

Deutsch – English Version below

# CHERRY SECURE BOARD 1.0

Für Administratoren:

## Einrichtung und Aktivierung des Secure Mode auf Windows Systemen

### 1 Beschreibung Systemkonzept

Das CHERRY SECURE BOARD 1.0 ist eine Tastatur mit integriertem Smartcard- und RF/NFC Leser, die neben der Standard-Funktion über einen zusätzlichen USB-Kanal zur verschlüsselten Übertragung der Tasten, dem sogenannten „Secure Mode“ verfügt.

Für die verschlüsselte Verbindung wird TLS1.3 eingesetzt. Dabei fungiert die Tastatur als Server, der die Ciphersuite *TLS\_CHACHA20\_POLY1305\_SHA256* unterstützt.

Um den verschlüsselten Modus nutzbar zu machen, müssen dafür notwendige Zertifikate und Schlüssel erzeugt und geladen werden. Die Tastatur wird mit einem Gerätezertifikat ausgeliefert, das zur Authentisierung des Gerätes und zum sicheren programmieren von User Zertifikaten und Schlüsseln verwendet wird.

Das Installationspaket beinhaltet folgende Softwarekomponenten:

- Gerätepersonalisierung zum Erzeugen einer Certificate Authority (CA) und zum Laden davon abgeleiteter Nutzer Zertifikate in die Tastatur.
- Dienst SECURE BOARD zum Aufbau der verschlüsselten Verbindung zur Tastatur.
- Desktop-Client zur Anzeige und Konfiguration des aktuellen Status der Verbindung mittels Tray Icon auf dem Default Desktop.
- SecureBoardSettings: Dies ist ein Tool zum bequemen Exportieren und Importieren von Registrierungsschlüsseln für die Masseneinführung.

**!!! Zum Betrieb der Software muss .Net Framework V4.8 installiert sein!!!**

**!!! Bitte stellen Sie sicher, dass Ihr SECURE BOARD 1.0 die Firmware 1.1.0 oder höher enthält !!!**

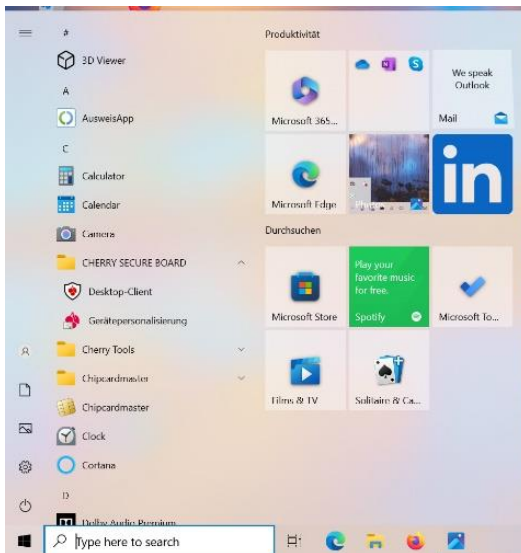
### 2 Empfohlener Ablauf einer Mehrfach-Installation

- 1 Installation der Software **auf einem vertrauenswürdigen System in sicherer Umgebung.**
- 2 Erstellung einer Zertifizierungsstelle auf diesem System und sichere Aufbewahrung des privaten Schlüssels
- 3 Personalisierung der Tastaturen mit davon abgeleiteten Benutzer-Zertifikaten an diesem System.
- 4 Verteilung und Installation der Software mit de-aktivierter Gerätepersonalisierung (Default) auf die Clients im Netzwerk.
- 5 Verteilung des CA-Registry Schlüssel an die Clients im Netzwerk.

**!!! Nach Verteilung und Installation der Komponenten startet der Dienst und der Desktop-Client automatisch nach jedem Neustart!!!**

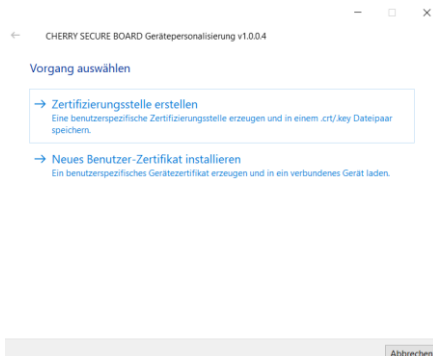
### 3 Herunterladen und Installation der Software

- 1 Laden Sie das Installationspaket von [www.cherry.de](http://www.cherry.de) → SERVICE → Downloads → Produktsuche: „SECURE BOARD 1.0“ herunter, um es anschließend **auf einem sicheren System zu installieren**.
- 2 Entpacken Sie die Dateien, aktivieren Sie die Komponenten, die installiert werden sollen und folgen Sie den Installationsanweisungen.
- 3 Nach korrekter Installation ist der Dienst „SECURE BOARD“ installiert, der zunächst inaktiv ist.
- 4 Im Applikationsordner finden Sie das Verzeichnis „CHERRY SECURE BOARD“. Es beinhaltet die Komponenten:
  - „Gerätepersonalisierung“ zum Generieren einer Zertifizierungsstelle sowie der Installation davon abgeleiteter Nutzer Zertifikate in der Tastatur.
  - „Desktop-Client“ zur Anzeige und Konfiguration des aktuellen Status mittels Tray Icon auf dem Default Desktop.

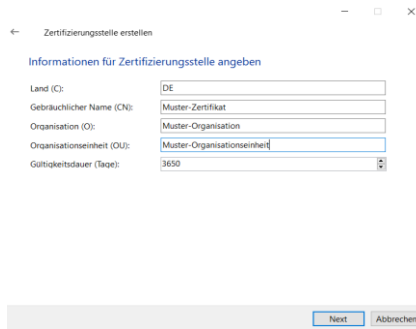


#### 3.1 Erzeugen einer Zertifizierungsstelle

- 1 Starten Sie die App und wählen Sie „Zertifizierungsstelle erstellen“.



## 2 Tragen Sie die entsprechenden Informationen ein.



← Zertifizierungsstelle erstellen

Informationen für Zertifizierungsstelle angeben

Land (C):

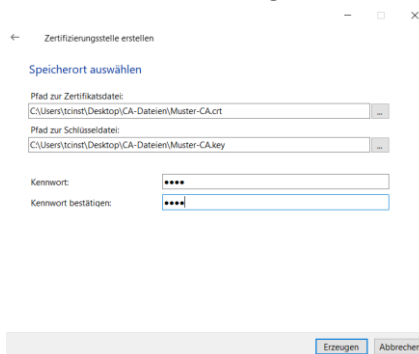
Gebrauchlicher Name (CN):

Organisation (O):

Organisationseinheit (OU):

Gültigkeitsdauer (Tage):

Wählen oder erstellen Sie ein Verzeichnis zum Speichern des CA-Zertifikats und des zugehörigen privaten Schlüssels, legen Sie ein Passwort fest und starten Sie die Erstellung durch Klick auf „Erzeugen“.



