CASTLES TECHNOLOGY

VEGA3000 EFT-POS Terminal / Pinpad

Book 2

User Manual

Confidential

Version1.29

AUG 2016

Castles Technology Co., Ltd.

2F, No. 205, Sec. 3, Beixin Rd., XindianDistrict,
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.

Revision History

Version	***Date***	***Descriptions***
1.0	May 27, 2014	Initial creation.
1.1	Aug 26, 2014	Add the description of new items of PM. 1. Bluetooth Setup. 2. Plug-in Mng.
1.2	Sep 10, 2014	Extend the terminal part to terminal / pinpad of this document.
1.21	Jul 3, 2015	Modify the description of V3CT rear side.
1.22	Jul 13, 2015	Modify the description of V3PT front and base(2.1). Modify the system info menu(3.3).
1.23	Jul 14, 2015	Add 2.7 Parts of the PinPad (Hardware)
1.24	Jul 24, 2015	Add Key Injection in System Menu(3.18).
1.26	Oct 8, 2015	Add Key Injection description(3.18).
1.28	May 26, 2016	Add description of COM port(2.1 & 6.1).
1.29	Aug 31, 2016	Revise COM1 from RJ11 to RJ9 (6.1)

Contents

1. Introduction

This document provides a guideline on operating and configuring Castles VEGA3000 terminal / pinpad.

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

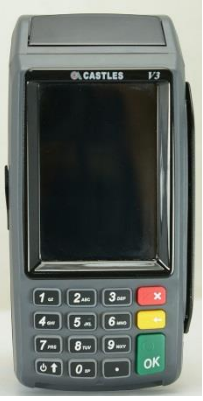
1.1. Type of Terminal

There are two types of VEGA3000 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, WiFi, Bluetooth 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

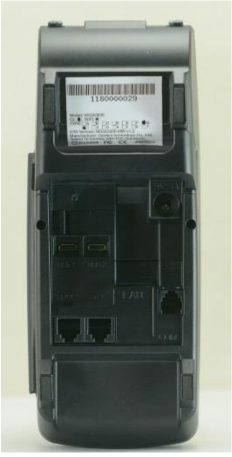
Rear View

Side View

Countertop type integrates all components into a single piece of hardware. Optional contactless reader, WiFi, Bluetooth and GRPS/UMTS modem is supported. The constraint is the countertop terminal can only housing up to four communication modules from selection of dial-up modem, Ethernet, WiFi/Bluetooth(one of them) and GPRS/UMTS modem.

Front View

Rear View



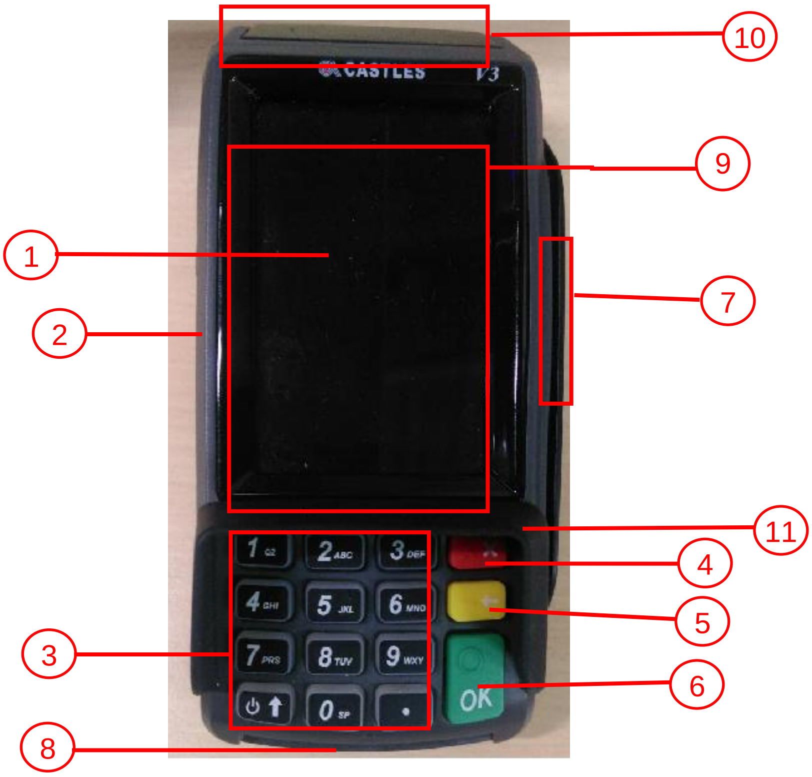
Side View

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

2. Hardware Setup (Portable and Countertop)

2.1. Parts of the Terminal

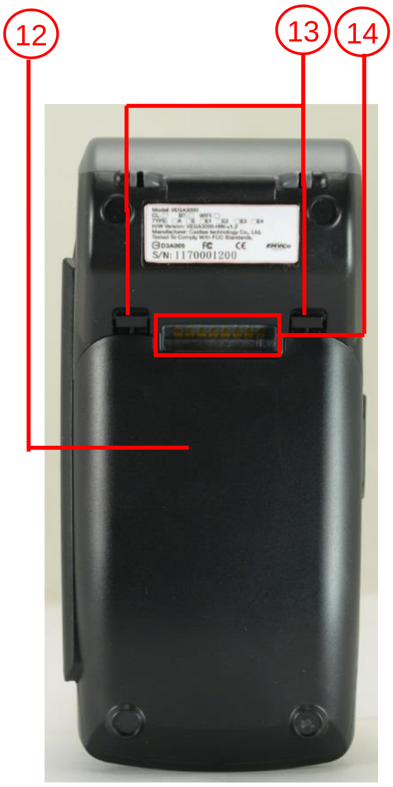
Front (Portable and Countertop)



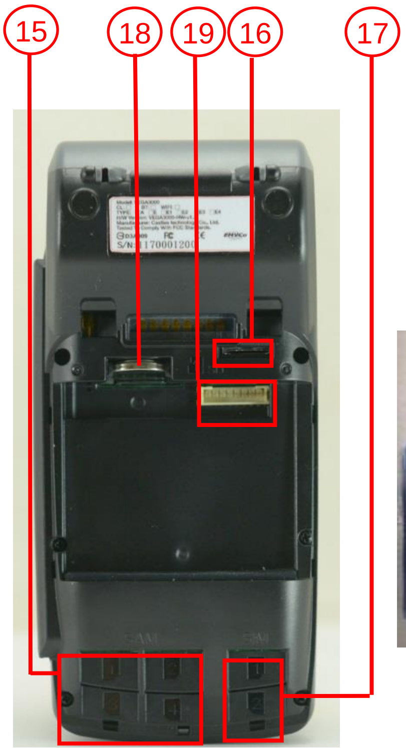
VEGA3000

1. **LCD Display (Color TFT)**
2. **Micro USB Cover**
3. **Keyboard(Power button on lower right conner)**
4. **Cancel Key**
5. **Clear Key**
6. **Enter Key**
7. **Magnetic Stripe Reader**
8. **Smart Card Reader**
9. **Contactless Card Landing Zone**
10. **Paper Roll Handle**
11. **Privacy Shields**

Rear (Portable)



VEGA3000



VEGA3000

VEGA3000
Rechargeable
Battery

12. RechargeableBattery Cover

13. Battery Cover Lock

14. Base Connector

15. SAM Slots

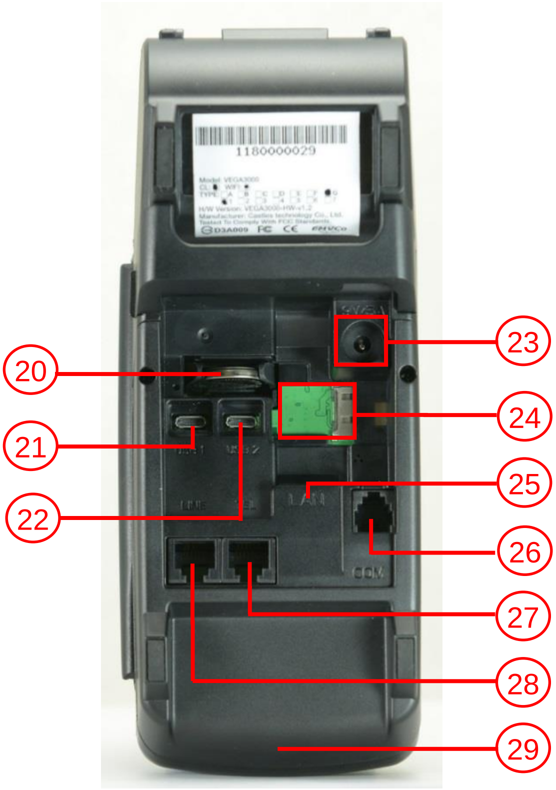
16. Micro SD Card Slot

17. GSM SIM Card Slots

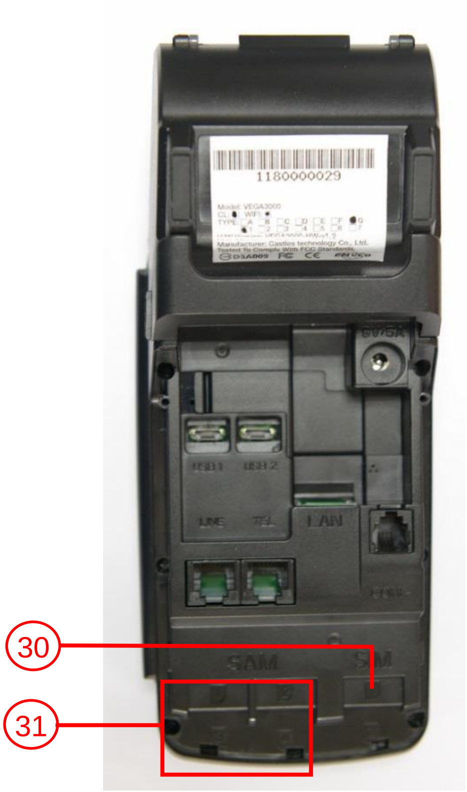
18. RTC Battery

19. Battery Connector

Rear (Countertop)



VEGA3000



VEGA3000

20. RTC Battery

21. USB Port

22. USB Port 2

23. Power Connector

24. Micro SD Card Slot

25. Ethernet Port

26. Com port 1 (4pin 9V/500mA**)**

27. Com port 2 (6pin 5V/1A**)**

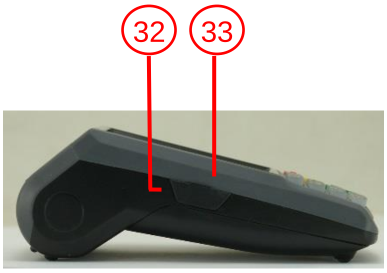
28. Modem – Line

29. Back Cover

30. SAM Card Slots

31. GSM SIM Card Slots

Side



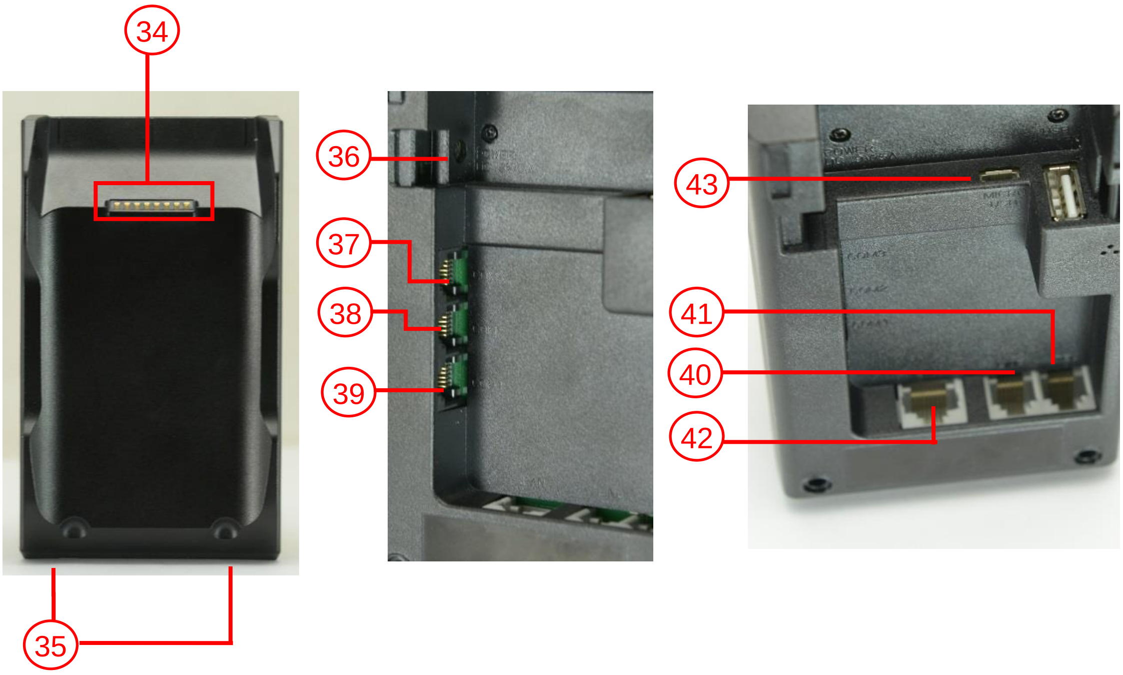
VEGA3000 Portable

VEGA3000 Countertop

32. Power Connector

33. USB Port

Base (Portable)



34. Base Connector

35. Base LED

36. Power Connector

37. Com port 1

38. Com port 2

39. Com port 3

40. Modem - Line Port

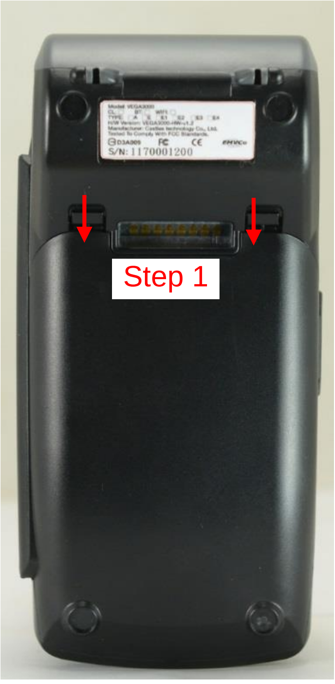
41. Modem – Tel Port

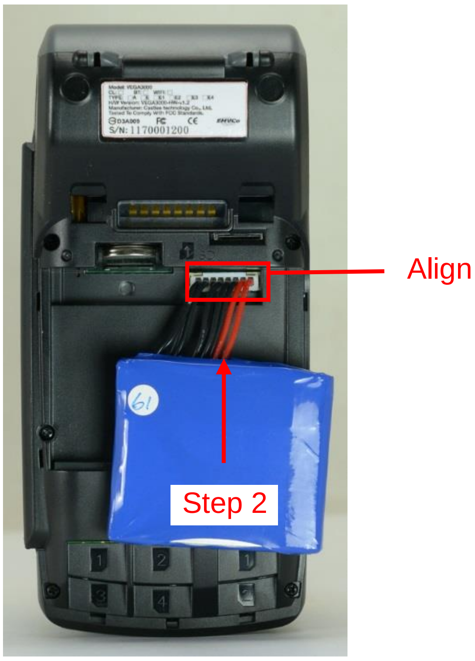
42. Ethernet Port

43. Micro USB Port

The 3 com ports can only afford grand total 2A, they use the same power supply path.

2.2. Inserting the Battery

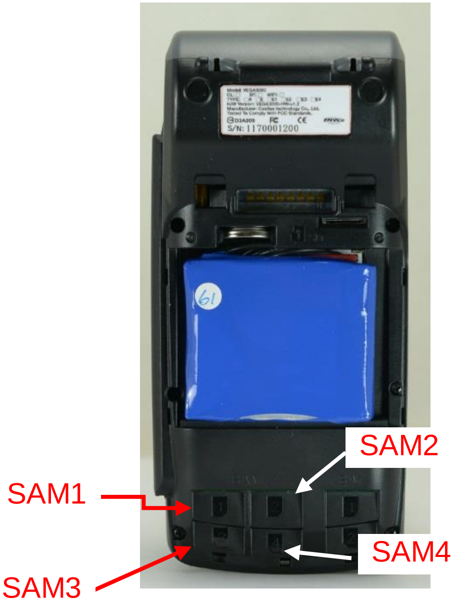




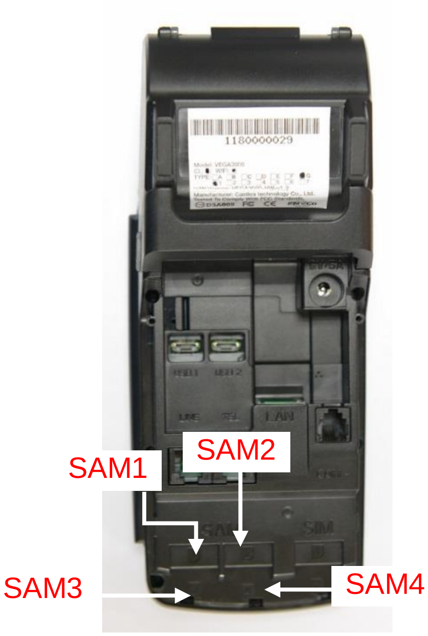
Step 1: Remove battery cover

Step 2: Insert battery into compartment, battery contact point must align with battery connector.

2.3. Inserting the SAM Card



VEGA3000 Portable



VEGA3000 Countertop

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

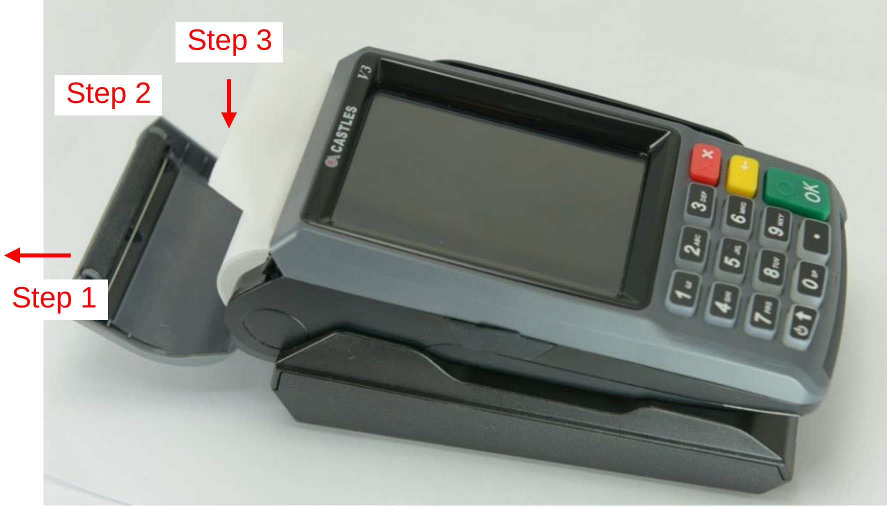
SAM 1 & 2 & 3:

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: Pull up paper roll box handle.

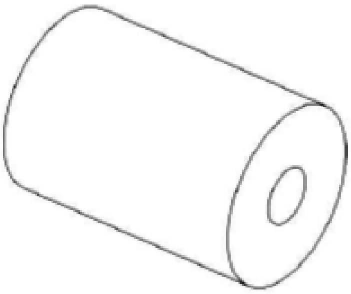
Step 2: Gentle open paper roll cover.

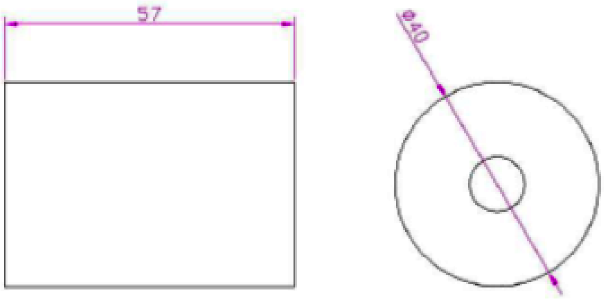
Step 3: Insert paper roll as direction showed.

Paper specification

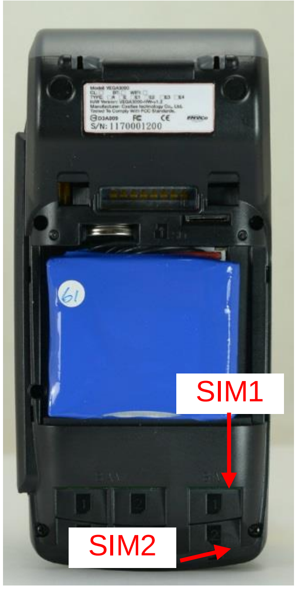
Width: 57mm

Outside diameter: 40mm

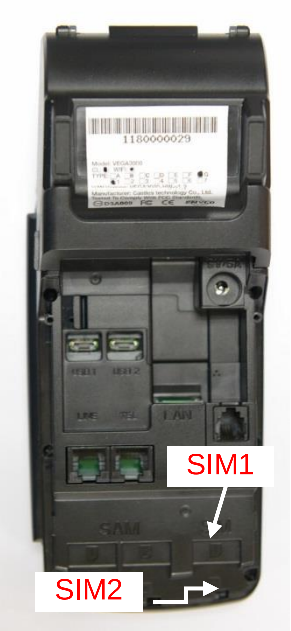




2.5. Inserting the GSM SIM Card



VEGA3000 Portable

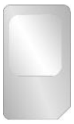


VEGA3000 Countertop

Step 1: Remove battery cover / back cover

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

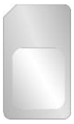
Portable



SIM 1 & 2:

Gold contact at upper side of card and facing down.

