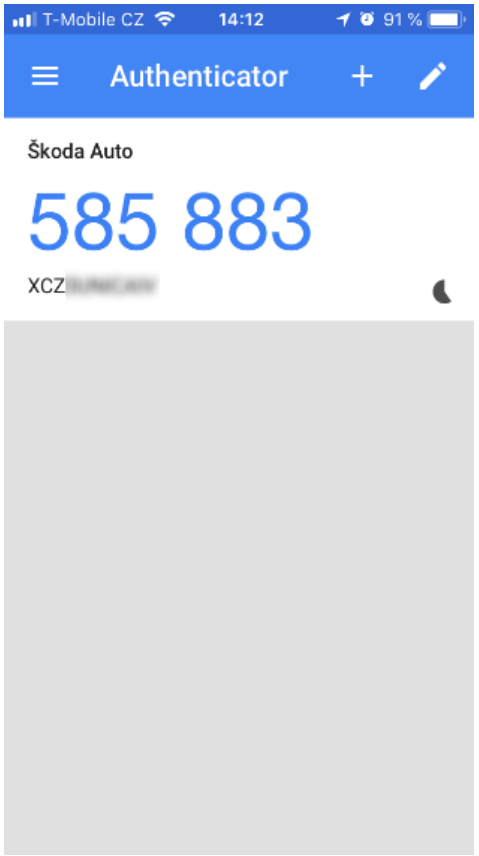
In case user has got only one device registered and activated, the device is chosen automatically and user is redirected to step 5 directly.

Continue

User name + password + One-time password from Authenticator

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

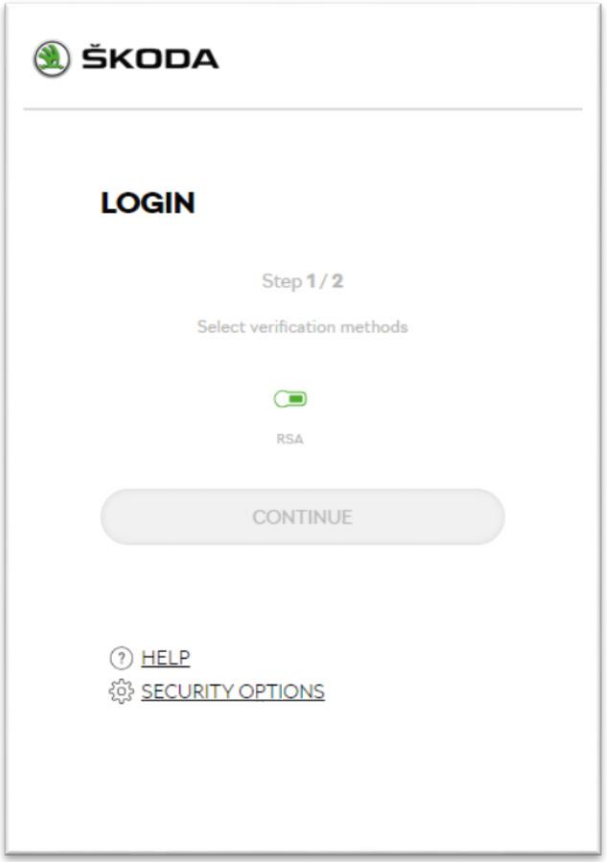


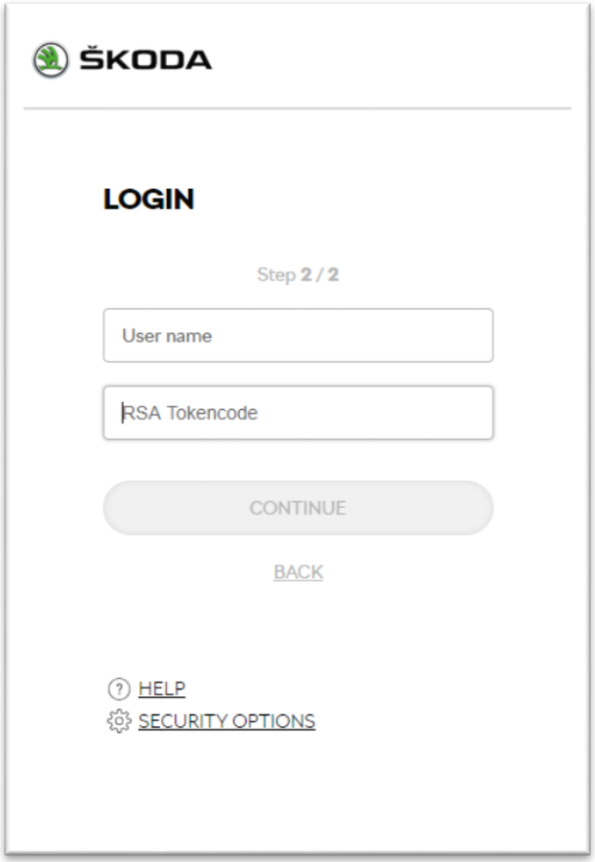


User name + Tokencode

Login instructions:

1. Enter the required URL.
2. Enter:
    - User name.
    - PIN + Tokencode.
3. Choose method of authentication RSA and confirm.
4. You are logged in.





PKI (Employee 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

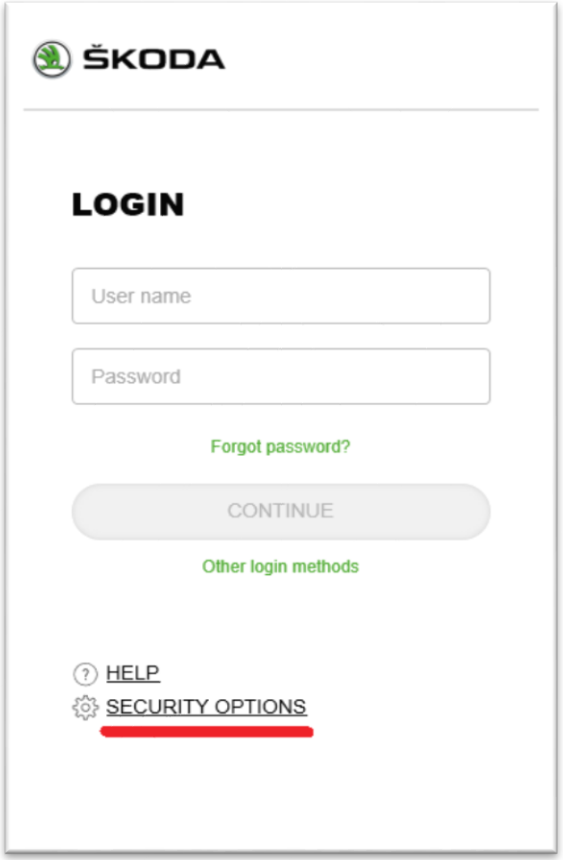
Click "Security options" for adding new device.

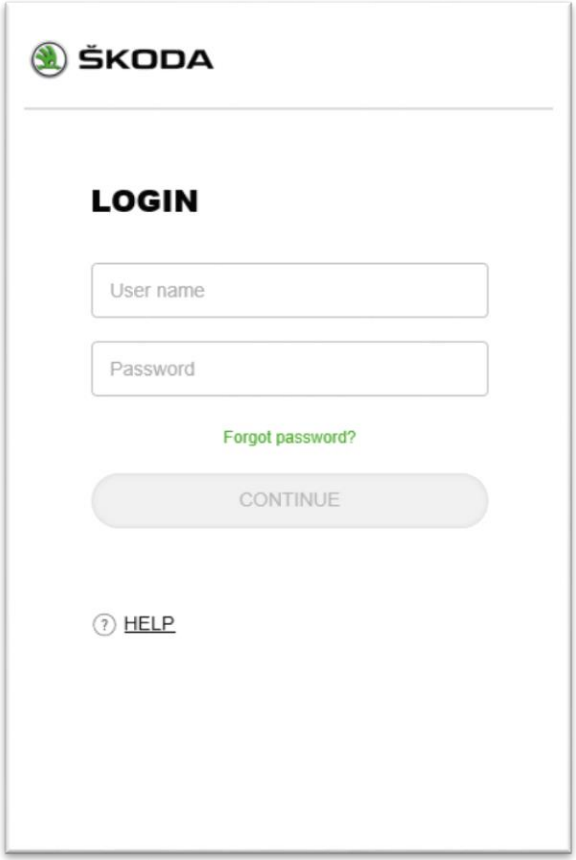
1. Click the link "Security options" - new tab will be opened.

