

MP200 Mobile POS

Book 2

User Manual

# Confidential

Version 2.4

Aug 2018

# Castles Technology Co., Ltd.

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

# WARNING

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

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

All trademarks mentioned are proprietary of their respective owners.

# **Revision History**

Version	Date	Descriptions		
1.0	Sep 10, 2014	Initial creation.		
		1. Add "Key Injection" on "System Menu" page		
		2. UI arrangement on "SYSTEM INFO" page		
2.0	Dec 19, 2014	3. Add "BT DIRECT ACCESS", "Halt Timeout", "PWM		
2.0	Dec 19, 2014	Auto", "PWM Mode", "PWM Time" on "SYS		
		SETTINGS" page		
		4. UI arrangement on "Test Utility" page		
		1. Add the description of Environment.		
2.1		2. Add the description of Power.		
		3. Add the UL caution of battery.		
2.2	Sep 06, 2016	1. Add "2.4. Wireless communication".		
2.3	Mar 06, 2018	1. Add warnings to "2.3 Power".		
		1. Remove "GPRS" and "UMTS" from 2.4 Wireless		
2.4	Aug 08, 2018	communication.		
2.4	Aug 00, 2010	2. Modify the description of RF Exposure Warning form		
		"20 centimeters" to "5 centimeters".		

# Contents

1.	1. Introduction						
2.	Hardware Setup						
	2.1.	2.1. Parts of the Surface					
	2.2.	Environment9					
	2.3.	Power	9				
	2.4.	Wireless communication	9				
3.	Basic	Basic Operation					
	3.1.	Program Manager	10				
	3.2.	Download AP	12				
	3.3.	System Info1					
	3.4.	Memory Status	14				
	3.5.	System Settings	15				
	3.6.	Test Utility	18				
	3.7.	Factory Reset	20				
	3.8.	Power Off					
	3.9.	Function Key Password Change	22				
	3.10.	<ol> <li>Share Object Management</li></ol>					
	3.11.	11. Castles TMS2					
	3.12.	2. Font Mng					
	3.13.	3. Debug Tools					
	3.14.	4. ULD Key Hash2					
	3.15.	5. Plug-in Mng					
	3.16.	16. Key Injection					
4.	Secu	re File Loading	30				
	4.1. ULD Key System						
		4.1.1. ULD Manufacturer Key	30				
		4.1.2. ULD User Key	32				
		4.1.3. Key Change	32				
	4.2.	File Signing	33				
		4.2.1. Signing Kernel Module	33				
		4.2.2. Signing User Files	35				
	4.3.	File Loading	39				
		4.3.1. Download by User Loader	39				

	4.4.	Changing ULD User Key	42	
5.	. Font Management			
	5.1.	Loading New Font	49	
	5.2.	Custom Font	52	
	5.3.	Using TrueType Font (TTF)	60	
6.	FCC	Warning	62	
	FCC	Caution	62	
	RF E	xposure Warning	62	
	FCC	Caution	62	

# 1. Introduction

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

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

# 2. Hardware Setup

### 2.1. Parts of the Surface

Front Side

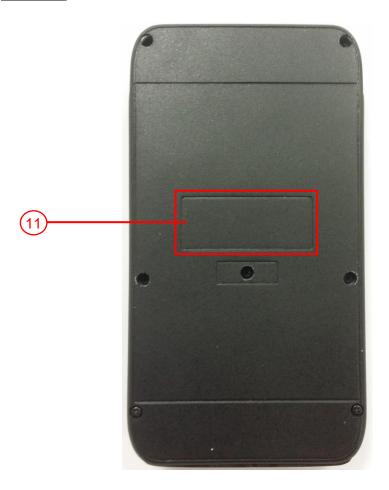


MP200

- 1. LCD Display (Mono Color)
- 2. Keyboard
- 3. Cancel Key
- 4. 0 / Funtion Key
- 5. Contactless Card Landing Zone Enter Key

- 6. Power Key
- 7. Up Key
- 8. Down Key
- 9. OK / Enter Key
- 10. Clear Key

<u>Rear Side</u>



11. Machine's Label



bottom Side



12. MSR 13. SCR





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

### 2.2. Environment

**Operating Temperature** : 0°C to 50°C **Storage Temperature** : -20°C to 70°C **Operating Humidity** : 5% to 90% non-condensing **Storage Humidity** : 5% to 95% non-condensing

### 2.3. Power

Input : 5V, 1A

This product is intended to be supplied by a Listed Power Adapter rated output 5Vdc, min. 1A, Tma is 40 degree C minimum.

### 2.4. Wireless communication

- 1. WiFi 802.11 bg / WiFi 802.11 n
- 2. Contactless Reader (NFC) Working Frequency 13.56MHz.
- 3. Bluetooth

#### CAUTION

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

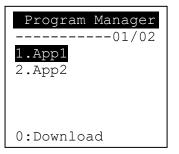
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

# 3. Basic Operation

### 3.1. Program Manager

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

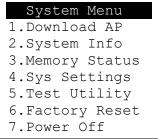
Program Manager



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

#### System Menu

### Page 1



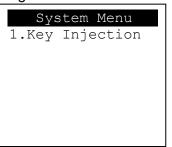
• Press [  $\downarrow$  ] button to page 2.

Page 2

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

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





Press [ ↑ ] button to page 2.

### 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



Select download source:

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

### 3.3. System Info

View kernel module firmware information.

#### System Menu

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

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

#### System Info Menu

SYSTEM INFO

---Kernel Ver---

LINUXKNL :VR0019

:VR0010

:VRF810

:VR9201

#### Page 1

BIOS SULD

ROOTFS

Page 2

\_\_\_

KMS

DRV

USB

SAM

CL

SYSTEM INFO

KO Ver

SECURITY :VR0025

\_\_\_

:VR0024

:VR0039

:VR0028

:VR0018

: N/A

Page 3

CACLENTRY

CAEMVL2AP

CAMPP

CAVPW CAEMVL2

_	0	
	SYST	EM INFO
	K	0 Ver2
	SC	:VR0011

■ Press [ ↓ ] button to next page.

Page 4		Page	5		 Page 6	
SO V UART USBH MODEM ETHERNET FONT	INFO /er :VR0014 :VR0011 :VR0014 :VR0029 :VR0025	PRT RTC ULD PPP KMS	PM	Ver2 :VR0020 :VR0013 :VR0022 EM:VR0026 :VR0022	SYSTEM SO V GSM BARCODE TMS TLS CLVW	er3 :VR0018 :VR0013 :VR0013 :VR0011 :VR0018
LCD	:VR0034	FS Page 9	<u> </u>	:VR0015	CTOSAPI	:VR9029
Page 8 SYSTEM HWM CRDL/ETHE	-		STEM ID:	0CA6A050	Page 10 SYSTEM EXT SO T CACLMDL	INFO Ver P.1 :VRg103

TIMM VET
CRDL/ETHE:ONCHIP
CLM-MP : N/A
AP Ver
ULDPM :VR0026

--Factory S/N---

FFFFFFFFFFFFFFFFF

:VRg103 :VR0302

:VR0014

:VR9113 :VR0005

### 3.4. Memory Status

View terminal flash memory and RAM information.

#### System Menu

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

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

Memory Status Menu

MEMORY	STATUS
FLASH	Memory
Total:	130688KB
Used :	96648KB
SDRAM	Memory
Total:	65408KB
Used :	32148KB

# 3.5. System Settings

View or	change	terminal	system	settings.

Setting	Descriptions
Key Sound	Enable (Y) or disable (N) the beep sound when
	pressing any key.
Exec DFLT AP	Enable (Y) or disable (N) execution of default
	selected application.
USB CDC Mode	Enable (Y) or disable (N) USB CDC mode.
FunKey PWD	Enable (Y) or disable (N) password protection to
	access function key $(0 \sim 3)$ 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></tbc>
BAT Threshld	Battery charging threshold value. [Portable model
	only]
Null Cradle	Enable (Y) if base is Type A cradle. [Portable
	model only]
Debug Mode	Enable (Y) or disable (N) console debug mode.
Debug Port	Serial port for console debug.
Mobil AutoON	Enable (Y) or disable (N) to auto turn on GSM
	module after start up the terminal.
Bklit Auto Off	Enable (Y) or disable (N) Auto Off LCD Backlight
Bklit Off Time	Threshold of Auto Off LCD Backlight
PWR KEY OFF	Power key function, power off (Y) or reboot(N)
GDB Mode	Enable (Y) or disable (N) GDB mode.
GDB Timeout	GDB connection timeout.
GDB Channel	GDB connection channel.
ETHER IP/PORT	GDB Ethernet connection setting.
DTO Time a Zara -	Set Time Zone of Real Time Clock.
RTC Time Zone	

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

### System Menu

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

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

### System Settings Menu

Page 1

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

### Page 3

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

-		
SYS SETTINGS		
SET USB Host	:	Ν
Base USB CDC	:	Х
List SHR Lib	:	Ν
Key MNG Mode	:	0
Bat Threshld	:	Х
Null Cradle	:	Х
1: Prev 2: No	22	κt



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

#### Page 5

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

SYS SETTINGS	5
BT DIRECT ACCESS	:X
Halt Timeout	:999
PWM Auto	: N
PWM Mode	: X
PWM Time	: X
1: Prev Page	

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

### 3.6. Test Utility

Perform terminal hardware components diagnosis.

#### System Menu

Press [5] button to enter Test Utility menu.

Test Utility Menu

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

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

, age -	
Main	Menu 9122
13.CL	14.WiFi
->	2/2

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

## 3.7. Factory Reset

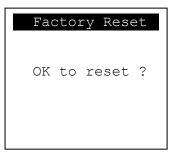
Perform factory reset, all user application, fonts and data will be deleted.

