



CASTLES TECHNOLOGY

VEGA3000UltraLite

Book 2

User Manual

Confidential

Version1.1

Aug 2016

Castles Technology Co., Ltd.

6F, No. 207-5, 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

<i>Version</i>	<i>Date</i>	<i>Descriptions</i>
1.0	Jul 12, 2016	Initial creation.
1.1	Aug 11,2016	1. Add "2.2. Power Supply". 2. Add "2.3. Environment".

Contents

1. Introduction.....	6
2. Hardware Setup.....	7
2.1. Parts of the Surface	7
2.2. Power Supply.....	9
2.3. Environment.....	9
3. Basic Operation	10
3.1. Program Manager.....	10
3.2. Download AP	11
3.3. System Info.....	12
3.4. Memory Status	13
3.5. System Settings.....	14
3.6. Test Utility	17
3.7. Factory Reset	19
3.8. Power Off	20
3.9. Password Manager.....	21
3.10. Share Object Management	23
3.11. Font Mng	24
3.12. ULD Key Hash.....	25
3.13. Plug-in Mng	26
3.14. Key Injection	27
3.15. HW Detect	28
4. Secure File Loading.....	29
4.1. ULD Key System	29
4.1.1. ULD Manufacturer Key.....	29
4.1.2. ULD User Key	31
4.1.3. Key Change	31
4.2. File Signing.....	32
4.2.1. Signing Kernel Module	32
4.2.2. Signing User Files	34
4.3. File Loading.....	38
4.3.1. Download by User Loader.....	38
4.4. Changing ULD User Key.....	41
5. Font Management	48

5.1.	Loading New Font.....	48
5.2.	Custom Font.....	51
5.3.	Using TrueType Font (TTF)	59
6.	FCC Warning	61
	FCC Caution.....	61
	RF Exposure Warning.....	61
7.	NCCWarning.....	62

1. Introduction

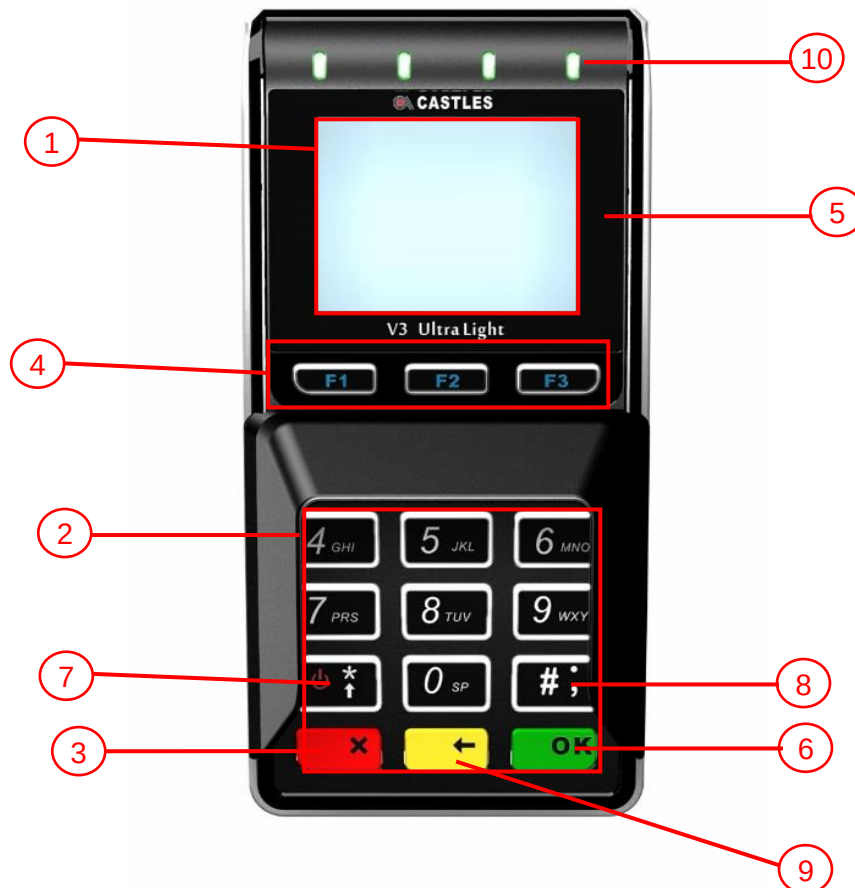
This document provides a guideline on operating and configuring Castles VEGA3000UltraLite.

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

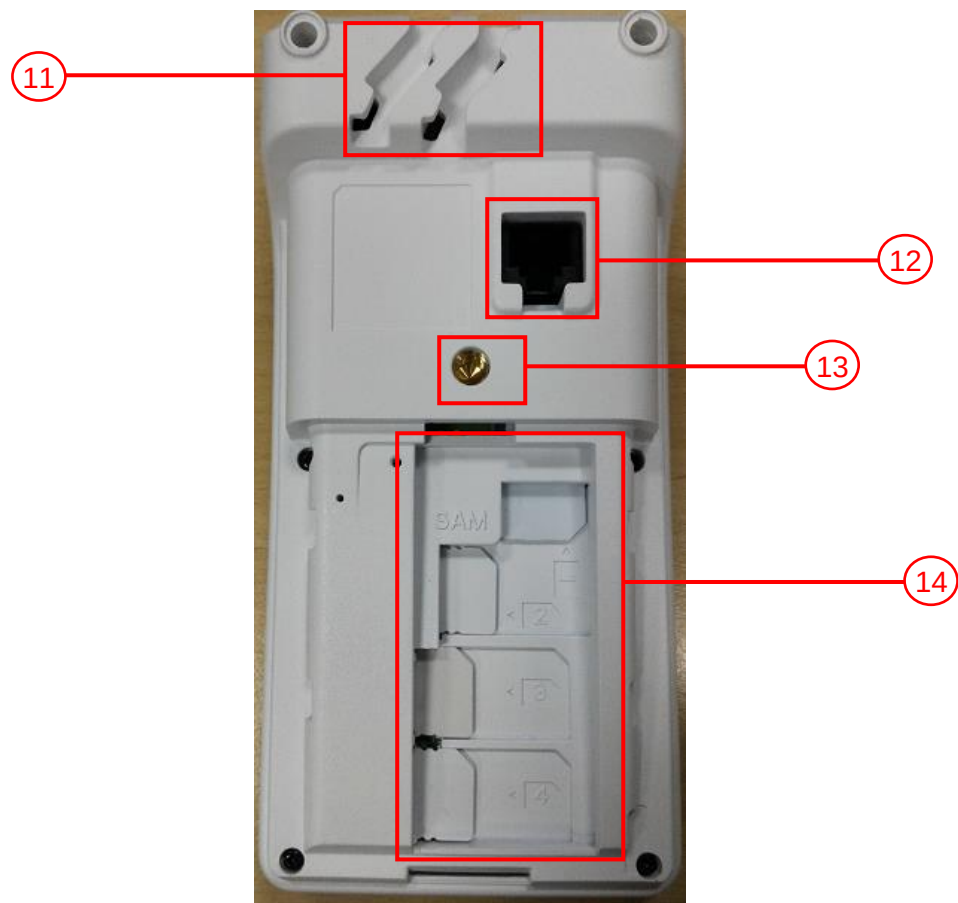
Front Side



VEGA3000 UltraLite

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

Rear Side



- 11. Wiring Slot
- 12. COM Port
- 13. Anti-theft Lock
- 14. SAM Slot (SAM1, SAM2, SAM3, SAM4)

Side



2.2. Power Supply

- DC Input: 9V/1A
- USB: 5V/1A

2.3. Environment

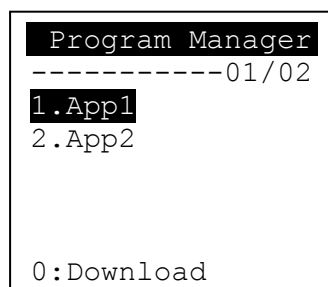
- Operating: 0°C~40°C, 5% to 90% non-condensing
- Storage: -20°C~70°C

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.

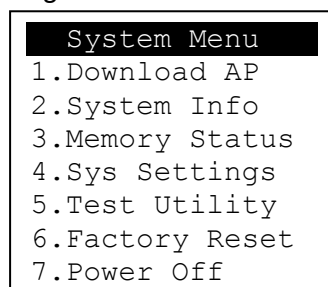
Program Manager



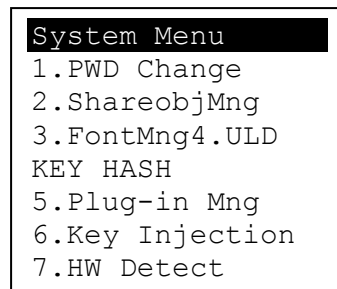
- Press[0] button to enter System Menu.
- Press [1] button to toggle default application selection.
- Press [2] button to delete application.
- Press [3] button to view application info.
- Press [OK] button to run application.
- Press [*] or [#] toup and down for applicationselection.

System Menu

Page 1



- Press [#] button to page 2.

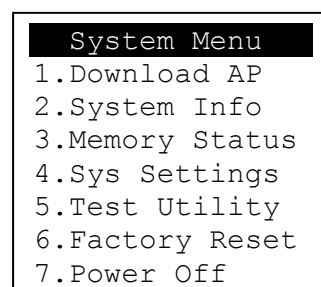


- Press [*] button to page1.
- Press [#] button to page3.

3.2. Download AP

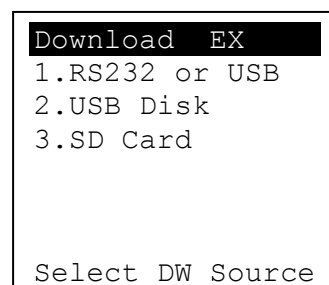
Download user application or kernel modules firmware.

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
PEDST     :VR0025

```

Page 2

```

SYSTEM INFO
--- KOver ---
SECURITY:VR0025
KMS      :VR0024
DRV:VR0039
USB:N/A
CIF:VR9020
SAM      :VR9131

```

Page 3

```

SYSTEM INFO
--- KOver2 ---
CL:VR0018
SC      :VR0011

```

- Press [#] button to next page.

Page 4

```

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

```

Page 5

```

SYSTEM INFO
--- SO Ver2 ---
PRT:VR0020
RTC      :VR0013
ULDPM    :VR0022
PPPMODEM: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 Page9

```

SYSTEM INFO
--- HWMVer ---
CRDL/ETHE:ONCHIP
CLM-MP   : N/A
--- APVer ---
ULDPM    :VR0026

```

Page 10

```

SYSTEM INFO
HUSBID:0CA6A050
CUSBID:N/A
--Factory S/N---
FFFFFFFFFFFFFFFF
CAEMVL2      :VR91
13
CAEMVL2AP    :VR00

```

```

SYSTEM INFO
--EXT SO Ver P.1--
CACLMDL      :VR0007
CACLENTY     :VR0007
CAMPP        :VR0006
CAVPW        :VR0018
CAAEP        :VR0004
CAJCT        :VR9407

```

```
SYSTEM INFO
--EXT SO Ver P.1--
CAVAP:VR0002
CACQP:VR6601
CAIFH      :VR0002
CAEMVL2    :VRA016
CAEMVL2AP  :VR0009
```

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 :52404KB

--SDRAM Memory--
Total: 65408KB
Used :38004KB
```

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, F1, F2, F3) 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>
BATThreshld	Battery charging threshold value. [Portable model only]
Null Cradle	Enable (Y) if base is Type Acradle. [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 OffLCDBacklight
Bklit Off Time	Thresholdof Auto Off LCD Backlight
PWR KEY OFF	Powerkeyfunction, power off (Y) or reboot(N)
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.
Auto Reboot	Terminal will reboot in specific time every day.
Reboot Hour	The specific hour of day for Auto Reboot.
Reboot Min	The specific minute of day for Auto Reboot.

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 *Page 2*

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

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: Prev2: Next

Page 3

SYS SETTINGS
Debug Mode: N
Debug Port : X
Mobil AutoON: N
Bklit Auto Off : N
BklitOff Time : X
PWR KEY OFF :N
1: Prev2: Next

Page 4

SYS SETTINGS
RTC Time Zon:GMT
NTP Enable:N
NTP Update F:X
1: Prev2: Next

SYS SETTINGS	
BT DIRECT ACCESS	:X
Halt Timeout	:999
PWM Auto	:N
PWM Mode	: X
PWM Time	
1: Prev2: Next	

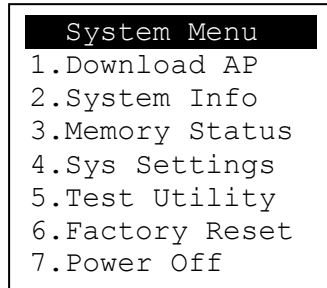
SYS SETTINGS	
Auto Reboot	:Y
Reboot Hour	:00
Reboot Min	:00
1: Prev Page	

- 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.

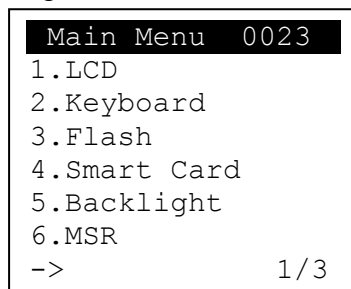
System Menu



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

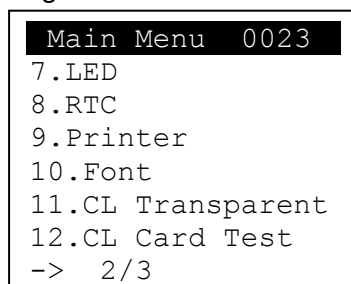
Test Utility Menu

Page 1



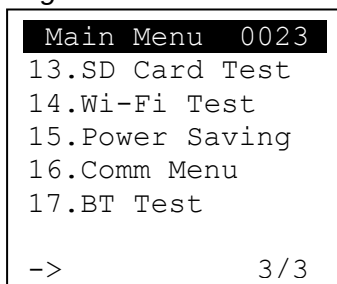
- Press [1] and [OK] to diagnose LCD.
- Press [2] and [OK] to diagnose keyboard.
- Press [3] and [OK] to diagnose flash memory.
- Press [4] and [OK] to diagnose smart card module.
- Press [5] and [OK] to diagnose backlight.
- Press [6] and [OK] to diagnose magnetic stripe card reader.
- Press [#] button to page 2.

Page 2



- Press [7] and [OK] to diagnose LED.
- Press [8] and [OK] to diagnose RTC.
- Press [9] and [OK] to check Printer.
- Press [10] and [OK] to check FONT file in VEGA3000 UltraLite.
- Press [11] and [OK] to check CL transparent.
- Press [12] and [OK] to test Contactless Card.
- Press [*] button to page 1.
- Press [#] button to page 3.

Page 2

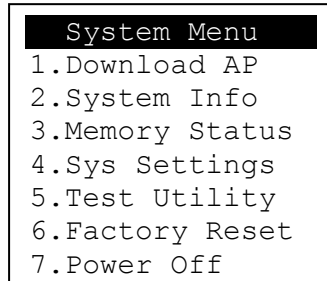


- Press [13] and [OK] to execute SD Card Test.
- Press [14] and [OK] to test functionality of WiFi.
- Press [15] and [OK] to test functionality of power saving.
- Press [16] and [OK] to test functionality of multiple communication ways.
- Press [17] and [OK] to test functionality of Bluetooth.
- Press [*] button to page 2.

3.7. Factory Reset

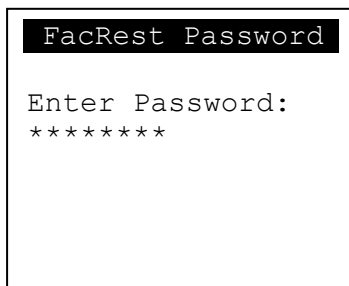
Perform factory reset, all user application, fonts and data will be deleted.

System Menu



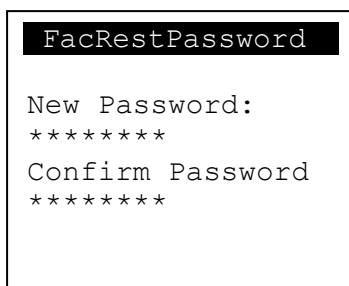
A screenshot of the 'System Menu' screen. It has a black header bar with the text 'System Menu' in white. Below the header, there is a list of seven menu items: '1.Download AP', '2.System Info', '3.Memory Status', '4.Sys Settings', '5.Test Utility', '6.Factory Reset', and '7.Power Off'.

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



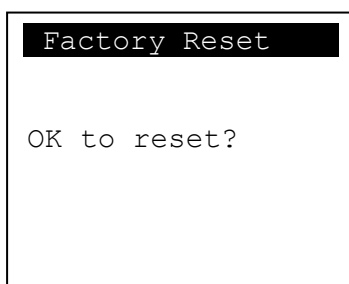
A screenshot of the 'FacRest Password' screen. It has a black header bar with the text 'FacRest Password' in white. Below the header, the text 'Enter Password:' is displayed, followed by a line of eight asterisks '*****' for password input.

- Enter password and press [OK].
- Enter factory reset password. (**Default password: 12345678**)



A screenshot of the 'FacRestPassword' screen. It has a black header bar with the text 'FacRestPassword' in white. Below the header, the text 'New Password:' is displayed, followed by a line of eight asterisks '*****'. Below that, the text 'Confirm Password' is displayed, followed by another line of eight asterisks '*****'.

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



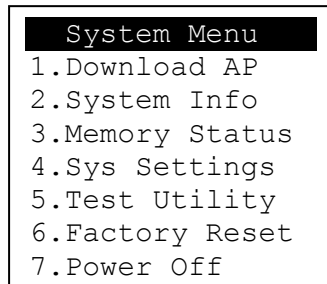
A screenshot of the 'Factory Reset' screen. It has a black header bar with the text 'Factory Reset' in white. Below the header, the text 'OK to reset?' is displayed.

- Press [OK] to execute the Factory Reset.

3.8. Power Off

Power off terminal.

System Menu

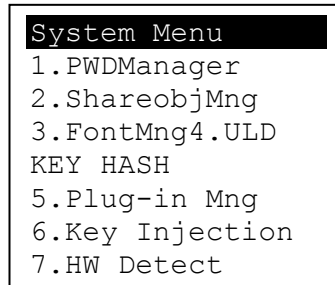


- Press [7] button to power off terminal.

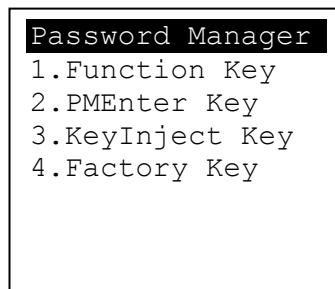
3.9. Password Manager

Change the keys in Password Manager.

System Menu (Page 2)



