



CASTLES TECHNOLOGY

VEGA5000S EFT-POS Terminal

Book 2

User Manual

Confidential

Version 1.1

May 2014

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

<i>Version</i>	<i>Date</i>	<i>Descriptions</i>
1.0	Nov 18, 2012	Initial creation.
1.01	May 12, 2014	Add the terminal starting up description
1.1	May 12, 2014	Add the description of GDB via USB

Contents

1. Introduction.....	6
1.1. Type of Terminal.....	6
2. Hardware Setup (Portable)	8
2.1. Parts of the Terminal	8
2.2. Inserting the Battery.....	11
2.3. Inserting the SAM Card	12
2.4. Inserting the Paper Roll	13
2.5. Inserting the GSM SIM Card.....	14
2.6. Inserting the Memory card	15
3. Basic Operation	16
3.1. Program Manager.....	16
3.2. Download AP	17
3.3. System Info.....	18
3.4. Memory Status	19
3.5. System Settings.....	20
3.6. Test Utility.....	23
3.7. Factory Reset	25
3.8. Power Off	26
3.9. Function Key Password Change.....	27
3.10. Share Object Management.....	28
3.11. CTOS TMS	29
3.12. ULD Key Hash.....	30
4. Secure File Loading.....	31
4.1. ULD Key System	31
4.1.1. ULD Manufacturer Key.....	31
4.1.2. ULD User Key	33
4.1.3. Key Change	33
4.2. File Signing.....	34
4.2.1. Signing Kernel Module	34
4.2.2. Signing User Files	36
4.3. File Loading	40
4.3.1. Download by User Loader.....	40
4.3.2. Download by Removable Media.....	43

4.4.	Changing ULD User Key.....	45
5.	Font Management	53
5.1.	Loading New Font.....	53
5.2.	Custom Font	56
5.3.	Using TrueType Font (TTF)	64
6.	Advance Features	66
6.1.	VEGA5000S GNU Project Debugger (GDB)	66
6.1.1.	About GDB.....	66
6.1.2.	SetupGDB.....	67
6.1.3.	Start Debugging	68
7.	Operation Notes	72
7.1.	Operation Notes	72

1. Introduction

This document provide a guideline on operating and configuring Castles VEGA5000S terminal.

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

1.1. Type of Terminal

There are two types of VEGA5000S terminal, portable and countertop. The major different is portable type can be battery operated.

Portable type is designed as two pieces of hardware, handset and base unit. Handset unit features major components, and also optional contactless reader and GRPS modem. Wired connection like power, modem, Ethernet, USB or serial ports, are be located in base unit. There are additional power connection and USB port on handset unit, allow the handset unit can be operated alone.

Handset

Front View



Rear View



Base

Front View



Rear View



Side View

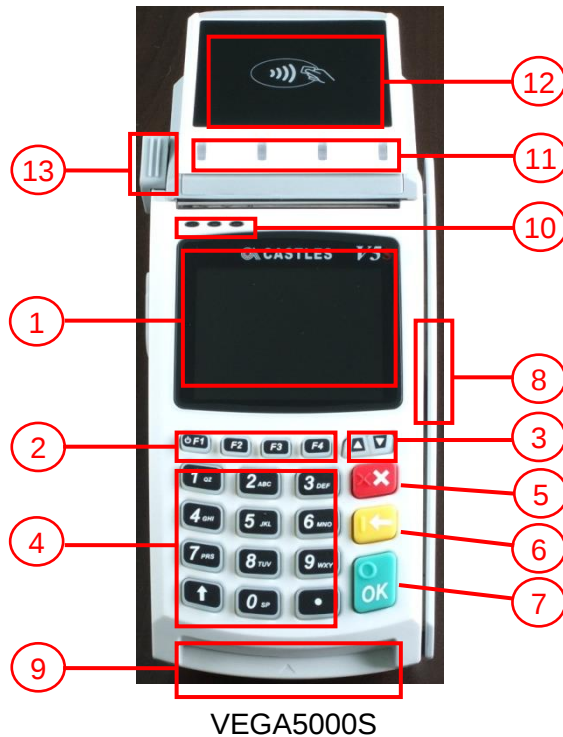


To start up the terminal, portable type needs to press "F1" key but countertop type will auto start when the power connector is connected with adapter.

2. Hardware Setup (Portable)

2.1. Parts of the Terminal

Front (Portable and Countertop)



1. LCD Display

ColorTFT : VEGA5000S

2. Programable Function Keys

F1 : Power keyfor PT
only.(Press 3s)

3. Navigation Key [▲▼]

4. Keyboard

5. Cancel Key

6. Clear Key

7. Enter Key

8. Magnetic Stripe Reader

9. Smart Card Reader

10. LED

Left : Green

Middle : Orange

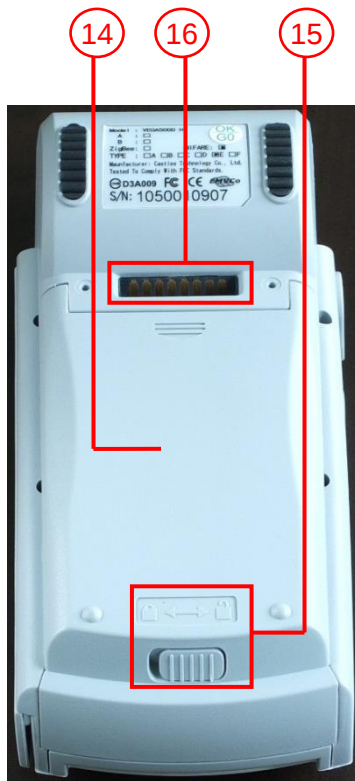
Right: Red

11. Contactless Module LED

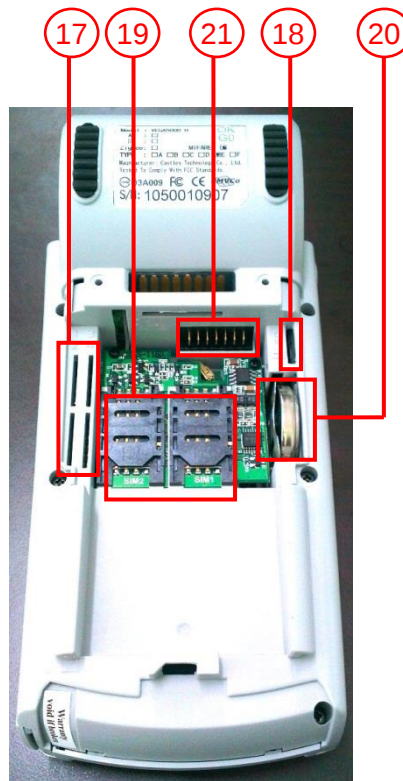
**12. Contactless Card Landing
Zone**

13. Paper Roll Handle

Rear (Portable)



VEGA5000S



VEGA5000S



VEGA5000S
Rechargeable
Battery

14. Recharable Battery Cover

15. Battery Cover Lock

16. Base Connector

17. SAM Slots

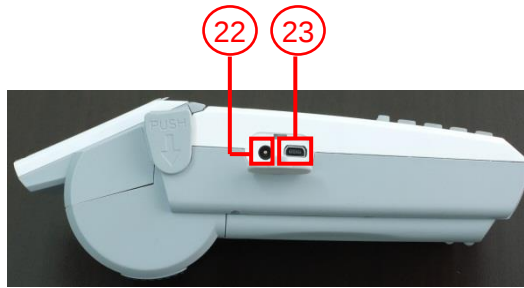
18. Micro SD Card Slot

19. GSM SIM Card Slots

20. RTC Battery

21. Battery Connector

Side



VEGA5000S Portable

22. Power Connector

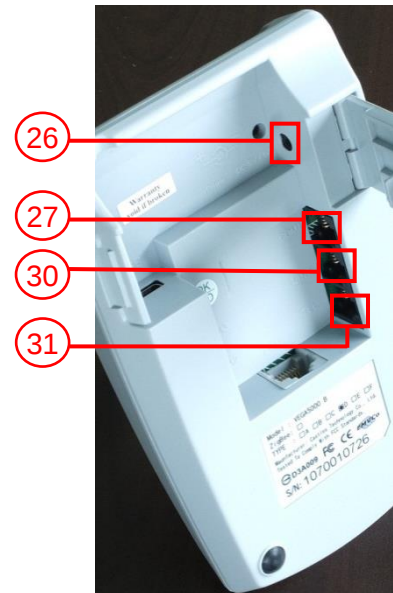
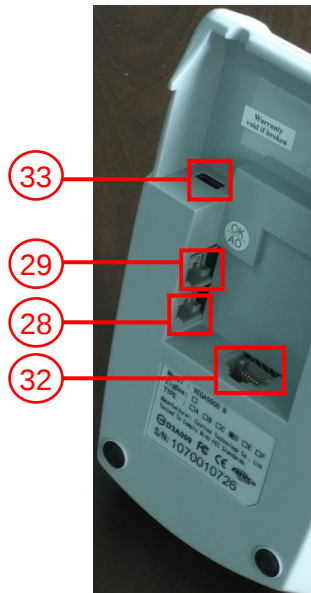
23. USB Port

Base (Portable)



24. Base Connector

25. Base LED



26. Power Connector

27. Com port 1

28. Com port 2

29. Com port 3

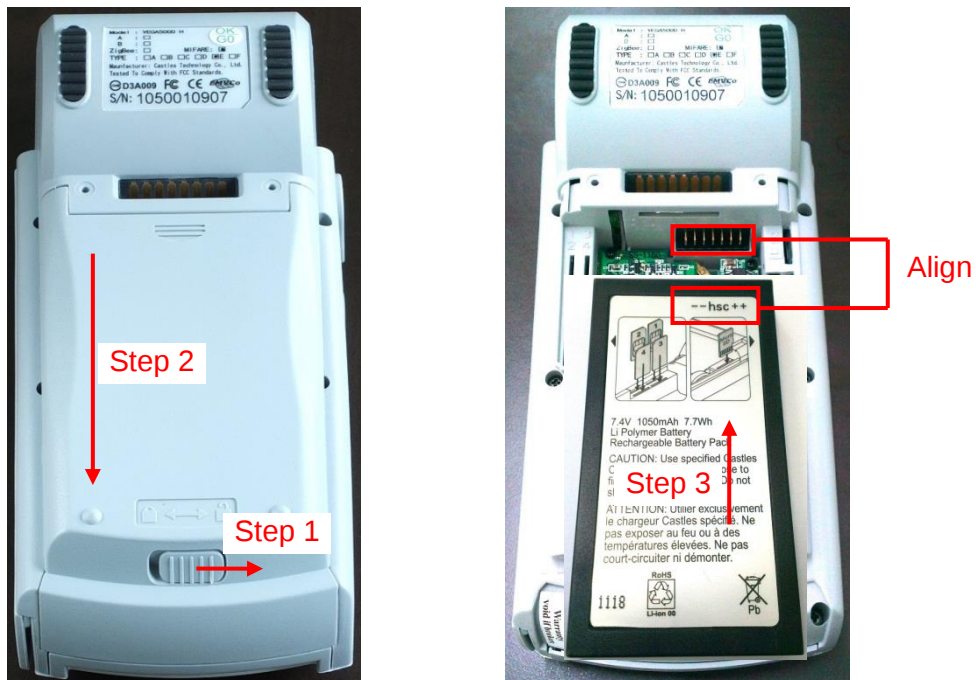
30. Modem - Line Port

31. Modem - Tel Port

32. Ethernet Port

33. USB Port

2.2. Inserting the Battery

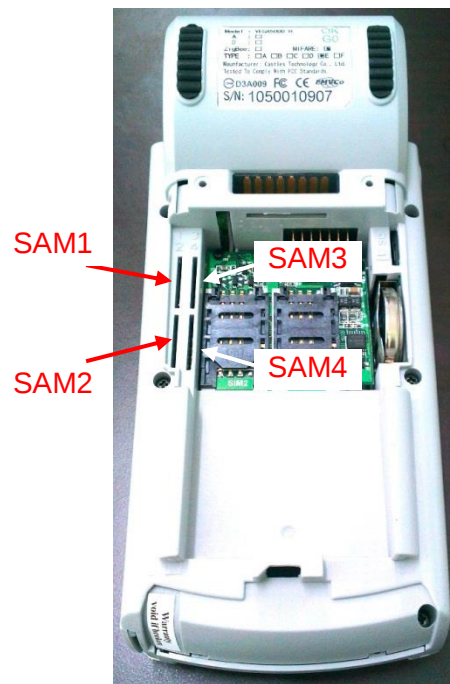


Step 1: Unlock Battery cover

Step 2: Remove battery cover

Step 3: Insert battery into compartment, battery contact point must align with battery connector.

2.3. Inserting the SAM Card



VEGA5000S Portable

Step 1: Remove battery cover / back cover

Step 2: Insert SAM card into desire slot.

Portable



SAM 1 & 2:

Gold contact at lower side of card and facing right.



SAM 3 & 4:

Gold contact at lower side of card and facing left.

Countertop



SAM 1 & 2 & 3:

Gold contact at upper side of card and facing down.



SAM 4 :

Gold contact at upper side of card and facing up.

2.4. Inserting the Paper Roll



Step 1: Push paper roll box handle.

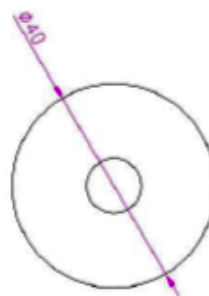
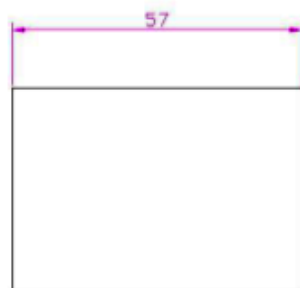
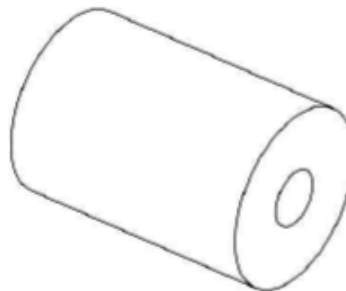
Step 2: Gentle open paper roll cover.

Step 3: Insert paper roll as direction showed.

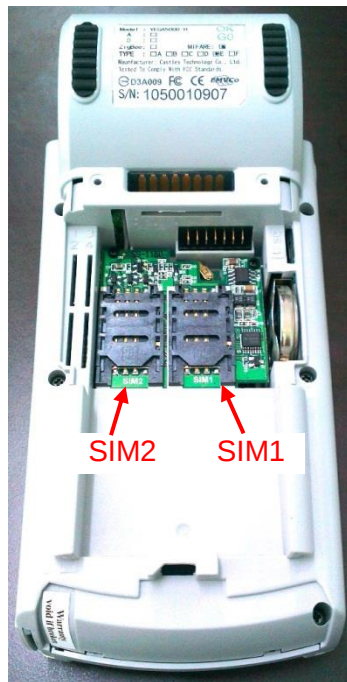
Paper specification

Width: 57mm

Outside diameter: 40mm



2.5. Inserting the GSM SIM Card



VEGA5000S Portable

Step 1: Remove battery cover / back cover

Step 2: Open SIM socket and insert GSM SIM card into desire slot.

Portable



SIM 1 & 2:

Gold contact at upper side of card and facing down.

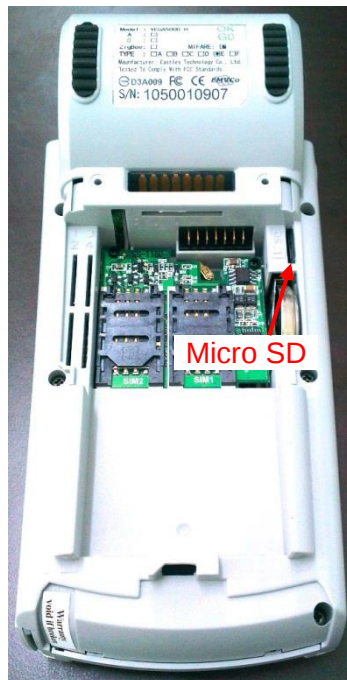
Countertop



SIM 1 & 2:

Gold contact at lower side of card and facing down.

