

VEGA3000 EFT-POS Terminal

Book 2

User Manual

Confidential

Version1.1

Sep 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	Mar 13, 2018	Initial creation.
1.1		 Correcting the description of page 9. Add chapter "6. Appendix". Add battery caution in page 10.

Contents

1.	Introd	duction	6	
2.	Hardy	ware Setup7		
	2.1.	Parts of the Terminal	7	
	2.2.	Inserting the Battery	10	
	2.3.	Inserting the SAM Card	11	
	2.4.	Inserting the Paper Roll	12	
	2.5.	Inserting the GSM SIM Card	13	
	2.6.	Inserting the Memory card	14	
3.	Basic	c Operation	15	
	3.1.	Program Manager	15	
	3.2.	Download AP	16	
	3.3.	System Info	17	
	3.4.	Memory Status	18	
	3.5.	System Settings	19	
	3.6.	Test Utility	23	
	3.7.	Factory Reset	26	
	3.8.	Power Off	27	
	3.9.	Password Manager	28	
	3.10.	Share Object Management	29	
	3.11.	Font Mng		
	3.12.	ULD Key Hash	31	
3.13. Hardware Detect		Hardware Detect	32	
	3.14.	Bluetooth Setup		
	3.15.	Plug-in Mng	34	
	3.16.	Key Injection		
4.	Secu	re File Loading		
	4.1.	ULD Key System		
		4.1.1. ULD Manufacturer Key		
		4.1.2. ULD User Key		
		4.1.3. Key Change		
	4.2.	File Signing		
		4.2.1. Signing Kernel Module		
		4.2.2. Signing User Files	42	

	4.3.	File Loading	
		4.3.1. Download by User Loader	.46
		4.3.2. Download by Removable Media	.49
	4.4.	Changing ULD User Key	.51
5.	Font	Management	.58
	5.1.	Loading New Font	.58
	5.2.	Custom Font	.61
	5.3.	Using TrueType Font (TTF)	.69
6.	Appe	ndix	.71
	6.1.	FCC Warning	.71
	6.2.	Safety Warning for External Power Source	.72

1. Introduction

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

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 Terminal

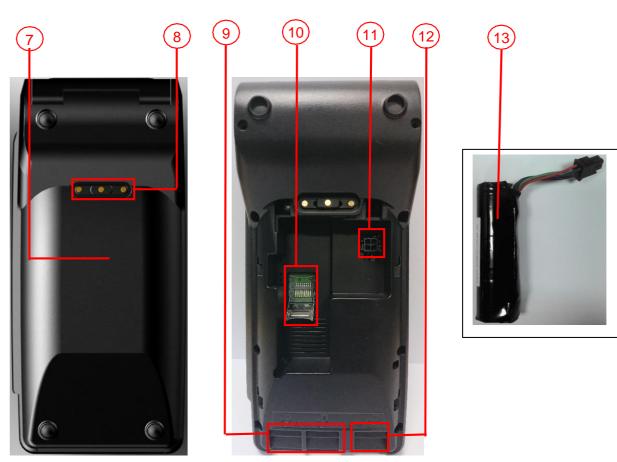
<u>Front</u>



- 1. LCD Display (Color TFT)
- 2. Keypad
- 3. Smart Card Reader

- 4. Magnetic Stripe Reader
- 5. Contactless Card Landing Zone
- 6. Paper Roll Handle

<u>Rear</u>



- 7. Battery Cover
- 8. Charger Base Connector
- 9. SAM Slots
- **10. Micro SD Card Slot**
- 11. Battery Connector
- 12. GSM SIM Card Slots
- **13. Rechargeable Battery**



14. USB Port (Type C)

2.2. Inserting the Battery





Step 1: Remove battery cover

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

Step 3: Reverse the operation of step 1 to install the battery cover.

Note: The battery must be installed. Otherwise, the printer function might not work normally.

CAUTION

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

DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

2.3. Inserting the SAM Card



Step 1: Remove battery cover / back cover

Step 2: Insert SAM card into desire slot.



SAM 1 & 3: Gold contact at upper side of card and facing down.



SAM 2 & 4: Gold contact at upper side of card and facing up.

Step 3: Reverse the operation of step 1 to install the battery cover.

2.4. Inserting the Paper Roll

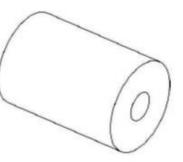


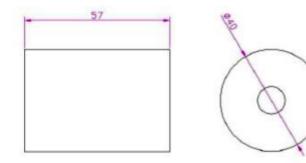
Step 1: Pull up paper roll box handle.

- Step 2: Gentle open paper roll cover.
- Step 3: Insert paper roll as direction showed.

Paper specification

Width: 57mm Outside diameter: 40mm





2.5. Inserting the GSM SIM Card



- Step 1: Remove battery cover / back cover
- Step 2: Open SIM socket and insert GSM SIM card into desire slot.



SIM 1:

Gold contact at upper side of card and facing down.



SIM 2:

Gold contact at upper side of card and facing up.