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



- Press [1] button to change Function Key password.
- Press [2] button to change Program Manager Key password.
- Press [3] button to change Key Injection Key password.
- Press [4] button to change Factory Reset Key password.

Please refer to the procedure of change Function Key password as below.



- Enter current password. (**Default password is "84188062"**)

FunKey Password

New Password:

Confirm Password

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

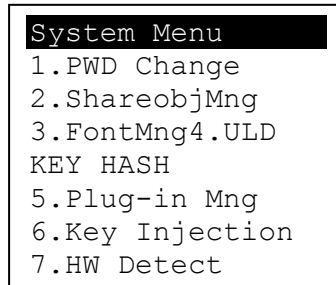
User must have to change the Default key to user own key at the first time.
The Default Key Value in Password Manager is as below:

Function Key	84188062
PMEnter Key	NA
KeyInject Key	87654321
Factory Key	12345678

3.10.Share Object Management

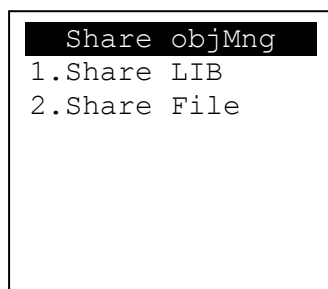
View share object in terminal.

System Menu (Page 2)



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

Share Object Management Menu

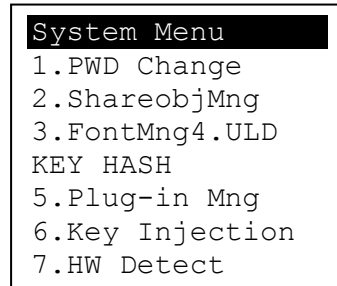


- Press [1] button to view shared library.
- Press [2] button to view shared file.

3.11.Font Mng

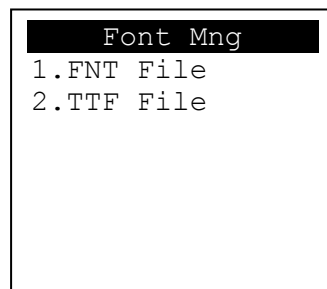
View Font Management.

System Menu (Page 2)



- Press [3] button to view Font Management.

FontManagment

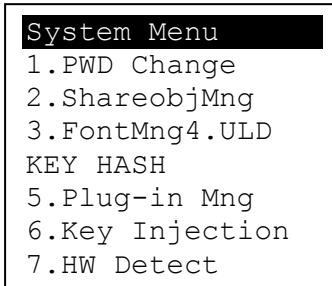


- Press [1] button to view FNT Font list.
- Press [2] button to view TTF Font list.

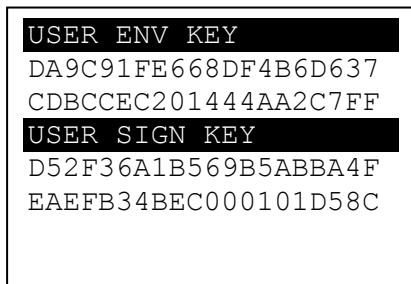
3.12.ULD Key Hash

View ULD user key hash value.

System Menu (Page 2)



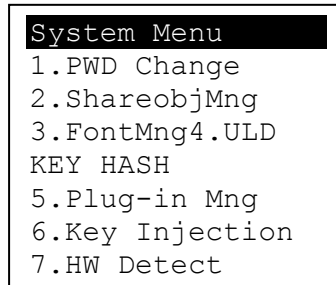
- Press [4] button to view hash value.



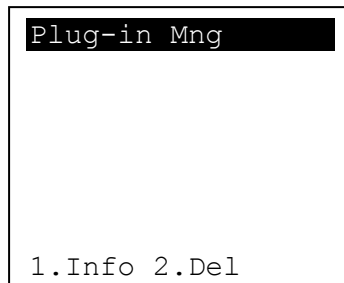
3.13.Plug-in Mng

View Plug-in Management.

System Menu (Page 2)



- Press [5] button to view Plug-in Management.

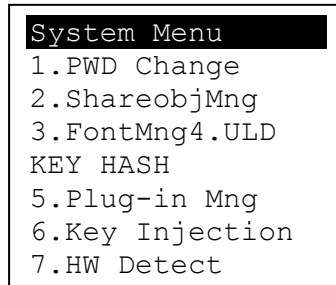


- Press [*]or[#]button to select item.
- Press [1]button to get item information.
- Press [2]button to delete item.

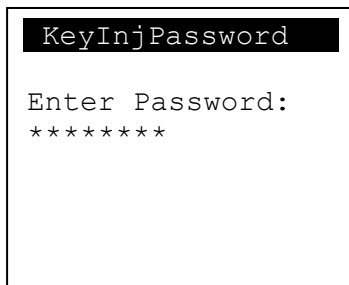
3.14.Key Injection

View Key Injection.

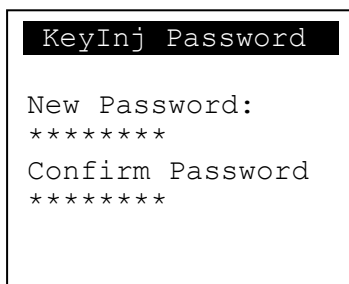
System Menu (Page 2)



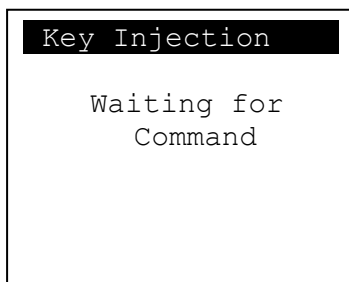
- Press [6] button to view Key Injection.



- Enter password and press [OK].
- Enter Key Injection password.(**Default password: 87654321**)



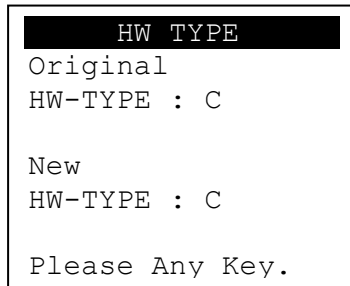
