CASTLES TECHNOLOGY

UPT1000M

Book 2

User Manual

Confidential

Version 1.1

Jul. 2019

Castles Technology Co., Ltd.

6F, No. 207-5, Sec. 3, Beixin Rd., Xindian District,
New Taipei City 23143, Taiwan R.O.C.
http://www.castech.com.tw

WARNING

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

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

All trademarks mentioned are proprietary of their respective owners.

ATTENTION

Les informations contenues dans ce document sont sujettes à modification sans préavis.

Aucune partie de cette publication ne peut être reproduite, transmise, stockée dans un système de recherche, ni traduite dans un langage humain ou informatique, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, magnétique, optique, chimique, manuel ou autre, sans l'autorisation écrite préalable de **Castles Technology Co., Ltd.**

Toutes les marques citées appartiennent à leurs propriétaires respectifs.

Revision History

Version	*Date*	*Descriptions*	*Author*
1.0	May 30, 2019	Initial creation.	Jeffrey
1.1	Jul 19, 2019	1. Modify the picture. 2. Modify the UL Caution.	Jeff

Contents

1. Introduction

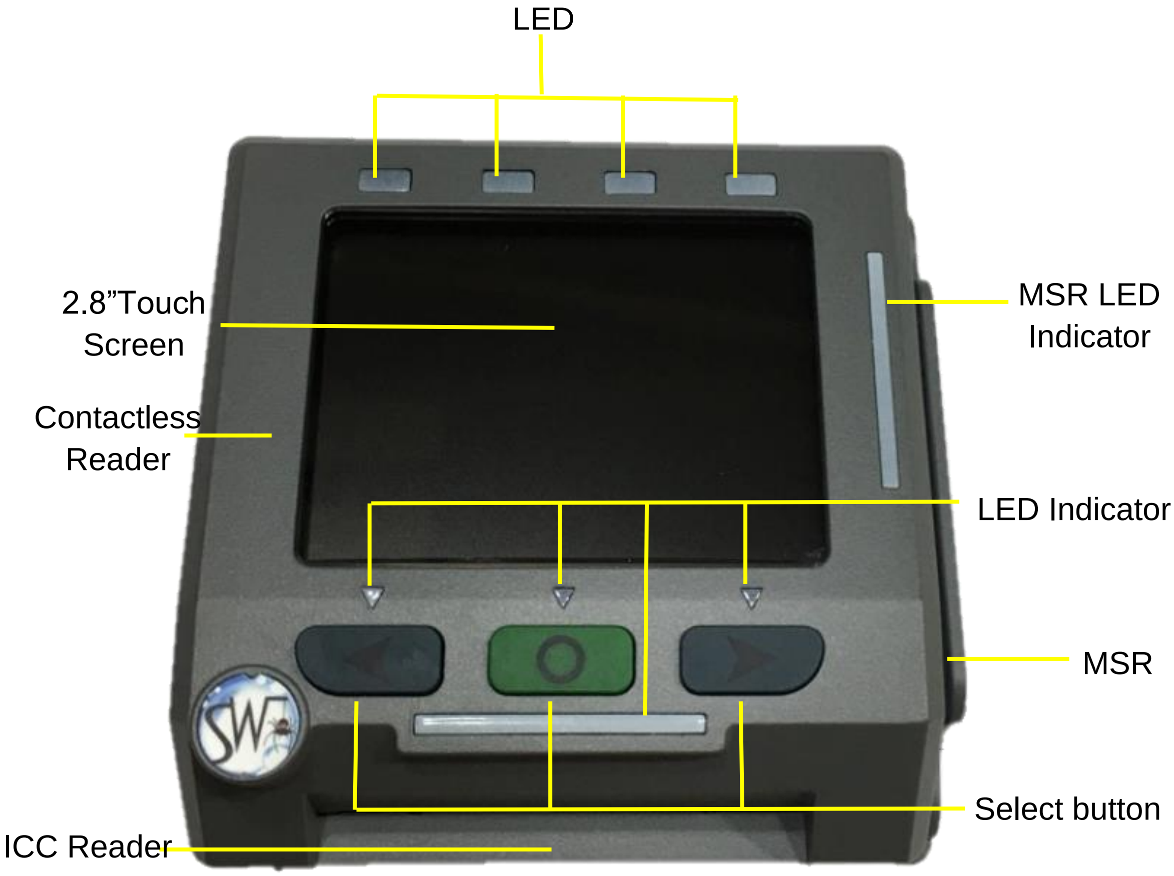
This document provides a guideline on operating and configuring Castles UPT1000M.

The scope of this document includes setting up the UPT1000M, basic operation, application life cycle, and some advance features.

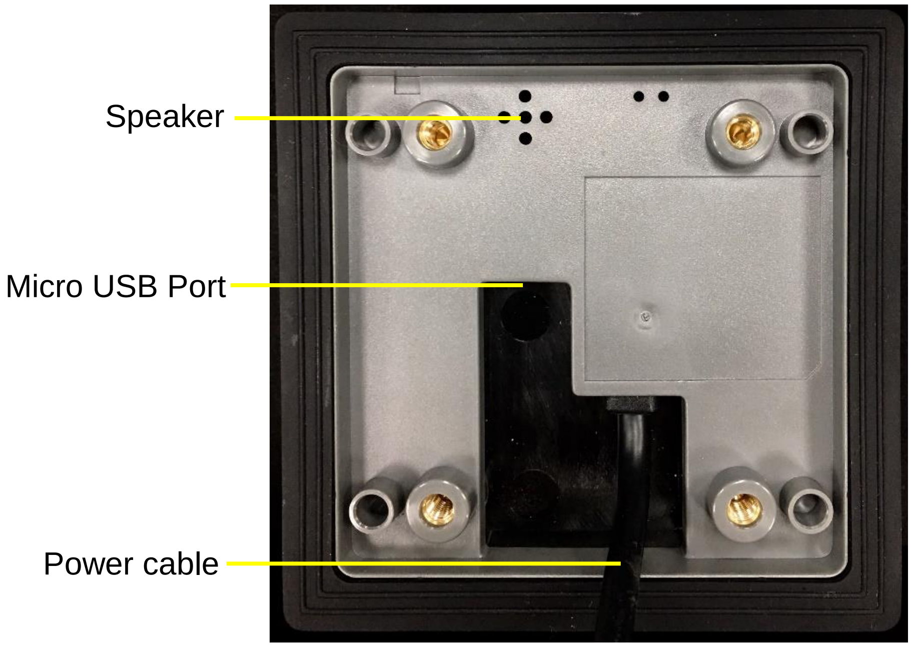
2. Hardware Setup

2.1. Parts of the UPT1000M

Front View



Rear View

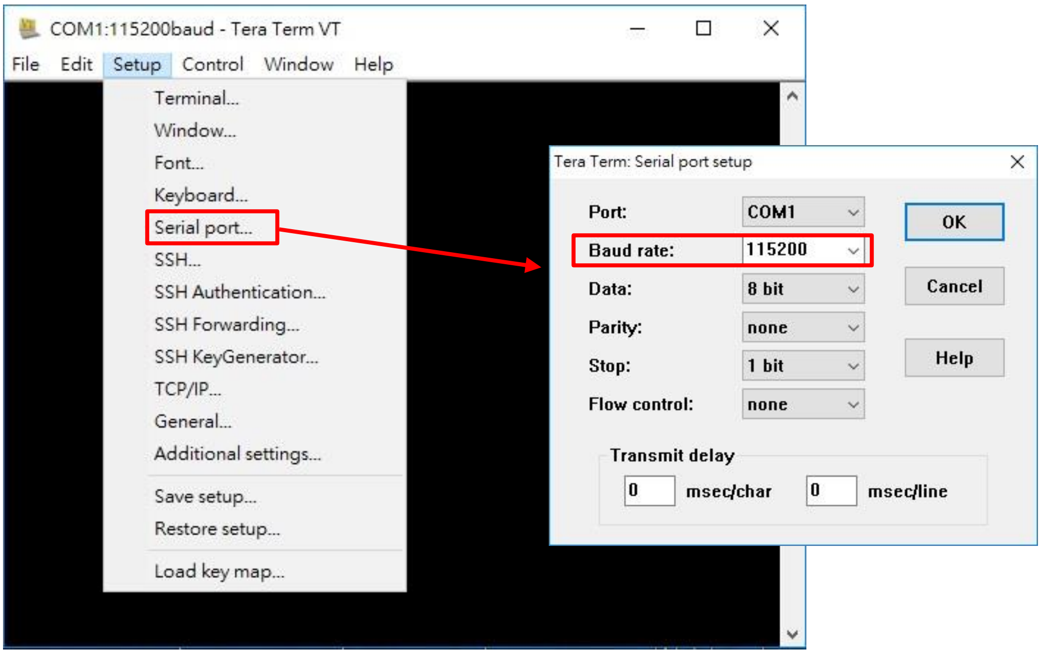


3. Basic Operation

3.1. Program Manager

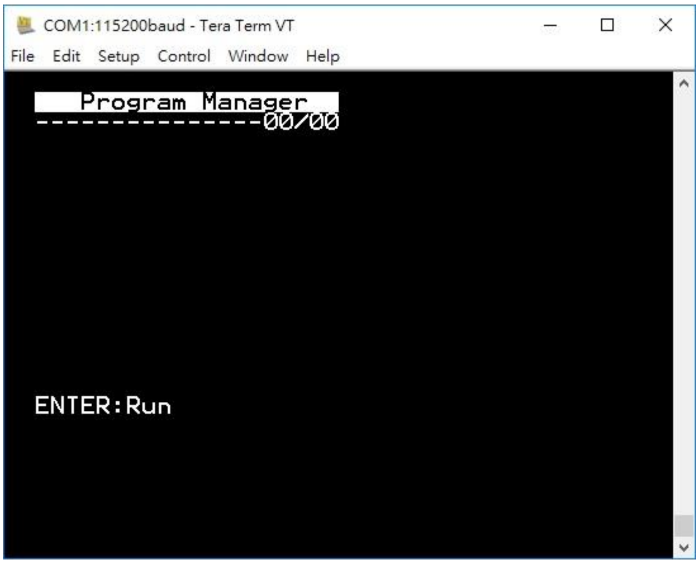
The UPT1000M is the terminal without keypad. Please follow the steps below to connect PC and UPT1000M for controlling.

- Power on UPT1000M and connect COM Port to PC.
- Run the application program such as “TeraTerm” or “PuTTY” on PC.
- Select “Serial port” to set the com port. The baud rate should be set to “115200”.



Port: COM1
Baud rate: 115200
Data: 8 bit
Parity: none
Stop: 1 bit
Flow control: none
Transmit delay
0 msec/char
0 msec/line

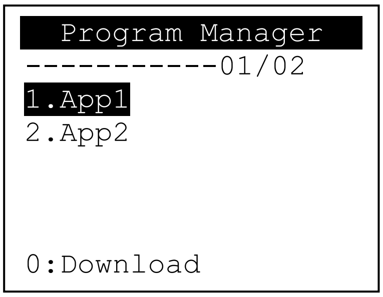
- Press any key on keyboard to refresh screen if doesn’t show “Program Manager” on “Tera Term” or PuTTY“.


COM1:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
 Program Manager 
----------------00/00



ENTER:Run
```

Once the power is on in normal status, UPT1000M will enter Program Manager if no default application selected. All user applications are listed in Program Manager. User 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 UPT1000M settings.

Program Manager

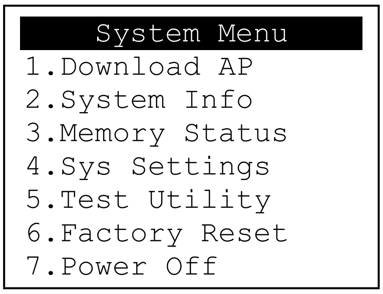


```
  Program Manager
-----------01/02
1.App1
2.App2



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 [↑] or [↓] as the up and down button to select application.

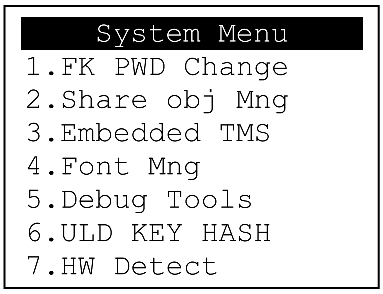
<u>System Menu</u>

Page 1



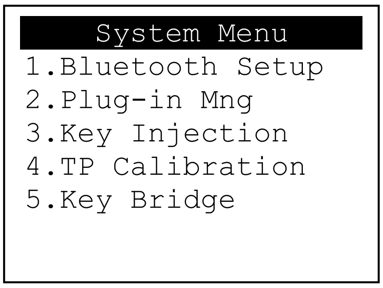
```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

Page 2



```
   System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

Page 3



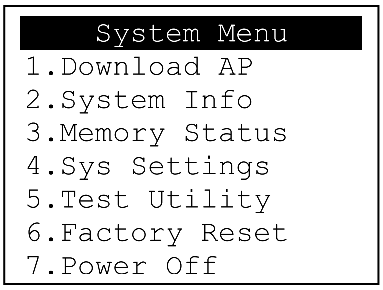
```
   System Menu
1.Bluetooth Setup
2.Plug-in Mng
3.Key Injection
4.TP Calibration
5.Key Bridge
```

- Press [↑] button to previous page.
- Press [↓] button to next page.

3.2. Download AP

Download user application or kernel modules firmware.

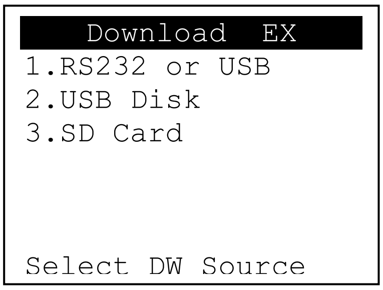
System Menu



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

- Press [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
```

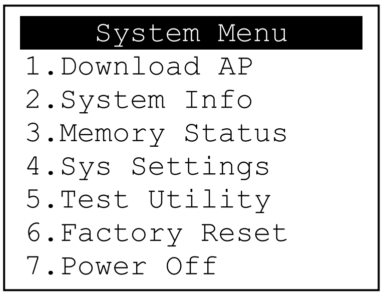
Select download source:

- 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. (Not support)

3.3. System Info

View kernel module firmware information.

System Menu

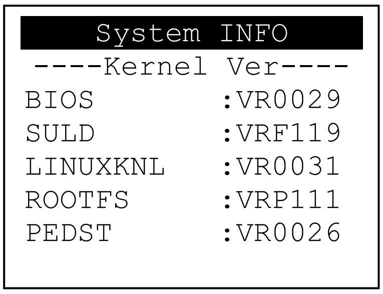


```
System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

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

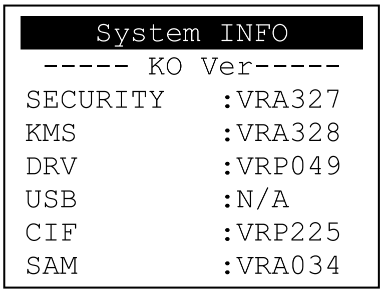
System Info Menu

Page 1



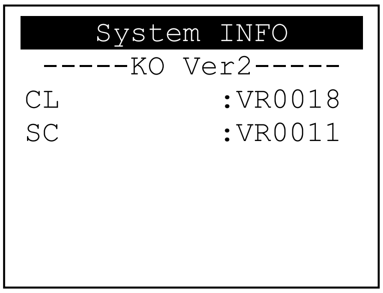
```
System INFO
----Kernel Ver----
BIOS          :VR0029
SULD          :VRF119
LINUXKNL      :VR0031
ROOTFS        :VRP111
PEDST         :VR0026
```

Page 2



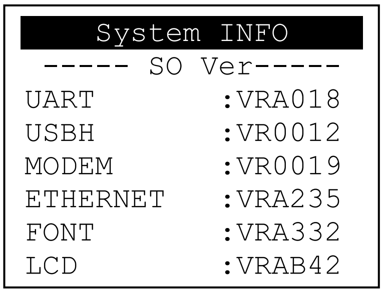
```
System INFO
----- KO Ver-----
SECURITY      :VRA327
KMS           :VRA328
DRV           :VRP049
USB           :N/A
CIF           :VRP225
SAM           :VRA034
```

Page 3



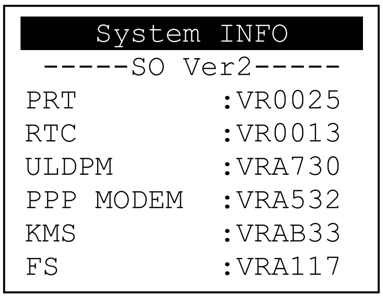
```
System INFO
-----KO Ver2-----
CL            :VR0018
SC            :VR0011
```

Page 4



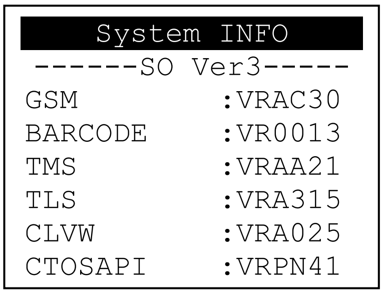
```
System INFO
----- SO Ver-----
UART          :VRA018
USBH          :VR0012
MODEM         :VR0019
ETHERNET      :VRA235
FONT          :VRA332
LCD           :VRAB42
```

Page 5



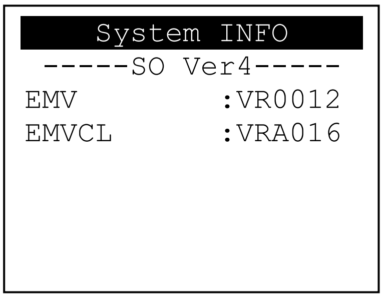
```
System INFO
-----SO Ver2-----
PRT           :VR0025
RTC           :VR0013
ULDPM         :VRA730
PPP MODEM     :VRA532
KMS           :VRAB33
FS            :VRA117
```