2.6. Inserting the Memory card



VEGA5000S Portable



VEGA5000S Countertop

Step 1: Remove battery cover / back cover

Step 2: Insert Micro SD memory card.

Portable



Micro SD :

Gold contact at lower side of card and facing right.

Countertop



Micro SD :

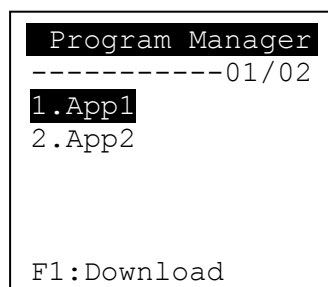
Gold contact at upper side of card and facing up.

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.

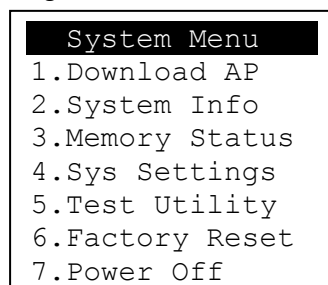
Program Manager



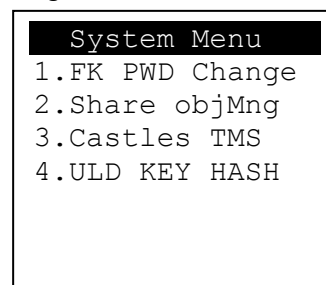
- Press [F1] button to enter System Menu.
- Press [F2] button to toggle default application selection.
- Press [F3] button to delete application.
- Press [F4] button to view application info.
- Press [OK] button to run application.
- Press [▲] or [▼] button to select application.

System Menu

Page 1



Page 2

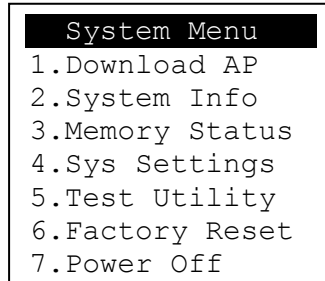


- Press [▼] button to page 2.

3.2. Download AP

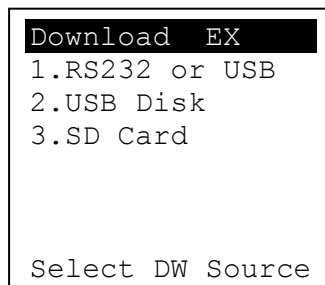
Download user application or kernel modules firmware.

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---
BOOTSULD : V0064
CRYPTOHAL: VF057
KMS : V0056
LINUXKNL : V0024
ROOTFS : V0050

Page 2

SYSTEM INFO
--- KOver ---
SECURITY : V0076
SYSUPD : V0080
KMODEM : N/A
DRV : V0089
USB : V0078
SC : V0083

Page 3

SYSTEM INFO
--- SO Ver 1 ---
UART : V0072
USBH : V0070
MODEM : V0075
ETHERNET : V0078
FONT : V0076
LCD : V0073

- Press [OK] button to next page.

Page 4

SYSTEM INFO
--- SO Ver 2 ---
PRT : V0073
RTC : V0073
ULDPM : V0078
PPP MODEM: V0086
EMVL2 : V0072
KMS : V0073

Page 5

SYSTEM INFO
--- SO Ver 3 ---
FS : V0075
GSM : V0080
BARCODE : V0073
TMS : V0072
TLS : V0071
CLVW : V0076

Page 6

SYSTEM INFO
--- SO Ver 4 ---
CTOSAPI : V0083

Page 7

SYSTEM INFO
--- HWMVer ---
CRDL/ETHE: V3004
CLM-MP : V0015
--- APVer ---
ULDPM : V0043

Page 8

SYSTEM INFO
--- HWMVer ---
HUSBID:0CA6A050
CUSBID:N/A
--Factory S/N--
0000010600035717

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:    31616KB
Used :    22640KB

--SDRAM Memory--
Total:    31872KB
Used :    10908KB
```

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 (F1 ~ F4) 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 null cradle. [Portable model only]
Debug Mode	Enable (Y) or disable (N) console debug mode.
Debug Port	Serial port for console debug.
Mobil AutoON	<TBC>
GDB Mode	Enable (Y) or disable (N) GDB mode. [VEGA5000S only]
GDB Timeout	GDB connection timeout. [VEGA5000S only]
GDB Channel	GDB connection channel. [VEGA5000S only]
ETHER IP/PORT	GDB Ethernet connection setting. [VEGA5000S only]

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
-AP Name
USB CDC Mode: Y
FunKeyPWD : N
PMEnterPWD : N
F3: Next Page

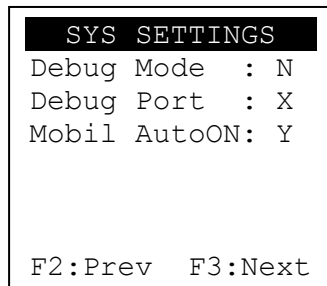
- Press [▲] or [▼] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇒ N ⇒ Y.
- Press [F3] button to next page.

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
F2:Prev F3:Next

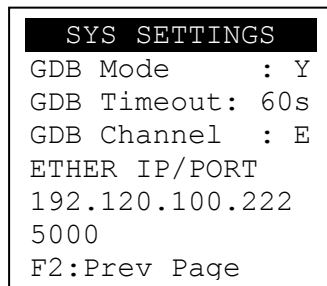
- Press [▲] or [▼] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇒ N ⇒ Y.
- Press [F2] button to previous page.
- Press [F3] button to next page.

Page 3



- Press [▲▼] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇌ N ⇌ Y.
- Press [F2] button to previous page.
- Press [F3] button to next page.

Page 4 (VEGA5000S only)



- Press [▲▼] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇌ N ⇌ Y.
- Press [F2] button to previous page.

3.6. Test Utility

Perform terminal hardware components diagnostic.

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.

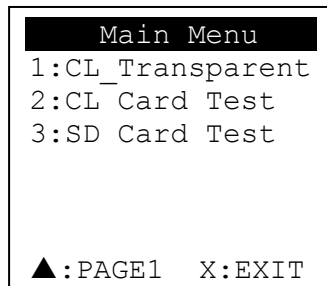
Test Utility Menu

Page 1

