

CASTLES TECHNOLOGY

UPT1000

Book 2

User Manual

Confidential

Version 1.1 Jan. 2017

Castles Technology Co., Ltd.

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

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	Author
1.0	Dec 19, 2016	Initial creation.	Jeff
1.1	Jan 11, 2017	Add "7. Appinex" and "7.1 Cautions".	Jeff

Contents

1.	Introd	duction		6	
2.	Hard	ware Se	etup	7	
	2.1.	Parts o	of the UPT1000	7	
	2.2.	Comm	unication Support	8	
3.	Basic	: Opera	tion	9	
	3.1.	Progra	ım Manager	9	
	3.2.	Downle	oad AP	10	
	3.3.	Systen	n Info	11	
	3.4.	Memor	ry Status	12	
	3.5.	Systen	n Settings	13	
	3.6.	Test U	tility	16	
	3.7.	Factor	y Reset	18	
	3.8.	Power	Off	19	
	3.9.	FK PW	/D Change	20	
	3.10.	Share	Object Management	21	
	3.11.	Embeo	ded TMS	22	
	3.12.	Font N	Ing	23	
	3.13. Debug Tools				
	3.14.	14. ULD Key Hash			
	3.15.	HW De	etect	26	
	3.16.	Blueto	oth Setup	27	
	3.17.	Plug-ir	ו Mng	28	
	3.18.	Key In	jection	29	
4.	Secu	re File I	Loading	30	
	4.1.	ULD K	ey System	30	
		4.1.1.	ULD Manufacturer Key	30	
		4.1.2.	ULD User Key	32	
		4.1.3.	Key Change	32	
	4.2.	File Sig	gning	33	
		4.2.1.	Signing Kernel Module	33	
		4.2.2.	Signing User Files	35	
	4.3.	File Lo	pading	39	
		4.3.1.	Download by User Loader	39	

		4.3.2. Download by Removable Media	42
	4.4.	Changing ULD User Key	44
5.	Font	Management	51
	5.1.	Loading New Font	51
	5.2.	Custom Font	54
	5.3.	Using TrueType Font (TTF)	62
6.	Tech	nical Notes	64
	6.1.	Serial Cable PIN Assignment	64
7.	Appe	ndix	65
	7.1.	Cautions	65

1. Introduction

This document provides a guideline on operating and configuring Castles UPT1000 .

The scope of this document includes setting up the UPT1000, basic operation, application life cycle, and some advance features.

2. Hardware Setup

2.1. Parts of the UPT1000

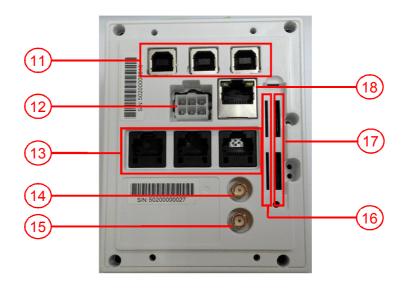
<u>Front</u>



UPT1000

- 1. LCD Display (Color TFT)
- 2. Keypad
- 3. Smart Card Reader
- 4. Enter Key
- 5. Return Key (RFU)
- 6. Clear Key

- 7. Cancel Key
- 8. Magnetic Stripe Reader
- 9. Contactless Card Landing Zone
- 10. LED indicator



UPT1000

- 11. USB port 1~3
- 12. MDB (power connector)
- 13. RS232 port 1~3
- 14. BT antenna socket
- 15. GPRS antenna socket
- 16. GSM SIM Card Slots 1~2
- 17. SAM Card Slots 1~4
- 18. LAN port

2.2. Communication Support

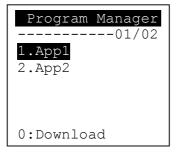
- 1. Ethernet
- 2. BT
- 3. UMTS 850/1900
- 4. GPRG 850/1900

3. Basic Operation

3.1. Program Manager

Once the power is on in normal status, UPT1000 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 UPT1000 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 [↓] as the up and down buttonto 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

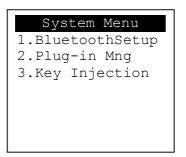
Press [↓] button to page 2.

Page 2

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

- Press [↑] button to page1.
- Press [\downarrow] button to page3.

Page 3



■ Press [↑] button to page2.

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. (Not support)

3.3. System Info

View kernel module firmware information.

System Menu

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

Press [2] button to enter System Info menu.