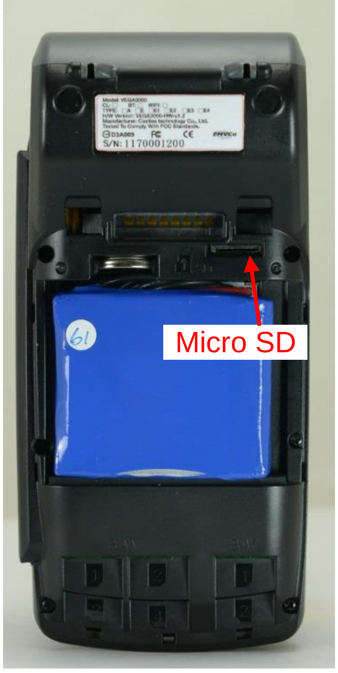
Countertop



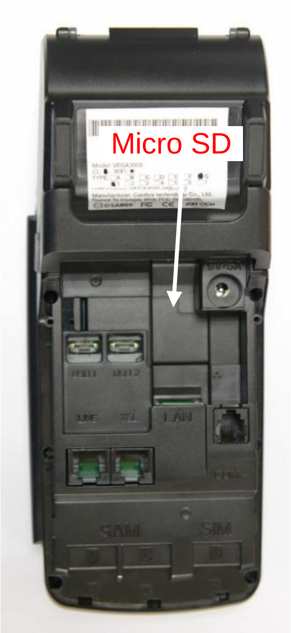
SIM 1 & 2:

Gold contact at lower side of card and facing down.

2.6. Inserting the Memory card



VEGA3000 Portable

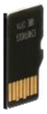


VEGA3000 Countertop

Step 1: Remove battery cover / back cover

Step 2: Insert Micro SD memory card.

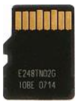
Portable



Micro SD:

Gold contact at lower side of card and facing right.

Countertop

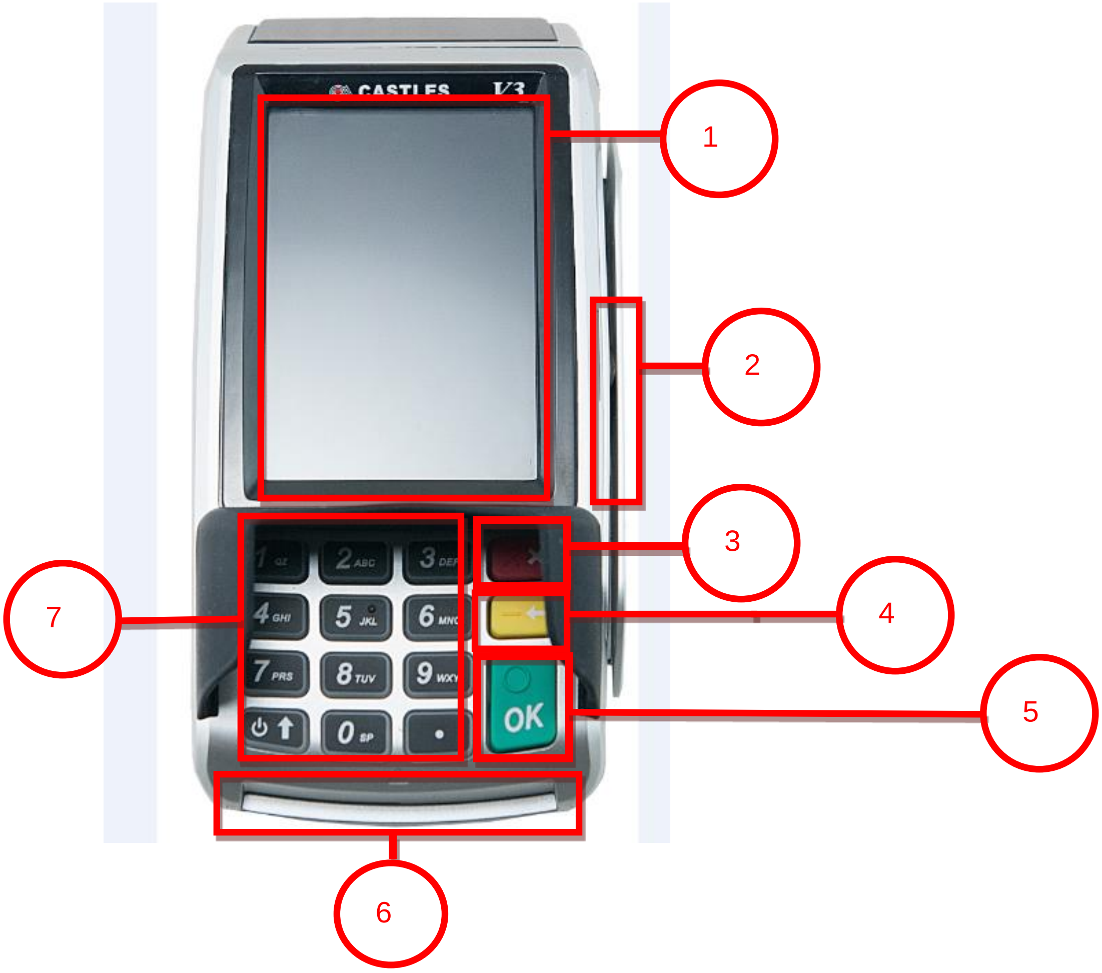


Micro SD:

Gold contact at upper side of card and facing up.

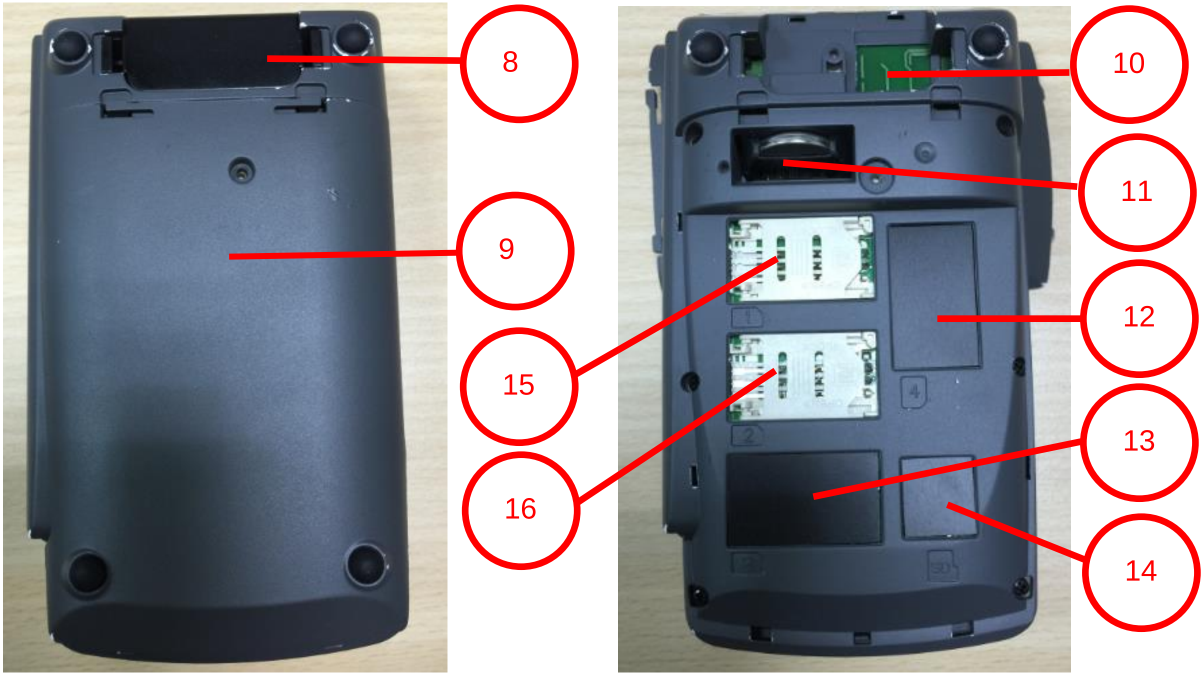
2.7. Parts of the PinPad

Front (*PinPad*)



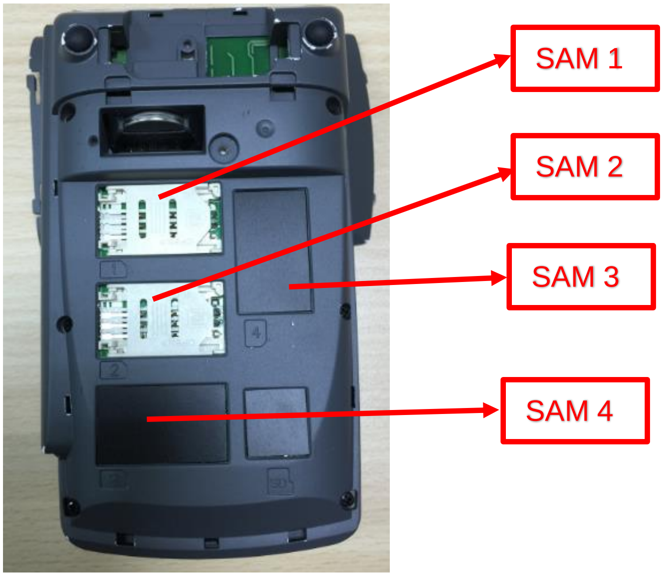
1. **LCD Display (Color TFT)**
2. **Magnetic Stripe Reader**
3. **Cancel Key**
4. **Clear Key**
5. **Enter Key**
6. **Smart Card Reader**
7. **Keyboard**

Rear (*PinPad*)



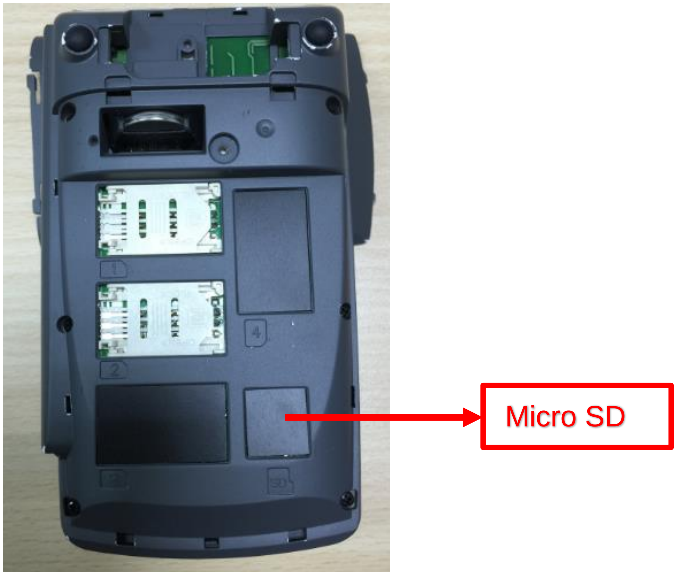
8. Battery Cover Lock
9. Back Cover
10. HDMI
11. RTC Batter
12. SAM Slot
13. SAM Slot
14. Micro SD Card Slots
15. SAM Slot
16. SAM Slot

2.7.1. Inserting the SAM Card (Option)



1. Step 1: Remove back cover
2. Step 2: Insert SAM card into desire slot.

2.7.2. Inserting the Memory card (Option)



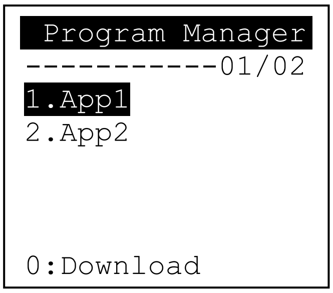
1. Remove back cover
2. Insert Micro SD memory card

3. Basic Operation

3.1. Program Manager

Once the power is on in normal status, terminal / pinpad will enter Program Manager if no default application selected. All user applications are listed in Program Manager. Users can select an application and run the application, view the application info, delete the application, or set application to the default one to run once the power is on. Users may enter System Menu to configure terminal /pinpad settings.

Program Manager

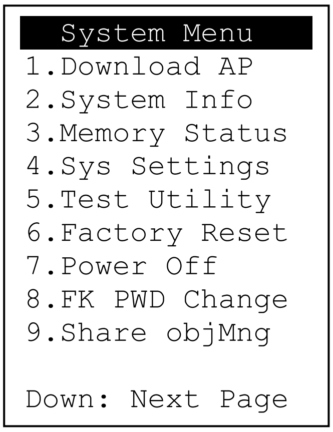


```
 Program Manager
-----------01/02
1.App1
2.App2



0:Download
```

- 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 [Power] or [·] as the up and down button to select application.

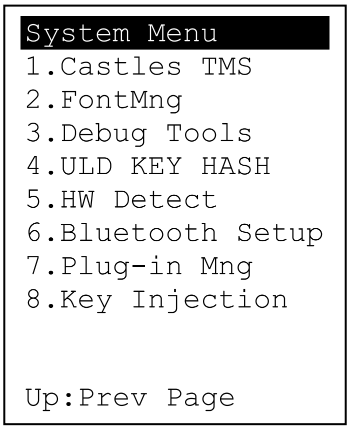
<u>System Menu</u>

Page 1



```
 System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

Page 2



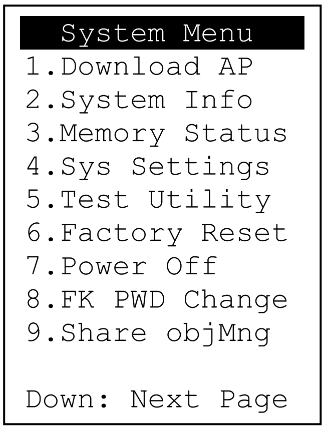
```
System Menu
1.Castles TMS
2.FontMng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection


Up:Prev Page
```

- Press [·] button to page 2.

3.2. Download AP

Download user application or kernel modules firmware.

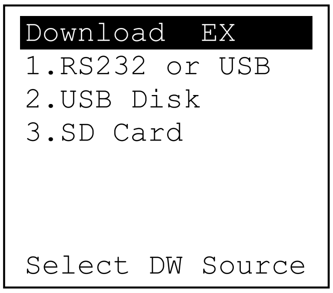
<u>System Menu</u>



```
 System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

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

Download AP Menu



```
Download  EX
1.RS232 or USB
2.USB Disk
3.SD Card



Select DW Source
```

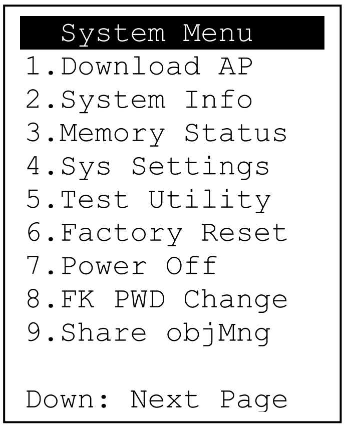
Select download source:

- 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

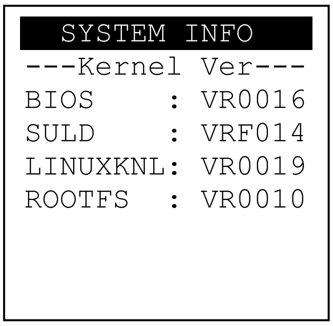


```
 System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

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

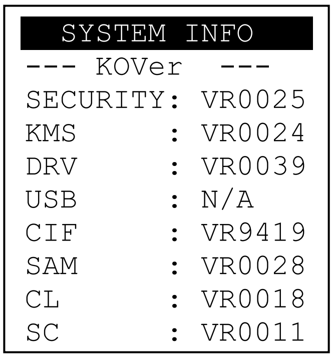
System Info Menu

Page 1



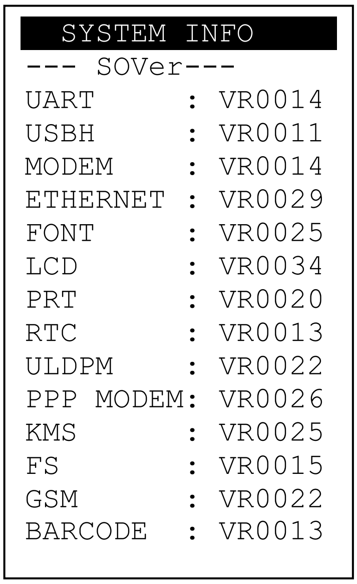
```
  SYSTEM INFO
---Kernel Ver---
BIOS     : VR0016
SULD     : VRF014
LINUXKNL: VR0019
ROOTFS   : VR0010
```

Page 2



```
  SYSTEM INFO
--- KOVer  ---
SECURITY: VR0025
KMS      : VR0024
DRV      : VR0039
USB      : N/A
CIF      : VR9419
SAM      : VR0028
CL       : VR0018
SC       : VR0011
```

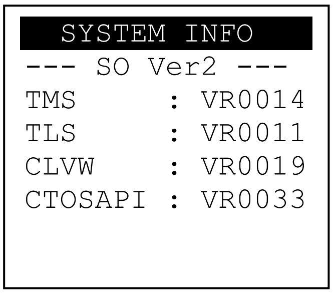
Page 3



```
  SYSTEM INFO
--- SOVer---
UART       : VR0014
USBH       : VR0011
MODEM      : VR0014
ETHERNET : VR0029
FONT       : VR0025
LCD        : VR0034
PRT        : VR0020
RTC        : VR0013
ULDPM      : VR0022
PPP MODEM: VR0026
KMS        : VR0025
FS         : VR0015
GSM        : VR0022
BARCODE   : VR0013
```

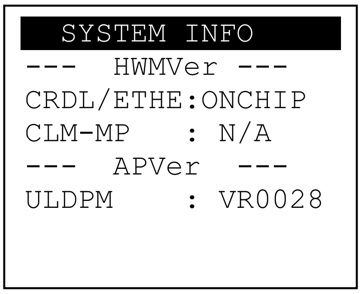
- Press [·] button to next page.

Page 4



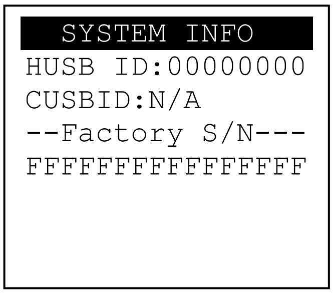
```
  SYSTEM INFO
--- SO Ver2 ---
TMS       : VR0014
TLS       : VR0011
CLVW      : VR0019
CTOSAPI : VR0033
```

Page 5



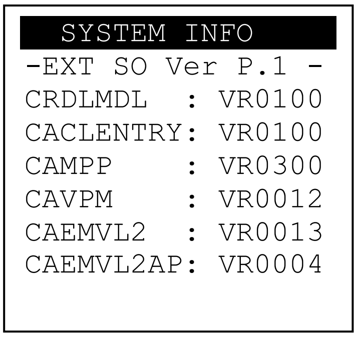
```
  SYSTEM INFO
---  HWMVer ---
CRDL/ETHE:ONCHIP
CLM-MP    : N/A
---  APVer  ---
ULDPM     : VR0028
```

Page 6



```
  SYSTEM INFO
HUSB ID:00000000
CUSBID:N/A
--Factory S/N---
FFFFFFFFFFFFFFFF
```

Page 7

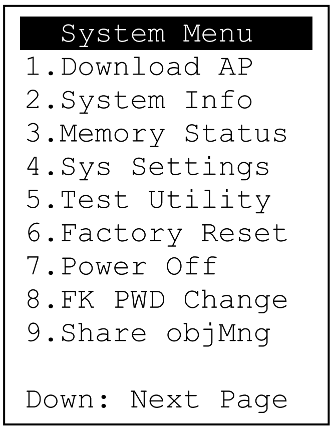


```
  SYSTEM INFO
-EXT SO Ver P.1 -
CRDLMDL  : VR0100
CACLENTRY: VR0100
CAMPP    : VR0300
CAVPM    : VR0012
CAEMVL2  : VR0013
CAEMVL2AP: VR0004
```

3.4. Memory Status

View terminal / pinpad flash memory and RAM information.

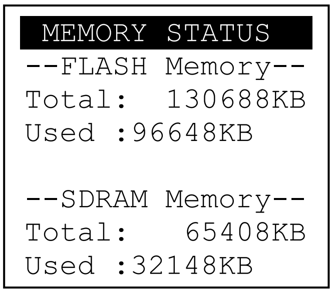
System Menu



```
  System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

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

Memory Status Menu



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

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

3.5. System Settings

View or change terminal / pinpad system settings.

