



CASTLES TECHNOLOGY

MP200 Mobile POS

Book 2

User Manual

Confidential

Version 2.1

Feb 2015

Castles Technology Co., Ltd.

2F, No. 205, Sec. 3, Beixin Rd., Xindian District,
New Taipei City 23143, Taiwan R.O.C.

<http://www.castech.com.tw>

WARNING

Information in this document is subject to change without prior notice.

No part of this publication may be reproduced, transmitted, stored in a retrieval system, nor translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of **Castles Technology Co., Ltd.**

All trademarks mentioned are proprietary of their respective owners.

Revision History

Version	Date	Descriptions
1.0	Sep 10, 2014	Initial creation.
2.0	Dec 19, 2014	1. Add "Key Injection" on "System Menu" page 2. UI arrangement on "SYSTEM INFO" page 3. Add "BT DIRECT ACCESS", "Halt Timeout", "PWM Auto", "PWM Mode", "PWM Time" on "SYS SETTINGS" page 4. UI arrangement on "Test Utility" page
2.1	Feb 12, 2015	1. Add the description of Environment. 2. Add the description of Power. 3. Add the UL caution of battery.

Contents

1. Introduction.....	6
2. Hardware Setup.....	7
2.1. Parts of the Surface	7
2.2. Environment	9
2.3. Power	9
3. Basic Operation	10
3.1. Program Manager.....	10
3.2. Download AP	12
3.3. System Info.....	13
3.4. Memory Status	14
3.5. System Settings.....	15
3.6. Test Utility	18
3.7. Factory Reset	20
3.8. Power Off	21
3.9. Function Key Password Change.....	22
3.10. Share Object Management	23
3.11. Castles TMS	24
3.12. Font Mng	25
3.13. Debug Tools	26
3.14. ULD Key Hash.....	27
3.15. Plug-in Mng	28
3.16. Key Injection.....	29
4. Secure File Loading.....	30
4.1. ULD Key System	30
4.1.1. ULD Manufacturer Key.....	30
4.1.2. ULD User Key	32
4.1.3. Key Change	32
4.2. File Signing.....	33
4.2.1. Signing Kernel Module	33
4.2.2. Signing User Files	35
4.3. File Loading	39
4.3.1. Download by User Loader.....	39
4.4. Changing ULD User Key.....	42

5. Font Management	49
5.1. Loading New Font.....	49
5.2. Custom Font.....	52
5.3. Using TrueType Font (TTF)	60
6. FCC Warning	62
FCC Caution.....	62
RF Exposure Warning.....	62

1. Introduction

This document provides a guideline on operating and configuring Castles MP200 Mobile POS.

The scope of this document includes setting up the terminal, basic operation, application life cycle, and some advance features.

2. Hardware Setup

2.1. Parts of the Surface

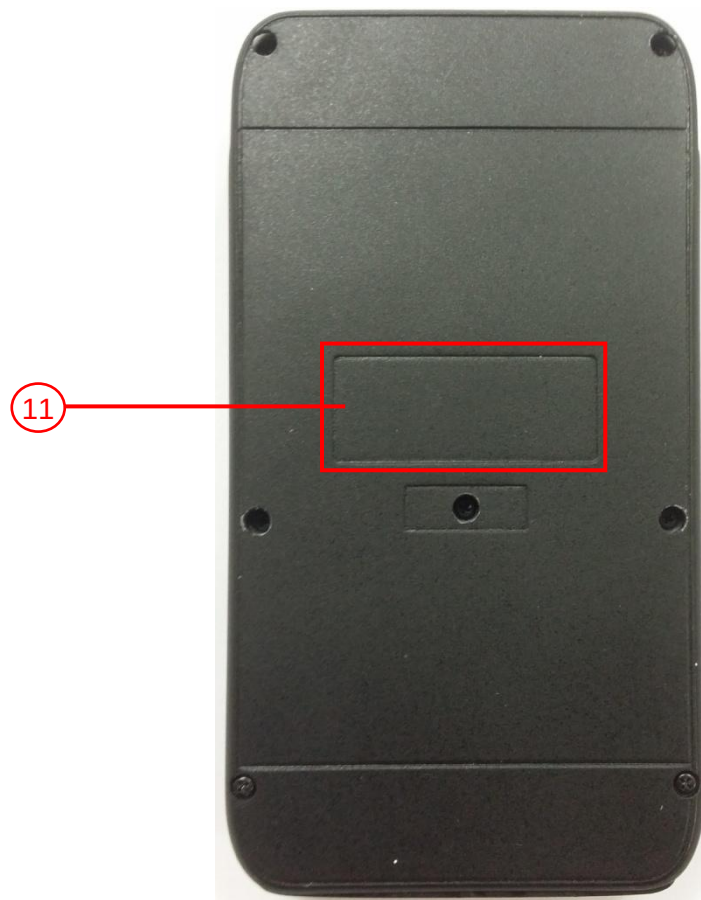
Front Side



MP200

- | | |
|---|-------------------|
| 1. LCD Display (Mono Color) | 6. Power Key |
| 2. Keyboard | 7. Up Key |
| 3. Cancel Key | 8. Down Key |
| 4. 0 / Function Key | 9. OK / Enter Key |
| 5. Contactless Card Landing
Zone Enter Key | 10. Clear Key |

Rear Side



11. Machine's Label

Up Side



12. MSR
13. SCR

bottom Side



Side



- 14. Power LED** (Charging: Orange light, Fully charged: Green light)
15. Micro USB Socket

2.2. Environment

Operating Temperature : 0°C to 50°C

Storage Temperature : -20°C to 70°C

Operating Humidity : 5% to 90% non-condensing

Storage Humidity : 5% to 95% non-condensing

2.3. Power

Input : 5V, 1A

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.

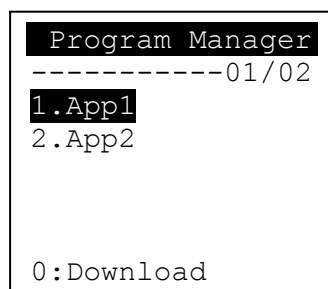
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

3. Basic Operation

3.1. Program Manager

Upon power on, terminal will enter Program Manager if not default application selected. All user applications are list in Program Manager. User may select an application and run the application or view the application info, delete the application or set to default run upon power on. User may enter System Menu to configure terminal settings.

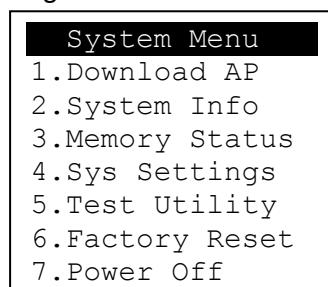
Program Manager



- Press [0] button to enter System Menu.
- Press [1] button to toggle default application selection.
- Press [2] button to delete application.
- Press [3] button to view application info.
- Press [OK] button to run application.
- Press [↑] or [↓] to select application.

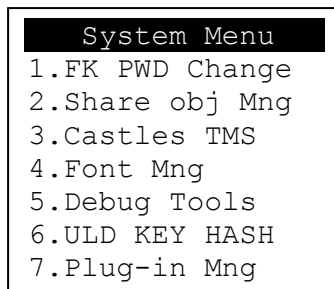
System Menu

Page 1



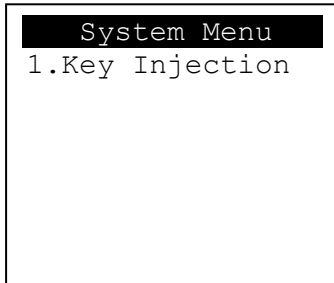
- Press [↓] button to page 2.

Page 2



- Press [↑] button to page 1.
- Press [↓] button to page 3.

Page 3

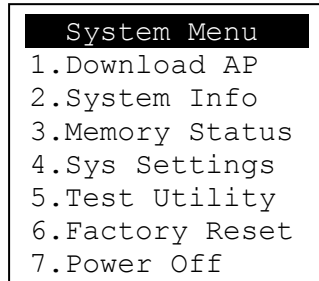


- Press [↑] button to page 2.

3.2. Download AP

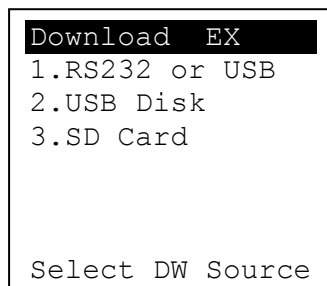
Download user application or kernel modules firmware.

System Menu



- Press [1] button to enter Download AP menu.

Download AP Menu



Select download source:

- Press [1] button to select source as RS232 or USB connection and enter ULD download mode.
- Press [2] button to select source as USB disk.
- Press [3] button to select source as SD card.

3.3. System Info

View kernel module firmware information.

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off

- Press [2] button to enter System Info menu.

System Info Menu

Page 1

SYSTEM INFO
---Kernel Ver---
BIOS :VR0010
SULD :VRF810
LINUXKNL :VR0019
ROOTFS :VR9201

Page 2

SYSTEM INFO
--- KO Ver ---
SECURITY :VR0025
KMS :VR0024
DRV :VR0039
USB : N/A
SAM :VR0028
CL :VR0018

Page 3

SYSTEM INFO
--- KO Ver2 ---
SC :VR0011

- Press [↓] button to next page.

Page 4

SYSTEM INFO
--- SO Ver ---
UART :VR0014
USBH :VR0011
MODEM :VR0014
ETHERNET :VR0029
FONT :VR0025
LCD :VR0034

Page 5

SYSTEM INFO
--- SO Ver2 ---
PRT :VR0020
RTC :VR0013
ULDPM :VR0022
PPP MODEM:VR0026
KMS :VR0022
FS :VR0015

Page 6

SYSTEM INFO
--- SO Ver3 ---
GSM :VR0018
BARCODE :VR0013
TMS :VR0013
TLS :VR0011
CLVW :VR0018
CTOSAPI :VR9029

Page 8

SYSTEM INFO
--- HWM Ver ---
CRDL/ETHE:ONCHIP
CLM-MP : N/A
--- AP Ver ---
ULDPM :VR0026

Page 9

SYSTEM INFO
HUSB ID:0CA6A050
CUSBID : N/A
--Factory S/N---
FFFFFFFFFFFFFFFF

Page 10

SYSTEM INFO
--EXT SO Ver P.1--
CACLM DL :VRg103
CACLENTRY :VRg103
CAMPP :VR0302
CAVPW :VR0014
CAEMVL2 :VR9113
CAEMVL2AP :VR0005

3.4. Memory Status

View terminal flash memory and RAM information.

System Menu

```
System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

- Press [3] button to enter Memory Status menu.

Memory Status Menu

