SECURITY CODE

Sobol
Version 4

Basic Operations

User Guide

Mailing address:	**P.O. Box 66, Moscow, Russian Federation, 115127**
Phone:	**+7 495 982 30 20**
Email:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Table of contents

Introduction

This guide is designed for users of Hardware Trusted Boot Module Sobol. Version 4 (hereinafter Sobol). It contains information that users need to work with Sobol.

Document structure

The guide is organized in the following way:

- the **Power on computer** section describes how to log on to the information system from a computer with Sobol;
- the **Change password** section describes how to change the individual password and Secure ID of Sobol;
- the **Shut down and restart computer** section describes how to shut down a computer with Sobol.

Additional information

Web- site. Information about Security Code products can be found on https://www.securitycode.ru.

Training. You can learn more about hardware and software products of Security Code in authorized education centers. List of the centers and information about learning environment can be found on https://www.securitycode.ru/. You can contact company representative for more information about organization of teaching process by email: education@securitycode.ru.

Power on computer

To make you able to work on a computer with Sobol, the administrator must register you as a Sobol user and give you the credentials listed in the chapter below.

After the user provides credentials and the control objects integrity is checked (if the integrity check mechanism is enabled by the administrator), the computer OS boots.

User credentials

Credentials are used to verify the user access to a computer.

To power on a computer with Sobol, a user needs the following credentials:

- security token which includes the user Secure ID.

  Note. Secure ID is a data structure that is involved in the procedure of user authentication. Each user has a unique Secure ID.

  The following types of security tokens are used in Sobol:

iButton keys	USB keys	Smart cards
DS1992	Rutoken	Rutoken Lite
DS1993	Rutoken Lite	
DS1994	Rutoken RF	
DS1995		
DS1996		

- password which corresponds to the security token;
- security token PIN (can be enabled when using USB keys and Smart cards)

Remember your password and PIN. Do not share them with anyone.

Keep your security token with you, it is needed every time you power on your computer.

Boot an OS

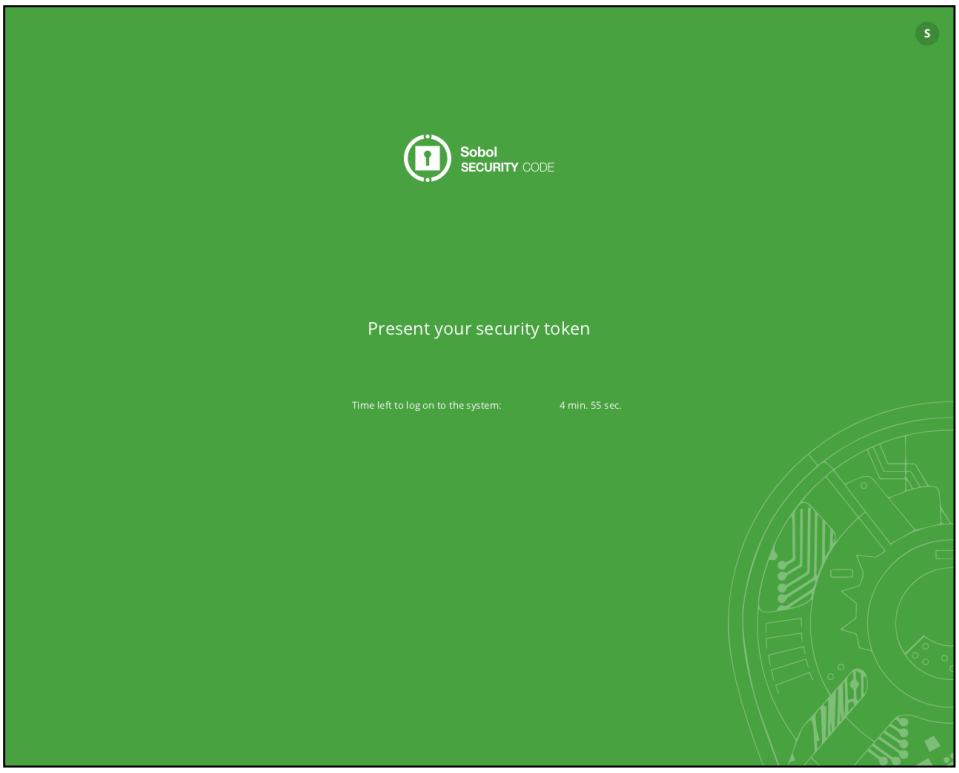
Attention! Before powering on a computer with Sobol, disconnect all USB Mass Storage devices (flash drives, CD, DVD drives, etc.) from USB ports.