```
Main Menu 0009
1:LCD 2:KBD
3:FLASH 4:SCM
5:Light 6:MSR
7:LED 8:RTC
9:PRNTR 0:FONT
[F2]Comm Menu
[F3]Power Off
```

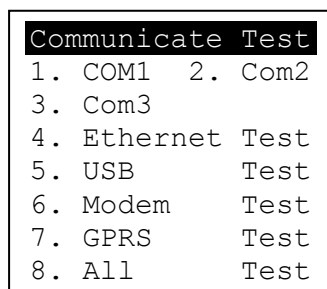
- Press [1] button to diagnose LCD.
- Press [2] button to diagnose keyboard.
- Press [3] button to diagnose flash memory.
- Press [4] button to diagnose smart card module.
- Press [5] button to diagnose backlight.
- Press [6] button to diagnose magnetic stripe reader.
- Press [7] button to diagnose LED.
- Press [8] button to diagnose real time clock.
- Press [9] button to diagnose printer.
- Press [0] button to view font.
- Press [F2] button to enter Communication Test Menu.
- Press [F3] button to power off.
- Press [▼] button to next page.

Note: Default password for changing RTC is 8418.



- Press [1] button to diagnose contactless reader in transparent mode.
- Press [2] button to diagnose contactless card.
- Press [3] button to diagnose SD memory card.
- Press [▲] button to previous page.
- Press [X] button to exit.

Communication Test Menu

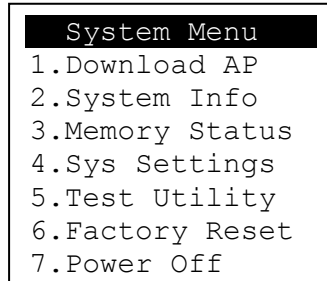


- Press [1] button to diagnose Com 1.
- Press [2] button to diagnose Com 2.
- Press [3] button to diagnose Com 3.
- Press [4] button to diagnose Ethernet module.
- Press [5] button to diagnose USB.
- Press [6] button to diagnose modem.
- Press [7] button to diagnose GPRS.
- Press [8] button to diagnose all, item 1 to 7.

3.7. Factory Reset

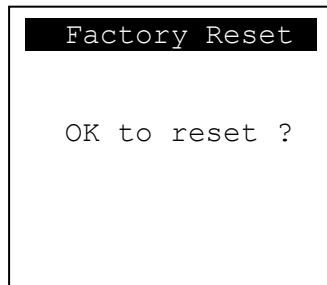
Perform factory reset, all user application, fonts and data will be deleted.

System Menu



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

Factory Reset Menu



- Press [OK] button to perform factory reset.

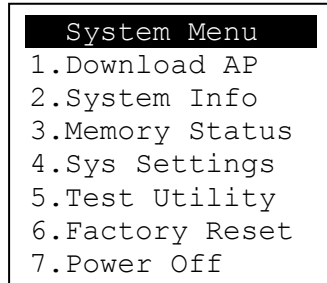


- Enter factory reset password. **Default password: 8418**

3.8. Power Off

Power off terminal.

System Menu

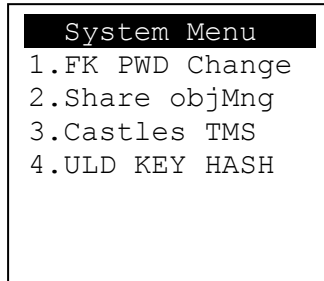


- Press [7] button to power off terminal.

3.9. Function Key Password Change

Change function key access password.

System Menu (Page 2)



A screenshot of a terminal window titled "System Menu". It displays a list of four options: "1.FK PWD Change", "2.Share objMng", "3.Castles TMS", and "4.ULD KEY HASH".

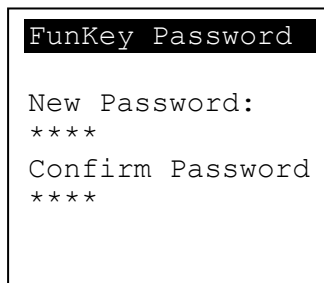
- Press [1] button to enter FunKey Password menu.

FunKey Password Menu



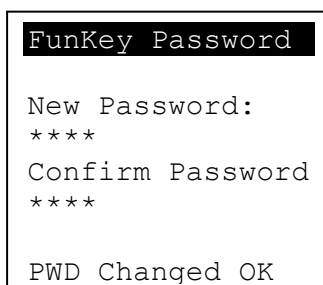
A screenshot of a terminal window titled "FunKey Password". It displays the prompt "Enter Password:" followed by four asterisks "****" on the next line.

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



A screenshot of a terminal window titled "FunKey Password". It displays the prompt "New Password:" followed by four asterisks "****" on the next line, and then "Confirm Password" followed by four asterisks "****" on the line below.

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

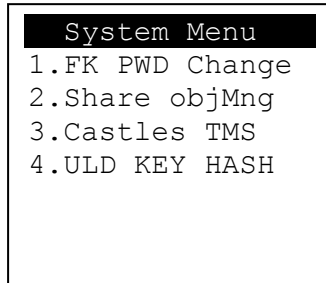


A screenshot of a terminal window titled "FunKey Password". It displays the prompt "New Password:" followed by four asterisks "****" on the next line, and then "Confirm Password" followed by four asterisks "****" on the line below. At the bottom of the screen, it displays the message "PWD Changed OK".

3.10.Share Object Management

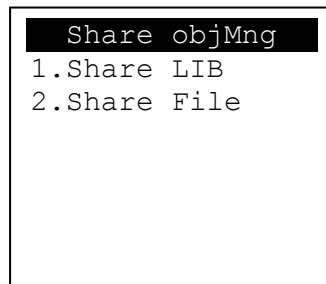
View share object in terminal.

System Menu (Page 2)



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

Share Object Management Menu

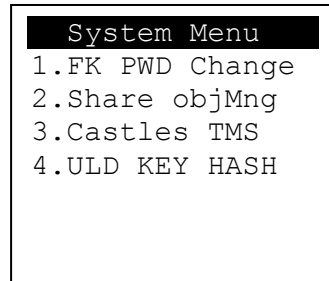


- Press [1] button to view shared library.
- Press [2] button to view shared file.

3.11.CTOS TMS

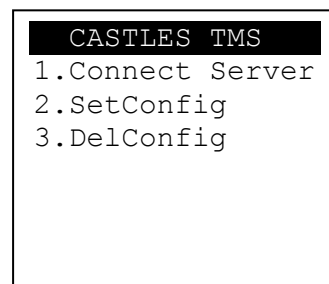
Connect to TMS (Terminal Management Software) server, set or delete TMS configuration.