Page 6



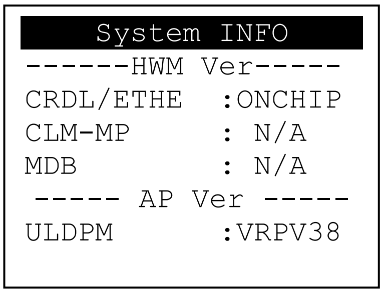
```
System INFO
------SO Ver3-----
GSM           :VRAC30
BARCODE       :VR0013
TMS           :VRAA21
TLS           :VRA315
CLVW          :VRA025
CTOSAPI       :VRPN41
```

Page 7



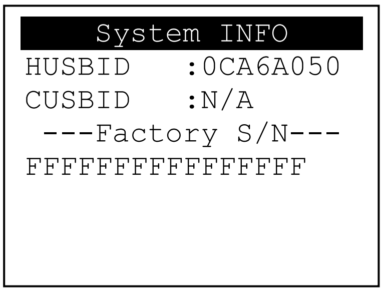
```
   System INFO
 -----SO Ver4-----
EMV          :VR0012
EMVCL        :VRA016
```

Page 8



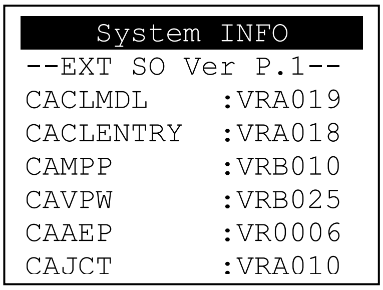
```
   System INFO
------HWM Ver-----
CRDL/ETHE   :ONCHIP
CLM-MP      : N/A
MDB         : N/A
 ----- AP Ver -----
ULDPM       :VRPV38
```

Page 9



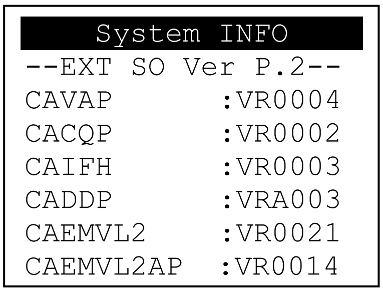
```
   System INFO
HUSBID   :0CA6A050
CUSBID   :N/A
 ---Factory S/N---
FFFFFFFFFFFFFFFF
```

Page 10



```
   System INFO
--EXT SO Ver P.1--
CACLMDL     :VRA019
CACLENTRY   :VRA018
CAMPP       :VRB010
CAVPW       :VRB025
CAAEP       :VR0006
CAJCT       :VRA010
```

Page 11



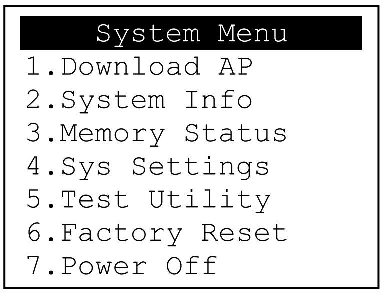
```
   System INFO
--EXT SO Ver P.2--
CAVAP       :VR0004
CACQP       :VR0002
CAIFH       :VR0003
CADDP       :VRA003
CAEMVL2     :VR0021
CAEMVL2AP   :VR0014
```

- Press [↑] button to previous page.
- Press [↓] button to next page.

3.4. Memory Status

View flash memory and RAM information.

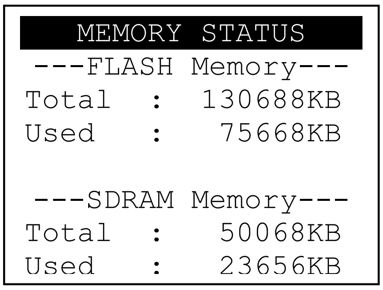
System Menu



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

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

Memory Status Menu



```
   MEMORY STATUS
 ---FLASH Memory---
Total  :  130688KB
Used   :   75668KB

 ---SDRAM Memory---
Total  :   50068KB
Used   :   23656KB
```

3.5. System Settings

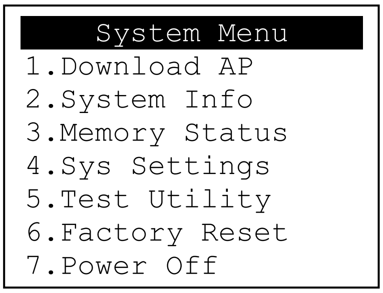
View or change system settings.

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 selected application after system boot up. Default AP Name will display on next line. Set Default AP in PM by pressing 1.DefSel. User can keep press and leave “X” button during System Initializing to force leave the default AP execution process.
USB CDC Mode	Enable (Y) or disable (N) USB CDC Mode to communicate with PC. Device will be recognized as a COM port in Windows Device Manager. Make sure this setting is Y before loading Files.
FunKey PWD	Enable (Y) or disable (N) password protection to access function key. Default password is 0000; User need to enter password if they would like to use function keys in Program Manager like 0: Download (System Menu), 1:Set Default AP, 2: Delete AP, 3: AP Info. User can change this password in System Menu “FK PWD Change”.
PMEnter PWD	Enable (Y) or disable (N) password protection to enter Program Manager. Default password is 0000. User need to enter password when accessing PM. E.g. After power up or Reboot device; leaving AP.
SET USB Host	Enable (Y) or disable (N) USB Host Mode for external accessories. Make sure this setting is N before download AP or File. The setting only can control USB1, USB 2 always use as USB Host Mode.(If terminal has USB2)
Base USB CDC	Enable (Y) or disable (N) USB CDC Mode of VEGA series base/cradle.(Not Support)

List SHR Lib	Enable (Y) or disable (N) to list all shared libraries in Program Manager. If the setting is N, PM will only display AP. User can also find the Share Lib in Share obj Mng -> Share LIB.
Key MNG Mode	**<TBC>**
BATThreshld	Not Support.
Null Cradle	Not Support.
Debug Mode	Enable (Y) or disable (N) console debug mode for output debug log from specific port..
Debug Port	Select serial port for console debug (1, U, F). (Press button "1", "2", "3", to choose "COM", , "USB", "File").
Mobil AutoON	Enable (Y) or disable (N) to auto turn on GSM module after power up. Enable this setting may consume more power of battery however it can buy some time for the first GSM module open in AP
Bklit Auto Off	Enable (Y) or disable (N) Auto Off LCD Backlight. Battery protect mode Standby/Sleep is more useful for saving the power.
Bklit Off Time	Threshold in seconds of Auto Off LCD Backlight.
PWR KEY OFF	Set the behavior for long pressing power key, Power off (Y), Reboot (N) or Disable function (D).
GDB Mode	Not Support.
GDB Timeout	Not Support.
GDB Channel	Not Support.
ETHER IP/PORT	Not Support.
RTC Time Zone	Set Time Zone of RTC (Real Time Clock).
NTP Enable	Enable (Y) or disable (N) Network Time Protocol
NTP Update Freq	Set update frequency of Network Time Protocol.
Halt Timeout	Set timeout of AP to get back to Program Manager whenever AP is in halt state.
PWM Auto	Enable (Y) or disable (N) power saving mode.
PWM Mode	Select (STB) standby mode or (SLP) sleep mode for power saving mode.

PWM Time	Set time period by which to make terminal getting into power saving mode from idle state.
BAT PROTECT MODE	Not support.
Redirect Mode	Enable (Y) or disable (N) redirect mode for communication between terminal and external device.
Redirect Port	Select redirect communication port
Redirect LCD	Enable (Y) or disable (N) to mapping the LCD message to console tool (e.g.Tera Term) in redirect mode.
Redirect KEY	Enable (Y) or disable (N) to mapping the keypad message to console tool (e.g.Tera Term) in redirect mode.

System Menu

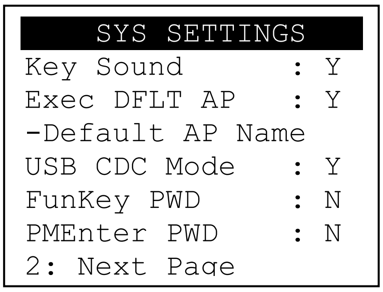


```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

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

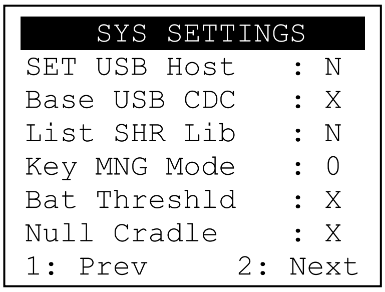
System Settings Menu

Page 1



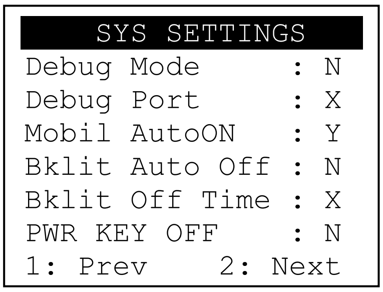
```
   SYS SETTINGS
Key Sound       : Y
Exec DFLT AP    : Y
-Default AP Name
USB CDC Mode    : Y
FunKey PWD      : N
PMEnter PWD     : N
2: Next Page
```

Page 2



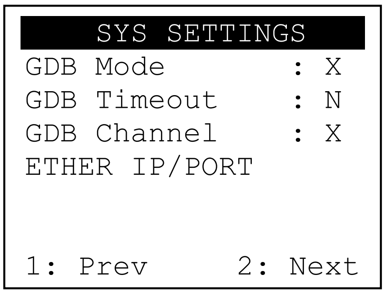
```
   SYS SETTINGS
SET USB Host    : N
Base USB CDC    : X
List SHR Lib    : N
Key MNG Mode    : 0
Bat Threshld    : X
Null Cradle     : X
1: Prev     2: Next
```

Page 3



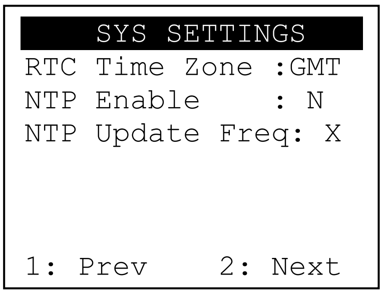
```
   SYS SETTINGS
Debug Mode      : N
Debug Port      : X
Mobil AutoON    : Y
Bklit Auto Off  : N
Bklit Off Time  : X
PWR KEY OFF     : N
1: Prev    2: Next
```

Page 4



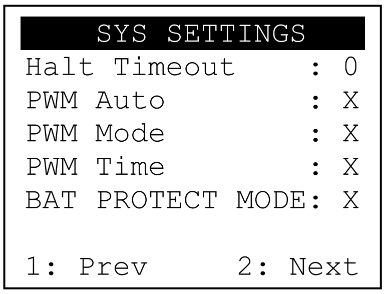
```
   SYS SETTINGS
GDB Mode        : X
GDB Timeout     : N
GDB Channel     : X
ETHER IP/PORT


1: Prev     2: Next
```

Page 5



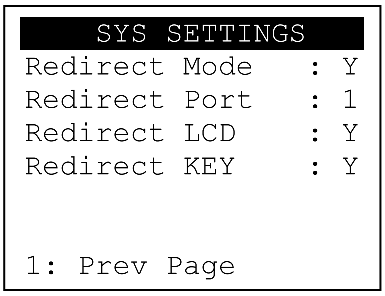
```
   SYS SETTINGS
RTC Time Zone :GMT
NTP Enable     : N
NTP Update Freq: X



1: Prev    2: Next
```

Page 6



```
   SYS SETTINGS
Halt Timeout     : 0
PWM Auto         : X
PWM Mode         : X
PWM Time         : X
BAT PROTECT MODE: X

1: Prev     2: Next
```

Page 7



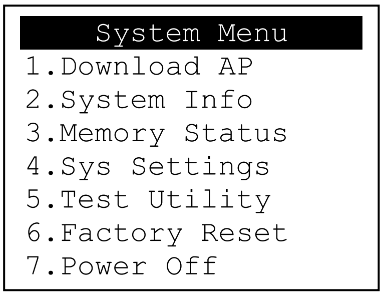
```
    SYS SETTINGS
Redirect Mode   : Y
Redirect Port   : 1
Redirect LCD    : Y
Redirect KEY    : Y


1: Prev Page
```

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

3.6. Test Utility

Perform hardware components diagnosis.

System Menu

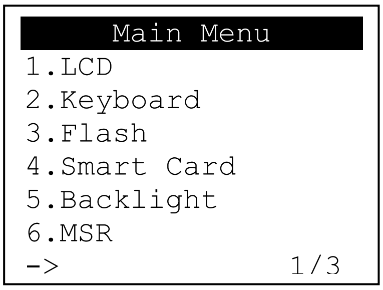


```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

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

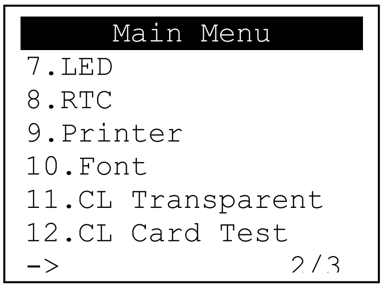
Test Utility Menu

Page 1



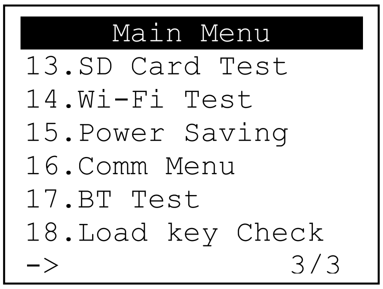
```
    Main Menu
1.LCD
2.Keyboard
3.Flash
4.Smart Card
5.Backlight
6.MSR
->              1/3
```

Page 2



```
    Main Menu
7.LED
8.RTC
9.Printer
10.Font
11.CL Transparent
12.CL Card Test
->              2/3
```

Page 3



```
    Main Menu
13.SD Card Test
14.Wi-Fi Test
15.Power Saving
16.Comm Menu
17.BT Test
18.Load key Check
->              3/3
```

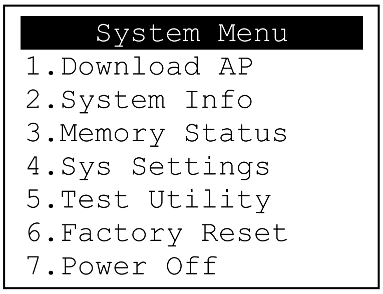
- Press [1] and [OK] to diagnose LCD.
- Press [2] and [OK] to diagnose keyboard.
- Press [3] and [OK] to diagnose flash memory.
- Press [4] and [OK] to diagnose smart card module.
- Press [5] and [OK] to diagnose backlight.
- Press [6] and [OK] to diagnose magnetic stripe card reader.

- Press [7] and [OK] to diagnose LED.
- Press [8] and [OK] to diagnose RTC. ***(Default password is "8418")***
- Press [9] and [OK] to check Printer.
- Press [10] and [OK] to check FONT file in UPT1000M.
- Press [11] and [OK] to check CL transparent.
- Press [12] and [OK] to test Cantactless Card.
- Press [13] and [OK] to execute SD Card Test. (Not support)
- Press [14] and [OK] to test functionality of WiFi.
- Press [15] and [OK] to test functionality of power saving.
- Press [16] and [OK] to test functionality of multiple communication ways.
- Press [17] and [OK] to test functionality of Bluetooth.
- Press [18] and [OK] to check the ULD key hash whether the default key or not.
- Press [↑] button to previous page.
- Press [↓] button to next page.

3.7. Factory Reset

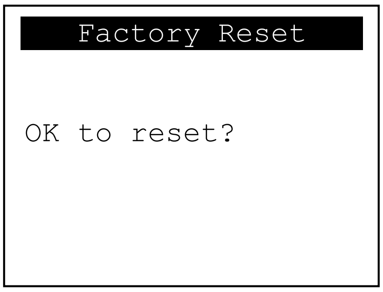
Perform factory reset, all user application, fonts and data will be deleted.

System Menu



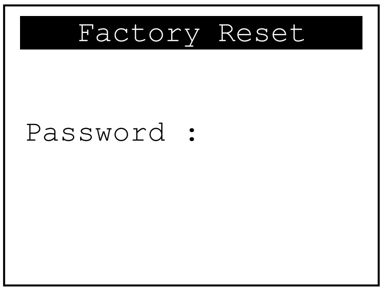
```
System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

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



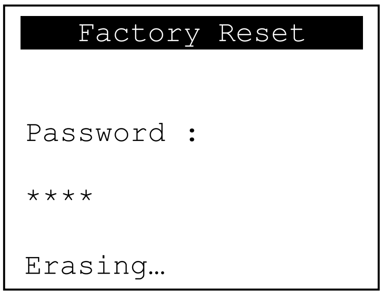
```
Factory Reset

OK to reset?
```

- Press [enter].