Setting	***Descriptions***
Key Sound	Enable (Y) or disable (N) the beep sound when pressing any key.
Exec DFLT AP	Enable (Y) or disable (N) execution of default selected application.
USB CDC Mode	Enable (Y) or disable (N) USB CDC mode.
FunKey PWD	Enable (Y) or disable (N) password protection to access function key (0 ~ 3) in Program Manager.
PMEnter PWD	Enable (Y) or disable (N) password protection to enter Program Manager.
SET USB Host	Enable (Y) or disable (N) USB host mode.
Base USB CDC	Enable (Y) or disable (N) USB CDC mode in base unit. [Portable model only]
List SHR Lib	Enable (Y) or disable (N) to list all shared libraries in Program Manager.
Key MNG Mode	**<TBC>**
Bat Threshld	Battery charging threshold value. [Portable model only]
Null Cradle	Enable (Y) if base is Type 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	Enable (Y) or disable (N) Power key rebooting
GDB Mode	Enable (Y) or disable (N) GDB mode.
GDB Timeout	GDB connection timeout.
GDB Channel	GDB connection channel.
ETHER IP/PORT	GDB Ethernet connection setting.
RTC Time Zone	Set Time Zone of Real Time Clock.
NTP Enable	Enable (Y) or disable (N) Network Time Protocol.

NTP Update Freq	Frequency of Network Time Protocol updating.

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
8.FK PWD Change
9.Share objMng

Down: Next Page
```

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

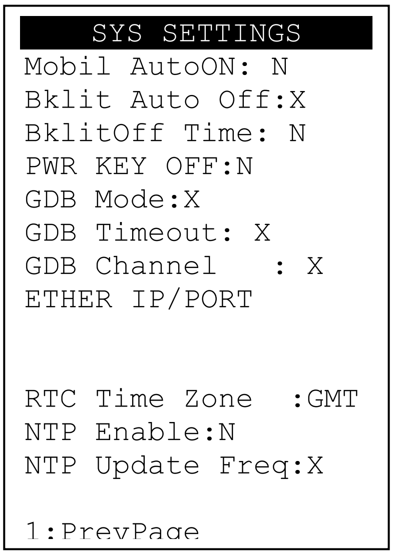
System Settings Menu

Page 1

```
  SYS SETTINGS
Key Sound   : Y
Exec DFLT AP: Y
 -AP Name
USB CDC Mode: Y
FunKeyPWD:N
PMEnterPWD:N
SET USB Host: N
Base USB CDC: X
List SHR Lib: N
Key MNG Mode: 0
Bat Threshld: X
Null Cradle : X
Debug Mode  :N
Debug Port  :X
2: Next Page
```

- Press [Power] or [·] button to select setting.
- Press [OK] button to change the setting value.
- Press [⇦] button to toggle Y ⇨ N ⇨ Y.
- Press [2] button to next page.

Page 2



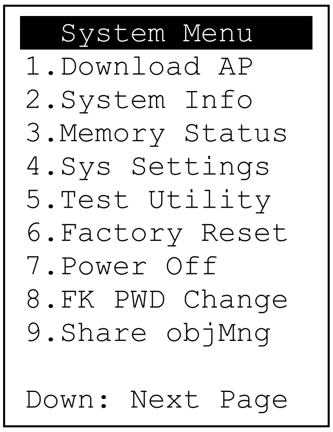
```
     SYS SETTINGS
Mobil AutoON: N
Bklit Auto Off:X
BklitOff Time: N
PWR KEY OFF:N
GDB Mode:X
GDB Timeout: X
GDB Channel   : X
ETHER IP/PORT


RTC Time Zone  :GMT
NTP Enable:N
NTP Update Freq:X

1:PrevPage
```

- Press [Power] 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

Diagnose terminal / pinpad hardware components.

System Menu

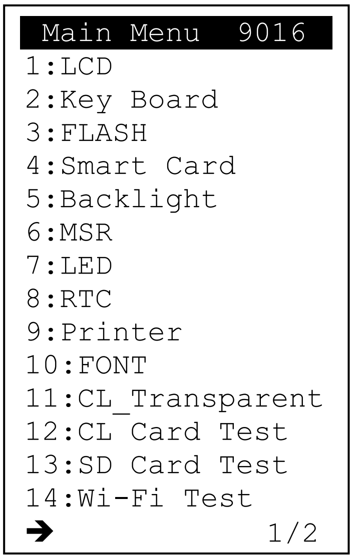


```
  System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

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

Test Utility Menu

Page 1



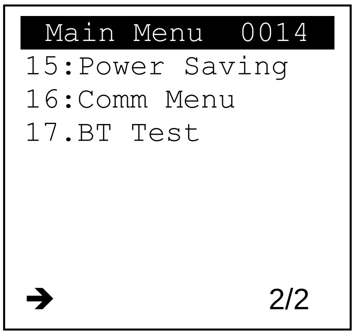
```
 Main Menu  9016
1:LCD
2:Key Board
3:FLASH
4:Smart Card
5:Backlight
6:MSR
7:LED
8:RTC
9:Printer
10:FONT
11:CL_Transparent
12:CL Card Test
13:SD Card Test
14:Wi-Fi Test
➔              1/2
```

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

- Press [7] and [OK] button to diagnose LED.
- Press [8] and [OK] button to diagnose real time clock.
- Press [9] and [OK] button to diagnose printer.
- Press [1], [0]and [OK] button to view font.
- Press [1], [1] and [OK] button to diagnose contactless reader in transparent mode.
- Press [1], [2]and [OK] button to diagnose contactless card.
- Press [1], [3] and [OK] button to diagnose SD memory card.
- Press [1], [4] and [OK] button to test Wi-Fi.
- Press [·] button to next page.

Note: Default password for changing RTC is 8418.

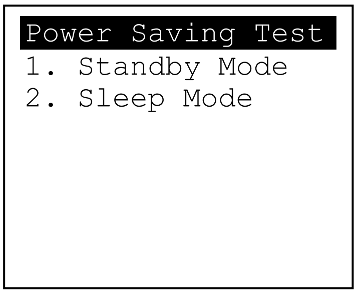
Page 2



```
 Main Menu  0014
15:Power Saving
16:Comm Menu
17.BT Test



➔             2/2
```

- Press [1], [5]and [OK]button to enter Power Saving Test Menu.
- Press [1], [6] and [OK] button to enter Communication Test Menu.
- Press [1], [7] and [OK] button to enter Bluetooth Test Menu.
- Press [Power] button to previous page.
- Press [X] button to exit.

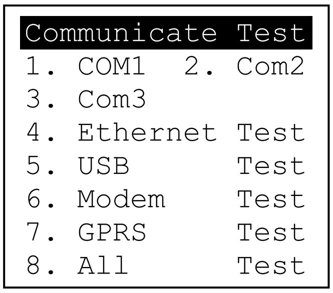
<u>Power Saving Test Menu</u>



```
Power Saving Test
1. Standby Mode
2. Sleep Mode
```

- Press [1] button to Standby Mode.
- Press [2] button to Sleep Mode.

Communication Test Menu



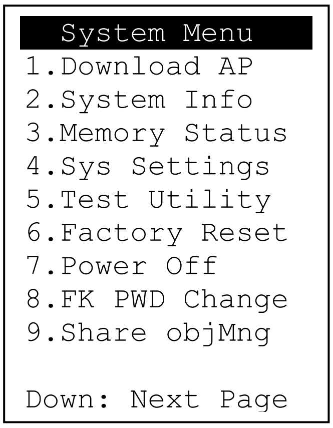
```
Communicate Test
1. COM1  2. Com2
3. Com3
4. Ethernet Test
5. USB      Test
6. Modem    Test
7. GPRS     Test
8. All      Test
```

- 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, from item 1 to 7.

3.7. Factory Reset

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

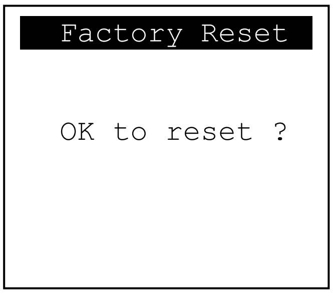
System Menu



```
  System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

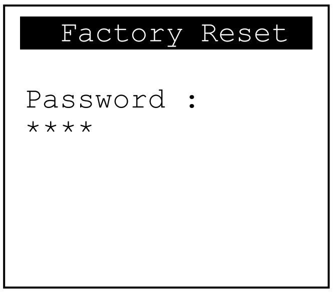
- Press [6] button to enter Factory Reset menu.

Factory Reset Menu



```
  Factory Reset


  OK to reset ?
```

- Press [OK] button to perform factory reset.



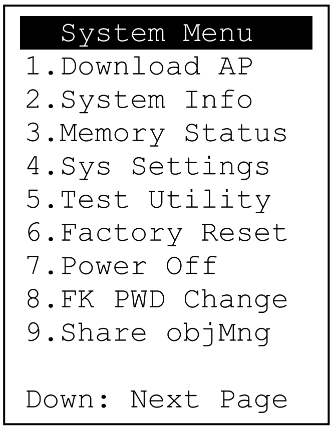
```
  Factory Reset

Password :
****
```

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

3.8. Power Off

Power off terminal / pinpad.

System Menu



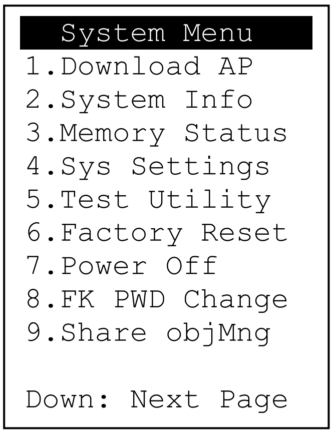
```
  System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

- Press [7] button to power off terminal / pinpad.

3.9. Function Key Password Change

Change function key access password.

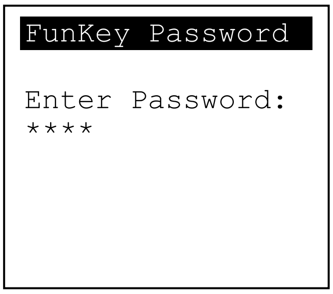
System Menu



```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

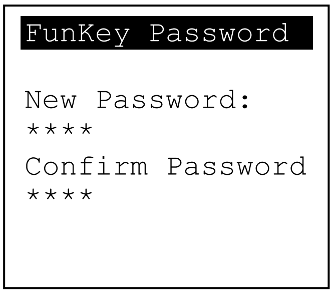
- Press [8] button to enter FunKey Password menu.

FunKey Password Menu



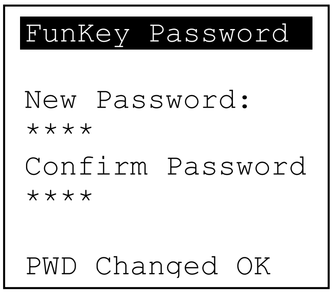
```
FunKey Password

Enter Password:
****
```

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



```
FunKey Password

New Password:
****
Confirm Password
****
```

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

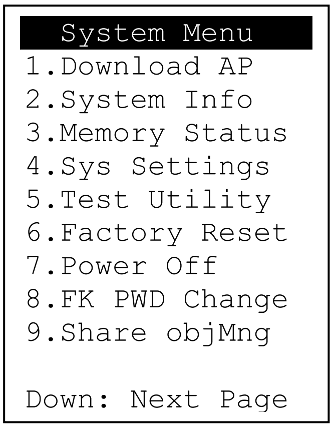


```
FunKey Password

New Password:
****
Confirm Password
****

PWD Changed OK
```

3.10.Share Object Management

View share object in terminal / pinpad.

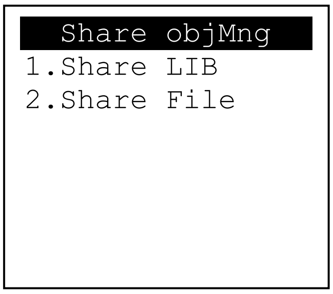
System Menu



```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.FK PWD Change
9.Share objMng

Down: Next Page
```

- Press [9] button to enter Share Object Management menu.

Share Object Management Menu



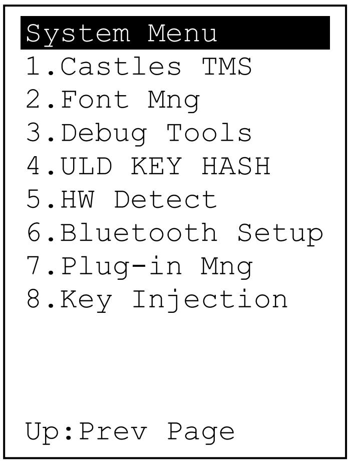
```
  Share objMng
1.Share LIB
2.Share File
```

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

3.11. CastlesTMS

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

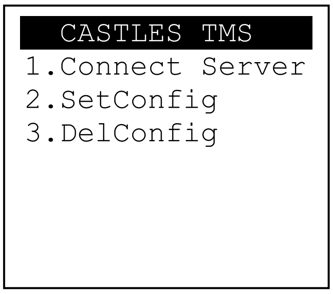
System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [1] button to enter Castles TMS menu.

Castles TMS Menu



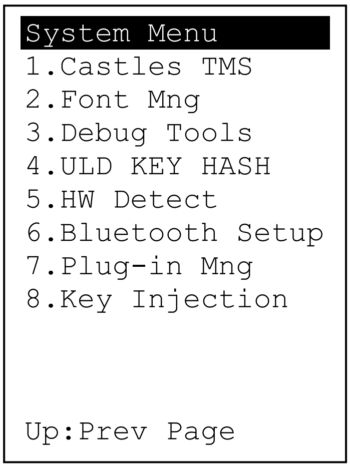
```
   CASTLES TMS
1.Connect Server
2.SetConfig
3.DelConfig
```

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

3.12.Font Mng

View Font Management.

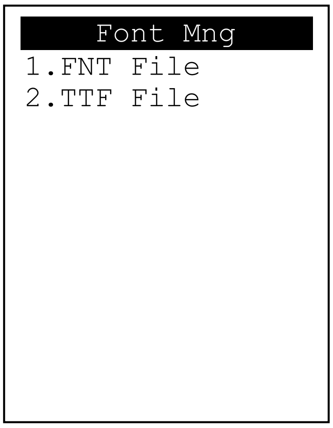
System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [2] button to view Font Management.

Font Management



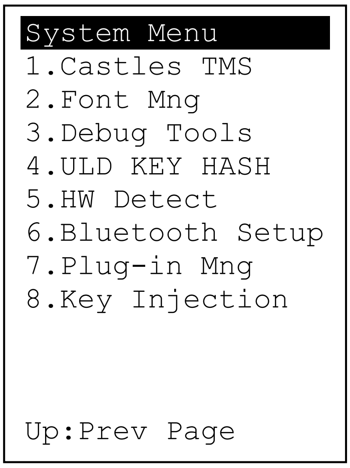
```
   Font Mng
1.FNT File
2.TTF File
```

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

3.13.Debug Tools

Perform the Debug Tools.

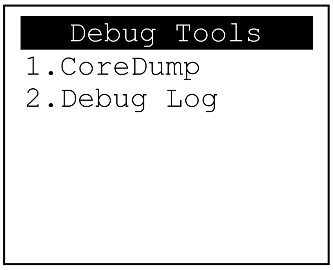
System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [3] go to the Debug Tools Menu.

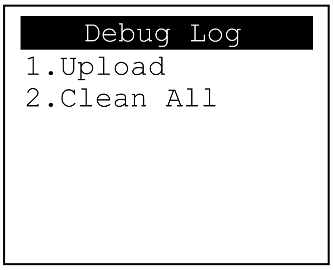
Debug Tools



```
   Debug Tools
1.CoreDump
2.Debug Log
```

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

Debug Log



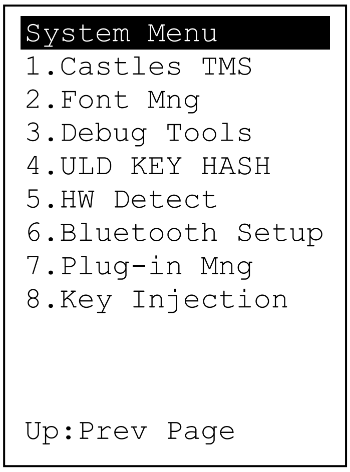
```
    Debug Log
1.Upload
2.Clean All
```

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

3.14. ULD Key Hash

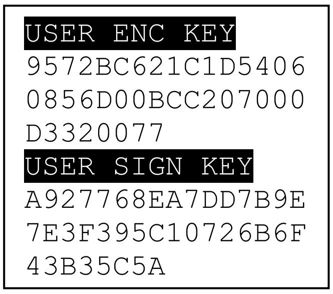
View ULD user keyset hash value.

System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [4] button to view hash value.

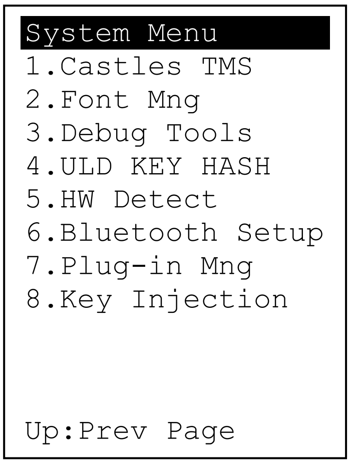


```
USER ENC KEY
9572BC621C1D5406
0856D00BCC207000
D3320077
USER SIGN KEY
A927768EA7DD7B9E
7E3F395C10726B6F
43B35C5A
```

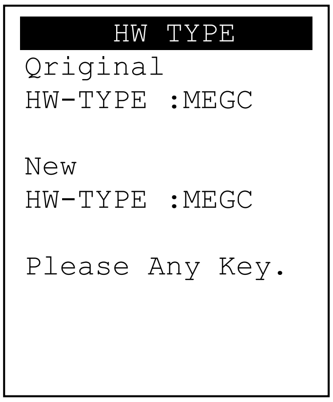
3.15. Hardware Detect

View the hardware type of the terminal / pinpad.

System Menu (Page 2)



- Press [5] button to view the hardware type of the terminal / pinpad.

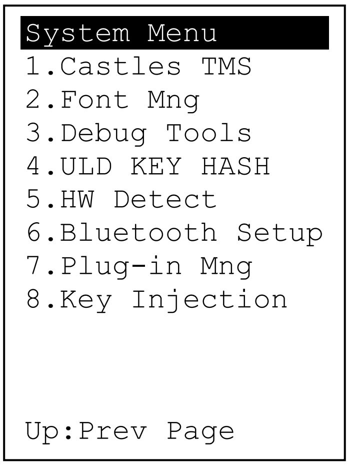


```
      HW TYPE
Qriginal
HW-TYPE :MEGC

New
HW-TYPE :MEGC

Please Any Key.
```

3.16.Bluetooth Setup

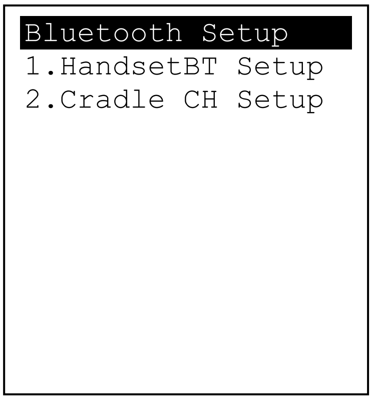
Set the settings of Bluetooth.This function will be available after installing the BT plug-in patch.

System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [6] go to the Bluetooth setup menu.



```
Bluetooth Setup
1.HandsetBT Setup
2.Cradle CH Setup
```

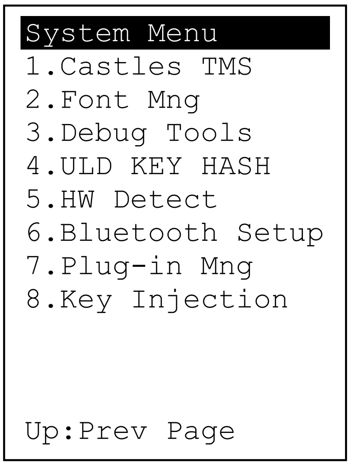
- Press [1] go to the Handset BT setup menu.
- Press [2] go to the Cradle CH setup menu.

  Formore detailedinformationof Bluetooth setup, please refer to the document‘Bluetooth Guideline on V3 EFT-POS Terminal’.

3.17.Plug-in Mng

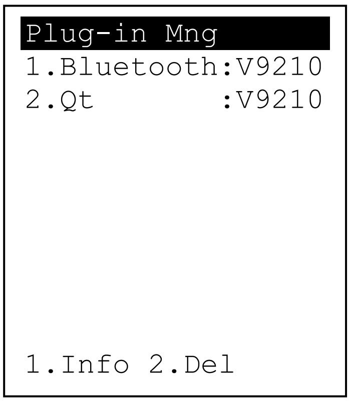
View Plug-in Management.

System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection




Up:Prev Page
```

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



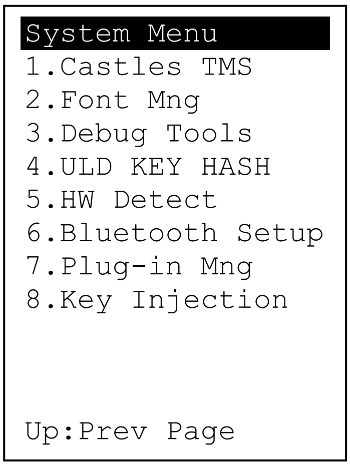
```
Plug-in Mng
1.Bluetooth:V9210
2.Qt       :V9210







1.Info 2.Del
```

- Press [Power] or[·]button to select item.
- Press [1]button to get item information.
- Press [2]button to delete item.