Step 3: Reverse the operation of step 1 to install the battery cover.

2.6. Inserting the Memory card



- Step 1: Remove battery cover / back cover
- Step 2: Insert Micro SD memory card.



Micro SD: Gold contact at lower side of card and facing down.

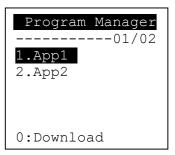
Step 3: Reverse the operation of step 1 to install the battery cover.

3. Basic Operation

3.1. Program Manager

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

Program Manager



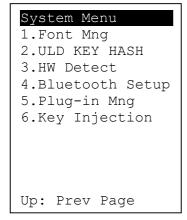
- Press [0] button to enter System Menu.
- Press [1] button to toggle default application selection.
- Press [2] button to delete application.
- Press [3] button to view application info.
- Press [OK] button to run application.
- Press [Power] or [·] as the up and down button to select application.

System Menu

Page 1

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.PWD Manager
9.Share obj Mng
5 5
Down: Next Page

Page	2
------	---



Press $[\cdot]$ 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
8.PWD Manager
9.Share obj Mng
Down: Next Page

• 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
8.PWD Manager
9.Share obj Mng
Down: Next Page

Press [2] button to enter System Info menu.

System Info Menu

Page 1		
SYSTEM	Ι	NFO
Kerne	1	Ver
BIOS	:	VR0026
SULD	:	VRF026
LINUXKNL	:	VR0029
ROOTFS	:	VRM119
PEDST	:	VR0027

Page 2

SYSTEM	INFO
KOVer	
SECURITY:	VRA126
KMS :	VRA127
DRV :	VRAK47
USB :	N/A
CIF :	VRA524
SAM :	VRA433
CL :	VR0018
SC :	VR0011

Page 3

Page 6

SYSTEM II	NFO
SOVer-	
UART :	VR0017
USBH :	VR0011
MODEM :	VRA218
ETHERNET :	VRAC34
FONT :	VRAE31
LCD :	VRAK41
PRT :	VRA924
RTC :	VRA114
ULDPM :	VRA730
PPP MODEM:	VRAH31
KMS :	VRAA32
FS :	VRA116
GSM :	VRA730
BARCODE :	VRA013

Press $[\cdot]$ button to next page.

Page 4

Page	5
i aye	J

SYSTEM INFO SO Ver2 TLS : VRA215 CLVW : VRA425 CTOSAPI : VRA040	SYSTEM INFO HWMVer CRDL/ETHE: N/A CLM-MP : N/A APVer ULDPM : VRMP35	SYSTEM INFO HUSBID: 0A6A050 CUSBID: N/A Factory S/N FFFFFFFFFFFFFFFF

Page 7

0	
SYSTEM II	NFO
-EXT SO Ve	r P.1 -
CRDLMDL :	VR0012
CACLENTRY:	VR0012
CAMPP :	VR0007
CAVPW :	VR0022
CAAEP :	VR0004
CACJT :	VR0008
CAVAP :	VR0003
CACQP :	VR0002
CAIFH :	VR0003
CADDP :	VR0002
CAEMVL2 :	VRA019
CAEMVL2AP:	VR0011
CABARCODESCAI	N:VR0002
CAMMS :	VR0002

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
8.PWD Manager
9.Share obj Mng
Down: Next Page

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

Memory Status Menu

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

3.5. System Settings

View or c	hange	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 ~ 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 Acradle. [Portable model
	only]
Debug Mode	Enable (Y) or disable (N) console debug mode.
Debug Port	Serial port for console debug.
Mobil AutoON	Enable (Y) or disable (N) to auto turn on GSM
	module after start up the terminal.
Bklit Auto Off	Enable (Y) or disable (N) Auto OffLCDBacklight
Bklit Off Time	Thresholdof Auto Off LCD Backlight
PWR KEY OFF	Enable (Y) or disable (N) Power key rebooting
RTC Time Zone	Set Time Zone of Real Time Clock.
NTP Enable	Enable (Y) or disable (N) Network Time Protocol.

NTP Update Freq	Frequency of Network Time Protocol updating.	
PWM Auto	Enable (Y) or disable (N) auto power management	
PWM Mode	Set power management mode. (Not support)	
PWM Time	Set power management time. (Not support)	
BAT PROTECT MODE	Set battery protect mode.	
	A:Auto(default), system will auto switch battery	
	protect mode.	
	N: Normal, without battery protect function mode.	
	P: Protect, with battery protect function mode.	
Auto Reboot	Enable terminal auto reboot.	
Reboot Hour	Set reboot time of hour.	
Reboot Min	Set reboot time of minute.	