2. Enter:

   - User name.
   - Password.

3. You are logged in.





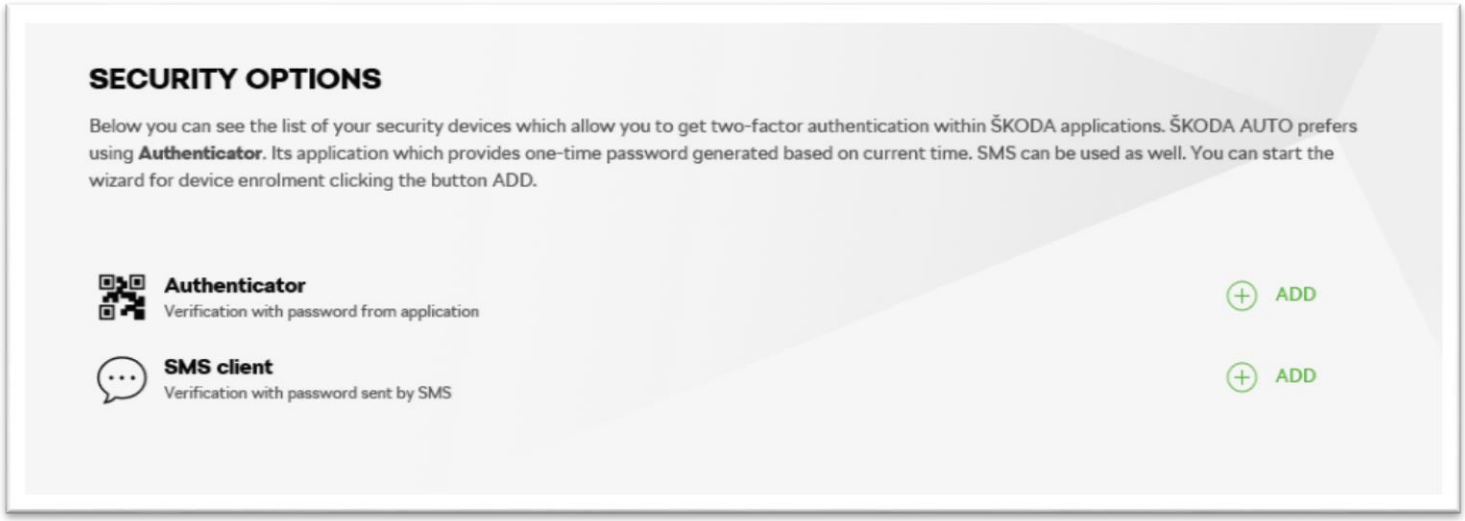
Continue

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.

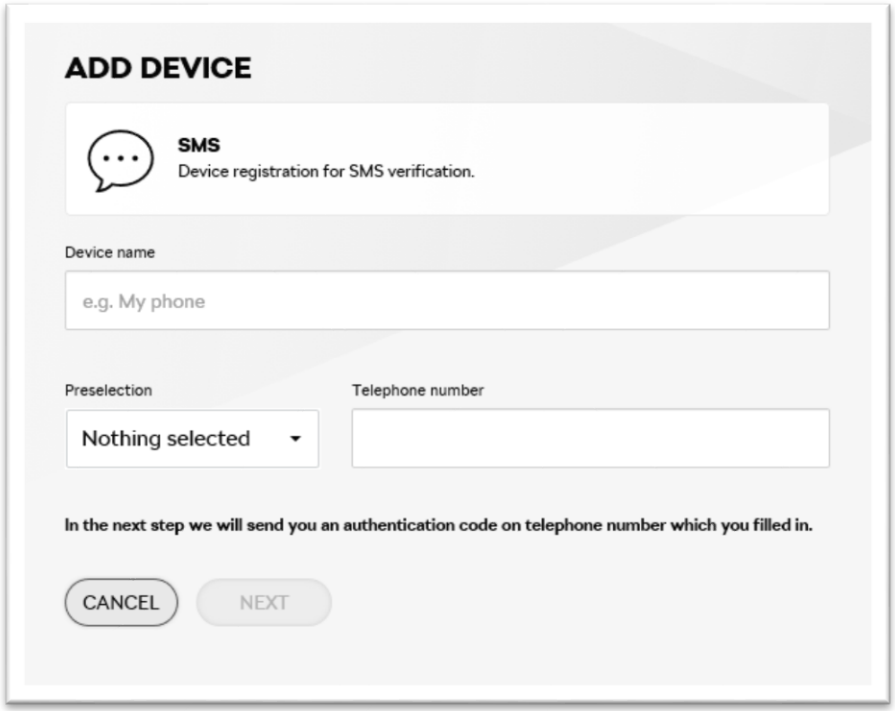
SMS

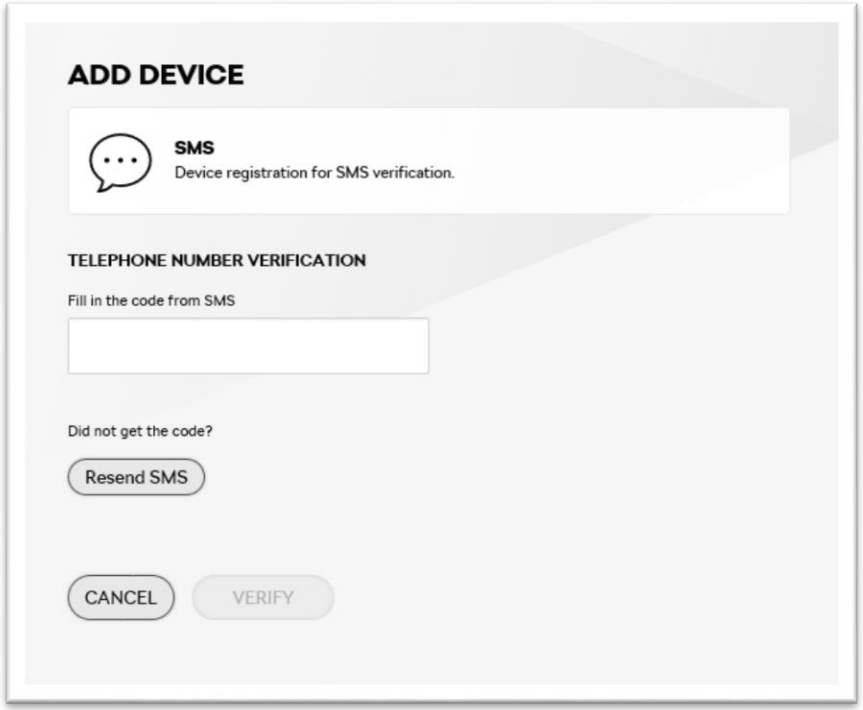
Authenticator



SMS

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





- The user is asked to enter the code from to SMS and confirms it.