System Info Menu

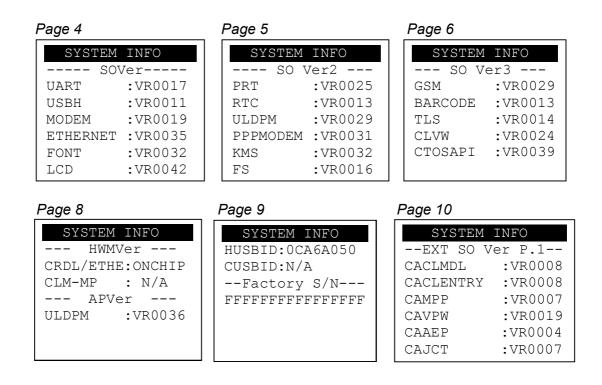
Page 1

Page 2

Page 3

SYSTE	M INFO	S	YSTEM INFO
KOV	er		KOVer2
SECURIT	Y :VR0025	CL	:VR0018
KMS	:VR0027	SC	:VR0011
DRV	:VR0046		
USB	:N/A		
CIF	:VR0025		
SAM	:VR0034		
	KOV SECURIT KMS DRV USB CIF	DRV :VR0046 USB :N/A CIF :VR0025	KOVer SECURITY :VR0025 CL KMS :VR0027 SC DRV :VR0046 USB :N/A CIF :VR0025

Press [\downarrow] button to next page.



3.4. Memory Status

View flash memory and RAM information.

System Menu

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

Press [3] button to enter Memory Status menu.

Memory Status Menu

MEMORY	STATUS
FLASH	Memory
Total:	130688KB
Used :	44644KB
SDRAM	Memory
Total:	65408KB
Used :	32384KB

3.5. System Settings

View or change system settings.

Setting	Descriptions
Key Sound	Enable (Y) or disable (N) the beep sound when
	pressing any key.
Exec DFLT AP	Enable (Y) or disable (N) execution of 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" 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. (Not support)
List SHR Lib	Enable (Y) or disable (N) to list all shared libraries
	in Program Manager.
Key MNG Mode	<tbc></tbc>
BATThreshld	Battery charging threshold value. (Not support)
Null Cradle	Enable (Y) if base is Type Acradle. (Not support)
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 boot up.
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 keyfunction, power off (Y) or reboot(N)
GDB Mode	Enable (Y) or disable (N) GDB (GNU Debugger)
	mode. (Needs to download GDB plugin FW first.)
GDB Timeout	Set GDB connection timeout.
GDB Channel	Set GDB connection channel.
ETHER IP/PORT	GDB Ethernet connection setting.
RTC Time Zone	Set Time Zone of RTC (Real Time Clock).

NTP Enable	Enable (Y) or disable (N) NTP (Network Time
	Protocol) function.
NTP Update Freq	Frequency of Network Time Protocol updating.
Halt Timeout	Set timeout of AP to get back to Program Manager
	whenever AP is in halt state.
PWM Auto	Enable (Y) or disable (N) power saving mode.
PWM Mode	Select (STB) standby mode or (SLP) sleep mode
	for power saving mode.
PWM Time	Set time period to make machine enter power
	saving mode from idle state.
BAT PROTECT MODE	Set battery protect mode. (Not support)

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

Page 3

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

Page 2

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: N	ez	xt

Page	4

SYS SET	TINGS
GDB Mode	: GMT
GDB Timeout	: N
GDB Channel	: X
ETHER IP/POF	RΤ
1: Prev	2: Next



GS
: GMT
: N
: X
Next

SYS SETTINGS	5	
Halt Timeout	:	0
PWM Auto	:	Х
PWM Mode	:	Х
PWM Time	:	Х
BAT PROTECT MODE	:	Х
1: Prev Page		

- Press [\uparrow] or [\downarrow]button to select setting.
- Press [OK] button to change the setting value.
- Press [<] 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 hardware components diagnosis.

System Menu

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

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

Test Utility Menu

Page 1

Main Menu 9	123
1.LCD	
2.Keyboard	
3.Flash	
4.Smart Card	
5.Backlight	
6.MSR	
->	1/3

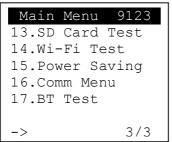
- Press [1] and [OK] to diagnose LCD.
- Press [2] and [OK] to diagnose keyboard.
- Press [3] and [OK] to diagnose flash memory.
- Press [4] and [OK] to diagnose smart card module.
- Press [5] and [OK] to diagnose backlight.
- Press [6] and [OK] to diagnose magnetic stripe card reader.
- Press [\downarrow]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

Page 2

Main Menu 9123	1
7.LED	
8.RTC	
9.Printer	
5 1 2 2 1 1 0 0 2	
10.Font	
11.CL Transparent	
12.CL Card Test	
-> 2/3	

- Press [7] and [OK] to diagnose LED.
- Press [8] and [OK] to diagnose RTC.
- Press [9] and [OK] to check Printer.
- Press [10] and [OK] to check FONT file in UPT1000.
- Press [11] and [OK] to check CL transparent.
- Press [12] and [OK] to test Cantactless Card.
- Press [↑] button to page 1.
- Press [↓] button to page 3.