```
MEMORY STATUS
--FLASH Memory--
Total:  130688KB
Used :   96648KB

--SDRAM Memory--
Total:   65408KB
Used :   32148KB
```

3.5. System Settings

View or change terminal system settings.

Setting	Descriptions
Key Sound	Enable (Y) or disable (N) the beep sound when pressing any key.
Exec DFLT AP	Enable (Y) or disable (N) execution of default selected application.
USB CDC Mode	Enable (Y) or disable (N) USB CDC mode.
FunKey PWD	Enable (Y) or disable (N) password protection to access function key (0 ~ 3) in Program Manager.
PMEnter PWD	Enable (Y) or disable (N) password protection to enter Program Manager.
SET USB Host	Enable (Y) or disable (N) USB host mode.
Base USB CDC	Enable (Y) or disable (N) USB CDC mode in base unit. [Portable model only]
List SHR Lib	Enable (Y) or disable (N) to list all shared libraries in Program Manager.
Key MNG Mode	<TBC>
BAT Threshld	Battery charging threshold value. [Portable model only]
Null Cradle	Enable (Y) if base is Type A cradle. [Portable model only]
Debug Mode	Enable (Y) or disable (N) console debug mode.
Debug Port	Serial port for console debug.
Mobil AutoON	Enable (Y) or disable (N) to auto turn on GSM module after start up the terminal.
Bklit Auto Off	Enable (Y) or disable (N) Auto Off LCD Backlight
Bklit Off Time	Threshold of Auto Off LCD Backlight
PWR KEY OFF	Power key function, power off (Y) or reboot(N)
GDB Mode	Enable (Y) or disable (N) GDB mode.
GDB Timeout	GDB connection timeout.
GDB Channel	GDB connection channel.
ETHER IP/PORT	GDB Ethernet connection setting.
RTC Time Zone	Set Time Zone of Real Time Clock.
NTP Enable	Enable (Y) or disable (N) Network Time Protocol.

NTP Update Freq	Frequency of Network Time Protocol updating.
BT DIRECT ACCESS	Enable (Y) or disable (N) Bluetooth direct access mode.
Halt Timeout	Set timeout for AP to back to Program Manager whenever AP is in halt state.
PWM Auto	Enable (Y) or disable (N) power saving mode.
PWM Mode	Select (STB) standby mode or (SLP) sleep mode for power saving mode.
PWM Time	Set time period by which to make terminal getting into power saving mode from idle state.

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off

- Press [4] button to enter System Settings menu.

System Settings Menu

Page 1

SYS SETTINGS
Key Sound : Y
Exec DFLT AP : Y
-Default AP Name
USB CDC Mode : Y
FunKeyPWD : N
PMEnterPWD : N
2: Next Page

Page 2

SYS SETTINGS
SET USB Host : N
Base USB CDC : X
List SHR Lib : N
Key MNG Mode : 0
Bat Threshld : X
Null Cradle : X
1: Prev 2: Next

Page 3

SYS SETTINGS
Debug Mode : N
Debug Port : X
Mobil AutoON : N
Bklit Auto Off : N
Bklit Off Time : X
PWR KEY OFF : N
1: Prev 2: Next

Page 4

SYS SETTINGS
GDB Mode : N
GDB Timeout : X
GDB Channel : X
ETHER IP/PORT
1: Prev 2: Next

Page 5

SYS SETTINGS		
RTC Time Zon	:	GMT
NTP Enable	:	N
NTP Update F	:	X
1: Prev	2: Next	

Page 6

SYS SETTINGS		
BT DIRECT ACCESS	:	X
Halt Timeout	:	999
PWM Auto	:	N
PWM Mode	:	X
PWM Time	:	X
1: Prev Page		

- Press [↑] or [↓] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇌ N ⇌ Y.
- Press [1] button to previous page.
- Press [2] button to next page.

3.6. Test Utility

Perform terminal hardware components diagnosis.

System Menu

System Menu	
1.Download AP	
2.System Info	
3.Memory Status	
4.Sys Settings	
5.Test Utility	
6.Factory Reset	
7.Power Off	

- Press [5] button to enter Test Utility menu.

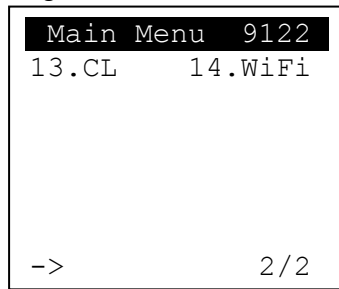
Test Utility Menu

Page 1

Main Menu 9122	
1.LCD	2.KBD
3.FLASH	4.SCM
5.Light	6.MSR
7.LED	8.RTC