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.PWD Manager
9.Share obj Mng
Down: Next Page

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

System Settings Menu

Page 1

SYS SETTIN	GS	
Key Sound	:	Y
Exec DFLT AP	: `	Y
-AP Name		
USB CDC Mode	:	Y
FunKeyPWD	:	N
PMEnterPWD	:	N
SET USB Host	:	N
Base USB CDC	: 3	Х
List SHR Lib	:	N
Key MNG Mode	:	0
Bat Threshld	:	Х
Null Cradle	:	Х
Debug Mode	:	Ν
Debug Port	:	Х
2: Next Page		

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

Page	2
гауе	2

SYS SETTI	NCC
	NG9
Mobil AutoON	: N
Bklit Auto Off	: X
BklitOff Time	: N
PWR KEY OFF	: N
RTC Time Zone	:GMT
NTP Enable	: N
NTP Update Free	y: X
PWM Auto PWM Mode	: 1 : X : X
PWM Time	: X
1:Prev 2	2.Next

SYS SETTINGS	
BAT PROTECT MODE:	A
Auto Reboot : Reboot Hour : Reboot Min :	
1:Prev Page	

Page 3

- Press [Power] or [·] button to select setting.
- Press [OK] button to change the setting value.
- Press [\triangleleft] button to toggle Y \Rightarrow N \Rightarrow Y.
- Press [1] button to previous page.
- Press [2] button to next page.

3.6. Test Utility

Diagnose terminal hardware components.

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.PWD Manager
9.Share obj Mng
Down: Next Page

Press [5] button to enter Test Utility menu.

Test Utility Menu

Page 1

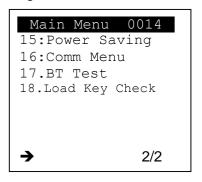
Main Menu 9016
1:LCD
2:Key Board
3:FLASH
4:Smart Card
5:Backlight
6:MSR
7:LED
8:RTC
9:Printer
10:FONT
11:CL_Transparent
12:CL Card Test
13:SD Card Test
14:Wi-Fi Test
→ 1/2

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

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

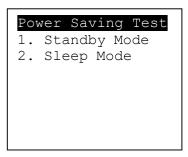
Note: Default password for changing RTC is 8418.

Page 2



- Press [1], [5] and [OK] button to enter Power Saving Test Menu.
- Press [1], [6] and [OK] button to enter Communication Test Menu. •
- Press [1], [7] and [OK] button to enter Bluetooth Test Menu.
- Press [1], [8] and [OK] button to check the ULD key.
- Press [Power] button to previous page.
- Press [X] button to exit.

Power Saving Test Menu



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

Communication Test Menu

Cor	nmunic	ate	Test
1.	COM1	2.	Com2
3.	Com3		
4.	Ether	net	Test
5.	USB		Test
6.	Moder	l	Test
7.	GPRS		Test
8.	All		Test

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

3.7. Factory Reset

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

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.PWD Manager
9.Share obj Mng
Down: Next Page

Press [6] button to enter Factory Reset menu.

Factory Reset Menu



• Enter factory reset password. *Default password: 00000000*

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
8.PWD Manager
9.Share obj Mng
Down: Next Page

• Press [7] button to power off terminal.

3.9. Password Manager

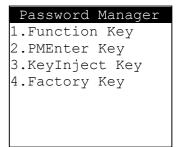
Change the access password.

System Menu

System Menu
1.Download AP
2.System Info
3.Memory Status
4.Sys Settings
5.Test Utility
6.Factory Reset
7.Power Off
8.PWD Manager
9.Share obj Mng
Down: Next Page

Press [8] button to enter Password Manager Menu.

Password Manager



- Press [1] button to change Function Key.
- Press [2] button to change PMEnter Key.
- Press [3] button to change Keylnject Key.
- Press [4] button to change Factory Key.

3.10. Share Object Management

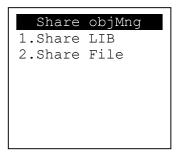
View share object in terminal.

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
8.PWD Manager
9.Share objMng
Down: Next Page

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

Share Object Management Menu



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

3.11.Font Mng

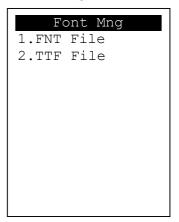
View Font Management.

System Menu (Page 2)

System Menu
1.Font Mng 2.ULD KEY HASH 3.HW Detect
4.Bluetooth Setup 5.Plug-in Mng 6.Key Injection
Up: Prev Page

• Press [1] button to view Font Management.

Font Management



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

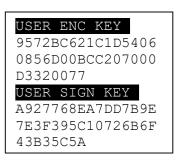
3.12.ULD Key Hash

View ULD user keyset hash value.

System Menu (Page 2)

System Menu
1.Font Mng 2.ULD KEY HASH 3.HW Detect 4.Bluetooth Setup 5.Plug-in Mng 6.Key Injection
O.Key Injection
Up: Prev Page

• Press [2] button to view hash value.



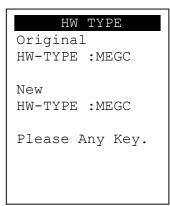
3.13. Hardware Detect

View the hardware type of the terminal.

System Menu (Page 2)

System Menu
1.Font Mng
2.ULD KEY HASH
3.HW Detect
4.Bluetooth Setup
5.Plug-in Mng
6.Key Injection
Up: Prev Page

• Press [3] button to view the hardware type of the terminal.



3.14. Bluetooth Setup

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

System Menu (Page 2)

System Menu
1.Font Mng
2.ULD KEY HASH
3.HW Detect
4.Bluetooth Setup
5.Plug-in Mng
6.Key Injection
Up: Prev Page

Press [4] go to the Bluetooth setup menu.



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

3.15. Plug-in Mng

View Plug-in Management.

System Menu (Page 2)

System Menu
1.Font Mng 2.ULD KEY HASH 3.HW Detect 4.Bluetooth Setup 5.Plug-in Mng 6.Key Injection
Up: Prev Page

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



- Press [Power] 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 Menu. This function is for castles internal only. User or developer cannot use this function.

System Menu (Page 2)

System Menu
 Font Mng ULD KEY HASH HW Detect Bluetooth Setup Plug-in Mng Key Injection
Up: Prev Page

• Press [6] button to view Key Injection Menu.

KeyInj Password	
Enter Pa	issword:

4. Secure File Loading

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

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

4.1. ULD Key System

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

ULD Manufacturer Key Set

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

ULD User Key Set

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

For VEGA3000, the RSA key length is 2048 bits.

4.1.1. ULD Manufacturer Key

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

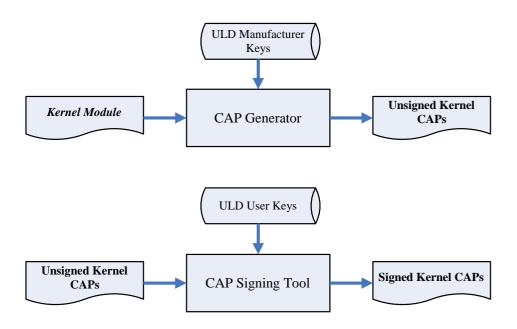
The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only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

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.

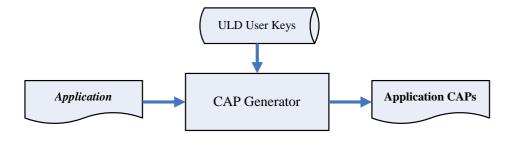
2. The "sign" action via ULD User Keys actually is done by" the second encryption". "The second encryption" is done by using the randomgenerated 3DES key, which is encrypted by ULD User Key Encryption Key, to perform Triple DES encryption again on the cipher data segment of the kernel CAP files. This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



4.1.2. ULD User Key

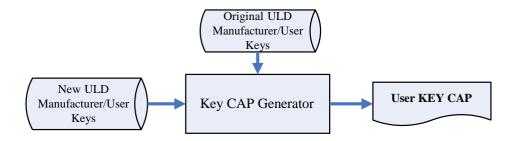
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the "signed' action via ULD User Keys.

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 provides a tool named "CAP Signing Tool" to perform this task.

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

Run CAP Signing Tool



Insert Key Card and select smart card reader

<u>F</u> ile <u>H</u> elp
-File Information-
Choose Reader
CASTLES EZ100PU 0
Processin
Reset

Enter Key Card PIN

<u>F</u> ile <u>H</u> elp			
-File Information			
laho			

		Enter	Cancel
		Entor	Cancer
	Select M	Cl 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 Information	
abc	
HEX	CAP
Kau Danaha	
Key Ready	
Select N	1Cl File
	Reset

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

4.2.2. Signing User Files

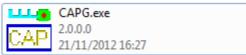
Following files are required to sign before load to terminal. This is to ensure the application data and codes confidential and integrity. The output file will be "CAP" file which format is defined by Castles.

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

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

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

Run CAP Generator



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

<u>F</u> ile <u>H</u> elp		
File Information File Name App Name App Version Company Date	TestApp 0001 CASTLES EZ100PU 0 20121219	Header Type 10 - Linux AP & Files Def Select Main Executable File 7z.dll 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 1	7z.dll
App Version	0001	7z.exe
Company	PIN : xxx	
Date		
	Enter	Cancel
	Step 2 : Sign Application	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-		Header
File Name App Name App Version Company Date	Test Application 1 0001 20121219	re 10 - Linux AP & Files 11 - Linux Font Maii E 20 - Share Library 12 - Share Files 7z. III 22 - AppData Files 7z. × 23 - System Setting 7-zo, 24 - App Library CAP C A0 - Linux Key CAP IFDAP1.dll
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash Sign Hash	3E278EA92CBF937370A24E5C219DF 45B7EC170D7260EB4B28AC9A00C37	

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	V5_HelloWorld	Main Executable File
		V5_HelloWorld
App Version	0001	
Company		
Date	20121219	
Finis	ned!	
	ñ	
	Step 2 : Sign Application	Step 1 : Select AP Executable File
		21.205005.20 4
Enc Hash	3E278EA92CBF937370A24E5C219DF	2172592E79A
Sign Hash	45B7EC170D7260EB4B28AC9A00C37	4299991F84D

• Enter file details and press "Step 2: Sign Application" to sign the file. 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 🗨
		Def Select
File Neme		Main Executable File
App Name	V5_HelloWorld	V5_HelloWorld
App Version	0001	
Company		
Date	20121219	
Finis	hed!	
	Step 2 : Sign Application	
	Step 2 : Sign Application	Step 1 : Select AP Executable File
	3E278EA92CBF937370A24E5C219DF	01705005704
Enc Hash	3E270EA32CBF337370A24E5C219DF	2172032E73A
Sign Hash	45B7EC170D7260EB4B28AC9A00C37	4299991F84D
-		

 The output file will be in a set. A "mci" file with one or more "CAP" files. The 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 VEGA3000terminal.

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

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

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

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

4.3.1. Download by User Loader

The User Loader works for VEGA3000.

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

Run User Loader



Select COM port

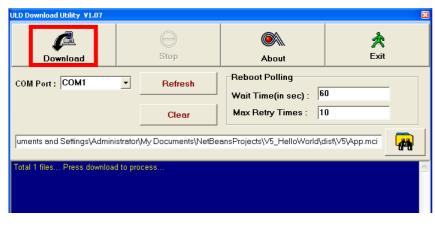
ULD Download Utility V1.07	Θ	e a	ا ج	
Download	Stop	About	Exit	
COM Port COM1	Refresh	Reboot Polling		
,		Wait Time(in sec) : 6	0	
	Clear	Max Retry Times : 1	0	
uments and Settings\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci				
Total 1 files Press download to	process			

Browse and select mci file or mmci file

ULD Download Utility ¥1.07				
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\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci				
Total 1 files Press download	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.



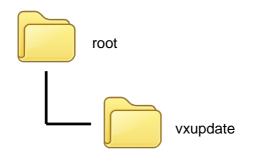
Note: To download using USB cable, terminal must enable CDC mode. Set USB CDC Mode to Y.

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

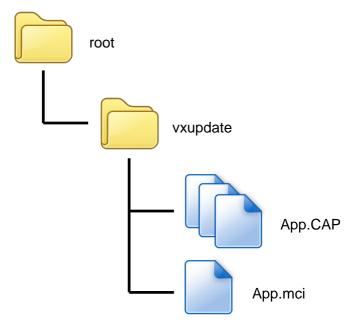
4.3.2. Download by Removable Media

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

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



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



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



 Insert removable media to terminal, and select the removable media type in "Download AP" menu.

Download AP Menu

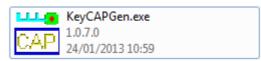
Download EX
1.RS232 or USB
2.USB Disk
3.SD Card
Select DW Source

- Press [2] button to select USB flash drive.
- Press [3] button to select Micro SD card.
- Finally, terminal will process the file "vxupdate" folder.

4.4. Changing ULD User Key

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

Run Secure Key Generator



Insert Key Card and select smart card reader

VEGASCOC Secure Key CAP Generator (RSA) V3.3	
File Uption Help	New Key
	Update PIN Save to Card
	Get Hash Beset
Secure Key	RSA Key for Kenc
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)
	назн

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

		Update PN	Save to Card
		Get Hash	Reset
	Secure Key	RSA Key for Kenc	0
	0001	Public Key Modulus (N)	Length =
		Public Key Exponent (E)	
		Private P	
		HASH	
			Enter Cancel
		RSA Key for Signature	
	Make Key CAP File	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.

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

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

Uption Help	- New Key
Key	Update PIN Save to Caro
File Name	Get Hash Reset
Secure Key	RSA Key for Kenc
0001	Public Key Modulus [N] Length =
2003 822/	Public Key Exponent (E)
	Private Key Exponent (D)
	HASH
	RSA Key for Signature Public Key Modulur (N) Length =
Make Key CAP File	Public Key Modulus (N) Length =
	Public Key Exponent (E) Private Key Exponent (D)
	HASH

urrent Key Setting	le l
Status	
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	IB2BE9B3E576
*	
RSA Key for Signature	
Public Key Modulus (N)	Key Length = 256
*******	***************************************
Public Key Exponent (E)	
Private Key Exponent (D)	
***************************************	***************************************
HASH	
FE0E7B6606EAE386FC29331E5AC41	34584584645
	Close

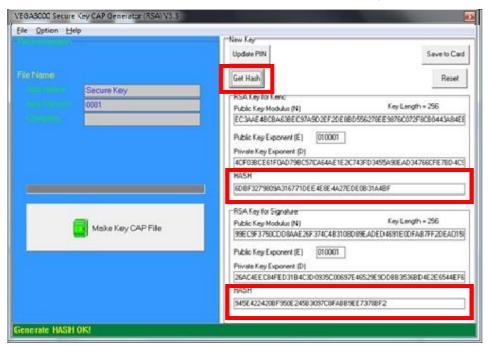
- To generate new user key set
 - Please generate the RSA key by yourself, the length of the RSA key set should be 2048 (bits).
 - Copy RSA key components to RSA Key for Kenc in Secure Key Generator.

e Option Help	New Key
	Update PIN Save to C
	Get Hash
Secure Key	
0001	Public Key Modulus (N) Key Length = 256
A CARGE AND A C	EC3AAE48C8A638EIC97A902EF20E88D556278EE9876C072F8C80443A84
	Public Key Exponent (E) 010001
	Private Key Exponent (D)
	ACF038CE61F0AD798C57CA64AE1E2C743FD3495A30EAD34766CFE78D-
	HASH
	RSA Key for Signature
Make Key CAP File	Public Key Modulus (N) Length =
	Public Key Exponent (E)
	Private Key Exponent (D)
	HASH

Generate second RSA key set for Signature.

ile Option Help	New Key
	Update PIN Save to Card
	Get Hada Reset
Secure Key 0001	RSA Key for Kenc Date Key Models (N) Key Length = 256
Streetsets	Public Key Modulus (N) Key Length = 256 EC3AAE 48CBA638EC97A902EF2DE88D556276EE5875C072F8C80443A84E0
	Public Key Exponent (E) 010001 Private Key Exponent (D) [4CF036CE61F0AD798C57CA544E1E2C743FD3455A30EAD34766CFE76D4C5 HASH
	C RSA Les la Sanates
Make Key CAP File	Public Key Modulus (N) Key Length = 256 [99E C9F 3750CDD 8AAE26F 374C48 3108D 89EADED 4681E0D FAB7FF2DEA015
	Public Key Exponent (E) [010001 Private Key Exponent (D) [26AC4E C04FED3184C300935C00697E46529E30D8835368D4E256544EF6
	HASH

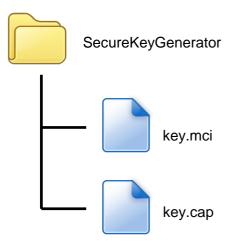
• Click [Get Hash] button to calculate the hash value for key sets.



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

ile Option Help	New Key
Norme Secure Key 0001	Updiate PIN Save to Card Get Hach Reset R
	4CF038CE61F0AD798C57CA64AE1E2C743FD3455A30EAD34766CFE78D4C5 NASM 6D8F3279803A316771DEE4E8E4A27EDE0831A48F
Make Key CAP File	RSA Key for Signature Public Key Modulus (N) Key Length = 256 [99E C3F3750CDDBAAE26F374C4B31080 69EADED4631E00FAB37F2DEA015]
	Public Key Exponent (E) 010001 Private Key Exponent (D) 26AC4EEC84FED3184C300335C00597E46523E50D-8835368D4E2E6544EF6
	HASH 945E 4224208F950E 2458:3097C8FAB89EE73788F2

• 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
File Name	Get Hash	Reset
Secure Key	RSA Key for Kenc	KeyLength = 256
(realized)	Public Key Modulus (N) EC3AAE48008A638EC97A90 2EF20	DE88D556278EE9876C072F8C80443484EE
	Public Key Exponent (E) 01000 Private Key Exponent (D) 40F0380E61F0AD798C57CA64AE	1 1E2C743FD3455A50EAD34766CFE76D4C5
	HASH	
	608F3279809A316771DEE4E8E44	A27EDE0831A48F
Make Key CAP File	PSA Key for Signature Public Key Modulus (N) 1996 CE9759CDD RAAE 295274C48	Key Length = 255 31080/89EADED4631E/00FAB7FF20EA015
	Public Key Exponent (E) 01000 Private Key Exponent (D)	
	26AC4EECB4FED3184C300935C0	10697E46529E90DB835368D4E2E6544EF6
	HASH	
	945E 4224208F950E 245B 3097C8F/	ABB9EE73788F2

5. Font Management

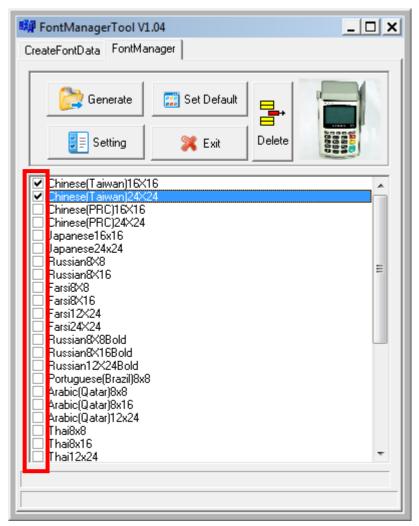
5.1. Loading New Font

Run FontManager.exe

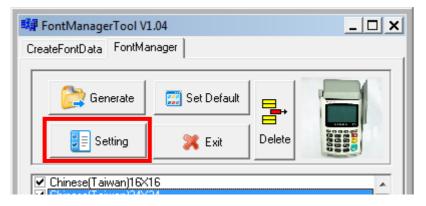


Located at C:\Program Files\Castles\Font Manager

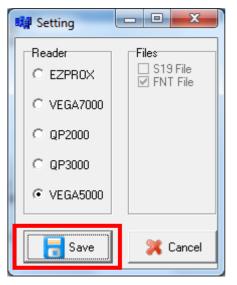
Select font to download



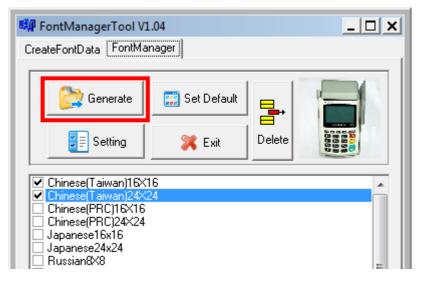
• Press [Setting] button to configure terminal type.



