



## MANUAL FOR ENTERING THE ADMINISTRATOR PASSWORD FOR THE 1ST TIME AND IMPORTING A CERTIFICATE TO CRYPTOSTICK

This manual describes how to unlock a cryptostick from SK by entering the administrator password and how to import an organization certificate issued by SK (e.g. e-Seal, certificate for encryption) to a cryptostick.

### VERSION INFO

Date	Version	Changes
03/2018	1.0	First published version.

### DEFINITIONS AND ABBREVIATIONS

**SAC** – SafeNet Authentication Client

**SK** – AS SK ID Solutions

### SYSTEM REQUIREMENTS (SAFENET AUTHENTICATION CLIENT TOOLS)

Importing a certificate to a cryptostick requires installed operation system with a graphical user interface as well as additionally installed SAC

SAC Tools is supported by the following operating systems:

- Windows;
- Linux;
- Mac OS X.

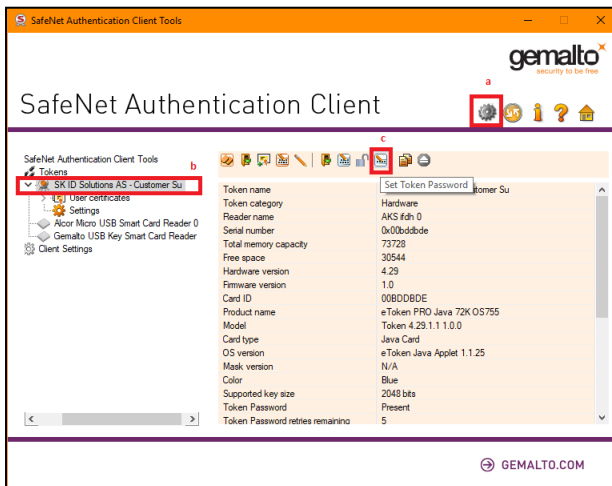
For more information on operation system versions, API's, browsers, etc. please refer to the manufacturer's website at <https://safenet.gemalto.com/multi-factor-authentication/security-applications/authentication-client-token-management>, see tab **Specifications**.

SAC Tools can be downloaded from <https://installer.id.ee/media/etoken>.

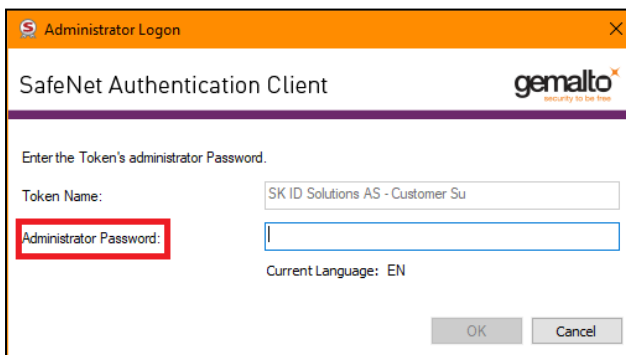
## ENTERING ADMINISTRATOR PASSWORD FROM SECURITY ENVELOPE FOR 1<sup>ST</sup> TIME

If you have ordered a crypto- or e-Seal certificate from SK on a cryptostick, then you have also received a security envelope, which includes cryptostick administrator password. Administrator password must be entered for 1<sup>st</sup> time by following these instructions:

- a) Launch **SAC** and click on **“Advanced view”** icon (reminds gear wheel);
- b) Under **“Tokens”** section find and select your cryptostick;
- c) Click on icon **“Set Token Password”**;



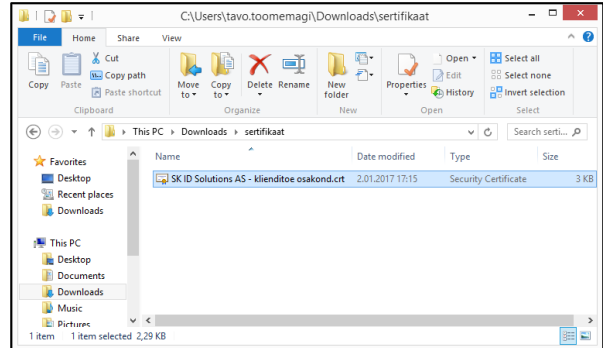
- d) Pop-up windows named **“Administrator Logon”** will be opened;
- e) Find an administrator password (it is printed to behind of the sticker the **“PIN-LOCK”** on the security envelope, which was issued by SK with the cryptostick”, enter it to the field **“Administrator Password”** and click **“OK”**.





## IMPORTING THE CERTIFICATE RECEIVED FROM SK TO THE CRYPTOSTICK

1. Connect the cryptostick to the USB port of the computer and make sure SAC identifies it.
2. Double-click on the certificate received from SK.



3. Click "Install Certificate..."
  - 3.1.1. **Store Location** – keep option "Current User" active and click "Next";
  - 3.1.2. **Certificate Store** – keep option "Automatically select the certificate store based on the type of certificate" active and click "Next" and "Finish".
4. Now you are prompted to enter the cryptostick PIN-code, enter it and the certificate will be imported to the cryptostick.
5. Verify the import by refreshing the SAC status (press F5 on keyboard) after which you should see the following:

