

CHERRY SECURE BOARD 1.0

Lokale Einrichtung auf Thin Clients

Local Setup on Thin Clients

CHERRY SECURE BOARD 1.0

Lokale Einrichtung auf Thin Clients

Inhalt

1	Tools und Zertifikate herunterladen.....	3
2	Customer-Zertifikate erstellen.....	3
2.1	Auf Windows-Systemen (z. B. Win10 64bit)	3
2.2	Auf einem Linux-System (z. B. Ubuntu 18.04):.....	3
3	Zertifikate installieren	4
3.1	Auf dem IGEL Thin Client.....	4
3.2	Im Terminal (IGEL Setup > Accessories > Terminals)	4
3.3	Bei einer Fehlermeldung.....	5
3.4	Nachdem die Personalisierung abgeschlossen ist.....	5
3.5	Tipps.....	5
4	Kontakt	6

CHERRY SECURE BOARD 1.0

Local Setup on Thin Clients

Content

1	Download tools and certificates.....	7
2	Create customer certificates	7
2.1	On windows system (e.g. Win10 64bit)	7
2.2	On linux system (e.g. Ubuntu 18.04):.....	7
3	Install certificates	8
3.1	On IGEL thin client	8
3.2	At terminal (IGEL Setup > Accessories > Terminals).....	8
3.3	In case of an error message.....	9
3.4	After the personalization is completed	9
3.5	Hints.....	9
4	Contact	10
4.1	For Europe.....	10
4.2	For USA.....	10

CHERRY SECURE BOARD 1.0

Lokale Einrichtung auf Thin Clients

1 Tools und Zertifikate herunterladen

- 1 Laden Sie das aktuelle Installationspaket "Quick Installation Package.zip" von https://www.cherry.de/download/us/download.php?product_id=387.
- 2 Entpacken Sie die Dateien.

2 Customer-Zertifikate erstellen

- 1 Falls gewünscht: Passen Sie den Inhalt der Erweiterungsdatei "user.ext" und/oder "SecureBoardCA.config" (z. B. Firmenname, ...) an.

2.1 Auf Windows-Systemen (z. B. Win10 64bit)

- 1 Installieren Sie "Openssl 64bit" (ab Version 1.1.0L).
- 2 Passen Sie das Skript "create_certs.bat" an.
- 3 Ggf.: Ändern Sie den Openssl-Pfad (Standardpfad ist: "C:\OpenSSL-Win64\bin").
- 4 Fügen Sie den Openssl\bin-Pfad zu Ihrer Systemumgebung hinzu:
Starten Sie "C:\Windows\System32\SystemPropertiesAdvanced.exe" als Admin und fügen Sie "C:\Openssl-64\bin" oder Ihren definierten Pfad unter "Umgebungsvariablen > Pfad" ein.
- 5 Führen Sie die Datei "create_certs.bat" aus.

2.2 Auf einem Linux-System (z. B. Ubuntu 18.04):

- 1 Ggf.: Installieren/aktualisieren Sie Openssl:
 - `sudo apt-get install openssl` oder
 - `sudo apt-get upgrade openssl`
- 2 Ggf.: Passen Sie die Ausführungsrechte für "create_certs.sh" an:
 - `sudo chmod 777 create_certs.sh [ENTER]`
- 3 Wechseln Sie zum Ordner und führen Sie das Skript aus:
 - `sudo (bash) ./create_certs.sh [ENTER]` or
 - `sudo bash create_certs.sh [ENTER]`
- 4 Kopieren Sie die folgenden Dateien auf einen externen Datenträger (z. B. USB-Stick):
 - `copy_certs.sh`
 - `certs.sh`
 - `p-20191030.pem` und/oder `p-20190712.pem` oder jeweils aktuelle Produktionszertifikate
 - `SecureboardRootCA.pem`

- clientca-cert.pem
- clientca-cert.srl (optional)
- user-cert.pem
- user-key.pem
- client-cert.pem
- client-key.pem

3 Zertifikate installieren

3.1 Auf dem IGEL Thin Client

Empfohlene IGEL OS-Version: 11.02.159 oder höher

- 1 Schließen Sie den Datenträger an den IGEL Thin Client an.
- 2 Ggf.: Aktivieren Sie die Option für Hotplug-Speichergeräte mit "Setup > Devices > Storage Devices > Storage Hotplug".
- 3 Ggf.: Setzen Sie das SECURE BOARD zurück:
 - Trennen Sie die Verbindung zum Gerät.
 - Drücken Sie gleichzeitig die Tasten [D], [J] und die [RECHTE WINDOWS-TASTE] und schließen Sie dabei das Gerät wieder an.
 - Halten Sie die Tasten etwa 5 Sekunden lang gedrückt, während die LEDs schnell blinken.
 - Trennen Sie das Gerät und schließen Sie es noch einmal an.