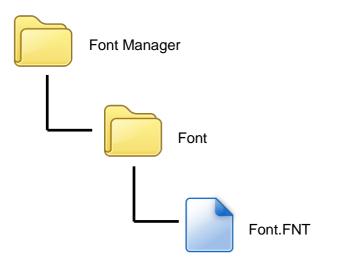
• Select **VEGA5000**, press [Save] button to save and return font manager.



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	enerator 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	3E278EA92CBF937370A24E5C219DF2172592E79A		
Sign Hash	45B7EC170D7260EB4B28AC9A00C3	74299991F84D	

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

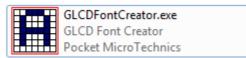
5.2. Custom Font

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

Following steps demonstrate how to create a 12x24 font.

Run GLCD Font Creator



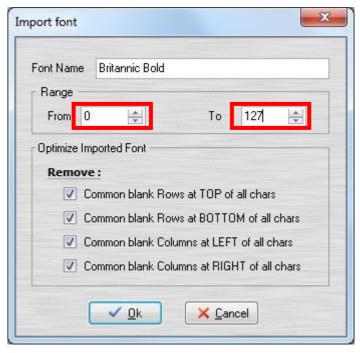
Select [File] ⇒ [New Font] ⇒ [Import An Existing System Font]

File Edit Effects Batch Tools			
New Font	A New Font From Scratch		B
🎽 Open Font	Import An Existing System Font		Prev
Save Font	📲 New HD44780 LCD Custom Characters Set	Set Full Column	
Save Char CtrI+S	Right Click : Clear Pixel Ctrl+Right Click	: Clear Full Column	
Export for MikroElektronika			Tool
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 Scalet MC7 Calibri Californian FB	Font style: Bold Bold A A A A A A A A A A A A A A A A A A A	Size: 11 12 14 16 18 20 22 ▼	OK Cancel
Effects Strik_eout Underline Color: Custom	Sample AaBbYyZ Script:	z	
	Western	•	

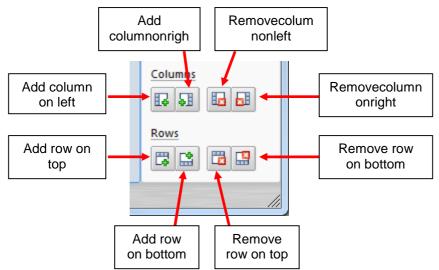
• Set the import range from 0 to 127.

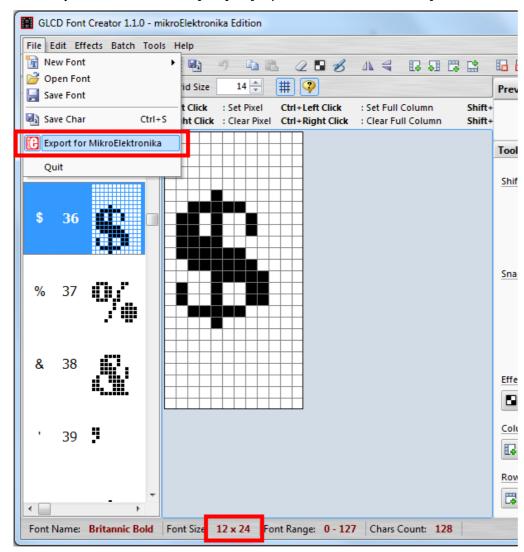


	fe <u>c</u> ts <u>B</u> atch <u>T</u> oo	1				20.00			
£ • 🔂 🗖				288					
ont Char Se		Grid Size	14	# ?			Preview	Blue	•
har Code	GLCD	Left Click Right Click	: Set Pixel : Clear Pixel	Ctrl+Left Click Ctrl+Right Click	: Set Full Co : Clear Full	Shift+ Shift+			
0							Tools		
							Shift / M	ove	
1							_	•	
÷.							4	5 ÷	
							Snap To I	Borders	
2								Ħ	
3								Ŧ	
5							Effects		
							8	4	
4							Columns		1
							12 21		
	-						Rows		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].



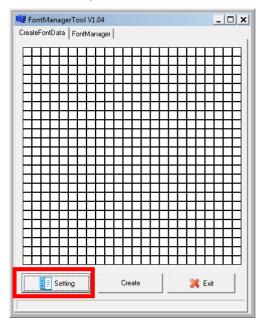
 Remove comment "// Code for char "from offset 0x00 to 0x1F. Remove empty line if found. Then click [Save] button to save to file.