Page 3



- Press [13] and [OK] to execute SD Card Test. (Not support)
- Press [14] and [OK] to testfunctionality ofWiFi.
- Press [15] and [OK] to test functionality of power saving.
- Press [16] and [OK] to test functionality of multiple communication ways.
- Press [17] and [OK] to testfunctionality of Bluetooth.
- Press [↑] button to page2.

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.

Fa	cRe	est Password
OK	to	reset?

Press [OK].



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

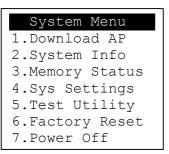


• Start erasing, and then go back to Program Manager.

3.8. Power Off

Power off the machine.

System Menu



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

3.9. FK PWD Change

Change the keyin password.

System Menu (Page 2)

Press [1] button to enter Password Manager Menu.

FunKe	ey Password
Enter ****	Password:

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

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

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

User must have to change the Default key to user own key at the first time. The Default Key Value in Password Manager is as below:

Function Key	0000
PMEnter Key	0000
Factory Key	8418

3.10. Share Object Management

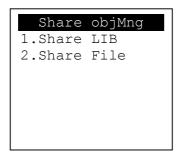
View share object in machine .

System Menu (Page 2)

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

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

Share Object Management Menu



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

3.11. Embedded TMS

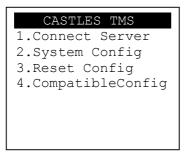
TMS (Terminal Managerment System) setting menu.

System Menu (Page 2)

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

Press [3] button to enter TMS setting menu.

CASTLES TMS



- Press [1] button to connect server.
- Press [2] button to enter system config menu.
- Press [3] button to reset config.
- Press [4] button to set compatible config.

3.12. Font Mng

View Font Management.

System Menu (Page 2)

• 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

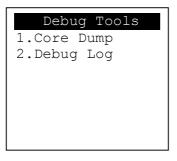
Get core dump or debug log.

System Menu (Page 2)

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

• Press [5] button to enter Debug Tools menu.

Debug Tools



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

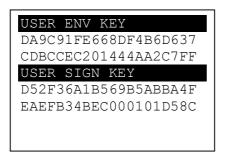
3.14. ULD Key Hash

View ULD user key hash value.

System Menu (Page 2)

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

• Press [6] button to view hash value.



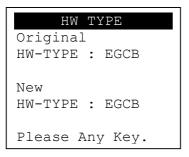
3.15. HW Detect

Run hardware detection.

System Menu (Page 2)

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

• Press [7] button to run HW detection.

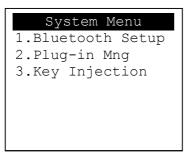


Press any key to reboot system.

3.16. Bluetooth Setup

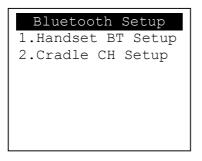
Setup Bluetooth config.

System Menu (Page 2)



• Press [1] button to enter Bluetooth setting menu.

Bluetooth Setup

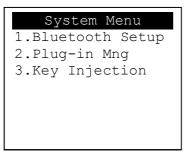


- Press [1] button to enter Handset BT Setup menu.
- Press [2] button to enter Cradle CH Setup menu.

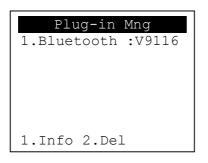
3.17. Plug-in Mng

View Plug-in Management.

System Menu (Page 2)



Press [2] button to view Plug-in Management.

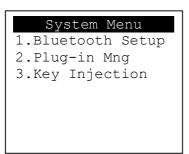


- Press [↑] or [↓] button to select item.
- Press [1] button to get item information.
- Press [2] button to delete item.

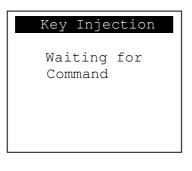
3.18. Key Injection

Key Injection function. (Factory use only.)

System Menu (Page 3)



• Press [3] button to view Key Injection.



4. Secure File Loading

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

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

4.1. ULD Key System

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

ULD Manufacturer Key Set

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

<u>ULD User Key Set</u>

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

For UPT1000, the RSA key length is 2048bits.

4.1.1. ULD Manufacturer Key

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

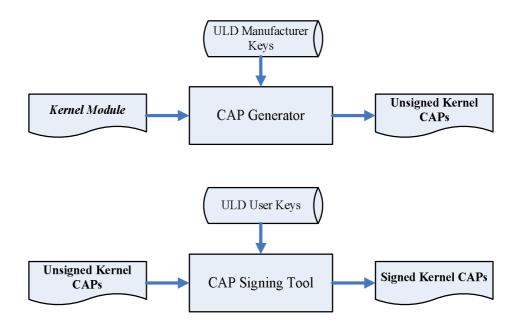
The ULD Manufacturer keys are managed and maintained by the manufacturer. The manufacturer uses these keys to generate kernel CAP files for updating the system. However, the system is not permitted to be updated with these kernel CAP files directly generated by the manufacturer. This is because only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

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

Notes:

1. The kernel modules are encrypted by a random-generated 3DES key, which is retrieved from the Key Encryption Block of the CAP by ULD Manufacturer Key Encryption Key, not directly encrypted by ULD RSA Key.