```
Factory Reset

Password :
```

- Enter factory reset password and press [enter].(***Default password: 8418)***



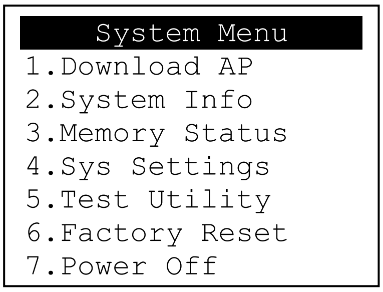
```
Factory Reset

Password :
****
Erasing…
```

- Start erasing, and then go back to Program Manager.

3.8. Power Off

Power off the machine.

System Menu



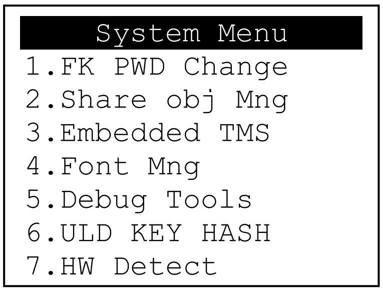
```
   System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
```

- Press [7] button to power off the machine.

3.9. FK PWD Change

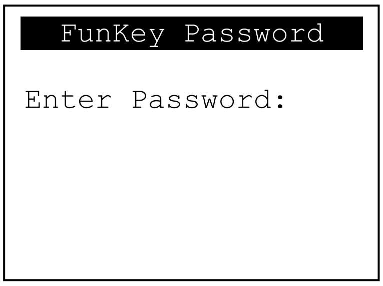
Change the function key password.

System Menu



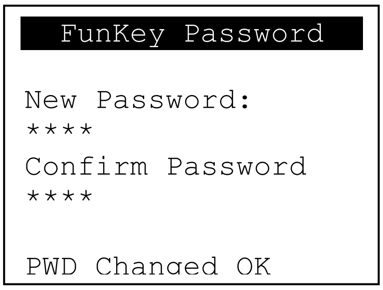
```
  System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

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



```
 FunKey Password

Enter Password:
```

- Enter current password and [enter]. ***(Default password is "0000")***



```
 FunKey Password

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

PWD Changed OK
```

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

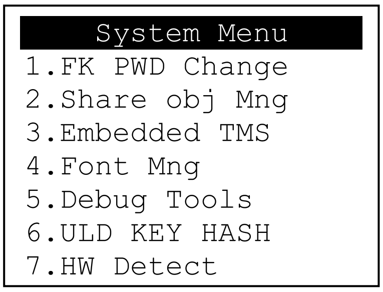
The Default Key Value are shown as below:

Function Key	**0000**
PMEnter Key	**0000**
Factory Reset Key	**8418**

3.10. Share Object Management

View share object in machine.

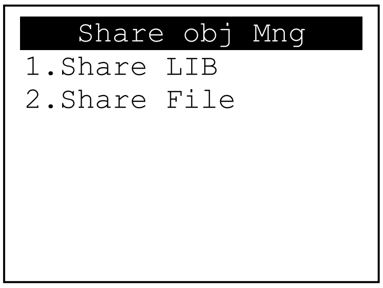
System Menu



```
   System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

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

Share Object Management Menu



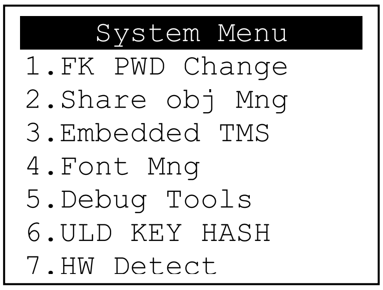
```
  Share obj Mng
1.Share LIB
2.Share File
```

- Press [1] button to view shared libraries.
- Press [2] button to view shared files.

3.11. Embedded TMS

TMS (Terminal Management System) setting menu.

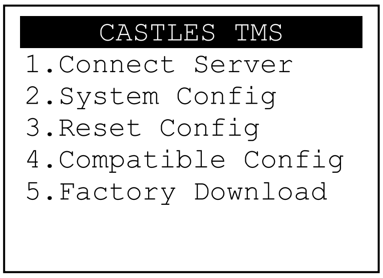
System Menu (Page 2)



```
System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

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

CASTLES TMS



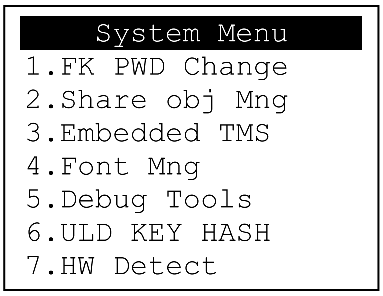
```
CASTLES TMS
1.Connect Server
2.System Config
3.Reset Config
4.Compatible Config
5.Factory Download
```

- Press [1] button to connect server.
- Press [2] button to enter system configuration menu.
- Press [3] button to reset configuration.
- Press [4] button to set compatible configuration.
- Press [5] button to enter factory download mode. (Factory use only)

3.12. Font Mng

View Font Management.

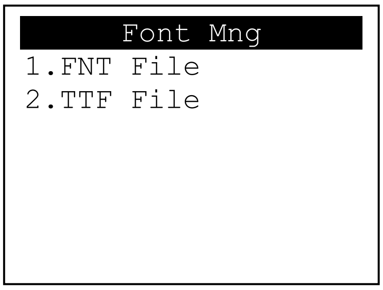
System Menu (Page 2)



```
      System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

- Press [2] button to view Font Management.

Font Management



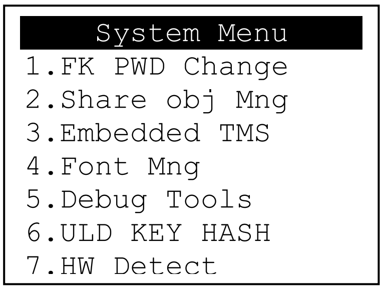
```
       Font Mng
1.FNT File
2.TTF File
```

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

3.13. Debug Tools

Get core dump or debug log.

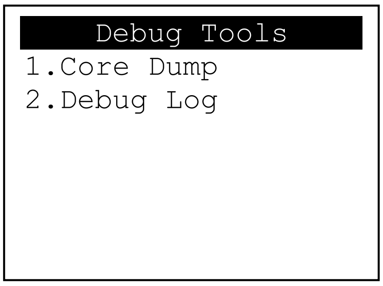
System Menu (Page 2)



```
    System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

- Press [3] button to enter Debug Tools menu.

Debug Tools



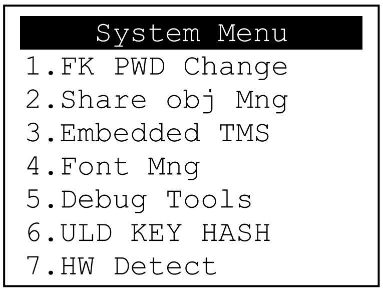
```
    Debug Tools
1.Core Dump
2.Debug Log
```

- Press [1] button to enter core dump menu.
- Press [2] button to enter debug log menu.

3.14. ULD Key Hash

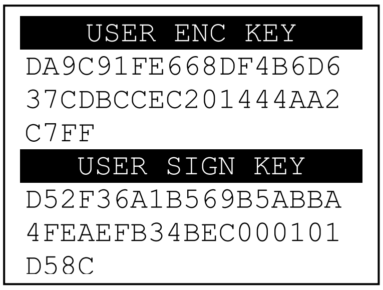
View ULD user key hash value.

System Menu (Page 2)



```
   System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

- Press [4] button to view hash value.

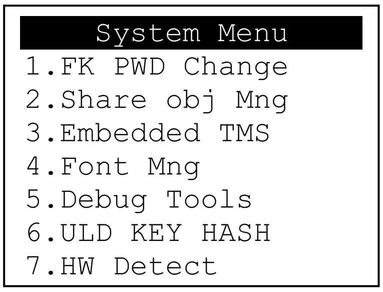


```
  USER ENC KEY
DA9C91FE668DF4B6D6
37CDBCCEC201444AA2
C7FF
  USER SIGN KEY
D52F36A1B569B5ABBA
4FEAEFB34BEC000101
D58C
```

3.15. HW Detect

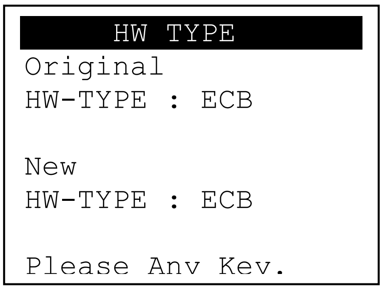
Run hardware detection.

System Menu (Page 2)



```
System Menu
1.FK PWD Change
2.Share obj Mng
3.Embedded TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.HW Detect
```

- Press [5] button to run HW detection.



```
HW TYPE
Original
HW-TYPE : ECB

New
HW-TYPE : ECB

Please Any Key.
```

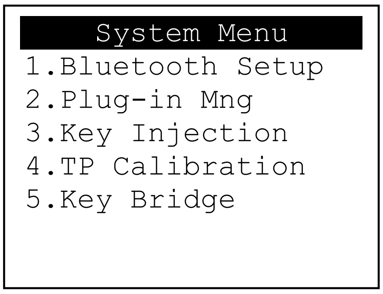
- Press any key to reboot system.

Type	Functions
E	Ethernet
G	GSM/GPRS
C	Contectless
B	Bluetooth
W	WiFi

3.16. Bluetooth Setup

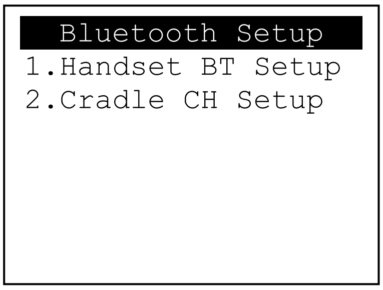
Setup Bluetooth configuration.

System Menu (Page 2)



- Press [6] button to enter Bluetooth setting menu.

Bluetooth Setup

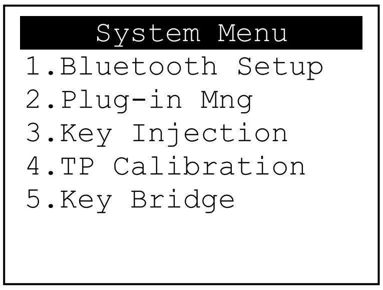


- Press [1] button to enter Handset BT Setup menu.
- Press [2] button to enter Cradle CH Setup menu.

3.17. Plug-in Mng

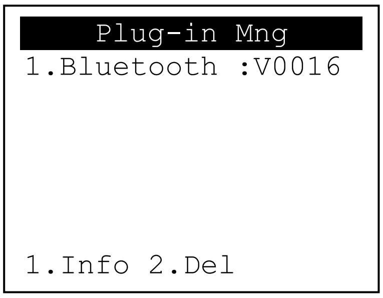
View Plug-in Management.

System Menu (Page 2)



```
     System Menu
1.Bluetooth Setup
2.Plug-in Mng
3.Key Injection
4.TP Calibration
5.Key Bridge
```

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



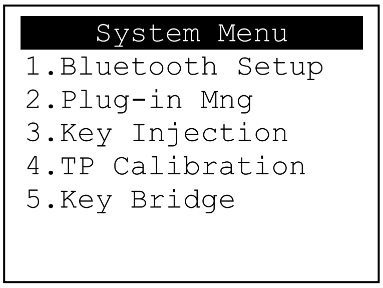
```
     Plug-in Mng
1.Bluetooth :V0016





1.Info 2.Del
```

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

3.18. Key Injection

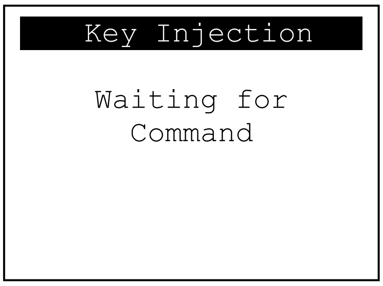
Key Injection function. (Factory use only.)

System Menu (Page 2)



```
   System Menu
1.Bluetooth Setup
2.Plug-in Mng
3.Key Injection
4.TP Calibration
5.Key Bridge
```

- Press [8] button to run Key Injection.

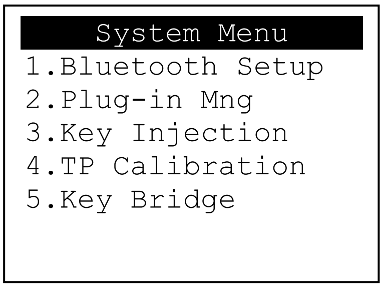


```
  Key Injection

   Waiting for
     Command
```

3.19. Key Bridge

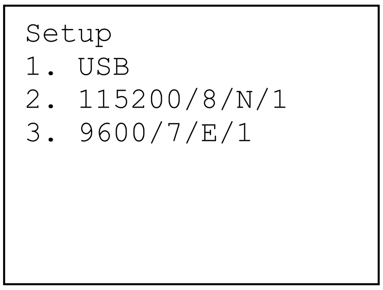
Support key injection for specific software.

System Menu (Page 3)



```
     System Menu
1.Bluetooth Setup
2.Plug-in Mng
3.Key Injection
4.TP Calibration
5.Key Bridge
```

- Press [1] button to enter key bridge menu.



```
Setup
1. USB
2. 115200/8/N/1
3. 9600/7/E/1
```

- Press [1] button to use USB communication for key injection.
- Press [2] button to use RS232 communication with baud rate 115200 for key injection.
- Press [3] button to use RS232 communication with baud rate 9600 for key injection.

4. Secure File Loading

Castles implemented an interface 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 UPT1000M, the RSA key length is 2048bits.

4.1.1. ULD Manufacturer Key

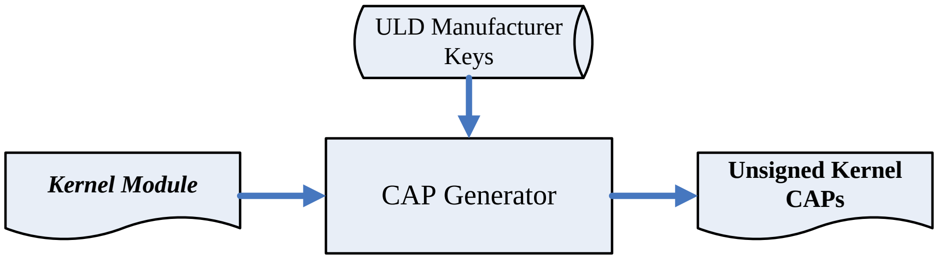
The system consists of several kernel modules. These kernel modules are provided by the Manufacturer, and released in CAP format file with encryption and signing via ULD Manufacturer Keys.

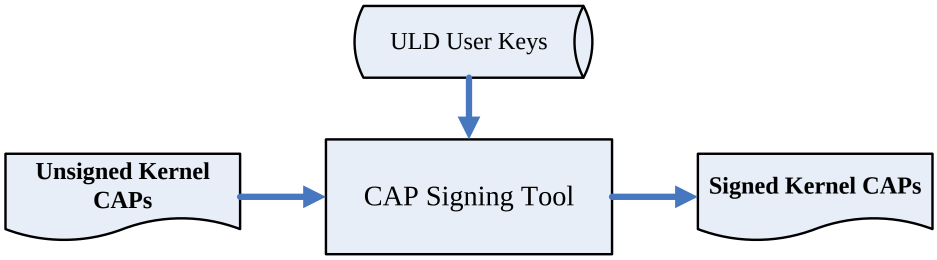
The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only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

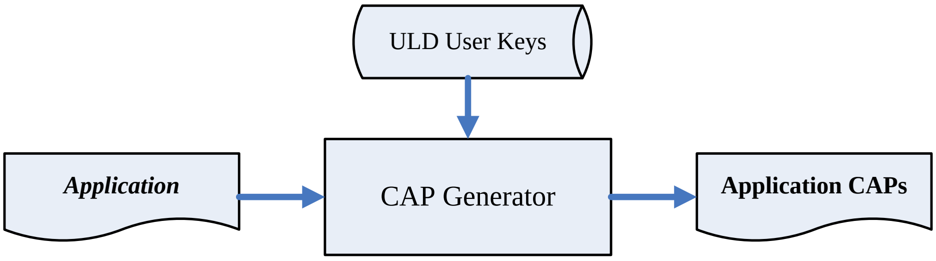




4.1.2. ULD User Key

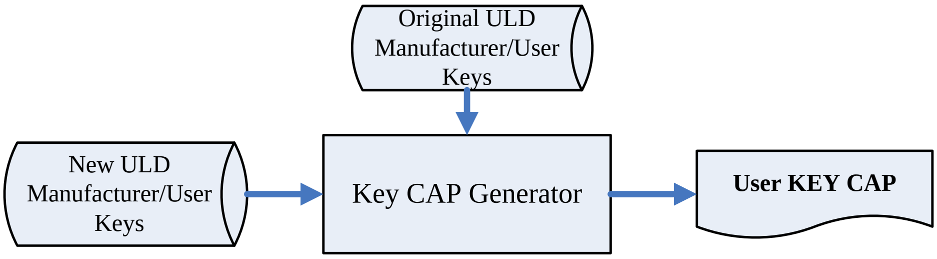
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the “signed’ action via ULD User Keys.

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

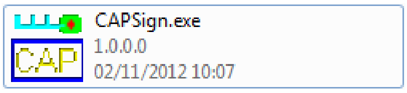
4.2.1. Signing Kernel Module

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 UPT1000M.

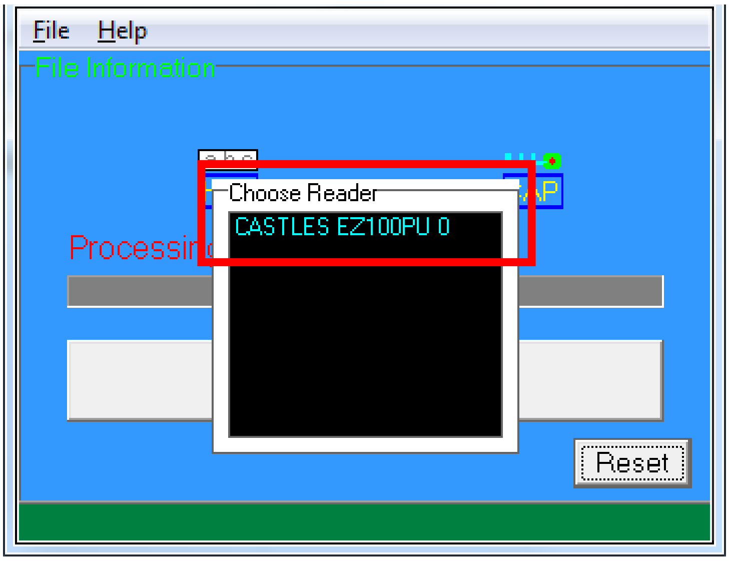
Castles Technology provides a tool named “CAP Signing Tool” to perform this task.

The CAP Signing Tool is located at:
C:\Program Files\Castles\UPT1000\tools\Signing Tool

- Run CAP Signing Tool

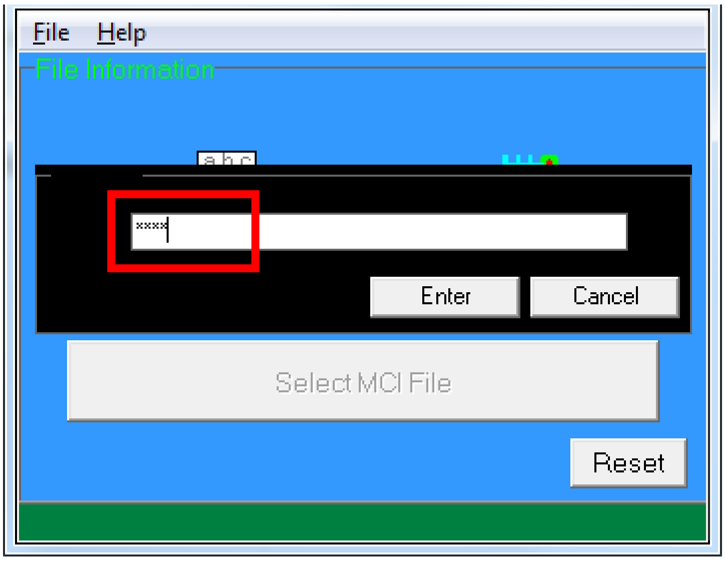

CAPSign.exe
1.0.0.0
02/11/2012 10:07

- Insert Key Card and select smart card reader

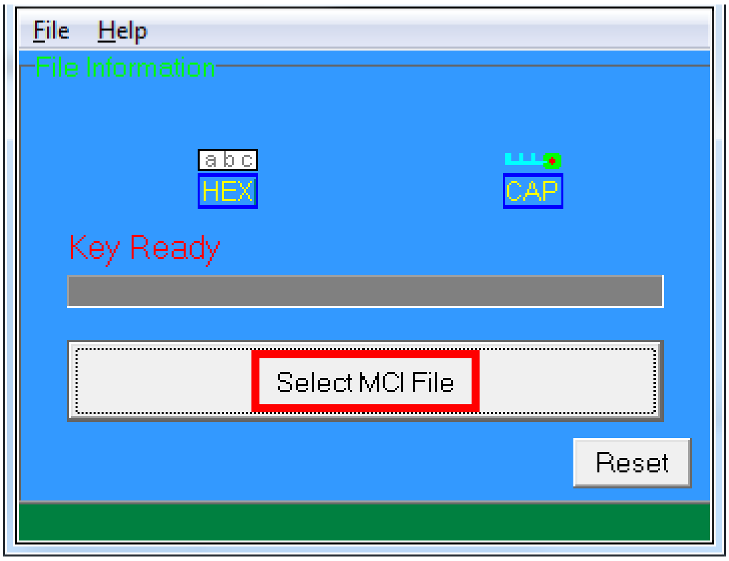


Choose Reader
CASTLES EZ100PU 0

- Enter Key Card PIN



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



Key Ready

- Output file will be located in “signed” folder.

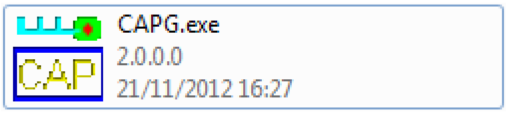
4.2.2. Signing User Files

Following files are required to sign before load to UPT1000M. 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.

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

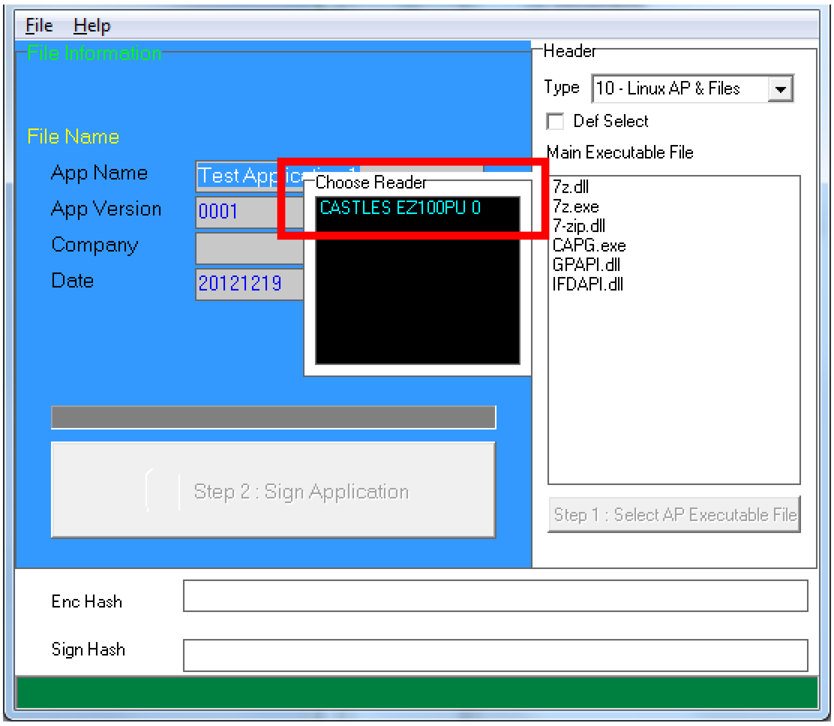
The CAP Generator is located at:
C:\Program Files\Castles\UPT1000\tools\CAPG (KeyCard)

- Run CAP Generator



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

- Insert Key Card and select smart card reader



File Help

File Information

File Name

App Name: Test Applica...

App Version: 0001

Company:

Date: 20121219

Choose Reader: CASTLES EZ100PU 0

Header

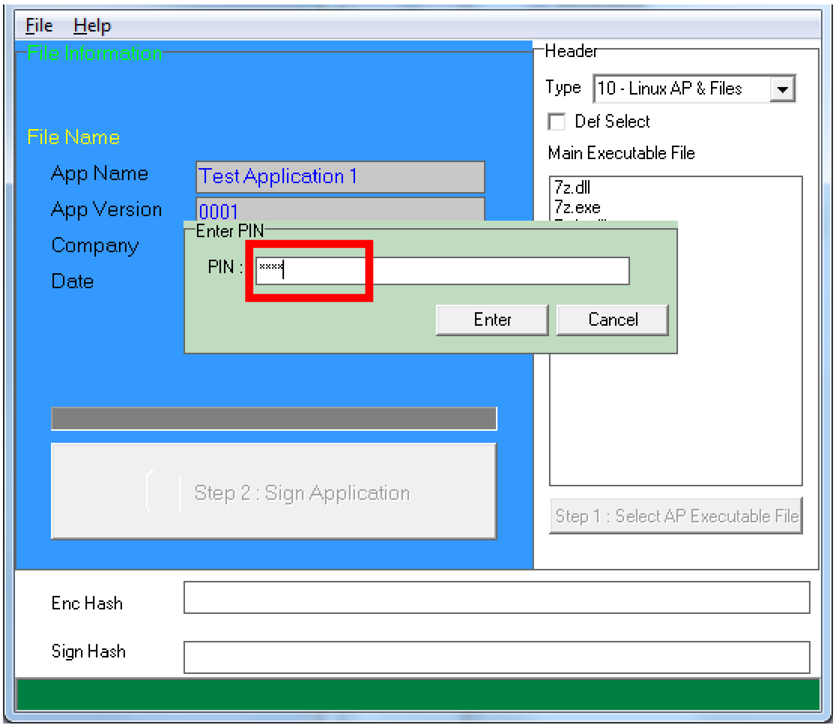
Type: 10 - Linux AP & Files

□ Def Select

Main Executable File

7z.dll
7z.exe
7-zip.dll
CAPG.exe
GPAPI.dll
IFDAPI.dll

- Enter Key Card PIN



File Help

File Information

File Name

App Name: Test Application 1

App Version: 0001

Company:

Date:

Enter PIN

PIN : ****

Header

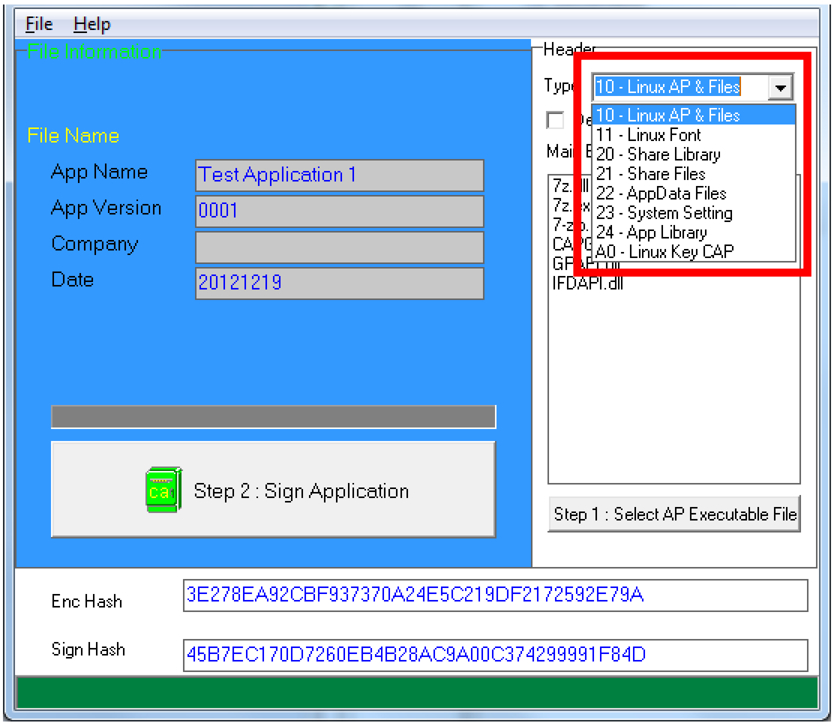
Type: 10 - Linux AP & Files

□ Def Select

Main Executable File

7z.dll
7z.exe

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



File Name

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

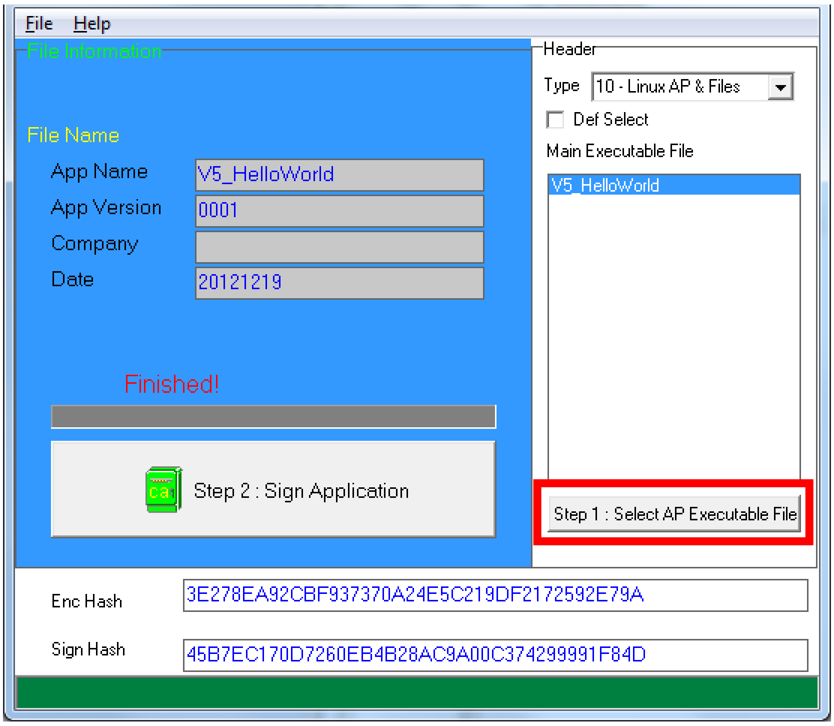
IFDAPI.dll

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A

Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

- 10- Linux AP & Files (User application, data files, or library)
- 11- Linux Font (TFT and FNT font)
- 20- Share library (Shared library for all application)
- 21- Share files (Shared file for all application)
- 22- AppData Files (Dedicated application's data file)
- 23- System setting (Configuration file)
- 24- AppData Library (Dedicated application's library)
- A0- Linux Key CAP (Manufacturer ULD Key Set)

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

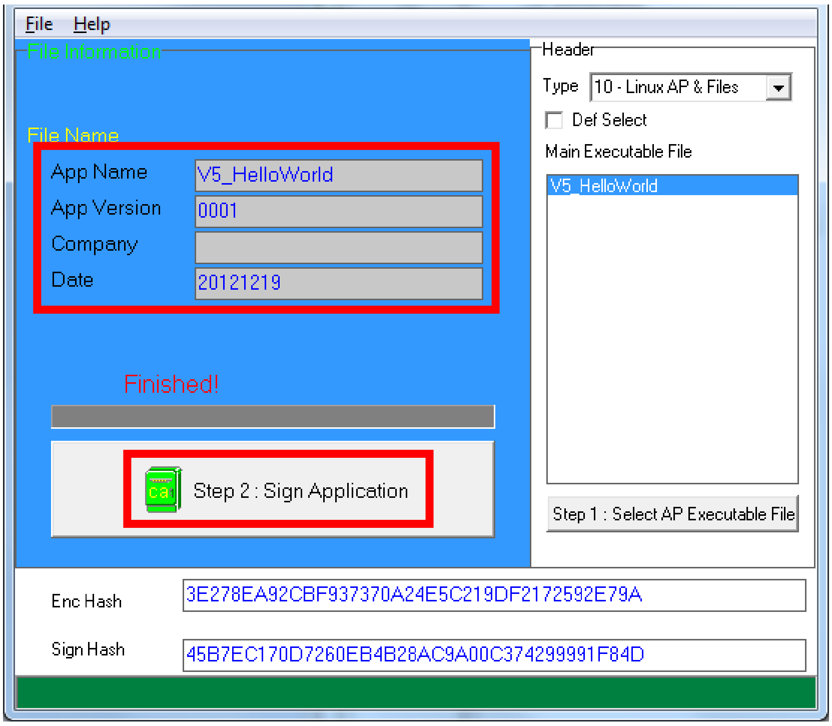


App Name: V5_HelloWorld
App Version: 0001
Company:
Date: 20121219

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 UPT1000M.

- 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 UPT1000M.

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

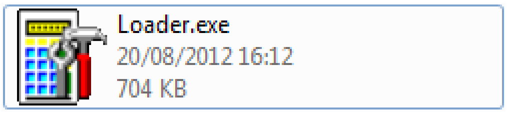
Castles TMS (CTMS or CASTLES Terminal Management System) is provided by Castles Technology. It uses to perform remote download via Ethernet, GPRS/UMTS or modem.

4.3.1. Download by User Loader

The User Loader works for UPT1000M.

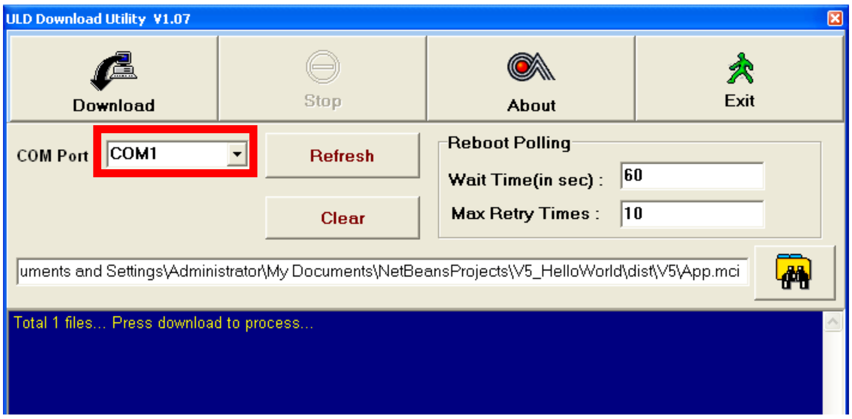
The Loader is located at:
C:\Program Files\Castles\UPT1000\tools\Loader

- Run User Loader



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

- Select COM port



ULD Download Utility V1.07

COM Port COM1

Reboot Polling

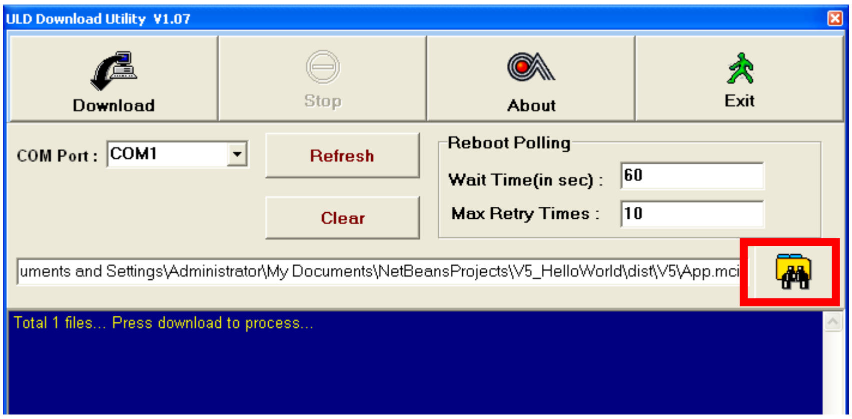
Wait Time(in sec) : 60

Max Retry Times : 10

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

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

- Browse and select mci file or mmci file



ULD Download Utility V1.07

COM Port : COM1

Reboot Polling

Wait Time(in sec) : 60

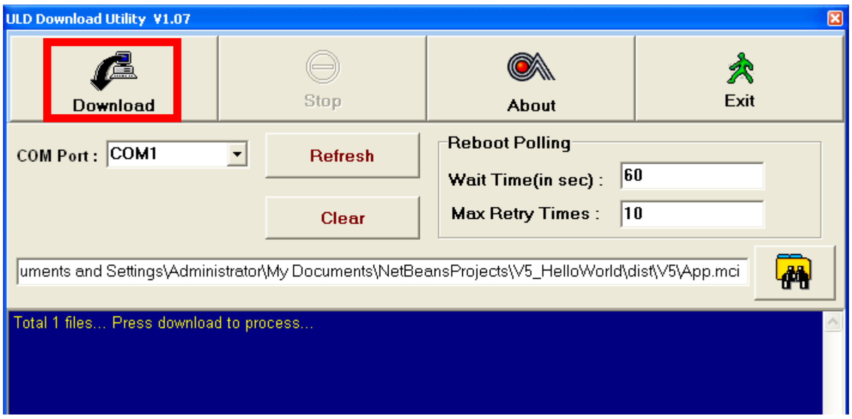
Max Retry Times : 10

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

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

- Setup UPT1000M 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.



COM Port : COM1

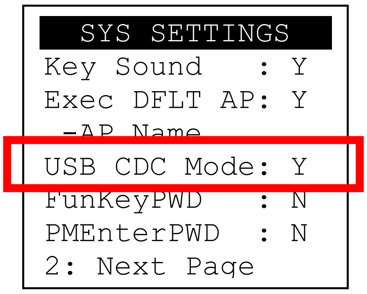
Wait Time(in sec) : 60

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, *UPT1000M* must enable CDC *mode. Set USB CDC Mode to Y.*

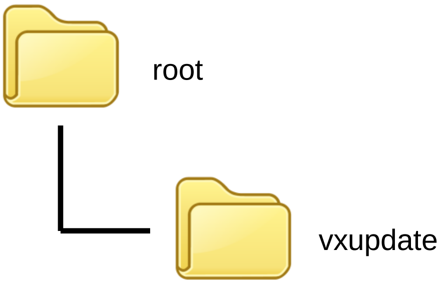