3.2 Im Terminal (IGEL Setup > Accessories > Terminals)

- 1 Melden Sie sich über "root" an: Zugang zum Datenträger:
 - cd/media/ [ENTER]
 - ls [ENTER]
 - cd<NAME DES DATENTRÄGERS> [ENTER]
- 2 Ggf.: Wechseln Sie auf dem Datenträger in das entsprechende Unterverzeichnis, in dem die kopierten Dateien gespeichert wurden.
- 3 Geben Sie "bash copy_certs.sh" [ENTER] ein.
Das Skript startet automatisch den Personalisierungsprozess.
- 4 Drücken Sie [Y].
- 5 Nach Abschluss des Personalisierungsversuchs drücken Sie [CTRL] + [C] (nötigenfalls mehrfach).

3.3 Bei einer Fehlermeldung

- 1 Prüfen Sie Folgendes:
 - Die Verzeichnisse wurden entsprechend den Befehlen im Skript "copy_certs.sh" erstellt.
 - Alle oben aufgeführten Dateien sind vorhanden.
 - Die Zertifikate wurden ordnungsgemäß ausgestellt.
 - Alle Einträge in den Erweiterungsdateien sind korrekt. Achten Sie auf die endgültige Größe (Bytes) der Zertifikate. Die Einträge müssen vor einer Neuerstellung ggf. entsprechend gekürzt werden.
- 2 Ggf.: Setzen Sie das SECURE BOARD wie oben beschrieben zurück und wiederholen Sie den Personalisierungsschritt mit "secureboard_personalize" [ENTER].
- 3 Nach der Anpassung der Konfiguration wiederholen Sie die Zertifikatserstellung und ersetzen Sie die alten Dateien durch die neuen Versionen.
- 4 Führen Sie die Personalisierung Ihres Geräts erneut durch.
- 5 Falls weiterhin Fehlermeldungen auftreten: Aktivieren Sie den Debug-Modus unter "Setup > System > Registry > Devices > Cherry Secureboard", um weitere Informationen zu erhalten und wiederholen Sie die beschriebenen Schritte.
- 6 Wenn Sie ein Skript nicht ausführen können: Versuchen Sie, die Zugriffsberechtigung über "sudo bash chmod 777 <Skript>" [ENTER] anzupassen.
- 7 Wenn Sie während der Ausführung Fehlermeldungen aufgrund fehlender Dateien/Befehle erhalten: Probieren Sie "(sudo) (bash) tr -d '[\000-\010\014-\037\177]' <Datei> <neuer Dateiname>" oder "(sudo) (bash) tr -d '[\015]' <Datei> <neuer Dateiname>" [ENTER].

3.4 Nachdem die Personalisierung abgeschlossen ist

- 1 Aktivieren Sie den Secure Mode unter "Setup > System > Registry > Devices > Cherry Secureboard".

Zunächst blinkt nur die rote LED des Gerätes bis der sichere Kanal aufgebaut ist.

Bei korrekter Konfiguration und Einrichtung leuchtet die rote LED ständig.

3.5 Tipps

- 1 Geben Sie einige Zeichen ein und versuchen Sie mit [TAB] die Ordner-/Dateinamen automatisch zu vervollständigen.
- 2 Bei Linux/Thin Client sind (sudo)/(bash) optional.
- 3 Ggf.: Ergänzen Sie Platzhalter in den Befehlen. Z. B. muss <Datei> durch einen Dateinamen ersetzt werden.

4 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 GmbH
Cherrystraße
91275 Auerbach/OPf.

Internet: www.cherry.de


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


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

Leave us a comment

#cherrykeyboards

 social.cherry.de/fbmx

 social.cherry.de/youtube

 social.cherry.de/twitter

 social.cherry.de/insta

 blog.cherry.de

 xing.com/companies/cherrygmbh

 linkedin.com/company/cherry-

CHERRY SECURE BOARD 1.0

Local Setup on Thin Clients

1 Download tools and certificates

- 1 Download the actual installation package "Quick Installation Package.zip" from https://www.cherry.de/download/us/download.php?product_id=387.
- 2 Unpack the files.

2 Create customer certificates

- 1 If desired: Adapt content of the extension file "user.ext" and/or "SecureBoardCA.config" (e.g. name of your company, ...).