- Enter new password.
- Enter new password again to confirm.



- Please refer to document of Key Injection which is released by Castles Technology.

3.15.HW Detect

View Key Injection.



- Press any key to go back to Program Manager.

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 VEGA3000 UltraLite, the RSA key length is 2048bits.

4.1.1. ULD Manufacturer Key

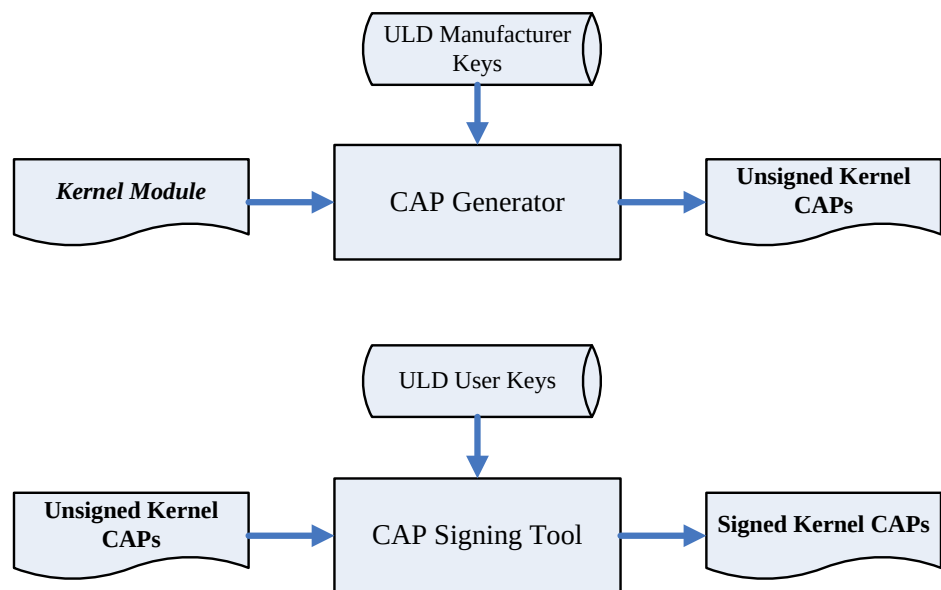
The system consists of several kernel modules. These kernel modules are provided by the Manufacturer, and released in CAP format file with encryption and signing via ULD Manufacturer Keys.

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:

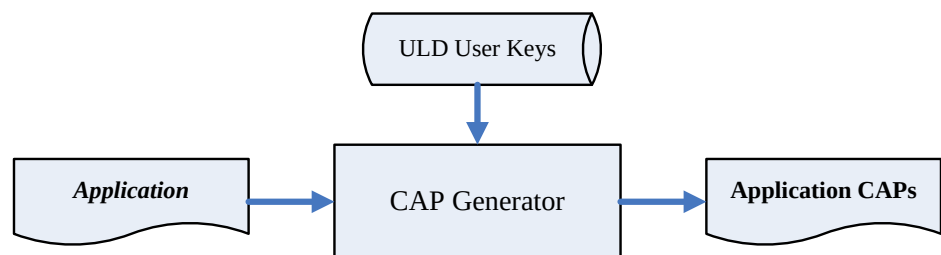
1. The kernel modules are encrypted by a random-generated 3DES key, which is retrieved from the Key Encryption Block of the CAP by ULD Manufacturer Key Encryption Key, not directly encrypted by ULD RSA Key.
2. The “sign” action via ULD User Keys actually is done by” the second encryption”. “The second 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

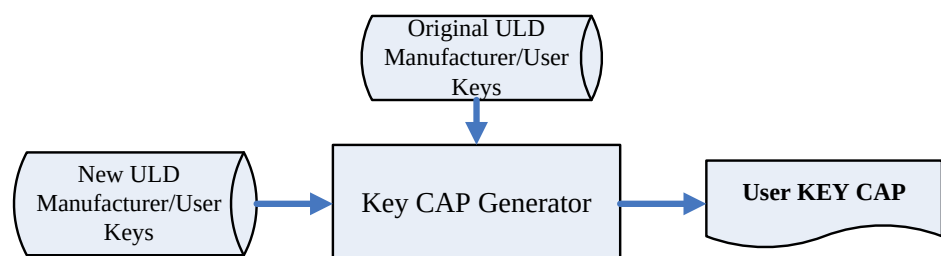
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the “signed” action via ULD User Keys.

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

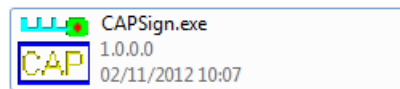
Castles will release new version of kernel module in “unsigned” form. This files required to sign with ULD User Key before it can load to terminal.

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

The CAP Signing Tool is located at:

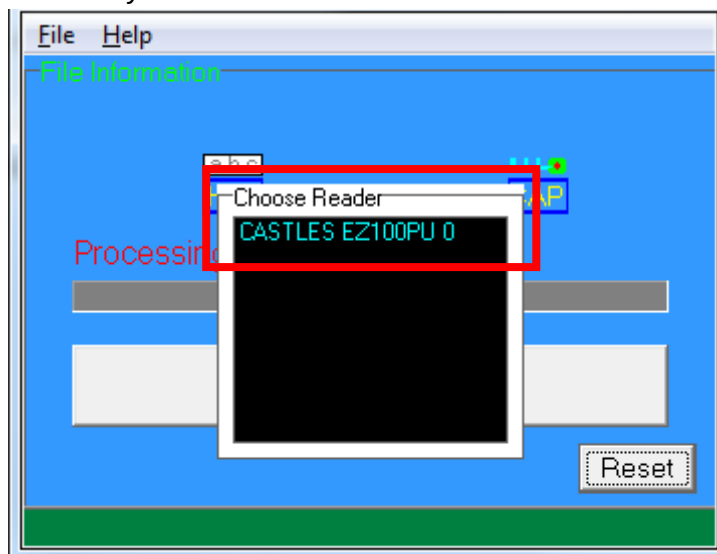
C:\Program Files\Castles\VEGA3000UL\tools\Signing Tool

- Run CAP Signing Tool

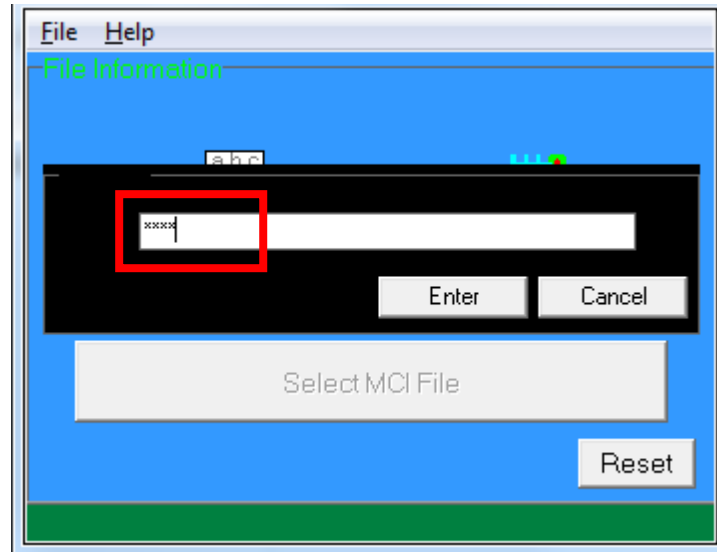


(VEGA3000 UltraLite)

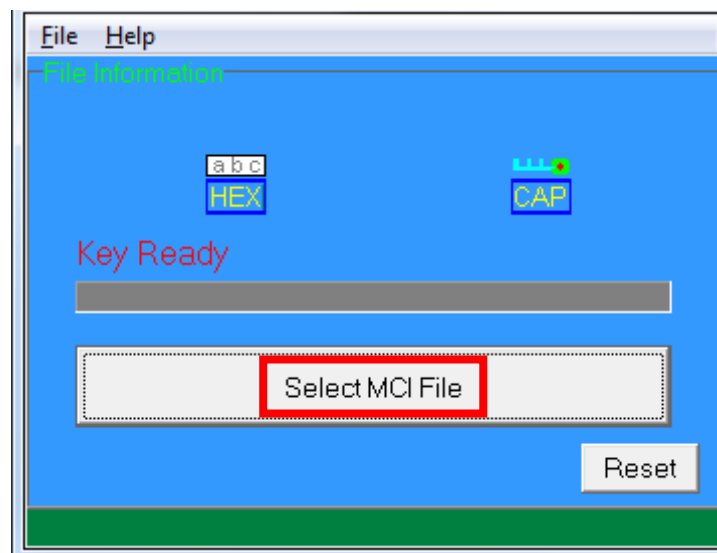
- Insert Key Card and select smart card reader



- 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.

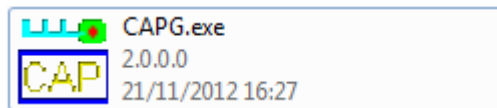
- User application
- User application data files
- User application library
- Font file
- Share library
- Share files
- System setting
- Key CAP (Manufacturer ULD Key Set)

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

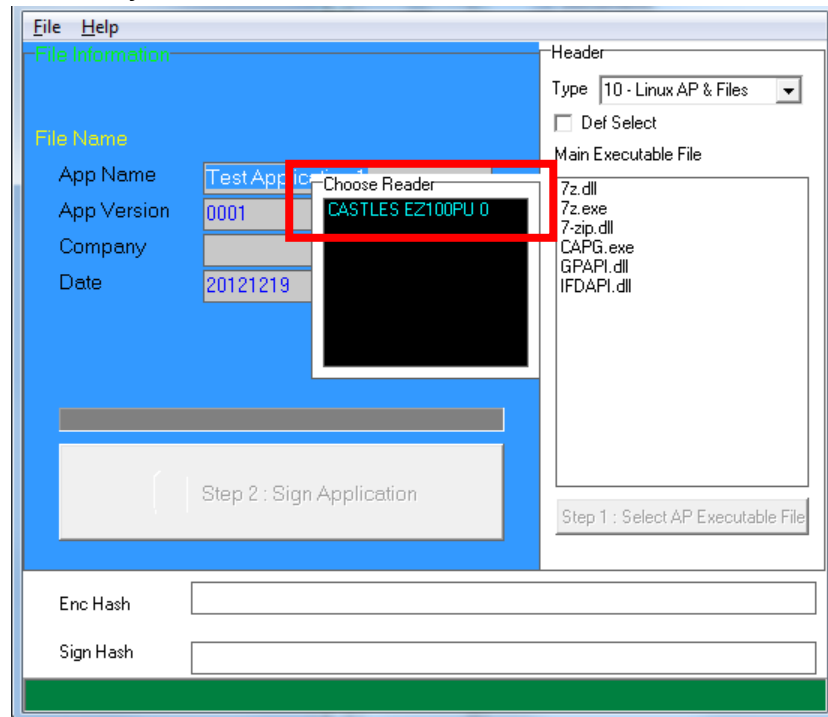
The CAP Generator is located at:

C:\Program Files\Castles\VEGA3000UL\tools\CAPG (KeyCard)