Activation

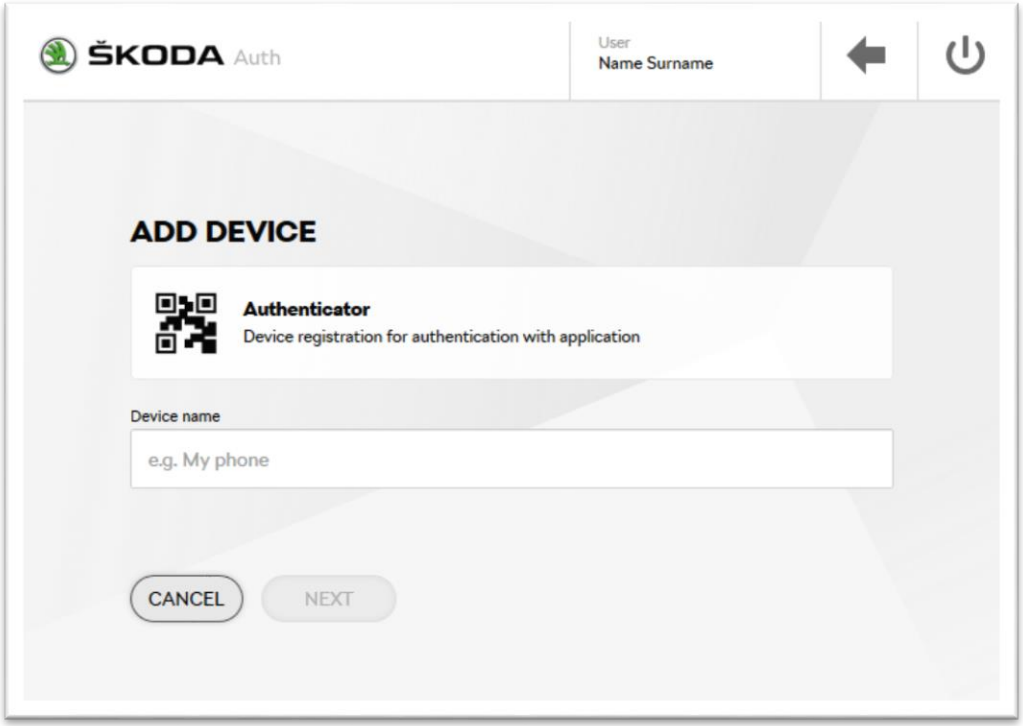
Authenticator

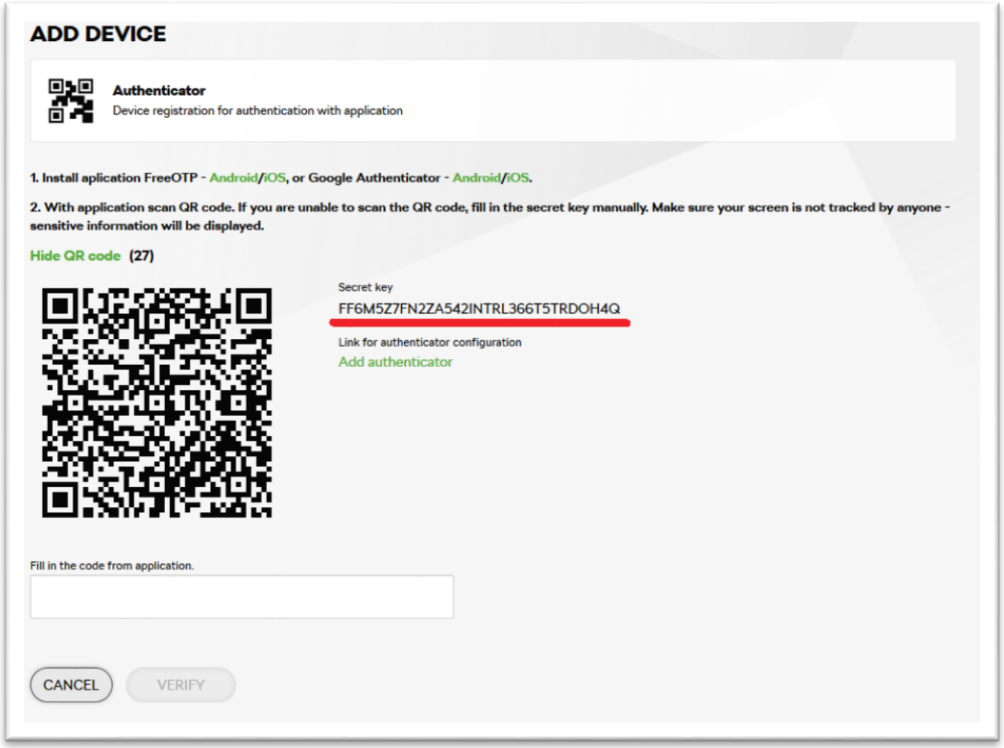
Authenticator – web browser application

Authenticator – mobile application

Authenticator registration

- 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 browser addon. Follow „Firefox addon installation guide“.

Continue

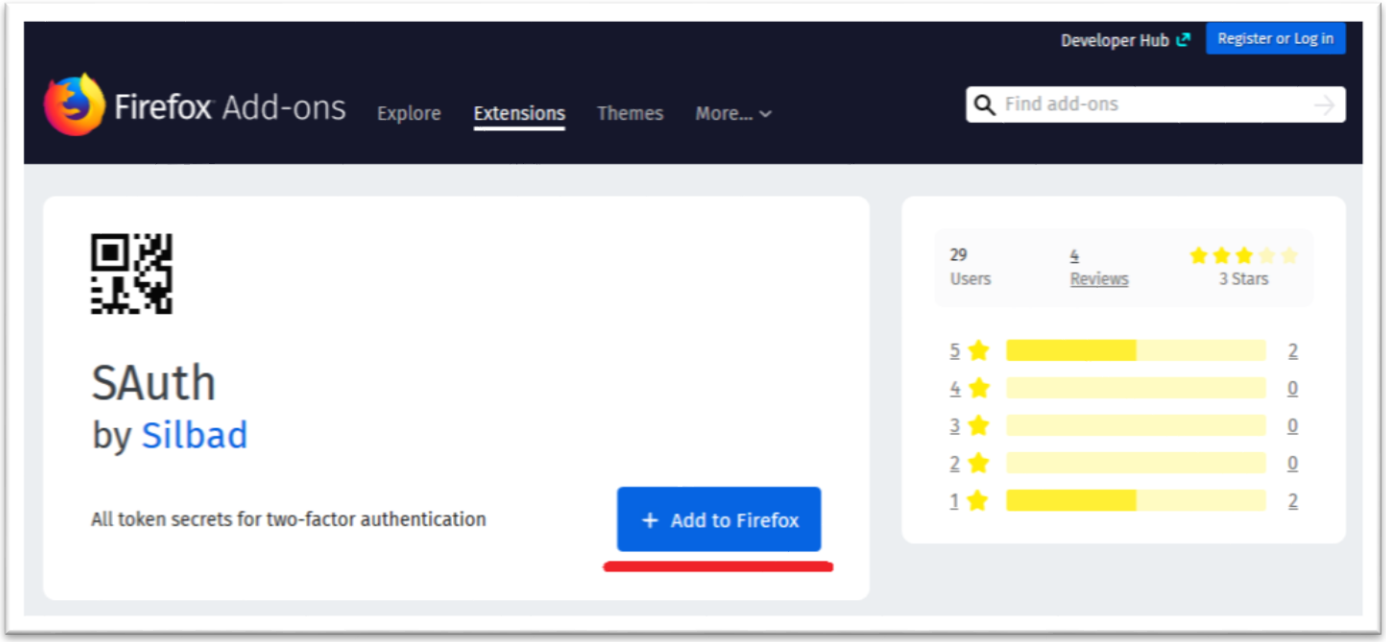
Firefox addon installation guide

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.

Attention: The guide is based on 3rd party application. We reserve the right to make changes.

If you don‘t have got the FF installed, follow this link: https://www.mozilla.org/firefox/new/

3.Open following URL in Firefox - https://addons.mozilla.org/firefox/addon/sauth/
4.Click the button “Add to Firefox“.