To boot an OS:

1. Power on your computer. The **Getting ready...** window appears.

   Note. If any error occurs during this step, contact the administrator.

   When Sobol boot is completed, you are prompted to present your security token.



   In the top right corner, you can see Sobol operation mode: **S** is for standalone mode, **J** is for joint mode.

   Note. Joint mode means that Sobol operates in tandem with other products (for example, Secret Net Studio).

   In the center of the window, a timer may appear counting down:

   - automatic logon timeout (in seconds) or
   - timeout for presenting your security token and entering the password (in minutes and seconds).

   Note.

   - Automatic logon timeout is displayed if Sobol is configured to boot automatically. In this case, you do not need to enter any credentials. When the specified time is over, the integrity check is performed (if the integrity check mechanism is enabled) and an OS boots (see p. 8).
   - The time left to present your security token and enter the password is displayed if the administrator has enabled the logon timeout. If you do not have the time to present your security token and enter the password, the computer will be blocked. Restart your computer and log on again.

2. Present your security token:
   - for iButton — place the security token to the reader;
   - for USB key — plug the security token in to a USB port;
   - for Smart card — plug the security token in to a USB smart card reader.

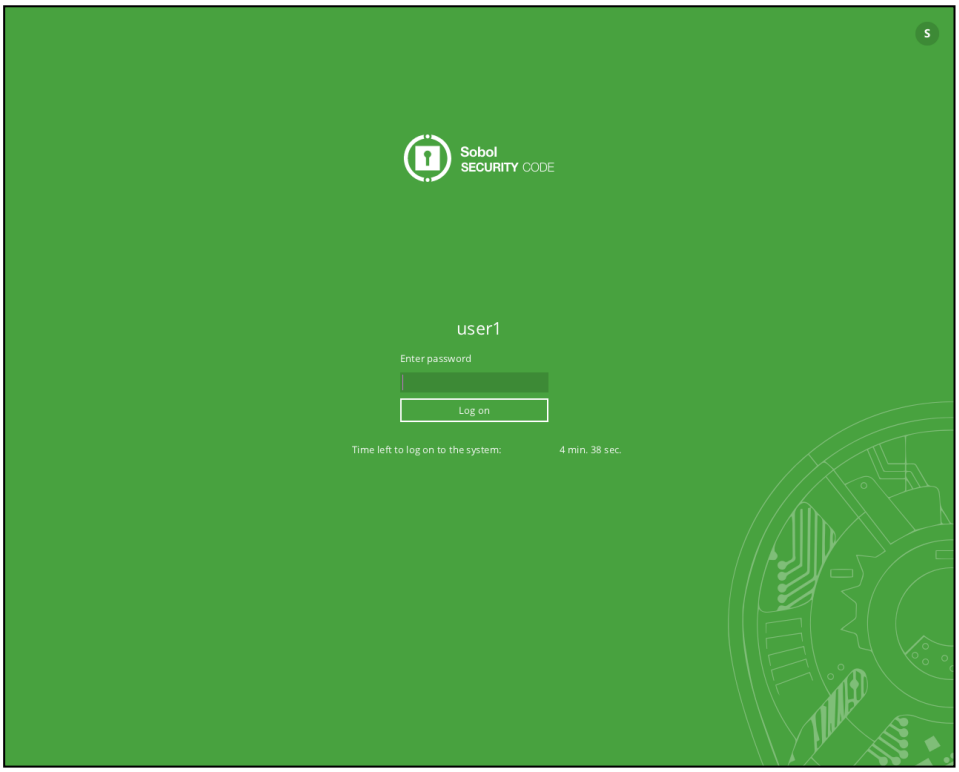
Note.