```
SYS SETTINGS
Key Sound    : Y
Exec DFLT AP: Y
  -AP Name
USB CDC Mode: Y
FunKeyPWD    : N
PMEnterPWD   : N
2: Next Page
```

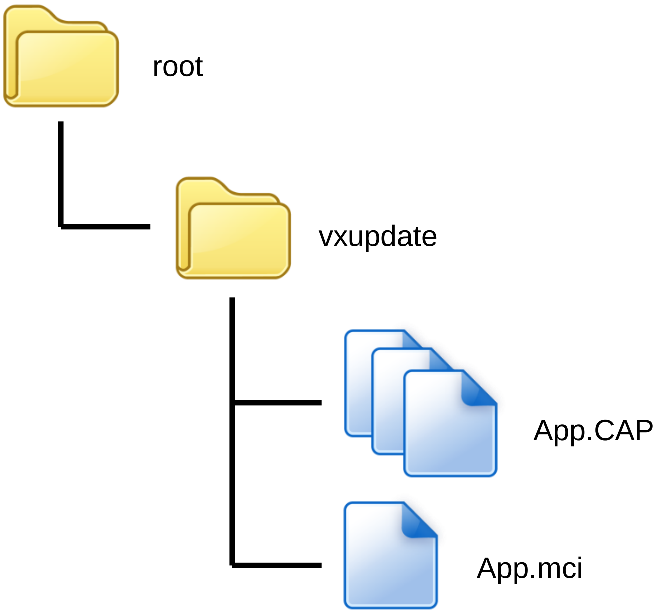
4.3.2. Download by Removable Media

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



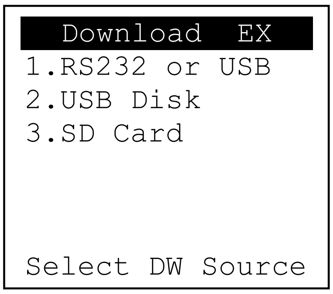
- Place the mci file and cap file to “vxupdate” folder.



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 UPT1000M, 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
  ```

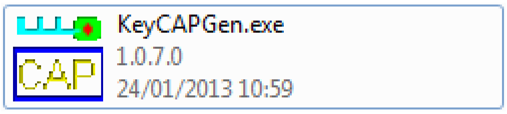
  - Press [2] button to select USB flash drive.
  - Press [3] button to select MicroSD card. (Not support)

- Finally, UPT1000M will process the file in “vxupdate” folder.

4.4. Changing ULD User Key

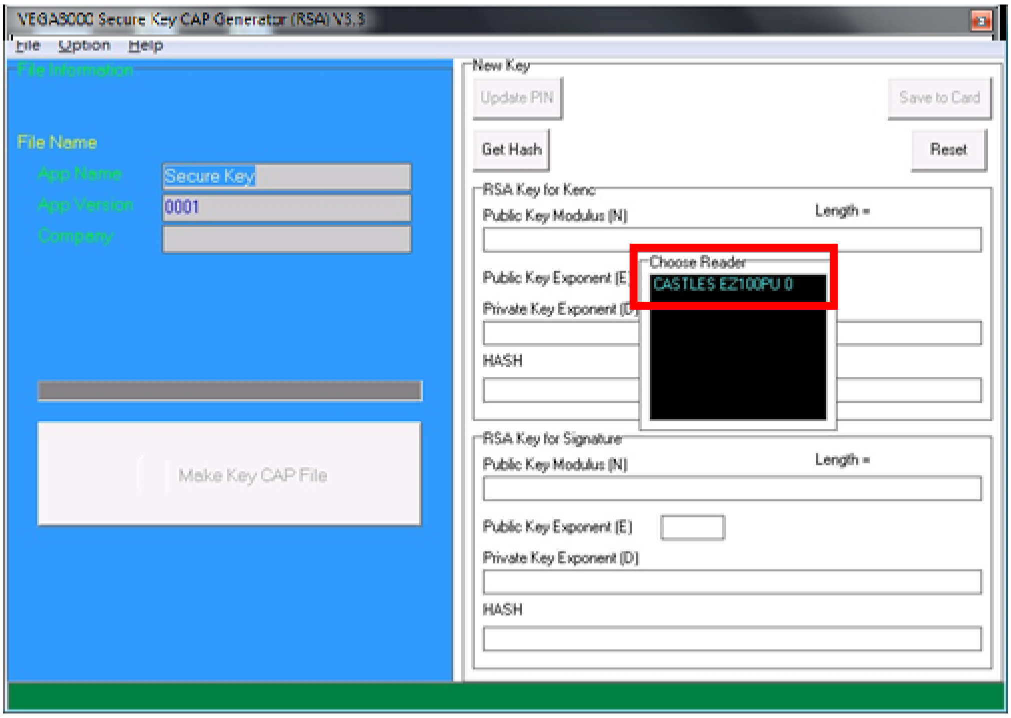
User may change their ULD User Key Set stored in Key Card. Castles Technology provided a tool named “Secure Key Generator” to perform this task.

- Run Secure Key Generator



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

- Insert Key Card and select smart card reader



VEGA3000 Secure Key CAP Generator (RSA) V3.3

File Information

File Name

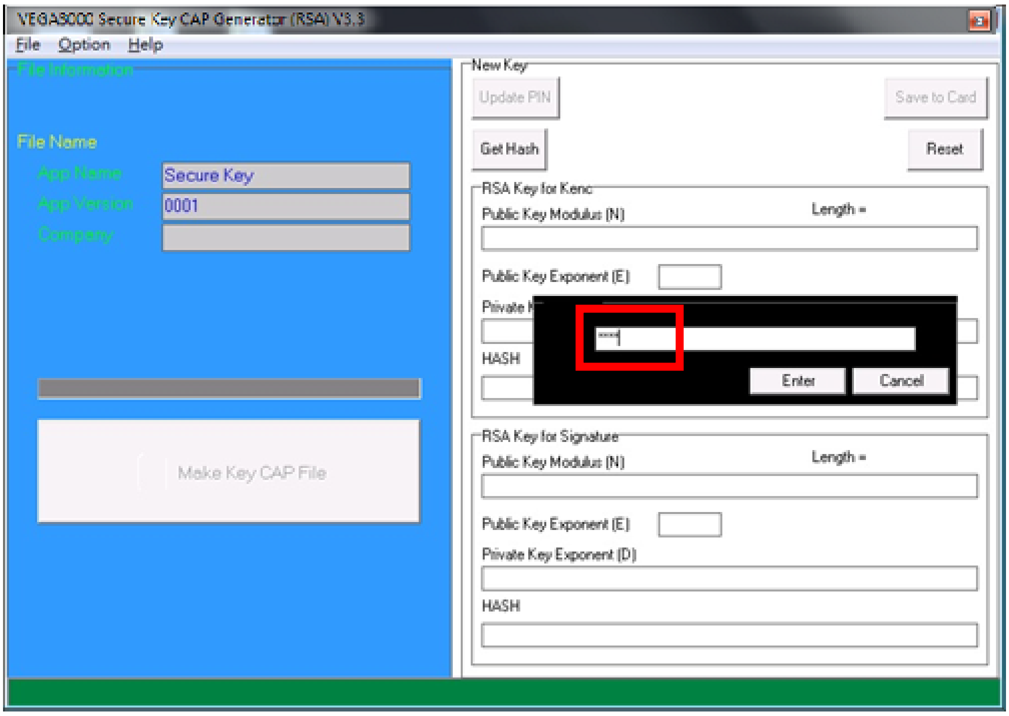
App Name: Secure Key

App Version: 0001

Company:

Choose Reader: CASTLES EZ100PU 0

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

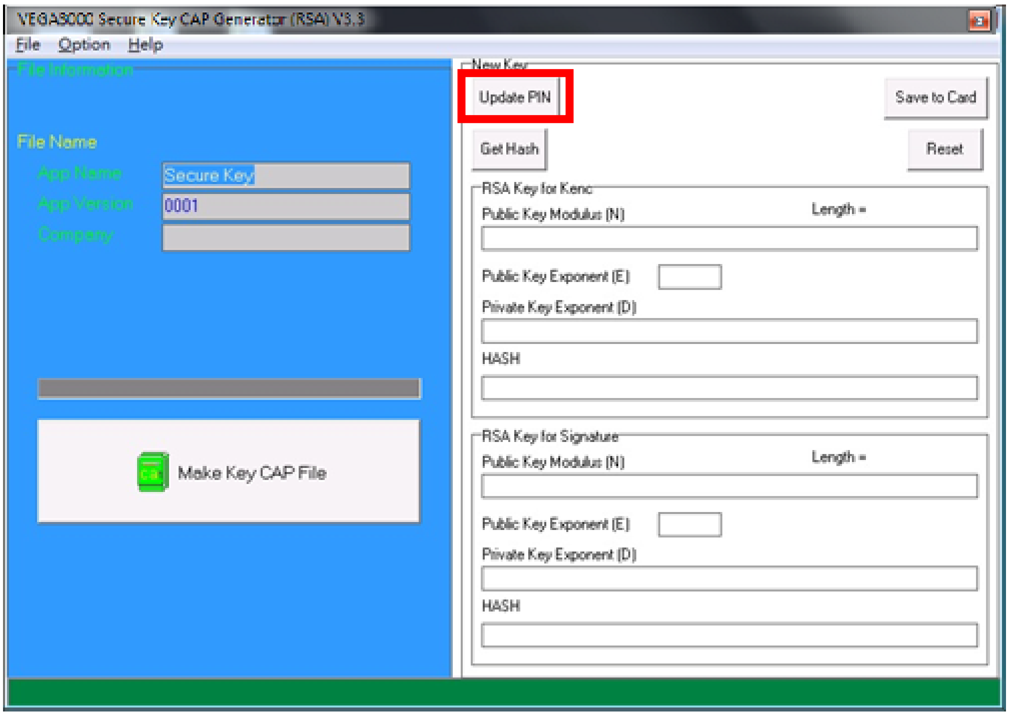


App Name: Secure Key

App Version: 0001

Company:

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

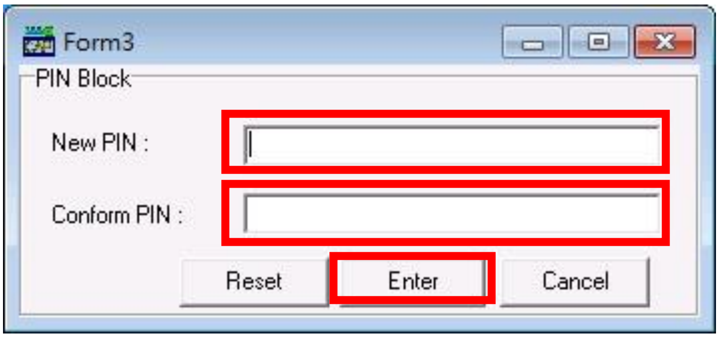


App Name: Secure Key

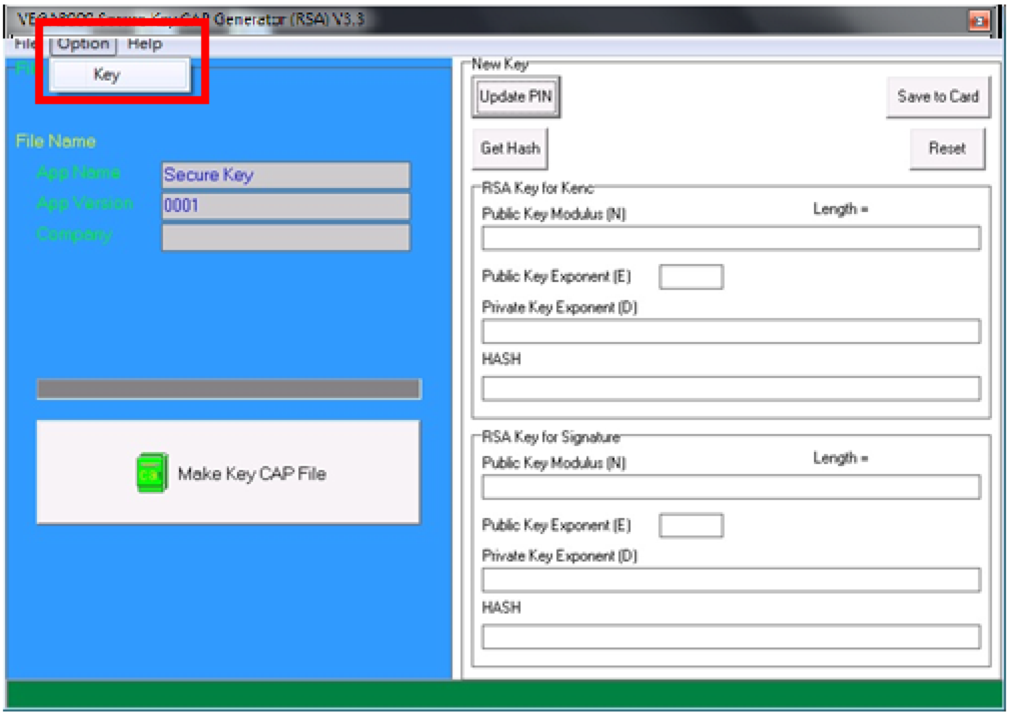
App Version: 0001

Company:

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



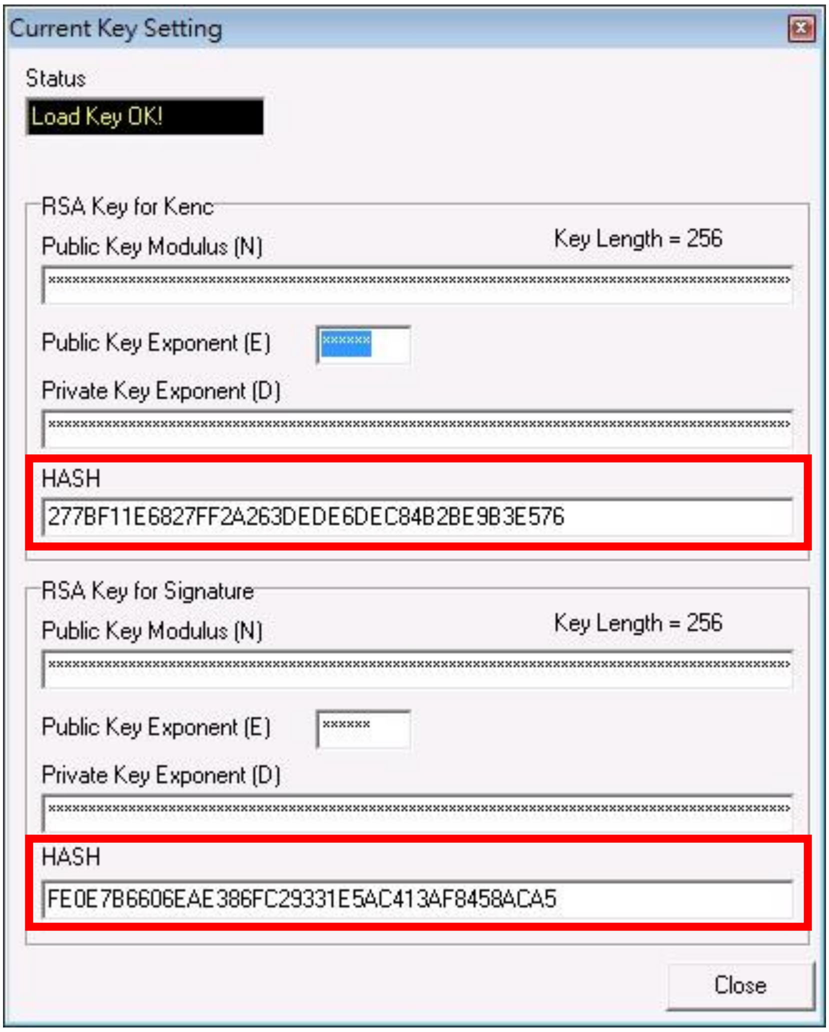
- To view current key set hash value, goto “Option” and select key.