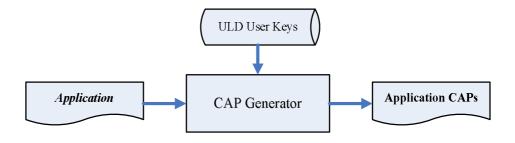
2. The "sign" action via ULD User Keys actually is done by" the second encryption". "The second encryption" is done by using the randomgenerated 3DES key, which is encrypted by ULD User Key Encryption Key, to perform Triple DES encryption again on the cipher data segment of the kernel CAP files. This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



4.1.2. ULD User Key

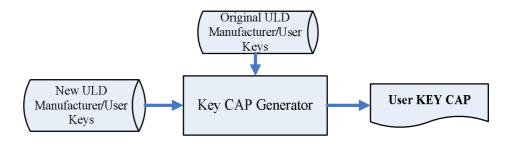
ULD User Key are used to encrypt and sign the user/shared applications. In addition, they are as goalkeepers to prevent the system updating without user permission. This is done by the kernel CAPs which are encrypted and signed by the manufacturer having to perform the "signed' action via ULD User Keys.

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 UPT1000.

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

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

Run CAP Signing Tool



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	1		

		Enter	Cancel
	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 Information	
abc	
HEX	CAP
Key Ready	
Select M	
Jelectivi	
	Reset
	110001

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

4.2.2. Signing User Files

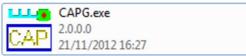
Following files are required to sign before load to UPT1000. This is to ensure the application data and codes confidential and integrity. The output file will be "CAP" file which format is defined by Castles.

- 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\UPT1000\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 C 0001 Choose Reader 0001 CASTLES EZ100PU 0 20121219 0	Header Type 10 - Linux AP & Files Def Select Main Executable File 72.dll 72.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
	The state of the state of the	Main Executable File
App Name	Test Application 1	7z.dll 7z.exe
App Version	0001	72.exe
Company	PIN : xxx	
Date		
	Enter	Cancel
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash		
Enc Hash		
Sign Hash		

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

<u>F</u> ile <u>H</u> elp		
File Name App Name App Version Company Date	Test Application 1 0001 20121219	Header Type 10 - Linux AP & Files 11 - Linux AP & Files 11 - Linux Font 420 - Share Library 12 - Share Files 72. II 22 - AppData Files 72. X 23 - System Setting 72. X 24 - App Library CA - Linux Key CAP GP AD-
	Step 2 : Sign Application	Step 1 : Select AP Executable File
Enc Hash Sign Hash	3E278EA92CBF937370A24E5C219DF 45B7EC170D7260EB4B28AC9A00C37	

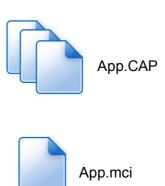
Press "Step 1: Select AP Executable File" to select file to sign. This is valid for all the files to sign.

<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
App Version	0001	V5_HelloWorld
Company	0001	
Date	00101010	
Dale	20121219	
Finish	bodi	
1 11 1151	iedi	
	Step 2 : Sign Application	
	Step 2. Sign Application	Step 1 : Select AP Executable File
		·
Enc Hash	3E278EA92CBF937370A24E5C219DF2172592E79A	
a:		
Sign Hash	45B7EC170D7260EB4B28AC9A00C374299991F84D	

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

<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	V5_HelloWorld	V5_HelloWorld
App Version	0001	
Company		
Date	20121219	
Finish	nedl	
	Step 2 : Sign Application	
	Step 2 : Sign Application	Step 1 : Select AP Executable File
		1 205005 20 4
Enc Hash	3E278EA92CBF937370A24E5C219DF2	172592E79A
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 UPT1000.

- 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 UPT1000.

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

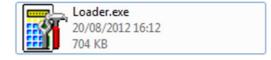
Castles TMS (CTMS or CASTLES Terminal Management System) is provided by Castles Technology. It uses to perform remote download via Ethernet, GPRS/UMTS or modem.

4.3.1. Download by User Loader

The User Loader works for UPT1000.