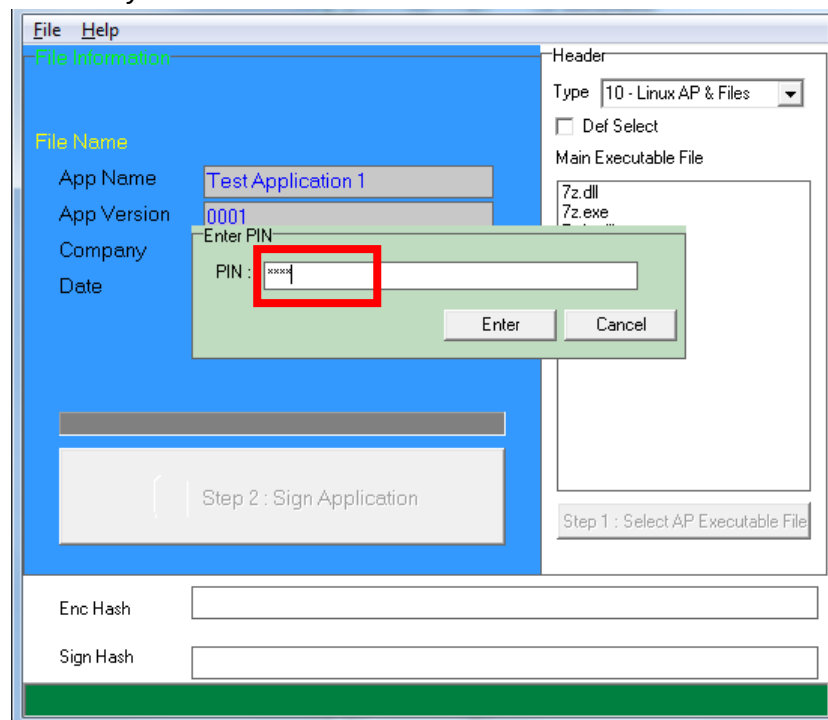
- Run CAP Generator



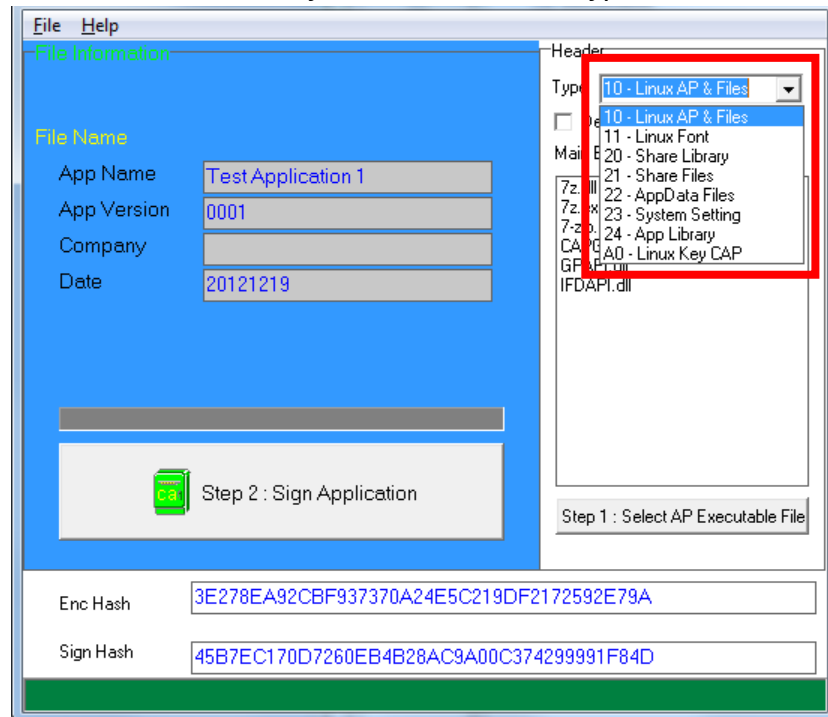
- Insert Key Card and select smart card reader



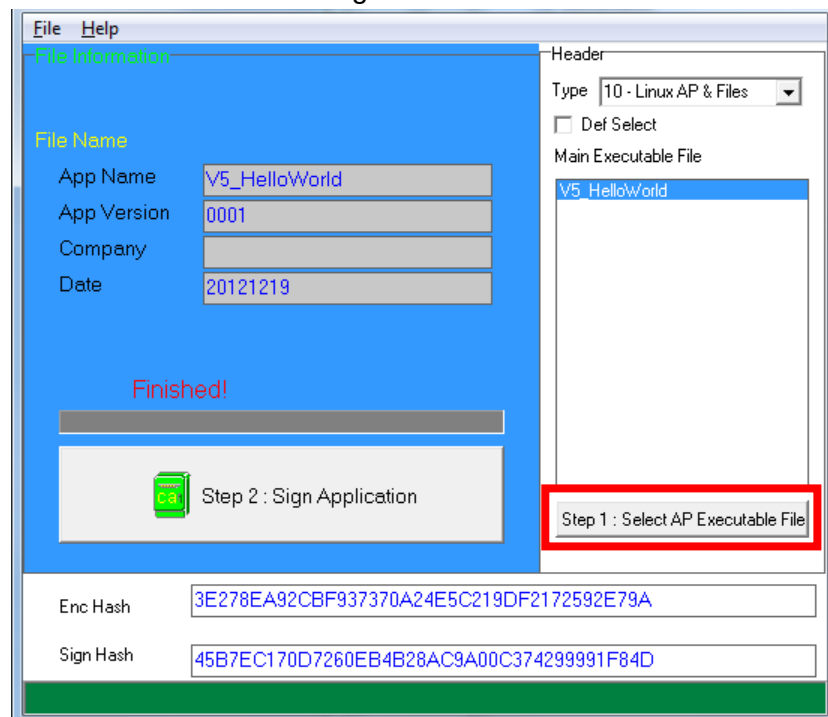
- Enter Key Card PIN



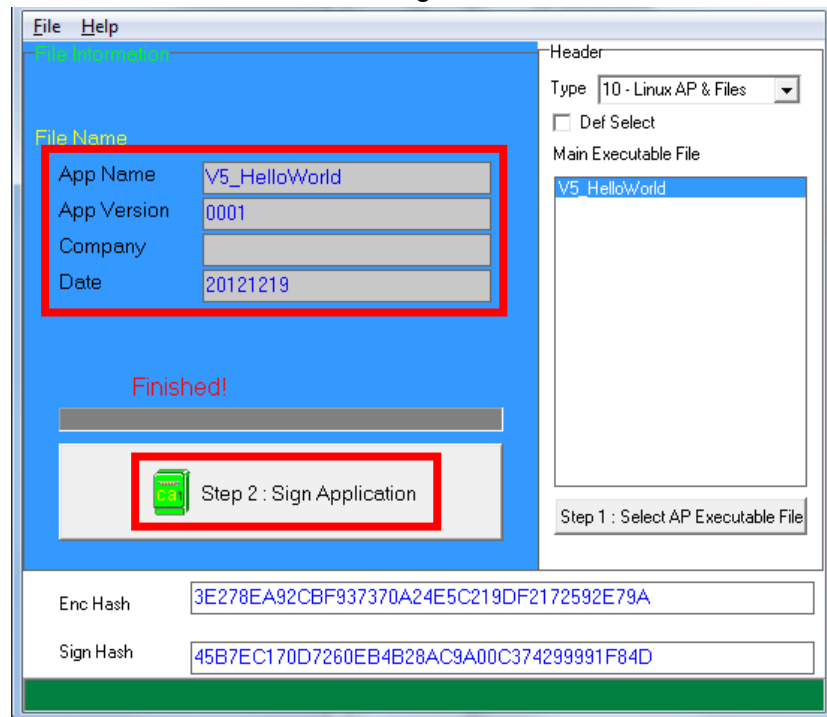
- CAP Generator is ready, select the correct Type from the list.



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



- 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 VEGA3000 UltraLite.

- 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.

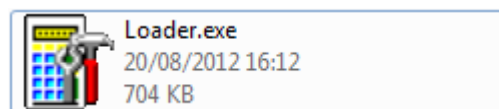
4.3.1. Download by User Loader

The User Loader works for VEGA3000 UltraLite.

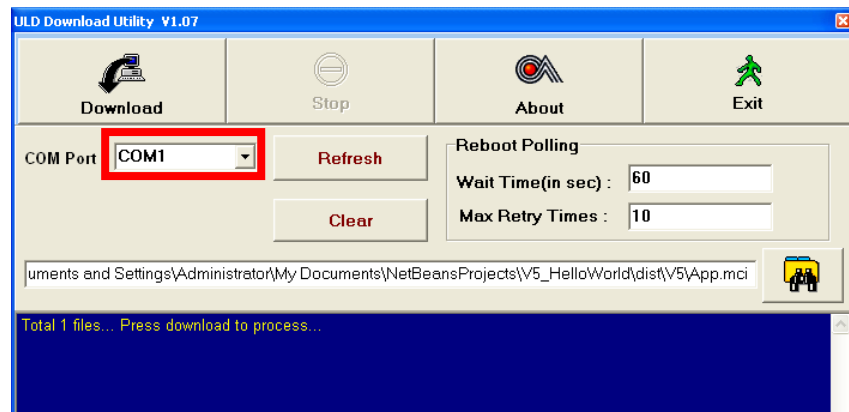
The Loader is located at:

C:\Program Files\Castles\VEGA3000UL\tools\Loader

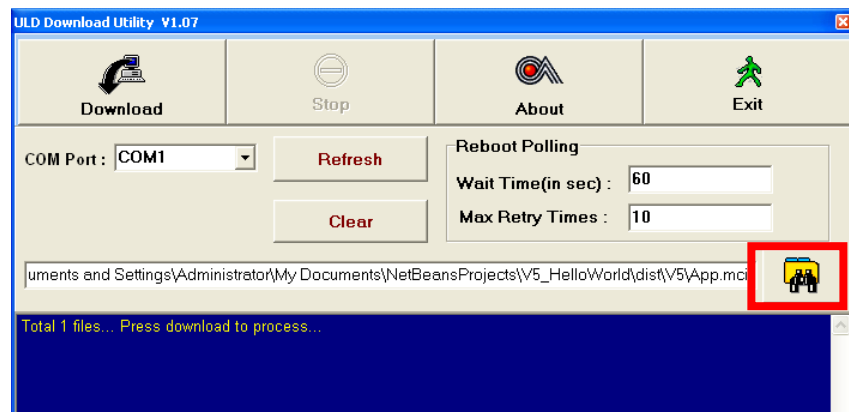
- Run User Loader



- Select COM port

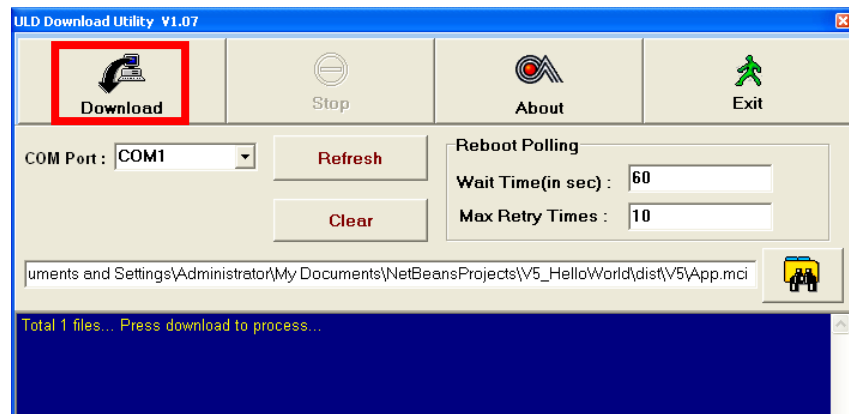


- Browse and select mci file or mmci file

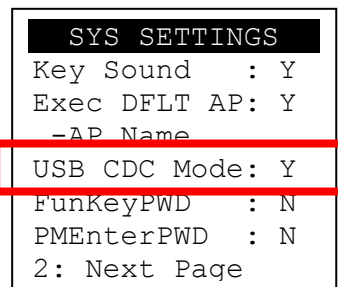


- Setup terminal to enter download mode
 - Press [0] button in Program Manager (PM)
 - Press [1] button to select “1. Download AP“
 - Press [1] button again to select download via RS232 or USB

- Press “Download” button to start.



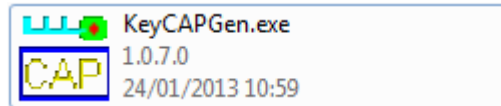
*Note: To download using USB cable, terminal must enable CDC mode.
Set USB CDC Mode to Y.*



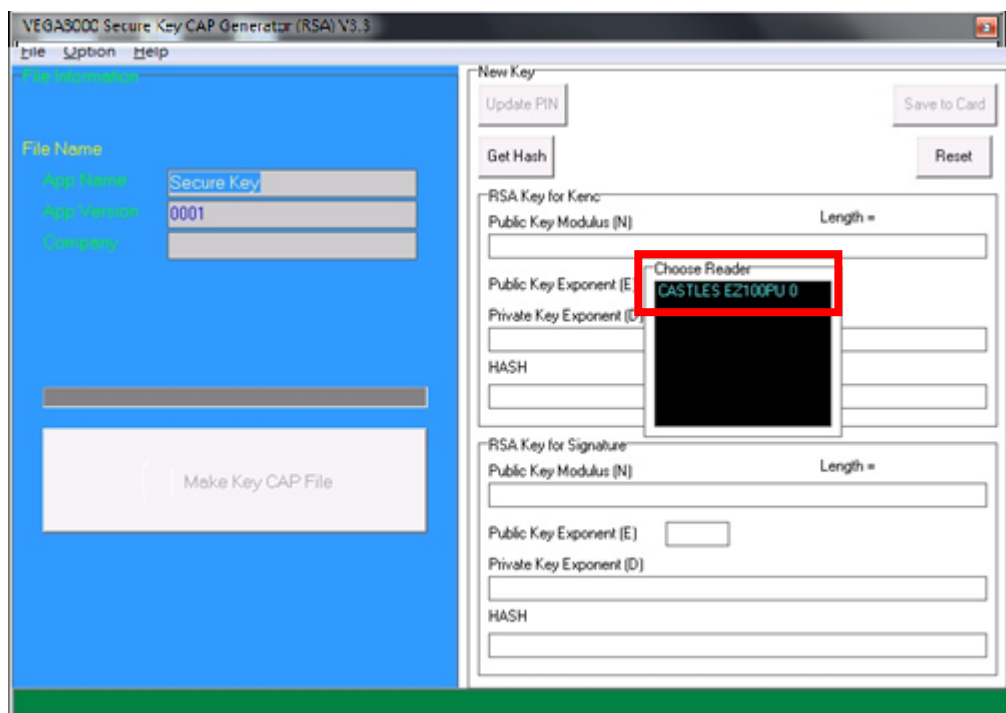
4.4. Changing ULD User Key

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.

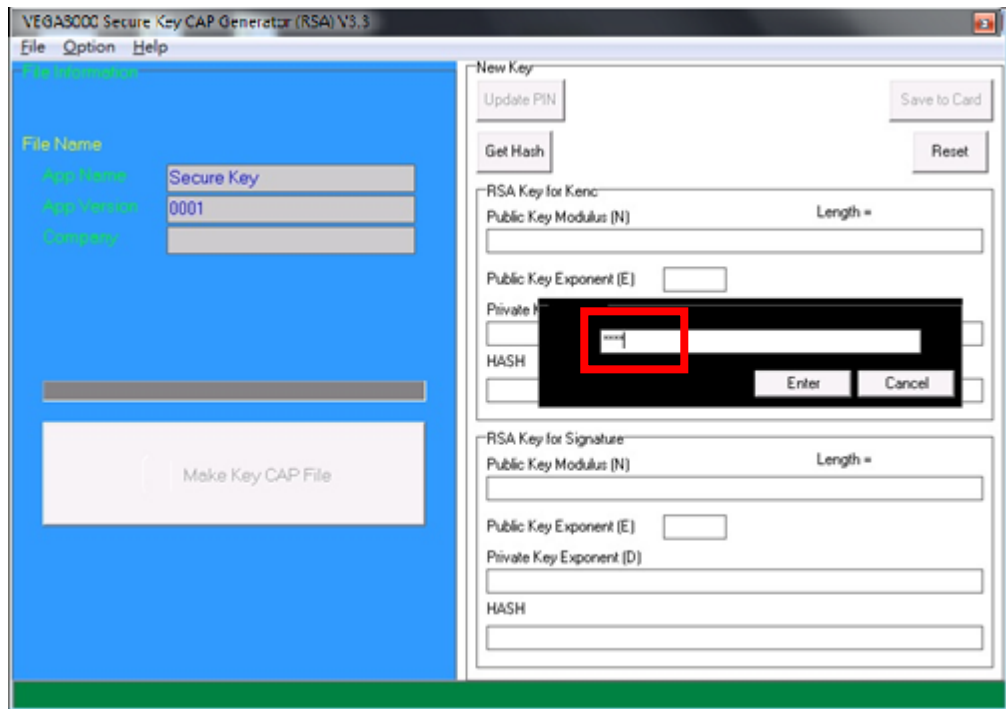
- Run Secure Key Generator



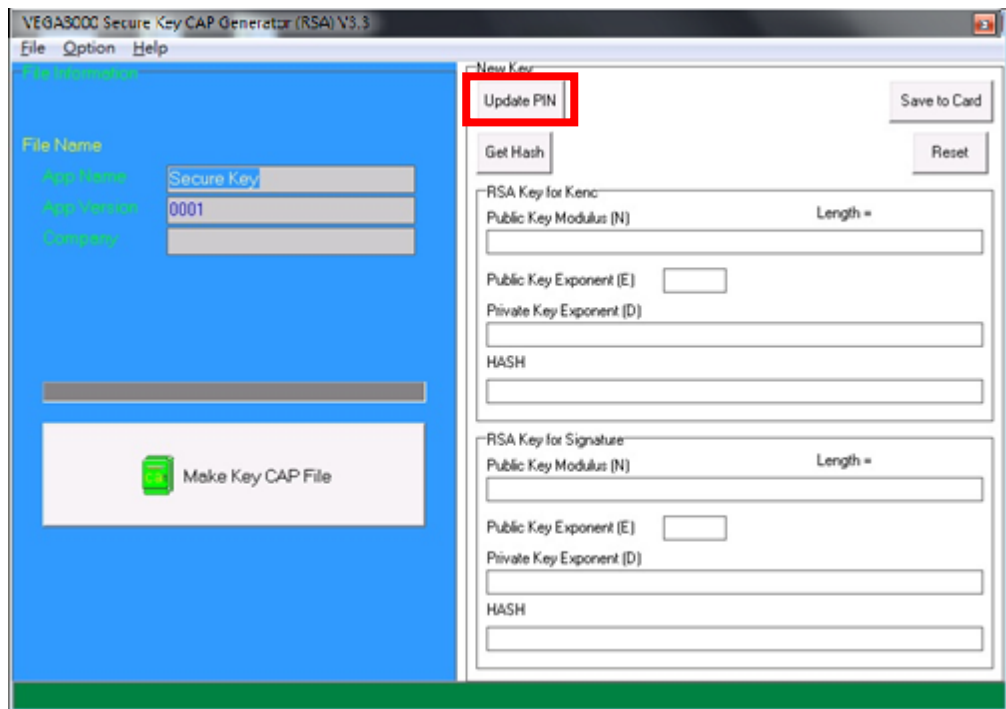
- Insert Key Card and select smart card reader



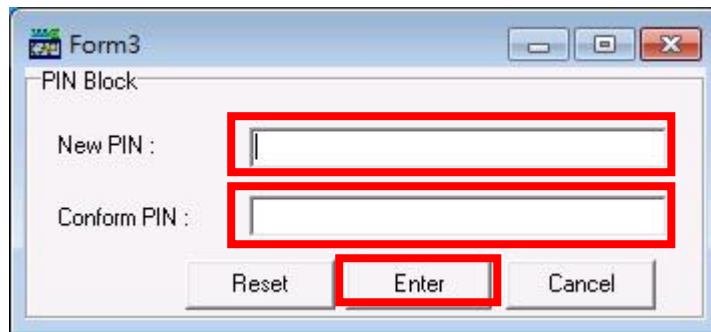
- Enter Key Card PIN, default PIN is “1234”.



- 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

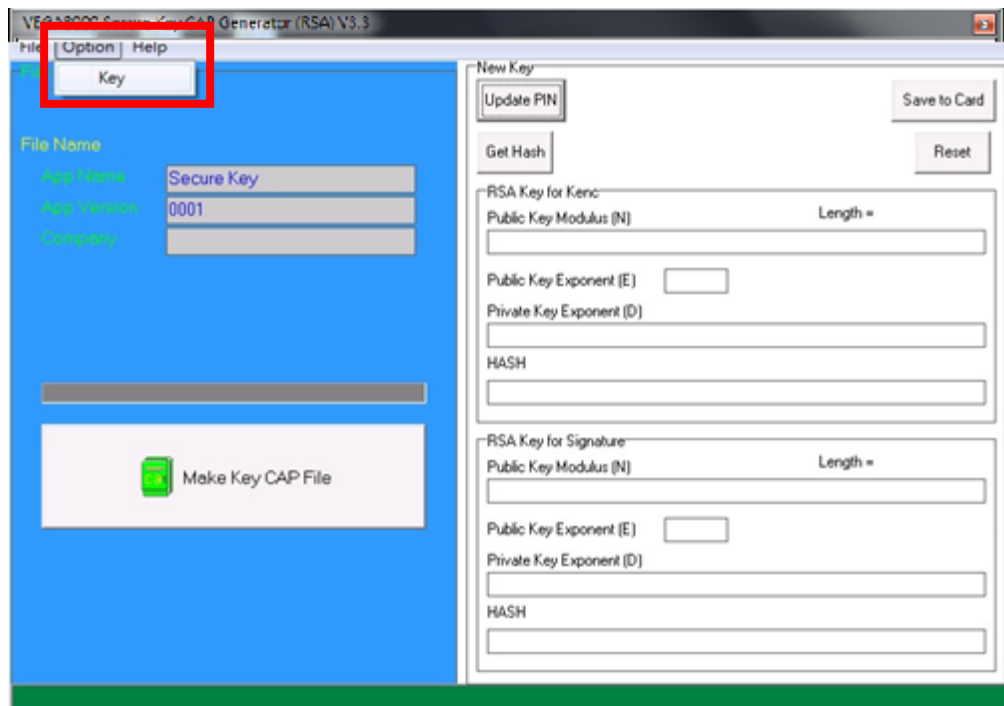
PIN Block

New PIN :

Conform PIN :

Reset Enter Cancel

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



VEEVA-0000-0000 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

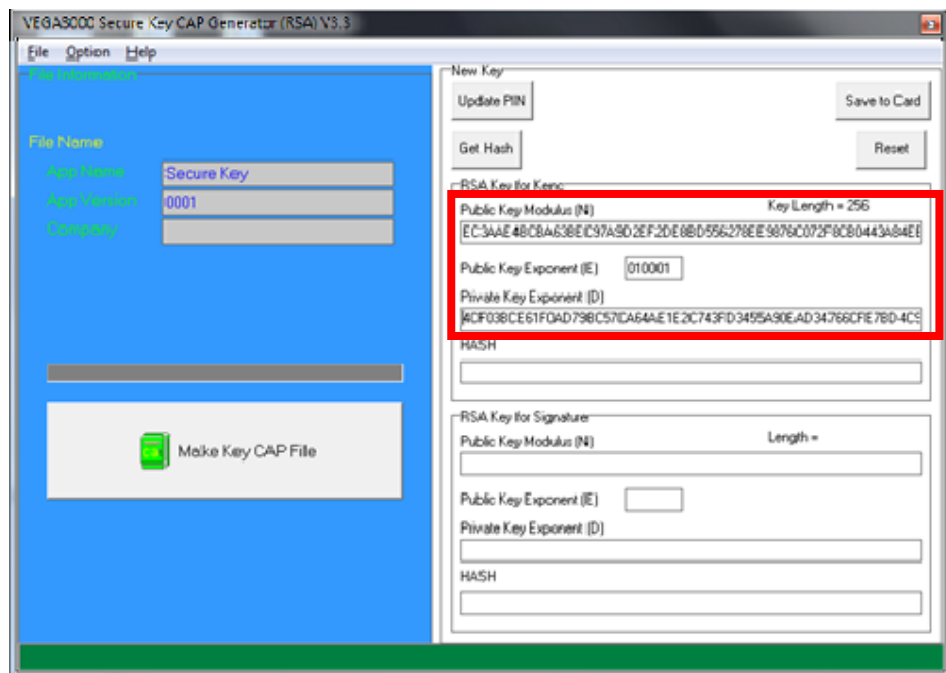
RSA Key for Signature

Public Key Modulus (N) Length =

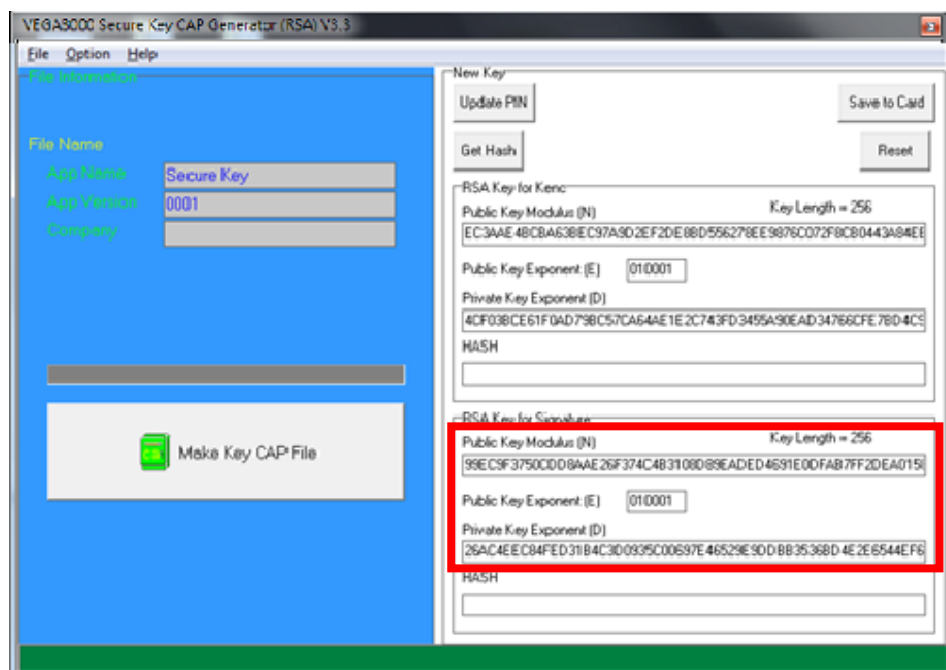
Public Key Exponent (E)

Private Key Exponent (D)

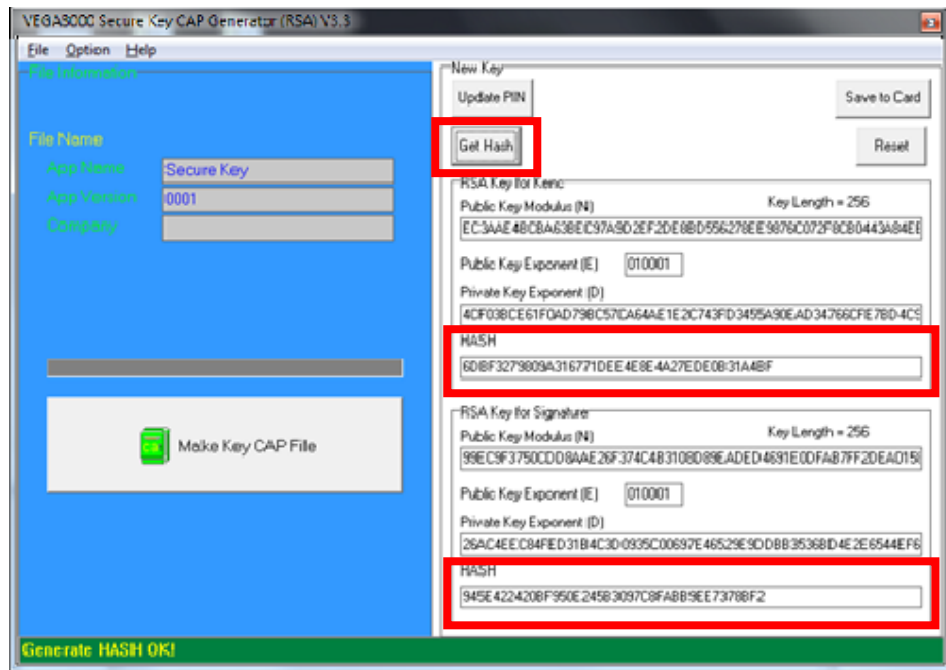
HASH



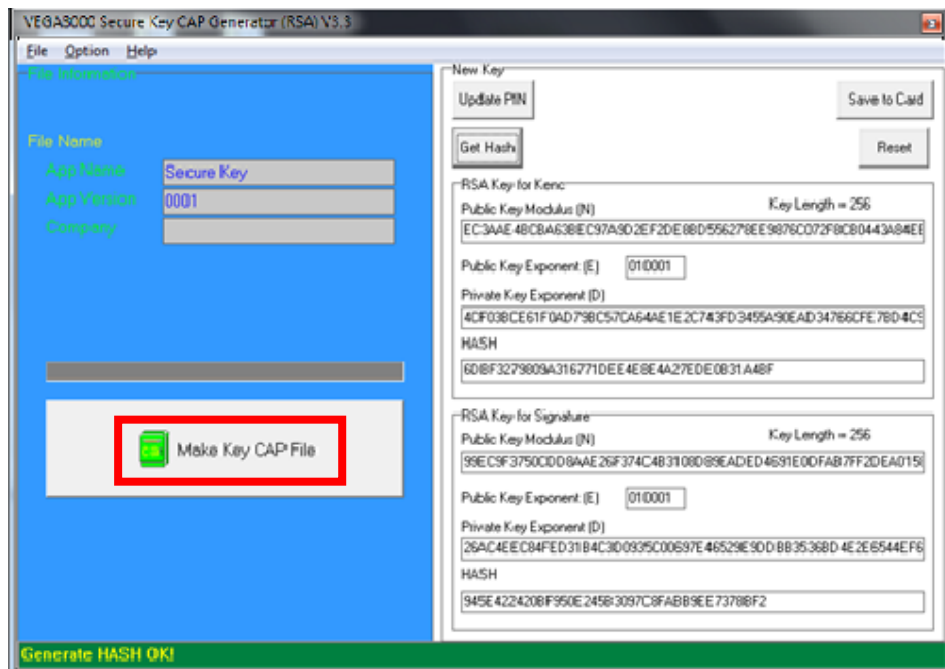