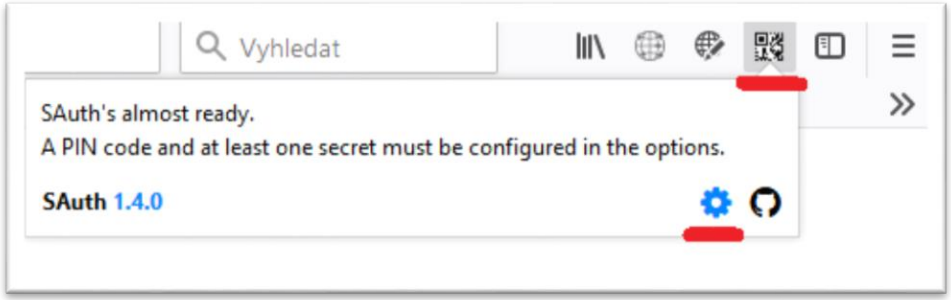


5.Accept the confimation dialogue. Click “Add“.

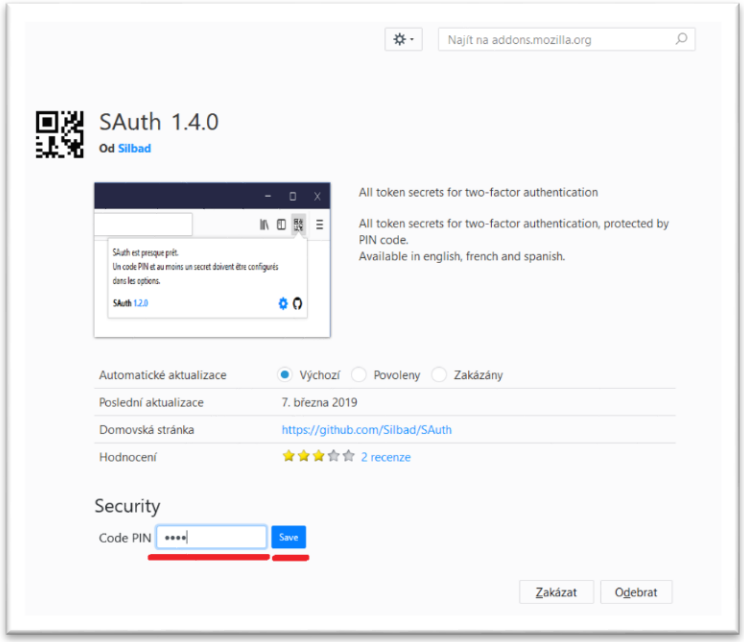
Continue

Firefox addon installation guide

6.Launch the Sauth appliacation.



7.Enter PIN and click “Save“.



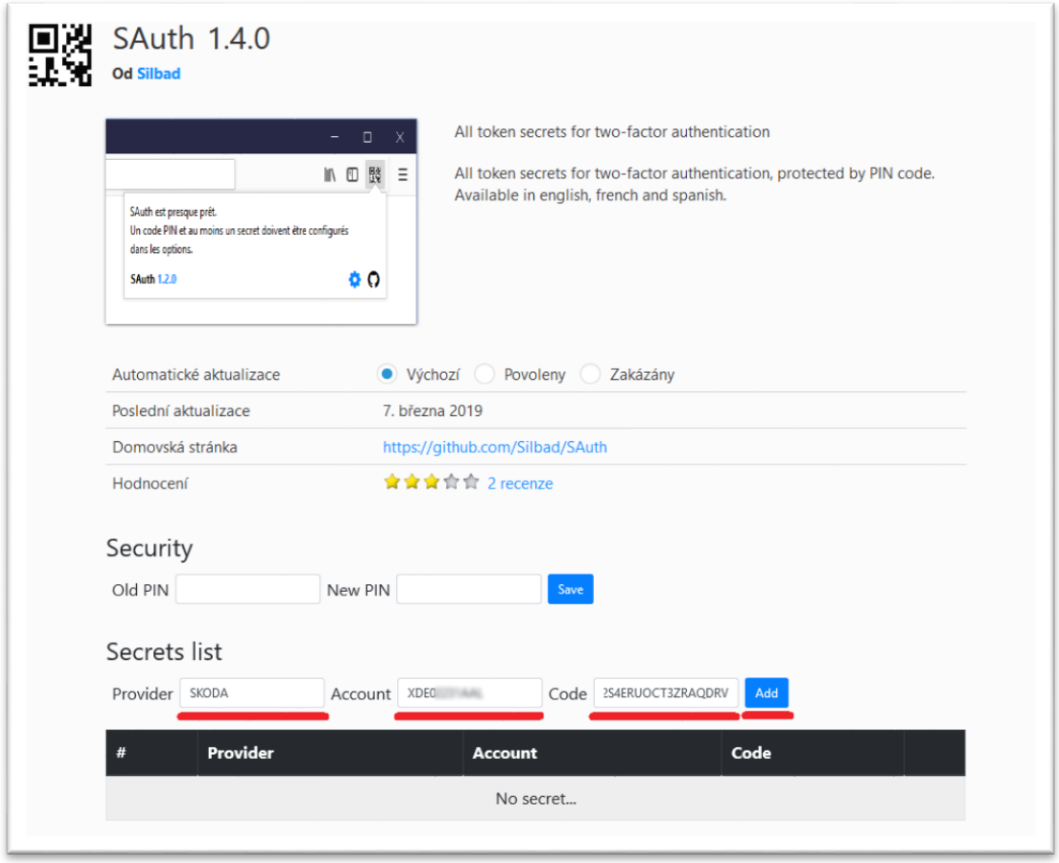
Continue

Firefox addon installation guide

8.In “Secrets list“ enter parameters:

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

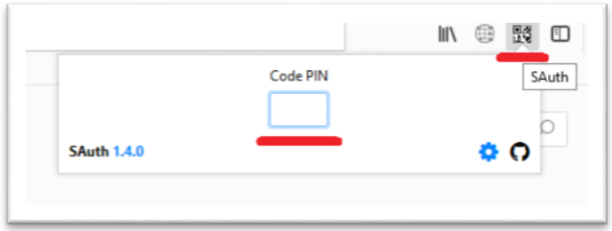
Click the button „Add“.



9.The device is succesfully added to the application and it‘is ready to use. You can close the window.