App Name Secure Key

App Version 0001

Company



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) ******

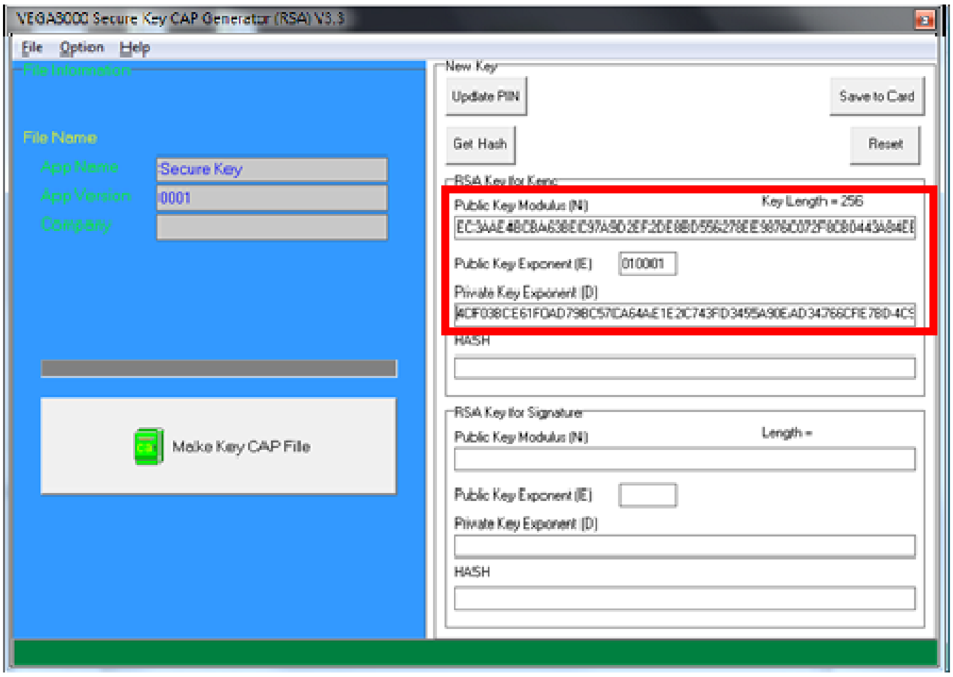
Private Key Exponent (D)

****

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) Key Length = 256

EC3AAE4BCBA63BEC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9

HASH

RSA Key for Signature

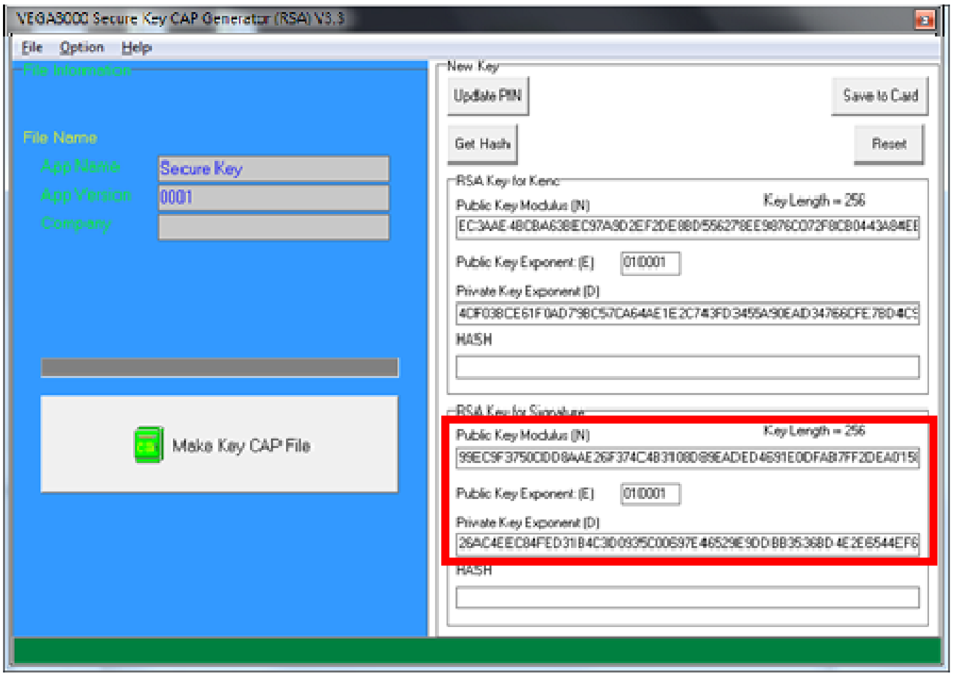
Public Key Modulus (N) Length =

Public Key Exponent (E)

Private Key Exponent (D)

HASH

- Generate second RSA key set for Signature.



App Name: Secure Key

App Version: 0001

Company:

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA63BEC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE

Public Key Exponent (E) 010001

Private Key Exponent (D)

4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9

HASH

RSA Key for Signature

Public Key Modulus (N) Key Length = 256

99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFAB7FF2DEA015

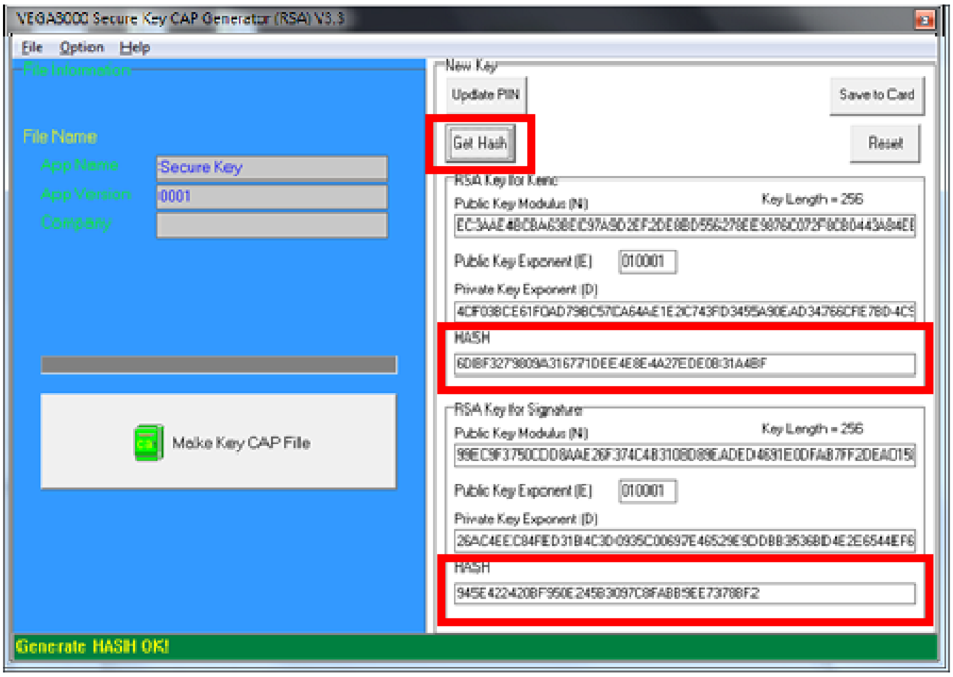
Public Key Exponent (E) 010001

Private Key Exponent (D)

26AC4EEC84FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6

HASH

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



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

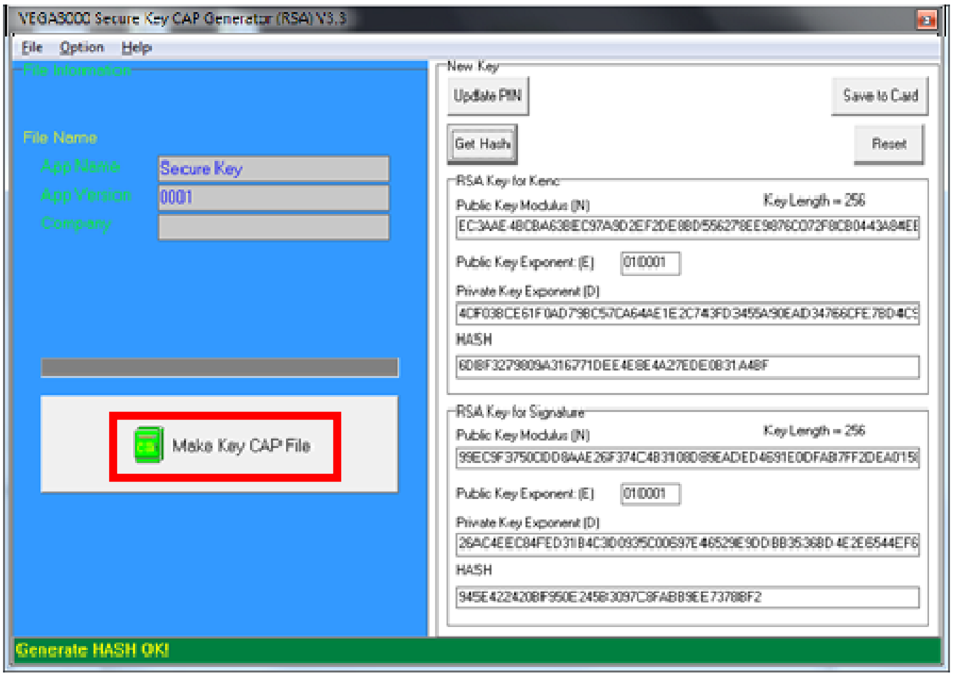
RSA Key for Kenc
Public Key Modulus (N) Key Length = 256
EC3AAE4BCBA638EC97A9D2EF2DE0BD556278EE9876C072F8C80443A84EE
Public Key Exponent (E) 010001
Private Key Exponent (D)
4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9
HASH
6D8F3279809A316771DEE4E8E4A27EDE0831A48F

RSA Key for Signature
Public Key Modulus (N) Key Length = 256
99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFAB7FF2DEA015
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.



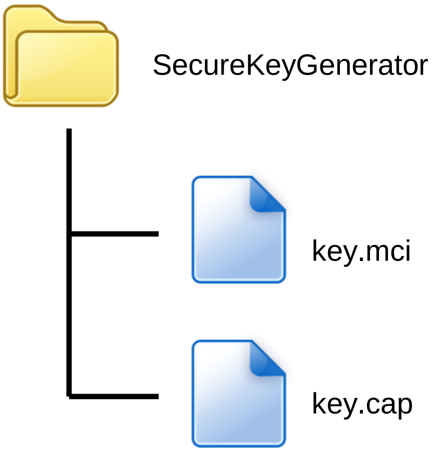
File Name
App Name: Secure Key
App Version: 0001
Company:

RSA Key for Kenc
Public Key Modulus (N) Key Length = 256
EC3AAE4BCBA638EC97A9D2EF2DE0BD556278EE9876C072F8C80443A84EE
Public Key Exponent (E) 010001
Private Key Exponent (D)
4CF038CE61F0AD798C57CA64AE1E2C743FD3455A90EAD34766CFE78D4C9
HASH
6D8F3279809A316771DEE4E8E4A27EDE0831A48F

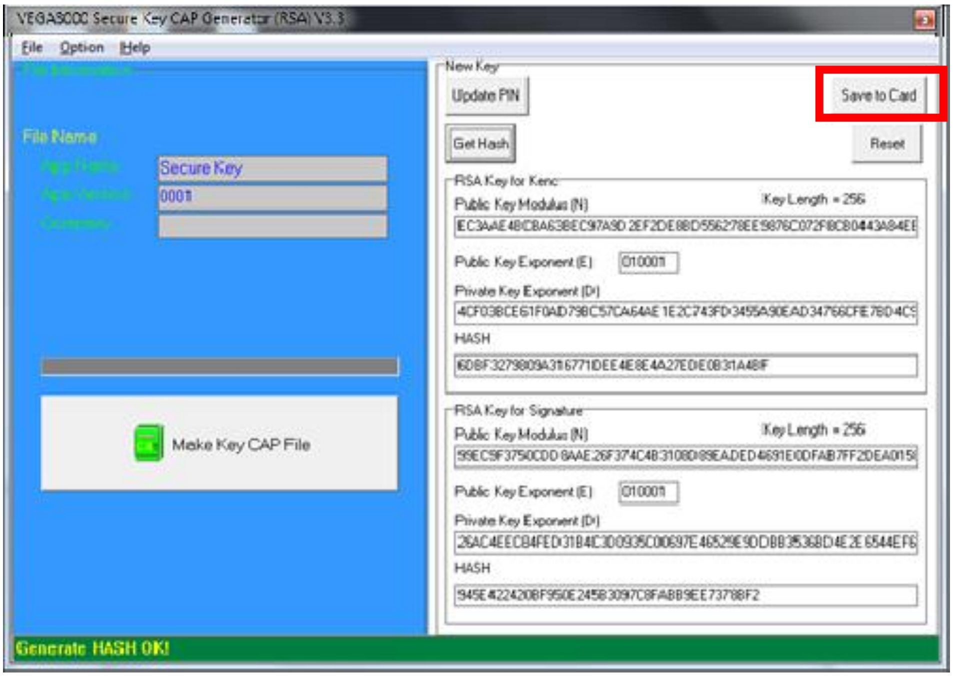
RSA Key for Signature
Public Key Modulus (N) Key Length = 256
99EC9F3750CDD8AAE26F374C4B3108D89EADED4691E0DFAB7FF2DEA015
Public Key Exponent (E) 010001
Private Key Exponent (D)
26AC4EEC84FED31B4C3D0935C00697E46529E9DDBB35368D4E2E6544EF6
HASH
945E422420BF950E245B3097C8FABB9EE73788F2

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.



Secure Key

00011

RSA Key for Kenc

Public Key Modulus (N) Key Length = 256

EC3AAE4BCBA63BEC97A9D2EF2DE8BD556278EE9876C072F8CB0443A84EE

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

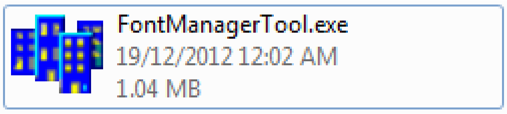
945E4224208F950E24583097C8FABB9EE73788F2

Generate HASH OK!

5. Font Management

5.1. Loading New Font

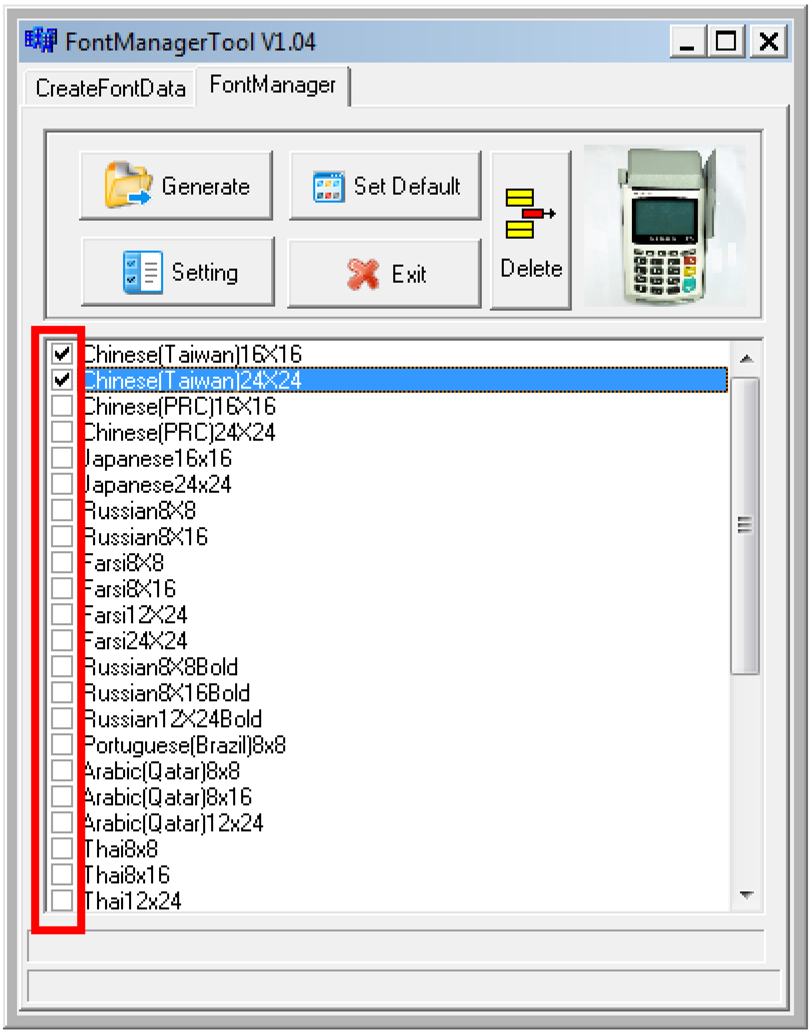
- Run FontManager.exe



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

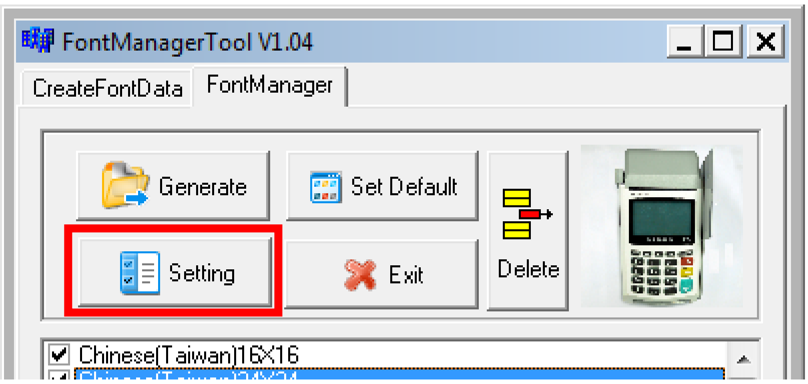
Located at C:\Program Files\Castles\Font Manager