- Generate second RSA key set for Signature.



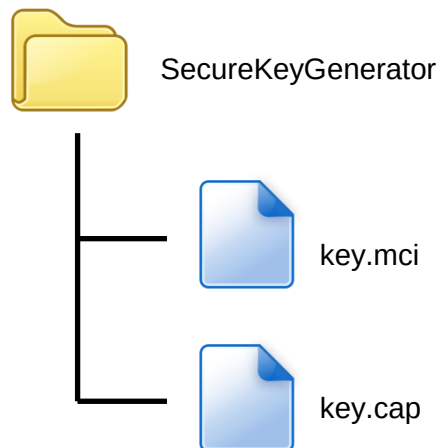
- Click [Get Hash] button to calculate the hash value for key sets.



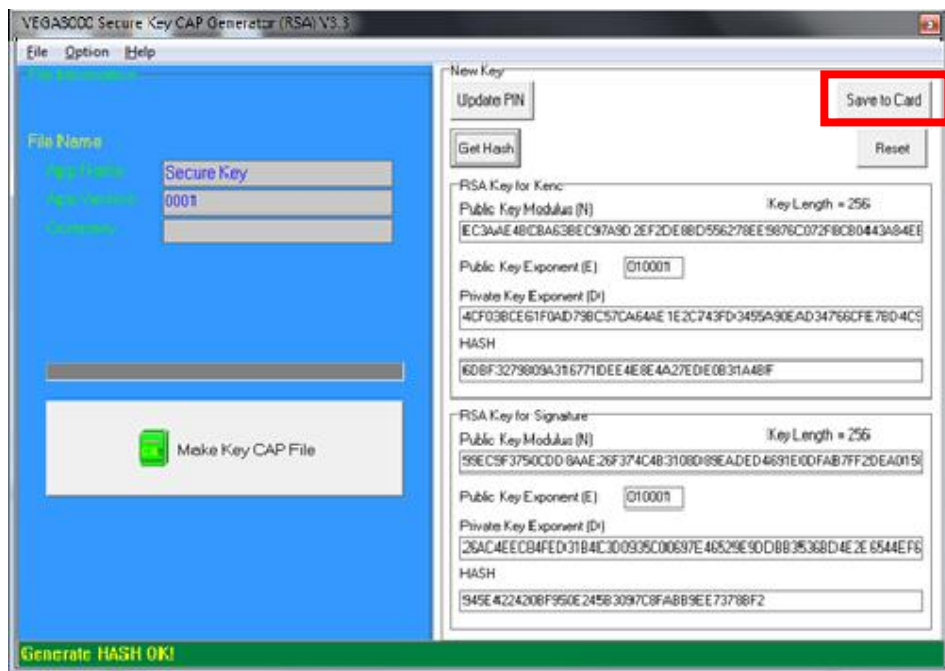
- Please copy down all the values into a text file and keep in a safe place. You will need this if you need to create duplicate Key Card.
- To generate the key CAP for the newly generated user key set, press [Make Key CAP File] button.



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



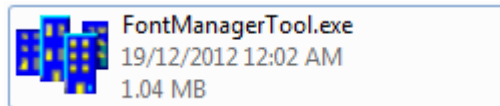
- To update the newly generated key set to Key Card, press [Save to Card] button to write the key set to Key Card.



5. Font Management

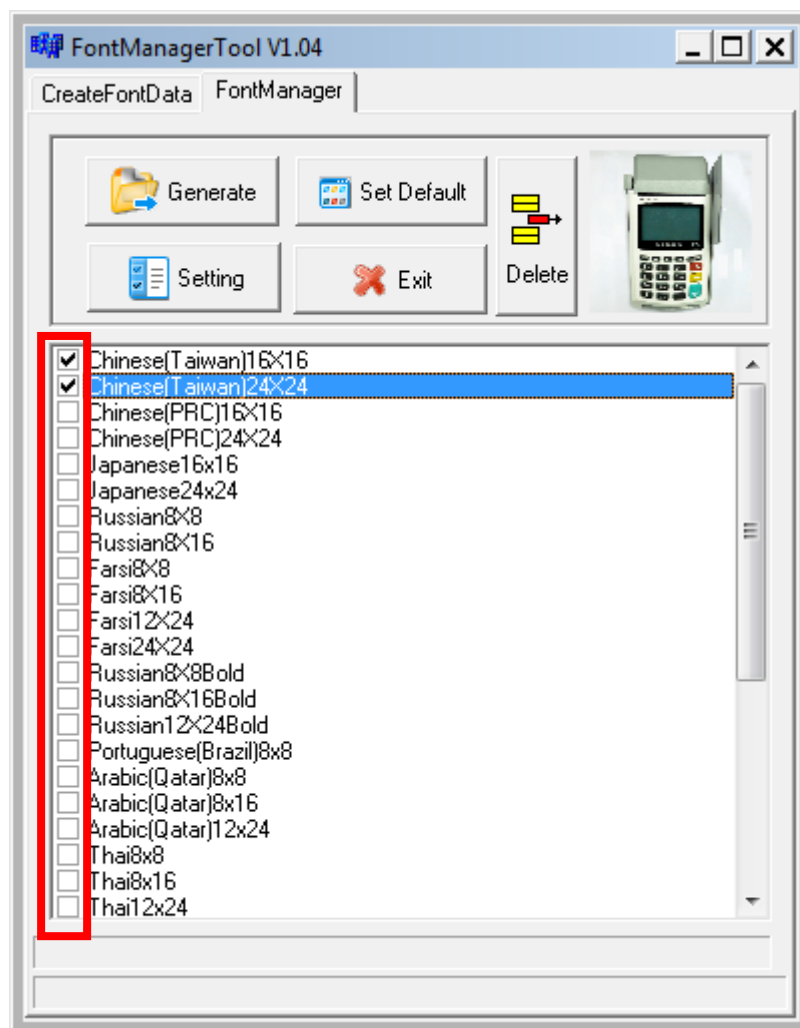
5.1. Loading New Font

- Run FontManager.exe

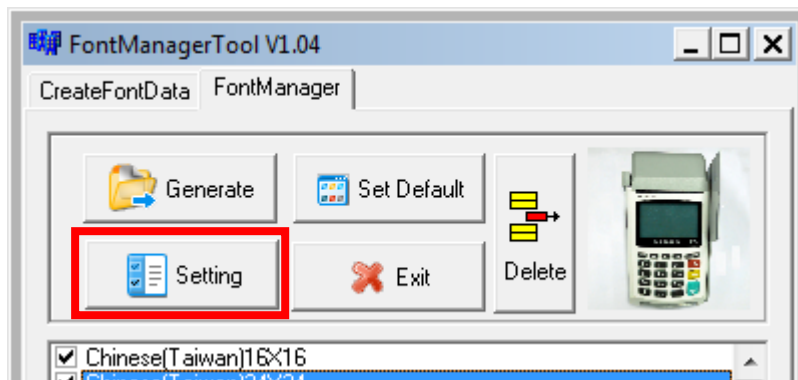


Located at C:\Program Files\Castles\Font Manager

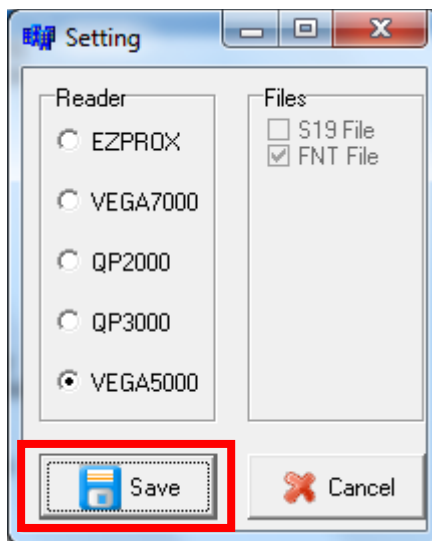
- Select font to download



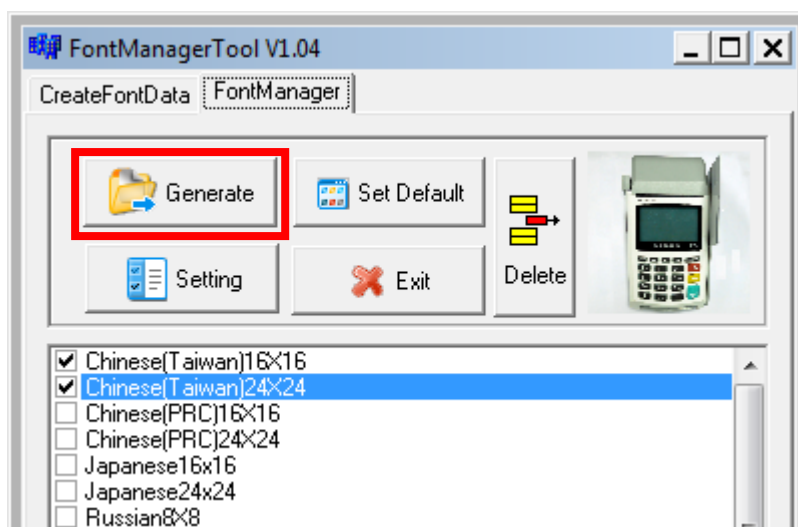
- Press [Setting] button to configure terminal type.



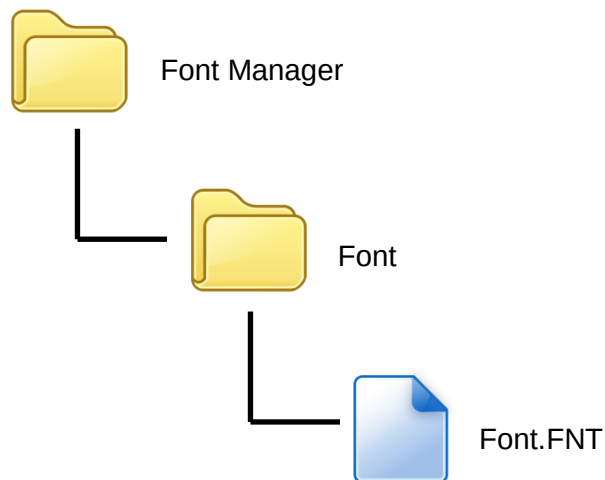
- Select **VEGA5000**, press [Save] button to save and return font manager.



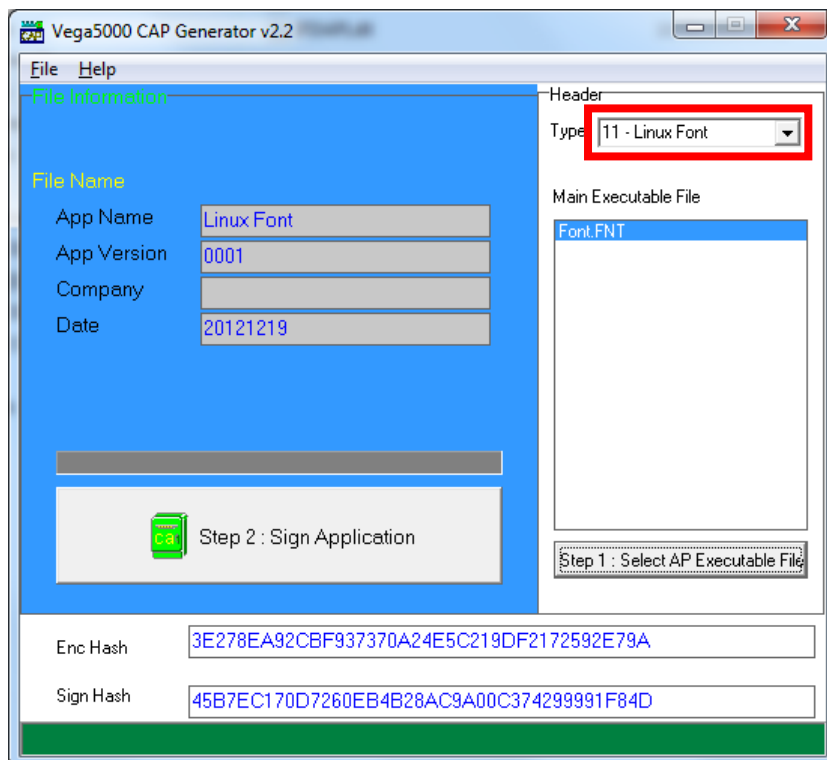
- Press [Generate] to create the font file.



- 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.

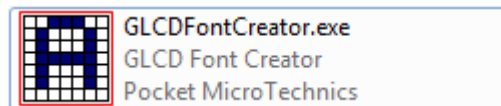
There are two zone defined:

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

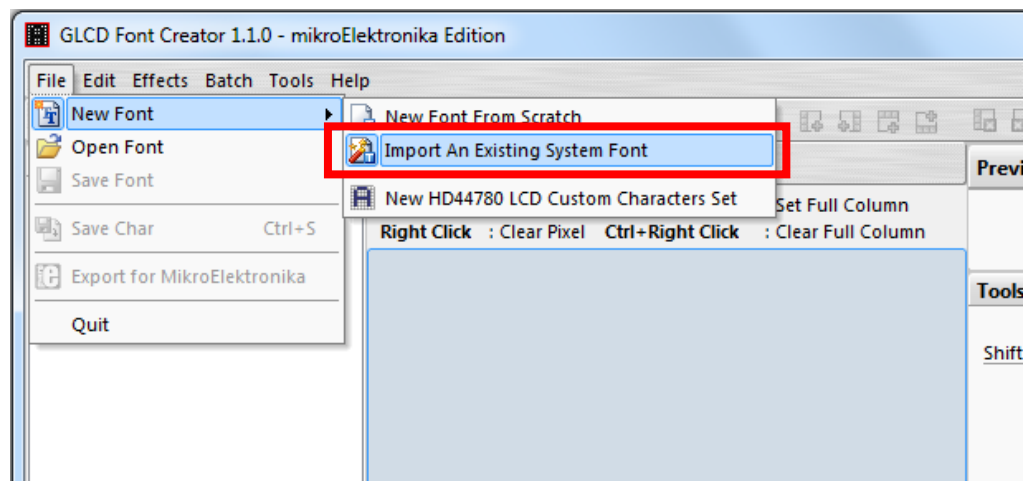
Zone 0x80 ~ 0xFF – Free to use, you may use for symbols.

Following steps demonstrate how to create a 12x24 font.

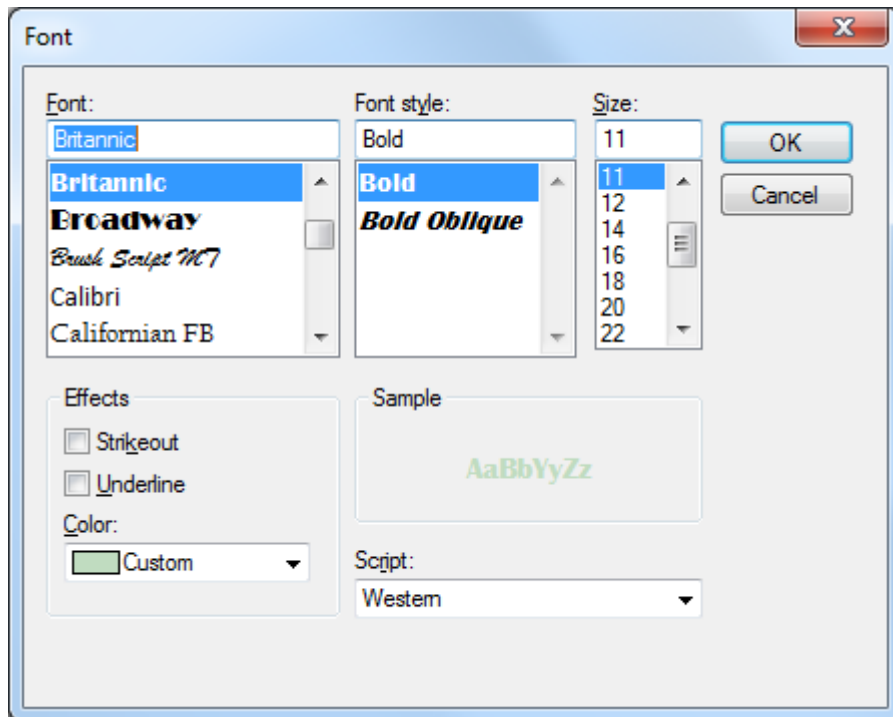
- Run GLCD Font Creator



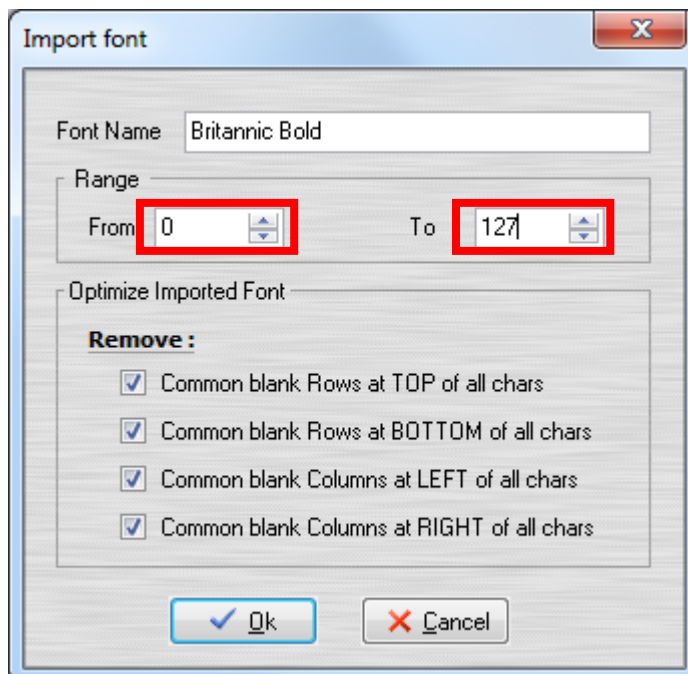
- Select [File] ⇒ [New Font] ⇒ [Import An Existing System Font]



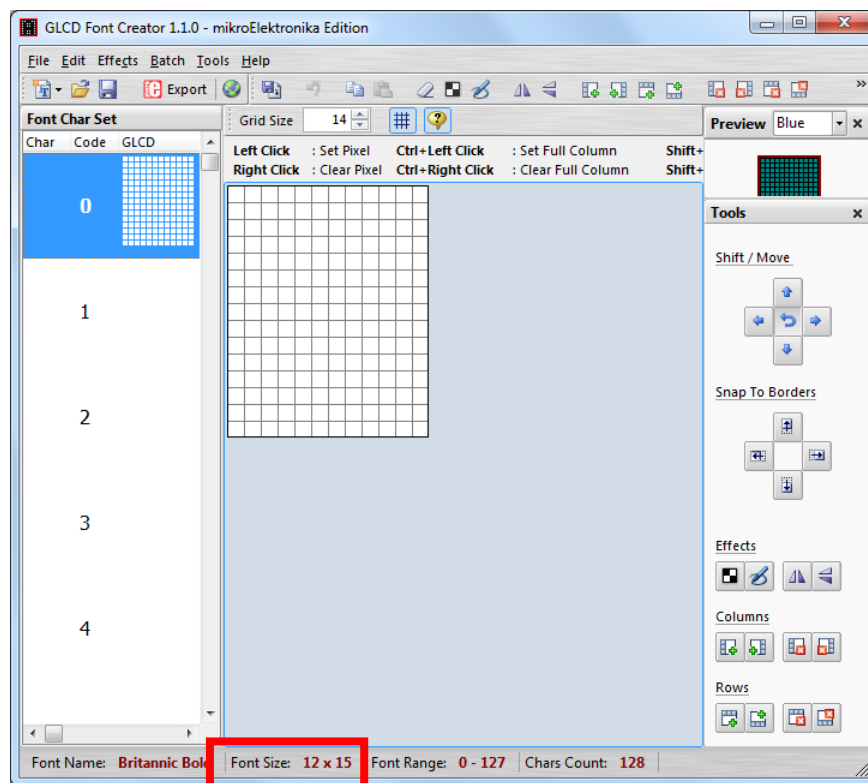
- Select the font needed, simply choose a font size. The final value of font size should be determined by the minimum pixel width. You may need to repeat this steps few times to find the best fit font size.



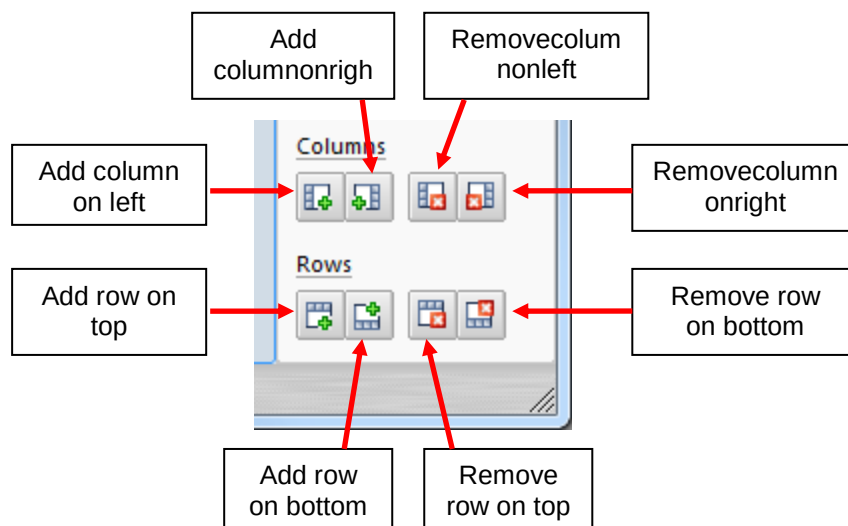
- Set the import range from 0 to 127.



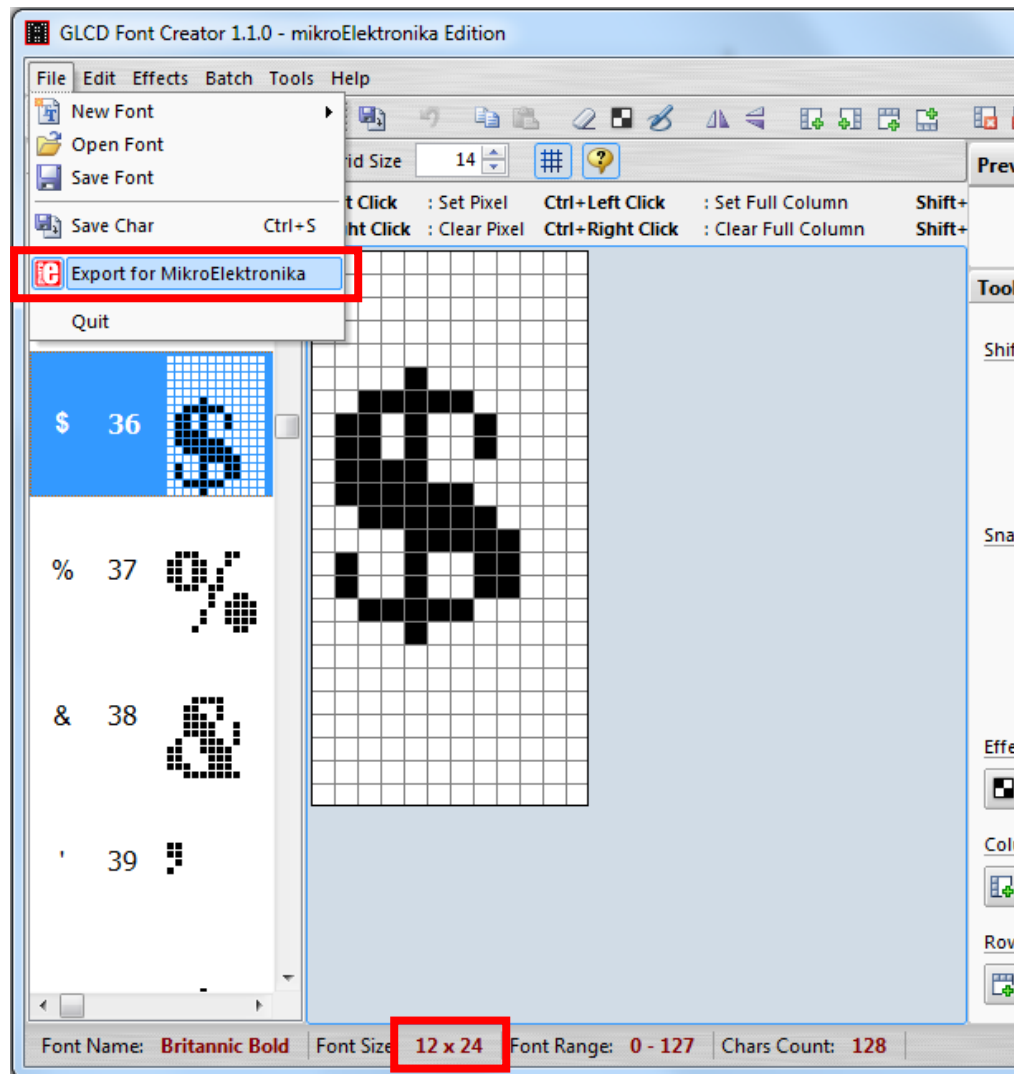
- Check the minimum pixel width and height.



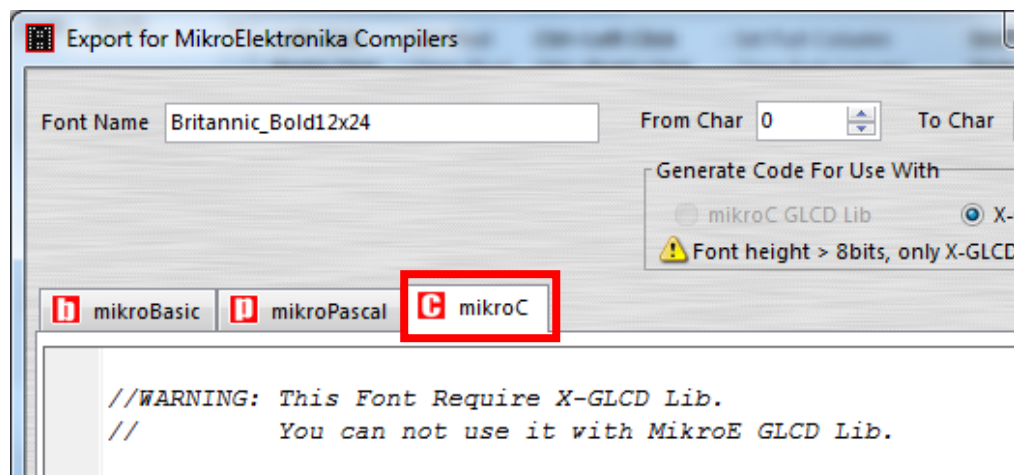