9.FONT	10.USB
11.BT	12.Power
->	1/2

- Press [1] and [OK] to diagnose LCD.
- Press [2] and [OK] to diagnose keyboard.
- Press [3] and [OK] to diagnose flash memory.
- Press [4] and [OK] to diagnose smart card module.
- Press [5] and [OK] to diagnose backlight.
- Press [6] and [OK] to diagnose magnetic stripe card reader.
- Press [7] and [OK] to diagnose LED.
- Press [8] and [OK] to diagnose RTC.
- Press [9] and [OK] to check FONT file in MP200.
- Press [10] and [OK] to diagnose USB.
- Press [11] and [OK] to check Bluetooth chip address and name.
- Press [12] and [OK] to test functionality of power saving.
- Press [↓] button to page 2.

Page 2

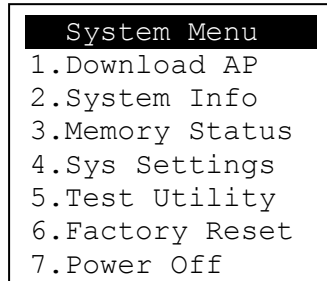


- Press [13] and [OK] to diagnose contactless card reader.
- Press [14] and [OK] to diagnose WiFi.
- Press [↑] button to page 1.

3.7. Factory Reset

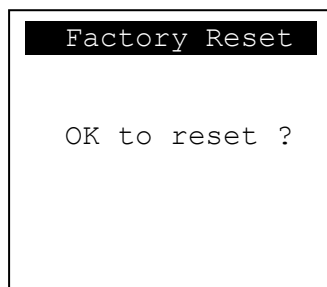
Perform factory reset, all user application, fonts and data will be deleted.

System Menu



- Press [6] button to enter Factory Reset menu.

Factory Reset Menu



- Press [OK] button to perform factory reset.



- Enter factory reset password. **Default password: 8418**

3.8. Power Off

Power off terminal.

System Menu

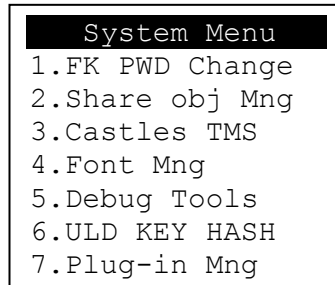
System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off

- Press [7] button to power off terminal.

3.9. Function Key Password Change

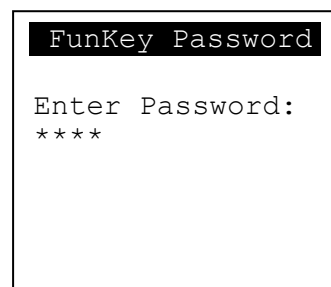
Change function key access password.

System Menu (Page 2)

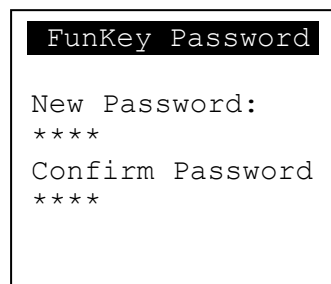


- Press [1] button to enter FunKey Password menu.

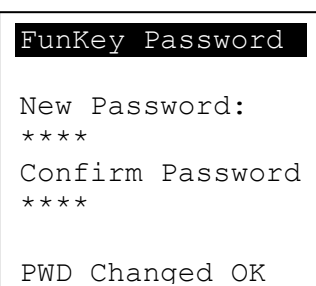
FunKey Password Menu



- Enter current password. (*Default password is "0000"*)



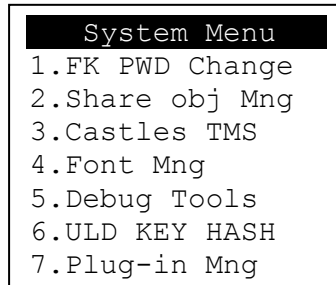
- Enter new password.
- Enter new password again to confirm.



3.10.Share Object Management

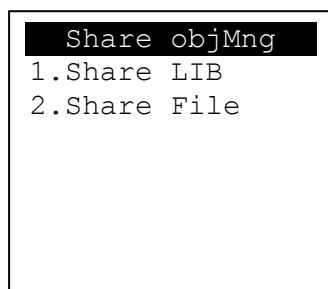
View share object in terminal.

System Menu (Page 2)



- Press [2] button to enter Share Object Management menu.

Share Object Management Menu

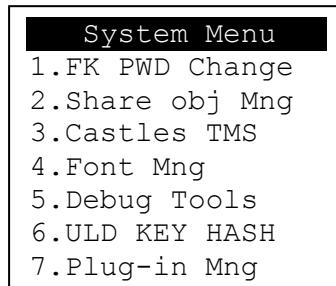


- Press [1] button to view shared library.
- Press [2] button to view shared file.

3.11.Castles TMS

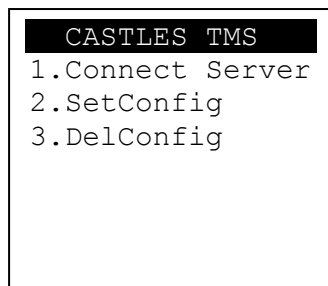
Connect to TMS (Terminal Management Software) server, set or delete TMS configuration.

System Menu (Page 2)



- Press [3] button to enter Castles TMS menu.

Castles TMS Menu

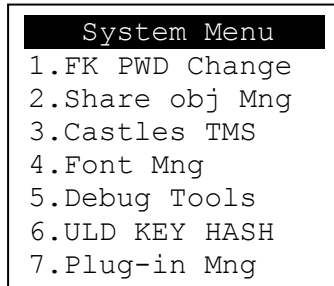


- Press [1] button to connect to TMS server.
- Press [2] button to set TMS configuration.
- Press [3] button to delete TMS configuration.

3.12.Font Mng

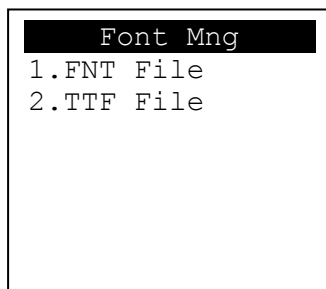
View Font Management.

System Menu (Page 2)



- Press [4] button to view Font Management.

FontManagment

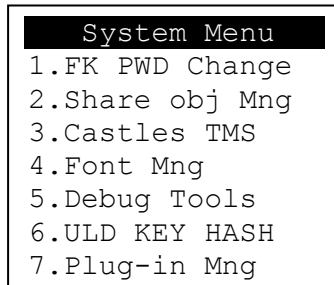


- Press [1] button to view FNT Font list.
- Press [2] button to view TTF Font list.

3.13.Debug Tools

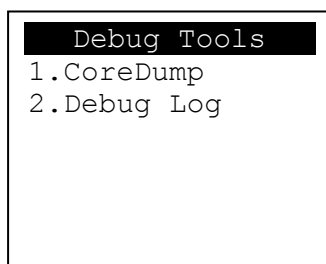
Perform the Debug Tools.

System Menu (Page 2)



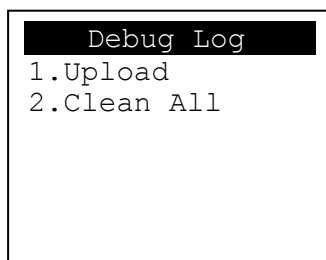
- Press [5] go to the Debug Tools Menu.

Debug Tools



- Press [1] go get the Core Dump error from terminal.
- Press [2] go to the Debug Log Menu.

Debug Log

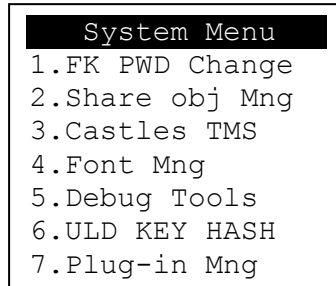


- Press [1] move the Debug Log from the memory of terminal to SD card.
- Press [2] clean all the Debug Log in MP200.

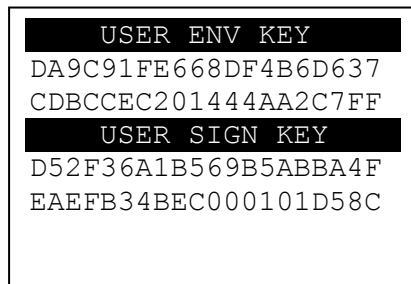
3.14.ULD Key Hash

View ULD user key hash value.

System Menu (Page 2)



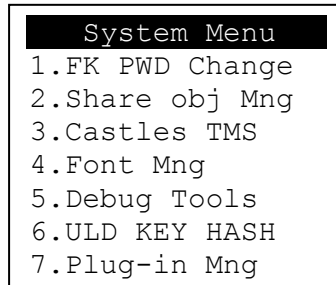