3.18.Key Injection

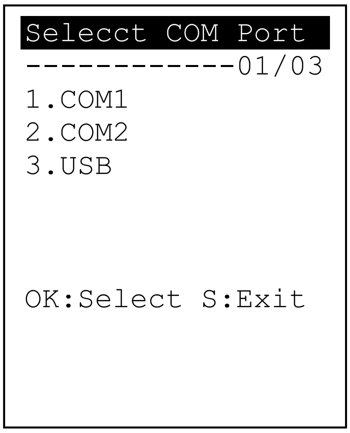
View Key Injection Menu. **This function is for castles internal only. User or developer do not allow to use this function.**

System Menu (Page 2)



```
System Menu
1.Castles TMS
2.Font Mng
3.Debug Tools
4.ULD KEY HASH
5.HW Detect
6.Bluetooth Setup
7.Plug-in Mng
8.Key Injection



Up:Prev Page
```

- Press [8] button to view Key Injection Menu.



```
Selecct COM Port
------------01/03
1.COM1
2.COM2
3.USB



OK:Select S:Exit
```

- Press [OK] to select the port and execute the Key Injection.
- Press [X] button to Exit.

4. Secure File Loading

Castles implemented an interface in terminal / pinpad 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, the RSA key length is 2048 bits.

4.1.1. ULD Manufacturer Key

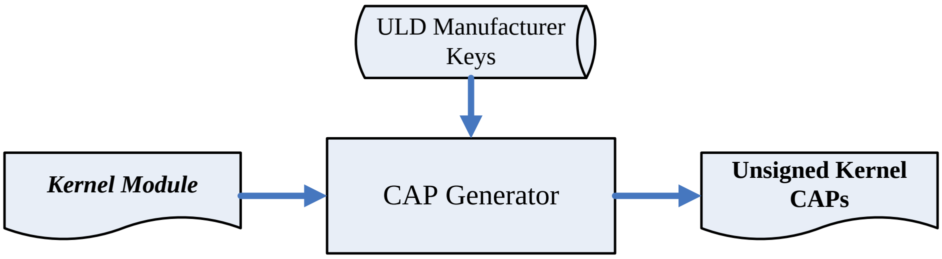
The system consists of several kernel modules. These kernel modules are provided by the Manufacturer, and released in CAP format file with encryption and signing via ULD Manufacturer Keys.

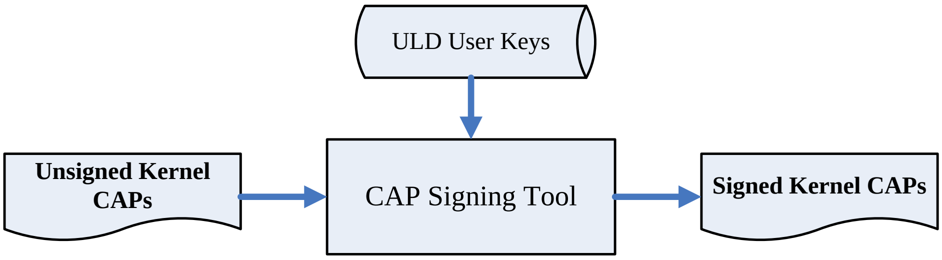
The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only 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 kennel 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.

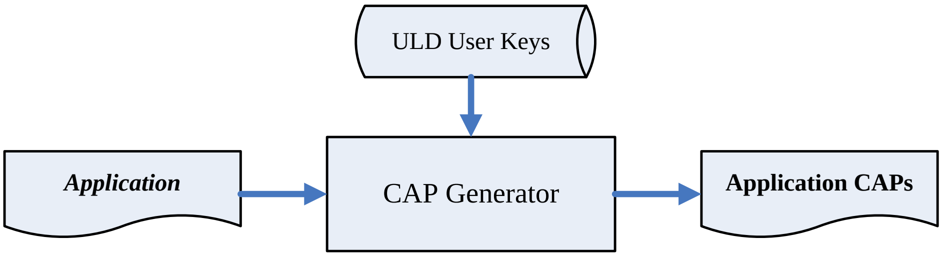




4.1.2. ULD User Key

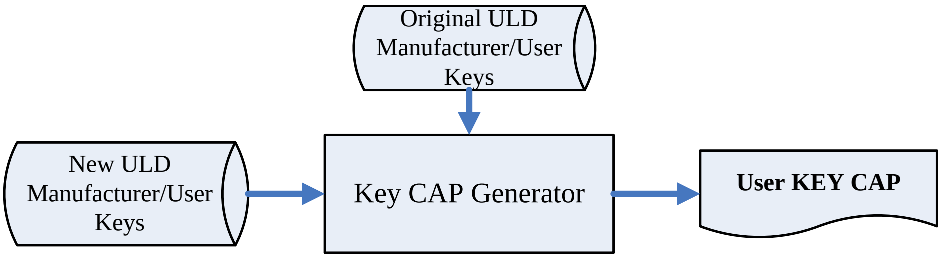
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the “signed’ action via ULD User Keys.

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.


Original ULD Manufacturer/User Keys
New ULD Manufacturer/User Keys
Key CAP Generator
User KEY CAP

4.2. File Signing

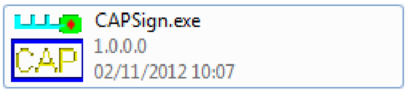
4.2.1. Signing Kernel Module

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 / pinpad.

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

The CAP Signing Tool is located at:
C:\Program Files\Castles\VEGA3000\tools\Signing Tool

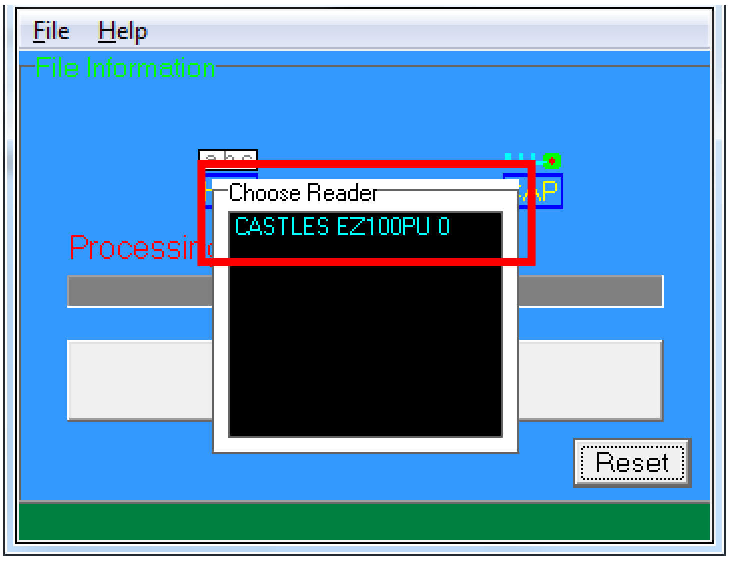
- Run CAP Signing Tool



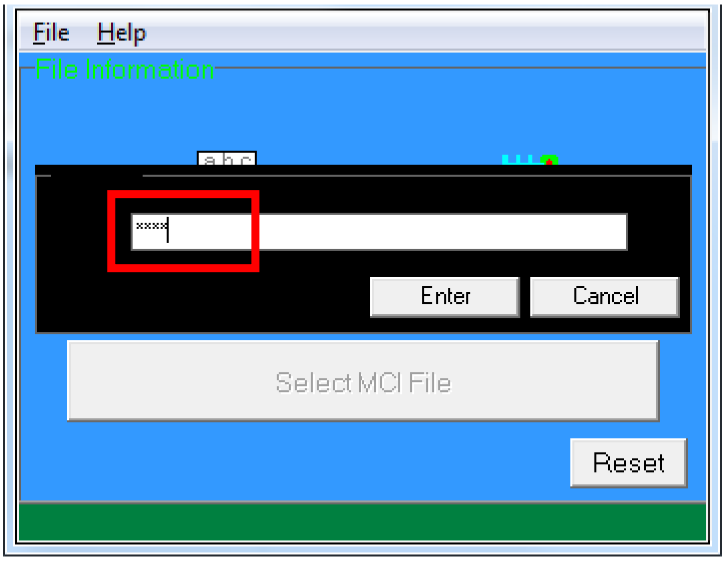
CAPSign.exe
1.0.0.0
02/11/2012 10:07

(VEGA3000)

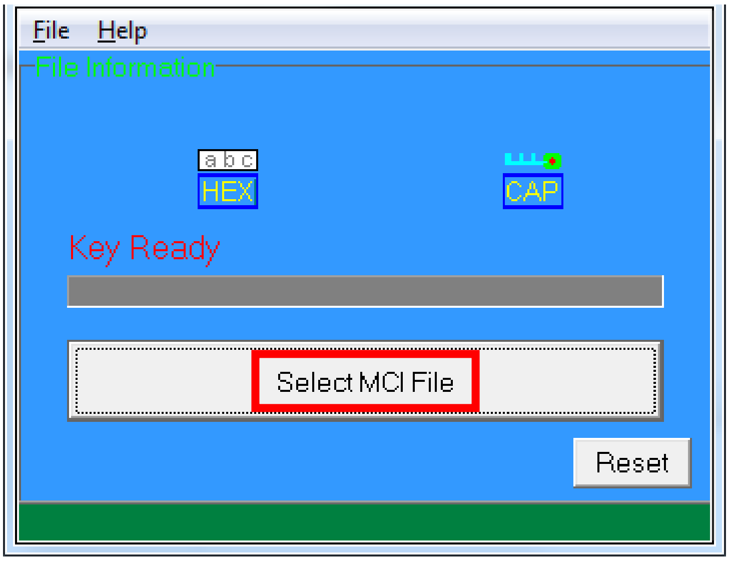
- Insert Key Card and select smart card reader



- 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

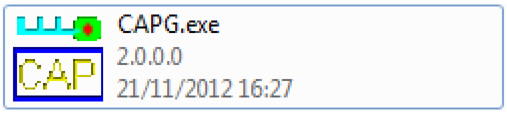
Following files are required to sign before load to terminal / pinpad. This is to ensure the application data and codes confidential and integrity. The output file will be "CAP" file which format is defined by Castles.

- 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.

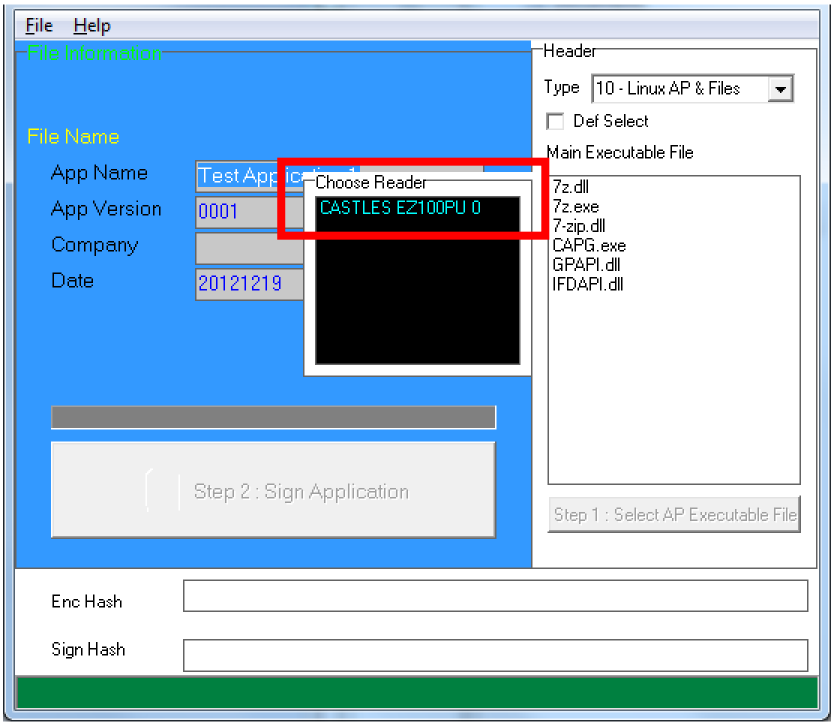
The CAP Generator is located at:
C:\Program Files\Castles\VEGA3000\tools\CAPG (KeyCard)

- Run CAP Generator



CAPG.exe
2.0.0.0
21/11/2012 16:27

- Insert Key Card and select smart card reader



App Name: Test Applica...

App Version: 0001

Date: 20121219

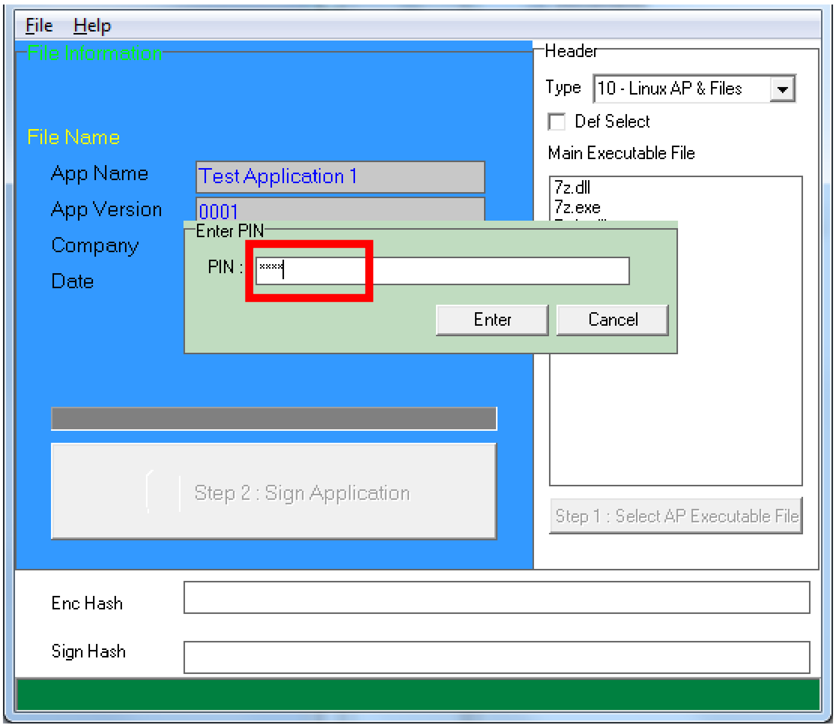
Choose Reader: CASTLES EZ100PU 0

Type: 10 - Linux AP & Files

□ Def Select

Main Executable File:
7z.dll
7z.exe
7-zip.dll
CAPG.exe
GPAPI.dll
IFDAPI.dll

- Enter Key Card PIN



App Name: Test Application 1

App Version: 0001

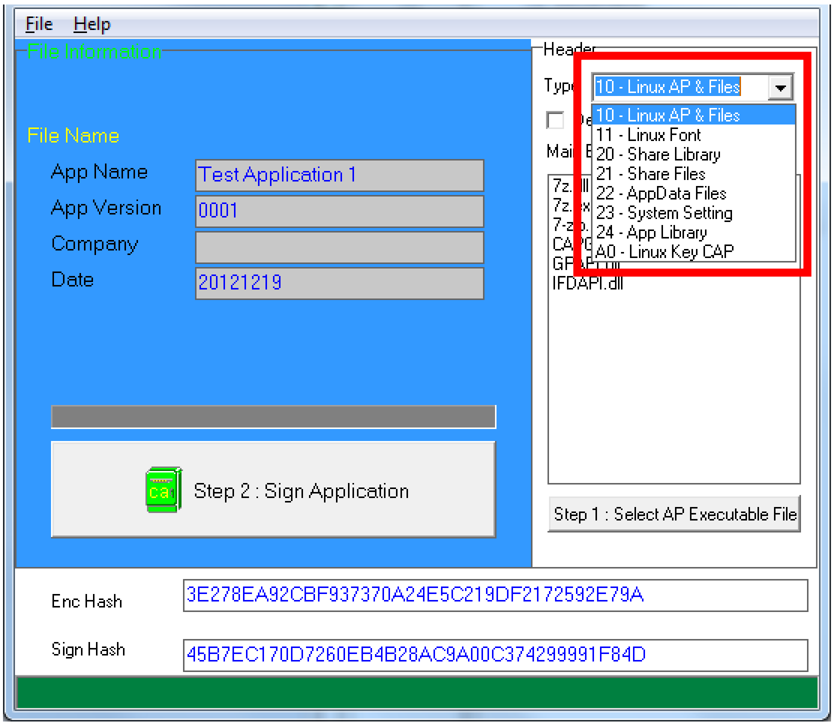
PIN : ****

Type: 10 - Linux AP & Files

□ Def Select

Main Executable File:
7z.dll
7z.exe

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



App Name: Test Application 1
App Version: 0001
Company:
Date: 20121219

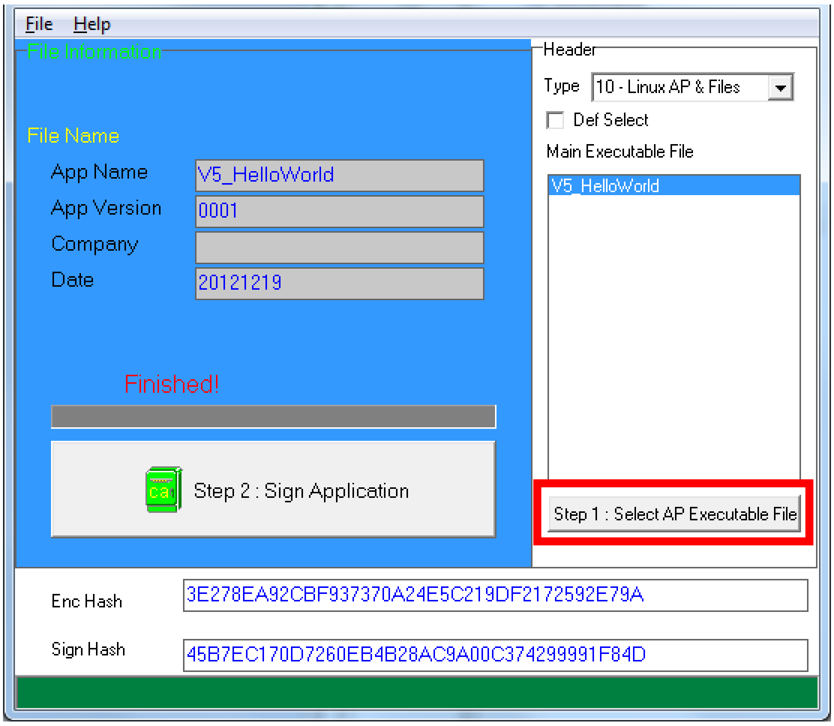
Type: 10 - Linux AP & Files

10 - Linux AP & Files
11 - Linux Font
20 - Share Library
21 - Share Files
22 - AppData Files
23 - System Setting
24 - App Library
A0 - Linux Key CAP

IFDAPI.dll

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A
Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

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



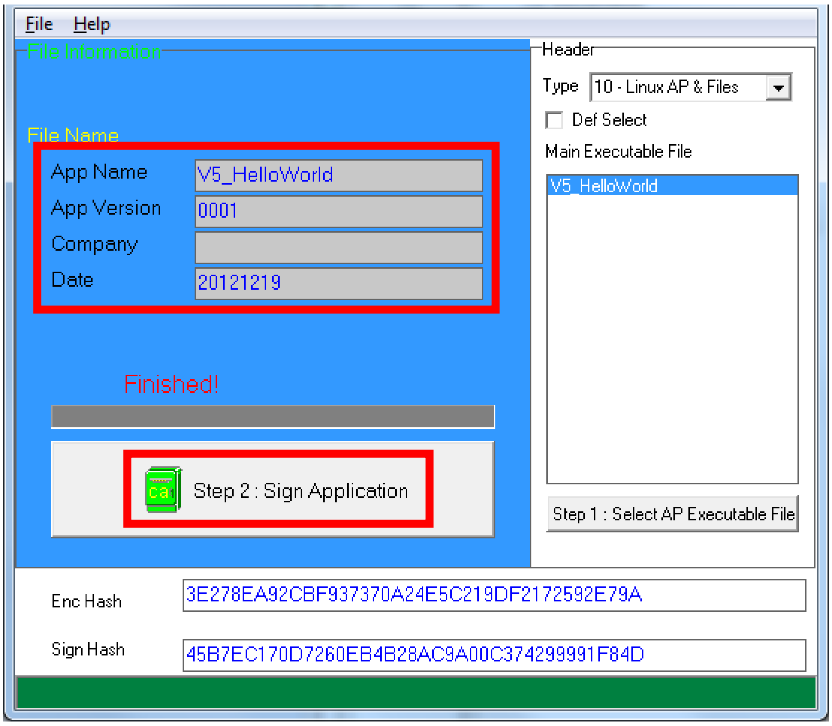
App Name: V5_HelloWorld
App Version: 0001
Company:
Date: 20121219

Finished!