#### System Menu

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 Menu



Press [OK] button to perform factory reset.



Enter factory reset password. Default password: 8418

### 3.8. Power Off

Power off terminal.

System Menu

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

• Press [7] button to power off terminal.

### 3.9. Function Key Password Change

Change function key access password.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

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

FunKey Password Menu



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



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

FunKey Password
New Password: ****
Confirm Password ****
PWD Changed OK

### 3.10.Share Object Management

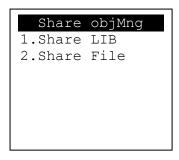
View share object in terminal.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

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

Share Object Management Menu



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

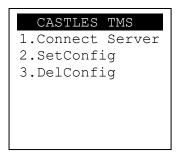
### 3.11.Castles TMS

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

System Menu (Page 2)

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

Castles TMS Menu



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

### 3.12.Font Mng

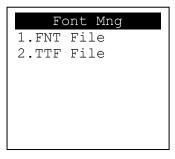
View Font Management.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

Press [4] button to view Font Management.

#### **FontManagment**



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

### 3.13. Debug Tools

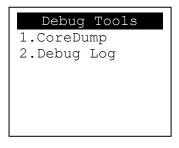
Perform the Debug Tools.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

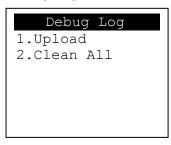
Press [5] go to the Debug Tools Menu.

Debug Tools



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

#### Debug Log



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

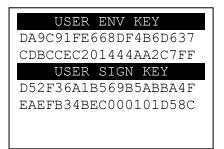
### 3.14.ULD Key Hash

View ULD user key hash value.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

• Press [6] button to view hash value.



### 3.15.Plug-in Mng

View Plug-in Management.

#### System Menu (Page 2)

System Menu
1.FK PWD Change
2.Share obj Mng
3.Castles TMS
4.Font Mng
5.Debug Tools
6.ULD KEY HASH
7.Plug-in Mng

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

Plug-in Mng
1.Info 2.Del

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

### 3.16.Key Injection

View Key Injection.

System Menu (Page 3)

System Menu
1.Key Injection

• Press [1] button to view Key Injection.

Select COM Port
01/03
1. COM 1
2. COM 2
3. USB
OK:Select X:Exit

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

# 4. Secure File Loading

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

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

### 4.1. ULD Key System

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

### ULD Manufacturer Key Set

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

### ULD User Key Set

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

For MP200, the RSA key length is 2048bits.

### 4.1.1. ULD Manufacturer Key

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

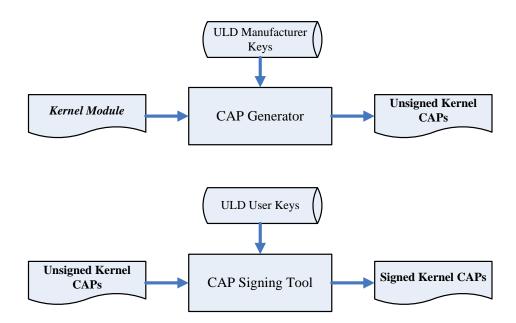
The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only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

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

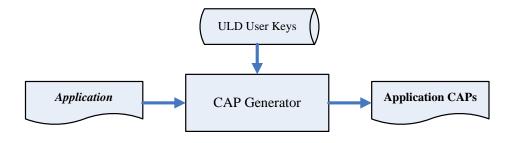
2. The "sign" action via ULD User Keys actually is done by" the second encryption". "The second encryption" is done by using the randomgenerated 3DES key, which is encrypted by ULD User Key Encryption Key, to perform Triple DES encryption again on the cipher data segment of the kernel CAP files. This ensures that the system cannot retrieve the correct data from the kernel CAPs without the user permission.



### 4.1.2. ULD User Key

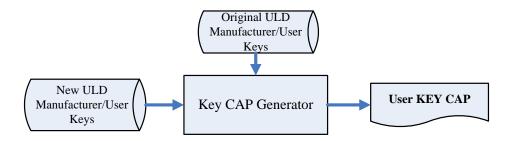
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the "signed' action via ULD User Keys.

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



### 4.1.3. Key Change

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



### 4.2. File Signing

### 4.2.1. Signing Kernel Module

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

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

The CAP Signing Tool is located at: C:\Program Files\Castles\MP200\tools\Signing Tool

Run CAP Signing Tool



Insert Key Card and select smart card reader

### Enter Key Card PIN

<u>F</u> ile	<u>H</u> elp			
File	Information			
	lahc			
	****			
			Enter	Cancel
			Enter	
		Select N	1Cl File	
				Reset

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

<u>F</u> ile <u>H</u> elp		
File Inform		
	abc 😐	
	HEX CA	4P
Key R	eady	
	, 	
	Select MCI File	
		Reset

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

### 4.2.2. Signing User Files

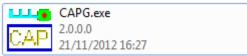
Following files are required to sign before load to terminal. This is to ensure the application data and codes confidential and integrity. The output file will be "CAP" file which is file format defined by Castles.

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

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

The CAP Generator is located at: C:\Program Files\Castles\MP200\tools\CAPG (KeyCard)

#### Run CAP Generator



•	Insert Key	Card and	select	smart	card	reader
---	------------	----------	--------	-------	------	--------

File Help File Information File Name App Name	Test Apr Choose Reader	Header Type 10 - Linux AP & Files Def Select Main Executable File 7z.dll
App Version Company Date	0001 CASTLES E2100PU 0	7z.exe 7-zip.dll CAPG.exe GPAPI.dll IFDAPI.dll
Step 2 : Sign Application		Step 1 : Select AP Executable File
Enc Hash Sign Hash		

### Enter Key Card PIN

<u>F</u> ile <u>H</u> elp	
File Information	Header
	Type 10 - Linux AP & Files 💌
File Name	🗖 Def Select
	Main Executable File
App Name Test Application	7z.dll 7z.exe
App Version 0001	
Company PIN : ****	
Date	
	Enter Cancel
Step 2 : Sign Appl	ication Step 1 : Select AP Executable File
Enc Hash	
Sign Hash	

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

<u>F</u> ile <u>H</u> elp		
File Information File Name App Name App Version Company Date	Test Application 1 0001 20121219	Header Type 10 - Linux AP & Files We 10 - Linux AP & Files 11 - Linux Font Mai E 20 - Share Library 21 - Share Files 72 III 22 - AppData Files 72 III 22 - AppData Files 73 - Stare Files 74 - Carrow CAP GP AP-UT IFDAP1.dl
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash	3E278EA92CBF937370A24E5C219Df	F2172592E79A
Sign Hash	45B7EC170D7260EB4B28AC9A00C3	74299991F84D

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

<u>F</u> ile <u>H</u> elp		
-File Information-		-Header
		Type 10 - Linux AP & Files 🔍
File Name		🔲 Def Select
App Name	ME LIEU-Mentel	Main Executable File
	V5_HelloWorld	V5_HelloWorld
App Version	0001	
Company -		
Date	20121219	
Finist	ned!	
	a	
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash	3E278EA92CBF937370A24E5C219D	F2172592E79A
Sign Hash	45B7EC170D7260EB4B28AC9A00C3	74200001 E94D
olginnaan	4967EC170D7260EB4620AC9A00C3	74233331F04D

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

File Information Header
Type 10 - Linux AP & Files
Def Select
File Name Main Executable File
App Name V5_HelloWorld V5_HelloWorld
App Version 0001
Company
Date 20121219
Finished!
Step 2 : Sign Application Step 1 : Select AP Executable F
Enc Hash 3E278EA92CBF937370A24E5C219DF2172592E79A
Circulture
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.



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



### 4.3. File Loading

There are several ways of loading file to MP200.

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

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

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

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

#### 4.3.1. Download by User Loader

The User Loader works for MP200.

The Loader is located at: C:\Program Files\Castles\MP200\tools\Loader

Run User Loader



#### Select COM port

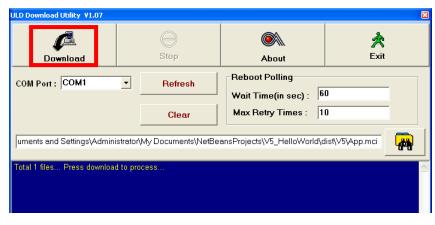
ULD Download Utility ¥1.07		1	8
ß			余
Download	Stop	About	Exit
COM Port COM1 -	Refresh	Reboot Polling	
		Wait Time(in sec) : 6	0
	Clear	Max Retry Times : 1	0
uments and Settings\Administrat	tor\My Documents\NetBe	ansProjects\V5_HelloWorld\c	list\V5\App.mci
Total 1 files Press download to	process		

Browse and select mci file or mmci file

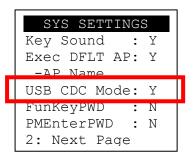
ULD Download Utility ¥1.07			×
<b>Download</b>	Stop	About	<b>À</b> Exit
COM Port : COM1	Refresh	Reboot Polling Wait Time(in sec) : [6	0
uments and Settings\Admini	Clear strator/My Documents/NetBe	ansProjects\V5_HelloWorld\	0 dist(\/5\App.mci
Total 1 files Press downloar	d to process		

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

• Press "Download" button to start.



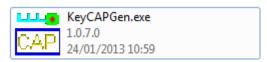
Note: To download using USB cable, terminal must enable CDC mode. Set USB CDC Mode to Y.