- Press [6] button to view hash value.



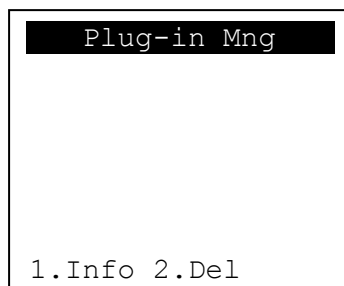
3.15.Plug-in Mng

View Plug-in Management.

System Menu (Page 2)



- Press [7] button to view Plug-in Management.

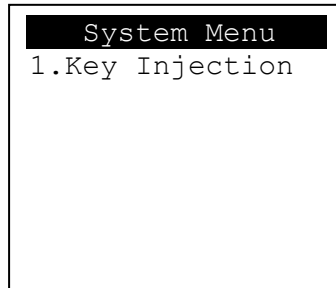


- Press [↑] or [↓] button to select item.
- Press [1] button to get item information.
- Press [2] button to delete item.

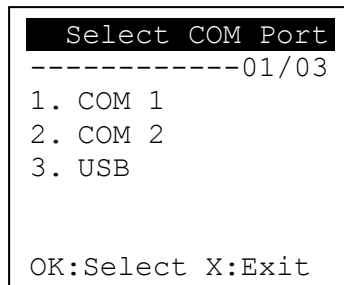
3.16.Key Injection

View Key Injection.

System Menu (Page 3)



- Press [1] button to view Key Injection.



- Press [1] to select COM 1.
- Press [2] to select COM 2.
- Press [3] to select USB.
- Press [OK] to set port.
- Press [X] to exit.

4. Secure File Loading

Castles implemented an interface in terminal named User Loader(ULD) to provide secure file loading to system memory. Loading of user application, kernel firmware, font and others must use User Loader.

The loading process is secure by signing the files using ULD Key System.

4.1. ULD Key System

The ULD Key System uses two key sets for securely managing the kernel updating and application downloading. Each key set contains two RSA key pairs. One is used for key encryption and the other is used for signature. These two key sets are specified as below:

ULD Manufacturer Key Set

- ULD Manufacturer Key Encryption Key (RSA)
- ULD Manufacturer Signature Key (RSA)

ULD User Key Set

- ULD User Key Encryption Key (RSA)
- ULD User Signature Key (RSA)

For MP200, the RSA key length is 2048bits.

4.1.1. ULD Manufacturer Key

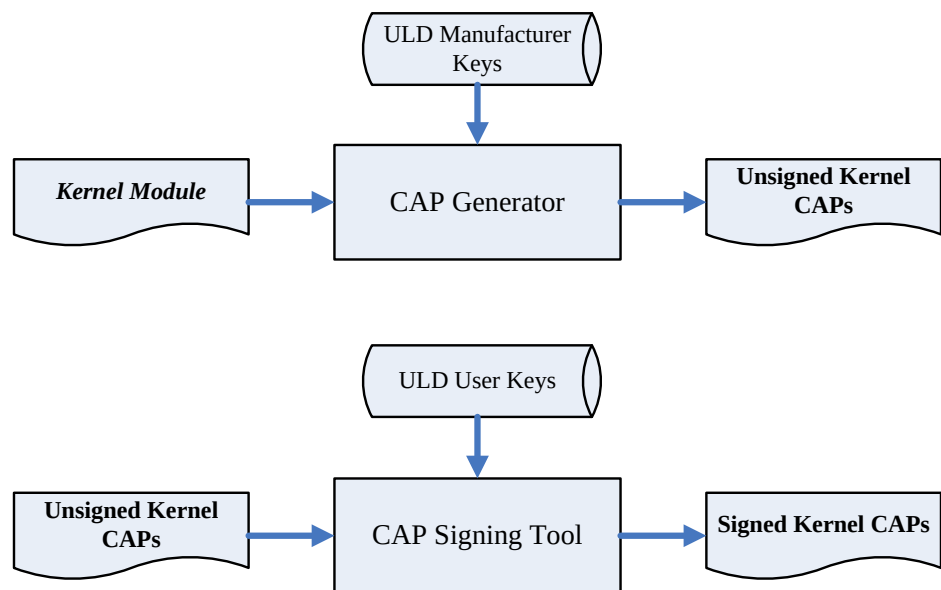
The system consists of several kernel modules. These kernel modules are provided by the Manufacturer, and released in CAP format file with encryption and signing via ULD Manufacturer Keys.

The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only the user can have the privilege to decide whether the system is to be updated. Therefore, before system

updating, the kernel CAP files must be “signed” via ULD User Key to get the user permission. For simple expression, we call the kernel CAP files generated by the manufacturer as “unsigned kernel CAP(s)” and call the kernel CAP files “signed” by the user later as “signed kernel CAP(s)”.

Notes:

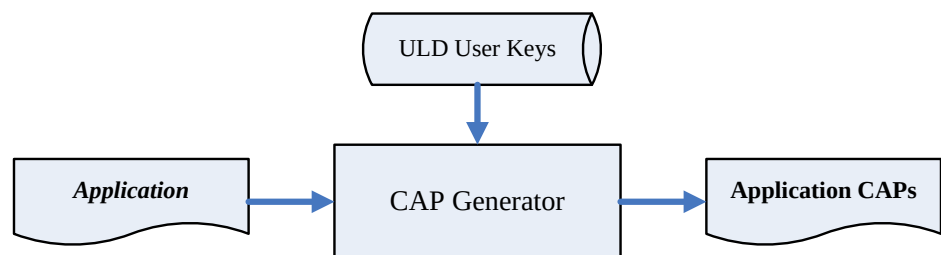
1. The kernel modules are encrypted by a random-generated 3DES key, which is retrieved from the Key Encryption Block of the CAP by ULD Manufacturer Key Encryption Key, not directly encrypted by ULD RSA Key.
2. The “sign” action via ULD User Keys actually is done by” the second encryption”. “The second encryption” is done by using the random-generated 3DES key, which is encrypted by ULD User Key Encryption Key, to perform Triple DES encryption again on the cipher data segment of the kernel CAP files. This ensures that the system cannot retrieve the correct data from the kernel CAPs without the user permission.



4.1.2. ULD User Key

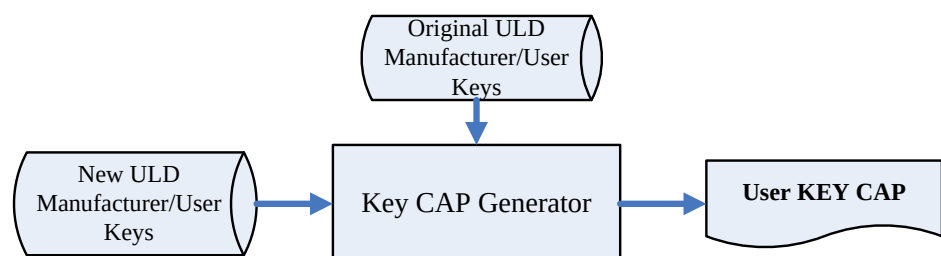
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the “signed” action via ULD User Keys.

Notes: Applications are encrypted by a random-generated 3DES key, which is retrieved from the Key Encryption Block of the CAP by ULD User Key Encryption Key, not directly encrypted by ULD RSA Key.



4.1.3. Key Change

The ULD RSA Keys are able to be changed. The system uses a special CAP file, KEY CAP, for the manufacturer and user to change their own keys. The KEY CAP contains a new set of ULD keys (Key Encryption Key and Signature Key). These new keys are encrypted and signed via the original keys. In other words, if the user would like to change the ULD User Keys, they have to use their original ULD User Keys with the new ULD User Keys to generate a KEY CAP.