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

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

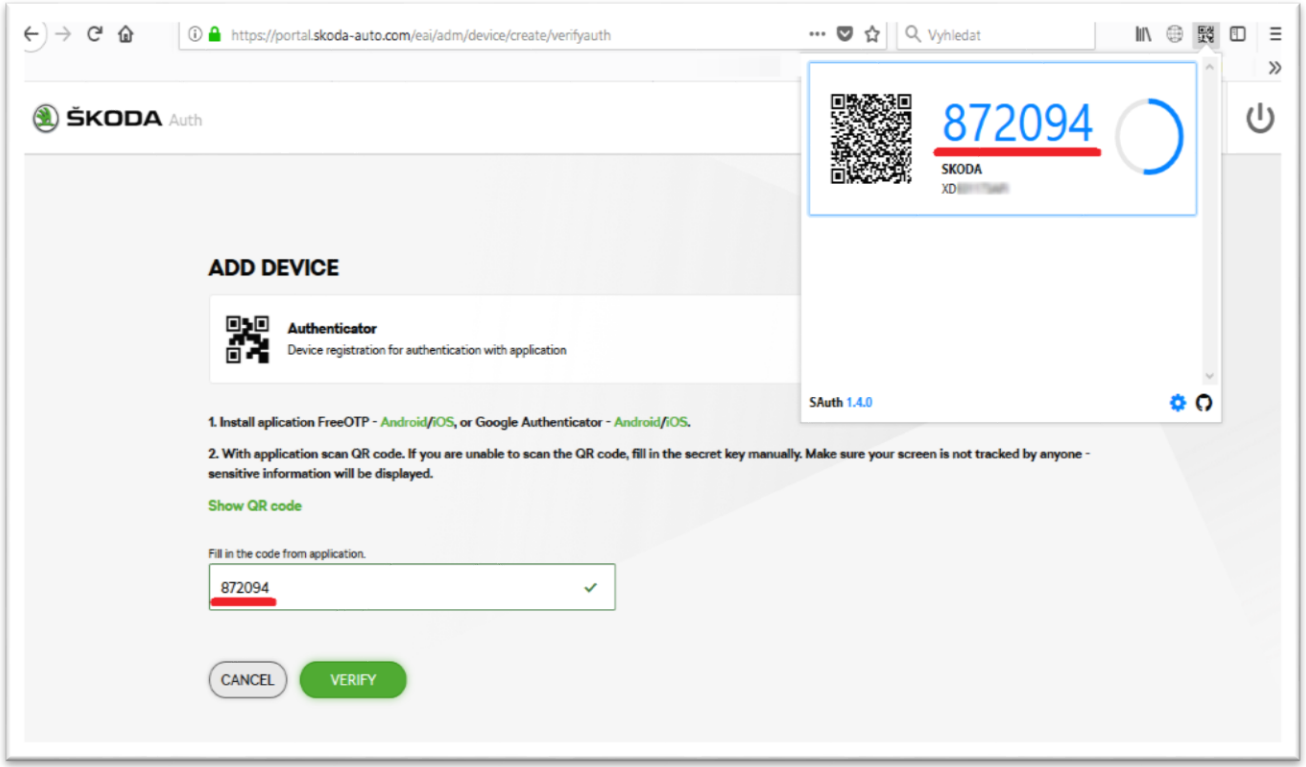


Continue

Firefox addon installation guide

Go back to the Security Options:

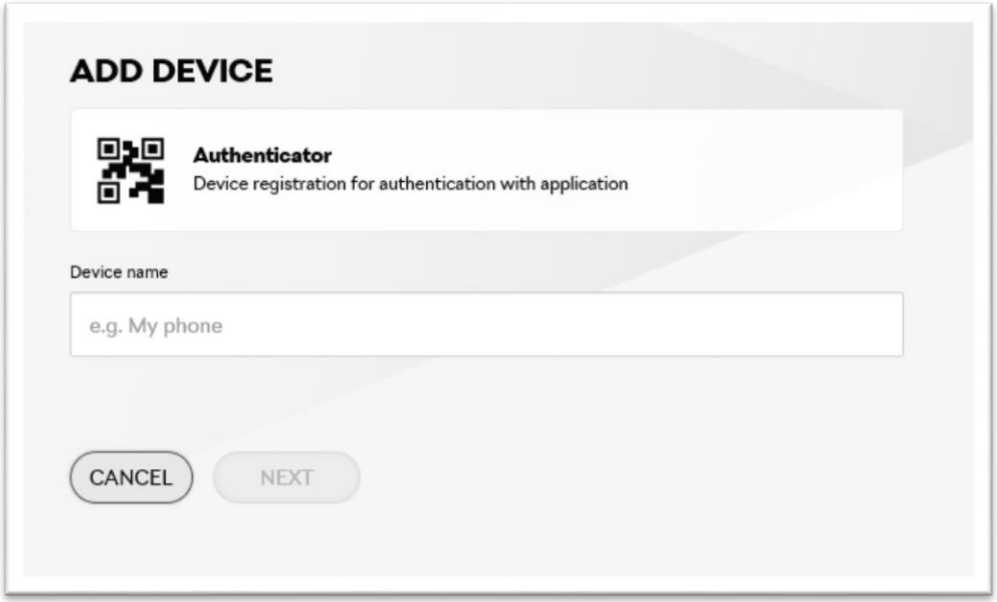
11. Re-type the generated code to the SECURITY OPTIONS. (It sould be done within 30 seconds).
12.Click the button “Verify“, the device is created.



Activation

Authenticator registration

- Enter:
  - Name of your device.



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

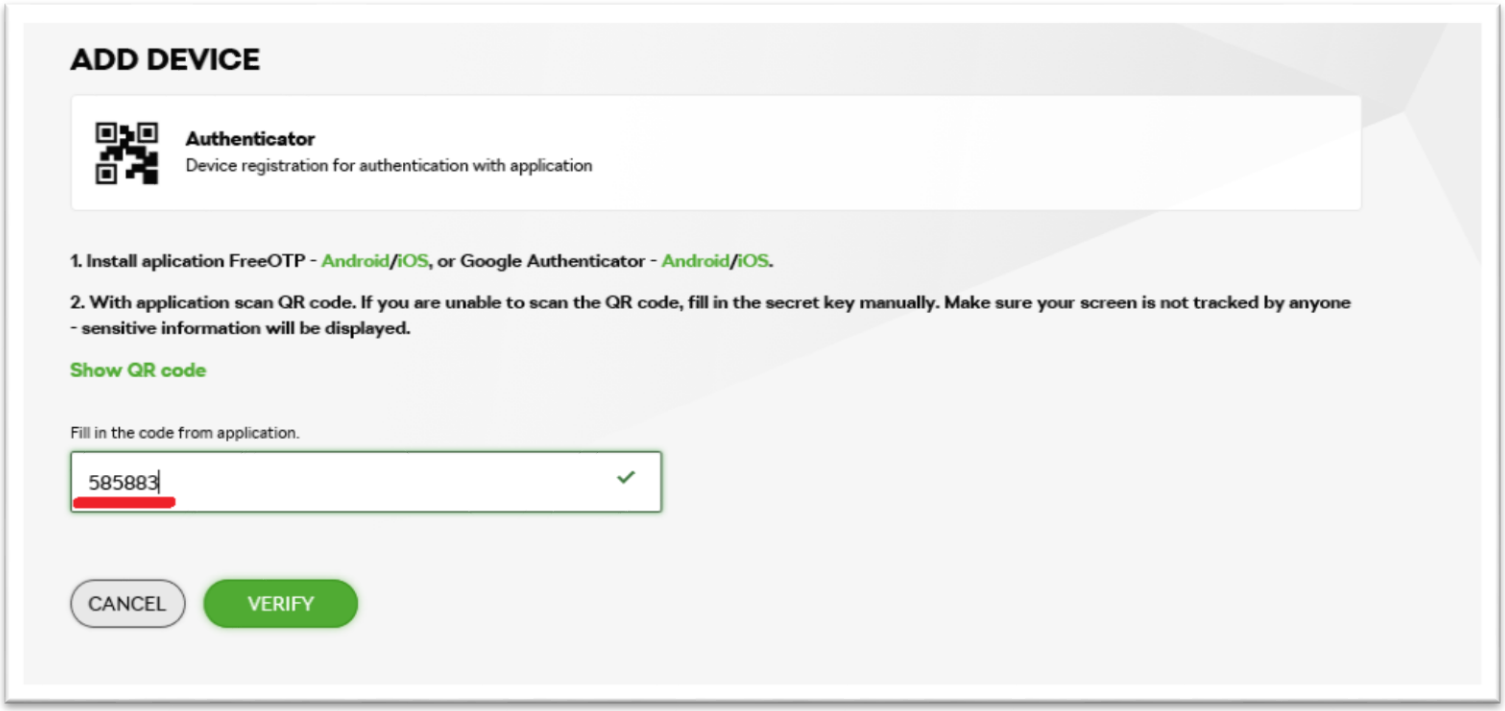
Continue

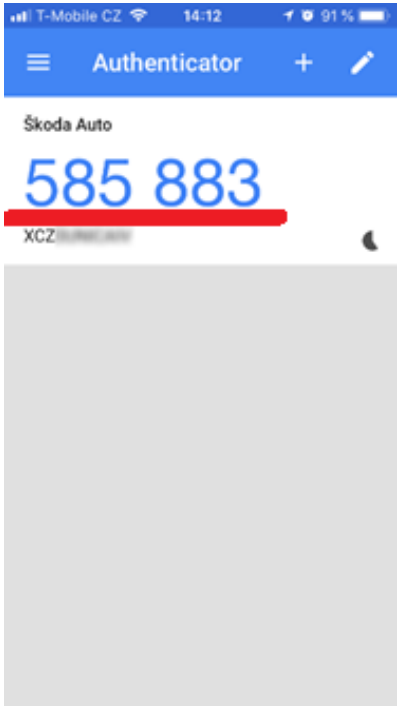
Authenticator registration

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.