System Menu (Page 2)



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

Castles TMS Menu

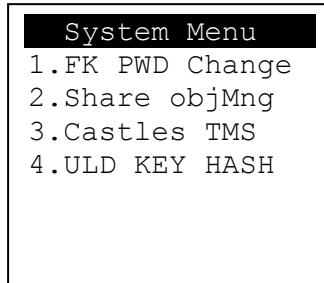


- Press [1] button to connect to TMS server.
- Press [2] button to set TMS configuration.
- Press [3] button to delete TMS configuration.

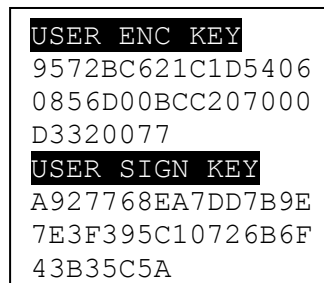
3.12.ULD Key Hash

View ULD user keyset hash value.

System Menu (Page 2)



- Press [4] button to view hash value.



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 VEGA5000S, the RSA key length is 2048bits.

4.1.1. ULD Manufacturer Key

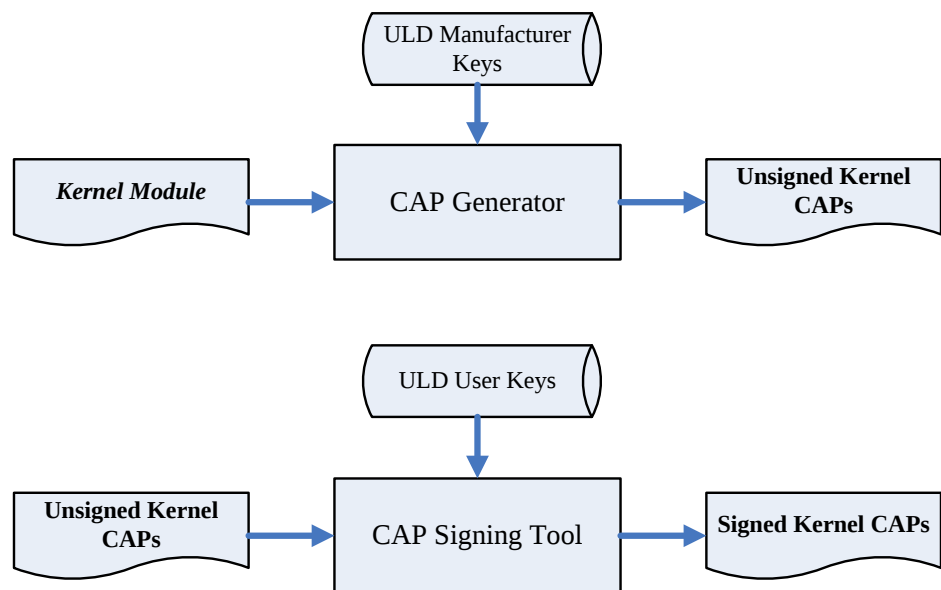
The system consists of several kernel modules. These kernel modules are provided by the Manufacturer, and released in CAP format file with encryption and signing via ULD Manufacturer Keys.

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:

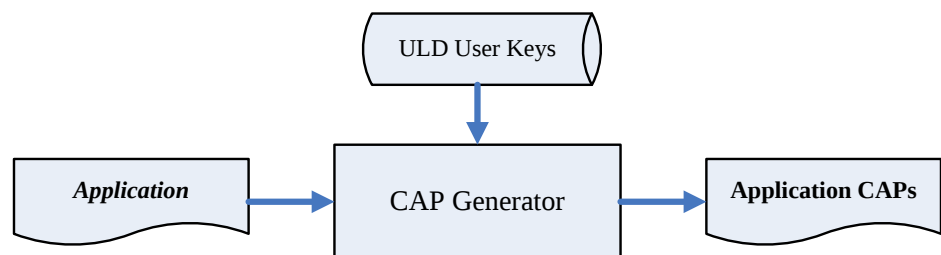
1. The kernel modules are encrypted by a random-generated 3DES key, which is retrieved from the Key Encryption Block of the CAP by ULD Manufacturer Key Encryption Key, not directly encrypted by ULD RSA Key.
2. The “sign” action via ULD User Keys actually is done by “the second encryption”. “The second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

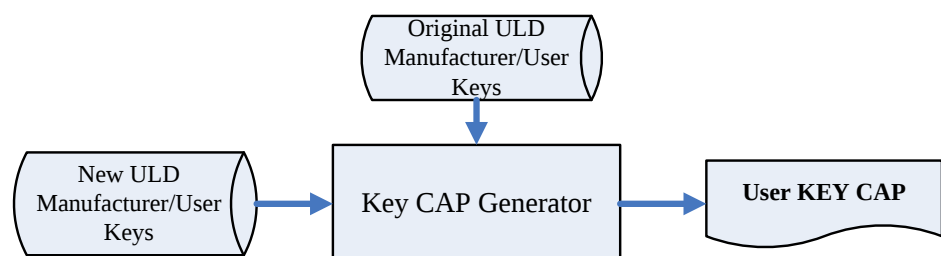
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the “signed” action via ULD User Keys.

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 provided a tool named “CAP Signing Tool” to perform this task.

The CAP Signing Tool is located at:

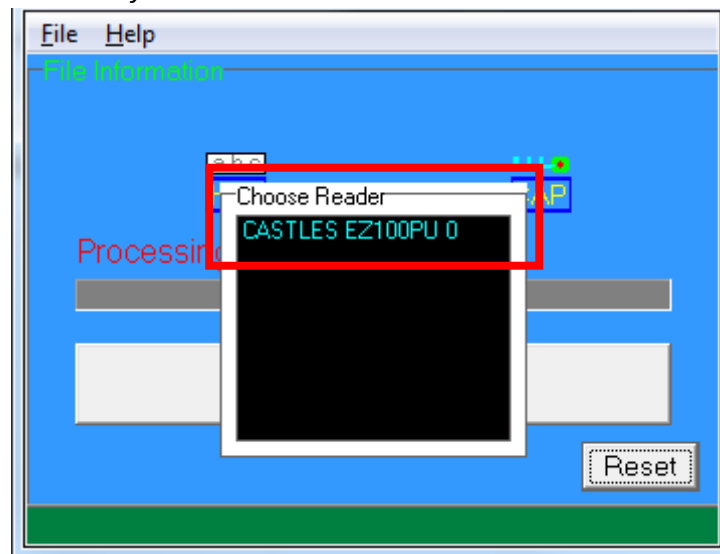
VEGA5000S

C:\Program Files\Castles\VEGA5000S\tools\Signing Tool

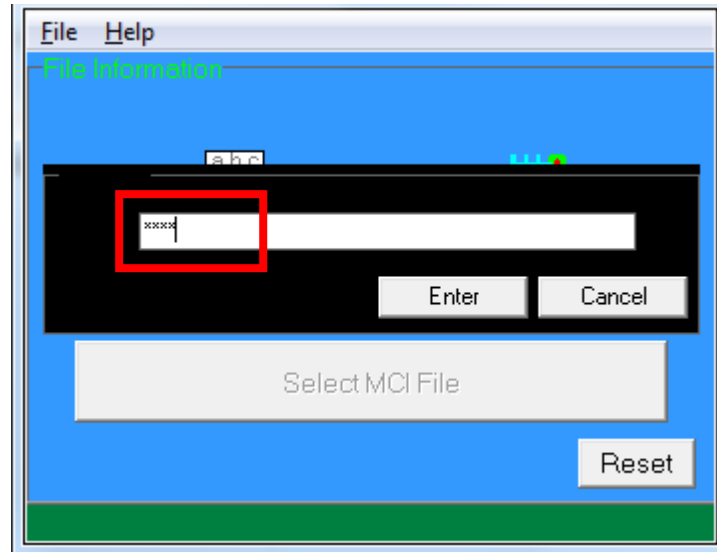
- Run CAP Signing Tool



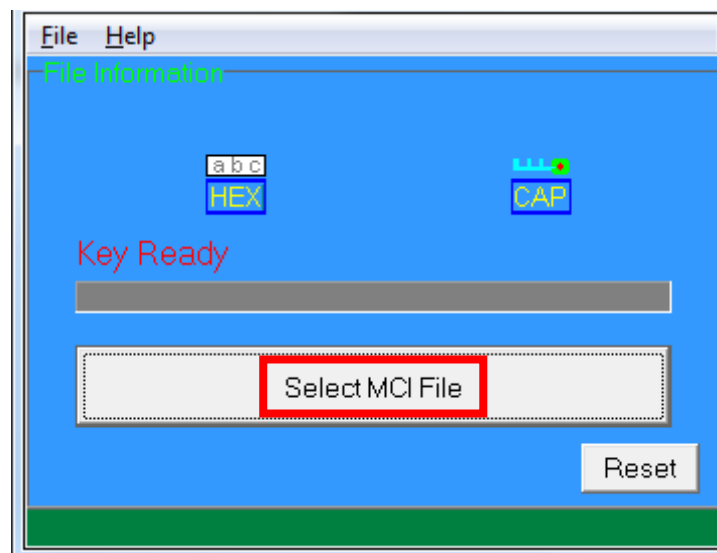
- Insert Key Card and select smart card reader



- 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)

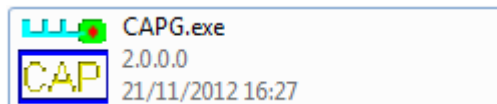
Castles Technology provided a tool named “CAP Generator” to perform this task.

The CAP Generator is located at:

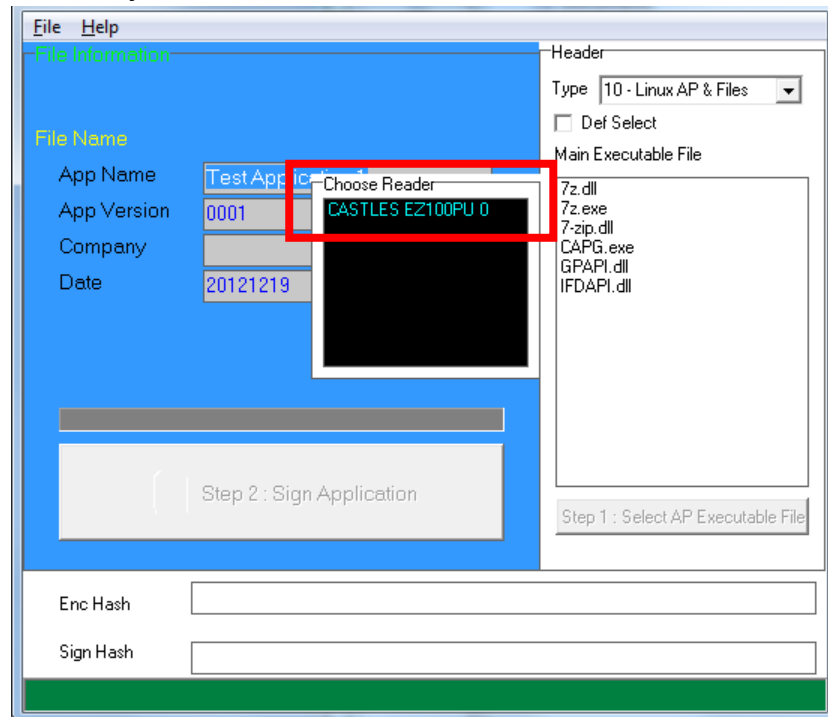
VEGA5000S

C:\Program Files\Castles\VEGA5000S\tools\CAPG (KeyCard)

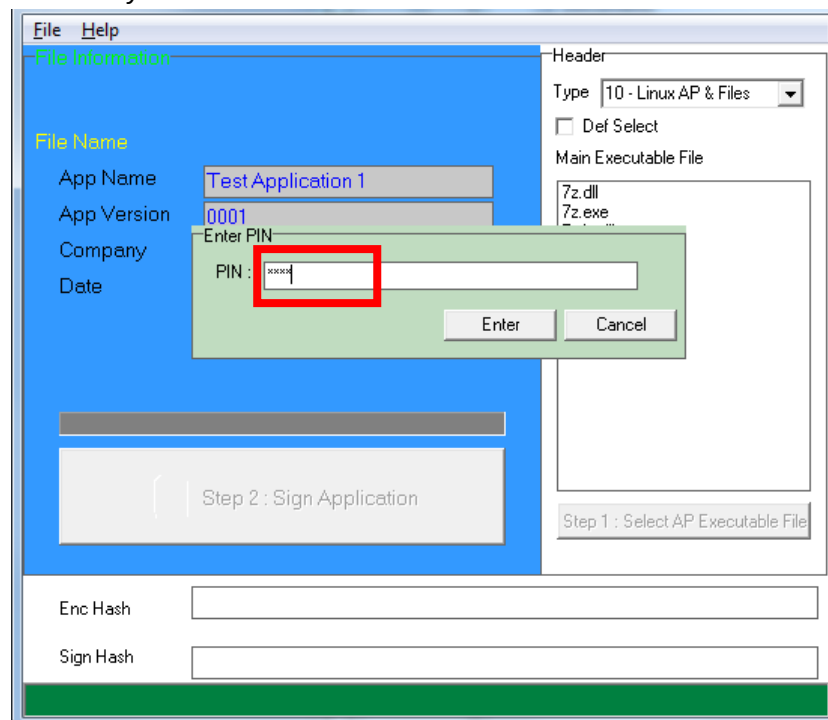
- Run CAP Generator



- Insert Key Card and select smart card reader



- Enter Key Card PIN



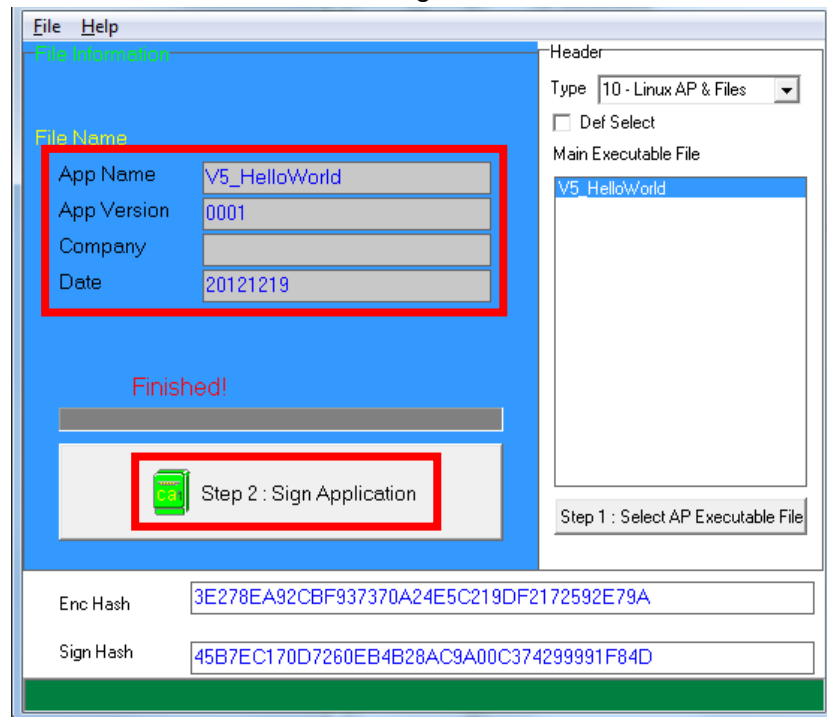
- CAP Generator is ready, select the correct Type from the list.

The screenshot shows the 'CAP Generator' application window. The 'File Information' tab is active. The 'Type' dropdown menu is open, showing a list of file types. The '10 - Linux AP & Files' option is selected and highlighted with a red box. The 'App Name' field contains 'Test Application 1', 'App Version' is '0001', 'Company' is empty, and 'Date' is '20121219'. The 'Enc Hash' and 'Sign Hash' fields are also visible at the bottom.

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

The screenshot shows the 'CAP Generator' application window. The 'File Information' tab is active. The 'Type' dropdown menu is closed. The 'Main Executable File' field is empty. The 'Step 1: Select AP Executable File' button is highlighted with a red box. The 'App Name' field contains 'V5_HelloWorld', 'App Version' is '0001', 'Company' is empty, and 'Date' is '20121219'. The 'Enc Hash' and 'Sign Hash' fields are also visible at the bottom.

- 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 VEGA5000S terminal.

- Download by User Loader
- Download by removable media
- 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.

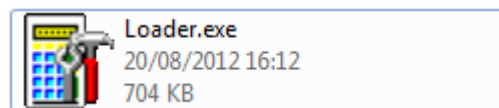
4.3.1. Download by User Loader