- If a security token is already presented (iButton is in contact with the reader / USB key is attached / smart card is in contact with the reader), Sobol automatically reads it.
- If several security tokens are presented, Sobol reads the first one being detected. To change the security token, press **Esc**.
- If the security token is presented incorrectly, the request will remain on the screen. Present the security token again.
- When the message **Logon is prohibited by administrator** appears, click **OK** and consult the administrator to find out the cause of blocking.

After you presented you security token,you are prompted to enter the PIN.

Note. The PIN request appears, if the administrator has set a PIN for your security token. If the request appears, enter the PIN and click **OK** or press **Enter**.

After the security token information is read successfully, you are prompted to enter your password.



Note. The password request will not appear if your password has zero length (blank password).

3. Type your password and click **Logon** or press **Enter** .

Note. All entered characters are displayed as **"*"**.

Attention!

- If the presented security token is invalid or the password is incorrect, the message **Invalid password or security token** will appear. Click **OK** and repeat steps **2–3**. Use your security token and enter the valid password.
- The number of unsuccessful logon attempts per session is 5. If you exceed the limit, your computer will be blocked. In this case, contact the administrator.
- The total number of unsuccessful logon attempts can be limited by the administrator. If you exceed this limit, the next time you try to log on, a message indicating that your computer is blocked will appear. In this case, contact the administrator.
- When the **This password does not meet complexity and/or minimum length requirements** or **Password expired** message appears:
  - if you are allowed to change the password, click **OK** and change it by following the instructions on p. 10.
  - if you are not allowed to change the password,the computer will be blocked. Contact the administrator.

If the password is entered successfully, a window similar to the following appears.

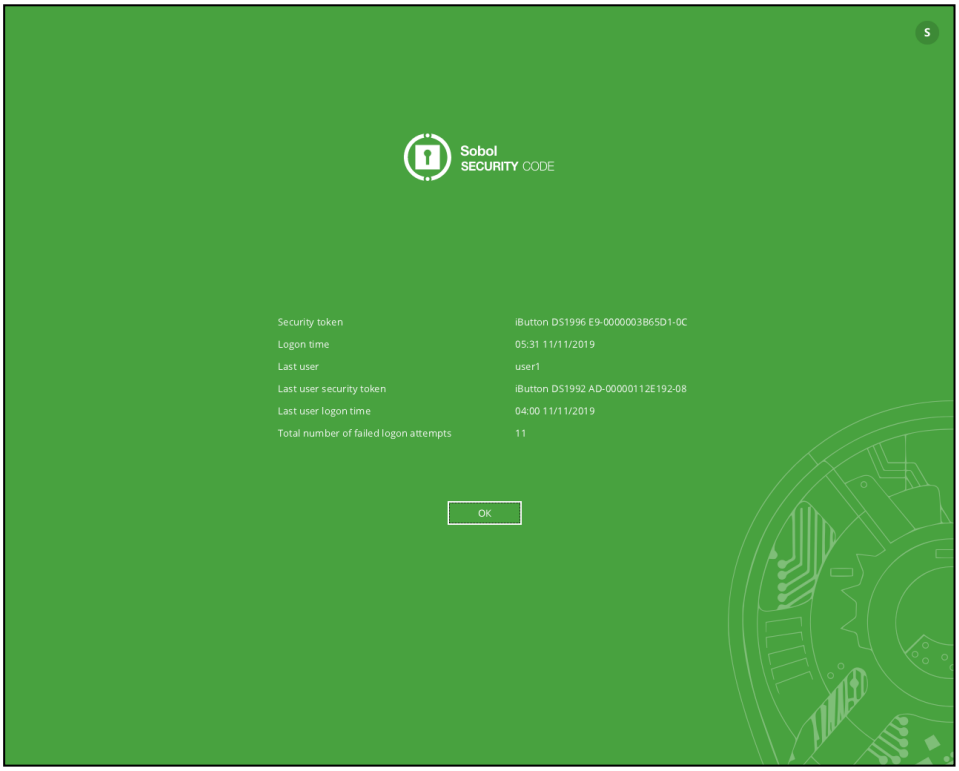


Fig. 1 Sobol window

Note. The window may contain the help information (see p. 9).