Activation

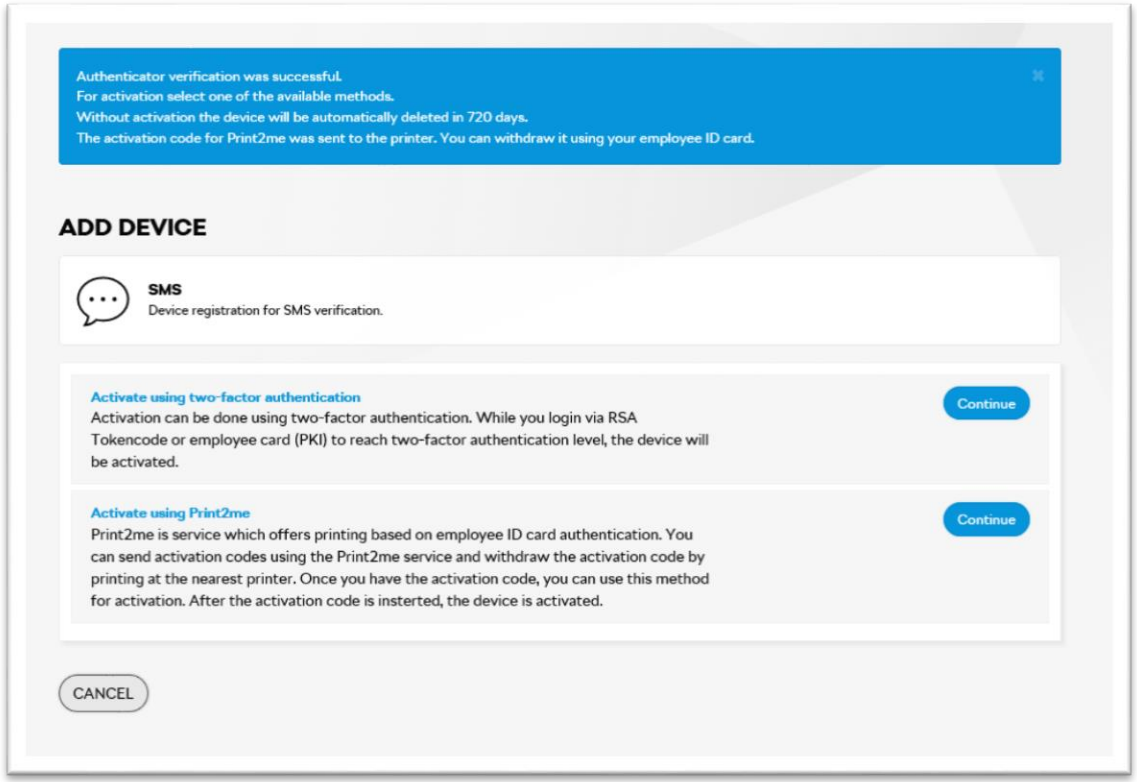
Activation

ŠKODA AUTO employee

Other B2B users

Device activation for ŠKODA AUTO employee

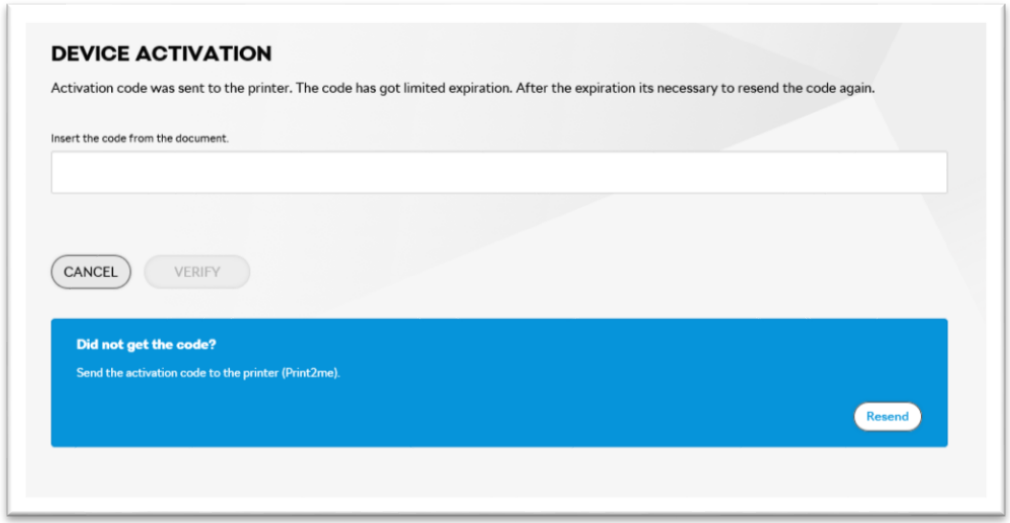
- List of available activation methods is dyplayed:
  - Activation using two-factor atuhentication
  - Activation using Print2me
- User chooses the wanted method by clicking the appropriate button Continue



Continue

Device activation for ŠKODA AUTO employee

- 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.