The Loader is located at:

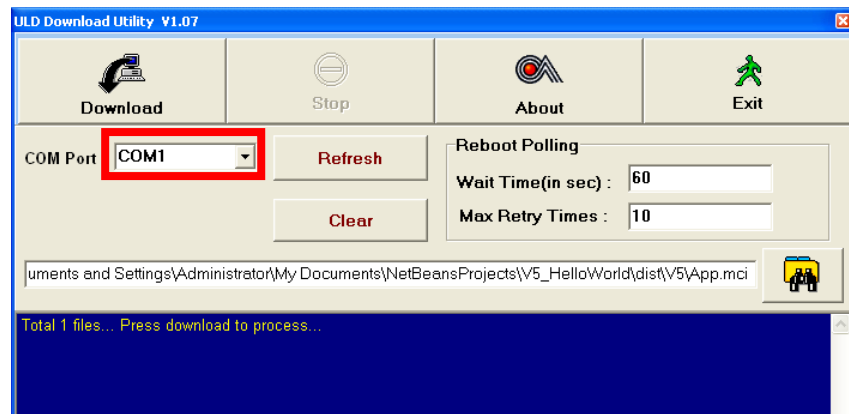
VEGA5000S

C:\Program Files\Castles\VEGA5000S\tools\Loader

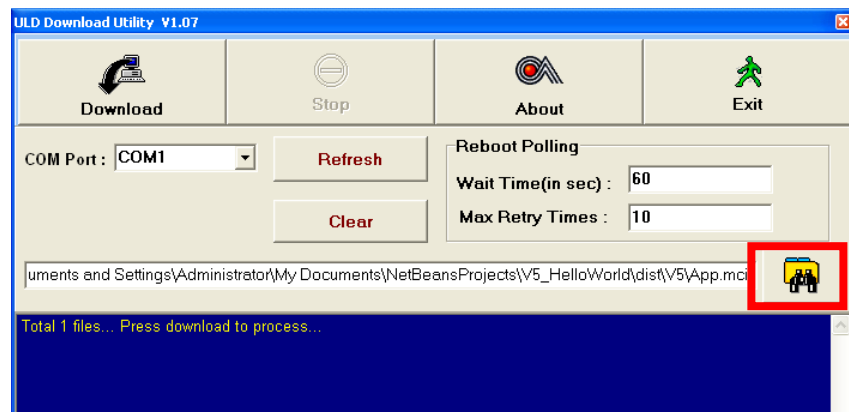
- Run User Loader



- Select COM port

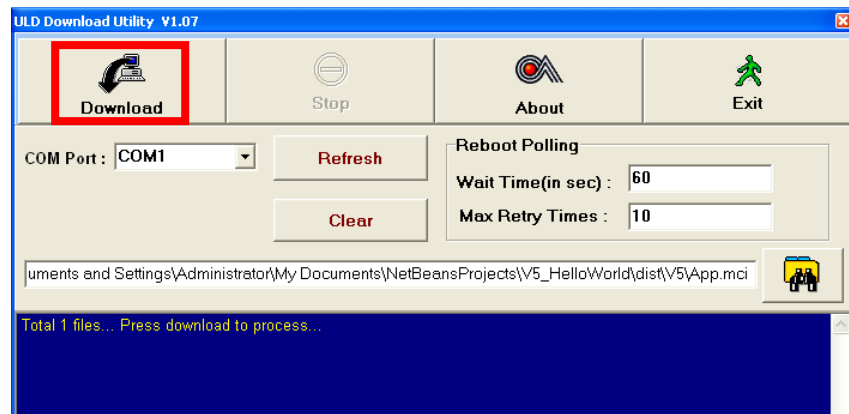


- Browse and select mci file or mmci file

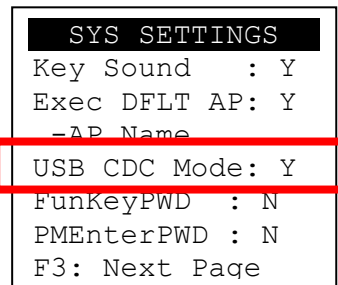


- Setup terminal to enter download mode
 - Press [F1] button in Program Manager (PM)
 - Press [1] button to select “1. Download AP”
 - Press [1] button again to select download via RS232 or USB

- Press “Download” button to start.



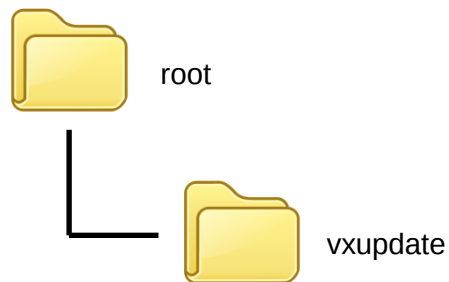
*Note: To download using USB cable, terminal must enable CDC mode.
Set USB CDC Mode to Y.*



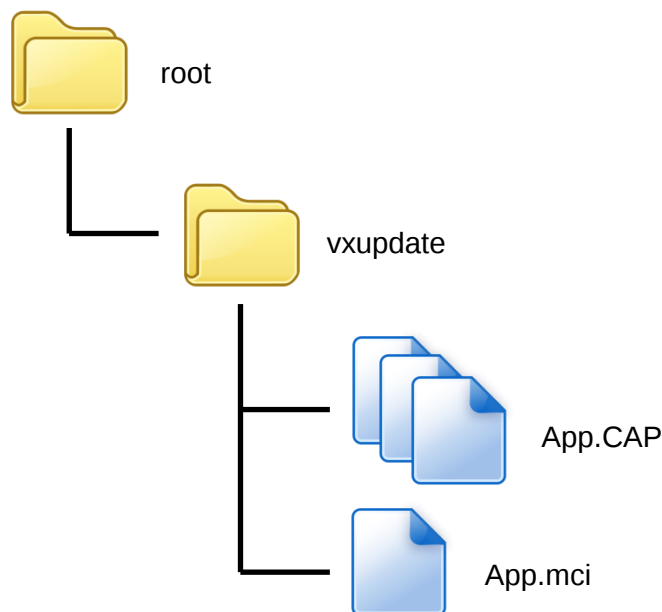
4.3.2. Download by Removable Media

The file download process can be achieved without PC by using removable media, USB flash drive or MicroSD memory card. We recommend don't put unwanted file to removable media, as it will increase the time during detection.

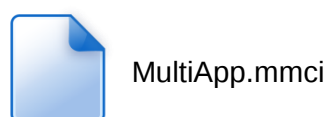
- Create a folder name "vxupdate" under root directory.



- Place the mci file and cap file to "vxupdate" folder.

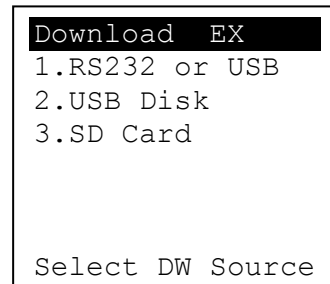


Note: If user would like to load multiple application, create a new file with extension of "mmci". Then put the mmci file contents with the list of mci file.



- Insert removable media to terminal, and select the removable media type in “Download AP” menu.

Download AP Menu



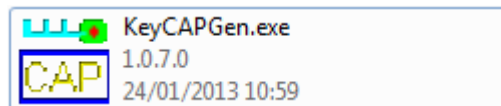
- Press [2] button to select USB flash drive.
 - Press [3] button to select MicroSD card.
-
- Finally, terminal will process the file “vxupdate” folder.

4.4. Changing ULD User Key

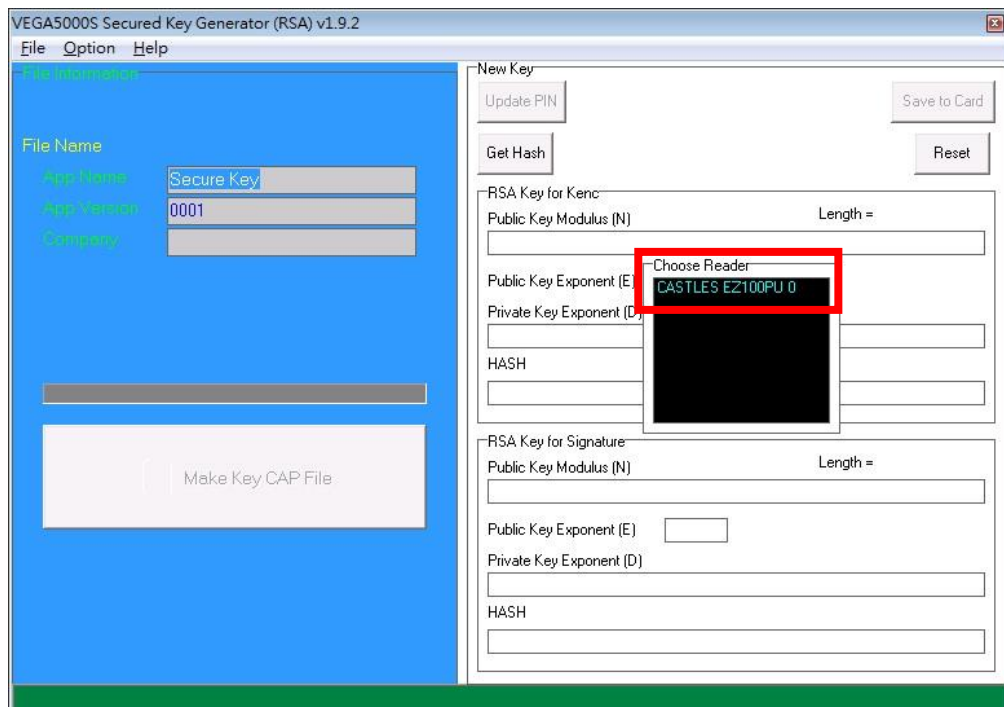
User may change their ULD User Key Set stored in Key Card. Castles Technology provided a tool named “Secure Key Generator” to perform this task.

For VEGA5000S

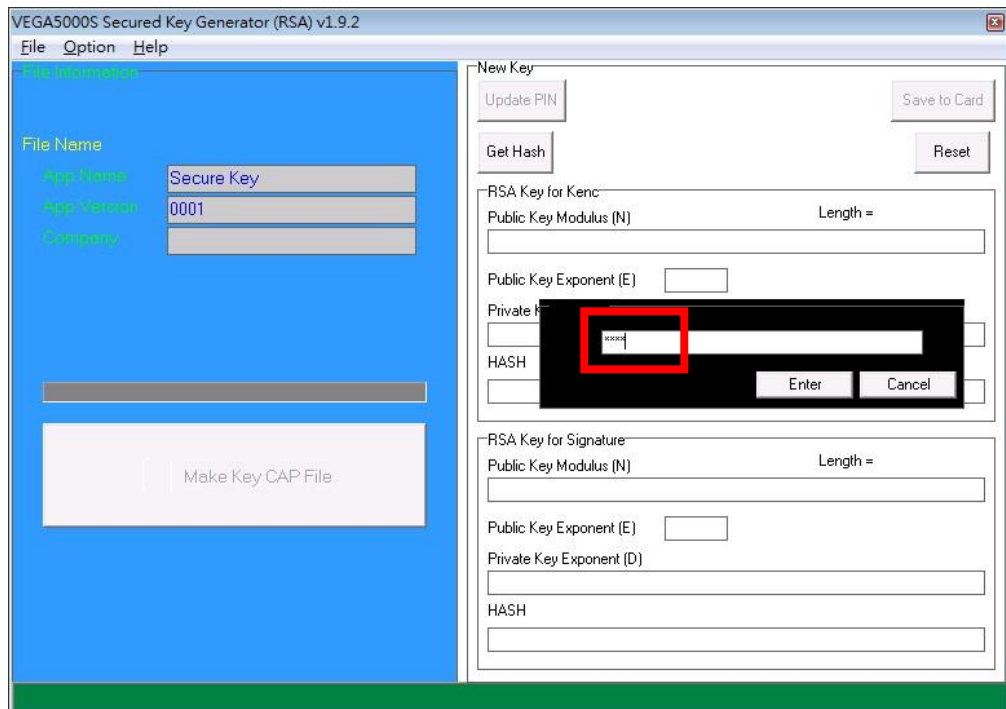
- Run Secure Key Generator



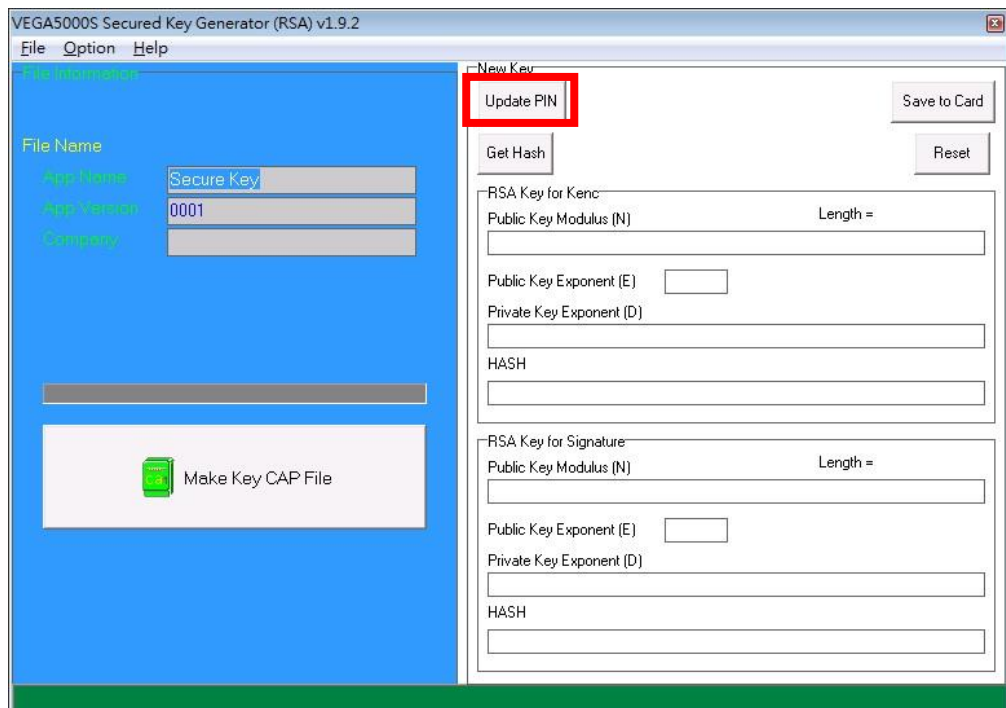
- Insert Key Card and select smart card reader



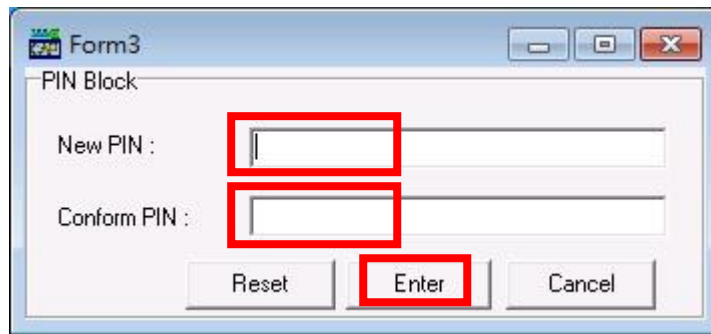
- Enter Key Card PIN, default PIN is “1234”.



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

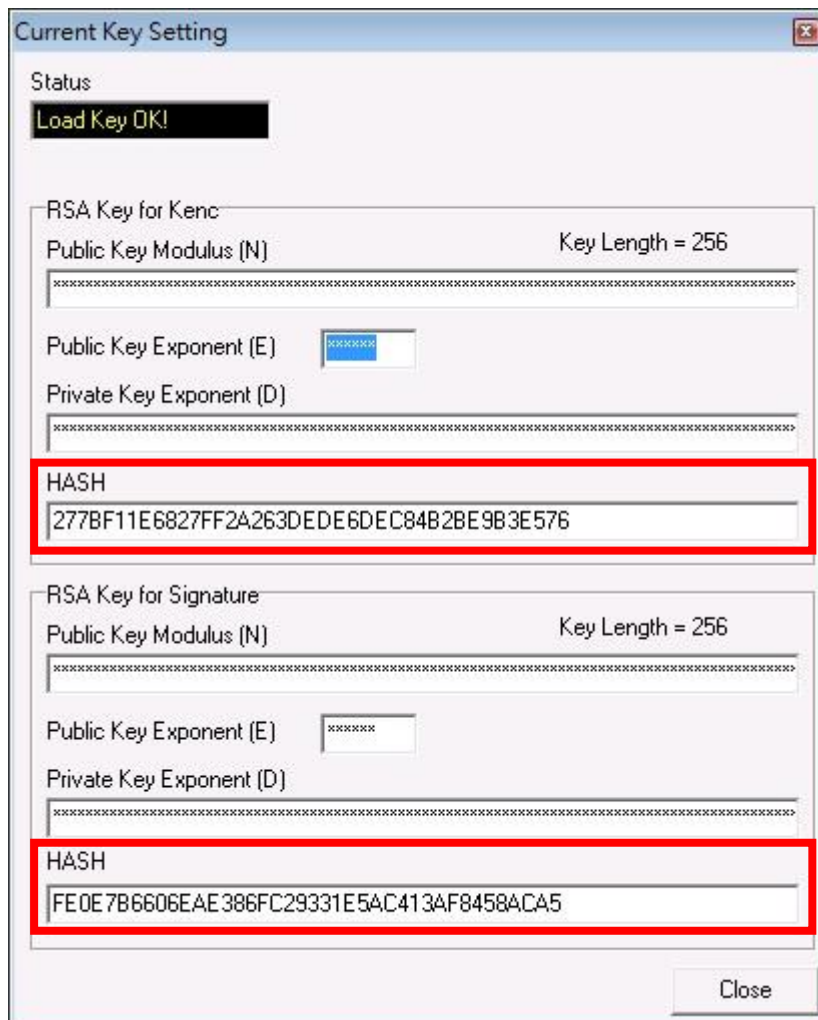
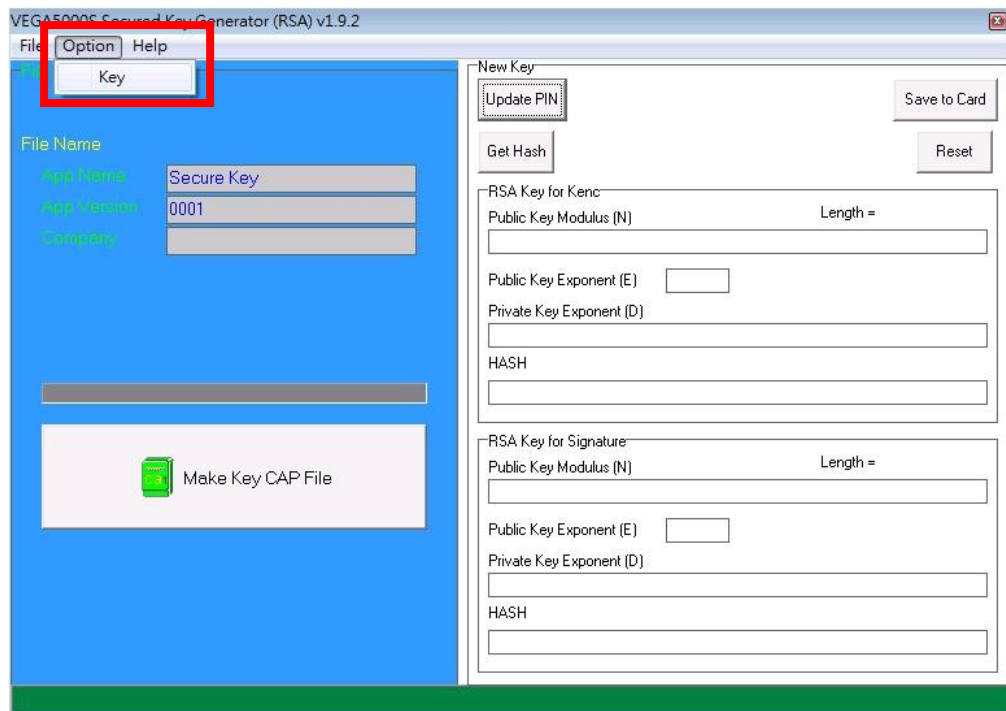


- Enter new PIN, enter new PIN again to confirm, then press [Enter] button to change PIN in Key Card.

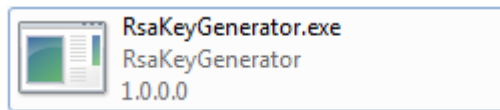


A screenshot of a Windows-style dialog box titled "Form3". The dialog has a standard title bar with minimize, maximize, and close buttons. The main content area is titled "PIN Block" and contains two text input fields. The first field is labeled "New PIN :" and the second is labeled "Conform PIN :". Both input fields are highlighted with red rectangular boxes. Below the input fields are three buttons: "Reset", "Enter", and "Cancel". The "Enter" button is also highlighted with a red rectangular box.

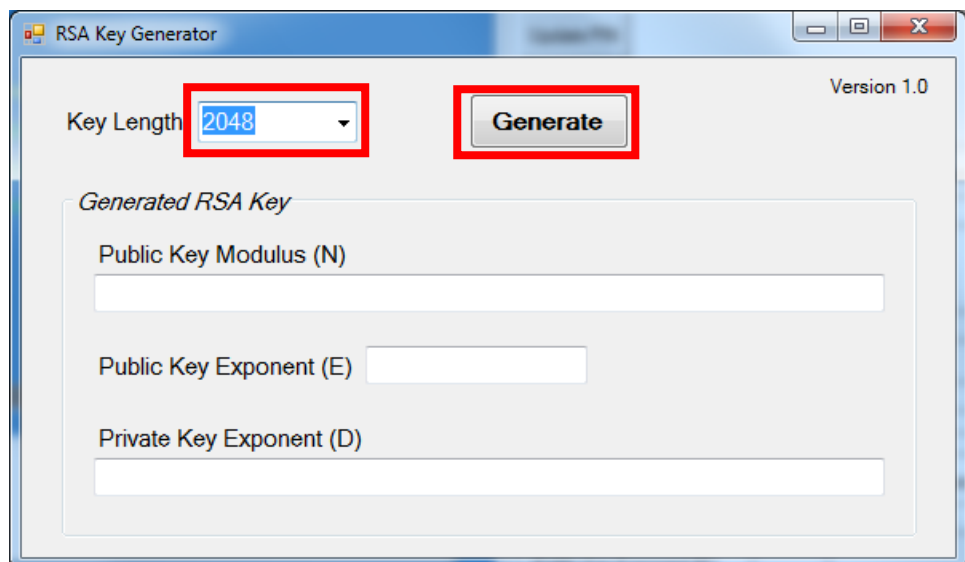
- To view current key set hash value, goto “Option” and select key.



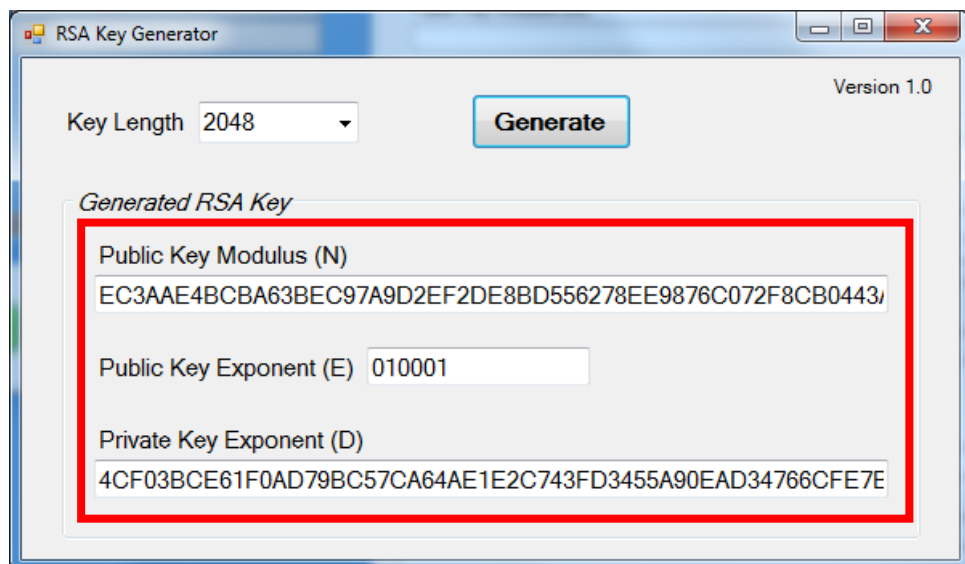
- To generate new user key set
 - Run RSA Key Generator



- Select Key Length as 2048 (bits), then press [Generate] button to generate the RSA key set.



Result:



- Copy RSA key components to RSA Key for Kenc in Secure Key Generator.

VEGA5000S Secured Key Generator (RSA) v1.9.2

File Option Help

File Information

File Name

App Name: Secure Key

App Version: 0001

Company:

Make Key CAP File

New Key

Update PIN

Get Hash

Save to Card

Reset