4.2. File Signing

4.2.1. Signing Kernel Module

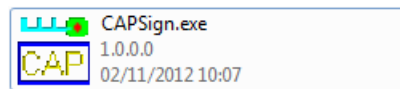
Castles will release new version of kernel module in “unsigned” form. This files required to sign with ULD User Key before it can load to terminal.

Castles Technology provideds a tool named “CAP Signing Tool” to perform this task.

The CAP Signing Tool is located at:

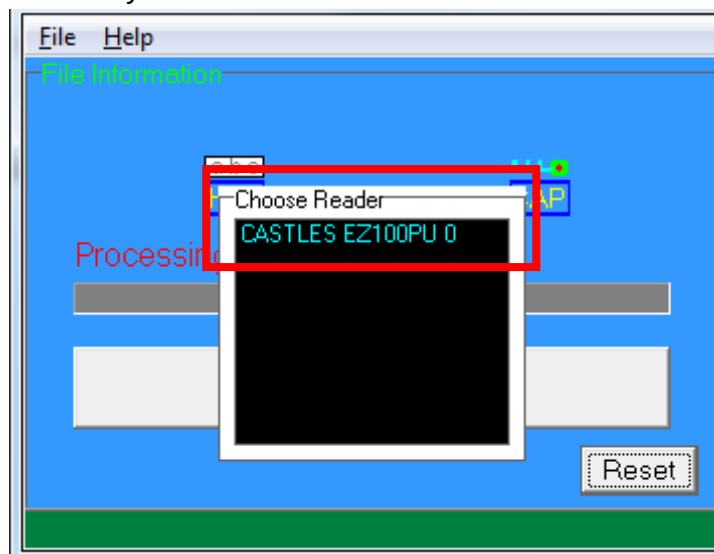
C:\Program Files\Castles\MP200\tools\Signing Tool

- Run CAP Signing Tool

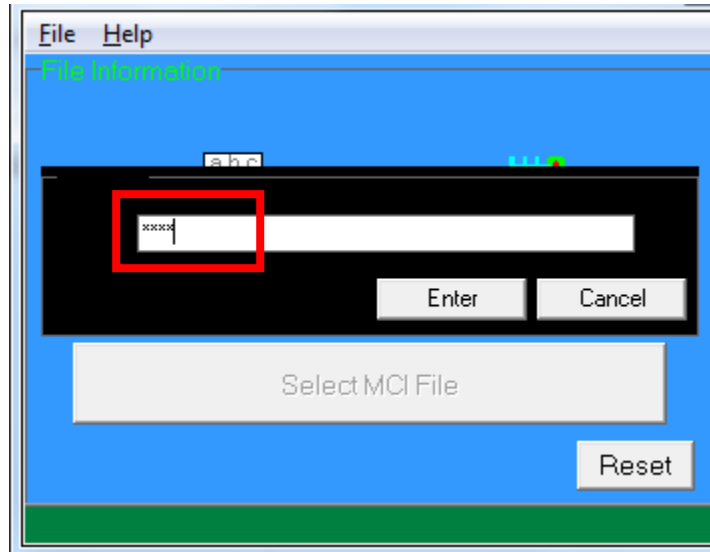


(MP200)

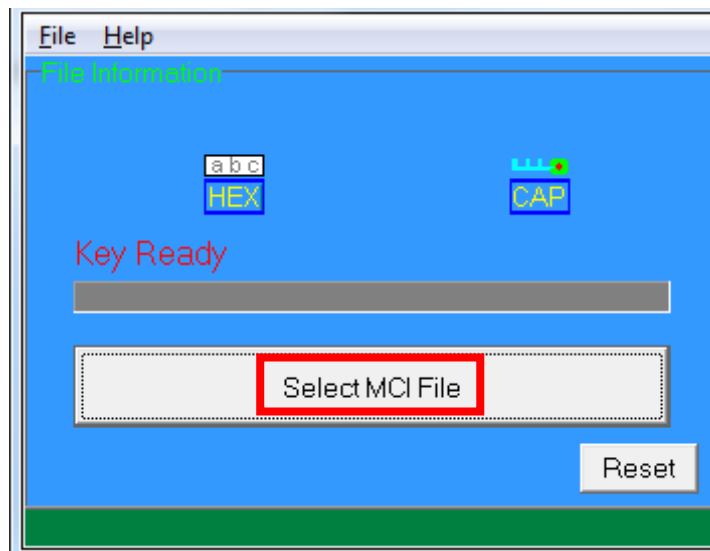
- Insert Key Card and select smart card reader



- Enter Key Card PIN



- CAP Signing Tool is ready, press "Select MCI File" button to browse the file.



- Output file will be located in "signed" folder.

4.2.2. Signing User Files

Following files are required to sign before load to terminal. This is to ensure the application data and codes confidential and integrity. The output file will be “CAP” file which is file format defined by Castles.

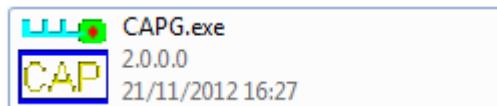
- User application
- User application data files
- User application library
- Font file
- Share library
- Share files
- System setting
- Key CAP (Manufacturer ULD Key Set)

Castles Technology provided a tool named “CAP Generator” to perform this task.

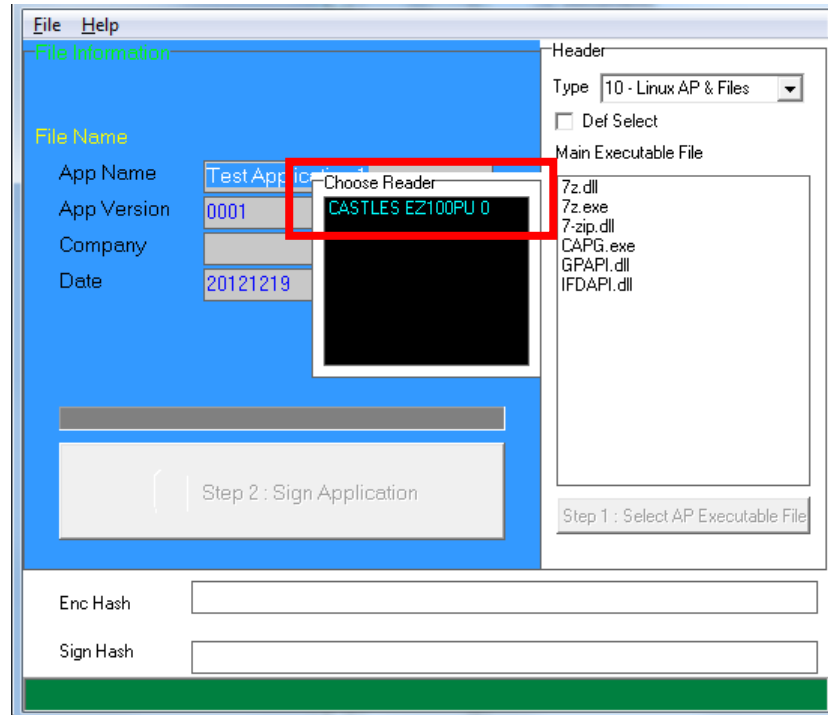
The CAP Generator is located at:

C:\Program Files\Castles\MP200\tools\CAPG (KeyCard)

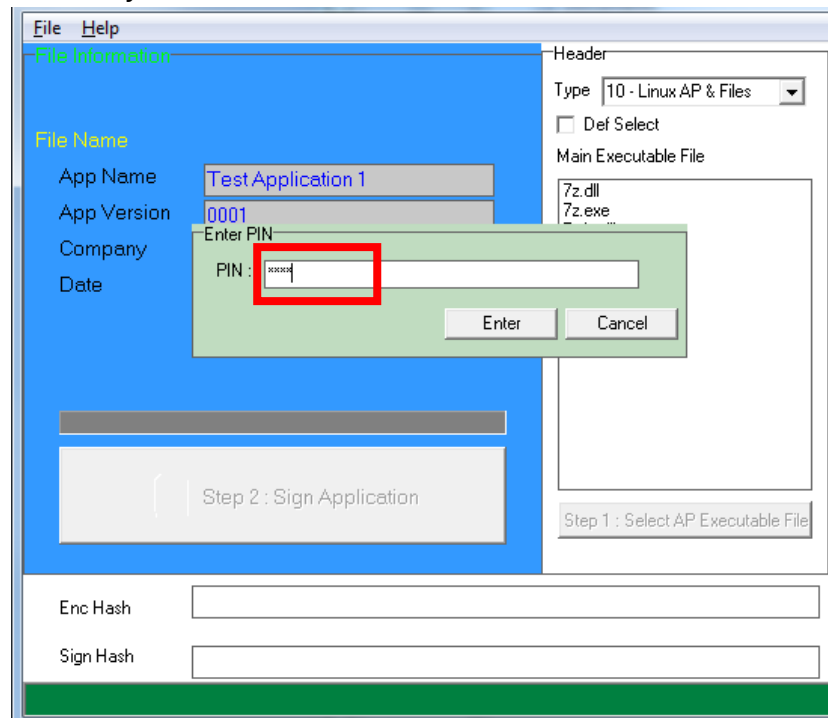
- Run CAP Generator



- Insert Key Card and select smart card reader



- Enter Key Card PIN



- CAP Generator is ready, select the correct Type from the list.

File Information

File Name

App Name: Test Application 1

App Version: 0001

Company:

Date: 20121219

Step 2: Sign Application

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A

Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

Header

Type: 10 - Linux AP & Files

10 - Linux AP & Files

11 - Linux Font

20 - Share Library

21 - Share Files

22 - AppData Files

23 - System Setting

24 - App Library

A0 - Linux Key CAP

IFDAPI.dll

Step 1: Select AP Executable File

- Press “Step 1: Select AP Executable File” to select file to sign. This is valid for all the files to sign.

File Information

File Name

App Name: V5_HelloWorld

App Version: 0001

Company:

Date: 20121219

Finished!

Step 2: Sign Application

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A

Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

Header

Type: 10 - Linux AP & Files

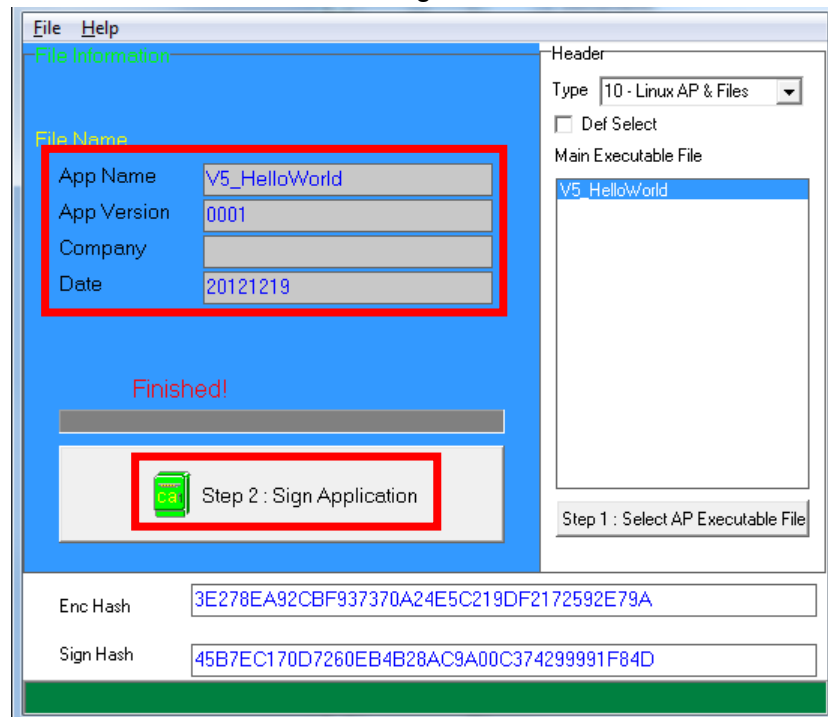
Def Select

Main Executable File

V5_HelloWorld

Step 1: Select AP Executable File

- Enter file details and press “Step 2: Sign Application” to sign the file. This is valid for all the files to sign.



- The output file will be in a set. A “mci” file with one or more “CAP” files. CAP file contents the signed file binaries, where MCI file contents the list of CAP files.



Note: If user would like to load multiple set of signed file, create a new file with extension of “mmci”. Then put the mmci file contents with the list of mci file.



4.3. File Loading

There are several ways of loading file to MP200.

- Download by User Loader
- Download by user application
- Download by Castles TMS