### 4.4. Changing ULD User Key

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

Run Secure Key Generator



Insert Key Card and select smart card reader

ile Uption He	Key CAP Generator (RSA) V3.3		<u>e</u>
18 bits motion		Update PIN	Save to Card
		Get Hash	Reset
	Secure Key 0001	BSA Key for Kenc     Public Key Modulus (N)	Length =
		Public Key Exponent [E] Private Key Exponent [U] HASH	Reader ES EZ100PU 0
	Make Key CAP File	RSA Key for Signature Public Key Modulus (N)	Length =
		Public Key Exponent (E) Private Key Exponent (D)	
		HASH	

• Enter Key Card PIN, default PIN is "1234".

	Update PIN	Save to Card
Secure Key	Get Hash	Reset
0001	RSA Key for Kenc Public Key Modulus (N)	Length =
	Public Key Exponent (E)	
		Enter Cancel
Make Key CAP File	RSA Key for Signature Public Key Modulus (N)	Length =
	Public Key Exponent (E) Private Key Exponent (D)	
	HASH	

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

VEGA3000 Secure Key CAP Generator (RSA) V3.3		<b>1</b>
<u>File Option Help</u>	-New Key	
	Update PIN	Save to Card
	Get Hash	Reset
Acto Names Secure Key	RSA Key for Kenc	
App Version 0001	Public Key Modulus (N) Length =	
	Public Key Exponent (E) Private Key Exponent (D) HASH	
Make Key CAP File	RSA Key for Signature     Public Key Modulus [N]     Length =	
	Public Key Exponent (E) Private Key Exponent (D) HASH	

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

Form3 PIN Block			
New PIN :	Į.		
Conform PIN :			
	Reset	Enter	Cancel

• To view current key set hash value, goto "Option" and select key.

VEGA38000 Service Key CAP Generator (RSA) V3.3	
Hie Option   Help	
Key	New Key Update PIN Save to Card
File Name     Secure Key       App Films     Secure Key       App Version     0001       Compton     Image: Compton	Get Hash     Reset       RSA Key for Kenc     Public Key Modulus (N)
	Public Key Exponent (E) Private Key Exponent (D) HASH
Make Key CAP File	RSA Key for Signature           Public Key Modulus (N)           Length =           Public Key Exponent (E)           Private Key Exponent (D)           HASH

irrent Key Setting	
itatus	
Load Key OK!	
RSA Key for Kenc	
Public Key Modulus (N)	Key Length = 256
***************************************	***************************************
Public Key Exponent (E)	
Private Key Exponent (D)	*****
1	*****
HASH	
277BF11E6827FF2A263DEDE6DEC84	B2BE9B3E576
1	
RSA Key for Signature	
	14 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
Public Key Modulus (N)	Key Length = 256
Public Key Modulus (N)	
***************************************	
***************************************	
Public Key Exponent (E)	
Public Key Exponent (E)	*****
Public Key Exponent (E) ****** Private Key Exponent (D)	***************************************
Public Key Exponent (E) Private Key Exponent (D) Private Key Exponent (D) Private Key Exponent (D)	*****
************************************	*****
Public Key Exponent (E) Private Key Exponent (D) Private Key Exponent (D) Private Key Exponent (D)	*****

- 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.

e Option He	4	-New Key	
		Update PIN	Save to Card
		Get Hash	Reset
	Secure Key	RSA Key for Kenc	
	0001	Public Key Modulus (N)	Key Length = 256
		EC3AAE48CBA638EC97A9D2EF2DE68D5562	278EE3876C072F8C80443A84E
		Public Key Exponent (E) 010001	
		Private Key Exponent (D)	
		ACF038CE61F0AD798C57CA64AE1E2C743F0	3455A90E.AD34766CFE78D-4C
		HASH	
-		RSA Key for Signature	
	-	Public Key Modulus (N)	Length =
	Make Key CAP File		
		Public Key Exponent (E)	
		Ptivate Key Exponent (D)	
		HASH	

• Generate second RSA key set for Signature.

Eile Option Hel	Key CAP Generator (RSA) V3.3	E
File Internetion File Name App Name App Version Company	Secure Key 0001	New Key         Save to Card           Get Hash         Reset           RSA.Key for Kenc         Reset           Public Key Modulus (N)         Key Length = 256           EC3AAE.480E8A638EC97ASD.2E.F2DE.88D556278EE.9876C072F8C80443A84EE         Public Key Exponent.(E)           Public Key Exponent.(E)         (010001           Private Key Exponent.(D)         4CF038CE51F0AD738C57CA64AE1E2C743FD3455A30EAD34766CFE.78D4C5           HASH
(	Make Key CAP File	BSA Key for Simplese     Public Key Modulus (N)     Key Length = 256     SSECSF37500D08AAE26F374C4831080695EADED4691E00FA87FF2DEA015     Public Key Exponent. (E)     010001
		Pixale Key Exponent (D) 26AC4EEC84FED3184C3D0335C00697E46529E9DD8B35368D4E2E6544EF6 NASH

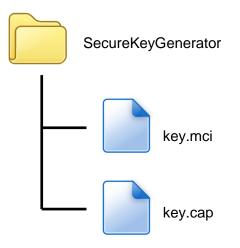
Click [Get Hash] button to calculate the hash value for key sets. 

	ey CAP Generator (RSA) V3.3	2
Ele Option Help File Intormation File Name App Name App Version	Secure Key 0001	New Key Update PIN Get Hash Reset PLole Key Modulus (N) Key Length = 256
		Public Key Modula (N)         EC:3AAE 4BCBA638EC97A9D 2EF2DE08D556278EE3976C072F902B0443A64EE           Public Key Exponent (E)         [010001]           Primate Key Exponent (D)         [40F0380261F0AD79805770664AE1620743FD3455A306AD347660FE78D405]           HASH         [608F32738038A3167710EE468E4A27EDE08/31A48F
-	Make Key CAP File	RSA Key for Signature     Public Key Modukus (N)     Key Length = 256     Sec 3F3750CD 08AAE28F374C483108089EADED4691E0DFA87FF2DEAD15     Public Key Exponent (E)     D10001     Private Key Exponent (D)
Generate HASH C	KI	26AC4EEC84FED31B4C30-0935C00697E46529ESDD8835368D4E2E6544EF6 HA5H 945E4224208F950E24583097C8FA8B5EE73788F2

- 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.

Eile Option Help		
File Information-		New Key Update PIN Save to Carr
	Secure Key 0001	Get Hash         Reset           RSA.Key for Kenc         RSA.Key for Kenc           Public Key Modulus (N)         Key Length = 256           EC344E 48C8A638EC97A9D2EF2DE88D556278EE9876C072F80C80443A84E
		Public Key Exponent (E) 010001 Private Key Exponent (D) 4CF038CE61F0AD738C57CA64AE1E2C743FD3455A30EAD34766CFE78D4C HA5H 6DIBF3279803A316771DEE4E8E4A27EDE0831A48F
	Make Key CAP File	RSA Key for Signature Public Key Modulus (N) Key Length = 256 (SSECSF37500DBAAE25F374C483108089EADED4691E00FAB7FF2DEA015
		Public Key Exponent (E) [010001 Private Key Exponent (D) [26AC4EEC84FED31B4C3D0935C00597E46529E30D B835368D 4E2E6544EFE HASH
Generate HASH 0		1455H 945E4224208F950E245B3097C8FABB9EE73788F2

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



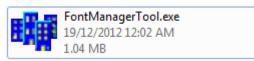
 To update the newly generated key set to Key Card, press [Save to Card] button to write the key set to Key Card.

ile Option Help	C New Key
	Update PIN Save to Card
	Get Hash Reset
Secure Key	PSA Keylor Kenc
0001	Public Key Modulus (N) Key Length = 256
A CALEMAN AND AND A CALEMAN AND AND A CALEMAN AND AND AND AND AND AND AND AND AND A	E C3AAE 48/CBA638E C97A9D 2EF2DE 88D556278EE 9876C072F8C80443A84EE
	Public Key Exponent (E) 010001
	Private Key Exponent (D) 40F03802651F0AD798057CA64AE1E20743FD3495A30EAD347660FE76D405
	HASH
	608F3279809A316771DEE4E8E4A27EDE0831A48F
	RSA Key for Signature
Make Key CAP File	Public Key Modulus (N) Key Length = 255
Make Ney CAC File	99EC9F3750CDD 8AAE.26F374C48/3108D/89EADED4691E0DFAB7FF2DEA015
	Public Key Exponent (E) 010001
	Private Key Exponent (DI)
	26AC4EEC84FED/3184C300935C00697E46529E90D8835368D4E2E6544EF8
	HASH
	945E4224208F950E245B3097C8FABB9EE73788F2