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA63BEC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF03BCE61F0AD79BC57CA64AE1E2C743FD3455A90EAD34766CFE7BD4C9

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.

VEGA5000S Secured Key Generator (RSA) v1.9.2

File Option Help

File Information

File Name

App Name: Secure Key

App Version: 0001

Company:

Make Key CAP File

New Key

Update PIN

Get Hash

Save to Card

Reset

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA63BEC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF03BCE61F0AD79BC57CA64AE1E2C743FD3455A90EAD34766CFE7BD4C9

HASH

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

99EC9F3750CDD8AAE26F374C4B3108D89EAD4691E0DFAB7FF2DEA0158

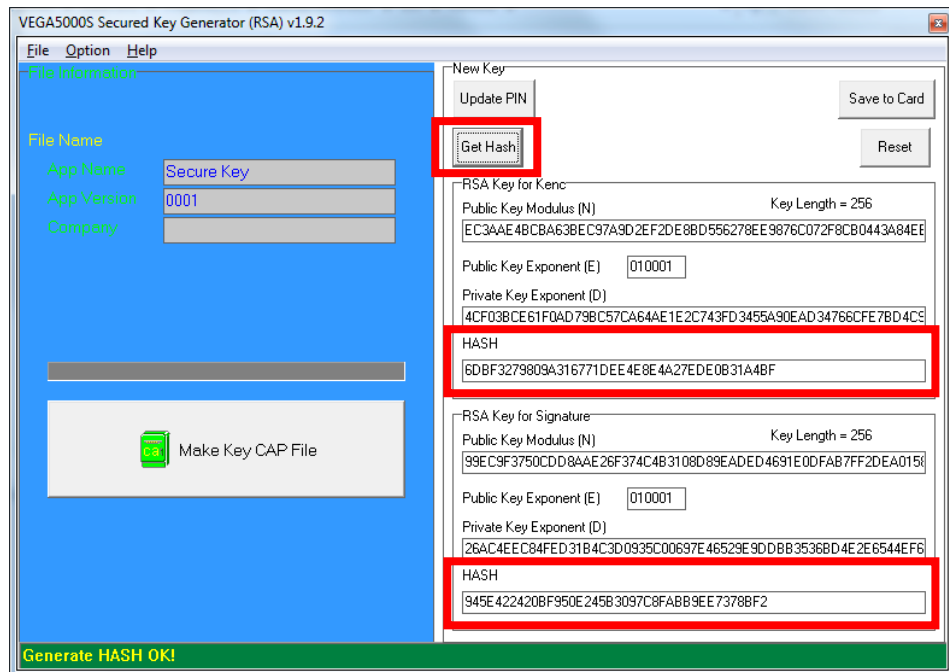
Public Key Exponent (E) 010001

Private Key Exponent (D)

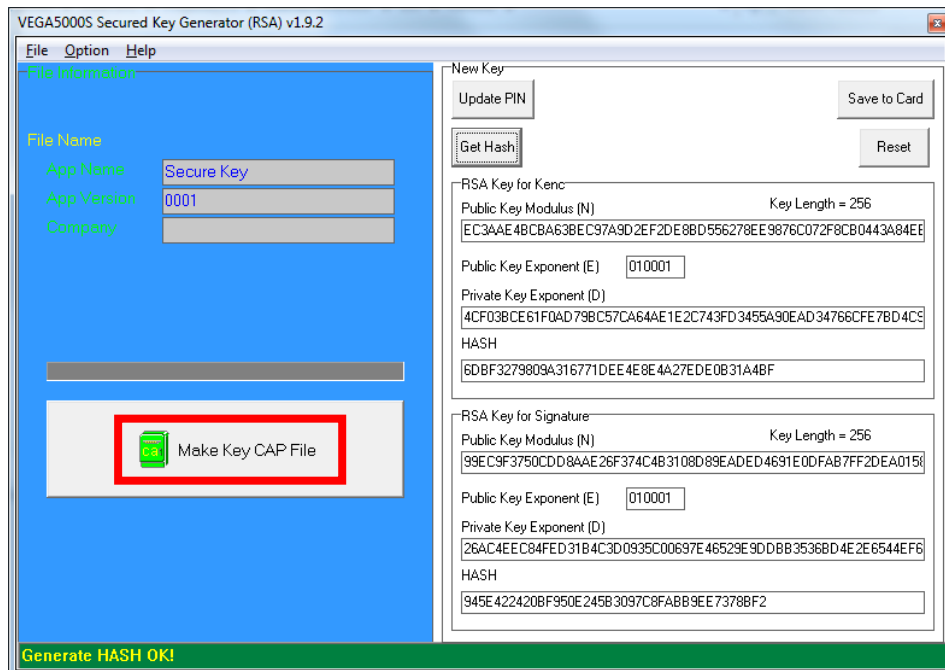
26AC4EEC84FED31B4C3D0935C00697E46529E9DD8B35368D4E2E6544EF6

HASH

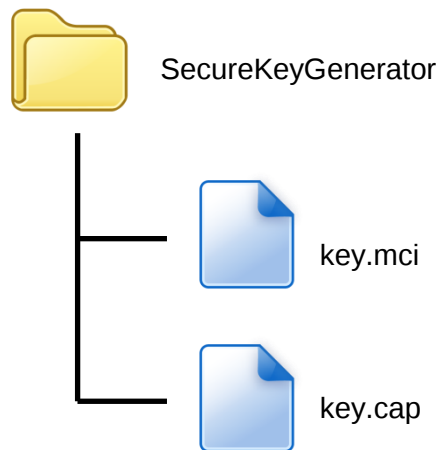
- Click [Get Hash] button to calculate the hash value for key sets.



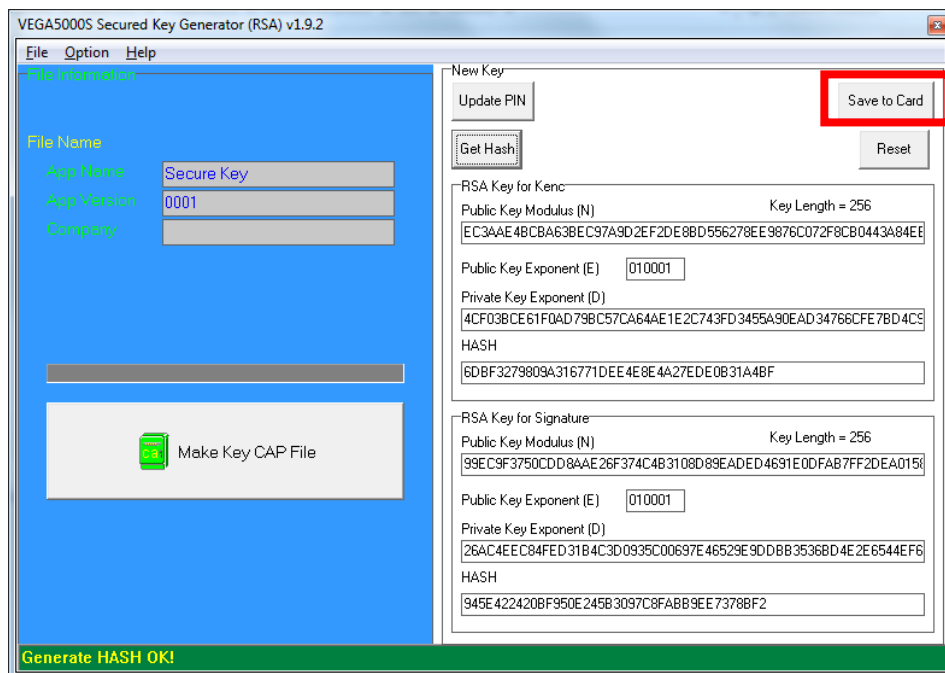
- Please copy down all the values into a text file and keep in a safe place. You will need this if you need to create duplicate Key Card.
- To generate the key CAP for the newly generated user key set, press [Make Key CAP File] button.



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



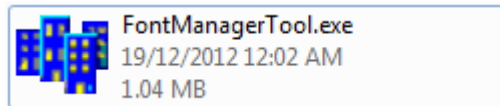
- To update the newly generated key set to Key Card, press [Save to Card] button to write the key set to Key Card.



5. Font Management

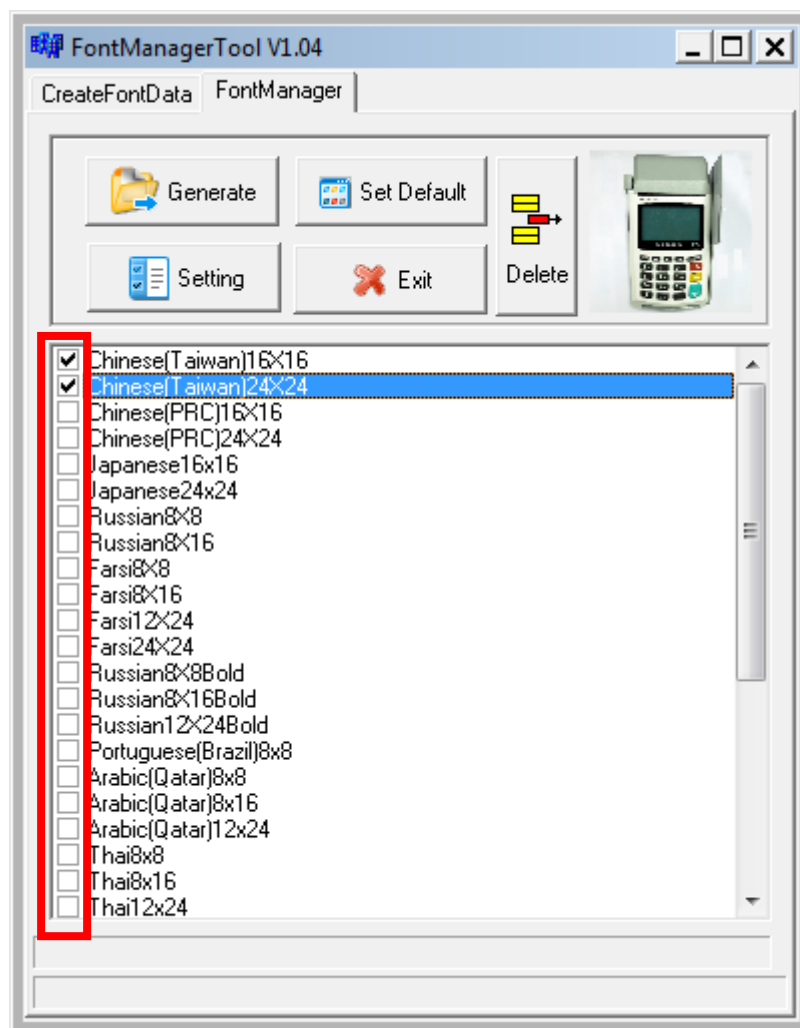
5.1. Loading New Font

- Run FontManager.exe

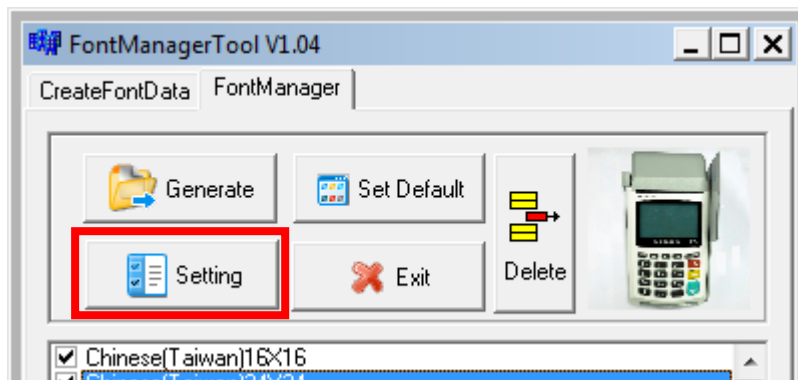


Located at C:\Program Files\Castles\Font Manager

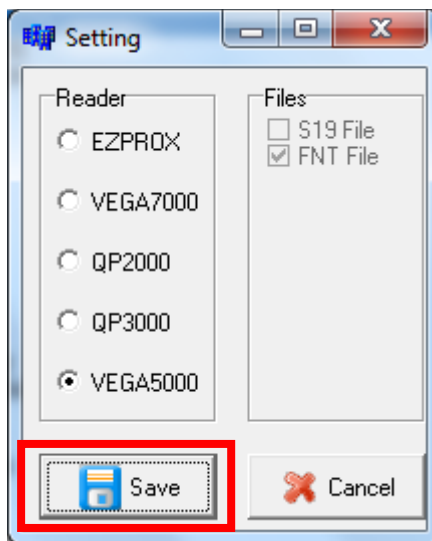
- Select font to download



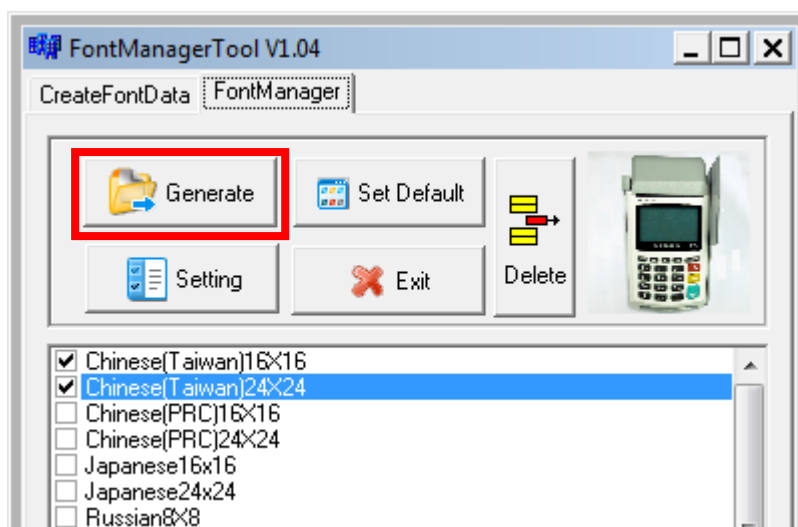
- Press [Setting] button to configure terminal type.



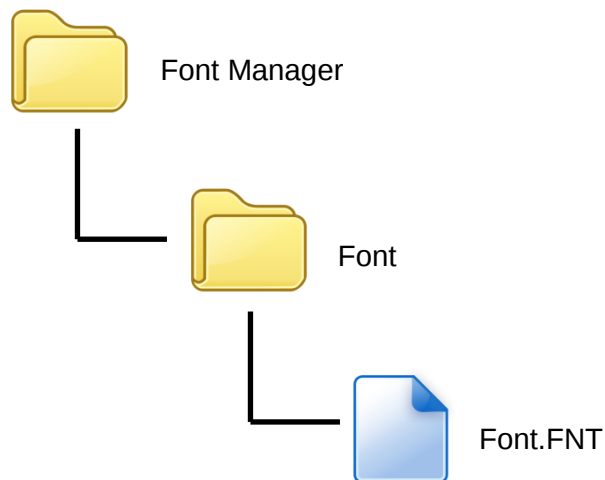
- Select **VEGA5000**, press [Save] button to save and return font manager.



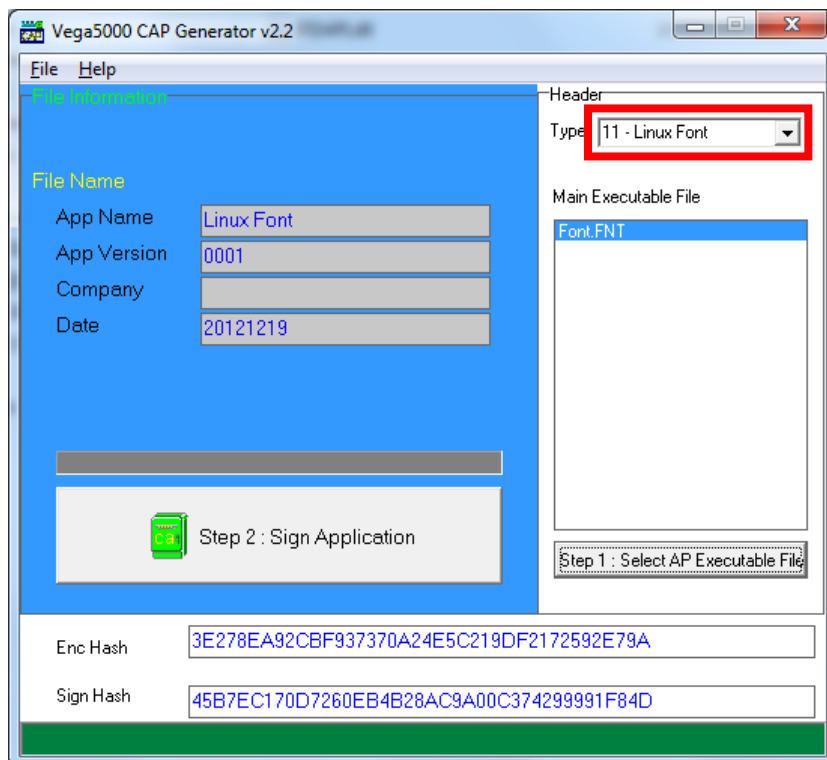
- Press [Generate] to create the font file.



- 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.

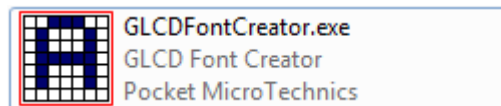
There are two zone defined:

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

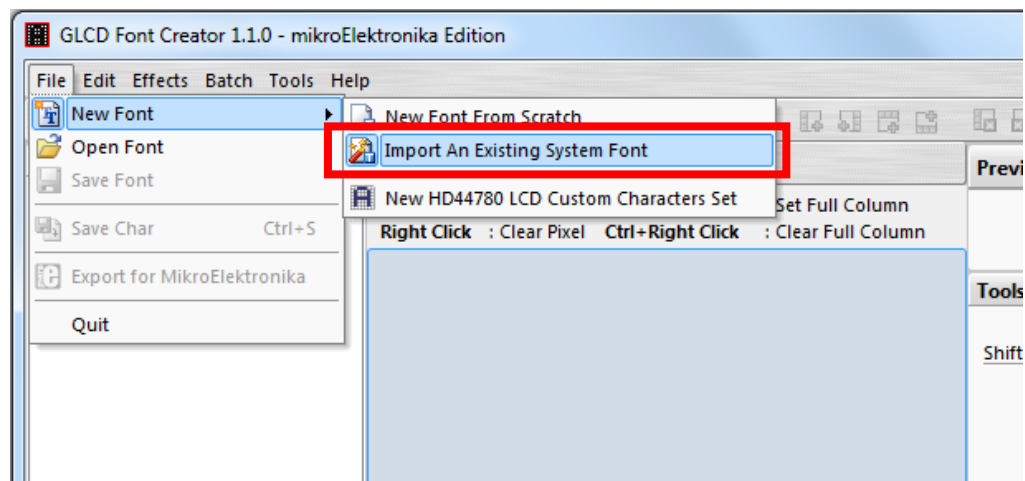
Zone 0x80 ~ 0xFF – Free to use, you may use for symbols.

Following steps demonstrate how to create a 12x24 font.

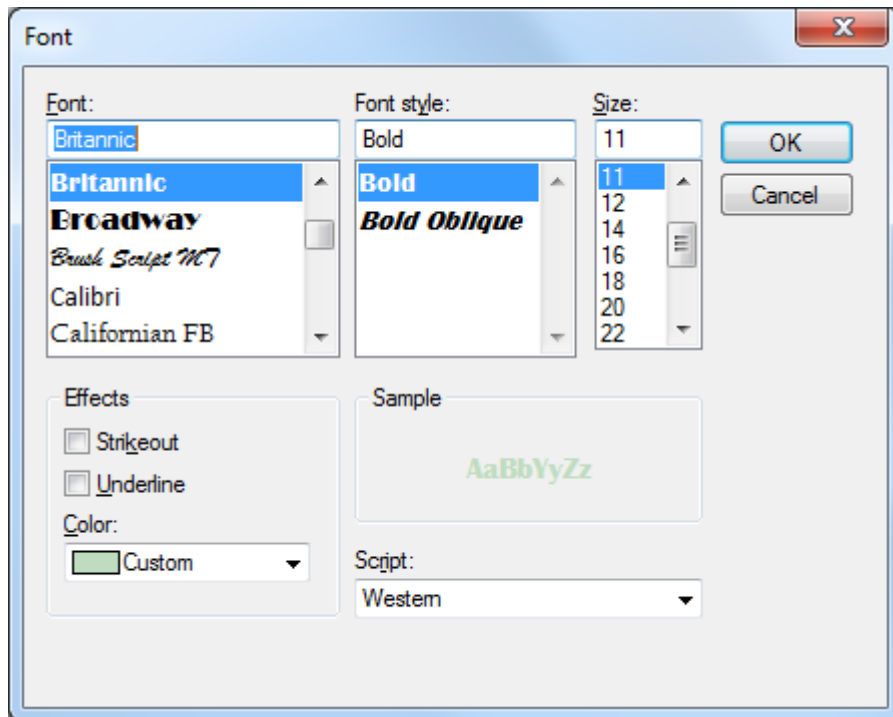
- Run GLCD Font Creator



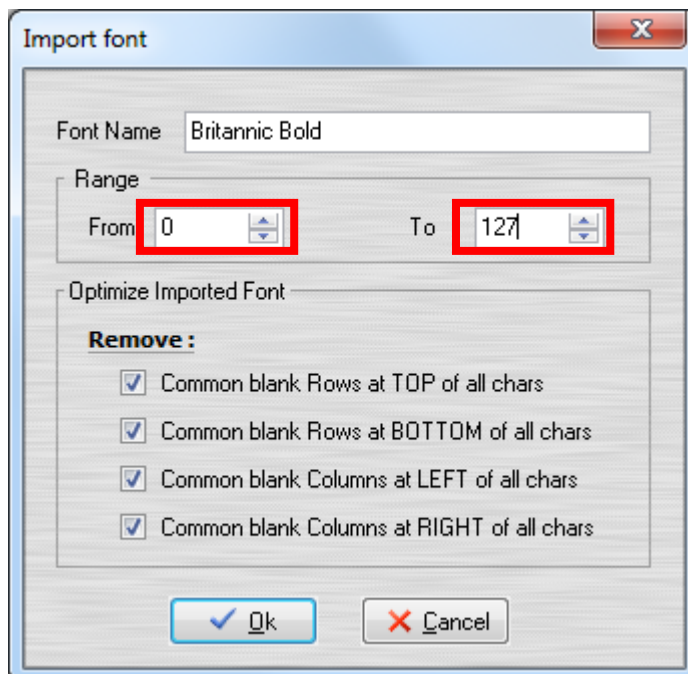
- Select [File] ⇒ [New Font] ⇒ [Import An Existing System Font]



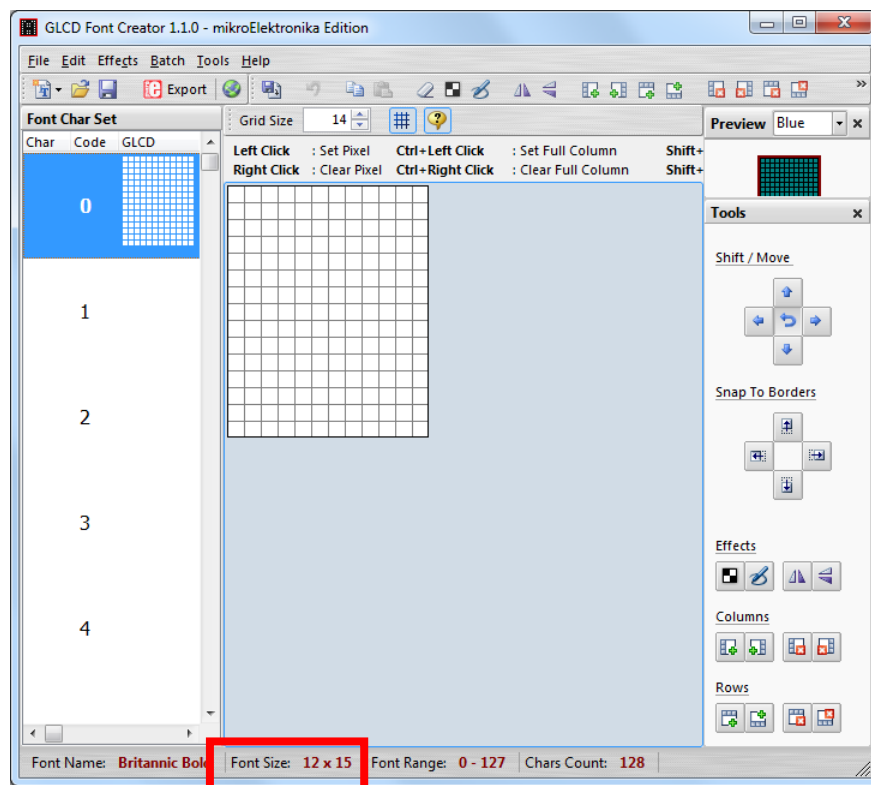
- Select the font needed, simply choose a font size. The final value of font size should be determine by the minimum pixel width. You may need to repeat this steps few times to find the best fit font size.



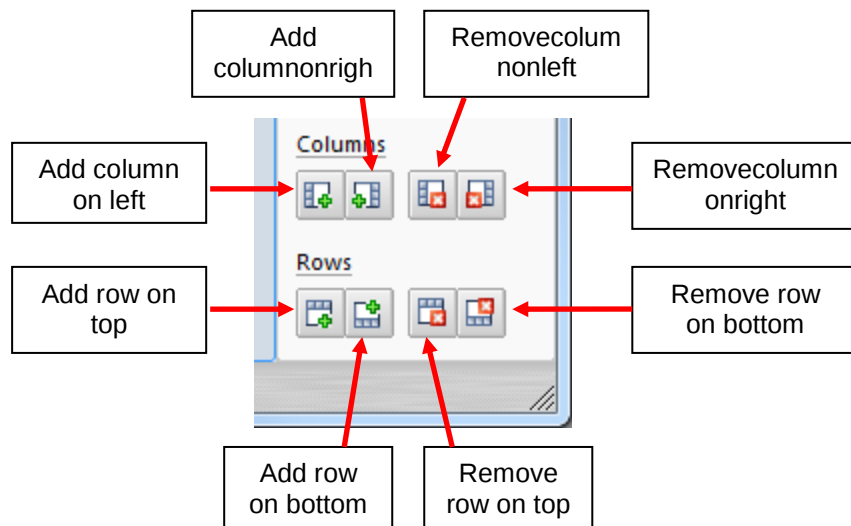
- Set the import range from 0 to 127.



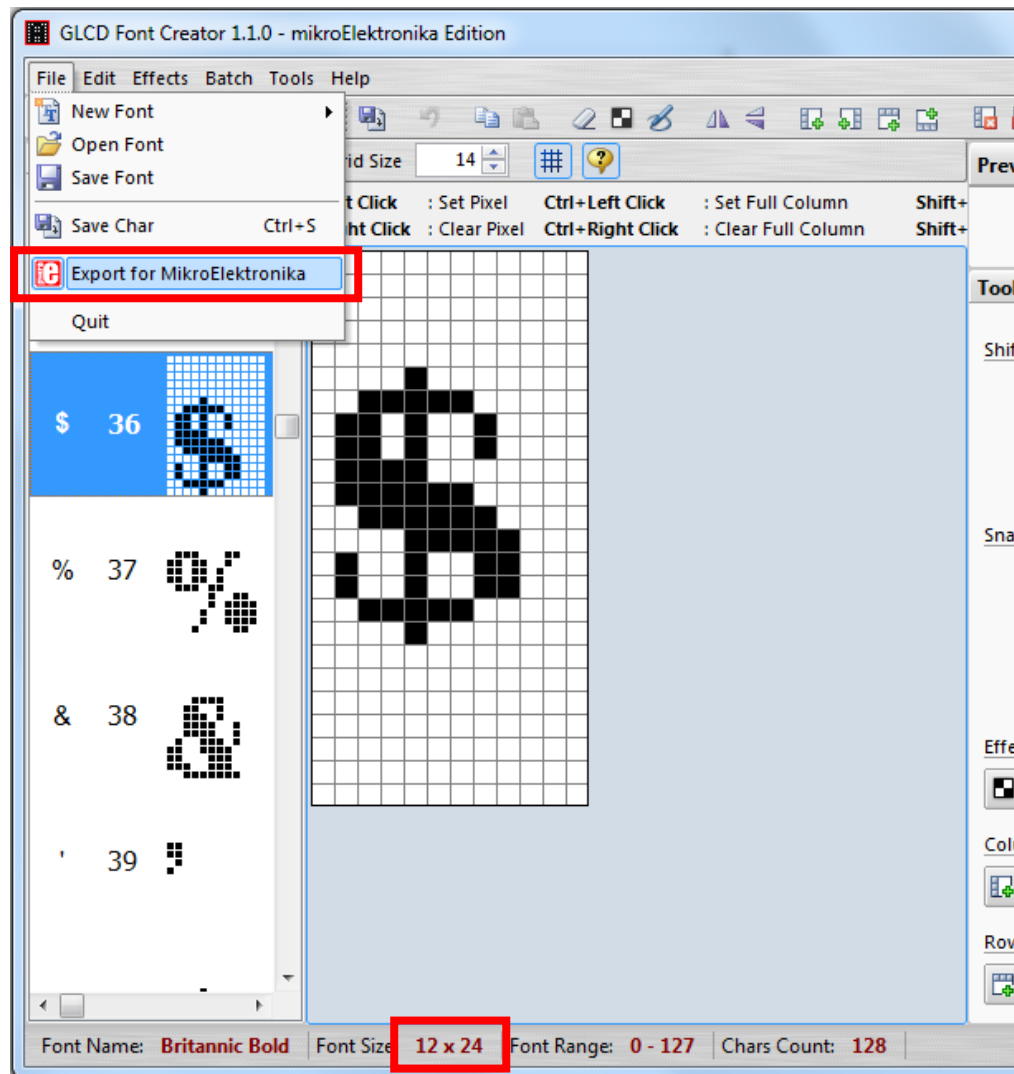
- Check the minimum pixel width and height.



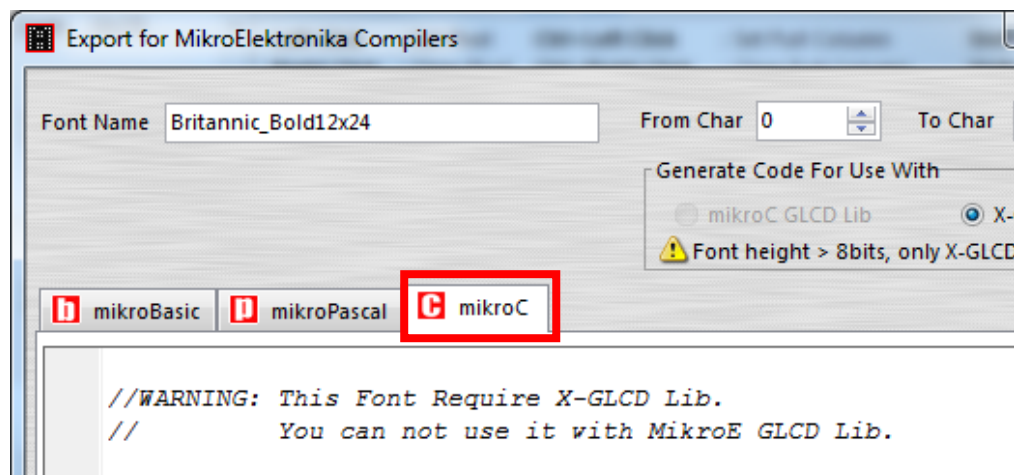
- If the pixel width of the font size is larger than expected, then you have to repeat the previous steps to import font with smaller size.
- Use the following buttons to adjust the font size to match with expected font size.



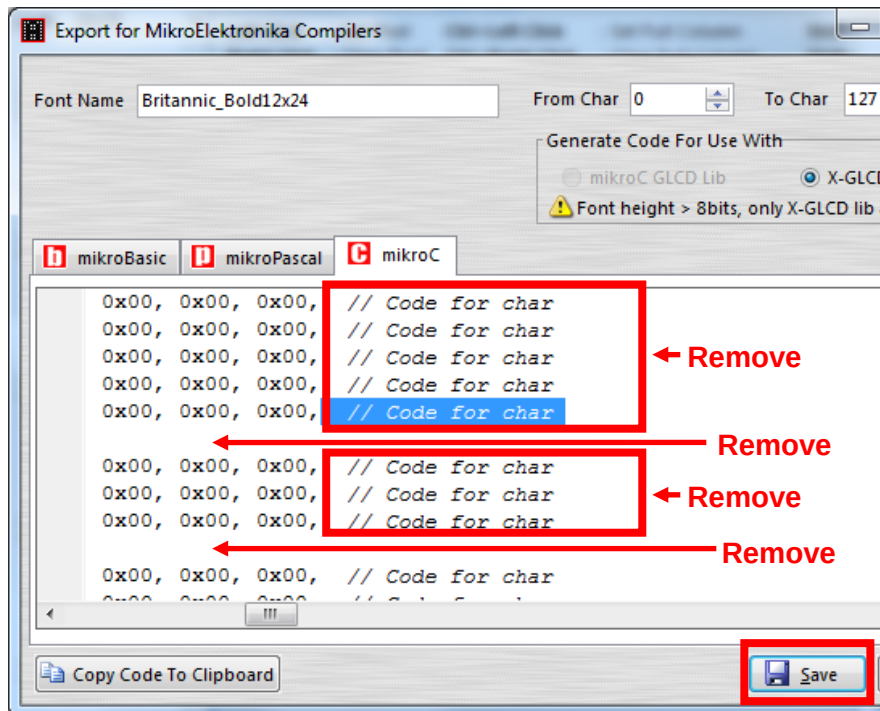
- After adjust font size, select [File] ⇒ [Export for MikroElektronika].



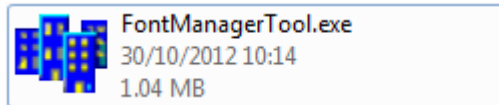
- Select output format as [mikroC].



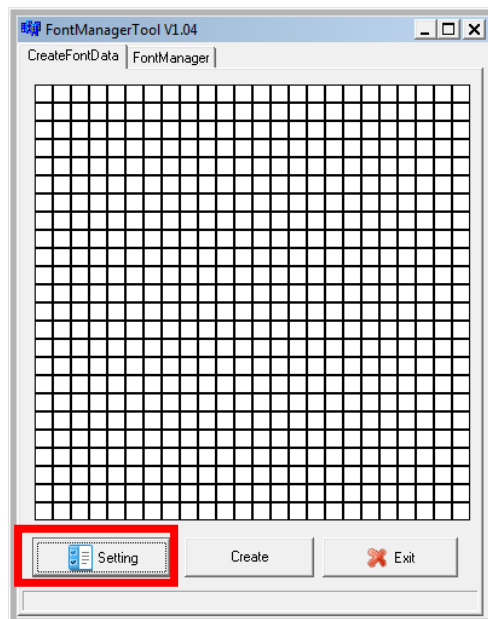
- Remove comment “// Code for char ” from offset 0x00 to 0x1F. Remove empty line if found. Then click [Save] button to save to file.