User Loader is a tool provided by Castles Technology. It's the formal way to download file to terminal.

User may implement their own ways of updating application or files using CTOS API provided, **CTOS_UpdateFromMMCI()**.

Castles TMS (CTMS or CASTLES Terminal Management System) is provided by Castles Technology. It's use to perform remote download via Ethernet, GPRS/UMTS or modem.

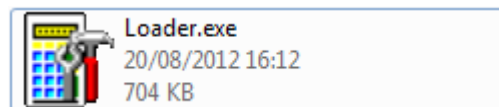
4.3.1. Download by User Loader

The User Loader works for MP200.

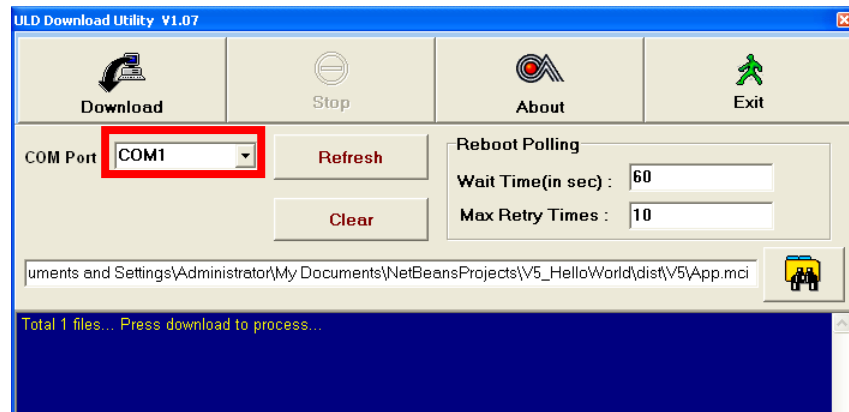
The Loader is located at:

C:\Program Files\Castles\MP200\tools\Loader

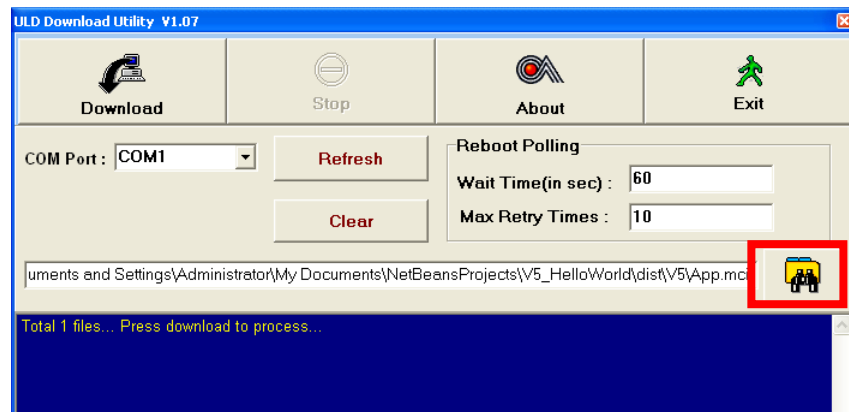
- Run User Loader



- Select COM port

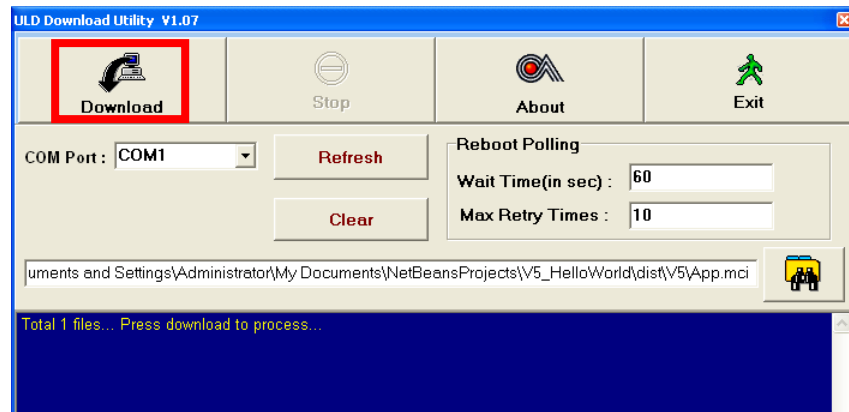


- Browse and select mci file or mmci file

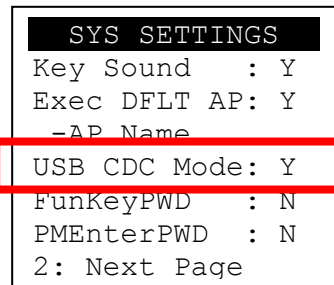


- Setup terminal to enter download mode
 - Press [0] button in Program Manager (PM)
 - Press [1] button to select "1. Download AP"
 - Press [1] button again to select download via RS232 or USB

- Press “Download” button to start.



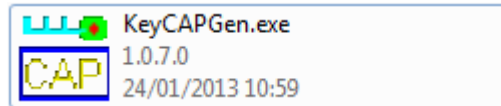
*Note: To download using USB cable, terminal must enable CDC mode.
Set USB CDC Mode to Y.*



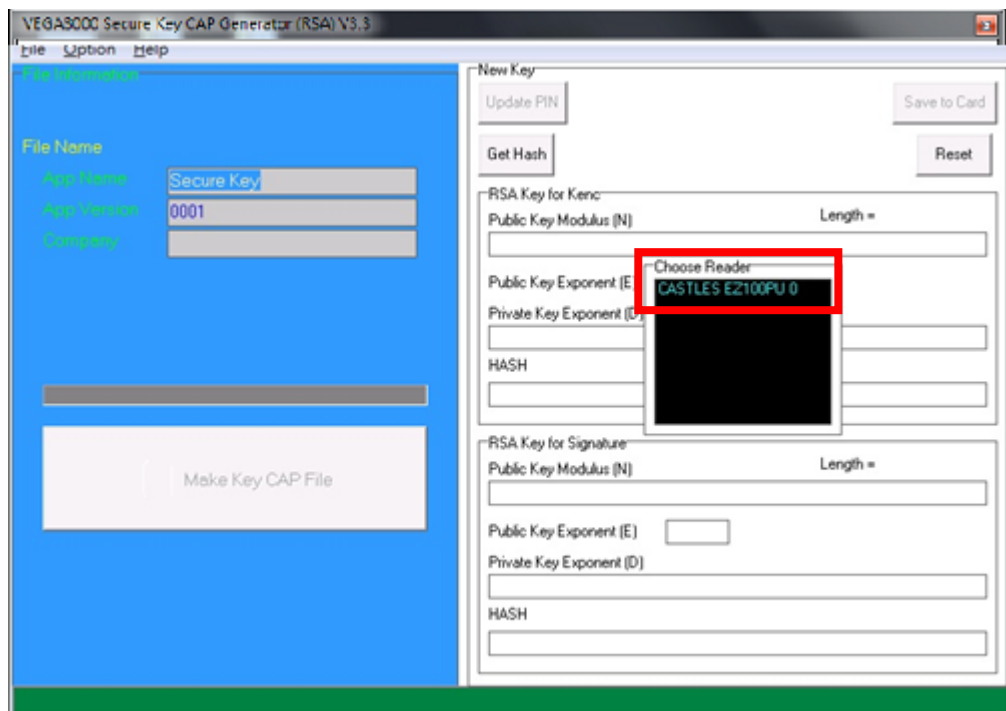
4.4. Changing ULD User Key

User may change their ULD User Key Set stored in Key Card. Castles Technology provided a tool named “Secure Key Generator” to perform this task.

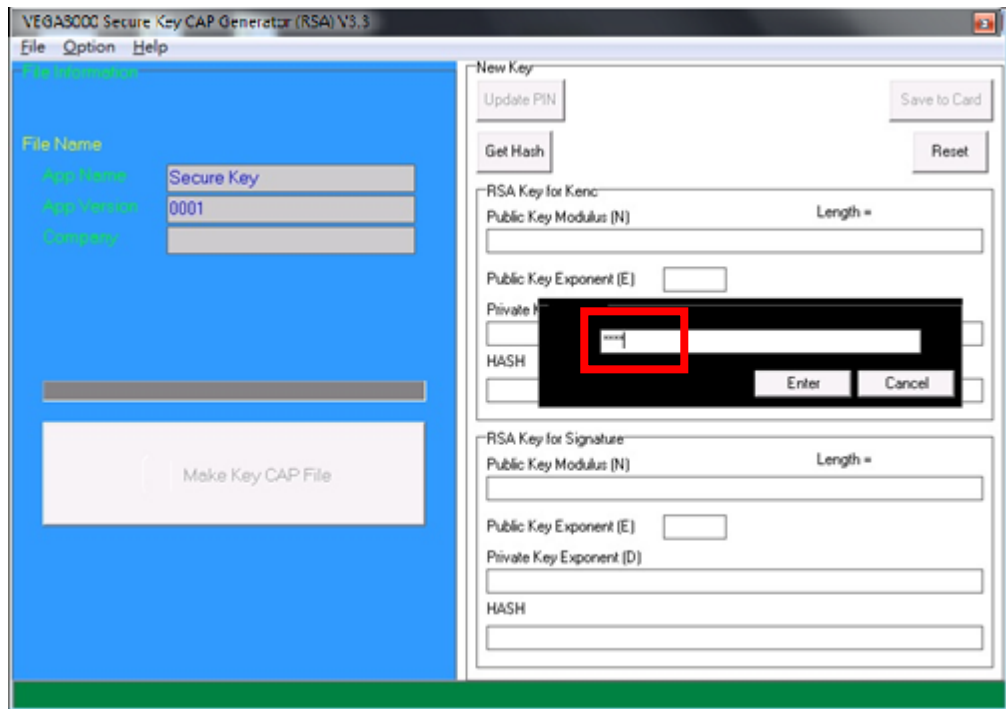
- Run Secure Key Generator



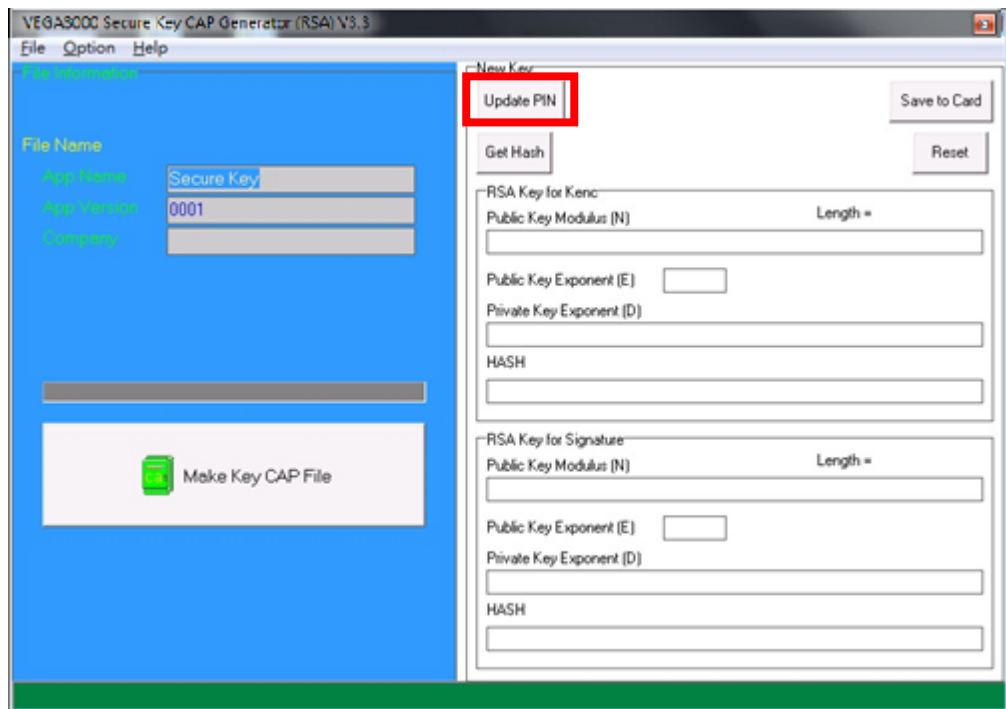
- Insert Key Card and select smart card reader



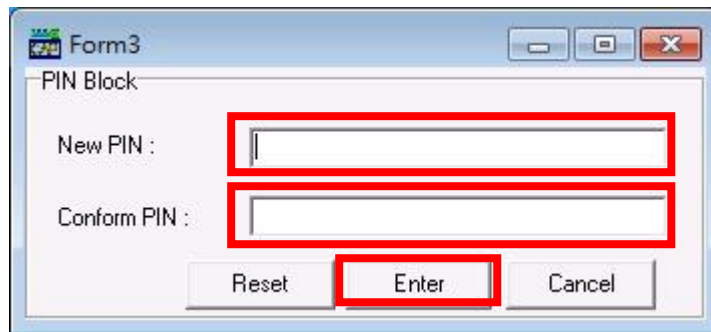
- Enter Key Card PIN, default PIN is “1234”.



- To change Key Card PIN, press “Update PIN” button. If not, please skip this steps.



- Enter new PIN, enter new PIN again to confirm, then press [Enter] button to change PIN in Key Card.



Form3

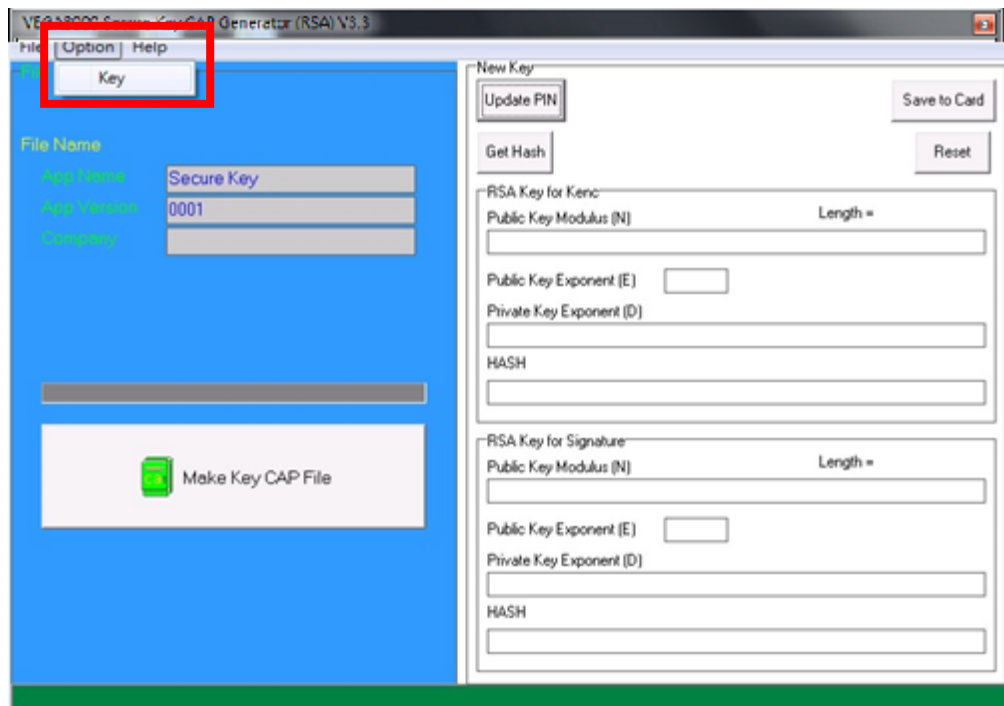
PIN Block

New PIN :

Conform PIN :

Reset Enter Cancel

- To view current key set hash value, goto “Option” and select key.



VEGA3000 Secure Key Generator (RSA) V3.3

File Name

App Name: Secure Key

App Version: 0001

Company:

Make Key CAP File

Option Help

Key

New Key

Update PIN Save to Card

Get Hash Reset

RSA Key for Kerio

Public Key Modulus (N) Length =

Public Key Exponent (E)

Private Key Exponent (D)

HASH

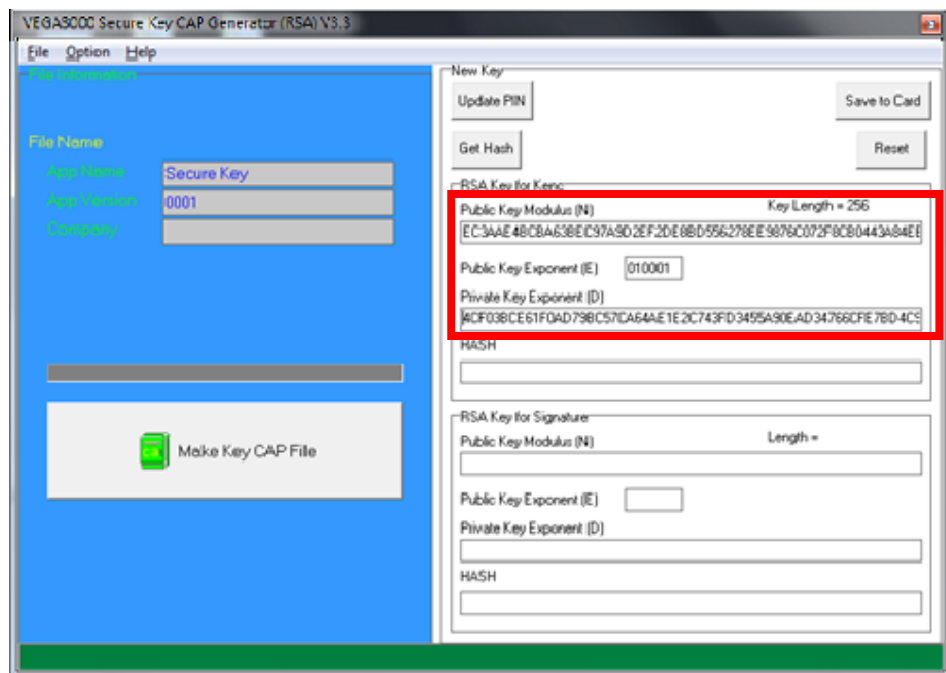
RSA Key for Signature

Public Key Modulus (N) Length =

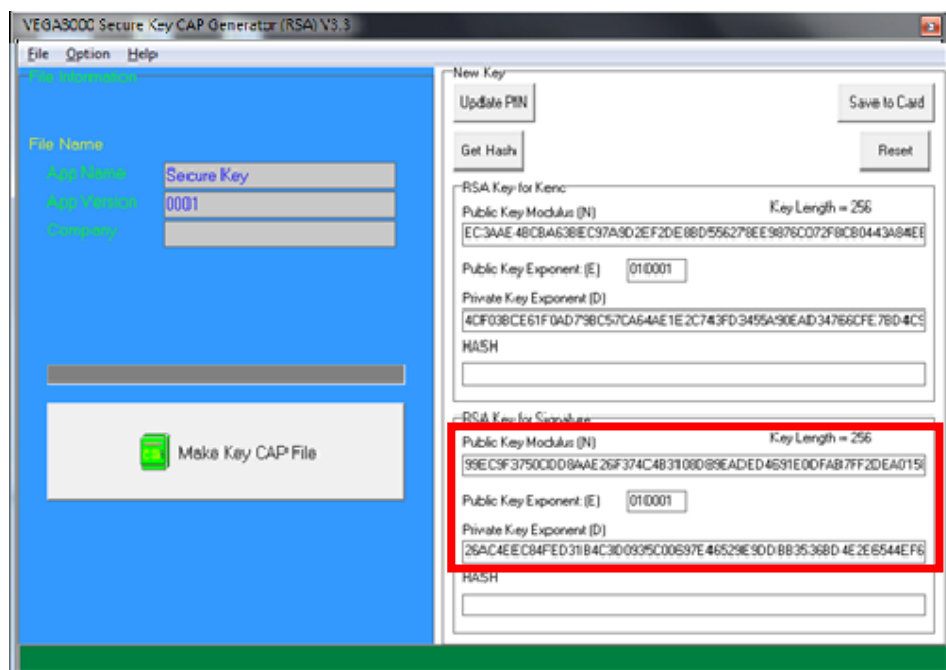
Public Key Exponent (E)

Private Key Exponent (D)

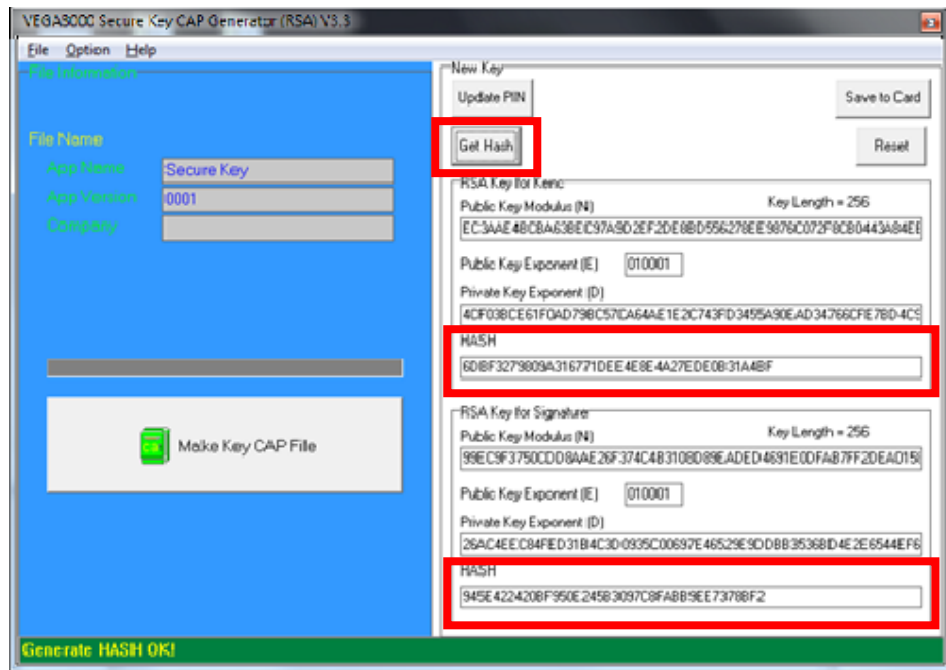
HASH



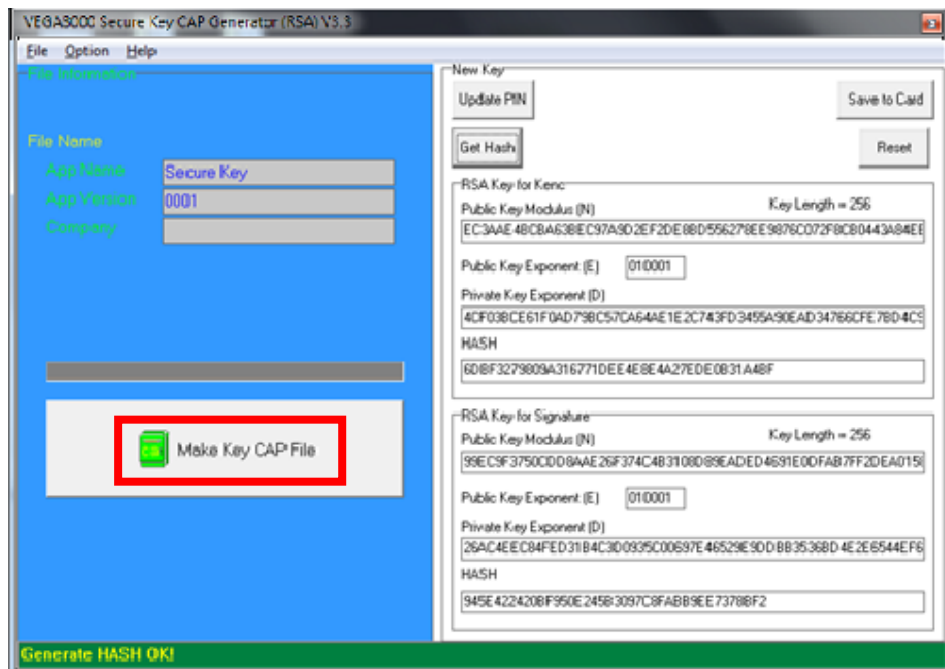
- Generate second RSA key set for Signature.



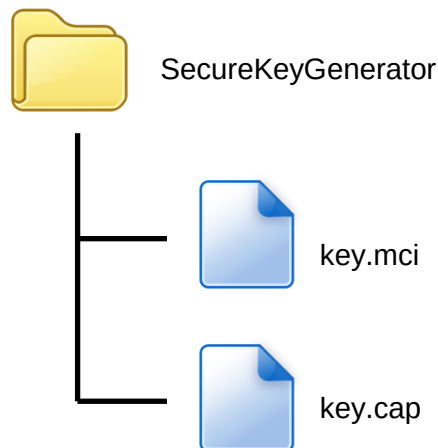
- Click [Get Hash] button to calculate the hash value for key sets.



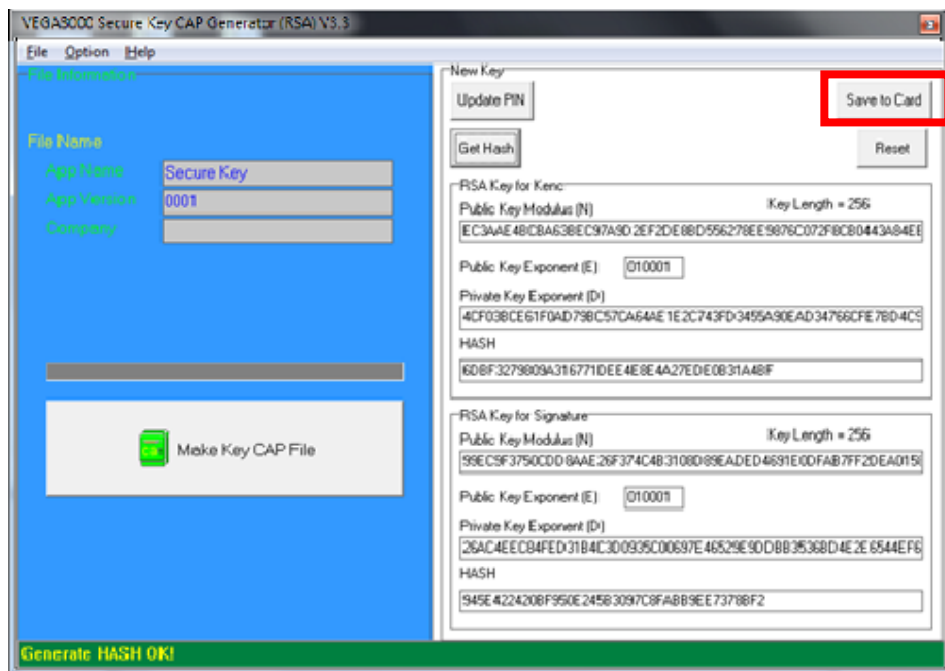
- Please copy down all the values into a text file and keep in a safe place. You will need this if you need to create duplicate Key Card.
- To generate the key CAP for the newly generated user key set, press [Make Key CAP File] button.



- The output file will be located in the Secure Key Generator folder.



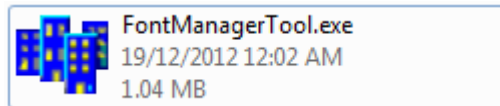
- To update the newly generated key set to Key Card, press [Save to Card] button to write the key set to Key Card.



5. Font Management

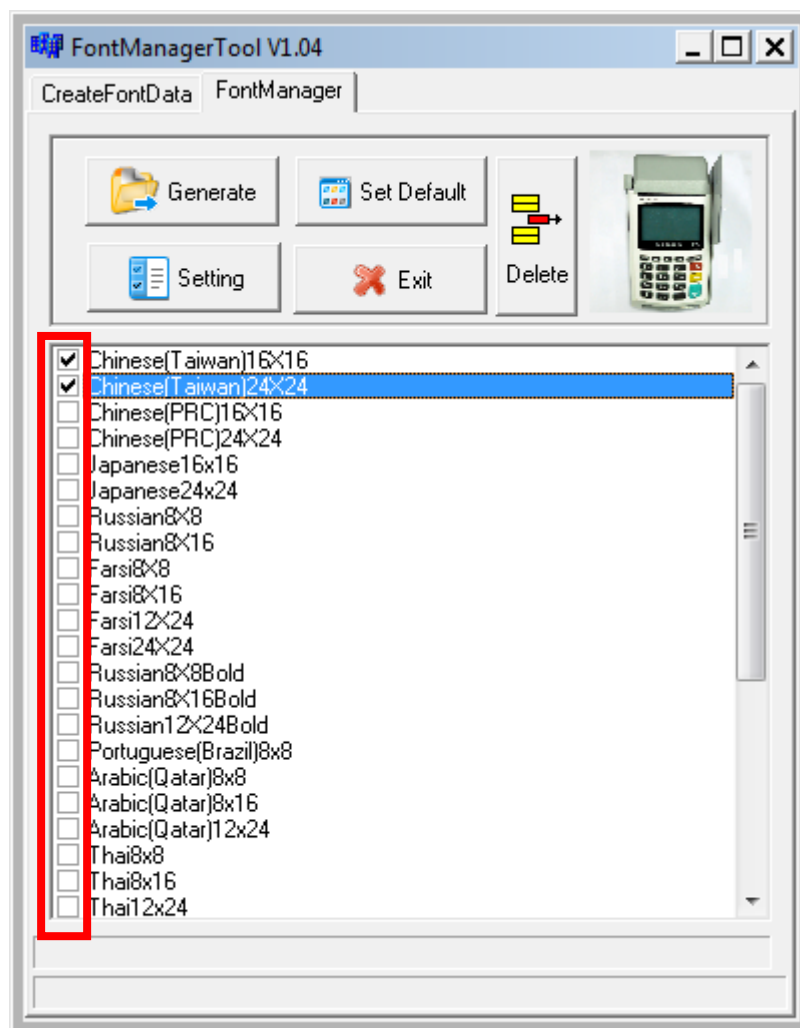
5.1. Loading New Font

- Run FontManager.exe

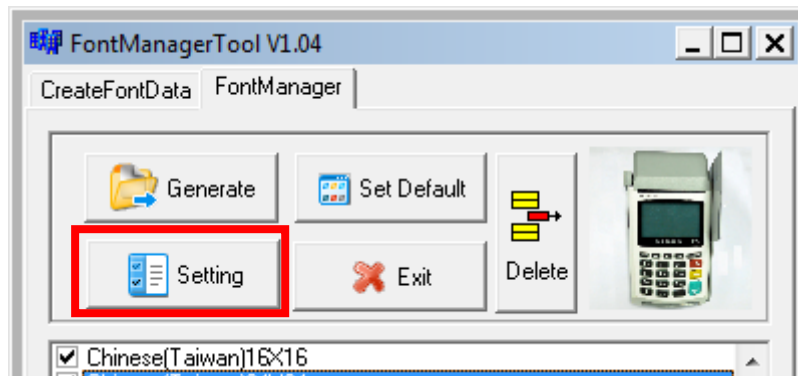


Located at C:\Program Files\Castles\Font Manager

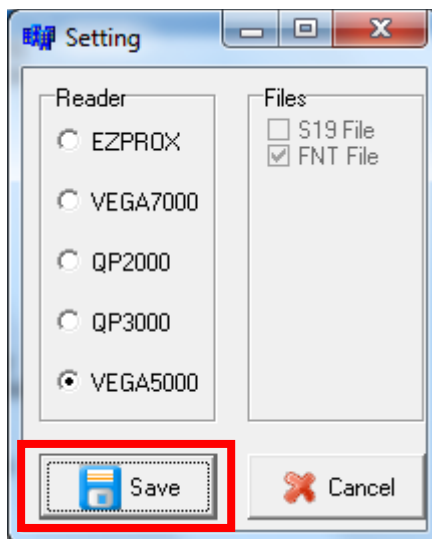