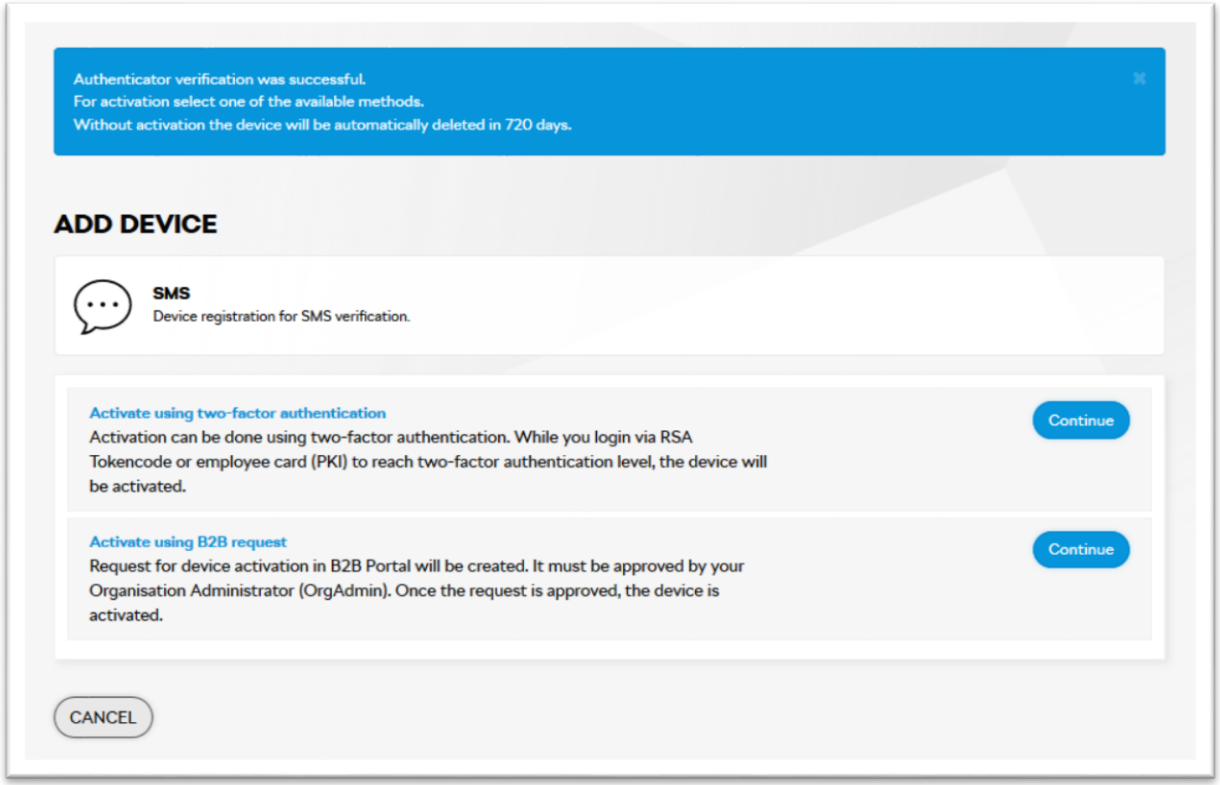


- Activation using two-factor authentication
- User is redirected to Login page where are two-factor methods available - SMS, Authenticator, RSA.
- Once user is logged in the device is activated within Security options.

Login

Device activation for other B2B users

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



Continue

Device activation for other B2B users

- Activationusing 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.
- 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.

Login

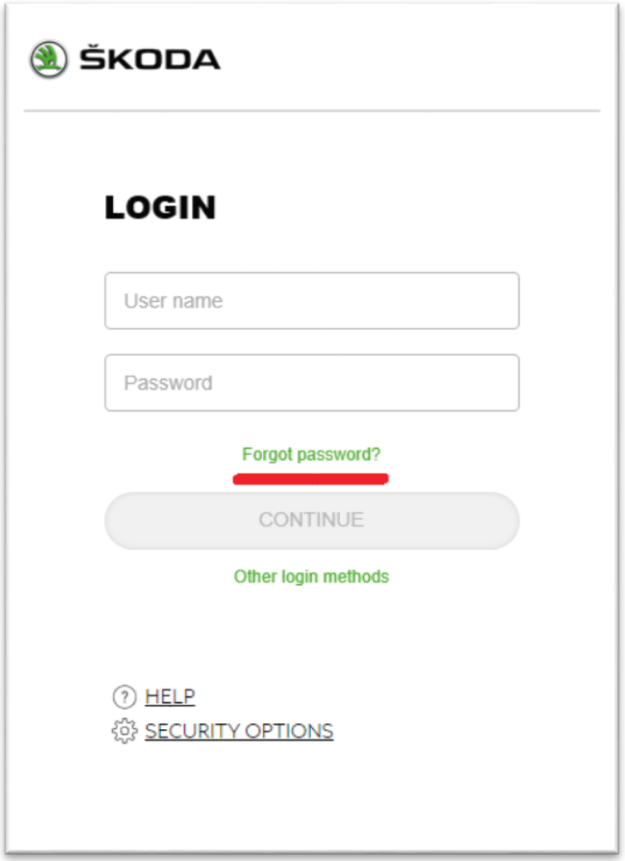
Password reset

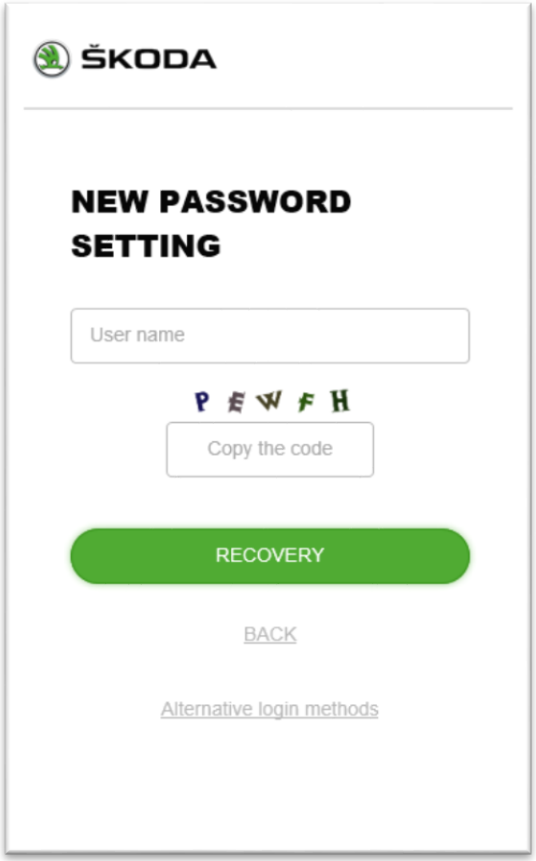
- It is possible to reset your password on login page of B2B Portal.
- The link „Forgot password“ is available in the „Basic login“ screen and as well from second step of SMS and Authenticator login method.

Instructions:

1. Click the link „Forgot password?“
2. User enters and confirms:
    - User name
    - 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.





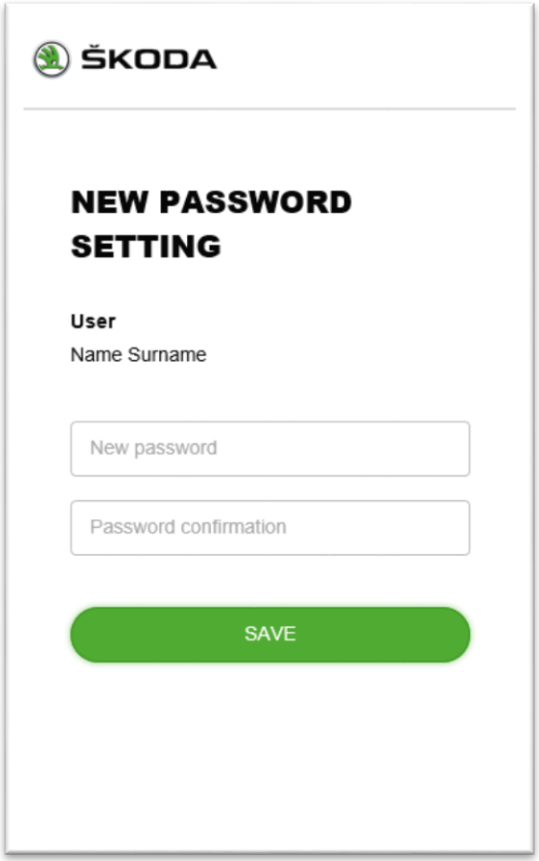
Continue

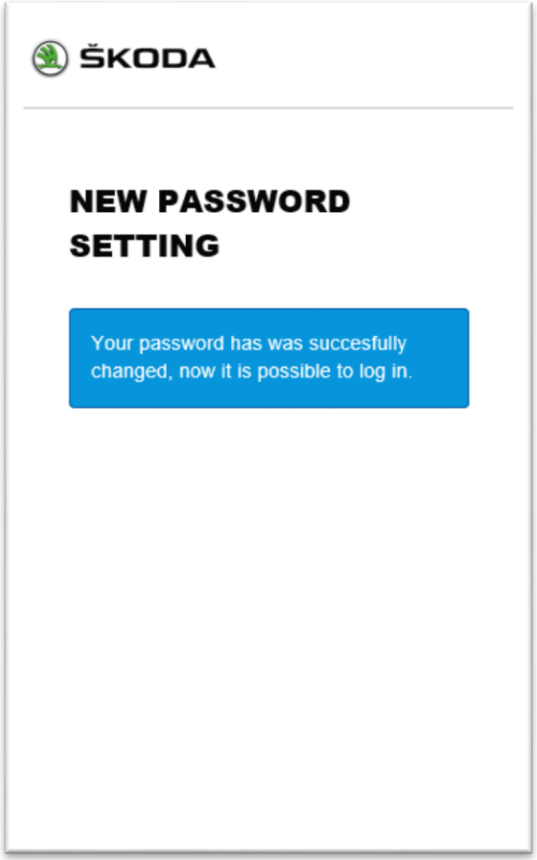
Password reset

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 successfull password change is displayed.