4. Click **Boot OS**.

After you presented your credentials, one of the following actions is taken:

- an OS boots;
- integrity check starts if the integrity check mechanism is enabled by administrator.

Note. Before the integrity check, the IC key can be updated with further checksum recalculation.

If the integrity check is successfully completed, the OS starts to boot.

Note.

- In case of an error, the check stops and an error message appears. Click **OK**.
- If you do not want to receive notifications during the integrity check, select **Don't ask anymore** in the error message window.
- When the integrity check is complete, click **Finish**. The message **Controlled object integrity violated** appears.
- If a hard integrity check mode is enabled, the computer will be blocked in case the control objects integrity is violated. Shut down the computer and contact the administrator.
- If a soft integrity check mode is enabled, you will be able to continue working on the computer in case the control objects integrity is violated. Click **OK**. The OS starts to boot.

Help information

If the help information display is enabled, after the credentials are entered, a window appears as in the figure below.

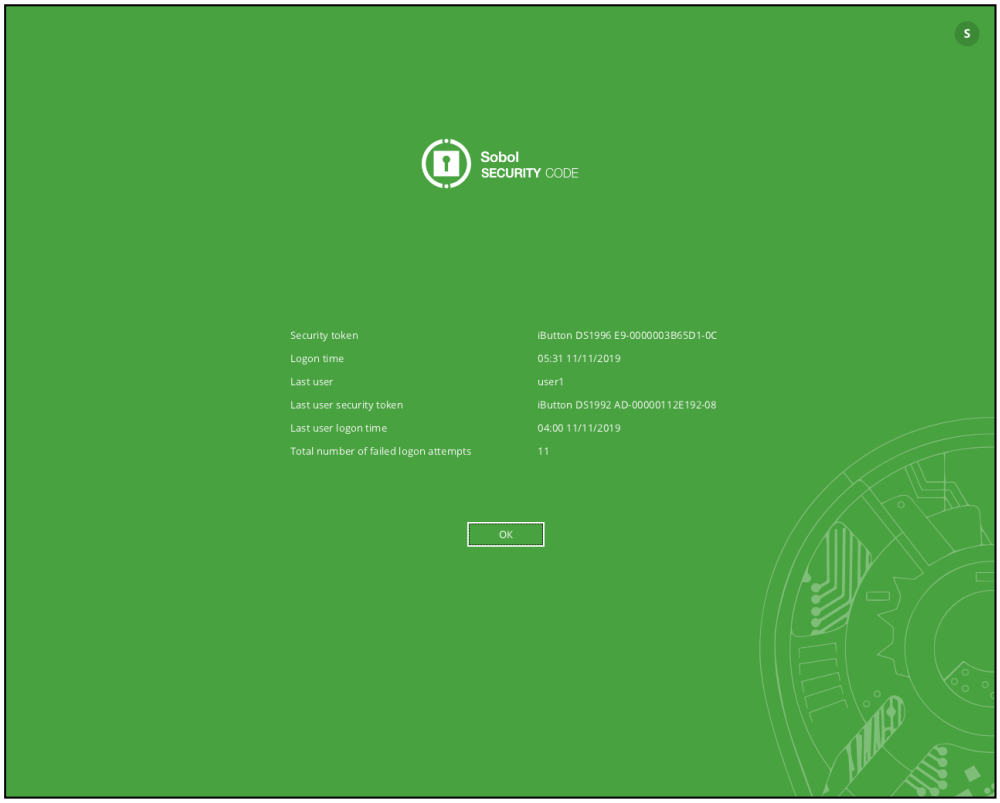


Fig. 2 Help information

Note. Help information is not displayed in joint mode.

The window displays the following information about the user account:

Parameter	Description
Security token	The type and number of the security token you present
Logon time	Time (hours:minutes) and date (day/month/year) of your successful logon in the current session
Last user	The name of the last user that logged on to the system
Last user security token	The type and number of the security token that the last user presented logging on to the system
Last user logon time	Time (hours:minutes) and date (day/month/year) of the last user successful logon
Total number of failed logon attempts	The number of all failed logon attempts performed on current computer

Change password

You can change the password by yourself if it is allowed by the administrator.