← Zertifizierungsstelle erstellen

Speicherort auswählen

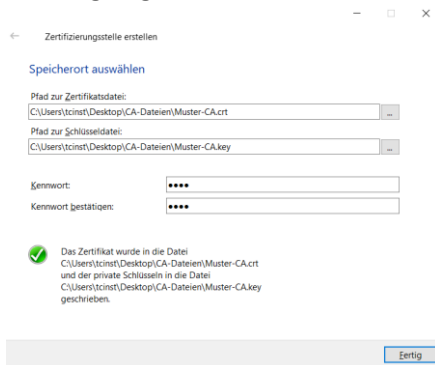
Pfad zur Zertifikatsdatei:

Pfad zur Schlüsseldatei:

Kenntwort:

Kenntwort bestätigen:

Im festgelegten Verzeichnis befindet sich nun Zertifikat und privater Schlüssel der CA.



← Zertifizierungsstelle erstellen

Speicherort auswählen

Pfad zur Zertifikatsdatei:

Pfad zur Schlüsseldatei:

Kenntwort:

Kenntwort bestätigen:

Das Zertifikat wurde in die Datei  
C:\Users\tcinst\Desktop\CA-Dateien\Muster-CA.crt  
und der private Schlüssel in die Datei  
C:\Users\tcinst\Desktop\CA-Dateien\Muster-CA.key  
geschrieben.

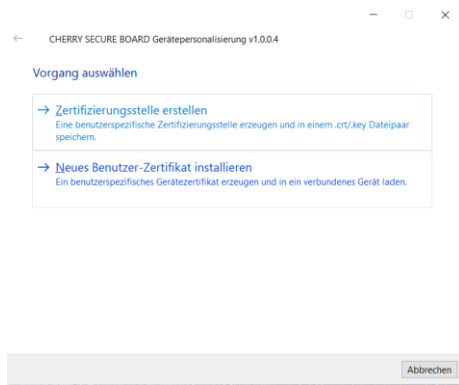
**!! Der private Schlüssel muss sicher verwahrt werden und darf nicht verteilt/publiziert werden!!**

## 3.2 Installation eines Benutzer-Zertifikates in der Tastatur

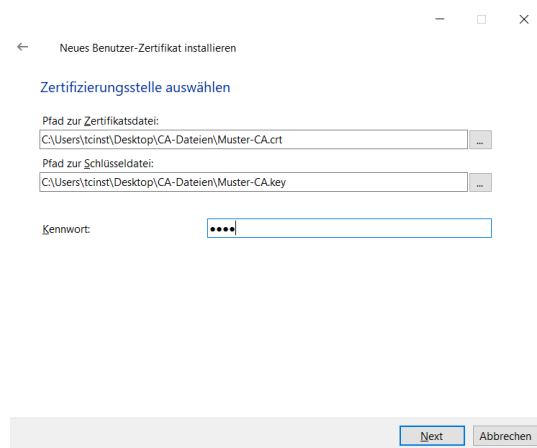
**!! Während dieses Vorgangs darf der Dienst „SECURE BOARD“ nicht aktiv sein!!**

**!! Falls bereits ein Benutzer-Zertifikat in die Tastatur geladen wurde, muss es gelöscht werden (Siehe 3.2.4)!!**

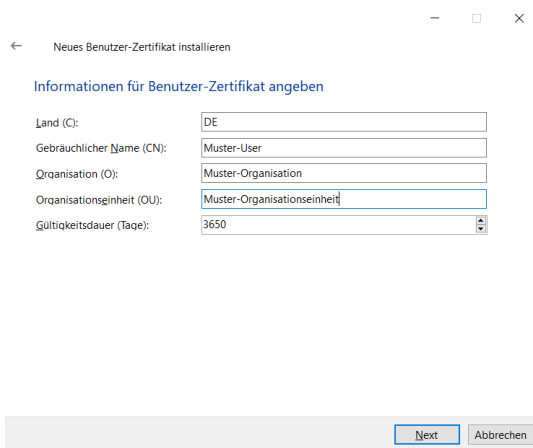
### 1 Starten Sie „Neues Benutzer-Zertifikat installieren“.



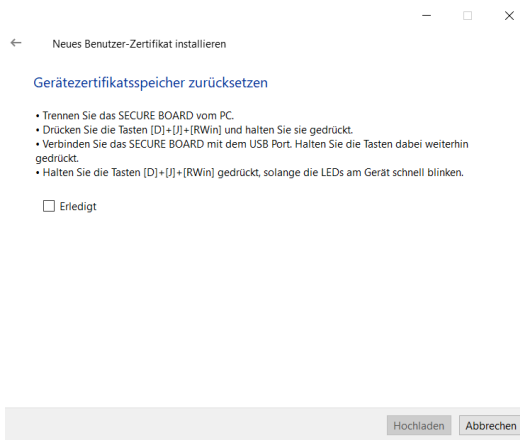
### 2 Wählen Sie das CA Zertifikat und den zugehörigen privaten Schlüssel aus und geben Sie das dafür festgelegte Passwort ein.



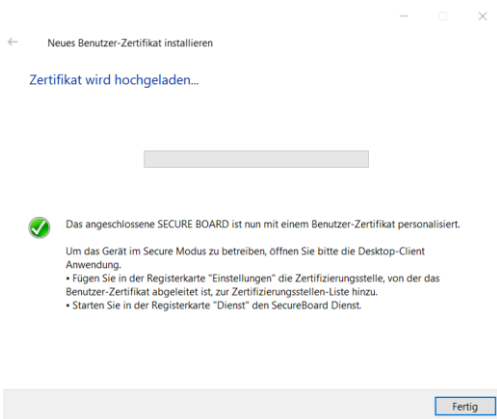
### 3 Legen Sie die Bezeichnungen für das Benutzer- Zertifikat der Tastatur fest.



- 4 Sie müssen evtl. bereits in der Tastatur gespeicherte Zertifikate löschen, sowie in der Menüführung beschrieben. Bei neuen Tastaturen im Auslieferungszustand können Sie den Schritt überspringen und mit „Erledigt“ bestätigen.

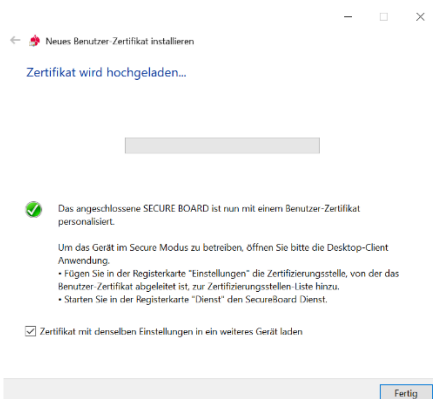


- 5 Starten Sie das Hochladen. Während dieses Vorgangs blinkt die rote Led.



- 6 Falls sie nur ein Gerät programmieren wollen, klicken Sie auf „Fertig“, damit sich die Applikation schließt.

Falls Sie mehrere Geräte mit dem Zertifikat programmieren wollen, setzen sie den Haken im Auswahlfeld, bevor sie „Fertig“ auswählen. Sie werden zu Schritt 4 weitergeleitet.