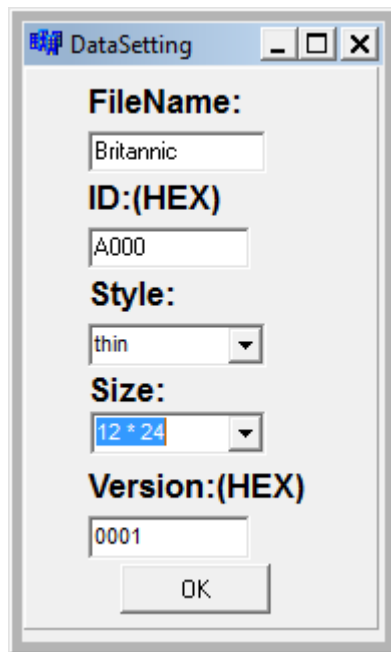
- Run Font Manager Tool.



- Click [Setting] button

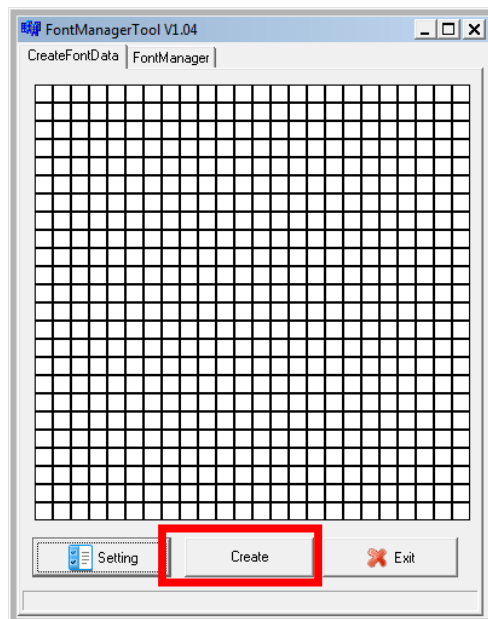


- Enter the file name, font id, and select the size.



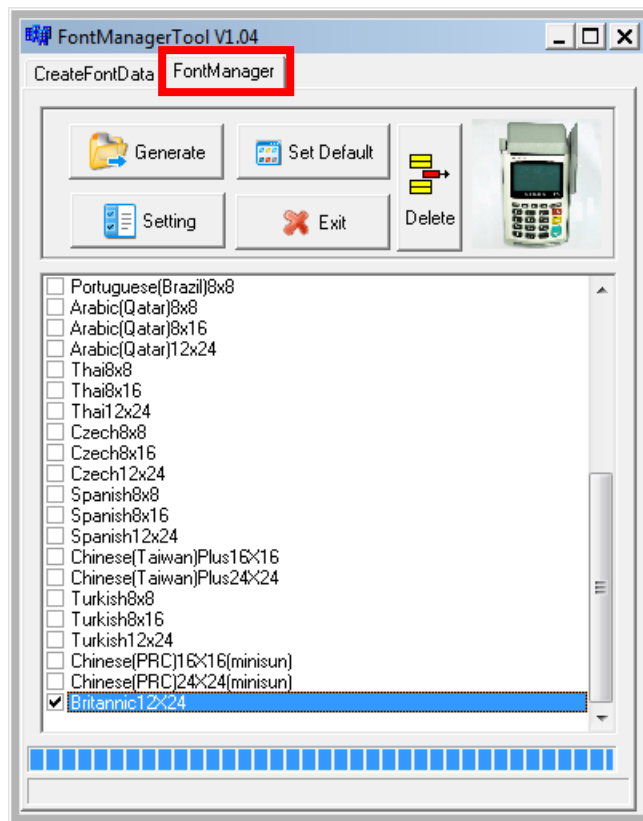
The image shows a dialog box titled "DataSeting". It contains several input fields and a dropdown menu. The "FileName:" field contains the text "Britannic". The "ID:(HEX)" field contains the text "A000". The "Style:" dropdown menu is set to "thin". The "Size:" dropdown menu is set to "12 * 24". The "Version:(HEX)"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

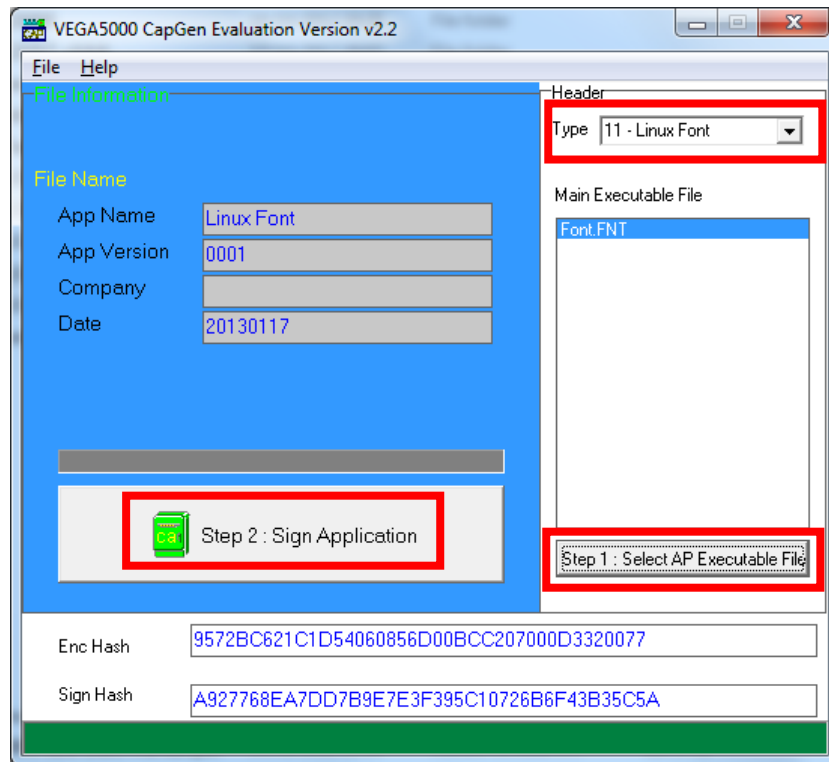


The image shows a window titled "FontManagerTool V1.04". It has a tabbed interface with "CreateFontData" and "FontManager" tabs. The "CreateFontData" tab is active, showing a large grid of small squares. At the bottom, there are three buttons: "Setting", "Create", and "Exit". The "Create" button is highlighted 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.

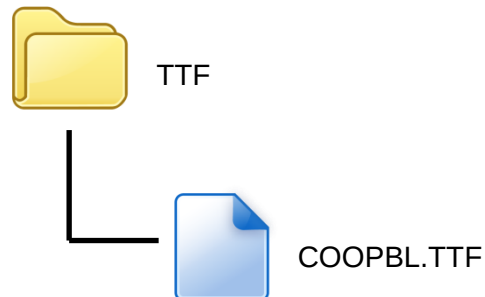
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

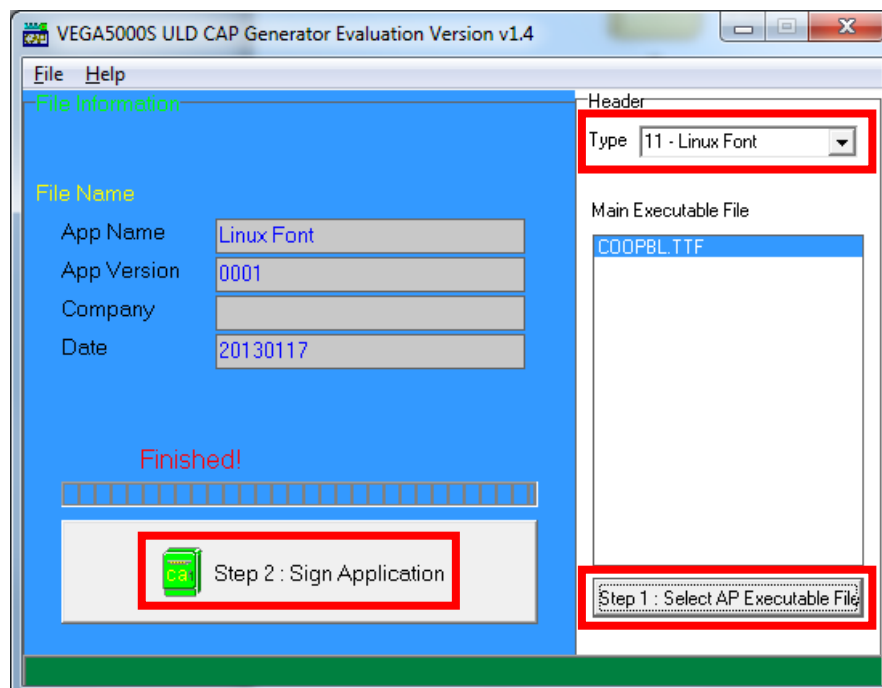
TrueType Font (TTF) is only supported in VEGA5000S terminal. You may download the TrueType font preferred to terminal for displaying or printing.

Following steps demonstrate how to use “Cooper Black” True Type 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. Advance Features

6.1. VEGA5000S GNU Project Debugger (GDB)

Developers may use GDB to debug the programs directly on VEGA5000Sterminal.

6.1.1. About GDB

GDB, the GNU Project debugger, allows you to see what is going on 'inside' another program while it executes -- or what another program was doing at the moment it crashed.

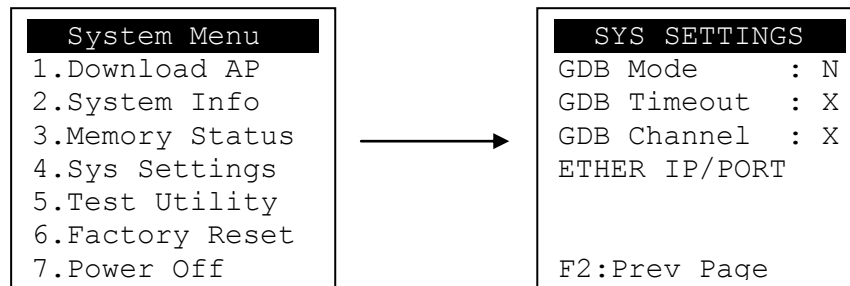
GDB can do four main kinds of things (plus other things in support of these) to help you catch bugs in the act:

- Start your program, specifying anything that might affect its behavior.
- Make your program stop on specified conditions.
- Examine what has happened, when your program has stopped.
- Change things in your program, so you can experiment with correcting the effects of one bug and go on to learn about another.

For more detail, please refer to <http://sources.redhat.com/gdb/>.

6.1.2. SetupGDB

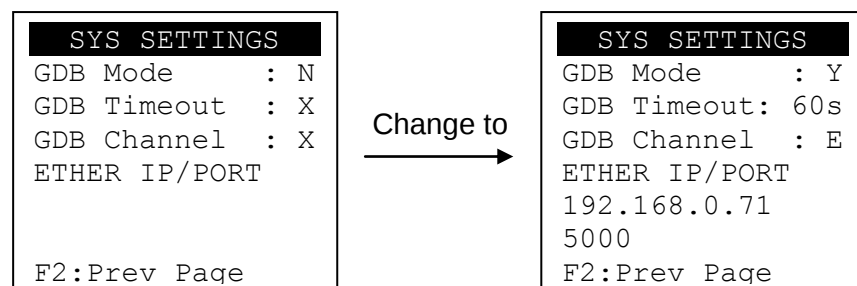
Access to GDB Setting Menu.



- Press [4] button to enter System Settings menu.
- Press [F3] button three times to GDB Setting Menu (page 4).

Change following settings:

- Set GDB Mode to Y (enable)
- Set GDB Timeout, the time that GDB server (on terminal) waits for connection. Default is 60 seconds.
- Set GDB Channel, the communication channel between GDB server (on terminal) and SDK IDE on PC.
'E' indicates to use TCP/IP channel
'U' indicates USB mode
- Set Ethernet IP & Port, terminal IP address and GDB server (on terminal) port. If communication channel is set to TCP/IP.



- Press [▲▼] button to select setting.
- Press [OK] button to change the setting value.
- Press [↔] button to toggle Y ⇌ N ⇌ Y.

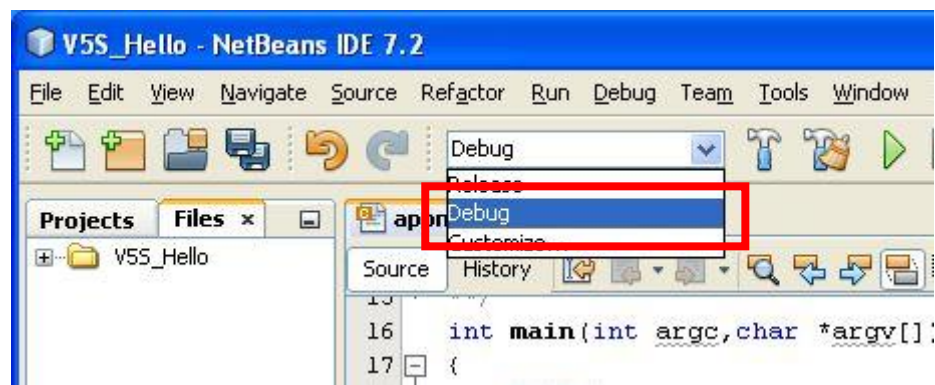
6.1.3. Start Debugging

The GDB function is supported in the Castles SDK version 6.10 or higher. Please ensure you have already installed this SDK into your computer before using GDB.

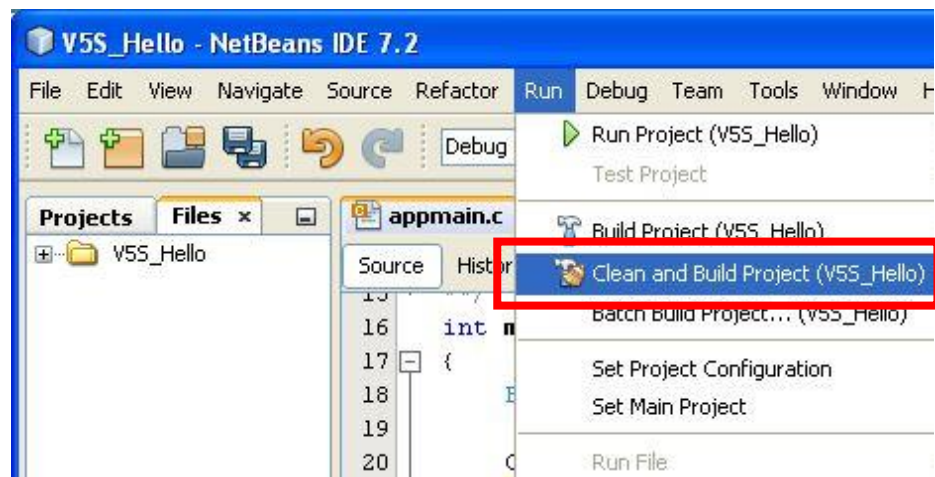
Step 1: Run Castles CTOS Development Suite

Step 2: Open project to debug

Step 3: Set project configuration to “Debug”



Step 4: Rebuild the project.



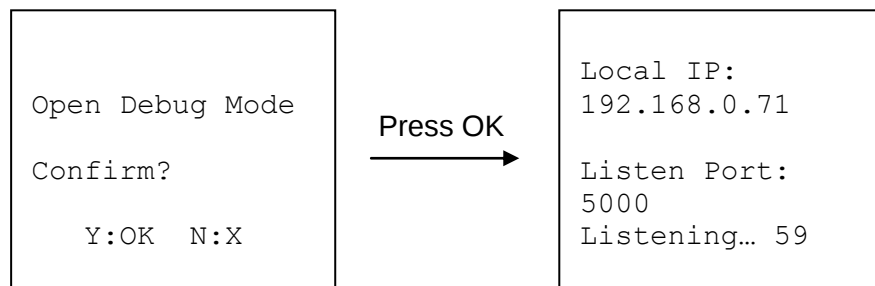
Step 5: Sign the application and load the CAP files to terminal.