Note. When changing the password, the Secure ID can also be changed if this mode is enabled by the administrator.

To change the password:

1. After you presented your credentials, in the Sobol window (see Fig. 1 on p. **8**), click **Change password**.

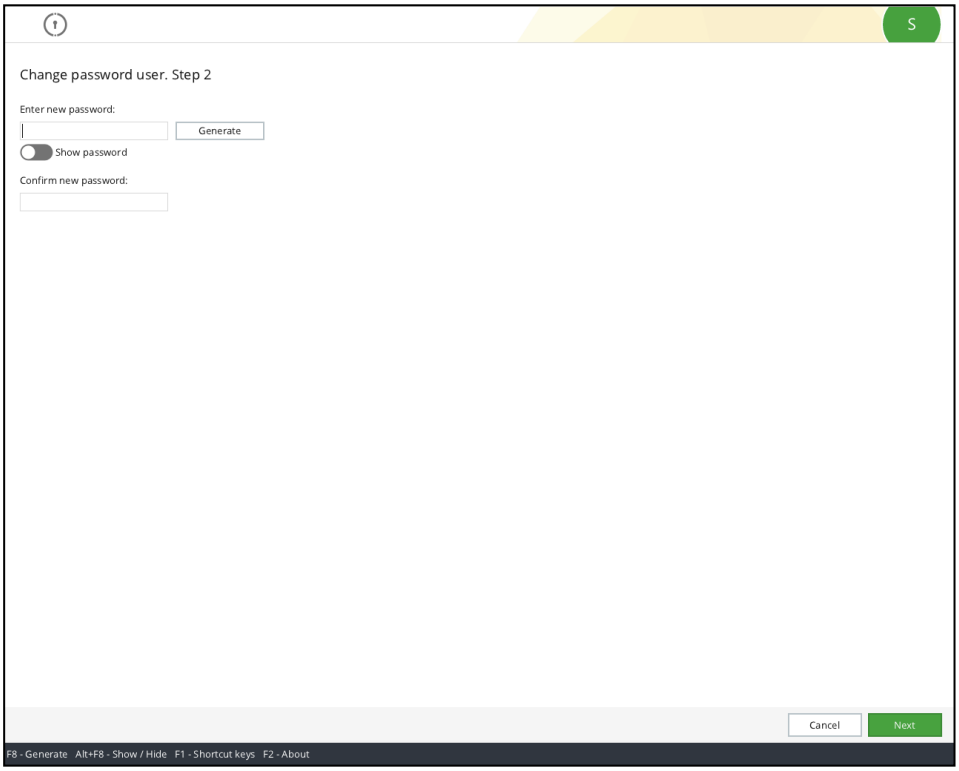
   Note. If the **Change password** button is inactive, you are not allowed to change the password.

   Your current (old) password appears on the screen.

2. Enter your current (old) password and click **Next**.

   Note. You can use the shortcut keys. To view the shortcut keys, press **<F1>**.

   The window to enter a new password appears.



3. In the **Enter new password:** field, type a new password or use the random password generation function.

   Note.
   The password can only contain the following characters:
   - 1234567890 — digits;
   - abcdefghijklmnopqrstuvwxyz — lowercase Latin letters;
   - ABCDEFGHIJKLMNOPQRSTUVWXYZ — uppercase Latin letters;
   - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — special characters;

   To generate a random password, click the **Generate** button or press **<F8>**.

   Note. When generating a random password, take into account the following:
   - if password complexity check is enabled, the generated password meets the complexity requirements set by the administrator;
   - If the password complexity check is disabled, the generated password consists of lowercase Latin letters and digits;
   - a generated password can be edited.

To view the password, press **Alt + F8** or turn on the **Show Password** toggle.

4. Remember the entered/generated password and enter it again in the **Confirm new password:** field.
5. Click **Next**.

Note. If the password you entered is incorrect, the message with an error description appears. Click **OK** and enter the correct password.

After the password is entered successfully, a security token request appears.

Tip. Before you present your security token, you can cancel the password change. To do this, click **Cancel**.