## 4 Aktivierung und Konfiguration des Secure Mode

### 4.1 Ablauf der Aktivierung und Konfiguration

1 Starten Sie den Desktop-Client über das Tray Icon.



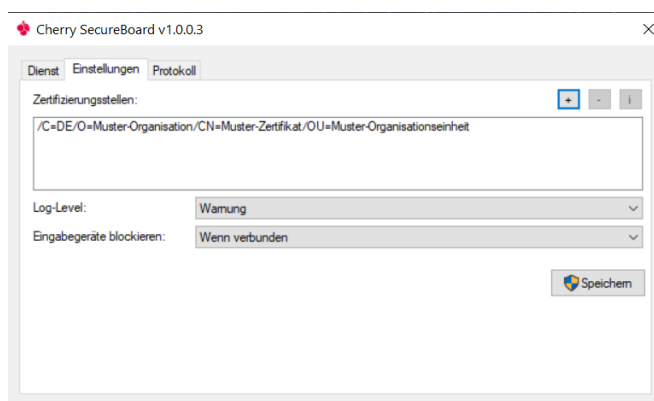
2 Für die initiale Einrichtung gehen Sie in den Reiter „Einstellungen“

- Hier kann durch Klicken auf „+“ eine gültige CA ausgewählt werden.
- Wählen Sie das gewünschte Log-Level.

3 In „Eingabegeräte blockieren“ können folgende Optionen gewählt werden:

- **„Niemals“:** alle HID Tastatur Eingabegeräte können (auch während einer Secure Mode Session genutzt werden (nicht empfohlen).
- **„Wenn verbunden“:** während einer aktiven Secure Mode Session kann kein weiteres an den Client angestecktes HID Tastatur Eingabegerät genutzt werden.
- **„Immer“:** Kein anderes HID Tastatur Eingabegerät kann genutzt werden. Nur SECURE BOARD 1.0 mit korrektem Benutzer Zertifikat sind funktionsfähig. Die Windows „Bildschirmtastatur“ kann weiterhin mittels der Maus zur Eingabe von Tastendrücken benutzt werden.

**!!! Diese Einstellungen können nur durch Windows Benutzer mit Admin Rechten geändert oder gespeichert werden!!!**



4 Durch „Speichern“ wird werden mehrere Registry-Einträge erzeugt in HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Cherry\SecureBoard („WOW6432Node\“ nur unter 64bit Windows). Ein Eintrag „Certificate Authority“ enthält die ausgewählten CAs in PEM-Codierung (öffentlicher Teil). Siehe 4.2 für Details zum Export und Import von Registry Schlüsseln.

- 5 Im Reiter „Dienst“ kann dieser manuell gestartet oder beendet werden. Es wird das jeweils in der Tastatur aktive Zertifikat angezeigt.

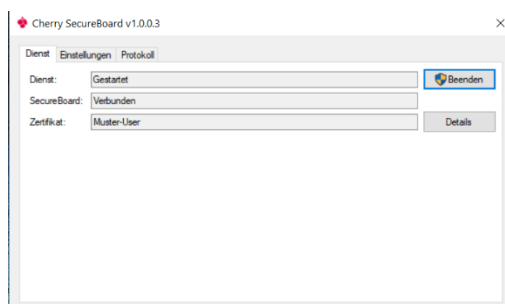
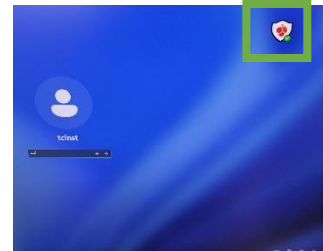
**!!! Dieser Dienst kann nur durch Windows Benutzer mit Admin Rechten gestartet/beendet werden!!!**



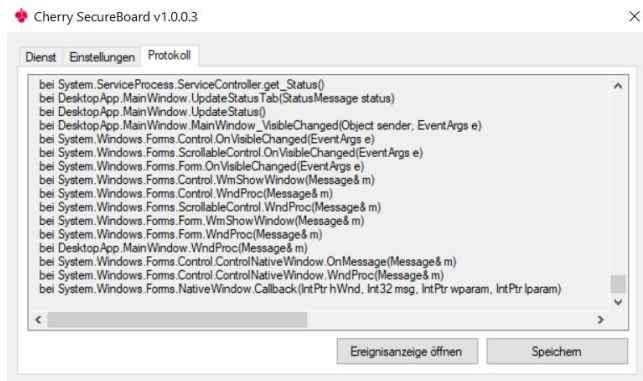
- 6 Durch Klicken auf „Starten“ wird der Secure Mode gestartet.
- Während des Aufbaus des verschlüsselten Tastatur Kanals blinkt zunächst die rote LED über dem Schloss Symbol. Bei erfolgreicher Verbindung leuchtet sie permanent.



Der Dienst startet automatisch nach jedem Neustart des PC und ist dann bereits vor Eingabe des User Passwortes aktiv. Dies wird durch das Tray Icon in der Taskleiste und durch ein Symbol im Passwort Eingabefenster angezeigt.



- Im Reiter „Protokoll“ findet man die entsprechenden Logs.



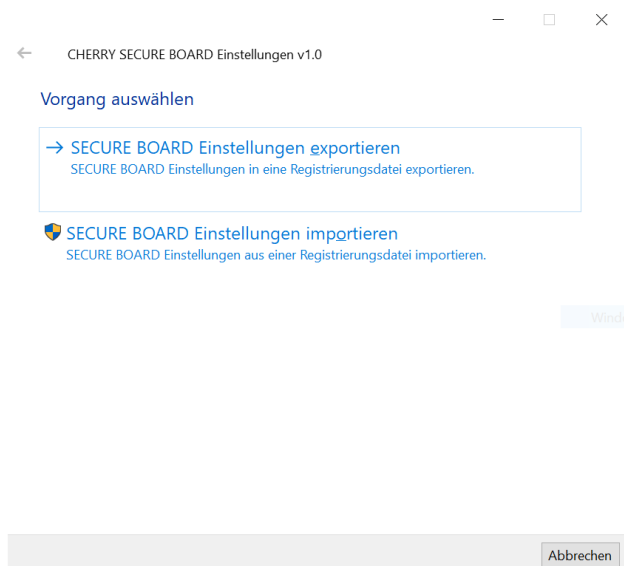
## 4.2 Export und Import von Registry Keys

Zur Verteilung der Einstellungen des Dienstes „SECURE BOARD“ mittels der Registry Keys (siehe 4.1.4) auf mehrere Clients im Netzwerk ist ein Tool SecureBoardSettings im Installationspaket enthalten.