## 5. Font Management

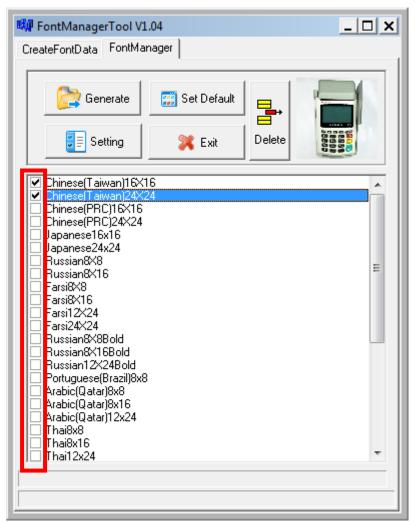
### 5.1. Loading New Font

Run FontManager.exe

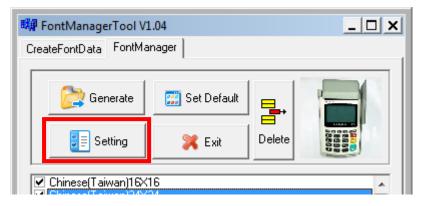


Located at C:\Program Files\Castles\Font Manager

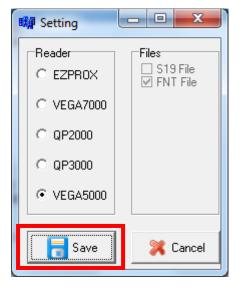
Select font to download



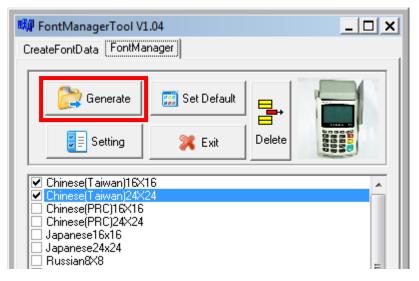
• Press [Setting] button to configure terminal type.



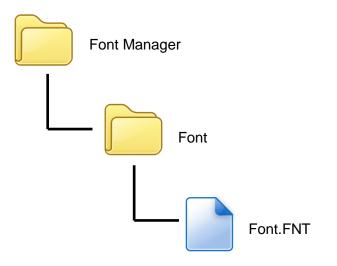
Select VEGA5000, press [Save] button to save and return font manager.



Press [Generate] to create the font file.



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



• Sign the file using CAP Generator, the type must set to "11 – Linux Font".

👼 Vega5000 CAP G	ienerator v2.2	
<u>F</u> ile <u>H</u> elp		
-File Information-		-Header Type 11 - Linux Font
File Name		Main Executable File
App Name	Linux Font	Font.FNT
App Version	0001	
Company		
Date	20121219	
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash	3E278EA92CBF937370A24E5C219DF	F2172592E79A
Sign Hash	45B7EC170D7260EB4B28AC9A00C3	74299991F84D

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

### 5.2. Custom Font

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

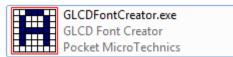
There are two zone defined:

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

Zone  $0x80 \sim 0xFF$  – Free to use, you may use for symbols.

#### Following steps demonstrate how to create a 12x24 font.

Run GLCD Font Creator



GLCD Font Creator 1.1.0 - mikr	oElektronika Edition		
File Edit Effects Batch Tools	Help		
🛐 New Font	New Font From Scratch		6
💕 Open Font	Minport An Existing System Font		Previ
Save Font	📕 New HD44780 LCD Custom Characters Set	Set Full Column	
Save Char Ctrl+S	Right Click : Clear Pixel Ctrl+Right Click	: Clear Full Column	
Export for MikroElektronika			Tools
Quit			
-	_		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			×
Eont: Britannic Britannic Broadway Brusk Script MC7 Calibri Californian FB	Font style: Bold Bold Oblique	Size: 11 12 14 16 18 20 22 ▼	OK Cancel
Effects Stri <u>k</u> eout Underline <u>C</u> olor:	Sample AaBbYyZ	'z	
Custom	Sc <u>ri</u> pt: Westem	•	

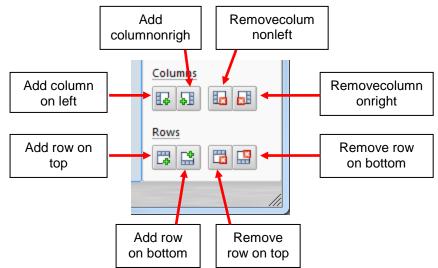
Set the import range from 0 to 127. 

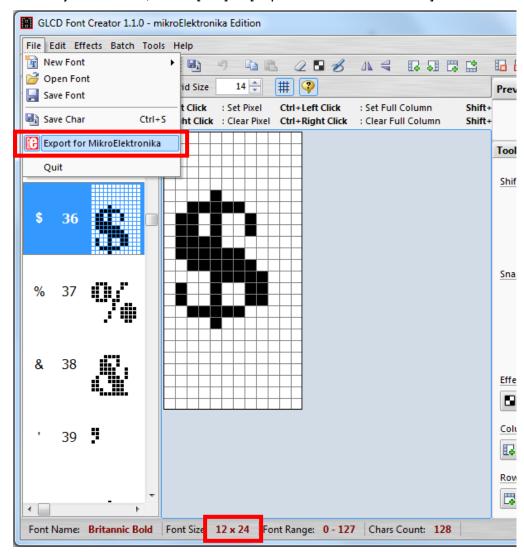
Import font
Font Name Britannic Bold
Range
From 0 🚔 To 127 🚖
Optimize Imported Font
Remove :
Common blank Rows at TOP of all chars
Common blank Rows at BOTTOM of all chars
Common blank Columns at LEFT of all chars
Common blank Columns at RIGHT of all chars
✓ <u>O</u> k

