Cryptostick initialization

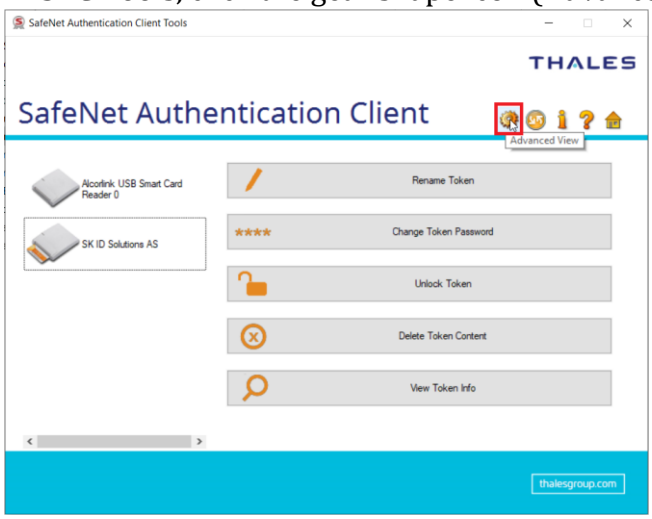
SK SELLS CRYPTOSTICKS WITH BOTH CC QSCD AND FIPS CERTIFICATES. WHEN SUBSCRIBING FOR E-SEAL CERTIFICATE FROM SK IT IS IMPORTANT THAT THE RESPECTIVE FUNCTIONALITY IS ENABLED WHEN INITIALIZING CRYPTOSTICK IN SAFENET AUTHENTICATION CLIENT.

NB! WHEN INITIALIZING THE CRYPTOSTICK, ALL THE KEYS AND CERTIFICATES ON THE CRYPTOSTICK WILL BE PERMANENTLY DELETED. INITIALIZE THE CRYPTOSTICK ONLY WHEN THE CERTIFICATES ARE NO LONGER USED IN THE ORGANISATION.

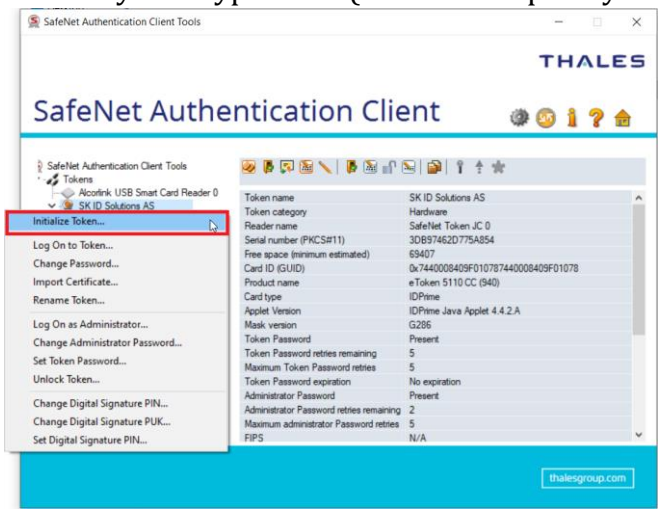
INITIALIZATION GUIDE (WINDOWS EXAMPLE)

For initialization you will need SafeNet Authentication Client (SAC) – It can be downloaded from https://installer.id.ee/media/etoken

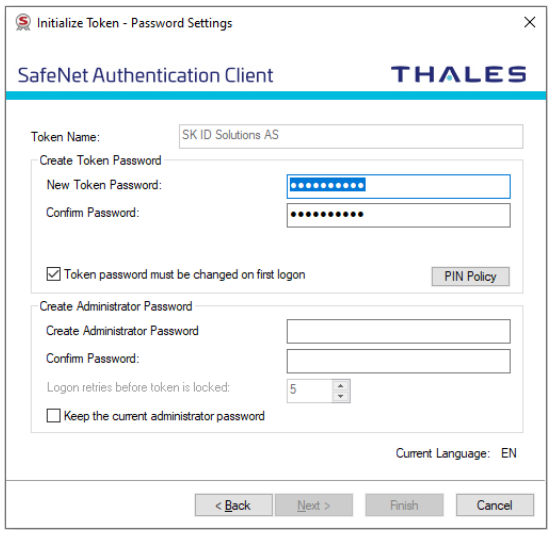
1. Connect the cryptostick to the USB port on your computer. Run SAC by double-clicking the SAC icon on the system tray
2. In SAC Tools, click the gear shape icon (Advanced View)



3. On the left, it displays cryptosticks identified in the USB ports (Tokens). Right-click on your cryptostick (In this example My Token) and select **Initialize Token**



4. Activate option **Configure all initialization settings and policies** and click **Next**. The following window is displayed (see below), provide the required information and click **Next**



5. Now it is possible to set requirements for the password entered in the previous step (length, expiration, period, whether upper case and/or lower-case letters are required, etc.). For a cryptostick initialized by SK this section is inactive since codes have only length requirements – PIN-code min. 5, administrator PIN-code 6 digits, see the latest version of the document https://www.skidsolutions.eu/repositoorium/CPS/ .
   Decide according to the safety rules of your organization – set password requirements or remove the tick from option **Enforce password quality settings (recommended)** and select **Next** to continue.
6. It is important to set FIPS or CC settings for the cryptostick. SK provides both, FIPS and CC certificates, which means further steps dependent on the specific cryptostick that is used.

FIPS	**CC**
▪ Activate option **Enforce FIPS settings** ▪ Click **Next**	▪ Activate option **Enforce Common Criteria settings** ▪ Enter password in the field **New Import Password**, which is used for importing CC certificate to the stick. *(Administrator password)* ▪ Select 2048-bit: 10 *(SK does not issue certificates with 1024-bit)* ▪ Click **Next**

7. In the displayed window make the following settings:
   - Private data caching: **Always (fastest)**
   - RSA key secondary authentication: **Never**
8. Click **Finish** to complete the initialization and in the displayed confirmation window click **OK**.

If you face issues – please send e-mail with description and if possible, a screenshot to support@skidsolutions.eu or in urgent case call +372 610 1883