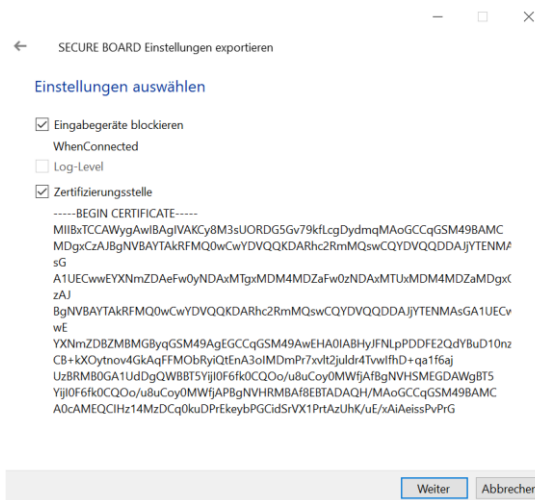
!!! Bitte nutzen Sie nicht die Export-Funktion des Windows Registry Editors. Hier gibt es Fehler bei der Formatierung des Eintrages „CertificateAuthority“. Ein Import über Windows Bordmittel ist möglich!!!

### Export von Registry Keys

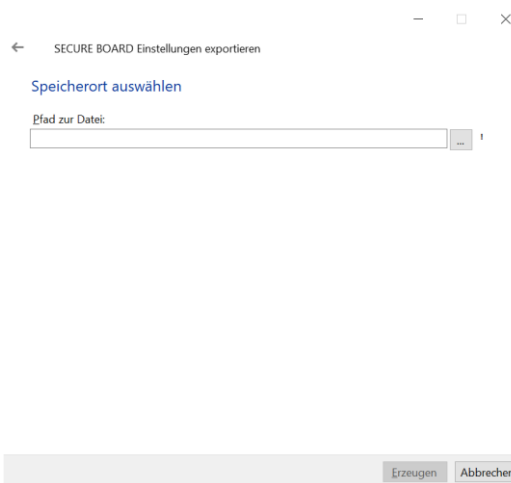
- 1 Starten Sie im Ordner SecureBoardSettings die Datei SecureBoardSettings.exe
- 2 Wählen Sie „SECURE BOARD Einstellungen exportieren“



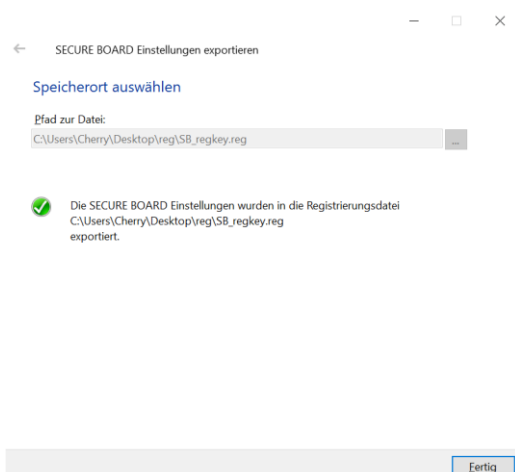
- 3 Ihnen wird nun die Einstellung des aktuellen Dienstes „SECURE BOARD“ und der public key angezeigt. Diese Einstellungen können Sie durch wie gewünscht auswählen und auf „Weiter“ klicken



- 4 Wählen Sie nun den Dateispeicherort und Dateinamen für die \*.reg Datei aus und klicken auf „Erzeugen“.



- 5 Die SECURE BOARD Einstellungen wurden in die ausgewählte Datei exportiert.

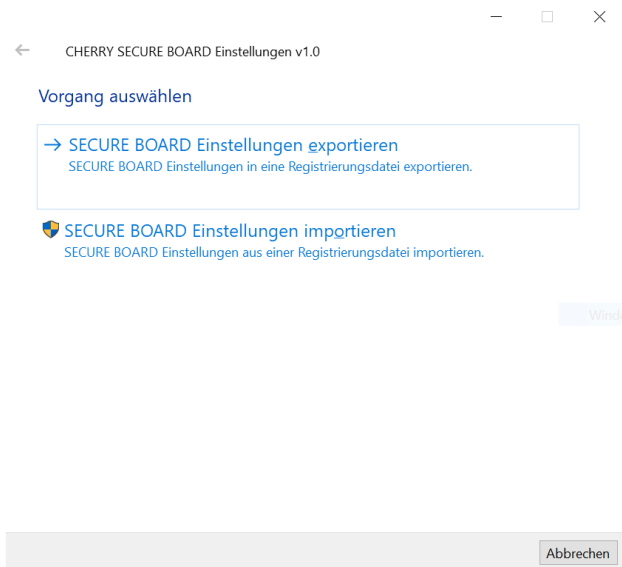


## Import von Registry Keys

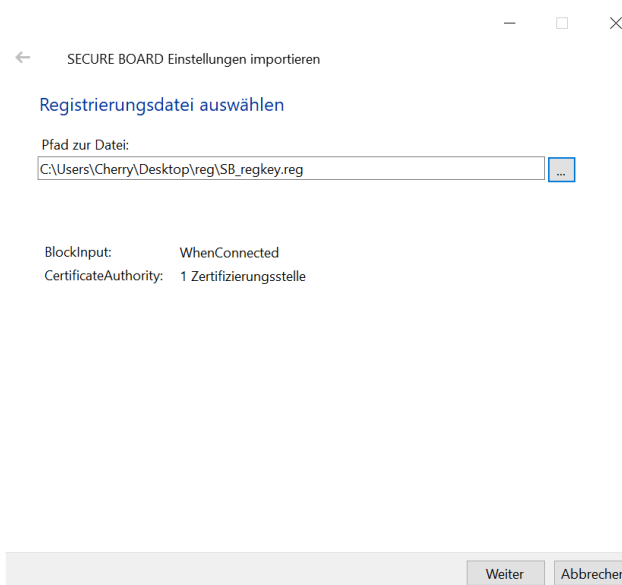
!!! Ein Import der durch obiges Tool exportierten \*.reg Datei über Windows Bordmittel, z.B. Login-Skript, ist möglich!!!

Alternativ steht Ihnen die folgende Benutzeroberfläche dafür zur Verfügung.

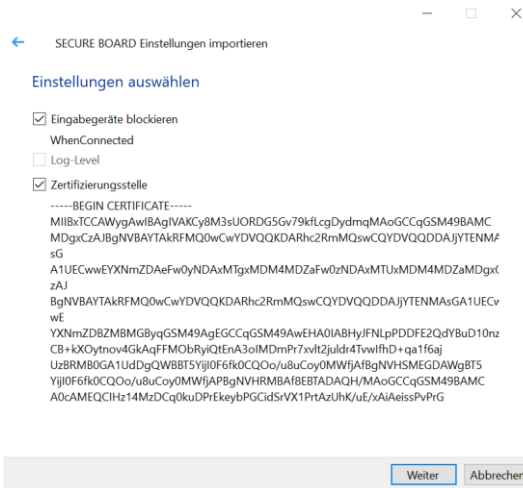
- 1 Starten Sie im Ordner SecureBoardSettings die Datei SecureBoardSettings.exe.
- 2 Wählen Sie „SECURE BOARD Einstellungen importieren“.  
!!! Diese Einstellungen können nur durch Windows Benutzer mit Admin Rechten geändert oder gespeichert werden!!!