6. Present your security token.

Note.
- If a security token is already presented (iButton is in contact with the reader / USB key is attached / smart card is in contact with the reader), Sobol automatically reads it.
- If several security tokens are presented, Sobol reads the first one being detected.

If the administrator has set a PIN for your security token, PIN request appears after security token presentation.

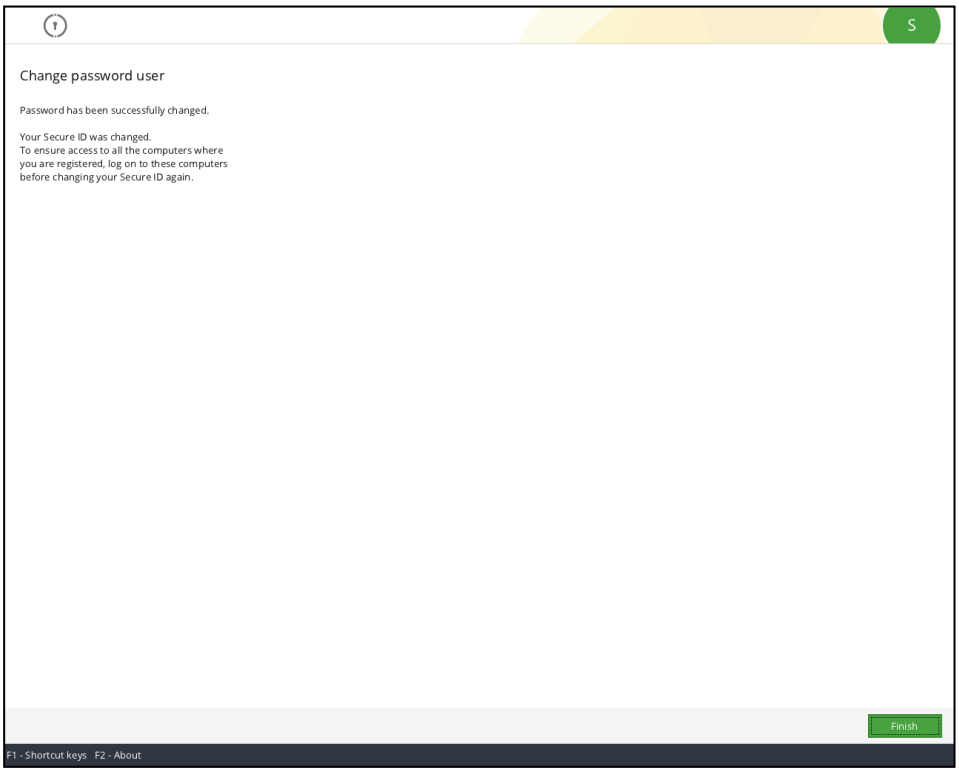
Note. When PIN request appears, enter the PIN and click **OK**.

When the security token is presented correctly, the entered old password is compared to the information stored in the security token memory:

- if the old password does not correspond to the presented security token, a warning **Invalid password or security token** appears. Click **OK**. Present your security token or click **Cancel** and change the password;
- If the old password corresponds to the presented security token, the security token saves the new password service information.

After service information is successfully saved, you receive the **Password has been successfully changed** message.

If your Secure ID is changed with your password , you receive the following message.



You need to log on with the changed Secure ID to each computer where you are registered as the Sobol user at least once before changing the Secure ID again.

Note. Your security token stores two Swcure IDs (the current one and the old one). When a new Secure ID is written, the old one is deleted and the current one is saved, allowing you to access the other computers on which you are registered as the Sobol user. If you have not logged on to any of these computers since the last time the Secure ID was changed, you will lose access to it, because the old Secure ID that is required for your authentication on this computer is already deleted from the security token memory.

7. Click **Finish**.

Shut down and restart computer

To shut down and restart the computer with installed Sobol, follow the instructions for the OS running on your computer.

Documentation

1. Hardware Trusted Boot Module Sobol. Version 4. Administrator guide.
2. Hardware Trusted Boot Module Sobol. Version 4. Administrator guide. Sobol software.
3. Hardware Trusted Boot Module Sobol. Version 4. User guide.
4. Hardware Trusted Boot Module Sobol. Version 4. Getting Started.