2.1 On windows system (e.g. Win10 64bit)

- 1 Install "Openssl 64bit" (from version 1.1.0L and higher).
- 2 Adapt the script "create_certs.bat".
- 3 If necessary: Change the Openssl path (default path is: "C:\OpenSSL-Win64\bin").
- 4 Add the "Openssl\bin" path to your system environment:
Start "C:\Windows\System32\SystemPropertiesAdvanced.exe" as an admin and add "C:\Openssl-64\bin" or your defined path under "environment variables > path"
- 5 Execute "create_certs.bat".

2.2 On linux system (e.g. Ubuntu 18.04):

- 1 If necessary: Install/update Openssl:
 - sudo apt-get install openssl or
 - sudo apt-get upgrade openssl
- 2 If necessary: Adapt execution rights for "create_certs.sh":
 - sudo chmod 777 create_certs.sh [ENTER]
- 3 Switch to the folder and run the script:
 - sudo (bash) ./create_certs.sh [ENTER] or
 - sudo bash create_certs.sh [ENTER]
- 4 Copy the following files to an external data carrier (e.g. USB stick):
 - copy_certs.sh
 - certs.sh
 - p-20191030.pem and/or p-20190712.pem or other always current production certificate
 - SecureboardRootCA.pem
 - clientca-cert.pem

- clientca-cert.srl (optional)
- user-cert.pem
- user-key.pem
- client-cert.pem
- client-key.pem

3 Install certificates

3.1 On IGEL thin client

Recommended IGEL OS version: 11.02.159 or higher

- 1 Connect the data carrier to the IGEL thin client.
- 2 If necessary: Activate the option for hotplug storage devices via "Setup > Devices > Storage Devices > Storage Hotplug".
- 3 If necessary: Reset the SECURE BOARD:
 - Disconnect the device.
 - Press [D] + [J] + [RIGHT WINDOWS KEY] simultaneously while reconnecting the device.
 - Keep the buttons pressed for about 5 seconds while noticing fast flashing of the LEDs.
 - Disconnect and reconnect the device one more time.

3.2 At terminal (IGEL Setup > Accessories > Terminals)

- 1 Log in as "root": Access to data carrier:
 - cd/media/ [ENTER]
 - ls [ENTER]
 - cd<NAME OF DATA CARRIER> [ENTER]
- 2 If necessary: Switch to the appropriate subdirectory on the data carrier in which the copied files were stored.
- 3 Type "bash copy_certs.sh" [ENTER]
The script starts the personalization process automatically.
- 4 Press (Y).
- 5 After completing the personalization attempt press [CTRL] + [C] (several times if necessary).

3.3 In case of an error message

- 1 Check the following:
 - The directories have been created correctly according to the commands in the "copy_certs.sh" script.
 - All essential files as listed above are present.
 - The certificates have been properly issued.
 - All entries in the extension files are correct. Here you have to pay attention to the final size (bytes) of the certificates. Entries may have to be shortened accordingly before a new creation.
- 2 If necessary: Reset the SECURE BOARD as described above and repeat the personalization step via: "secureboard_personalize" [ENTER].
- 3 After adjusting the configuration, repeat the certificate creation and replace the old files with the new versions.
- 4 Perform the personalization of your device again.
- 5 If error messages still occur: Activate the debug mode under "Setup > System > Registry > Devices > Cherry Secureboard" in order to get further information and repeat the described steps.
- 6 If you cannot execute a script: Try to adapt the access permission via "sudo bash chmod 777 <script>" [ENTER].
- 7 If you receive errors while execution regarding missing files/commands: Try "{sudo} (bash) tr -d '\000-\010\014-\037\177' <file> <new filename>" or "{sudo} (bash) tr -d '\015' <file> <new filename>" [ENTER].

3.4 After the personalization is completed

- 1 Activate the Secure Mode under "Setup > System > Registry > Devices > Cherry Secureboard".

The red LED of the device flashes until the secure channel is established.

Finally, when correctly configured and set up, the red LED lights up permanently.

3.5 Hints

- 1 Type in some characters and press [TAB] in order trying to autocomplete the folder/file names.
- 2 On linux/thin client: {sudo}/{bash} are optional.
- 3 If necessary: Complete the placeholders in the commands. I.e. <file> needs to be replaced with a filename.

4 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

4.1 For Europe

Cherry GmbH
Cherrystraße
91275 Auerbach/OPf.
Germany

Internet: www.cherry.de

4.2 For USA

Cherry Americas, LLC
5732 95th Avenue
Suite 850
Kenosha, WI 53144
USA

Tel.: +1 262 942 6508

Email: sales@cherryamericas.com


Internet: www.cherryamericas.com

Leave us a comment

#cherrykeyboards

 social.cherry.de/fbmx

 social.cherry.de/youtube

 social.cherry.de/twitter

 social.cherry.de/insta

 blog.cherry.de

 xing.com/companies/cherrygmbh

 linkedin.com/company/cherry-