ile <u>E</u> dit Effe <u>d</u>				0						
🛐 🕶 🧀 🔚	Export	Grid Size		► 2 🖬 쒿  #  🖓		16 91 L6	6			-
har Code G	LCD ^	Left Click	: Set Pixel	Ctrl+Left Click	: Set Full	Caluma	Shift+	Preview	Blue 🔻	
				Ctrl+Right Click			Shift+			
0										
								Tools		_
								Shift / Mo	ve	
								ſ	•	
1								4	5 4	
									4	
				++				U.		
2				+-+-1				Snap To B		
Z									<b>1</b>	
								<b>H</b>		
								l	<b>U</b>	
3										
								Effects		
								<b>B</b> 💋	4⊾ 🚭	
4								Columns		
4								<b>14 41</b>		
	-							Rows	m 🖪	
•	•							<b>1</b>	1	

• 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].

Select output format as [mikroC].

Generate Code For Use With
mikroC GLCD Lib 🔘 X-4
Font height > 8bits, only X-GLCD
CD Lib.

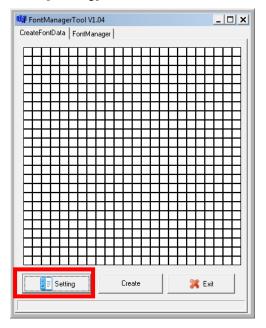
 Remove comment "// Code for char " from offset 0x00 to 0x1F. Remove empty line if found. Then click [Save] button to save to file.

ont Name Brit	annic_Bold12x24			Fro	m Char 0	To Char 12
				G	enerate Co	de For Use With
						GLCD Lib
i mikroBasic	🚺 mikroPaso	al 🕒 mikroC				
0x00, 0x00,	0x00, 0x00 0x00, 0x00 0x00, 0x00 0x00, 0x00	, // Code , // Code	for for	char char		← Remove
0x00,	0x00, 0x00	, // Code	for	char		Remove
	0x00, 0x00 0x00, 0x00					← Remove Remove
0x00, ∢	0x00, 0x00	, // Code	for	char		Kelliove

Run Font Manager Tool.



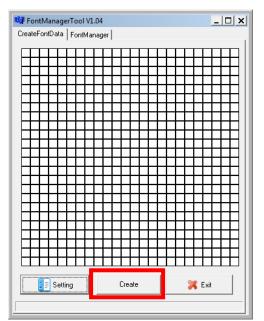
Click [Setting] button



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

🗱 DataSetting 📃 🗖 🗙			
FileName:			
Britannic			
ID:(HEX)			
A000			
Style:			
thin 💌			
Size:			
12 * 24			
Version:(HEX)			
0001			
ОК			

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



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

🙀 FontManagerTool V1.04			_ 🗆 🗙	
CreateFontData FontMa	nager		1	
Cenerate	🧱 Set Default			
Setting	💢 Exit	Delete		
Portuguese(Brazil)8x8 Arabic(Qatar)8x8 Arabic(Qatar)8x16 Arabic(Qatar)12x24 Thai8x8 Thai8x8 Thai8x8 Czech8x8 Czech8x8 Czech8x16 Czech8x8 Czech8x16 Spanish8x16 Spanish8x16 Spanish12x24 Chinese(T aiwan)Plus16×16 Chinese(T aiwan)Plus16×16 Turkish8x16 Turkish8x16 Turkish8x16 Chinese(PRC)16×16(minisun) Chinese(PRC)24×24(minisun) W Britannic12×24				
1				

Use CAP Generator to conver 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 CapGe	en Evaluation Version v2.2		
<u>F</u> ile <u>H</u> elp			
-File Information-		Header Type 11 - Linux Font	
File Name		Main Executable File	
App Name	Linux Font	Font.FNT	
App Version	0001		
Company			
Date	20130117		
	Step 2 : Sign Application	Step 1 : Select AP Executable File	
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.

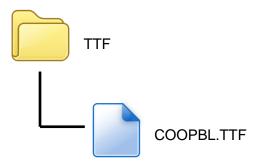
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

## 5.3. Using TrueType Font (TTF)

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

#### Following steps demonstrate how to use "Cooper Black" TrueType font.

• Copy the TTF file needed to a empty folder.



Use CAP Generator to conver 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	X
<u>File</u> <u>H</u> elp		
File Information		Type 11 - Linux Font
File Nome		Main Executable File
App Name	Linux Font	COOPSL TTF
App Version	0001	
Company		
Date	20130117	
Finish	ed! Step 2 : Sign Application	Step 1 : Select AP Executable Filg

Download the font CAP file to terminal.

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

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

#### Or print message using the newly added font.

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

# 6. FCC Warning

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

### **FCC** Caution

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

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

### **RF Exposure Warning**

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

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

This equipment should be installed and operated with a minimum distance of 5 centimeters between the radiator and your body.

#### ~ END ~