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

Run User Loader



Select COM port

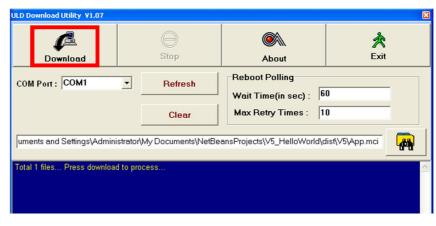
ULD Download Utility V1.07) Stop	About	Exit
COM Port	Refresh	Reboot Polling Wait Time(in sec) : 6	0
	Clear	Max Retry Times : 1	
1		ansProjects\V5_HelloWorld\c	
Total 1 files Press download	to process		

Browse and select mci file or mmci file

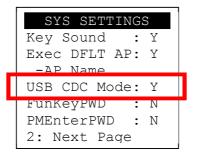
ULD Download Utility ¥1.07			X
Download	Stop	About	Å Exit
COM Port : COM1	Refresh	Reboot Polling Wait Time(in sec) : 6	
Clear Max Retry Times : 10 uments and Settings\Administrator\My Documents\NetBeansProjects\V5_HelloWorld\dist\V5\App.mci Image: Clear			
Total 1 files Press download	d to process		

- Setup UPT1000 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.



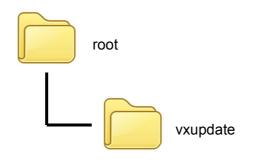
Note: To download using USB cable, UPT1000 must enable CDC mode. Set USB CDC Mode to Y.



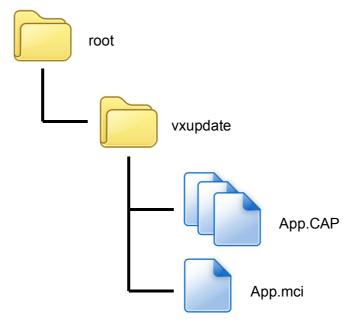
4.3.2. Download by Removable Media

The file download process can be achieved without PC by using removable media, USB flash drive. We recommend don't put unwantedfile 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 UPT1000, and select the removable media type in "Download AP" menu.

Download AP Menu

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

- Press [2] button to select USB flash drive.
- Press [3] button to select MicroSD card. (Not support)
- Finally, UPT1000 will process the file in "vxupdate" folder.

4.4. Changing ULD User Key

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

Run Secure Key Generator



Insert Key Card and select smart card reader

tile Uption He	Np		1999 (1999) (199
te bir mokere		New Key	
		Update PIN	Save to Card
		Get Hash	Reset
	Secure Key	RSA Key for Kenc	
	0001	Public Key Modulus (N)	Length =
		Public Key Exponent (E)	Reader ES EZ100PU 0
		Private Key Exponent (D	CS E2100P0 0
		HASH	
-		RSA Key for Signature	
1.1.1	NUL Y ODDE	Public Key Modulus (N)	Length =
	Make Key CAP File		
		Public Key Exponent (E)	
		Private Key Exponent (D)	
		HASH	

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

		New Key Update PIN	Save to Card
		Oppose Pilv	Save to Caro
		Get Hash	Reset
	Secure Key	-RSA Key for Kenc	
	0001	Public Key Modulus (N) Length =	
		Public Key Exponent (E)	
		Private P	
		md	_
		HASH	Cancel
		RSA Key for Signature	
1	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.

VEGA3000 Secure Key CAP Generator (RSA) V3.3	and the second se	
Ele Option Help The Instruction	Vew Key Update PIN	Save to Card
File Name App Name Secure Key App Version 0001	Get Hash RSA Key for Kenc Public Key Modulus (N) Length =	Reset
	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 :	I		
Conform PIN :			
	Reset	Enter	Cancel

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

VEGASOOD Service CercCAP Generator (RSA) V3.3	
The Option Help	
Кеу	Update PIN Save to Card
File Name App Filewik Secure Key	Get Hash Reset
Applykosen 0001 Campere	RSA Key for Kenc 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

Current Key Setting	
Status	
Load Key OK!	
RSA Key for Kenc	
Public Key Modulus (N)	Key Length = 256
***************************************	***************************************
Public Key Exponent (E)	-
Private Key Exponent (D)	

HASH	
277BF11E6827FF2A263DEDE6DEC8	34B2BE9B3E576
RSA Key for Signature	
Public Key Modulus (N)	Key Length = 256
***************************************	***************************************
Public Key Exponent (E)	-
Private Key Exponent (D)	*****
HASH	
FE0E7B6606EAE386FC29331E5AC4	13AF8458ACA5
	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.