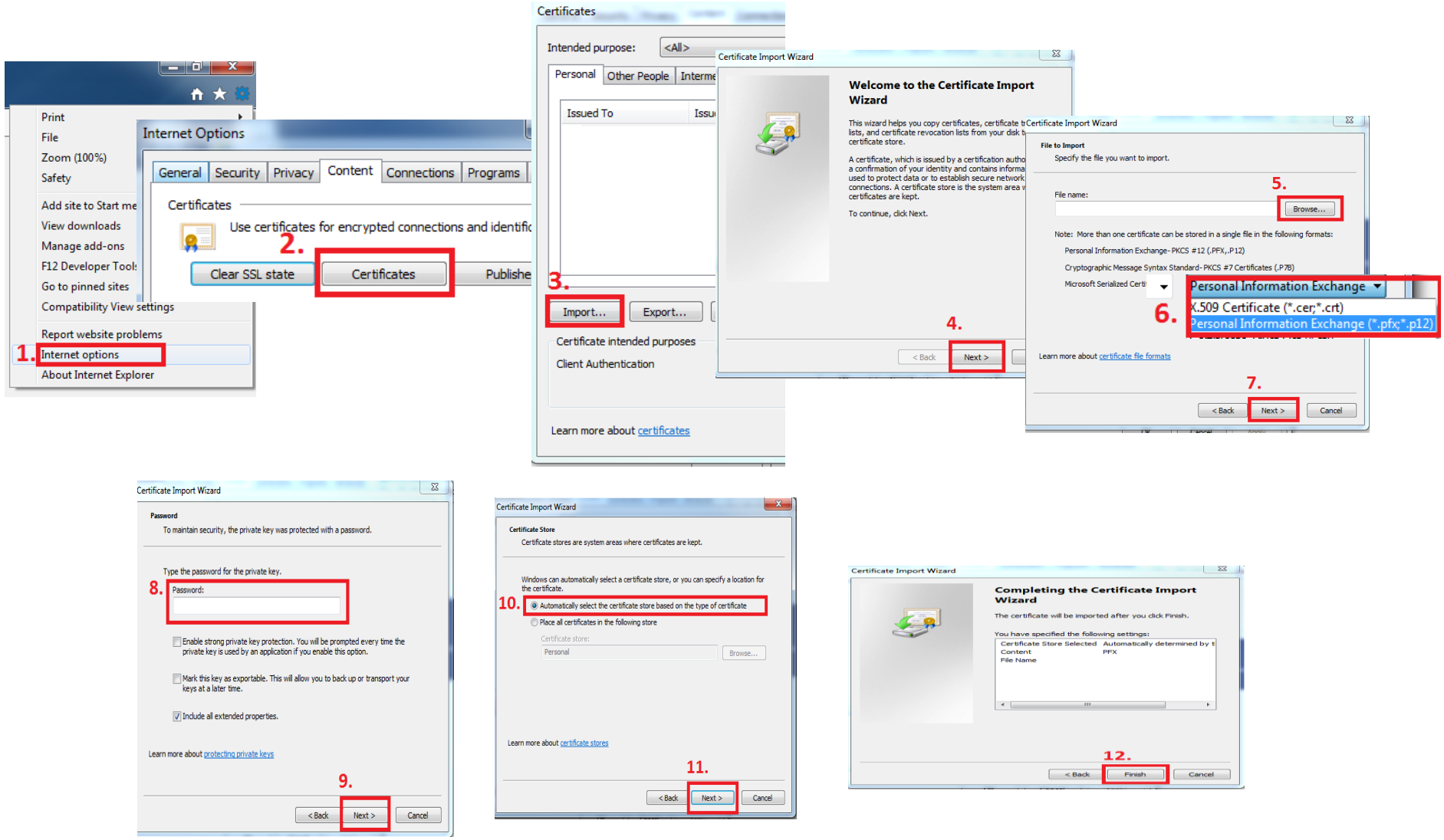


Certificate installation

Internet Explorer

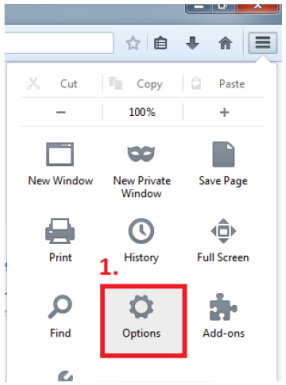
Mozilla Firefox

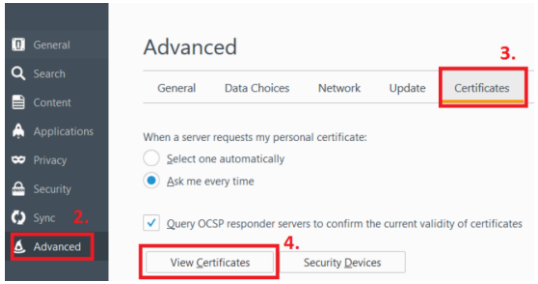
Internet Explorer – certificate installation

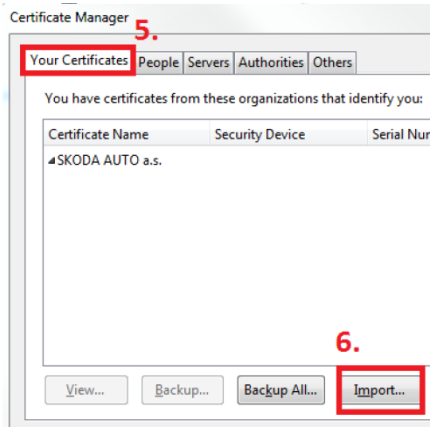


1) Internet options
2) Certificates
3) Import
4) Next
5) Browse
6) Choose ***.pfx*.p12** and choose your certificate
7) Open
8) Enter password from PDF file
9) Next
10) Choose automatically...
11) Next on next screen again
12) Finish

Mozilla 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

ŠKODA

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

Date ..... signature

Classified information

yes ☐ no ☐

Control of user´s integrity*

yes ☐ no ☐

Approved by (superior of user)

..... 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 ..... department ..... signature

* => Checks a fils in the superior of user, in case of confidential information
** = ~~ovšem~~ 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" ~~and~~ "Sustaining a confidential ~~information~~".

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

Ev. č. / ~~Svůj~~ 1701 ŠKODA AUTO a.s., Tř. Václava Klementa 869, 293 60 Mladá Boleslav, Czech Republic

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 expires 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 have to be verifying on the same device. For another login you will use only Login + your password to B2B Portal.

Rules for code from Autenticator

- 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 have to 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.

Login for 24 hours

- The expiration time for SMS code or Authenticator is 24 hours. Within one day you're no longer asked for two-factor authentication – you're logged in if basic credentials are inserted (Username + password) and SMS or Authenticator method is selected. You can use this feature if you're using the same device (PC, Tablet...).

Continue

Login

Expiration time for Password recovery link

- The expiration time for password recovery link is 24hours. In case the link is already used / expired appropriate message is displayed and the recovery process must ne repeated.

Fingerprint2

- In case you use Adblock which is set for blocking Fingerprint2 library, the feature of login for 24 hours is lost and you will be asked for SMS or Authenticator code.

Registration

Rules for one-time password

- Sending SMS is possible up to 3 times.
- Password is valid for 15 minutes.

Rules for verification code

- Stays in printer for 24h. After this time it is necessary to send the key again.
- Code is valid for 2 days.
- If you have more devices registrated, all keys, that have validity longer than 2 days, will be sent. It is not defined, which key belongs to which device. You can use the key only once and with arbitary device.