- Select font to download



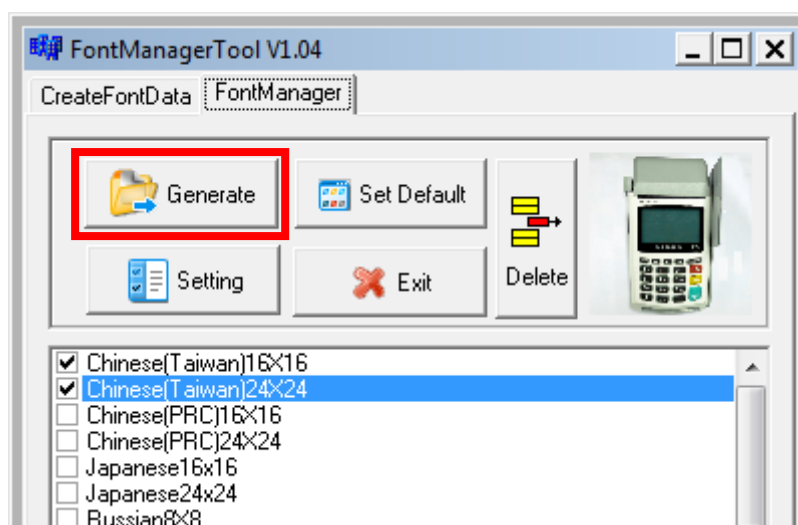
- Press [Setting] button to configure terminal type.



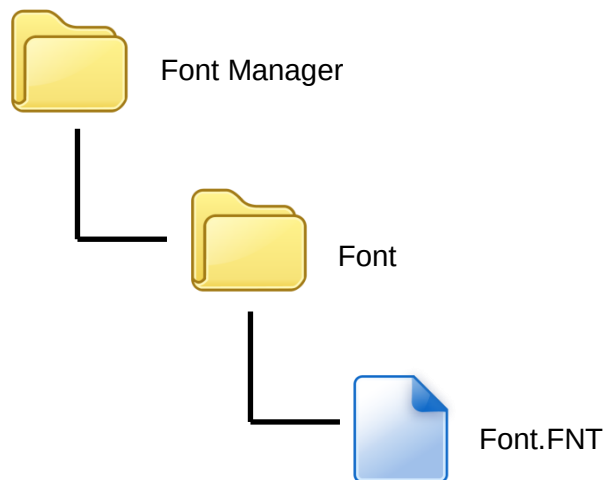
- Select **VEGA5000**, press [Save] button to save and return font manager.



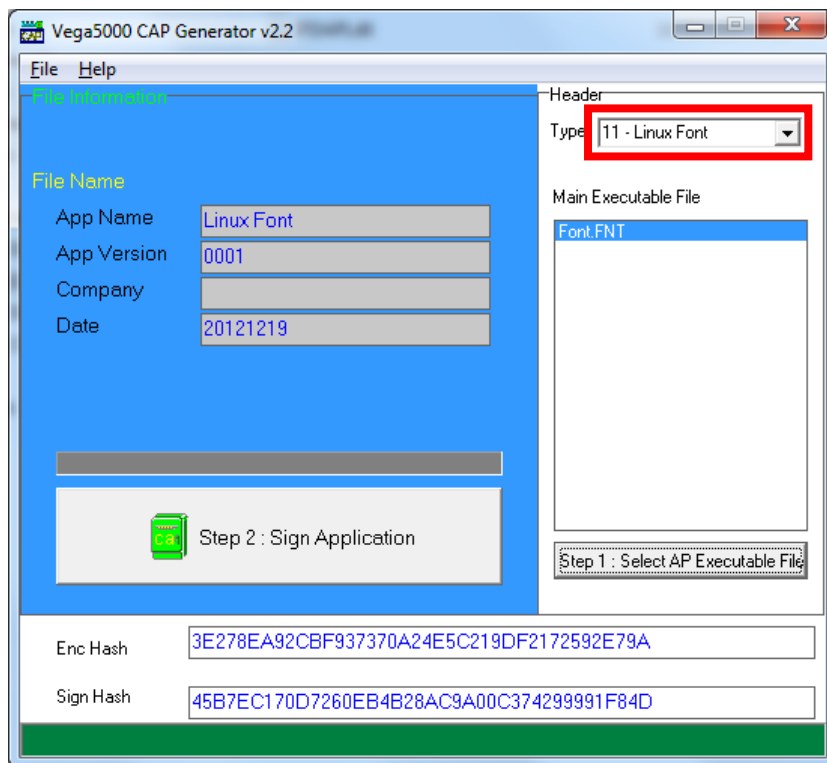
- Press [Generate] to create the font file.



- Output file “Font.FNT” will be located at sub-directory named “Font” in “Font Manager” folder.



- Sign the file using CAP Generator, the type must set to “11 – Linux Font”.



- Lastly, download the signed file (CAP file) to terminal using Loader.

5.2. Custom Font

User may create font they preferred for displaying or printing on terminal.

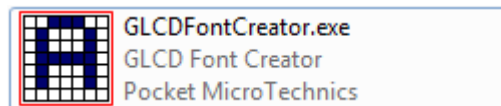
There are two zone defined:

Zone 0x00 ~ 0x7F – ASCII characters, you may replace with the font type preferred or your own language character set.

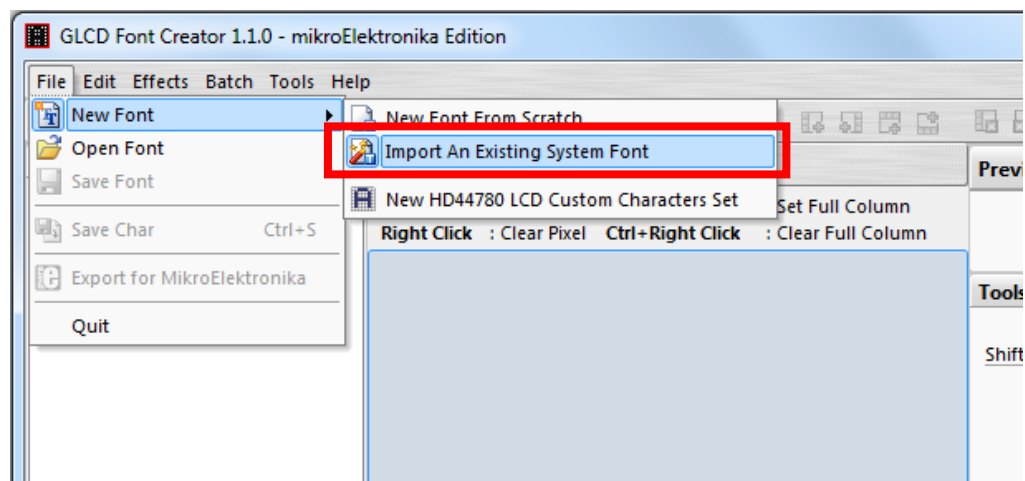
Zone 0x80 ~ 0xFF – Free to use, you may use for symbols.

Following steps demonstrate how to create a 12x24 font.

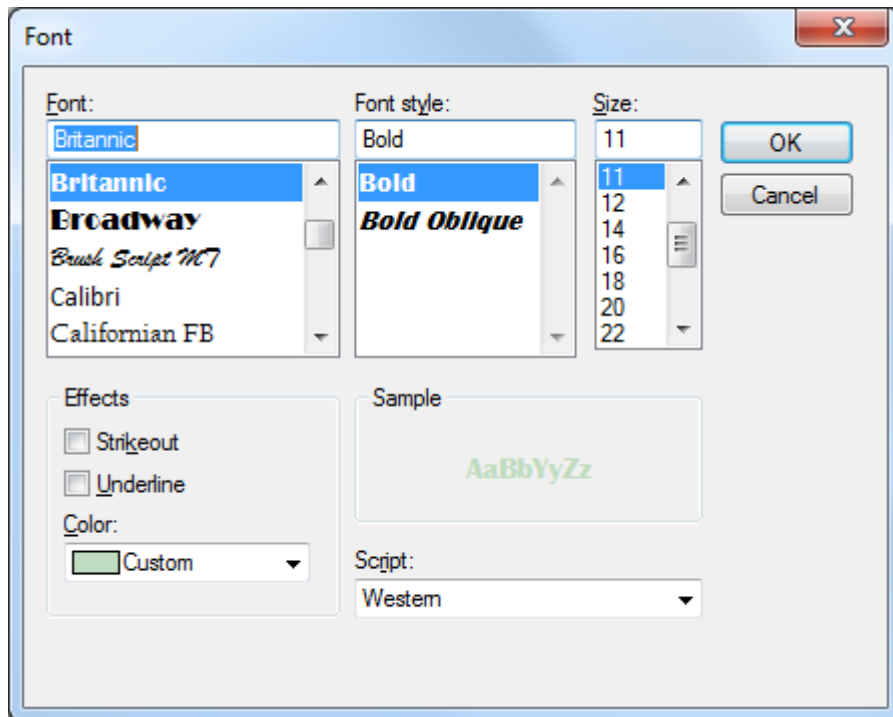
- Run GLCD Font Creator



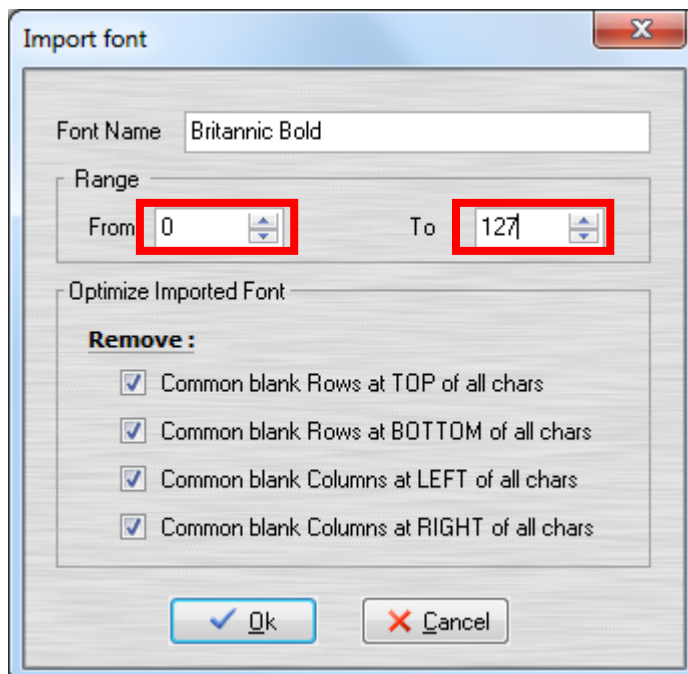
- Select [File] ⇒ [New Font] ⇒ [Import An Existing System Font]



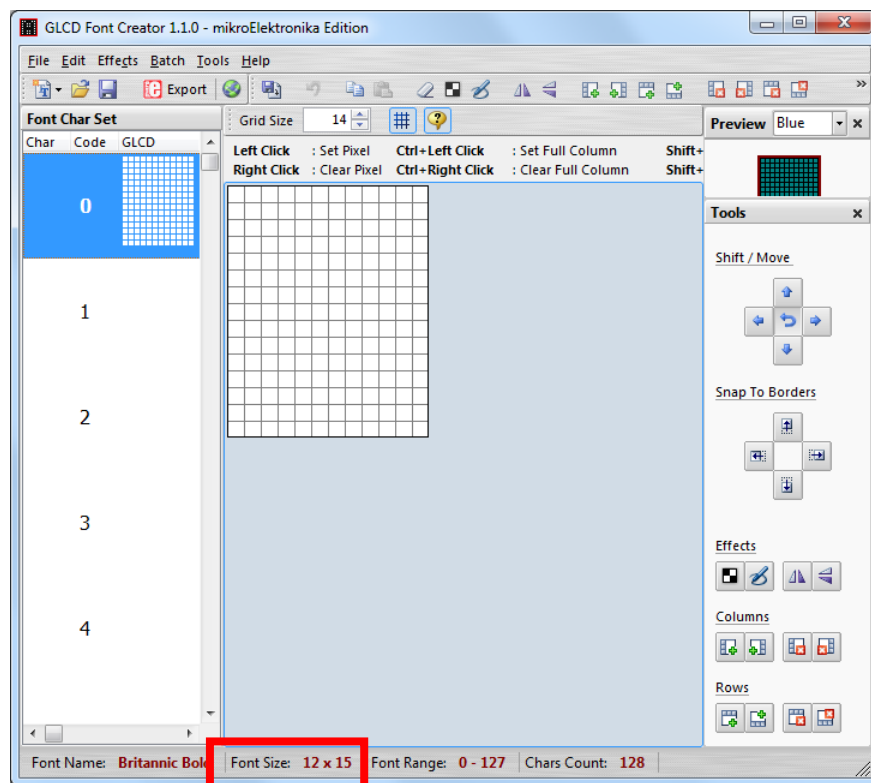
- Select the font needed, simply choose a font size. The final value of font size should be determined by the minimum pixel width. You may need to repeat this steps few times to find the best fit font size.



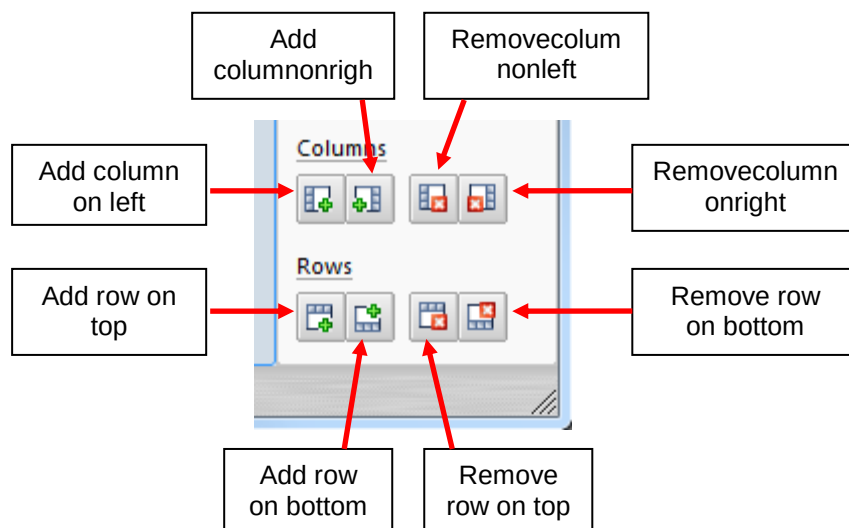
- Set the import range from 0 to 127.



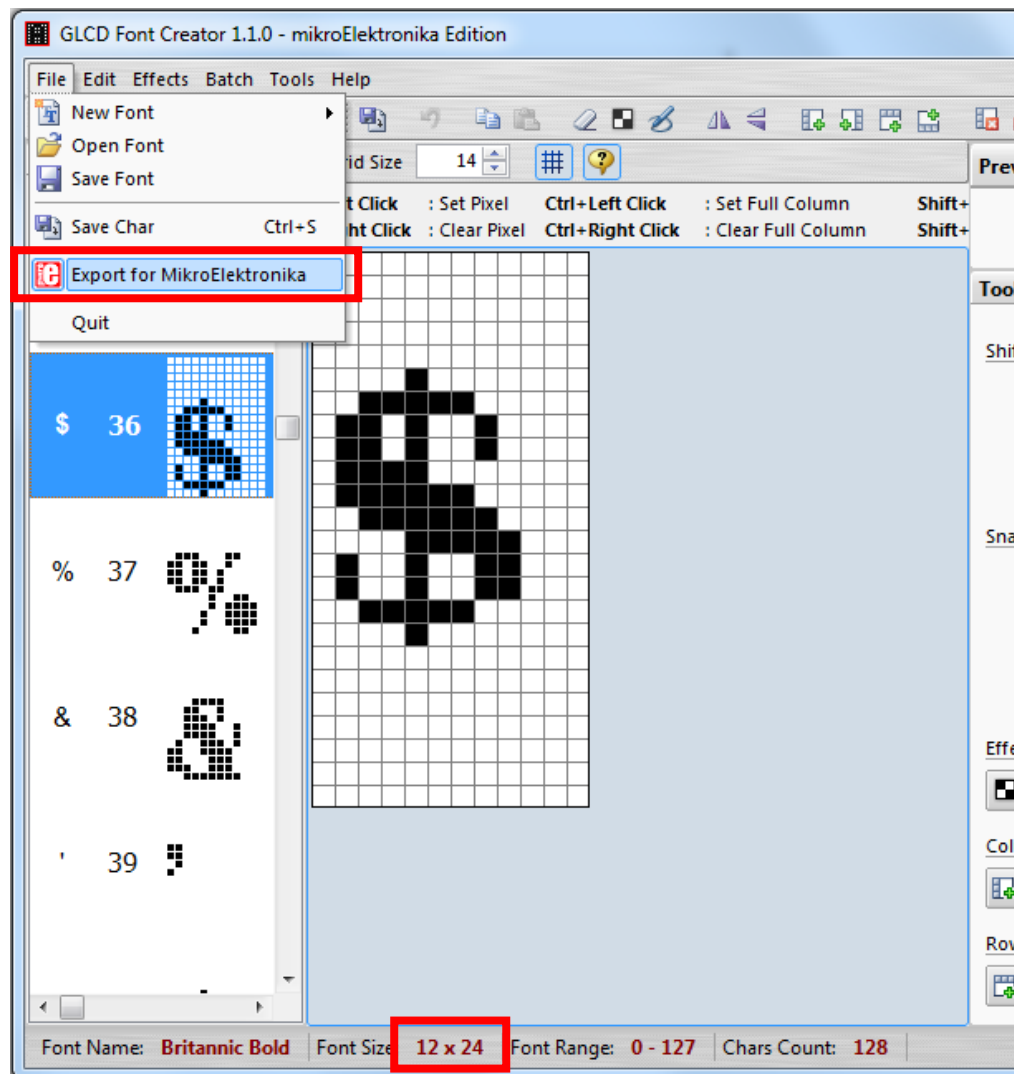
- Check the minimum pixel width and height.



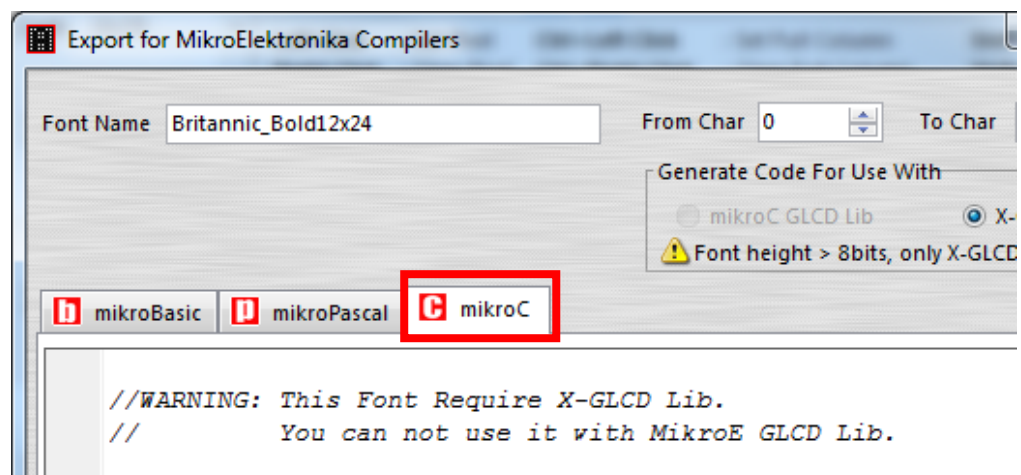
- If the pixel width of the font size is larger than expected, then you have to repeat the previous steps to import font with smaller size.
- Use the following buttons to adjust the font size to match with expected font size.



- After adjust font size, select [File] ⇒ [Export for MikroElektronika].



- Select output format as [mikroC].

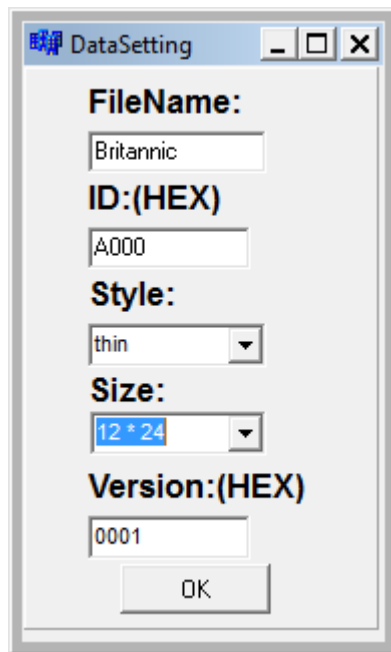


- [illegible]

- FontManagerTool.exe
30/10/2012 10:14
1.04 MB

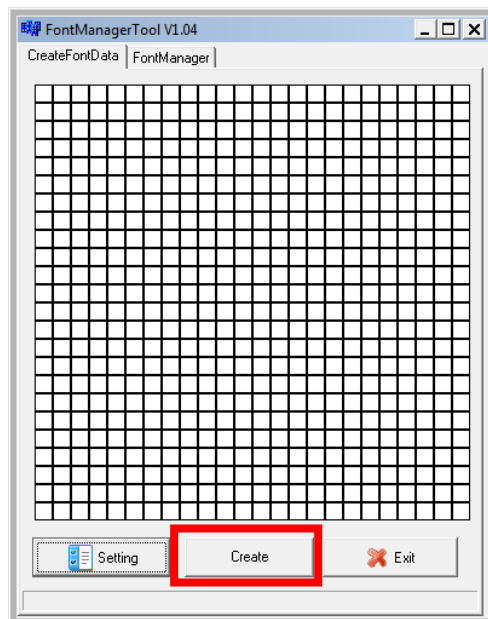
-

- Enter the file name, font id, and select the size.



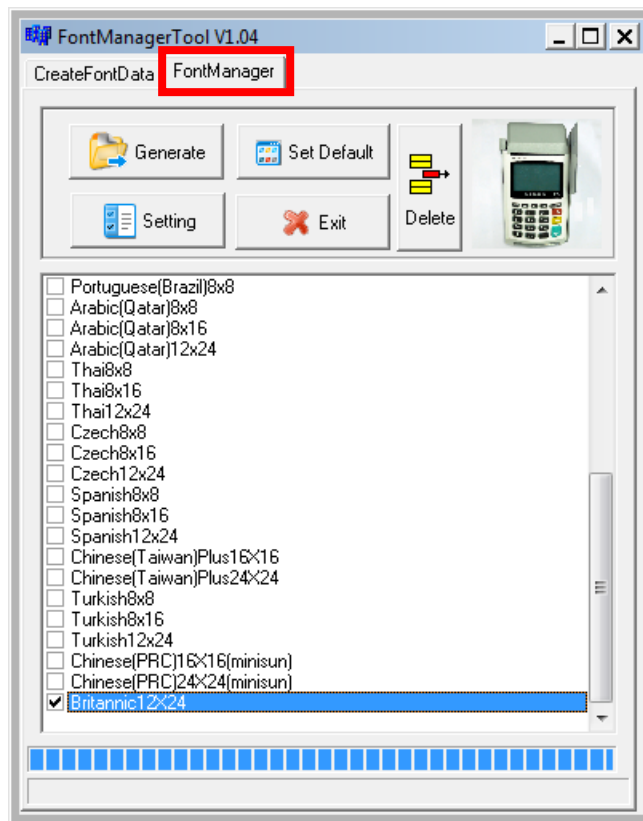
The image shows a dialog box titled "DataSeting". It contains several input fields and a dropdown menu. The "FileName:" field contains the text "Britannic". The "ID:(HEX)" field contains the text "A000". The "Style:" dropdown menu is set to "thin". The "Size:" dropdown menu is set to "12 * 24". The "Version:(HEX)" field contains the text "0001". There is an "OK" button at the bottom.

- Click [Create] button, and select the C file previously created using GLCD Font Generator.

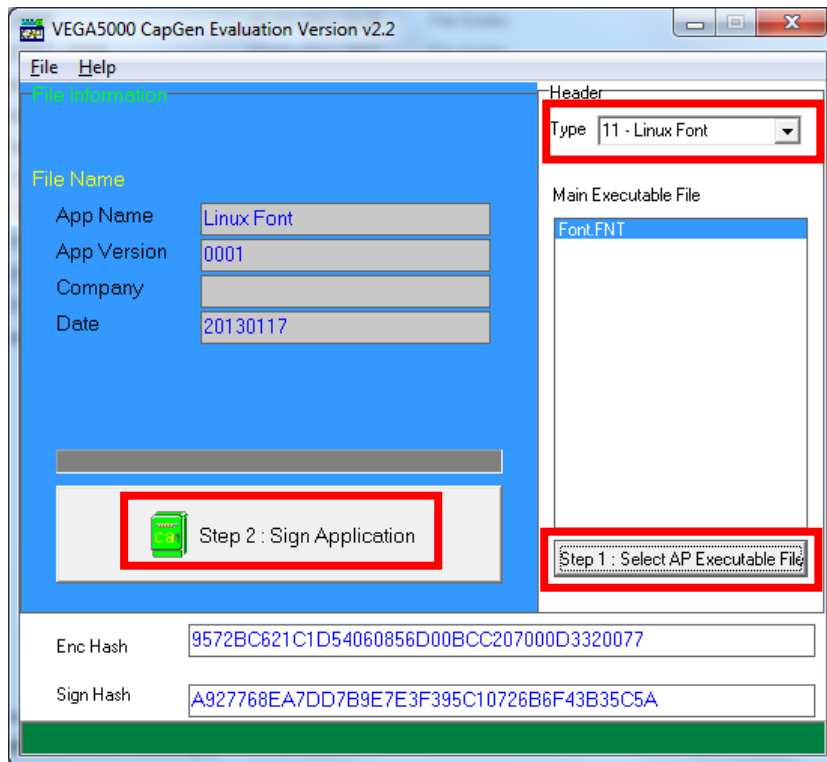


The image shows a window titled "FontManagerTool V1.04". It has a menu bar with "CreateFontData" and "FontManager". The main area is a large grid. At the bottom, there are three buttons: "Setting", "Create", and "Exit". The "Create" button is highlighted with a red rectangle.

- Select [Font Manager] tab and tick the newly created font, and press [Generate] button to export to FNT file.



- Use CAP Generator to convert the FNT file to CAP.
Set type to [11 – Linux Font], press [Step 1] button select the FNT file. Then press [Step 2] to generate CAP file.



- Download the font CAP file to terminal.
- In terminal application, add following code to display message using the newly created font.