- Select font to download

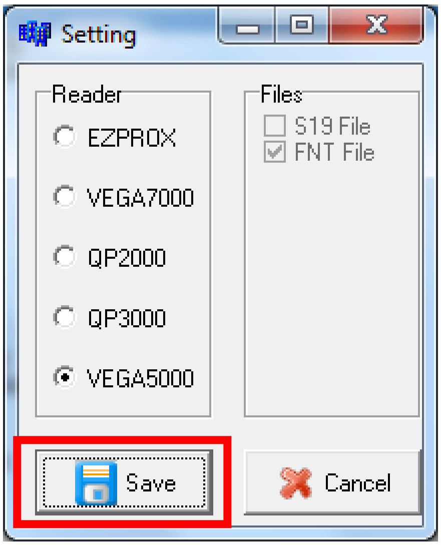


☑ Chinese(Taiwan)16X16
☑ Chinese(Taiwan)24X24
□ Chinese(PRC)16X16
□ Chinese(PRC)24X24
□ Japanese16x16
□ Japanese24x24
□ Russian8X8
□ Russian8X16
□ Farsi8X8
□ Farsi8X16
□ Farsi12X24
□ Farsi24X24
□ Russian8X8Bold
□ Russian8X16Bold
□ Russian12X24Bold
□ Portuguese(Brazil)8x8
□ Arabic(Qatar)8x8
□ Arabic(Qatar)8x16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

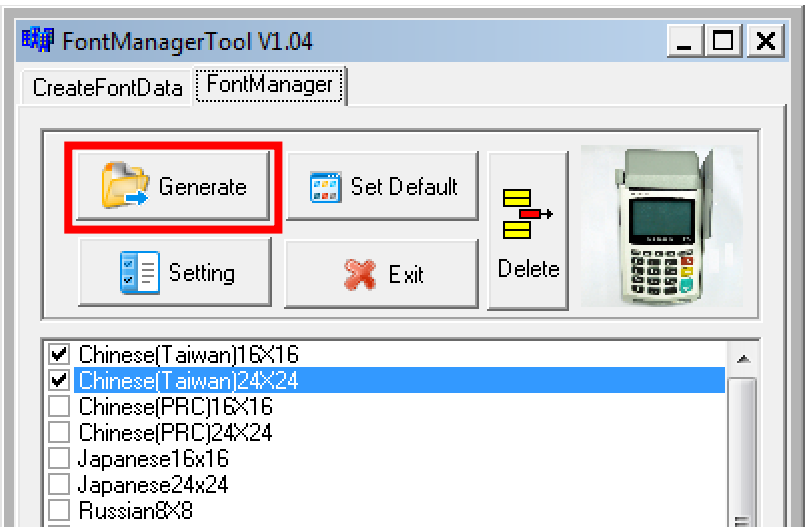
- Press [Setting] button to configure the type.



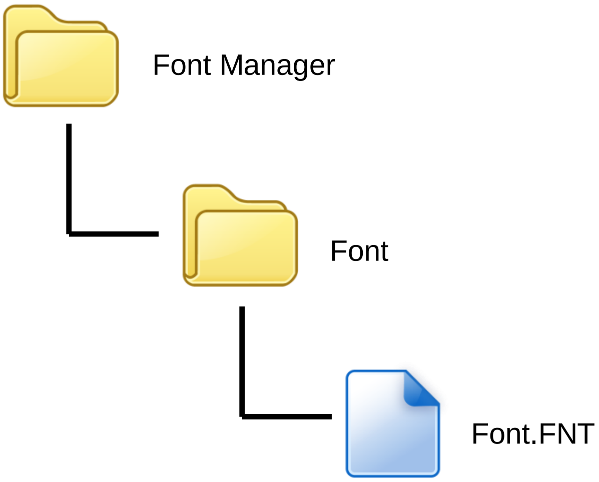
- Select **VEGA5000**, press [Save] button to save and return font manager.



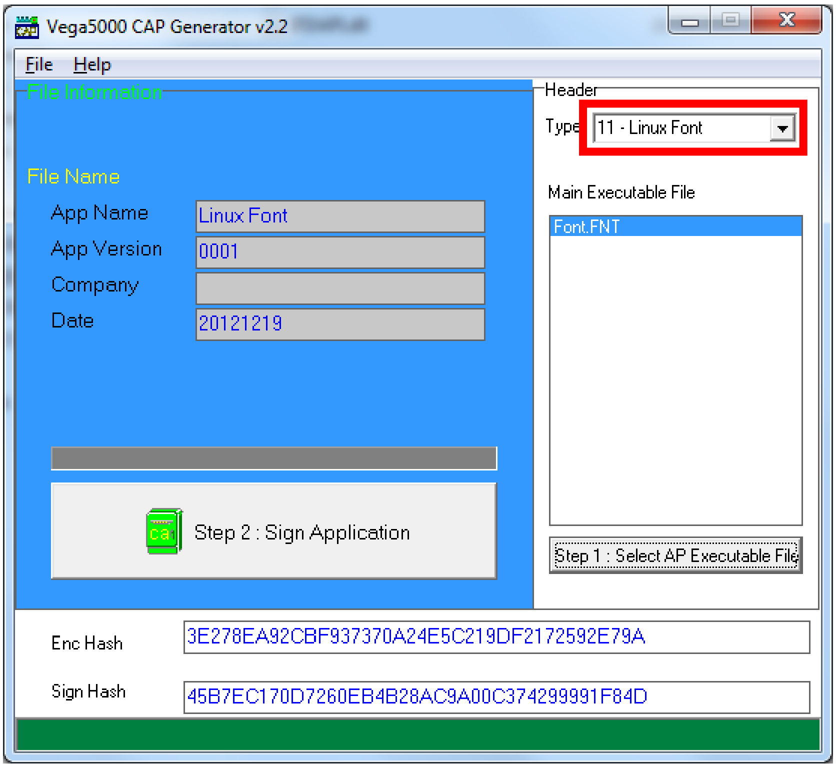
- Press [Generate] to create the font file.



- 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”.


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

Type: 11 - Linux Font

Main Executable File: Font.FNT

File Name

App Name: Linux Font

App Version: 0001

Company:

Date: 20121219

Enc Hash: 3E278EA92CBF937370A24E5C219DF2172592E79A

Sign Hash: 45B7EC170D7260EB4B28AC9A00C374299991F84D

- Lastly, download the signed file (CAP file) to UPT1000M using Loader.

5.2. Custom Font

User may create font they preferred for displaying or printing on UPT1000M.

There are two zone defined:

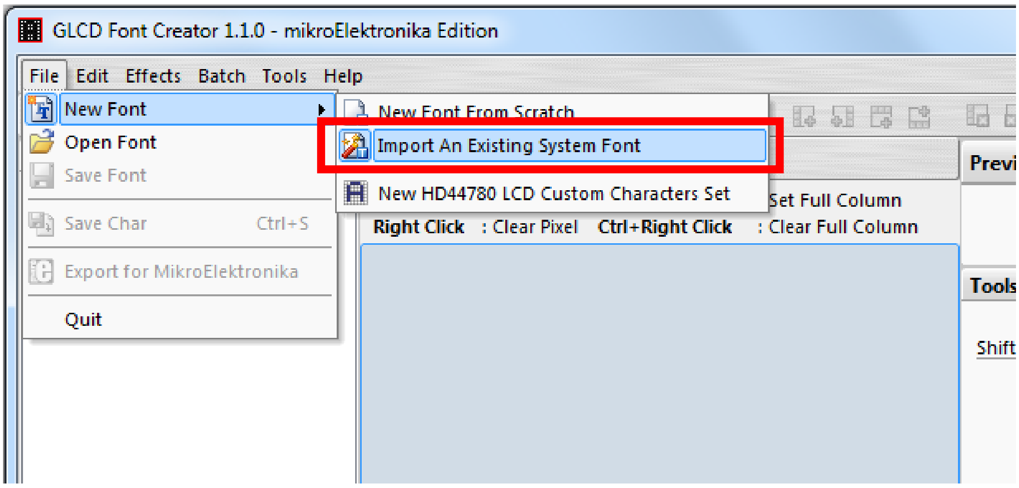
Zone 0x00 ~ 0x7F – ASCII characters, you may replace with the font type preferred or your own language character set.

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

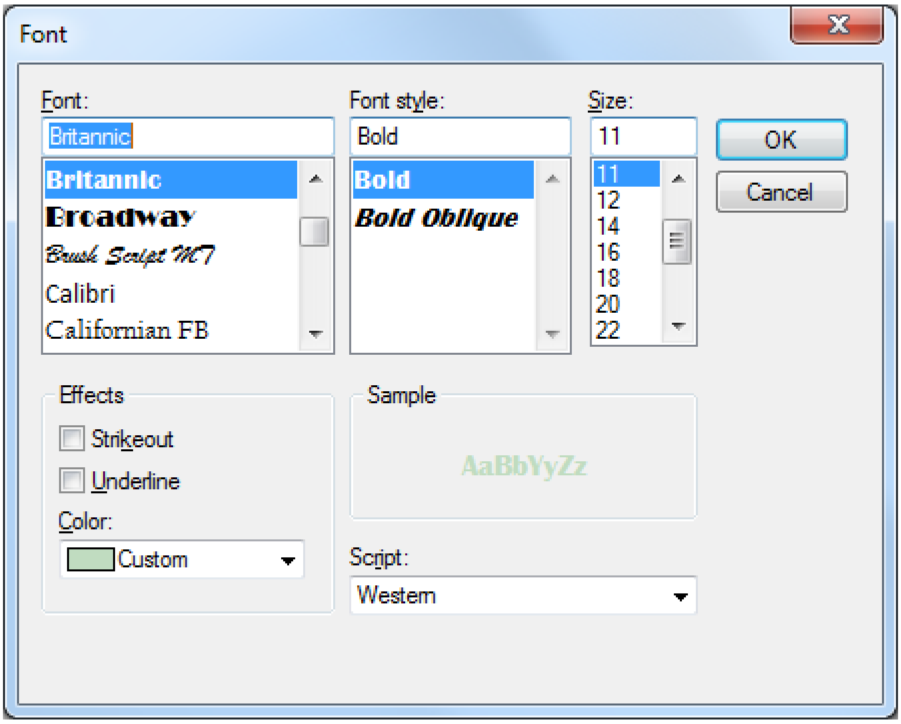
Following steps demonstrate how to create a 12x24 font.

- Run GLCD Font Creator

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


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

Font style: Bold

Size: 11

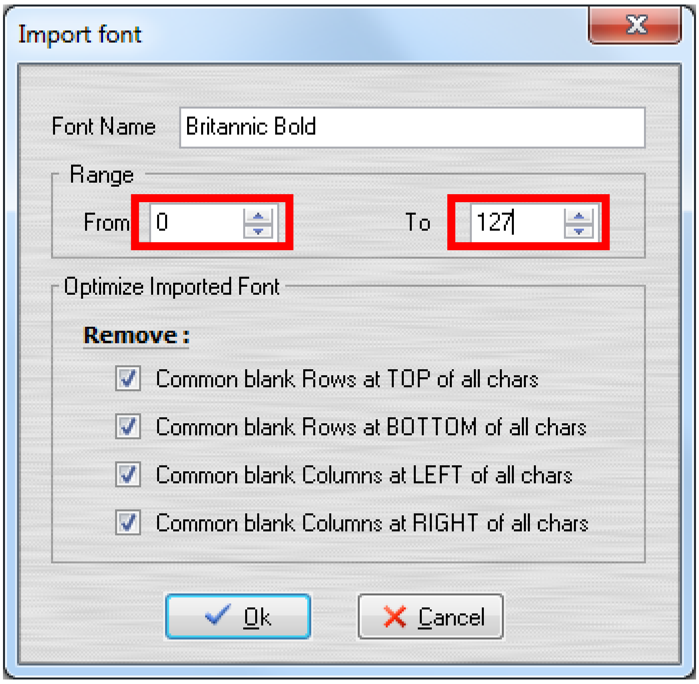
□ Strikeout

□ Underline

Color: Custom

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 :

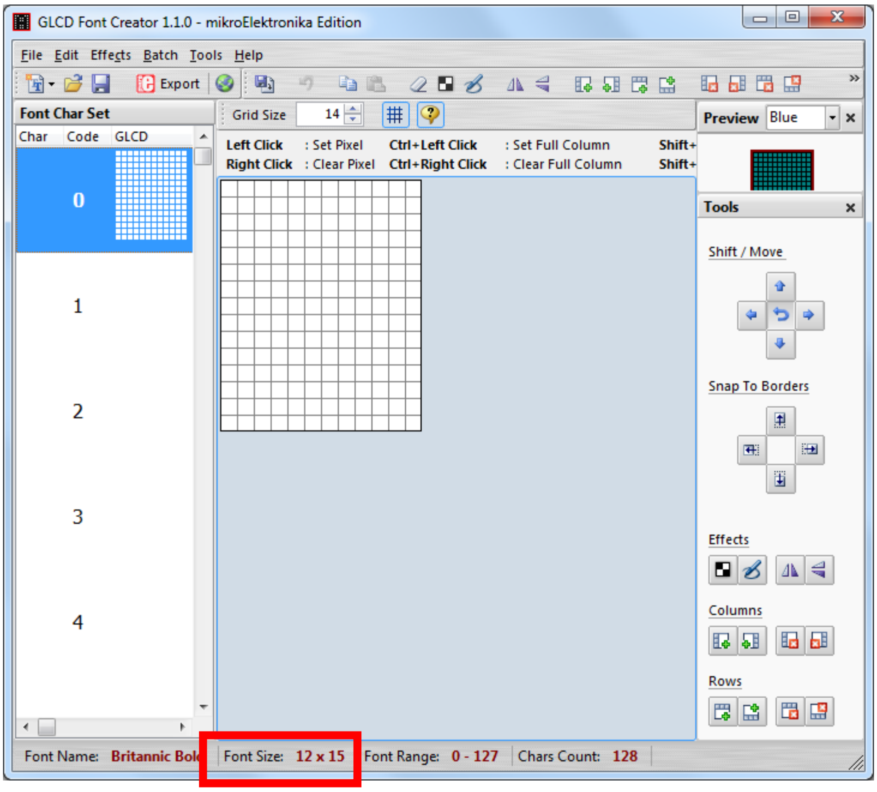
☑ Common blank Rows at TOP of all chars

☑ Common blank Rows at BOTTOM of all chars

☑ Common blank Columns at LEFT of all chars

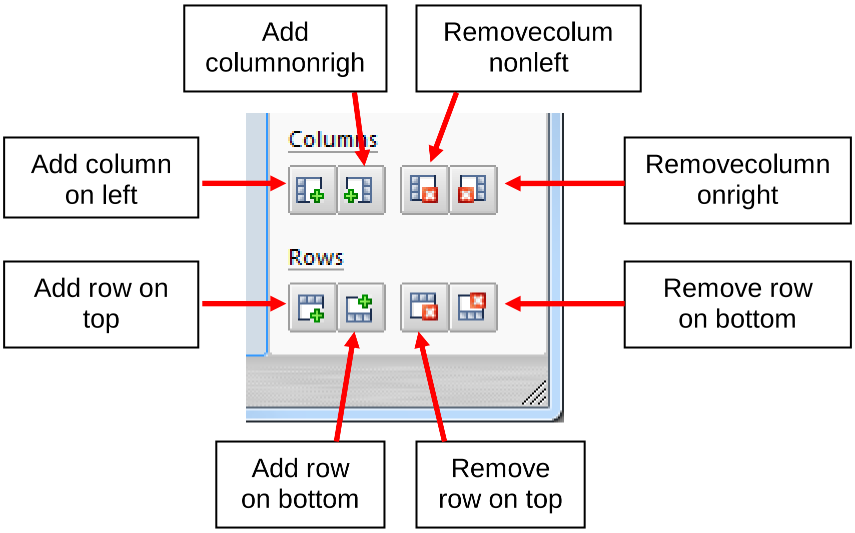
☑ Common blank Columns at RIGHT of all chars

- Check the minimum pixel width and height.

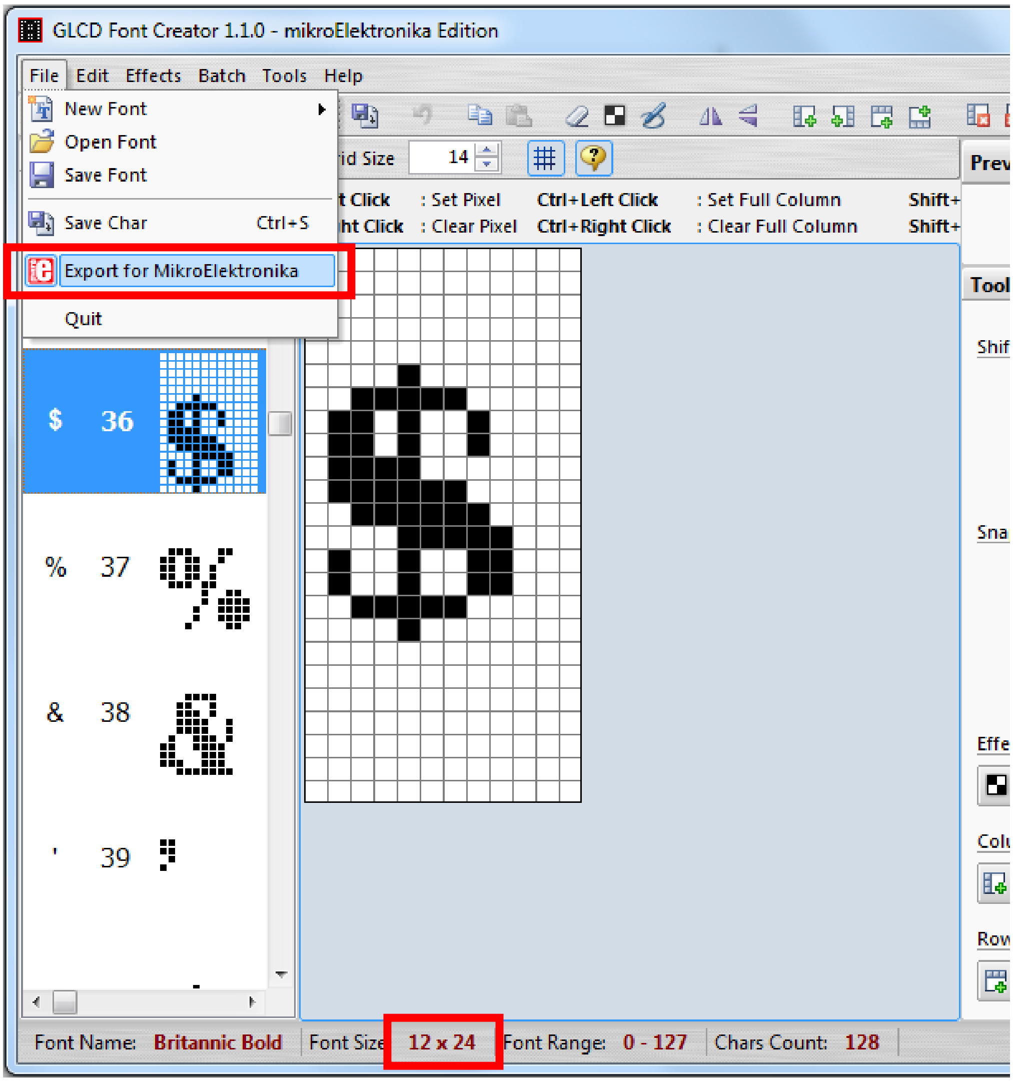


- If the pixel width of the font size is larger than expected, then you have to repeat the previous steps to import font with smaller size.