Brit	annic_Bo	ld12x24				F	rom Char	0	*	To Char	127
						ſ	Generate	Code	For Use	With	
							📄 mikr	oC GL	CD Lib	() X	-GLC
							🖲 Font I	neight	> 8bits,	only X-GLC	D lib
Basic	mil 🛄	kroPascal	C	mikroC							
00,	0x00,	0x00,	11	Code	for	cha	r				
00,	0x00,	0x00,	11	Code	for	cha:	r				
00,	0x00,	0x00,	11	Code	for	cha:	r	•	- Rem	love	
00,	0x00,	0x00,	11	Code	for	cha:	r				
00,	0x00,	0x00,	11	Code	for	cha	r				
		201						_	- Re	emove	
				10000000000		C	72.02				
		1000 K 1000 K 1000 K						- ←	- Rem	love	
00,	0x00,	0x00,	11	Code	for	cha:	r		_		
00	0x00.	0x00	11	Code	for	cha			R	emove	
~~	000	000	1.	~ .	-	,					
	Basic 00, 00, 00, 00, 00, 00, 00,	Basic II mil 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00, 00, 0x00,	00, 0x00, 0x00, 00, 0x00, 0x00, 00, 0x00, 0x00, 00, 0x00, 0x00, 00, 0x00, 0x00, 00, 0x00, 0x00, 00, 0x00, 0x00,	Basic ImikroPascal ImikroPascal 00, 0x00, 0x0	Basic mikroPascal mikroC 00, 0x00, 0x00	Basic ImikroPascal ImikroC 00, 0x00,	Basic MikroPascal MikroC D0, 0x00, 0x00, 0x00, // Code for chai 00, 0x00, 0x00, // Code for chai 00, 0x00, 0x00, // Code for chai	Generate mikro Basic ■ mikroPascal ■ mikroC 00, 0x00, 0x00, // Code for char 00, 0x00, 0x00, // Code for char	Generate Code → mikroC GL → Font height Basic → mikroPascal → mikroC 00, 0x00, 0x00, // Code for char 00, 0x00, 0x00, // Code for char	Generate Code For Use ■mikroC GLCD Lib Font height > 8bits, Basic ■ mikroPascal ■ mikroC 00, 0x00, 0x00, 00, 0x00, 0x00	Generate Code For Use With ■ mikroC GLO Lib ● X Pont height > 8bits, only X-GLC Basic ■ mikroPascal ■ mikroC 00, 0x00, 0x00, // Code for char 00, 0x00, 0x00, // Code for char

• Run Font Manager Tool.



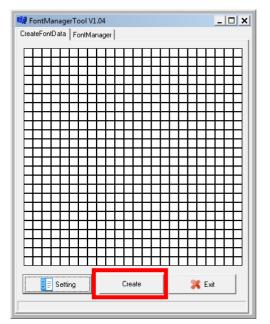
Click [Setting] button



• 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 created font, and press [Generate] button to export to FNT file.

🗱 FontManagerTool VI	1.04		_ 🗆 🗙
CreateFontData FontMa	nager		
Cenerate	📰 Set Default		
Setting	💢 Exit	Delete	
Portuguese(Brazil)8x8 Arabic(Qatar)8x8 Arabic(Qatar)8x16 Arabic(Qatar)12x24 Thai8x16 Thai8x16 Czech8x16 Czech8x16 Czech12x24 Spanish8x8 Spanish8x8 Spanish12x24 Chinese(Taiwan)Plus Turkish8x16 Turkish8x16 Turkish8x16 Chinese(PRC)15x16(Chinese(PRC)12x24 Chinese(PRC)12x24	16×16 24×24 minisun)		E

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 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	9572BC621C1D54060856D00BCC20	7000D3320077
Sign Hash	A927768EA7DD7B9E7E3F395C1072	6B6F43B35C5A

- Download the font CAP file to terminal.
- In terminal application, add following code to display message using the newly created font.

```
CTOS_LanguageConfig(0xA000,d_FONT_12x24,0,d_FALSE);
CTOS_LanguageLCDSelectASCII(0xA000);
CTOS_LCDTPrintXY(1, 1, "ABCDEFGH");
```

Or print message using the newly created font.

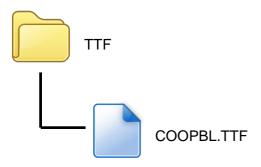
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

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

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

• Copy the TTF file needed to an empty folder.



Use CAP Generator to convert the TTF file to CAP.
 Set type to [11 – Linux Font], press [Step 1] button select the TTF file.
 Then press [Step 2] to generate CAP file.

the himmedice		Type 11 - Linux Font
ile Nome		Main Executable File
App Name	Linux Font	COOPBLITTE
App Version	0001	
Company		
Date	20130117	
Finist	Step 2 : Sign Application	

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. 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.

Radiation Exposure Statement:

This device meets the government's requirements for exposure to radio waves.

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

The exposure standard for wireless device employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. ^{*}Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands.

6.2. Safety Warning for External Power Source

To reduce potential safety issues, only the AC adapter provided with the product, a replacement AC adapter provided by agency, or an AC adapter purchased as an accessory from agency should be used with the product.

~ END ~