	New Key	
	Update PIN	Save to Car
	Get Hash	Reset
Secure Key	BSA Key for Kenc	
0001	Public Key Modulus (N)	Key Length = 256
	EC:3AAE 48C8A638EIC97A902EF2DE	08D556278EE9076C072F9C80443A84E
	Public Key Exponent (E) 010001]
	Private Key Exponent (D)	-
		2C743FD 3455A90EAD 34766CFE 78D-4C
	HASH	
	RSA Key for Signature	Least
Make Key CAP File	Public Key Modulus (N)	Length =
	Public Key Exponent (E)	1
		J
	Private Key Exponent (D)	
	HASH	

• Generate second RSA key set for Signature.

ile Option Help	New Key
	Update PIN Save to C
Nome App124min Secure Key	Get Hash
App Yession 0001 Company	Public Key Modulus (N) Key Length = 256 EC3AAE 48028.4638EC97A9D2EF2DE88D556278EE9876C072F8C80443A8 Public Key Exponent (E) 010001 Private Key Exponent (D) 400080261F0AD7980C57CA64AE1E2C743FD3455A30EAD34766CFE78D HASH
Make Key CAP File	
	Private Key Exponent (D) 26A/C4EE084FED3184C3D0335C00637E46529E5DD8835368D4E2E6544 HASH

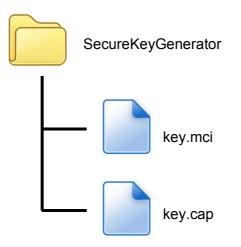
Click [Get Hash] button to calculate the hash value for key sets. •

Eile Option Help		
File Name App Name App Name App Verson Company	New Key Update PIN Get Hash RSA Key Tor Kenc Public Key Modulus (N) EC304E 48C8A638EC974502EF20 Public Key Exponent (E) [010001 Private Key Exponent (D)	Save to Card Reset Key Length = 256 E08D556276EE5976C072F9CB0443A64E8
	4CF038CE61F0AD798C57EA64AE1 HASH 6D8F3279809A316771DEE4E8E4A	E2C743FD3495A30EAD34766CFE78D4CS 27EDE08/31A4BF
Make Key CAP	File Public Key Modulus (N) 99EC9F3750CD08AAE26F374C483 Public Key Exponent (E) 010001 Private Key Exponent (D)	Key Length = 256 1108D89EADED4691E0DFA87FF2DEA015
Generate HASH OKI	945E4224208F950E24583097C8FA	88%E73788F2

- 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.

le Option Help	P		
		Vew Key Updale PIN S.	ave to C-ar
	Secure Key 0001	Get Hash -RSA Key-for Kenc Public Key Modulus (N) Key Length = 22 EC:SAAE 48C58A638EC597A90.2EF20E58D756278EE5987600729028	
		Public Key Exponent. (E) 010001 Private Key Exponent. (D) 4CF038CE61F0AD738C57CA64AE1E2C743F03455A30EAD34766C NASH 6DIBF3273803A316771DEE4E8E4A27EDE0831A48F	FE 780-40
l	Make Key CAP File	RSA Key for Signature Public Key Modulus (N) Key Length = 2 SSECSF37500DDBAAE26F374C483100D89EADED4631E0DFA87F1 Public Key Exponent. (E) 010001	
		Private K-ey Exponent (D) [26AC4EEC84FED31B4C3D0335C00697E46523E30D8B35368D4E2 HASH [945E4224208F950E2458:3097C8FABB9EE73788F2	£6544EF

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



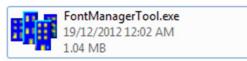
 To update the newly generated key set to Key Card, press [Save to Card] button to write the key set to Key Card.

Eile Option Help		- New Key	
		Update PIN	Save to Card
File Name App Name App Version Company	Secure Key 0001	Public Key Exponent (E) 010001 Private Key Exponent (D)	Reset Key Length = 256 DE68D556278EE5876C072F8C80443484EE 1 1 1E2C743FD3455A30EAD34766CFE78D4CS
		HASH 608F32798034316771DEE4E8E44	
	Make Key CAP File	PISA Key for Signature Public Key Modulus (N) 995EC5F3750CDD BAAE26F374C483	Key Length = 256 31080/89EA.DED-4691E/00FAB7FF2DEA015]
		Public Key Exponent (E) 010001 Private Key Exponent (D) 26AC4EEC84FED3184C3D0935C00 HASH 545E4224208F950E24583097C8FA	

5. Font Management

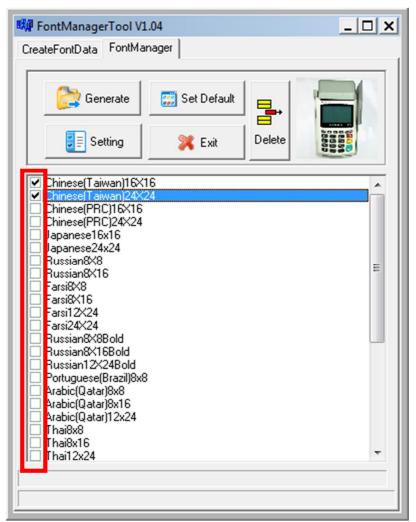
5.1. Loading New Font

Run FontManager.exe

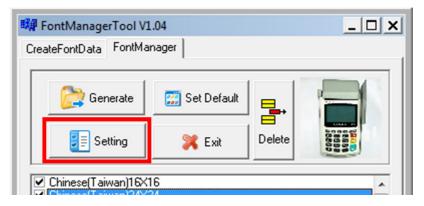


Located at C:\Program Files\Castles\Font Manager

Select font to download



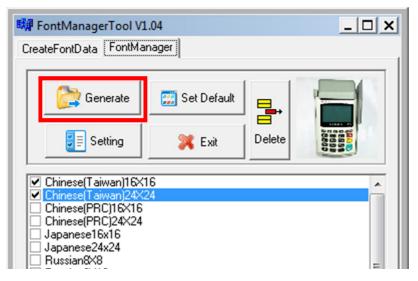
• Press [Setting] button to configure the type.