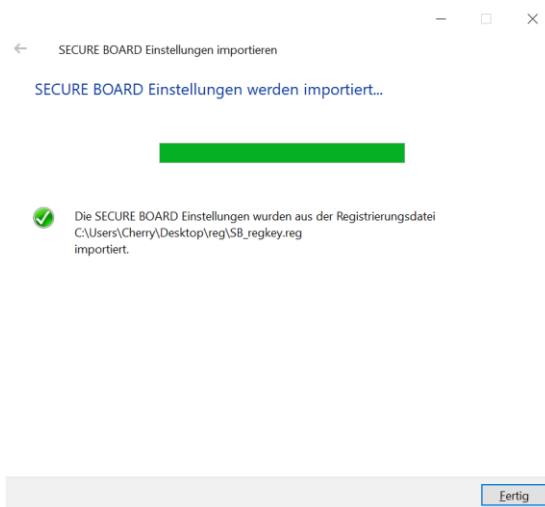
- 3 Bestätigen Sie die Windows Abfrage der Benutzerrechte
- 4 Wählen sie die zu importierende \*.reg Datei und klicken Sie auf „Weiter“



- 5 Ihnen wird der Inhalt der \*.reg Datei angezeigt. Mit Klick auf „Weiter“ wird der Registry Key importiert



## 6 Der Import ist abgeschlossen. „Fertig“ beendet die Applikation.



## 5 Kontakt

Bitte halten Sie bei Anfragen an den Technischen Support folgende Informationen bereit:

- Artikel- und Serien-Nr. des Produkts
- Bezeichnung und Hersteller Ihres Systems
- Betriebssystem und ggf. installierte Version eines Service Packs

Cherry Digital Health GmbH  
 Cherrystraße 2  
 91275 Auerbach/OPf.

Internet: [www.cherry.de](http://www.cherry.de)

Telefon: +49 (0) 9643 2061-100\*

\*zum Ortstarif aus dem deutschen Festnetz, abweichende Preise für Anrufe aus Mobilfunknetzen möglich

English

# CHERRY SECURE BOARD 1.0

For administrators:

## Installation and activation of the Secure Mode on Windows Clients

### 1 Description of the system concept

The CHERRY SECURE BOARD 1.0 is a keyboard with an integrated smartcard- and RF/NFC reader. In addition to the standard keyboard functionality, the device can operate through a separate USB-channel for the encrypted transfer of key inputs. This is called Secure Mode.

In Secure Mode, all keystrokes are transmitted securely using a TLS 1.3 channel to the host. In this mode, the keyboard acts as a server using the ciphersuite *TLS\_CHACHA20\_POLY1305\_SHA256*.

To activate Secure Mode, the necessary certificates and keys must be created and stored. The keyboard is delivered with a device certificate, which is used for authentication of the device and for safely storing the client certificates and keys. The software suite includes the following software components:

- Device Personalization for the creation of a CA (Certificate Authority) and uploading of CA-based user certificates in the individual SECURE BOARD 1.
- Service SECURE BOARD for establishing a secure channel to the keyboard.
- Desktop Client for the setup and visualization of the current state of the Secure Mode through a Tray Icon and Icon on the windows password insertion screen.
- SecureBoardSettings: this is a tool to conveniently export and import registry keys for mass rollout.

**!!! For the correct functionality of the software .Net Framework V4.8 must be installed!!!**

**!!! Please ensure that your SECURE BOARD 1.0 contains the firmware 1.1.0 or Higher !!!**

### 2 Recommended procedure for multiple installations

- 1 The software must be installed on a **trusted system in a secure Environment**.
- 2 Creation of a CA on this system and storing of the private key.
- 3 Personalization of one or more devices through CA-based user certificates on this system.
- 4 Distribution and installation of the software with deactivated Device Personalization on the client systems in the network.
- 5 Distribution of the CA registry key to the clients in the (See 4).

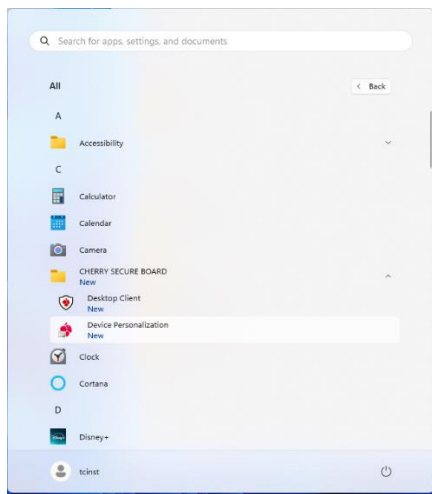
**!!! After the correct installation and distribution of the software, the service and the desktop client will automatically start with every restart!!!**

### 3 Download and installation of the software

- 1 Download the software from
  - For Europe:  
[www.cherry.de](http://www.cherry.de) → SERVICE → Downloads → Search product: „SECURE BOARD 1.0“ and install it on a **secure system**.
  - For USA:  
[www.cherryamericas.com](http://www.cherryamericas.com) → SERVICE → Downloads → Search product: „SECURE BOARD 1.0“ and install it on a **secure system**.
- 2 Unpack the zip file, start the msi file and install the software components.
- 3 After Installation the service „SECURE BOARD“ is present on the system, but initially deactivated.

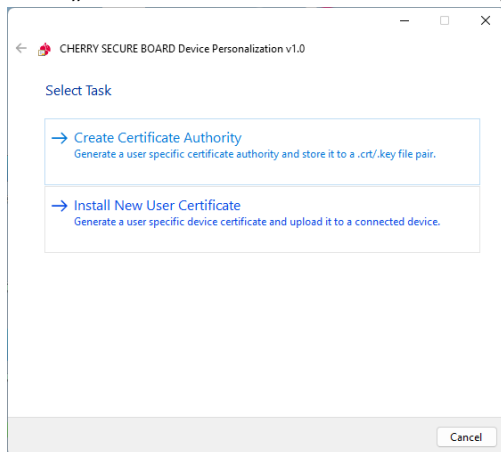
In the application drawer the folder „CHERRY SECURE BOARD“ is now present. It contains the following components:

- „Device Personalization“ is used to generate a CA and upload of CA-based user certificates to a keyboard.
- „Desktop Client“ for the setup and visualization of the current state of the Secure Mode through a Tray Icon and Icon on the windows password insertion screen.