- If the pixel width of the font size is larger than expected, then you have to repeat the previous steps to import font with smaller size.
- Use the following buttons to adjust the font size to match with expected font size.



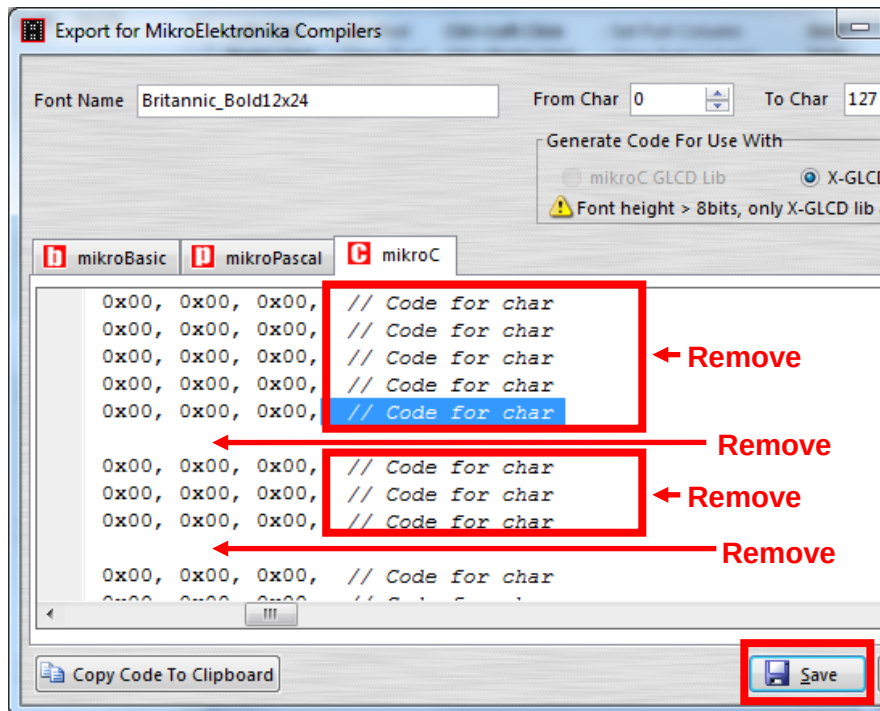
- After adjust font size, select [File] ⇒ [Export for MikroElektronika].



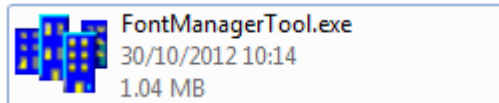
- Select output format as [mikroC].



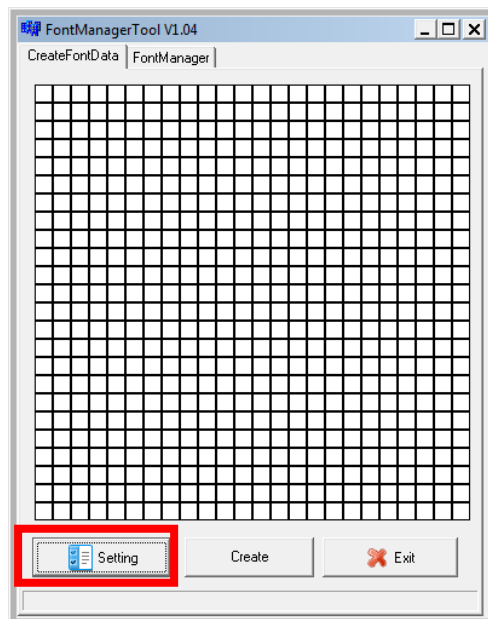
- Remove comment “// Code for char ” from offset 0x00 to 0x1F. Remove empty line if found. Then click [Save] button to save to file.



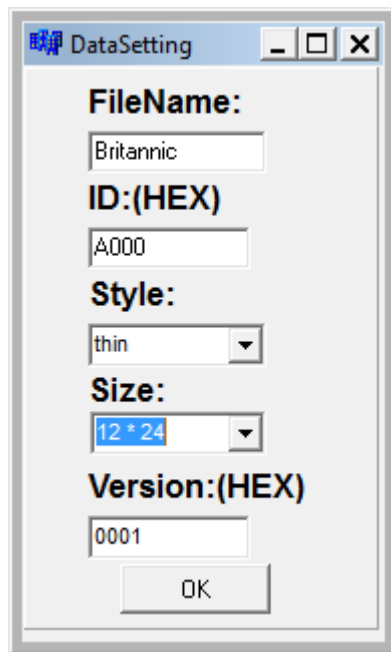
- Run Font Manager Tool.



- Click [Setting] button

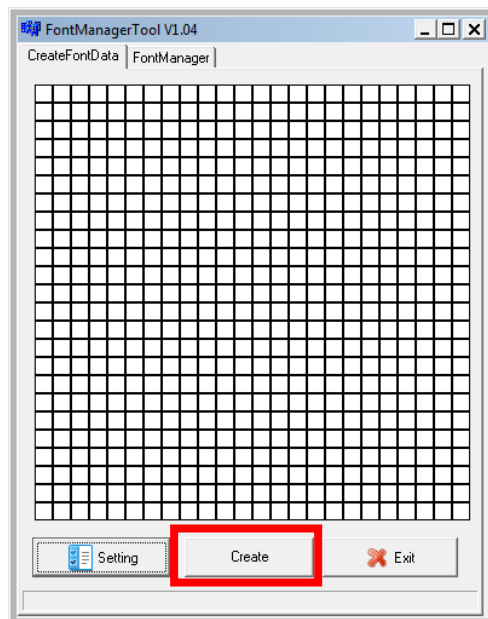


- Enter the file name, font id, and select the size.



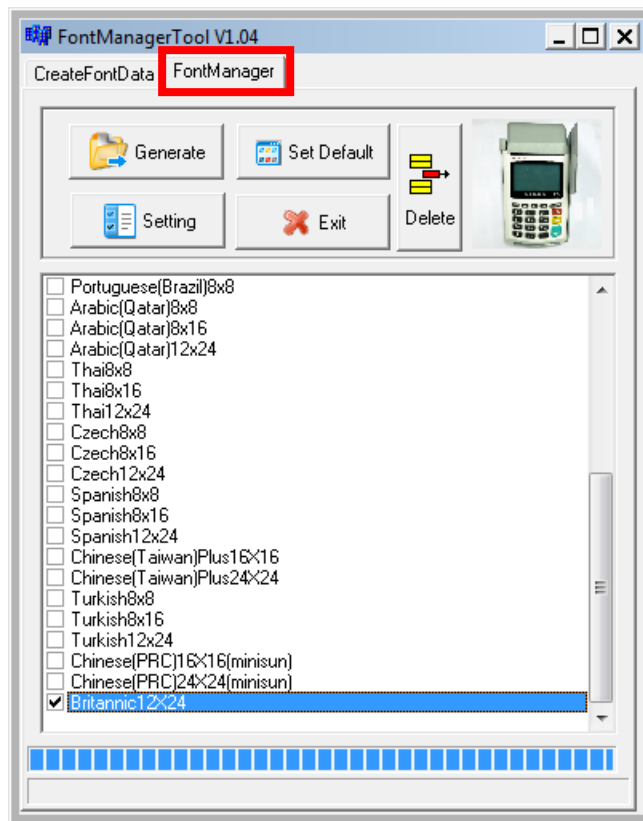
The image shows a dialog box titled "DataSeting". It contains several input fields and a button. The fields are labeled "FileName:", "ID:(HEX)", "Style:", "Size:", and "Version:(HEX)". The "FileName:" field contains the text "Britannic". The "ID:(HEX)" field contains the text "A000". The "Style:" field is a dropdown menu with "thin" selected. The "Size:" field is a dropdown menu with "12 * 24" selected. The "Version:(HEX)" field contains the text "0001". At the bottom of the dialog is an "OK" button.

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

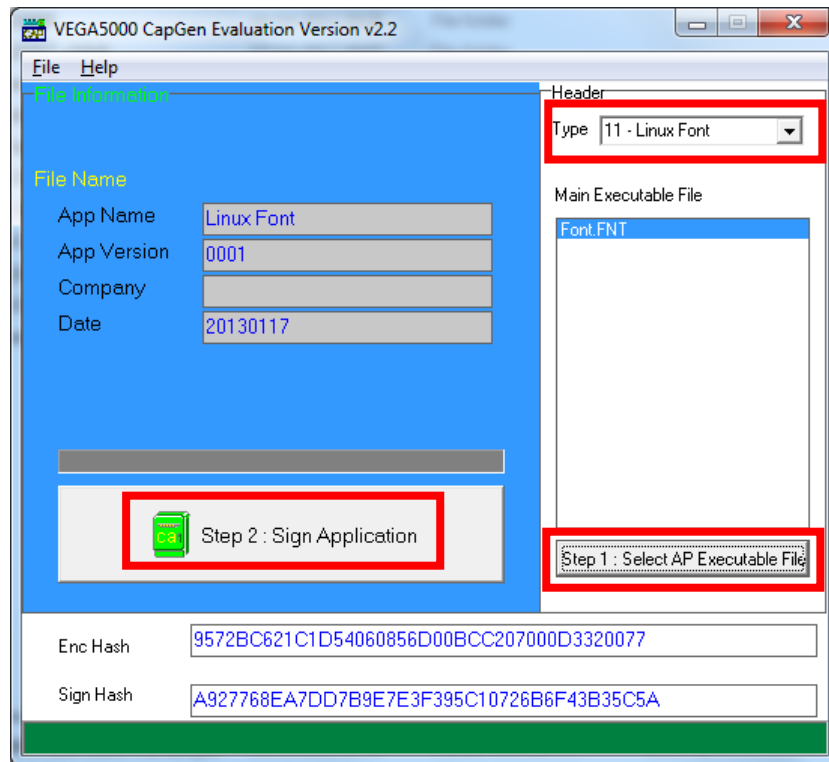


The image shows a window titled "FontManagerTool V1.04". It has a menu bar with "CreateFontData" and "FontManager". The main area is a large grid. At the bottom, there is a toolbar with three buttons: "Setting", "Create", and "Exit". The "Create" button is highlighted with a red rectangle.

- 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.

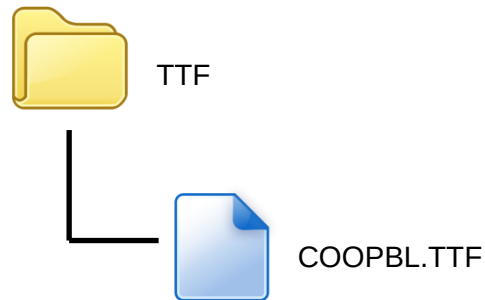
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

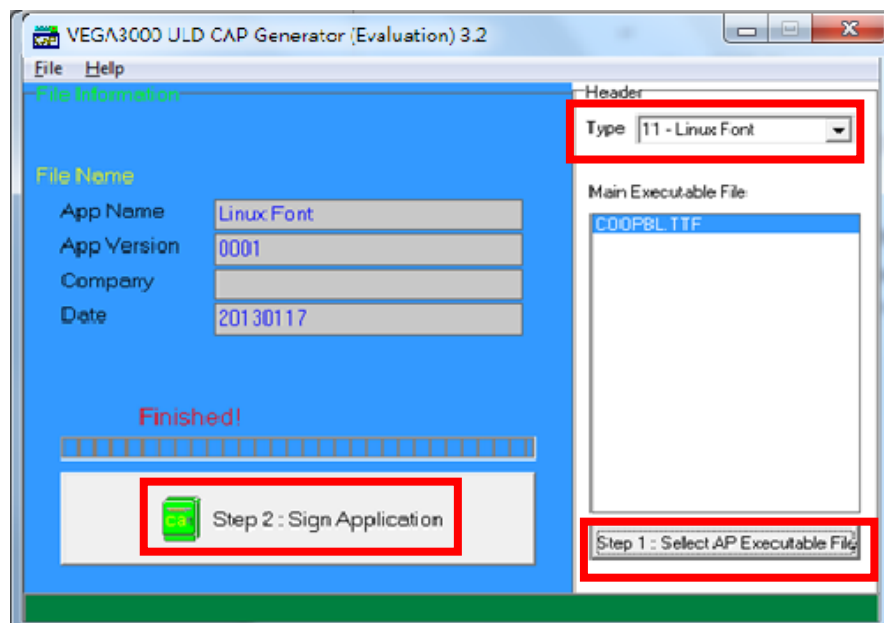
TrueType Font (TTF) is supported in VEGA3000 UltraLite. You may download the TrueType font preferred to terminal for displaying or printing.

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.

7. NCCWarning

根據 NCC 低功率電波輻射性電機管理辦法規定:

第十二條	經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條	低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。 前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。