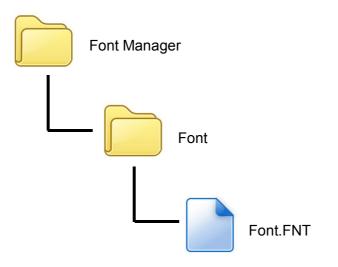
Select VEGA5000, press [Save] button to save and return font manager.



Press [Generate] to create the font file.



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



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

Vega5000 CAP 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	3E278EA92CBF937370A24E5C219	3DF2172592E79A
Sign Hash	45B7EC170D7260EB4B28AC9A00	C374299991F84D

• Lastly, download the signed file (CAP file) to UPT1000 using Loader.

5.2. Custom Font

User may create font they preferred for displaying or printing on UPT1000.

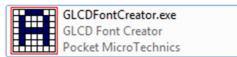
There are two zone defined:

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

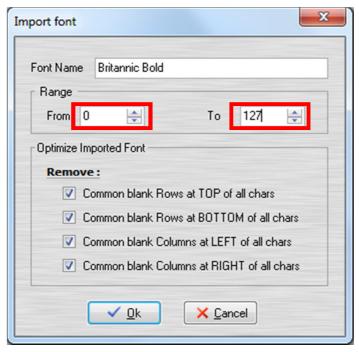


GLCD Font Creator 1.1.0 - mik	roElektronika Edition	
File Edit Effects Batch Tools	Help	
🙀 New Font	New Font From Scratch	6
💕 Open Font	Import An Existing System Font	Previ
Save Font	Rew HD44780 LCD Custom Characters Set	
Save Char Ctrl+S	Right Click : Clear Pixel Ctrl+Right Click : Clear Full Column	
Export for MikroElektronika		Tools
Quit		10013
		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	Font st <u>v</u> le: Bold	Size:
Britannic Broadway Brush Script M7 Calibri Californian FB	Bold A Bold Oblique	11 ^ Cancel 12 14 E 16 E 18 20 22 ~
Effects Strikeout Underline Color:	Sample AaBbYyZ	lz
Custom	Script: Western	•

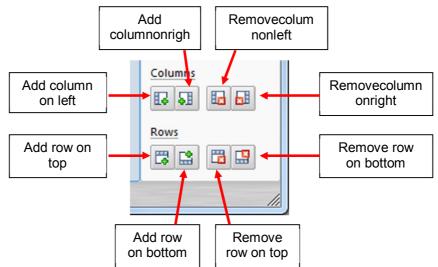
• Set the import range from 0 to 127.

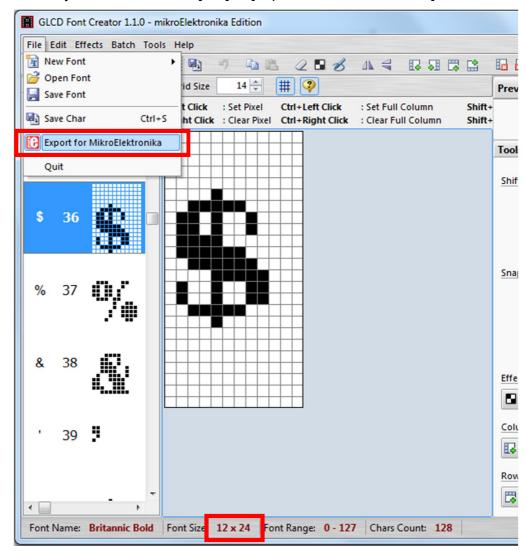


	❷ ❷ ↗ ▙ 2 ₽ ♂ A < ₽ ₽ ₽ ₽	-
ont Char Set	Grid Size 14 💭 🇰 🖓	Preview Blue -
	Right Click : Clear Pixel Ctrl+Right Click : Clear Full Column Shift+	
0		Tools
		Shift / Move
1		4 C 4
		4
		Snap To Borders
2		
		•
		۲
3		544 - 4-
		Effects
4		Columns
		Rows

• 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].