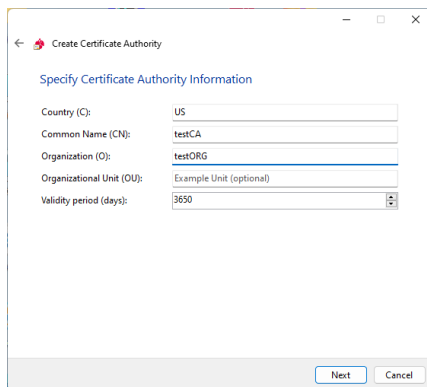


### 3.1 Creation of a CA

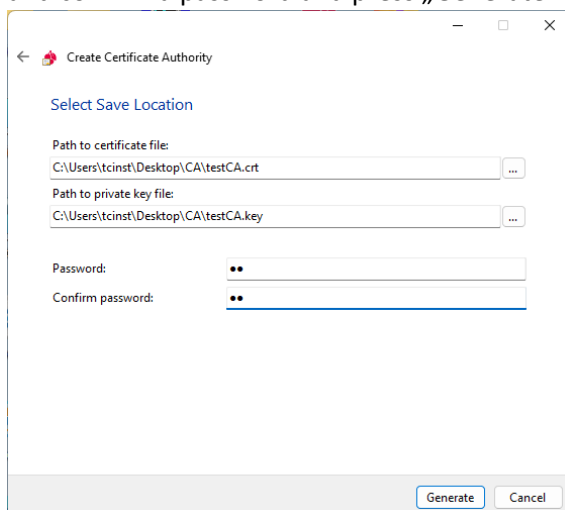
- 1 Start „Device Personalization“ and select „Create Certificate Authority“.



- 2 Insert the CA information



- 3 Select or create a folder, where the CA-certificate and the private key shall be stored. Chose and confirm a password and press „Generate“.



- 4 The CA-certificate and the private key is now stored in the defined folder.

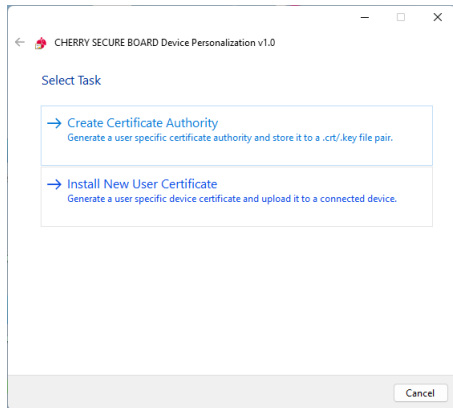
**!! The private key must be stored safely an must not be distributed/published!!**

## 3.2 Upload of a user certificate to a device

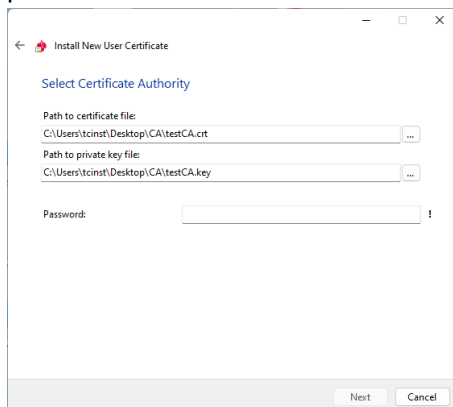
!! The service „SECURE BOARD“ must be deactivated on the current system!!

!! In case a user certificate has previously been installed in the keyboard, this must be erased (see 3.2.4)!!

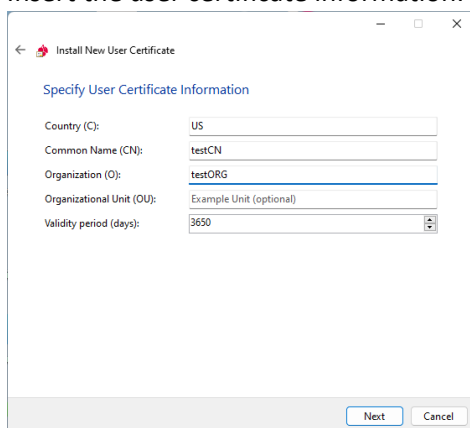
### 1 Start „Install New User Certificate“



### 2 Select the CA certificate and the private key in the file selector and insert the password and press “Next”.

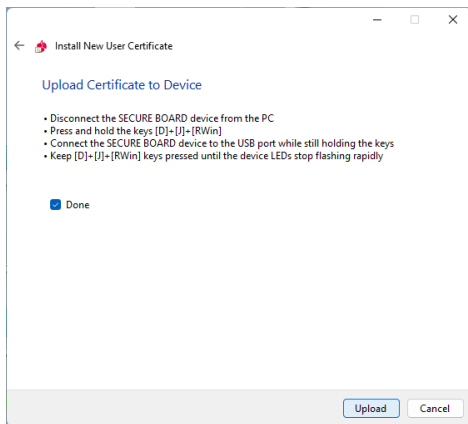


### 3 Insert the user certificate information.

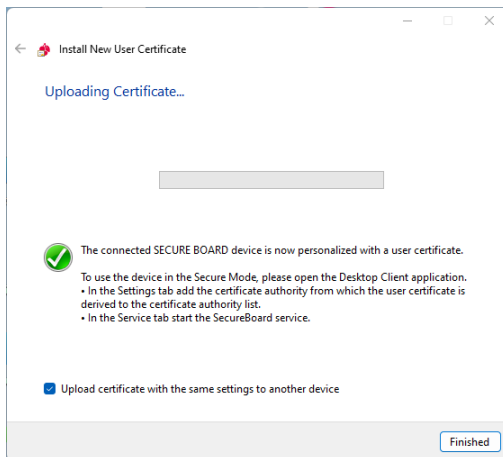


### 4 In case a user certificate has previously been installed in the keyboard, this must now be erased. Please proceed as shown.

This does NOT apply for unused devices as delivered by CHERRY. If that case this case, you can skip this procedure and directly mark the checkbox as „Done“. Proceed with “Upload”



5 During the upload, the red LED flashes red.



6 In case you only wanted to upload one device certificate, you can now press “Finished” to close the application.

In case you want to update more than one CHERRY SECURE BOARD 1.0 please activate the checkbox before pressing “Finished” and proceed as shown with step 4.

## 4 Activation and configuration of the Secure Mode

### 4.1 Procedure of Activation and configuration

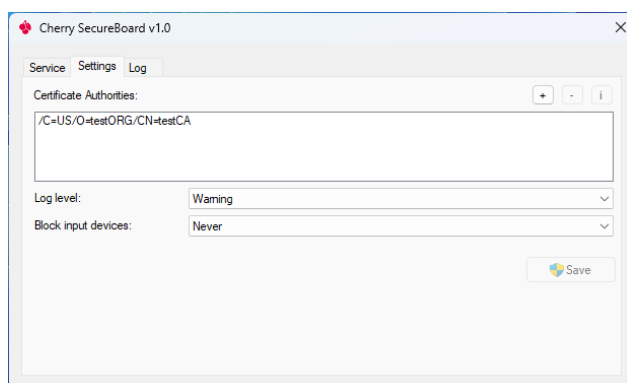
- 1 Start the Desktop Client through the Tray Icon.



- 2 For initial setup please first go to the sheet "Settings".
  - The Sheet "Settings" is used to define the approved CA through pressing "+". Please select the CA, on which the user certificate was based on.
  - Then set up the log level.
- 3 In "Block input devices" the following settings can be made:
  - **"Never"**: All other HID keyboard devices can be used. (not recommended).
  - **"When connected"**: No other HID keyboard devices can be used during an active Secure Mode (SECURE BOARD 1.0 devices with the correct user certificate) session.
  - **"Always"**: No other HID keyboard devices can be used. Only SECURE BOARD 1.0 devices with the correct user certificate and active Secure Mode can be used.