Type: 10 - Linux AP & Files
□ Def Select
Main Executable File
V5_HelloWorld

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A
Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

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



App Name: V5_HelloWorld
App Version: 0001
Company:
Date: 20121219

Type: 10 - Linux AP & Files
□ Def Select
Main Executable File: V5_HelloWorld

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A
Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

- 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.

App.CAP

App.mci

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.

MultiApp.mmci

4.3. File Loading

There are several ways of loading file to VEGA3000terminal / pinpad.

- 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 / pinpad.

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

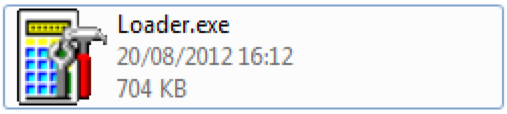
Castles TMS (CTMS or CASTLES Terminal Management System) is provided by Castles Technology. It uses to perform remote download via Ethernet, GPRS/UMTS or modem.

4.3.1. Download by User Loader

The User Loader works for VEGA3000.

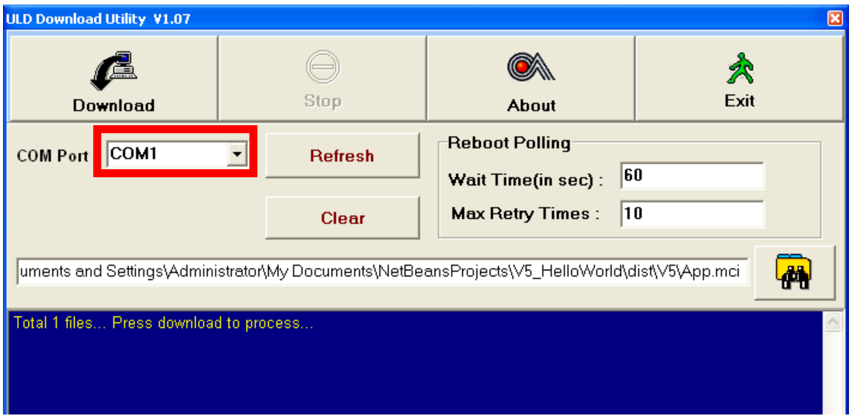
The Loader is located at:
C:\Program Files\Castles\VEGA3000\tools\Loader

- Run User Loader



Loader.exe
20/08/2012 16:12
704 KB

- Select COM port



COM Port COM1

Reboot Polling

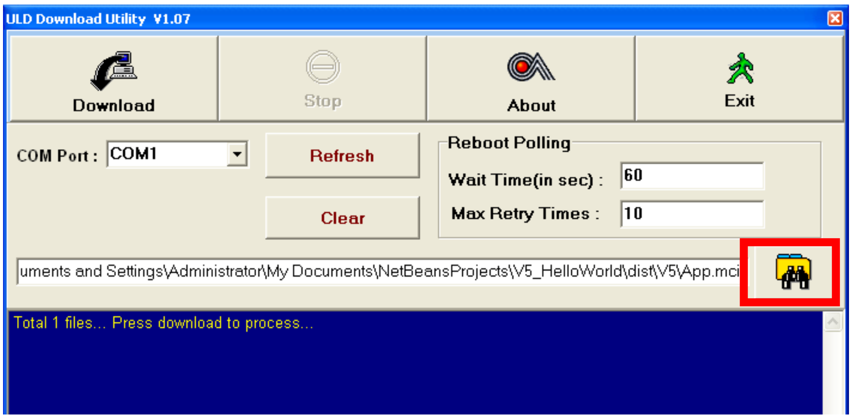
Wait Time(in sec) : 60

Max Retry Times : 10

uments and Settings\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci

```
Total 1 files... Press download to process...
```

- Browse and select mci file or mmci file



COM Port : COM1

Reboot Polling

Wait Time(in sec) : 60

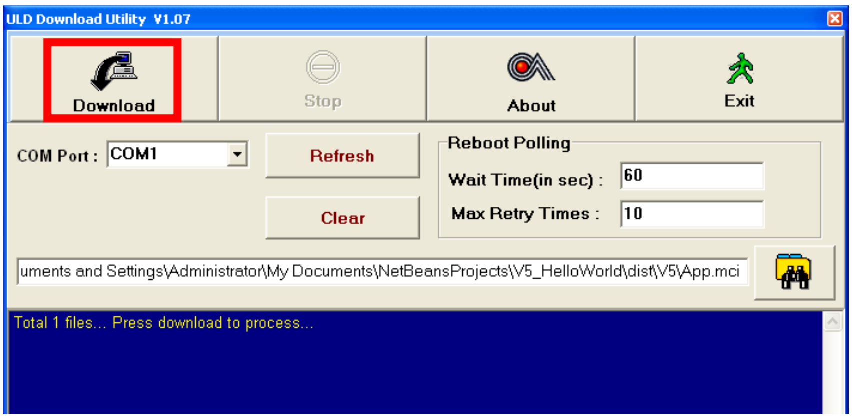
Max Retry Times : 10

uments and Settings\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci

```
Total 1 files... Press download to process...
```

- Setup terminal / pinpad 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.



ULD Download Utility V1.07

COM Port : COM1

Reboot Polling

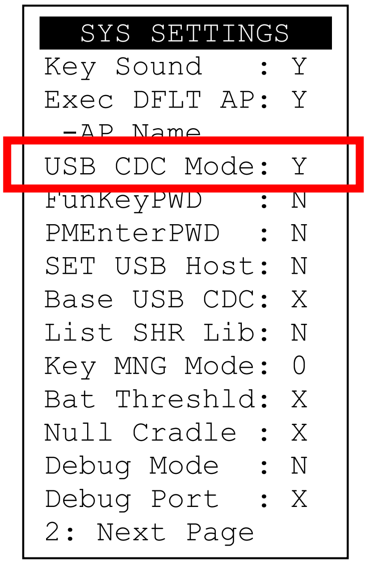
Wait Time(in sec) : 60

Max Retry Times : 10

uments and Settings\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci

Total 1 files... Press download to process...

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

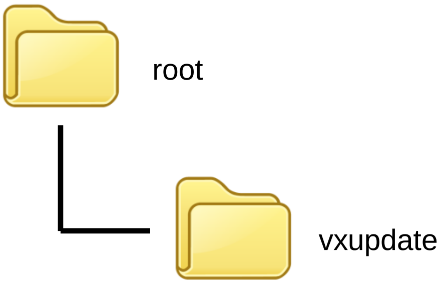


```
 SYS SETTINGS
Key Sound    : Y
Exec DFLT AP: Y
 -AP Name
USB CDC Mode: Y
FunKeyPWD    : N
PMEnterPWD   : N
SET USB Host: N
Base USB CDC: X
List SHR Lib: N
Key MNG Mode: 0
Bat Threshld: X
Null Cradle : X
Debug Mode   : N
Debug Port   : X
2: Next Page
```

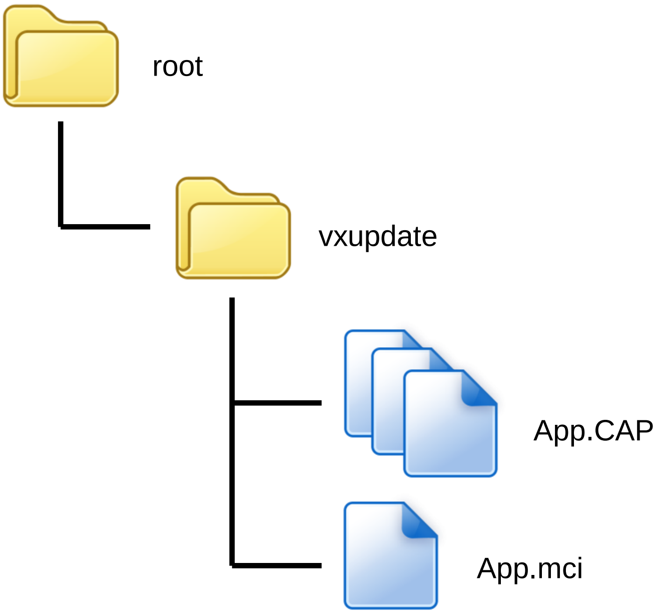
4.3.2. Download by Removable Media

The file download process can be achieved without PC by using removable media, USB flash drive or Micro SD 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.

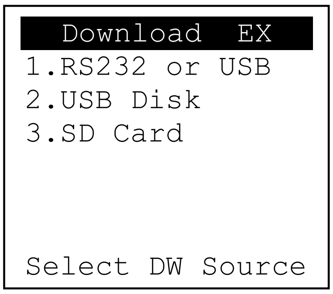


Note: If user would like to load multiple application, create a new file with extension of “mmci”. Then put the mmci file contents with the list of mci file.

MultiApp.mmci

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

  Download AP Menu

  ```
     Download  EX
  1.RS232 or USB
  2.USB Disk
  3.SD Card




  Select DW Source
  ```

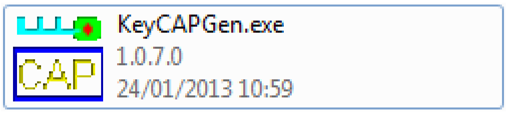
  - Press [2] button to select USB flash drive.
  - Press [3] button to select Micro SD card.

- Finally, terminal will process the file “vxupdate” folder.

4.4. Changing ULD User Key

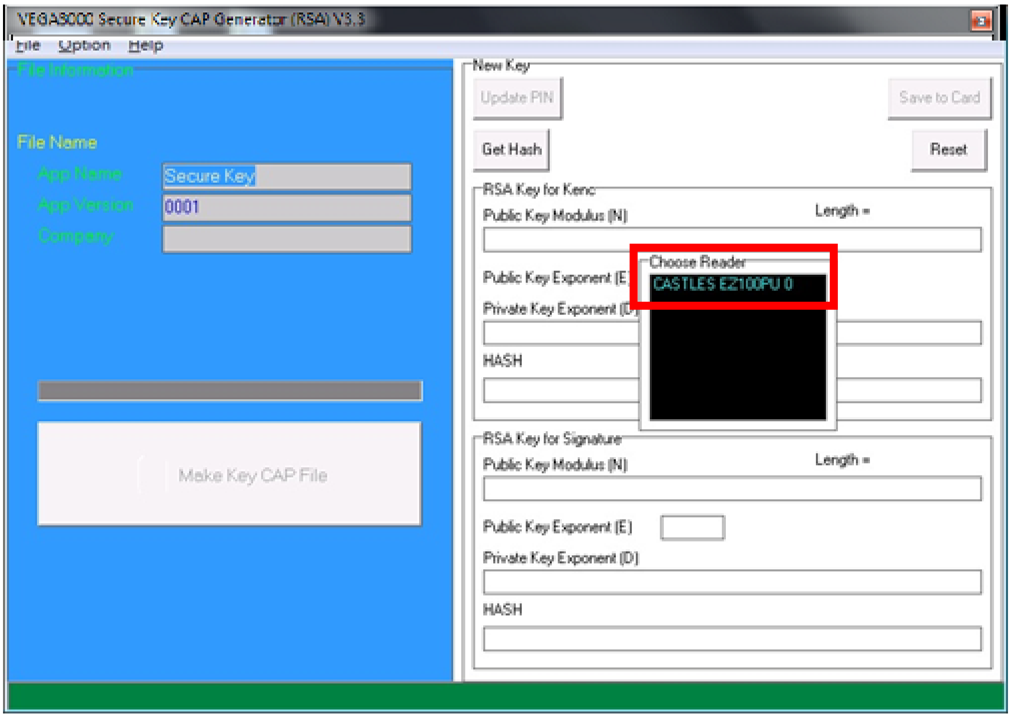
User may change their ULD User Key Set stored in Key Card. Castles Technology provided a tool named “Secure Key Generator” to perform this task.

- Run Secure Key Generator



KeyCAPGen.exe
1.0.7.0
24/01/2013 10:59

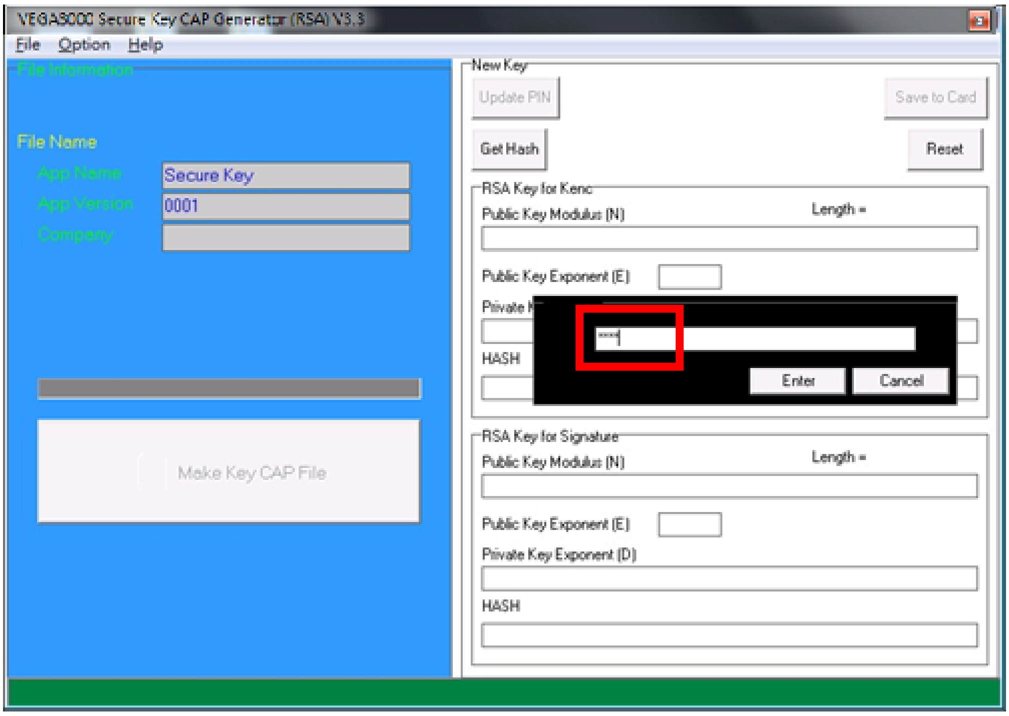
- Insert Key Card and select smart card reader



File Name
App Name: Secure Key
App Version: 0001
Company:

Choose Reader: CASTLES EZ100PU 0

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

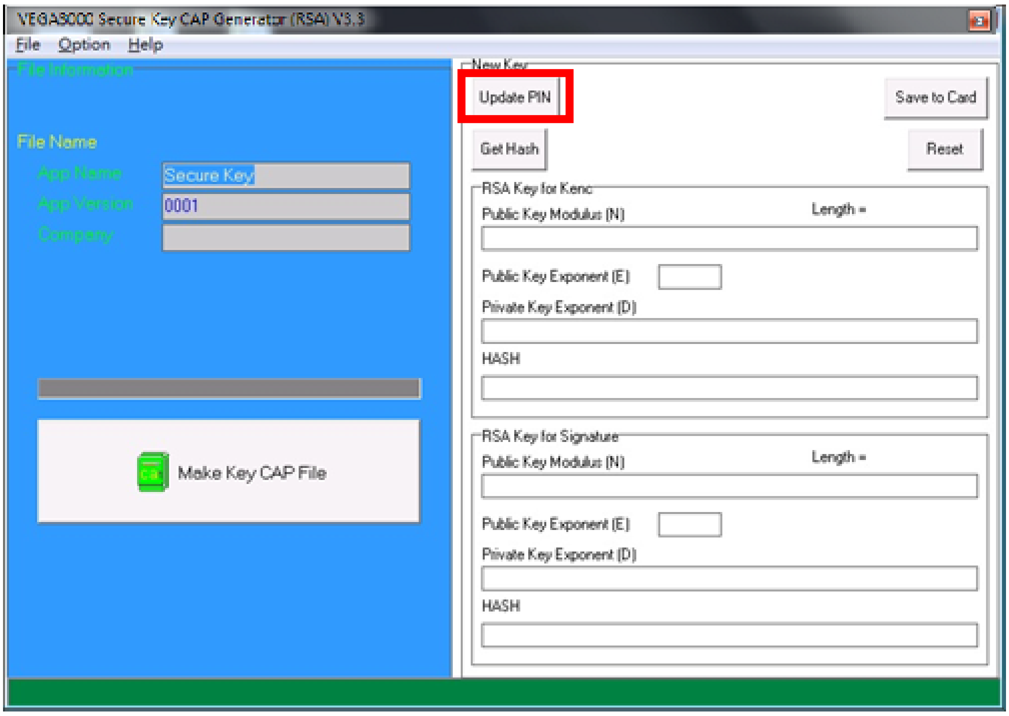


App Name: Secure Key

App Version: 0001

Company:

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

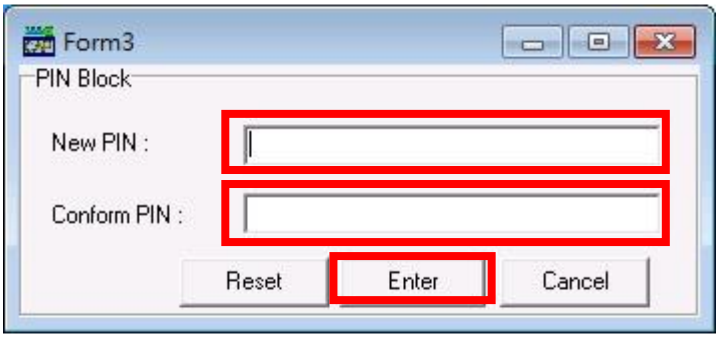


App Name: Secure Key

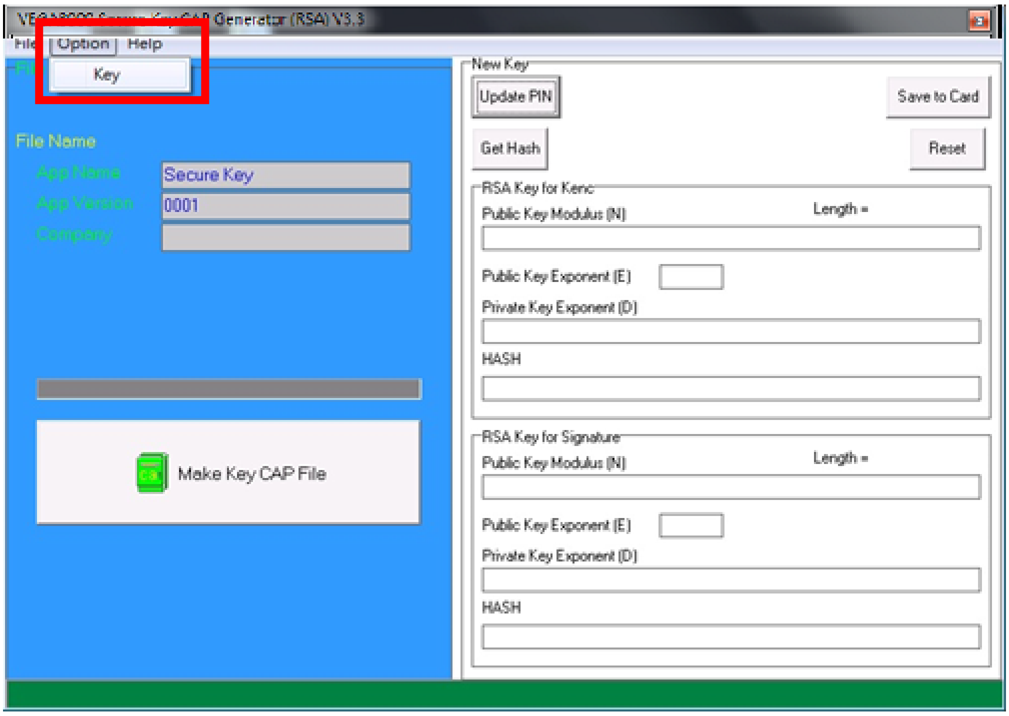
App Version: 0001

Company:

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

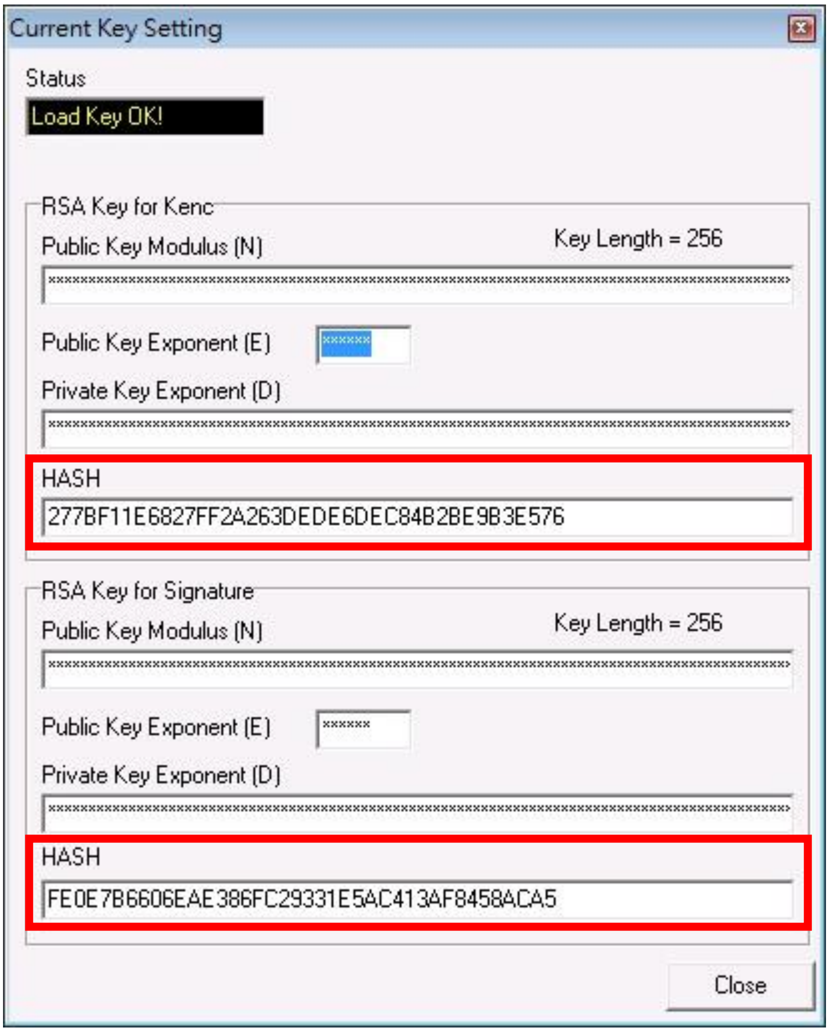


- To view current key set hash value, go to “Option” and select key.