```
CTOS_LanguageConfig(0xA000,d_FONT_12x24,0,d_FALSE);
CTOS_LanguageLCDSelectASCII(0xA000);
CTOS_LCDTPrintXY(1, 1, "ABCDEFGH");
```

Or print message using the newly created font.

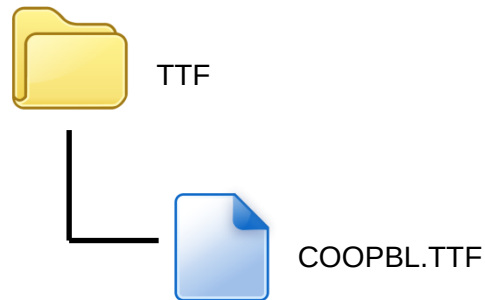
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

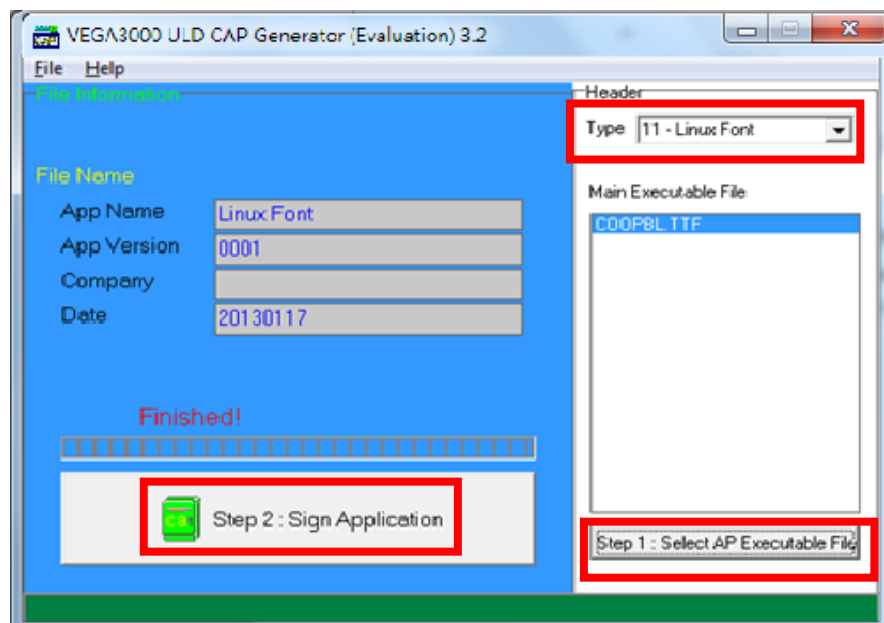
TrueType Font (TTF) is supported in MP200. You may download the TrueType font preferred to terminal for displaying or printing.

Following steps demonstrate how to use “Cooper Black” TrueType font.

- Copy the TTF file needed to a empty folder.



- Use CAP Generator to convert the TTF file to CAP.
Set type to [11 – Linux Font], press [Step 1] button select the TTF file.
Then press [Step 2] to generate CAP file.



- Download the font CAP file to terminal.

- In terminal application, add following code to display message using the newly added font.

```
CTOS_LCDTTFSelect("COOPBL.TTF", 0);  
CTOS_LCDFontSelectMode(d_FONT_TTF_MODE);  
CTOS_LCDTSelectFontSize(0x203C); // 32x60  
CTOS_LCDTClearDisplay();  
CTOS_LCDTPrintXY(1, 1, "Hello World");
```

Or print message using the newly added font.

```
CTOS_PrinterTTFSelect("COOPBL.TTF", 0);  
CTOS_PrinterFontSelectMode(d_FONT_TTF_MODE);  
CTOS_LanguagePrinterFontSize(0x203C, 0, 0); // 32x60  
CTOS_PrinterPutString("Hello World");
```

6. FCC Warning

Federal Communication Commission interference statement. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: -Reorient or relocate the receiving antenna. -Increase the separation between the equipment and receiver. -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. -Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference and
- (2) this device must accept any interference received, including interference that may cause undesired operation

RF Exposure Warning

The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device and its antenna(s) must not be co-located or operated in conjunction with any antenna or transmitter not described under this FCC ID, except in accordance with FCC multi-transmitter RF exposure procedures.

~ END ~