Remark: If no SECURE BOARD 1.0 with correct user certificates is available. The windows "On-Screen Keyboard" can still be used to input keys, using the mouse.

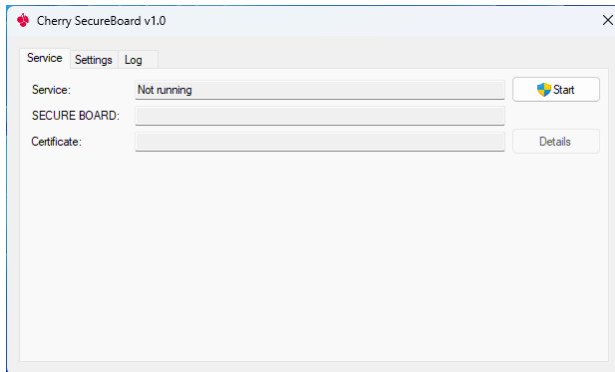
!!! These settings can only be altered/saved by windows users with admin rights.!!!



- 4 The Button „Save“ creates several registry-entries in HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Cherry\SecureBoard („WOW6432Node\“ only in 64bit Windows). One entry „Certificate Authority“ contains the selected CA in PEM-coding (public key). See 4.2 for details on the export, distribution and import of this registry key.

- The Sheet „Service“ shows the current state of the Secure Mode service and the currently active CA. The service SECURE BOARD and can be started and ended, and the certificate details can be shown.

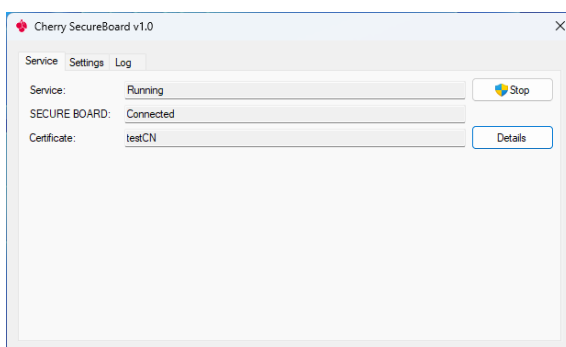
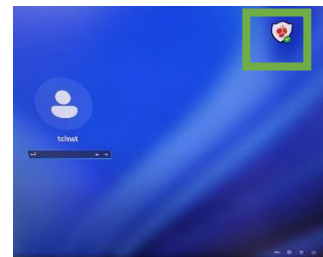
!!! This service can only be started/stopped by windows users with admin rights.!!!



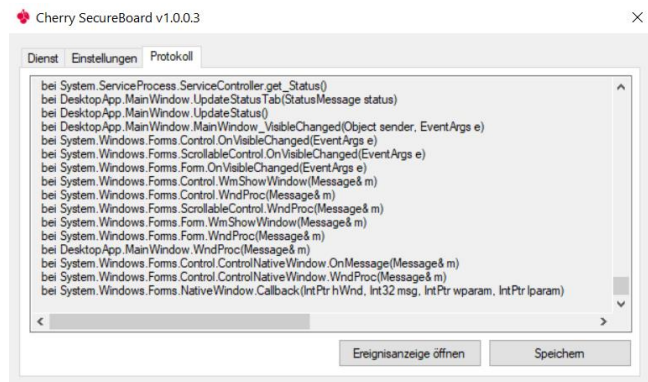
- When pressing „Start“, the Secure Mode session will be started. The red LED above the LOCK symbol of the SECURE BOARD 1.0 will FLASH until a secure connection is established. Then the red LED will be always ON.



- Once activated, this service will automatically start with each client restart and is active before the Windows password insertion.
- Other than the red LED, the status can also be checked in the tray icon and the icon on the password insertion screen.



In the sheet „Log“ the logs are shown as set up in the settings screen.



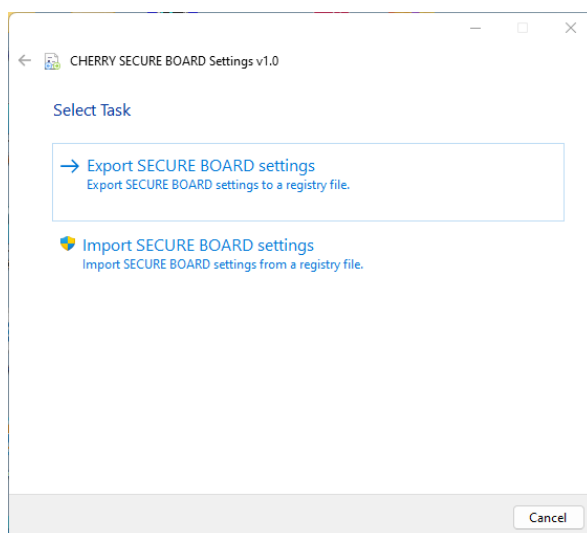
## 4.2 Export and import of registry keys

The application SecureBoardSettings, as included in the software suite, can be used for the distribution of the settings of the service „SECURE BOARD“ through registry keys (see 4.1.4) on multiple clients in the network.

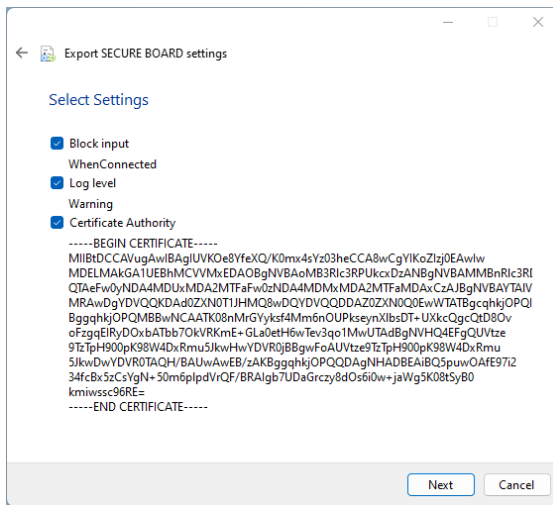
**!!! Please do not use the export-function of the Windows registry editors. There is a problem with the formatting of the key „CertificateAuthority“. An import through Windows tooling, e.g. login-scripts is possible!!!**

### Export of registry keys

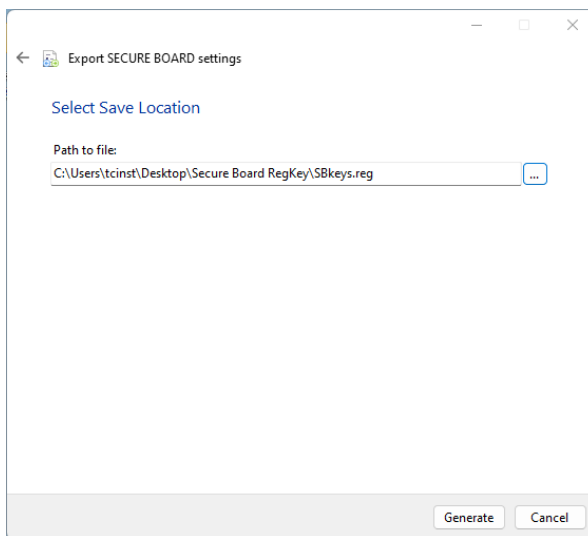
- 1 Start the file SecureBoardSettings.exe in the folder SecureBoardSettings
- 2 Select „Export SECURE BOARD settings“