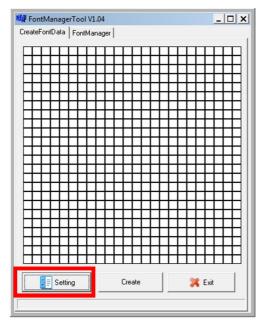
 Remove comment "// Code for char "from offset 0x00 to 0x1F. Remove empty line if found. Then click [Save] button to save to file.

Font Nam	e Brit	annic_Bo	ld12x24				F	rom Char	0	-	To Char	12
							[Generate	Code F	or Use \	With	
								-) only X-GLO	
🚺 mikr	oBasic	🚺 mi	kroPascal	C	mikroC							
0	x00,	0x00,	0x00,	11	Code	for	cha	r				
0	x00,	0x00,	0x00,	11	Code	for	cha	r				
			0x00,	11	Code	for	cha	r	←	Rem	ove	
			0x00,	11	Code	for	cha	r				
0	x00,	0x00,	0x00,	11	Code	for	cha	r				
		-	0.00			_			_	– Re	emove	
			0x00,					-		_		
			0x00,		Code				←	Rem	ove	
	x00,	0x00,	0x00,	11	Code	IOT	cna	r		D		
0	x00.	0x00.	0x00,	11	Code	for	cha	r		-R	emove	
-		000			~ .	-		-				
•												

• Run Font Manager Tool.



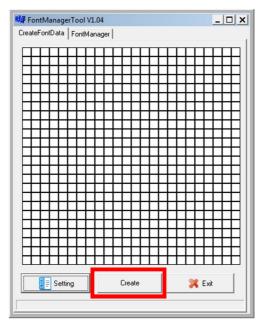
Click [Setting] button



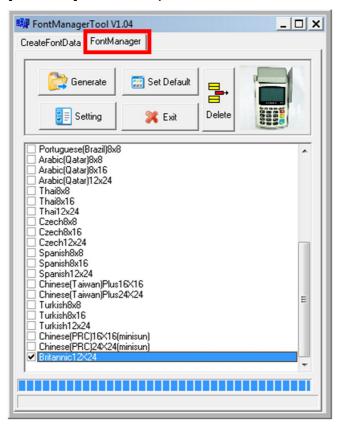
• Enter the file name, font id, and select the size.

🗱 DataSetting 📃 🗖 🗙
FileName:
Britannic
ID:(HEX)
A000
Style:
thin 💌
Size:
<u>12 * 24</u> ▼
Version:(HEX)
0001
OK

 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.



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 CapG	en Evaluation Version v2.2	
<u>F</u> ile <u>H</u> elp		
-File Information-		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		
Sign nash	A927768EA7DD7B9E7E3F395C1072	2000004383505A

- Download the font CAP file to UPT1000.
- In the application, add following code to display message using the newly created font.

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

Or print message using the newly created font.

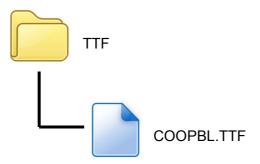
```
CTOS_LanguagePrinterSelectASCII(0xA000);
CTOS_PrinterPutString("ABCDEFGH");
```

5.3. Using TrueType Font (TTF)

TrueType Font (TTF) is supported in UPT1000. You can download the TrueType font to UPT1000 for displaying or printing.

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

• Copy the TTF file needed to an empty folder.



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

VEGA3000 ULD CAP Generator (Evaluation) 3.2		
<u>File</u> <u>H</u> elp		
-File Information-		Type 11 - Linux Font
File Name		Main Executable File
App Name	Linux Font	COOPBL TTF
App Version	0001	COOP DC. TH
Company		
Date	20130117	
Finished!		Step 1 : Select AP Executable Filg

Download the font CAP file to UPT1000.

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

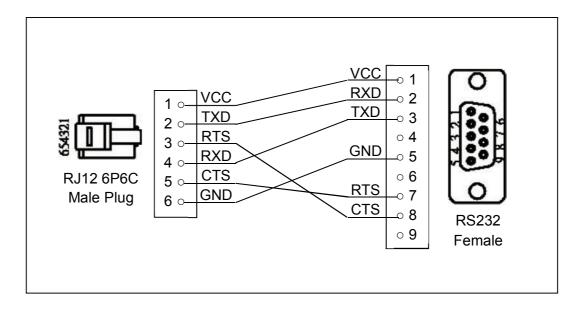
```
CTOS_LCDTTFSelect("COOPBL.TTF", 0);
CTOS_LCDFontSelectMode(d_FONT_TTF_MODE);
CTOS_LCDTSelectFontSize(0x203C); // 32x60
CTOS_LCDTClearDisplay();
CTOS_LCDTPrintXY(1, 1, "Hello World");
```

Or print message using the newly added font.

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

6. Technical Notes

6.1. Serial Cable PIN Assignment



7. Appendix

7.1. Cautions

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 \geq 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 \geq antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

~ END ~