```
Program Manager
-----01/02
1.V5S_Hello

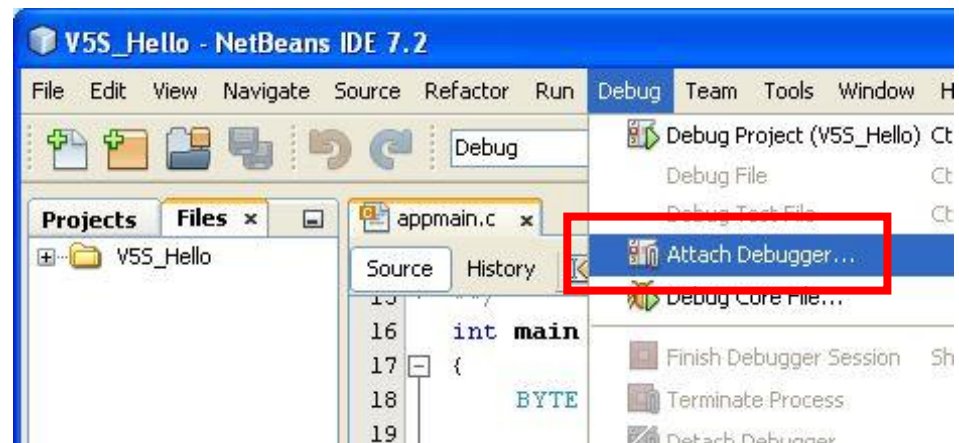
F1:Download
```

Step 6: Execute the application.

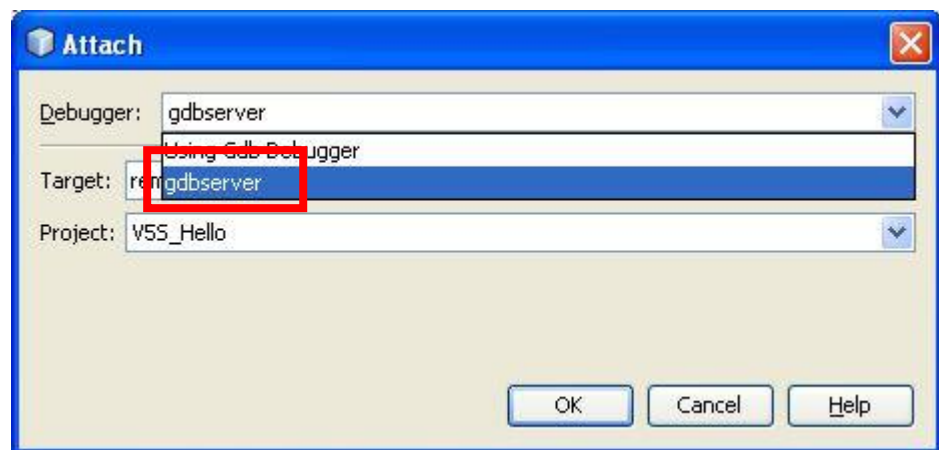
Step 7: Press [OK] button to confirm open debug mode. Terminal will wait for connection from SDK IDE until timeout.



Step 7: In SDK IDE, from Debug menu select “Attach Debugger...”.



Step 8: Select debugger as “gdbserver”.



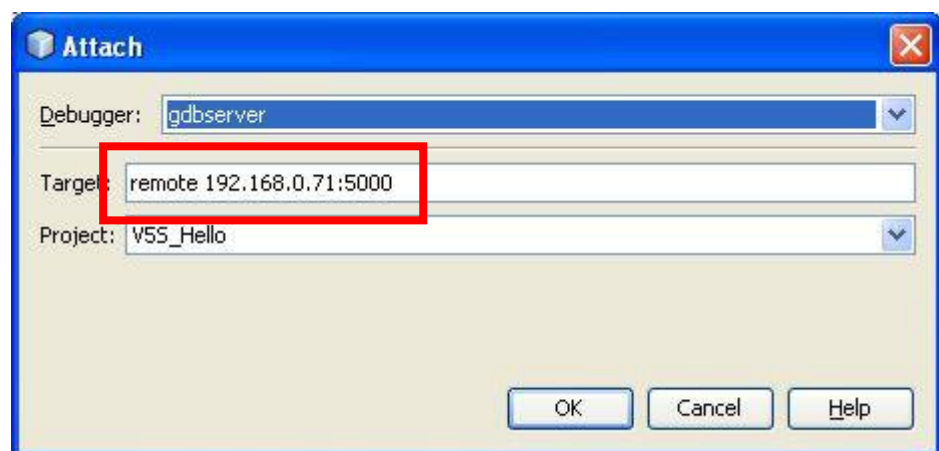
Step 8:

Ethernet Channel:

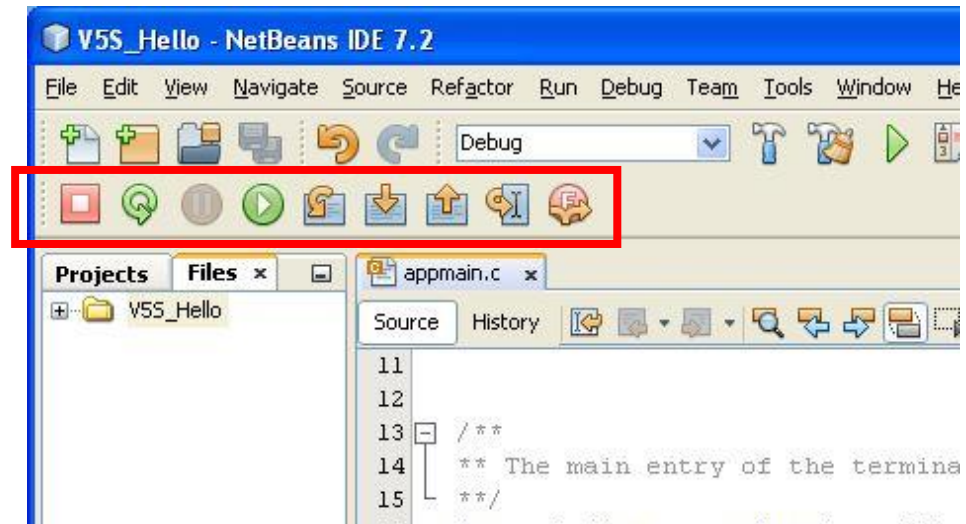
Please input the terminal IP address and GDB port in the format “remote HostIP:HostPort” on the “Target” editor. And select your application from the “Project” combobox. When finishing, press ‘OK’ button to connect with the terminal.

USB Channel:

If using USB channel to debug, input port number in the format “remote/dev/ttySn” on the “Target” editor. ‘n’ indicates comport number minus 1. For example, if the PC port that the terminal connects with is COM3, please input “remote /dev/ttyS2” on the “Target” editor. And select your application from the “Project” combobox. When finishing, press ‘OK’ button to connect with the terminal.



Step 9: Press OK. After successful connected to terminal, the debug menu will be enable. User may use breakpoint or use “Step Over” for tracing.



7. Operation Notes

7.1. Operation Notes

1. VEGA5000S mainly used both on table and hand-held.
2. When inserting or swiping the cards, there will be some distance between the terminal and human body, rather than be appressed to the human body.
3. The VEGA5000S would not be put into the pocket or tie around the waist.

~ END ~

FCC Regulations

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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This device should be installed and operated with minimum distance 10 mm between the radiator & your body.