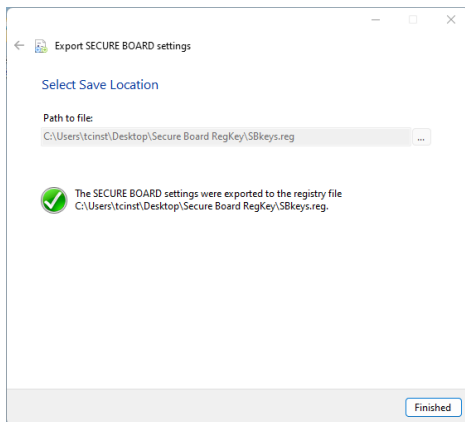
- You can see the current settings of the service „SECURE BOARD“, including the public key. Please select the desired settings and click on „Next“.



- Select or create a folder and filename of the \*.reg key and press „Generate“.



- 5 Die SECURE BOARD Einstellungen wurden in die ausgewählte Datei exportiert. A click on „Finished“ will close the application.

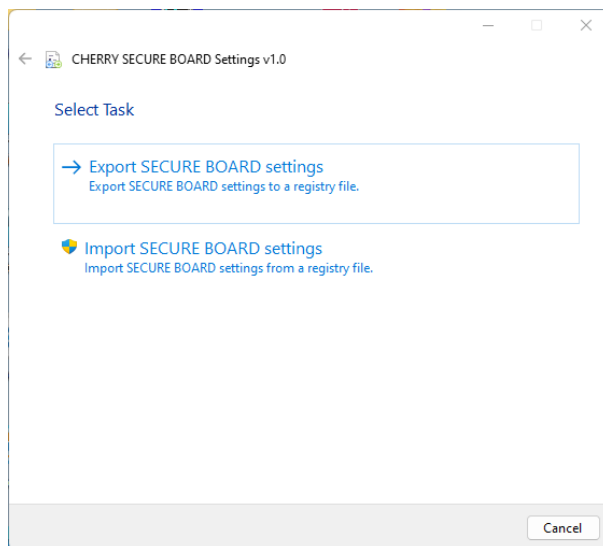


### Import of registry keys

!!! The import of the \*.reg file, which was exported through “SecureBoardSettings.exe” by using Windows standard tooling, e.g. login-script, is possible!!!

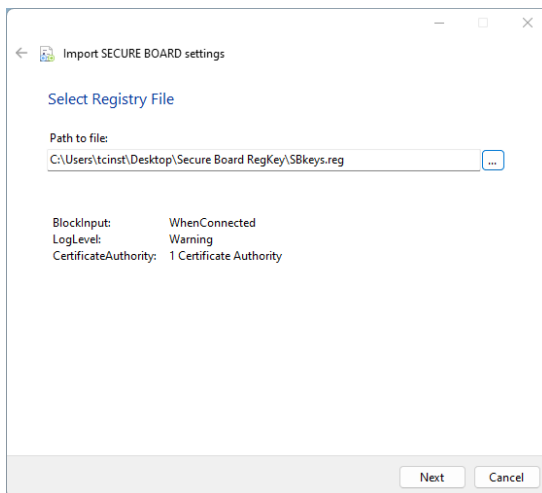
Alternatively, you can use the following user interface.

- 1 Start the file SecureBoardSettings.exe in the folder SecureBoardSettings.
- 2 Select „Import SECURE BOARD settings“  
!!! These settings can only be done with a windows user with admin rights!!!

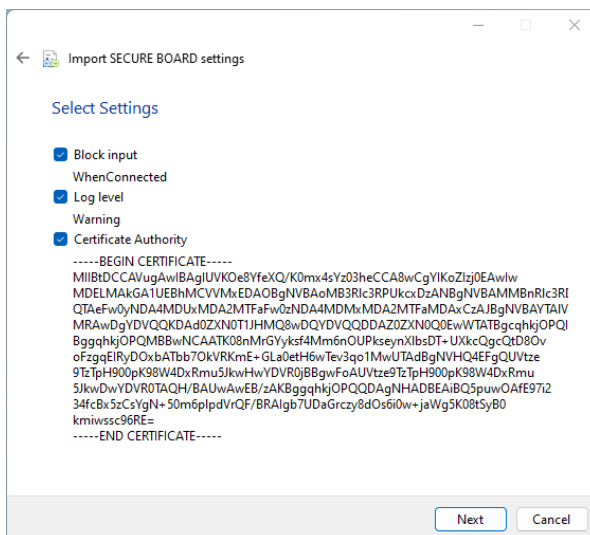


- 3 Confirm the windows User Account Control

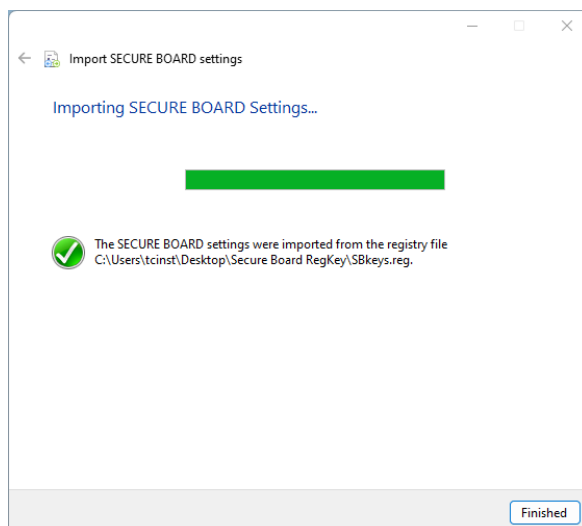
- 4 Select the \*.reg for import and click on „Next“



- 6 You can see the available settings of the service „SECURE BOARD“, including the public key. Please select the desired settings and click on „Next“ to import.



- 7 The import is done. Click on „Finished“ closes the application.



## 5 Contact

Please provide the following information about the device when contacting technical support:

- Item and serial no. of the product
- Name and manufacturer of your system
- Operating system and, if applicable, installed service pack version

For Europe:

Cherry Digital Health GmbH

Cherrystraße 2

91275 Auerbach/OPf.

Germany

Internet: [www.cherry.de](http://www.cherry.de)

For USA:

Cherry Americas LLC

C/O Industrious 5th Floor - 111 W. Illinois St  
Chicago, Illinois 60654

United States

Tel.: +1 262 942 6508

Email: [sales@cherryamericas.com](mailto:sales@cherryamericas.com)

Internet: [www.cherryamericas.com](http://www.cherryamericas.com)