App Name: Secure Key

App Version: 0001



Current Key Setting

Status

Load Key OK!

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

****

Public Key Exponent (E) ******

Private Key Exponent (D)

****

HASH

277BF11E6827FF2A263DEDE6DEC84B2BE9B3E576

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

****

Public Key Exponent (E) ******

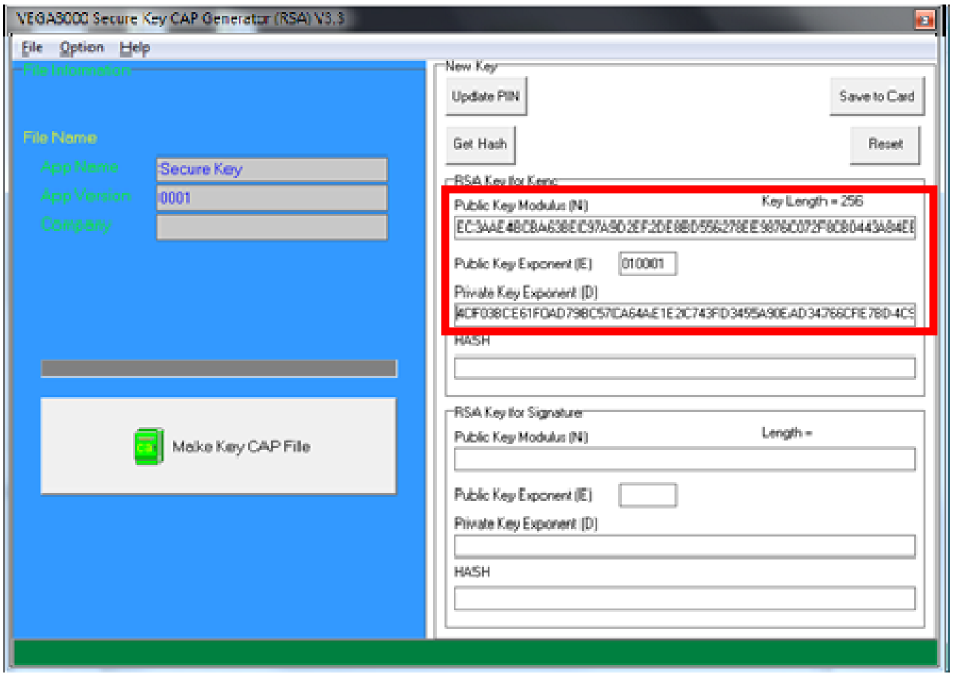
Private Key Exponent (D)

****

HASH

FE0E7B6606EAE386FC29331E5AC413AF8458ACA5

- To generate new user key set
  - Please generate the RSA key by yourself, the length of the RSA key set should be 2048 (bits).
  - Copy RSA key components to RSA Key for Kenc in Secure Key Generator.

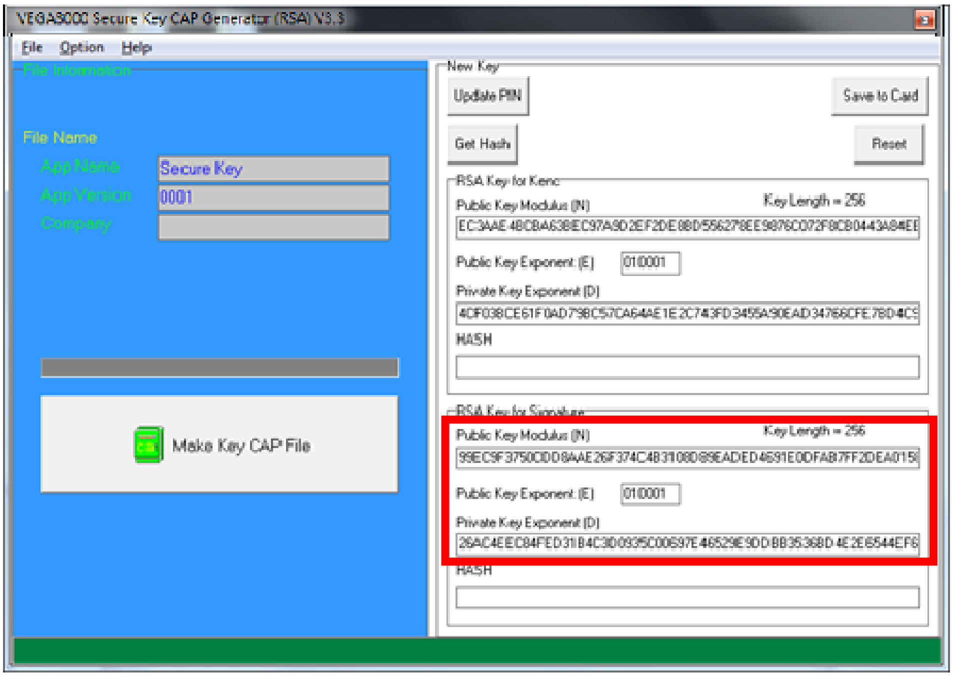


App Name: Secure Key
App Version: 0001
Company:

RSA Key for Kenc
Public Key Modulus (N): EC3AAE4BCBA638EC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE
Key Length = 256
Public Key Exponent (E): 010001
Private Key Exponent (D): 4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9
HASH:

RSA Key for Signature
Public Key Modulus (N):
Public Key Exponent (E):
Private Key Exponent (D):
HASH:

- Generate second RSA key set for Signature.

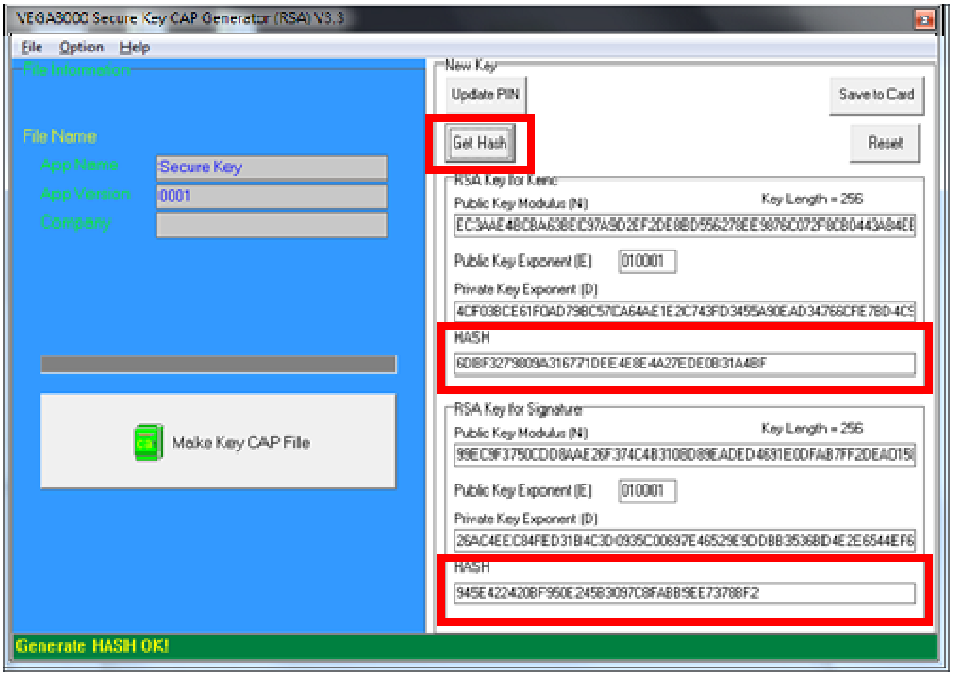


App Name: Secure Key
App Version: 0001
Company:

RSA Key for Kenc
Public Key Modulus (N): EC3AAE4BCBA638EC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE
Key Length = 256
Public Key Exponent (E): 010001
Private Key Exponent (D): 4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9
HASH:

RSA Key for Signature
Public Key Modulus (N): 99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFAB7FF2DEA015
Key Length = 256
Public Key Exponent (E): 010001
Private Key Exponent (D): 26AC4EEC84FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6
HASH:

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



VEGA3000 Secure Key CAP Generator (RSA) V3.3

File Option Help

File Information

File Name

App Name: Secure Key

App Version: 0001

Company:

Make Key CAP File

New Key

Update PIN | Save to Card | Get Hash | Reset

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA638EC97A9D2EF2DE0BD556278EE9876C072F8CB0443A84E

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C

HASH

6D8F3279809A316771DEE4E8E4A27EDE0831A48F

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFA87FF2DEA015

Public Key Exponent (E) 010001

Private Key Exponent (D)

26AC4EEC84FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6

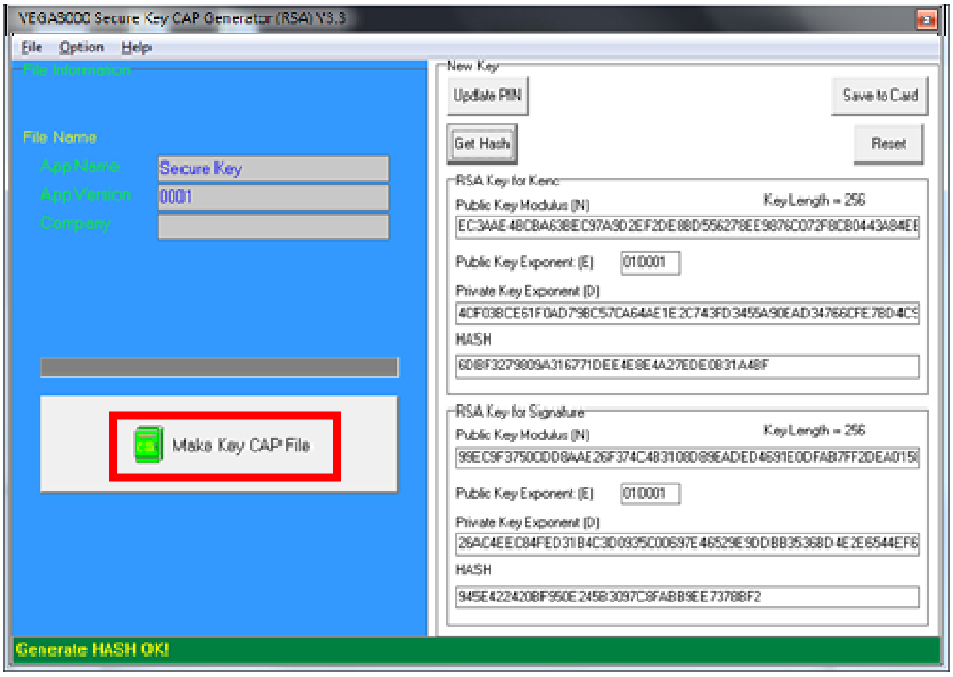
HASH

945E422420BF950E245B3097C8FABB9EE73788F2

Generate HASH OK!

- 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.



VEGA3000 Secure Key CAP Generator (RSA) V3.3

File Option Help

File Information

File Name

App Name: Secure Key

App Version: 0001

Company:

Make Key CAP File

New Key

Update PIN | Save to Card | Get Hash | Reset

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA638EC97A9D2EF2DE0BD556278EE9876C072F8CB0443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C

HASH

6D8F3279809A316771DEE4E8E4A27EDE0831A48F

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFA87FF2DEA015

Public Key Exponent (E) 010001

Private Key Exponent (D)

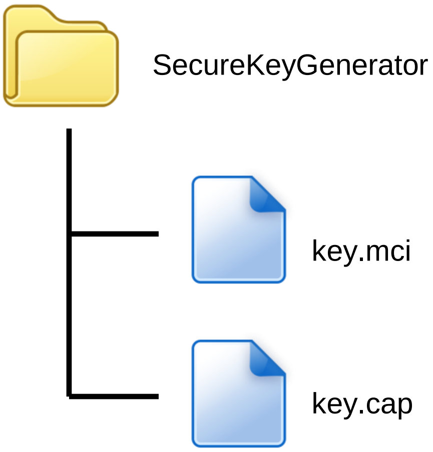
26AC4EEC84FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6

HASH

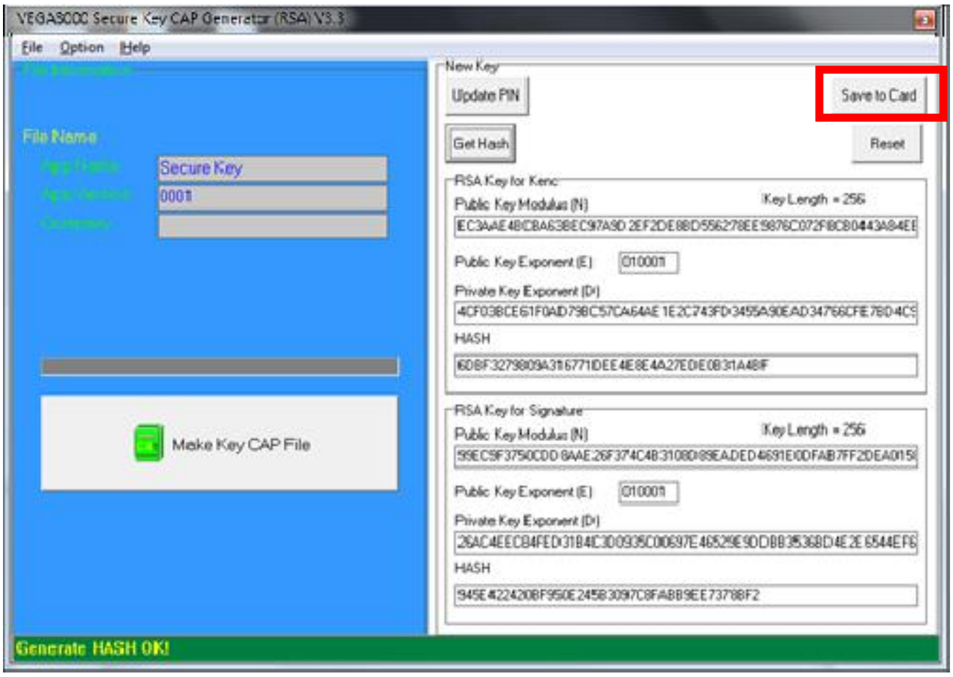
945E422420BF950E245B3097C8FABB9EE73788F2

Generate HASH OK!

- 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.



File Name

App Name: Secure Key

App Version: 0001

Company:

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BDBA63BEC97A9D2EF2DE8BD556278EE9876C072F8C80443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF03BCE61F0AD79BC57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9

HASH

6DBF3279809A3116771DEE4E8E4A27EDE0831A48F

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

59EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFAB7FF2DEA015

Public Key Exponent (E) 010001

Private Key Exponent (D)

26AC4EECB4FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6

HASH

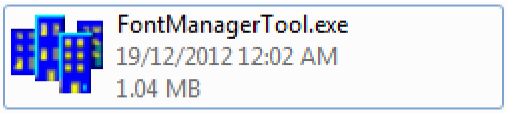
945E4224208F950E2458309 7C8FABB9EE73788F2

Generate HASH OK!

5. Font Management

5.1. Loading New Font

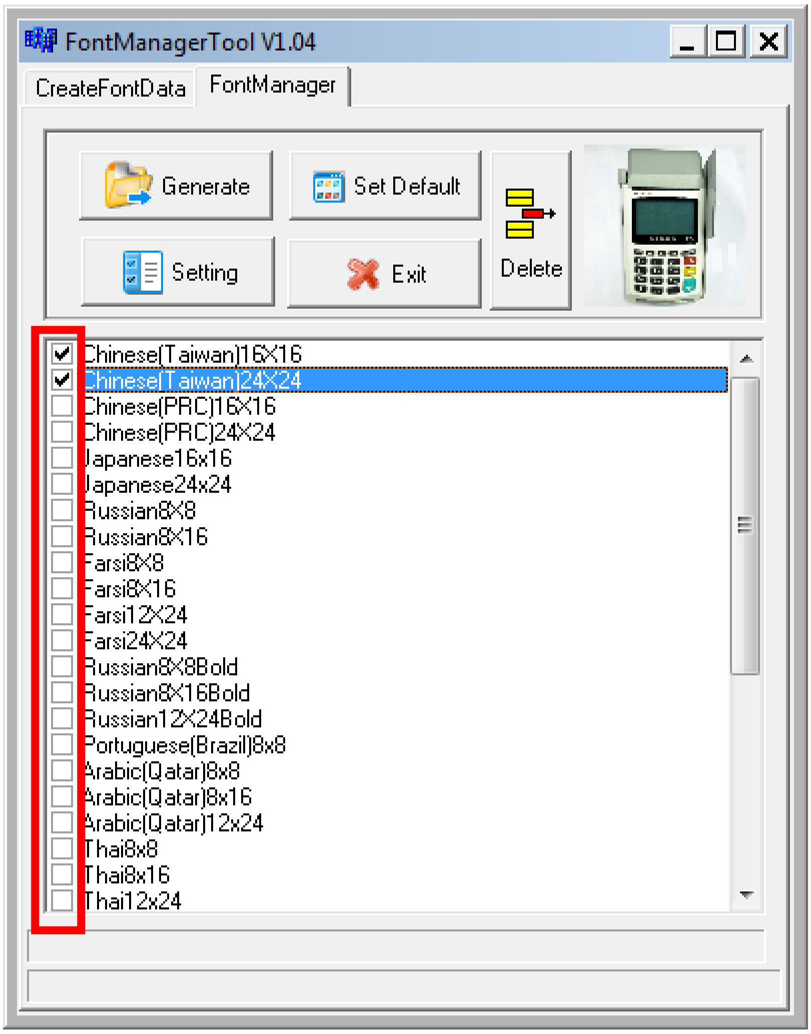
- Run FontManager.exe



FontManagerTool.exe
19/12/2012 12:02 AM
1.04 MB

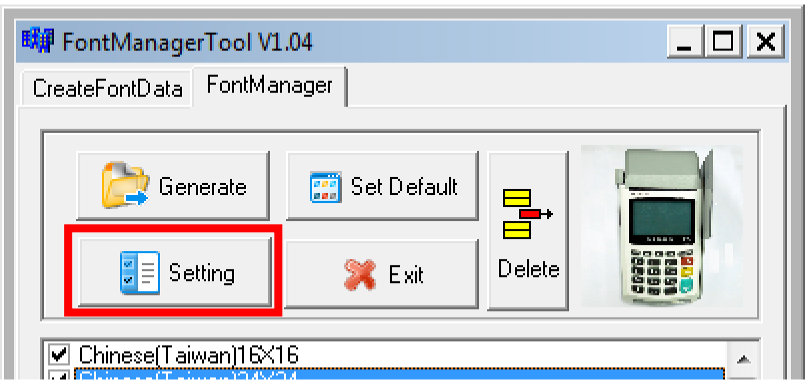
Located at C:\Program Files\Castles\Font Manager

- Select font to download



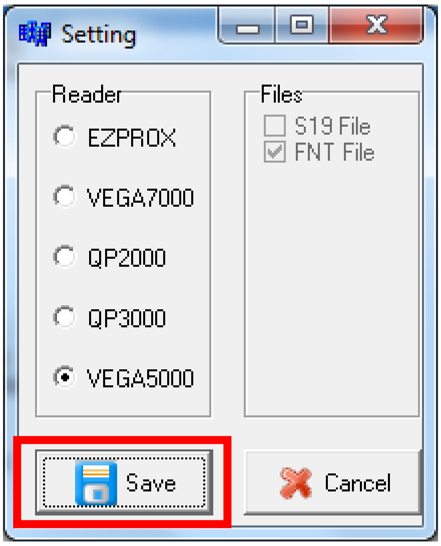
☑ Chinese(Taiwan)16X16
☑ Chinese(Taiwan)24X24
□ Chinese(PRC)16X16
□ Chinese(PRC)24X24
□ Japanese16x16
□ Japanese24x24
□ Russian8X8
□ Russian8X16
□ Farsi8X8
□ Farsi8X16
□ Farsi12X24
□ Farsi24X24
□ Russian8X8Bold
□ Russian8X16Bold
□ Russian12X24Bold
□ Portuguese(Brazil)8x8
□ Arabic(Qatar)8x8
□ Arabic(Qatar)8x16
□ Arabic(Qatar)12x24
□ Thai8x8
□ Thai8x16
□ Thai12x24

- Press [Setting] button to configure terminal type.