- Use the following buttons to adjust the font size to match with expected font size.

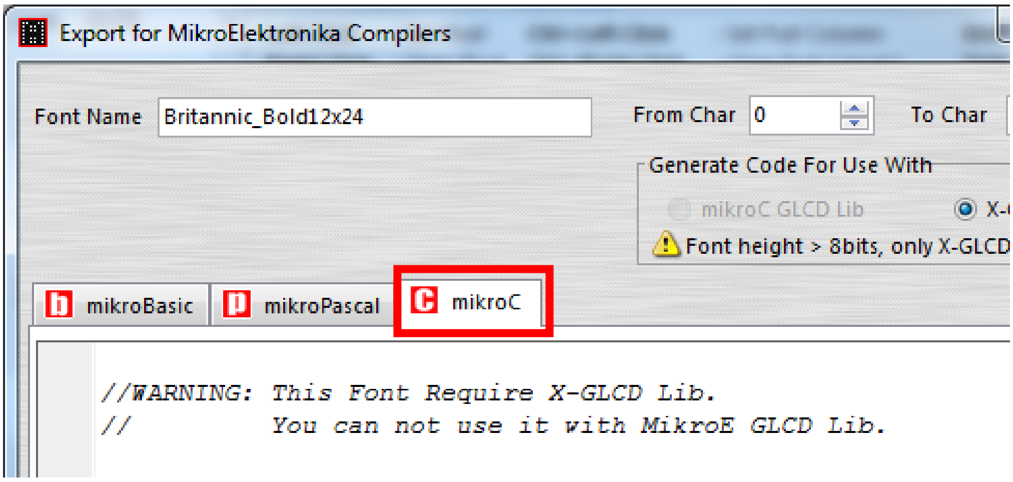


- After adjust font size, select [File] ⇨ [Export for MicroElektronika].



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

- Select output format as [mikroC].



Font Name Britannic_Bold12x24

From Char 0

To Char

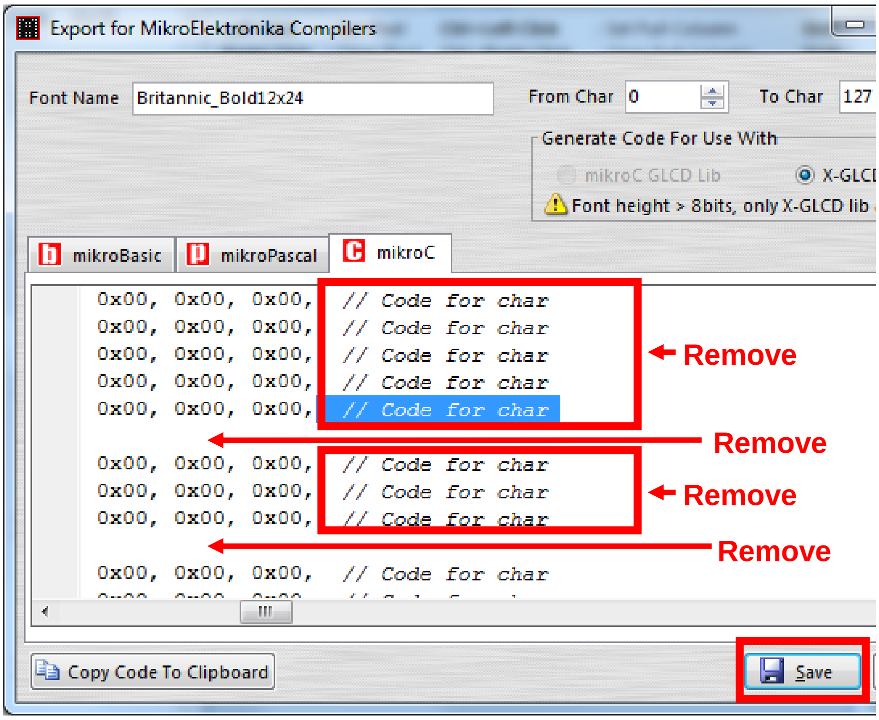
Generate Code For Use With

○ mikroC GLCD Lib   ● X-

⚠ 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

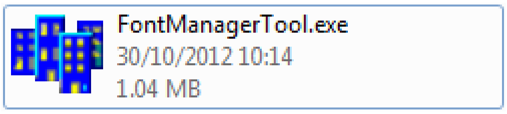
Generate Code For Use With

○ mikroC GLCD Lib ● X-GLCI

⚠ Font height > 8bits, only X-GLCD lib

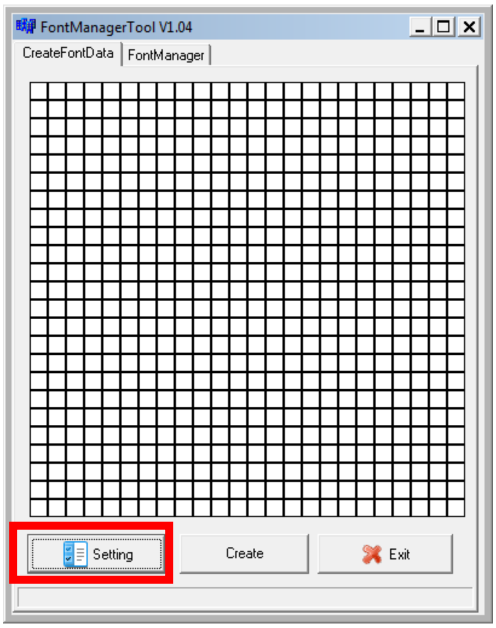
```
0x00, 0x00, 0x00,   // Code for char
0x00, 0x00, 0x00,   // Code for char
0x00, 0x00, 0x00,   // Code for char
0x00, 0x00, 0x00,   // Code for char
0x00, 0x00, 0x00,   // Code for char

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.

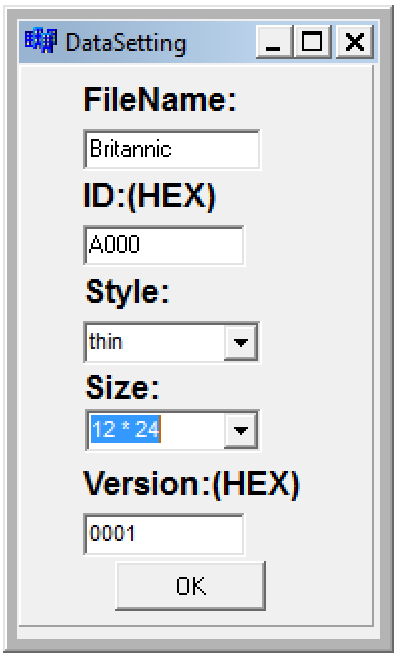


FontManagerTool.exe
30/10/2012 10:14
1.04 MB

- Click [Setting] button



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



FileName:
Britannic

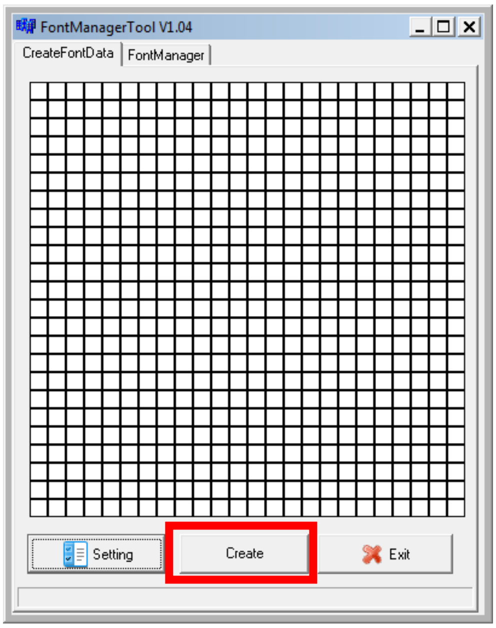
ID:(HEX)
A000

Style:
thin

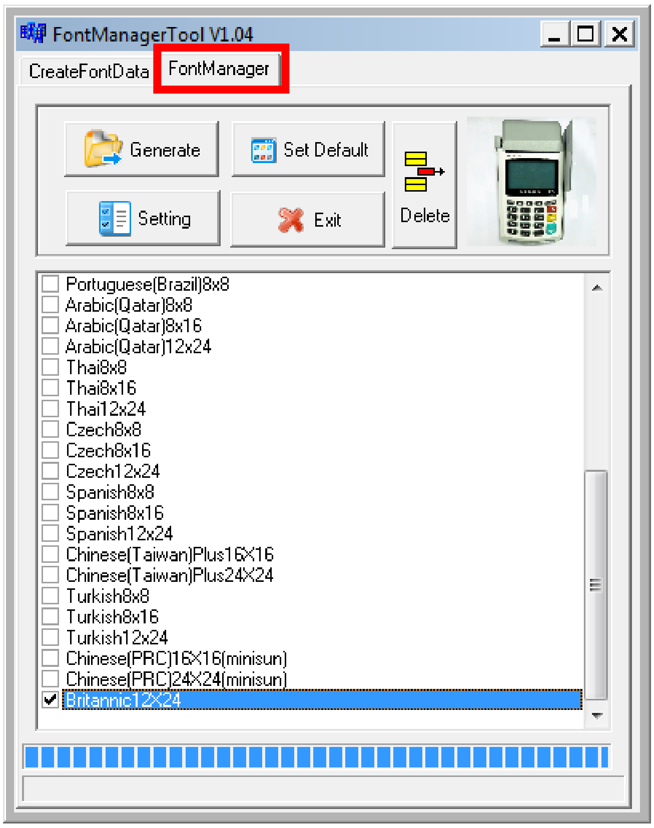
Size:
12 * 24

Version:(HEX)
0001

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



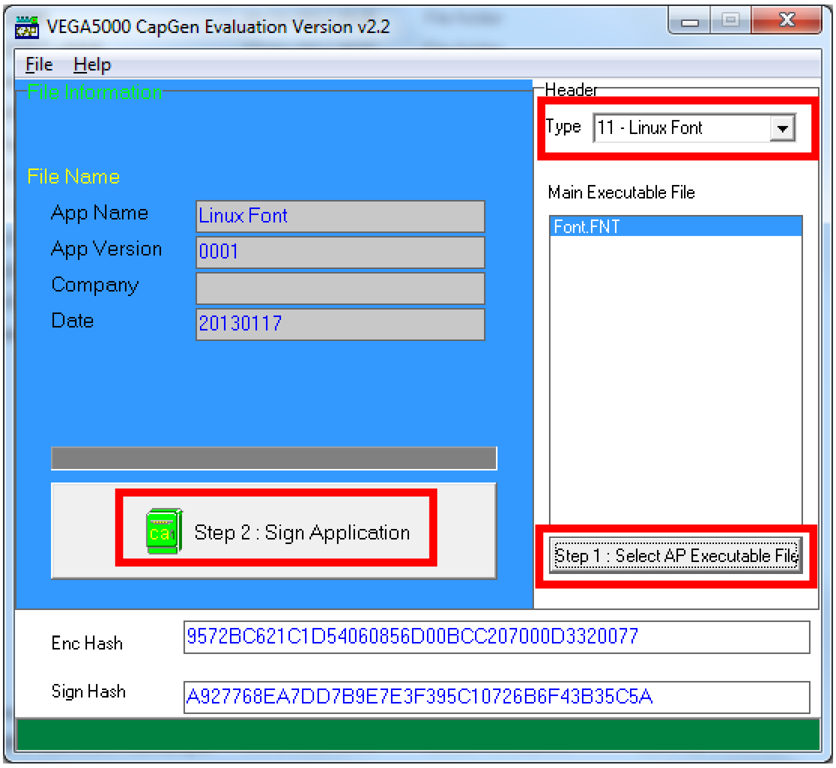
- Select [Font Manager] tab and tick the newly created font, and press [Generate] button to export to FNT file.



□ 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

Type: 11 - Linux Font

Main Executable File: Font.FNT

File Name

App Name: Linux Font

App Version: 0001

Company:

Date: 20130117

Enc Hash: 9572BC621C1D54060856D00BCC207000D3320077

Sign Hash: A927768EA7DD7B9E7E3F395C10726B6F43B35C5A

- Download the font CAP file to UPT1000M.
- In the 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.

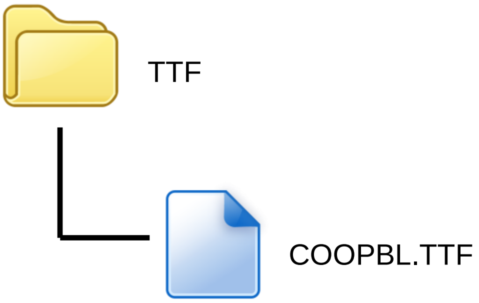
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

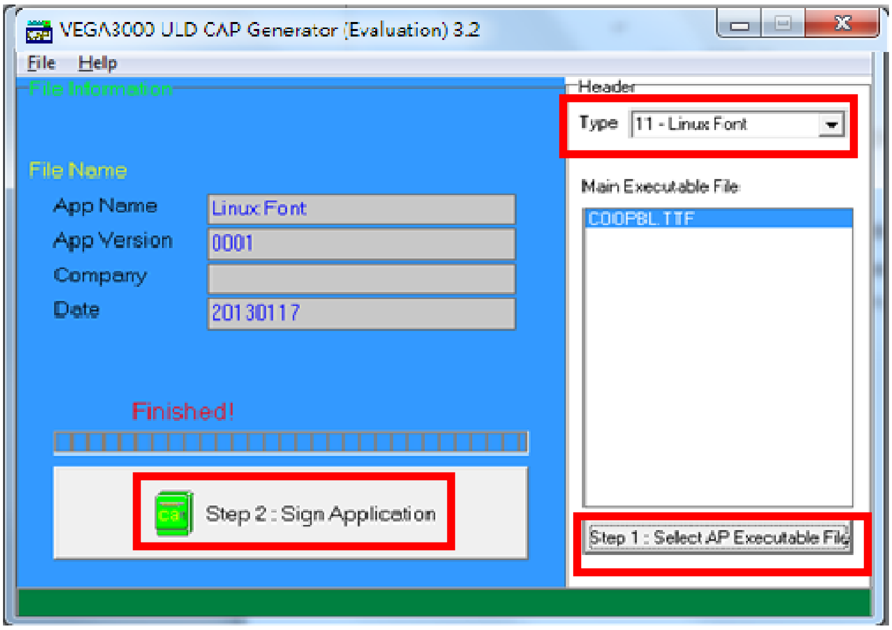
TrueType Font (TTF) is supported in UPT1000M. You can download the TrueType font to UPT1000M for displaying or printing.

<u>Following steps demonstrate how to use “Cooper Black” TrueType font.</u>

- 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 Information

File Name

App Name: Linux Font

App Version: 0001

Company:

Date: 20130117

Finished!

Header

Type: 11 - Linux Font

Main Executable File: COOPBL.TTF

- Download the font CAP file to UPT1000M.

- In the 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. Appendix

6.1. FCC Warning

Federal Communication Commission Interference Statement

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.

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 of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

RF exposure statements

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body or nearby persons.

UL Caution:

This product is intended to be supplied by an UL Listed power supply suitable for use at minimum Tma 65 degree C, altitude during operation up to 5000 m whose output meets Limited Power Source (LPS) or PS2, SELV or ES1, and is rated 5-9Vdc, 2A min., if need further assistance, please contact CASTLES TECHNOLOGY CO LTD for further information.

Ce produit est destiné à être alimenté par une alimentation répertoriée UL pouvant être utilisée à une température minimale de 65 degrés Celsius, une altitude en fonctionnement inférieure à 5 000 m et dont la sortie est conforme à la source d'alimentation limitée (LPS) ou au PS2, au SELV ou à l'ES1, 5-9Vdc, 2A min., Si vous avez besoin d'aide, veuillez contacter CASTLES TECHNOLOGY CO LTD pour plus d'informations.

CAUTION

MISE EN GARDE

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

RISQUE D'EXPLOSION SI LA PILE EST REMPLACÉE PAR UN TYPE INCORRECT.

DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

JETER LES PILES USÉES SELON LES INSTRUCTIONS

~ END ~