☑ Chinese(Taiwan)16X16

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



Reader

○ EZPROX

○ VEGA7000

○ QP2000

○ QP3000

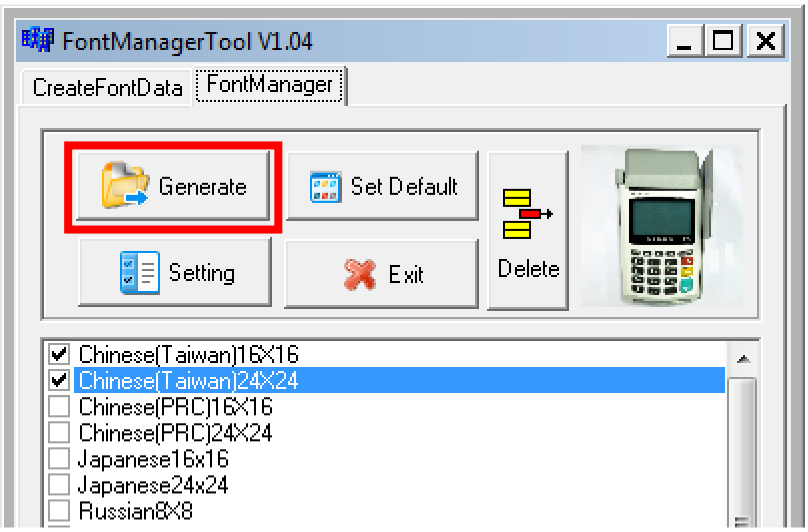
● VEGA5000

Files

□ S19 File

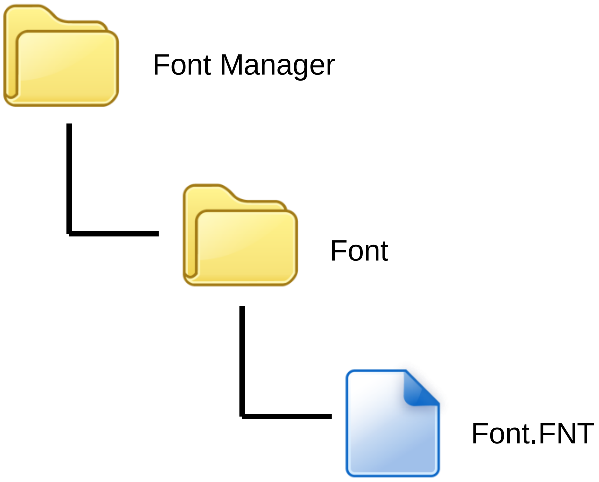
☑ FNT File

- Press [Generate] to create the font file.

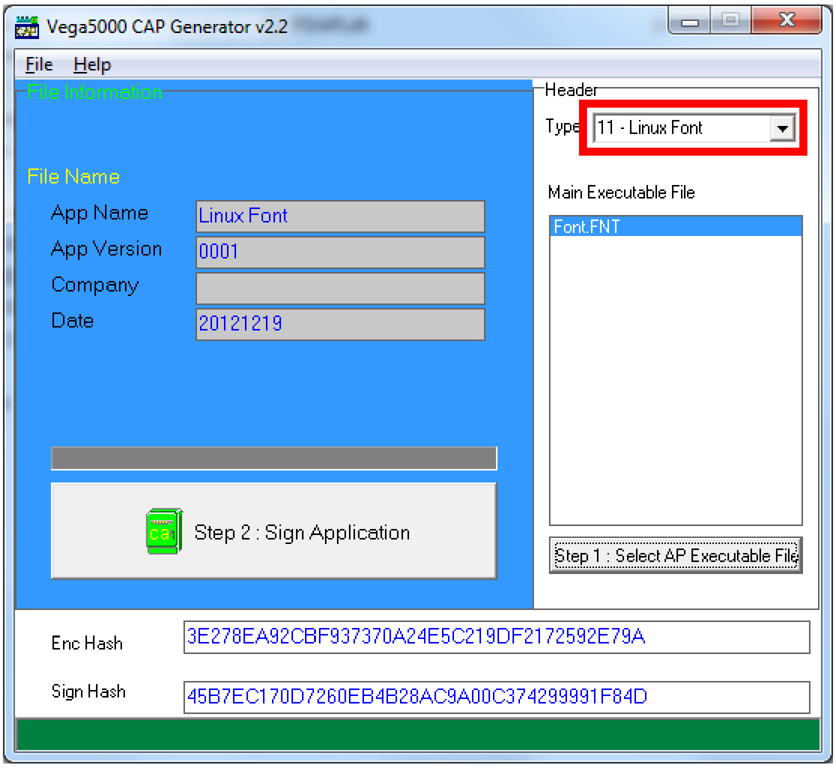


☑ Chinese(Taiwan)16X16
☑ Chinese(Taiwan)24X24
□ Chinese(PRC)16X16
□ Chinese(PRC)24X24
□ Japanese16x16
□ Japanese24x24
□ Russian8X8

- 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”.


Vega5000 CAP Generator v2.2
File
Help
File Information
Header
Step 2 : Sign Application
Step 1 : Select AP Executable File

Type: 11 - Linux Font

File Name

App Name: Linux Font

App Version: 0001

Company:

Date: 20121219

Main Executable File: Font.FNT

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A

Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

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

5.2. Custom Font

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

There are two zone defined:

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

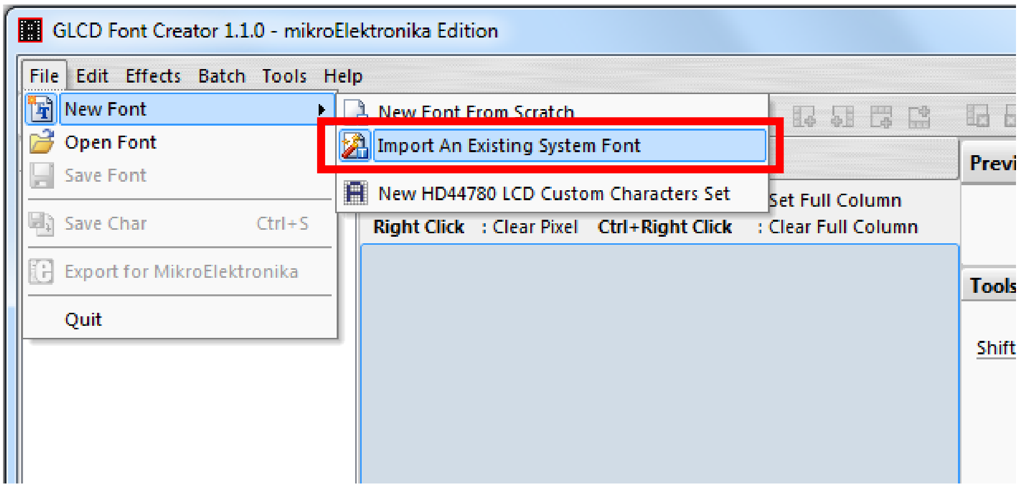
Zone 0x80 ~ 0xFF – Free to use, you may use for symbols.

<u>Following steps demonstrate how to create a 12x24 font.</u>

- Run GLCD Font Creator

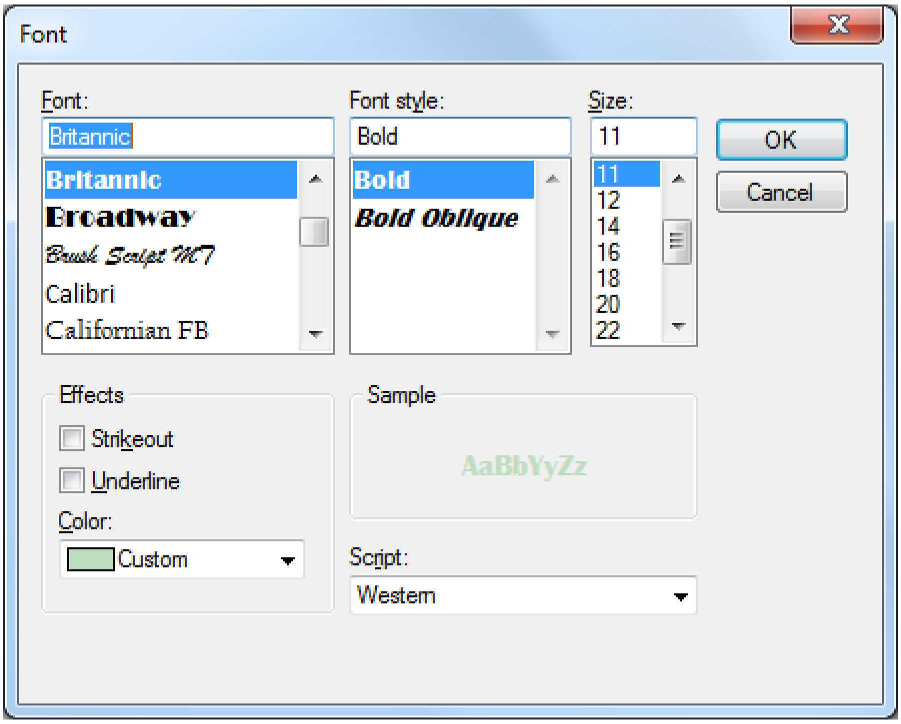
GLCDFontCreator.exe
GLCD Font Creator
Pocket MicroTechnics

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



GLCD Font Creator 1.1.0 - mikroElektronika Edition
File
Edit
Effects
Batch
Tools
Help
New Font
Open Font
Save Font
Save Char Ctrl+S
Export for MikroElektronika
Quit
New Font From Scratch
Import An Existing System Font
New HD44780 LCD Custom Characters Set
Set Full Column
Right Click : Clear Pixel
Ctrl+Right Click : Clear Full Column
Previ
Tools
Shift

- 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.



Font

Font: Britannic

Britannic
Broadway
Brush Script MT
Calibri
Californian FB

Font style: Bold

Bold
Bold Oblique

Size: 11

11
12
14
16
18
20
22

Effects

□ Strikeout

□ Underline

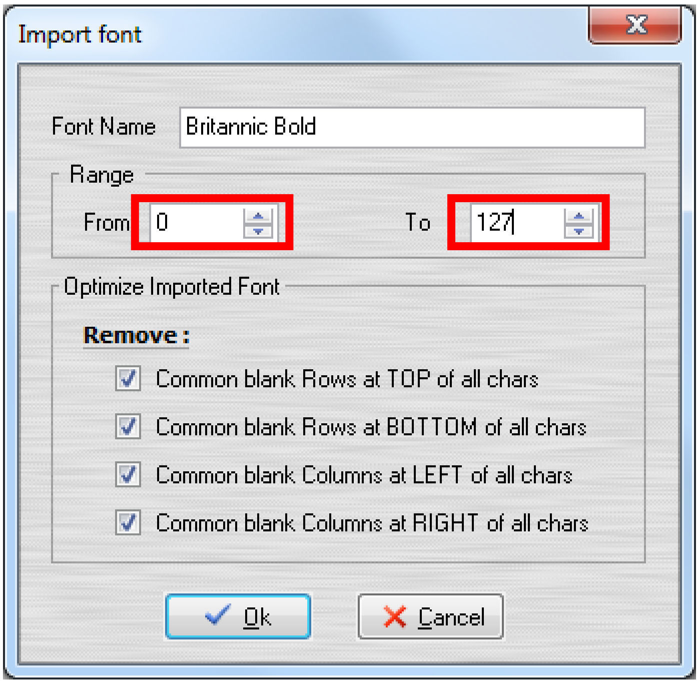
Color: Custom

Sample

AaBbYyZz

Script: Western

- Set the import range from 0 to 127.



Import font

Font Name Britannic Bold

Range

From 0 To 127

Optimize Imported Font

Remove :

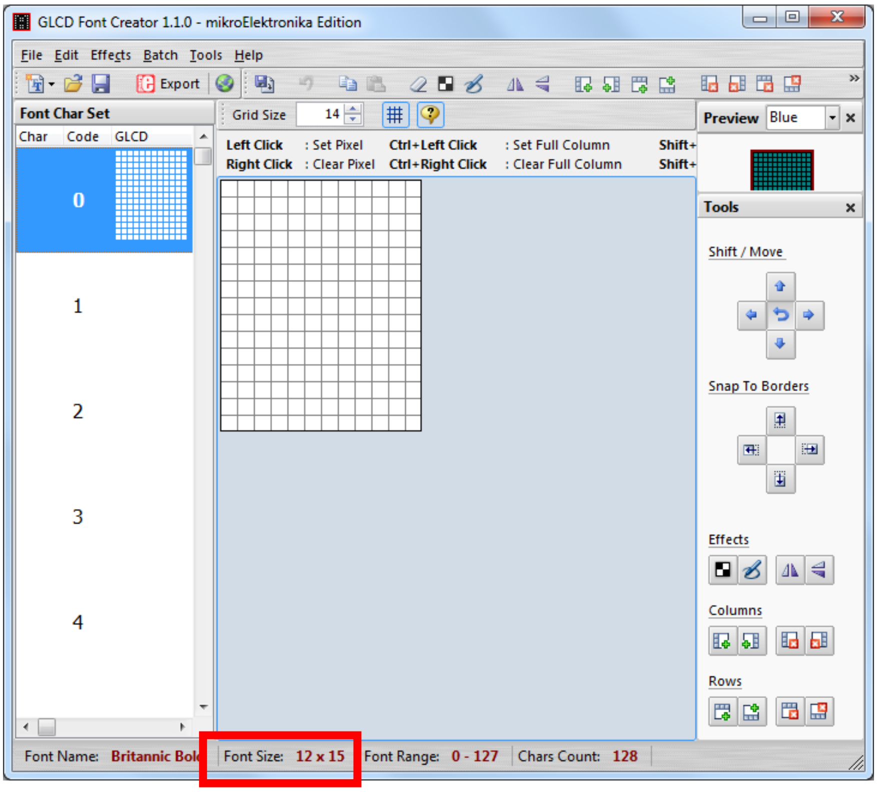
☑ Common blank Rows at TOP of all chars

☑ Common blank Rows at BOTTOM of all chars

☑ Common blank Columns at LEFT of all chars

☑ Common blank Columns at RIGHT of all chars

- Check the minimum pixel width and height.

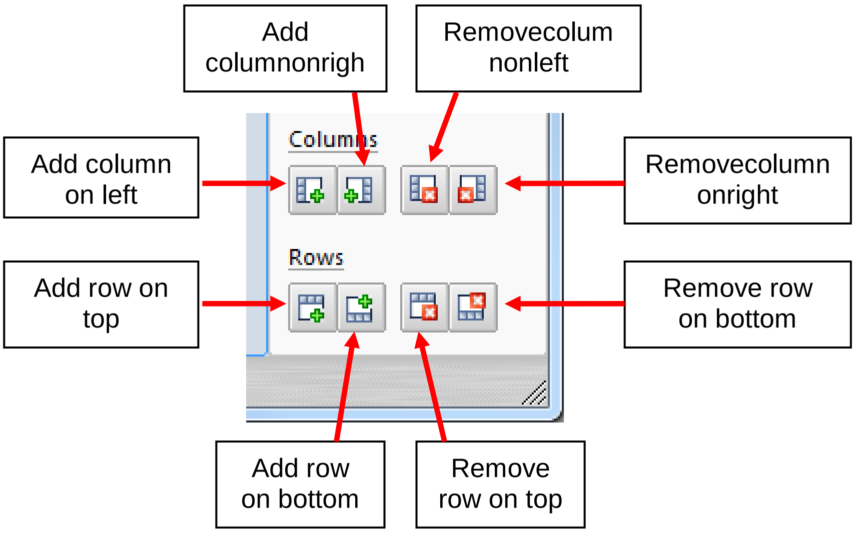


Left Click : Set Pixel
Right Click : Clear Pixel
Ctrl+Left Click : Set Full Column
Ctrl+Right Click : Clear Full Column
Shift+
Shift+

Font Name: Britannic Bol | Font Size: 12 x 15 | Font Range: 0 - 127 | Chars Count: 128

- 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.



Add columnonrigh

Removecolum nonleft

Add column on left

Removecolumn onright

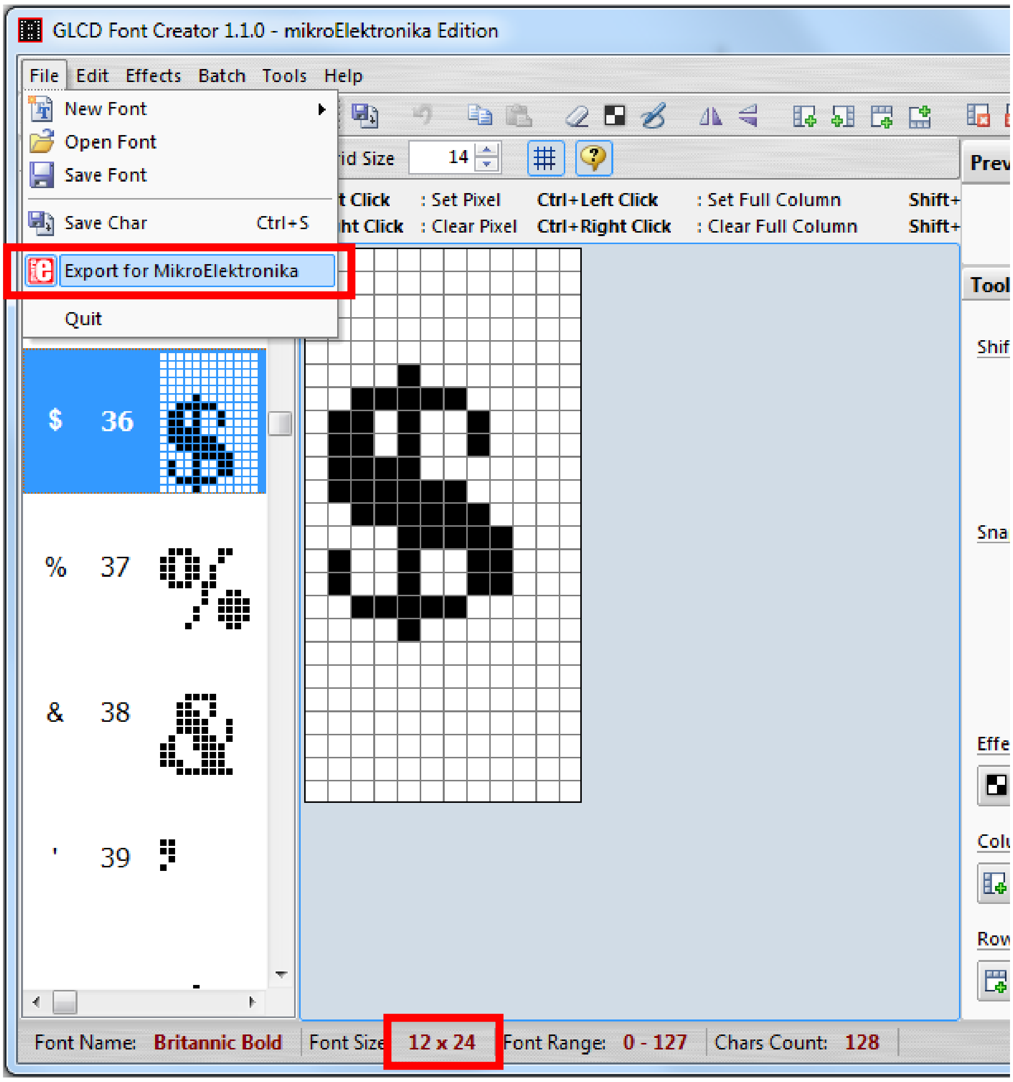
Add row on top

Remove row on bottom

Add row on bottom

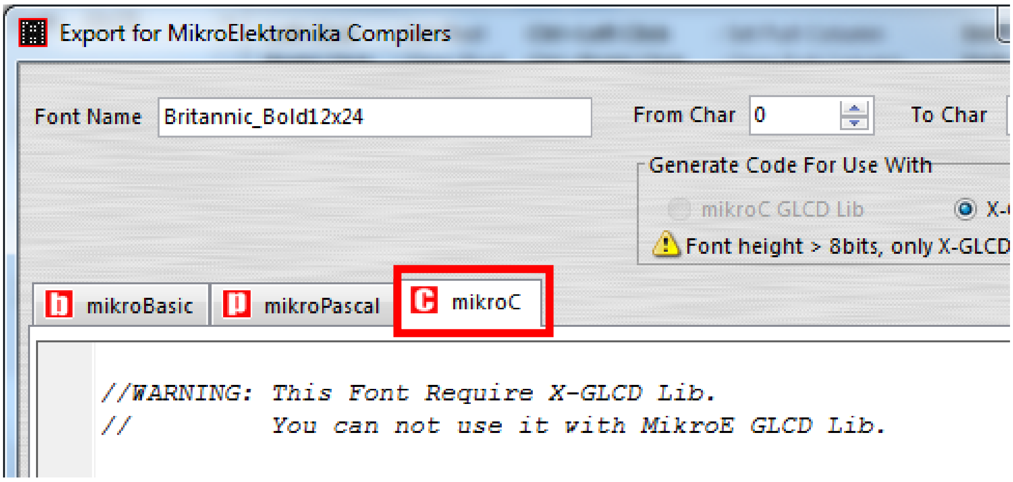
Remove row on top

- After adjust font size, select [File] ➪ [Export for MicroElektronika].


GLCD Font Creator 1.1.0 - mikroElektronika Edition
File Edit Effects Batch Tools Help
New Font
Open Font
Save Font
Save Char Ctrl+S
Export for MikroElektronika
Quit
id Size 14
Prev
t Click : Set Pixel Ctrl+Left Click : Set Full Column Shift+
ht Click : Clear Pixel Ctrl+Right Click : Clear Full Column Shift+
Tool
$ 36
% 37
& 38
' 39

Font Name: Britannic Bold | Font Size 12 x 24 | Font Range: 0 - 127 | Chars Count: 128

- Select output format as [mikroC].

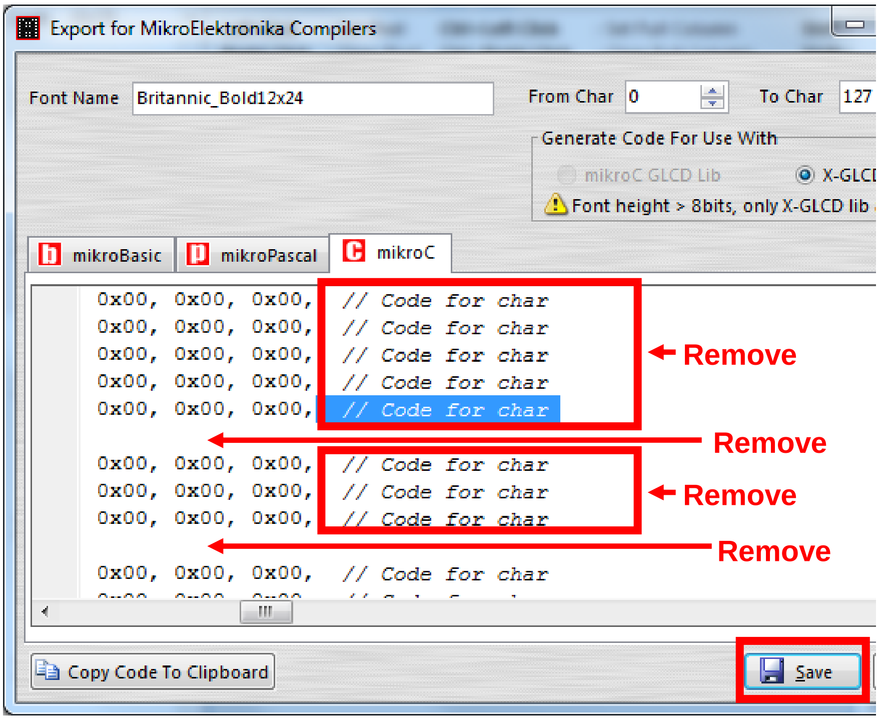

Export for MikroElektronika Compilers
Generate Code For Use With
○ mikroC GLCD Lib
● X-
mikroBasic
mikroPascal
mikroC

Font Name: Britannic_Bold12x24
From Char: 0
To Char

⚠ Font height > 8bits, only X-GLCD

```
//WARNING: This Font Require X-GLCD Lib.
//         You can not use it with MikroE GLCD Lib.
```

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



Export for MikroElektronika Compilers

Font Name Britannic_Bold12x24

From Char 0 To Char 127

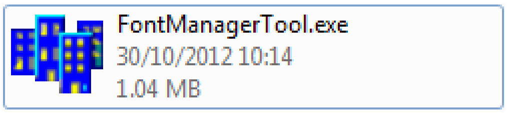
Generate Code For Use With

○ mikroC GLCD Lib ● X-GLCD

Font height > 8bits, only X-GLCD lib

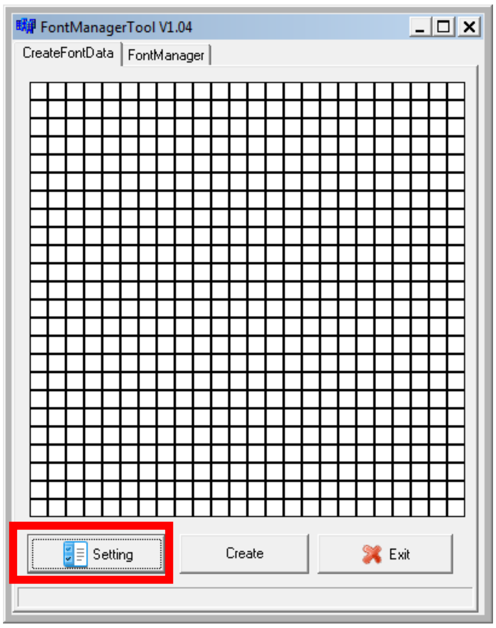
```
0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char

0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char
0x00, 0x00, 0x00,  // Code for char

0x00, 0x00, 0x00,  // Code for char
```

- Run Font Manager Tool.

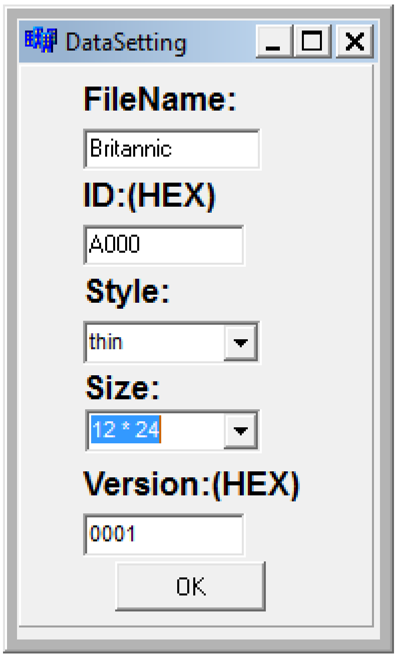


FontManagerTool.exe
30/10/2012 10:14
1.04 MB

- Click [Setting] button



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



FileName: Britannic

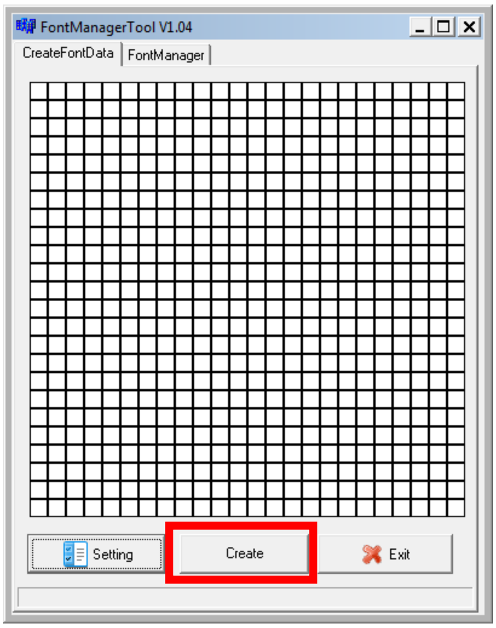
ID:(HEX) A000

Style: thin

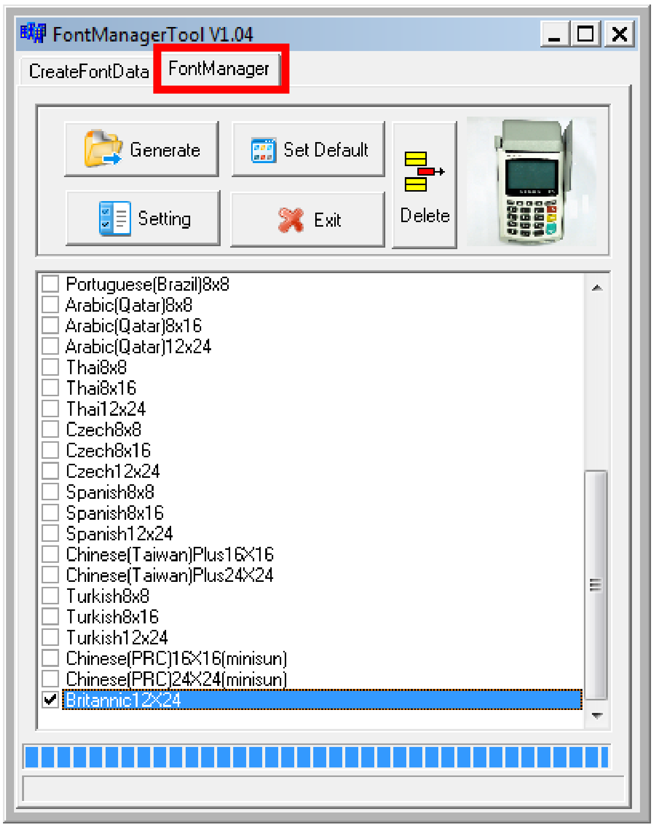
Size: 12 * 24

Version:(HEX) 0001

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



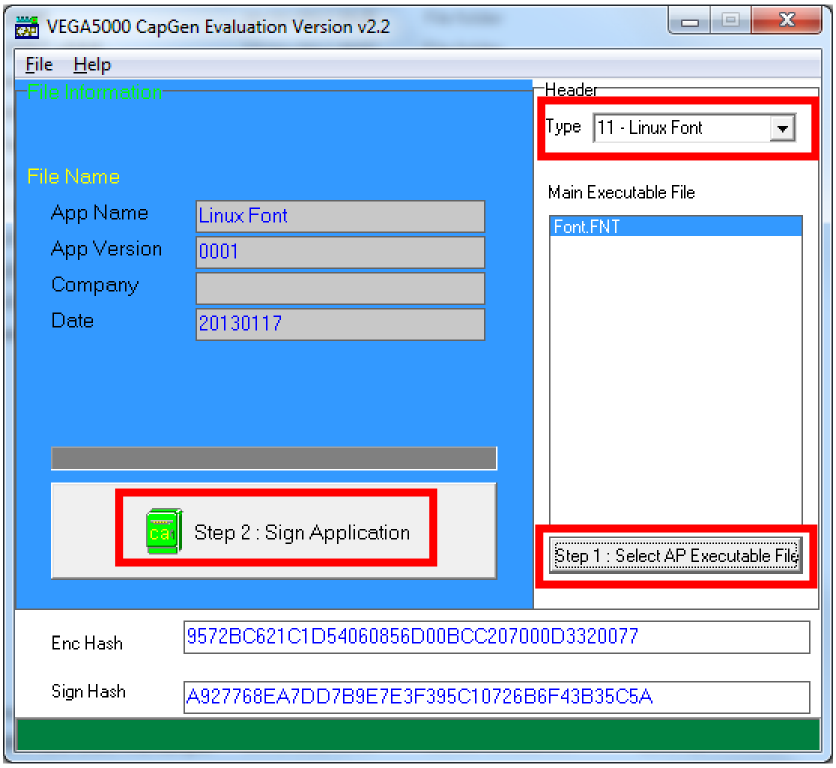
- Select [Font Manager] tab and tick the newly created font, and press [Generate] button to export to FNT file.



□ Portuguese(Brazil)8x8
□ Arabic(Qatar)8x8
□ Arabic(Qatar)8x16
□ Arabic(Qatar)12x24
□ Thai8x8
□ Thai8x16
□ Thai12x24
□ Czech8x8
□ Czech8x16
□ Czech12x24
□ Spanish8x8
□ Spanish8x16
□ Spanish12x24
□ Chinese(Taiwan)Plus16X16
□ Chinese(Taiwan)Plus24X24
□ Turkish8x8
□ Turkish8x16
□ Turkish12x24
□ Chinese(PRC)16X16(minisun)
□ Chinese(PRC)24X24(minisun)
☑ Britannic12X24

- 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.


VEGA5000 CapGen Evaluation Version v2.2
File
Help
File Information
Header
Step 2 : Sign Application
Step 1 : Select AP Executable File

Type: 11 - Linux Font

File Name

App Name: Linux Font

App Version: 0001

Company:

Date: 20130117

Main Executable File: Font.FNT

Enc Hash: 9572BC621C1D54060856D00BCC207000D3320077

Sign Hash: A927768EA7DD7B9E7E3F395C10726B6F43B35C5A

- 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.

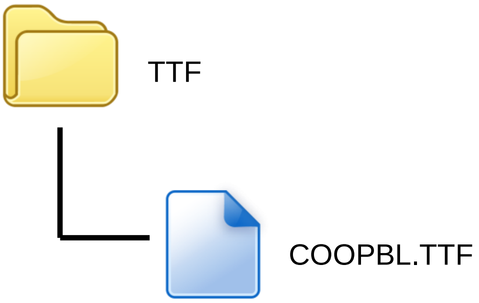
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

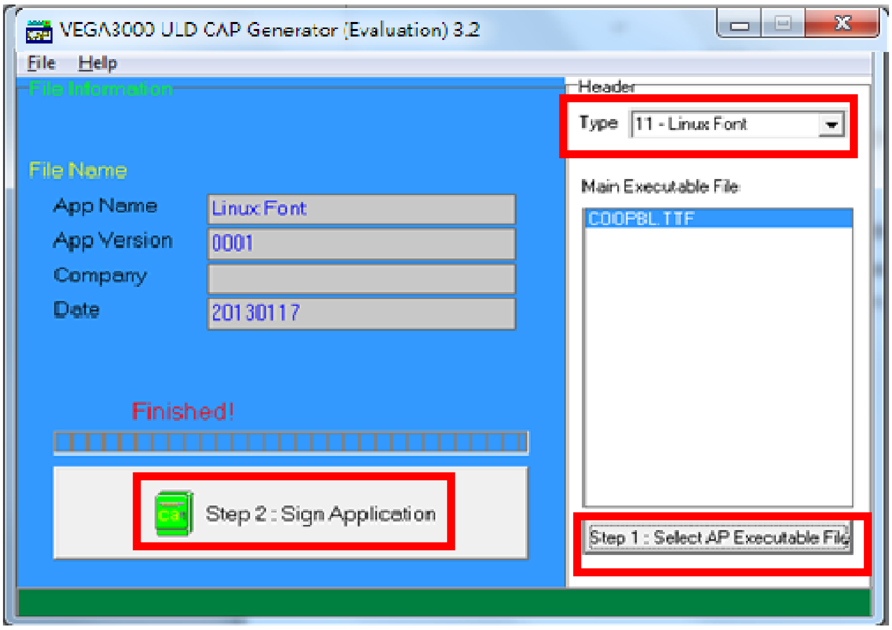
TrueType Font (TTF) is supported in VEGA3000 terminal / pinpad. You can download the TrueType font to terminal / pinpad for displaying or printing.

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

- Copy the TTF file needed to an 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.


VEGA3000 ULD CAP Generator (Evaluation) 3.2
File
Help
File Information
Header
File Name
Finished!
Step 2 : Sign Application
Main Executable File
Step 1 : Select AP Executable File

Type: 11 - Linux Font

App Name: Linux Font

App Version: 0001

Company:

Date: 20130117

COOPBL.TTF

- Download the font CAP file to terminal / pinpad.

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

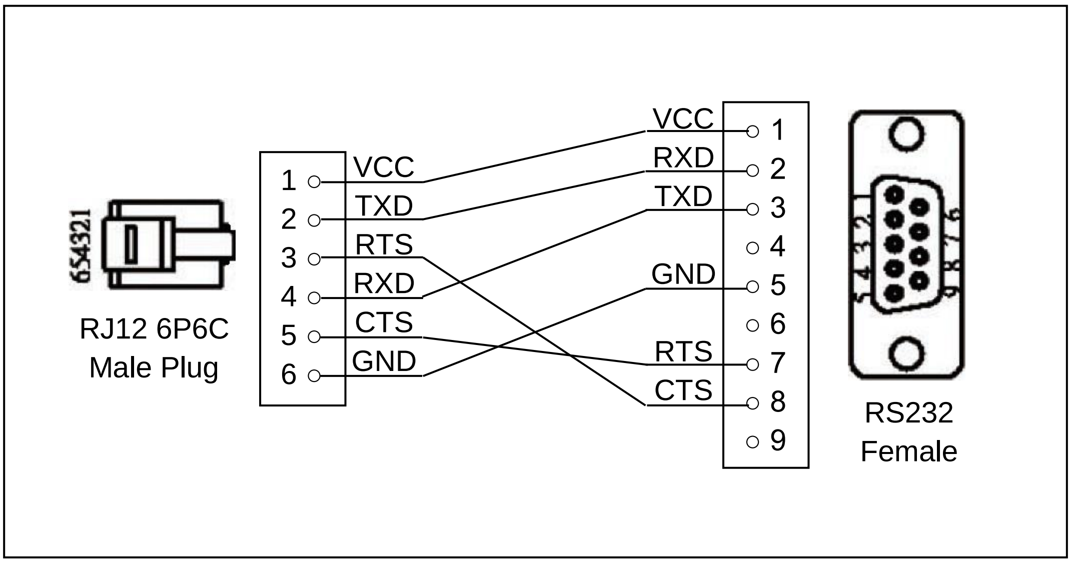
```
CTOS_LCDTTFSelect("COOPBL.TTF", 0);
CTOS_LCDFontSelectMode(d_FONT_TTF_MODE);
CTOS_LCDTSelectFontSize(0x203C); // 32x60
CTOS_LCDTClearDisplay();
CTOS_LCDTPrintXY(1, 1, "Hello World");
```

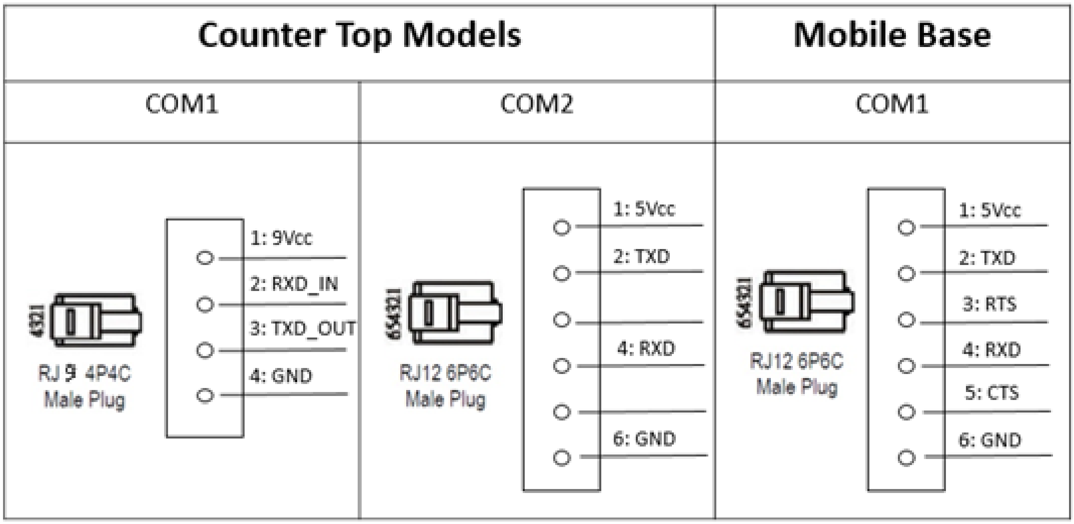
Or print message using the newly added font.

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

6. Technical Notes

6.1. Serial Cable PIN Assignment





Counter Top Models		Mobile Base
COM1	COM2	COM1
4321 RJ 9 4P4C Male Plug 1: 9Vcc 2: RXD_IN 3: TXD_OUT 4: GND	654321 RJ12 6P6C Male Plug 1: 5Vcc 2: TXD 4: RXD 6: GND	654321 RJ12 6P6C Male Plug 1: 5Vcc 2: TXD 3: RTS 4: RXD 5: CTS 6: GND

~ END ~