



beyond  
payment

## iWL220/250

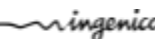




# Contents

---

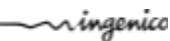
<b>1. Document</b>	<b>11</b>
1.1. Document change history	11
1.2. Document sign off	11
<b>2. Equipment</b>	<b>13</b>
2.1. Introduction	13
2.2. General hardware description	13
2.2.1. Terminal's description	13
2.2.1.1. Dimensions & weight	13
2.2.1.1.1. With 25 mm paper roll	13
2.2.1.1.2. With 40 mm paper roll	14
2.2.1.2. Functional overview	14
2.2.2. Base description	16
2.3. Technical hardware characteristics	16
2.3.1. Processor	16
2.3.2. Memory capacity	17
2.3.3. Booster	17
2.3.4. Data security	17
2.3.4.1. Hardware design	17
2.3.4.2. Software design	18
2.3.4.3. Product activation	18
2.3.5. The isolation mechanism by electronic locking system	18
2.3.5.1. Isolation	18
2.3.5.2. MMU features	19
2.3.5.3. Inviolable memory protection	19
2.3.5.4. OS is inviolable and protected	19
2.3.5.5. The OS ensures the inter-violability of software application	19
2.3.6. Card readers	19
2.3.6.1. Main smart card reader	19
2.3.6.2. 2 <sup>nd</sup> card reader	20



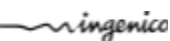
2.3.6.3. Magnetic stripe reader	21
2.3.6.4. Contactless reader	21
2.3.6.4.1. Introduction to Contactless	22
2.3.6.4.2. What is Contactless card payment?	23
2.3.6.4.3. The advantages of Contactless technology	23
2.3.6.5. SAM readers	23
2.3.7. Keypad , navigation pad	24
2.3.8. Display	25
2.3.9. Printer	25
2.3.10. Audio	26
2.3.11. Battery	26
2.3.12. Power supply unit	27
<b>3. Connectivity</b>	<b>29</b>
3.1. On terminal	29
3.1.1. Wired Connectivity:	29
3.1.1.1. micro USB type A/B	29
3.1.1.2. Base Interface	29
3.1.2. Wireless Connectivity	30
3.1.2.1. GPRS	30
3.1.2.2. 3G - HSDPA	30
3.1.2.3. Bluetooth	31
3.1.2.4. Wifi	31
3.2. On base	31
3.2.1. Base charger	33
3.2.2. USB	33
3.2.3. Bluetooth	34
3.2.4. Modem (PSTN)	34
3.2.5. Ethernet	35
<b>4. Standards</b>	<b>37</b>
4.1. Immunity characteristics	37
4.2. Disturbance produced by the equipment	37
4.3. Operating conditions	37
4.4. Storage conditions	37

<b>5. Norms and certifications</b>	<b>39</b>
<b>6. Software</b>	<b>41</b>
6.1. Software architecture	41
6.2. Memory space allocation	42
6.3. Software security management	43
6.4. Operating system	43
6.4.1. Bootstrap	43
6.4.2. Operating system (OS) characteristics	44
6.5. Manager	45
6.5.1. Terminal initialisation	45
6.5.2. Terminal maintenance	45
6.6. Software downloading	47
6.6.1. Downloading	47
6.6.2. LLT(Local Loading Tool)	47
6.6.3. Downloading by USB key	48
6.6.4. TMS (Terminal Management Server)	48
6.6.5. Downloading and managing memory allocation in the terminal	48
6.6.6. Improved software downloading	48
6.6.7. Starting the downloading	49
6.7. Development workstation	50
<b>7. TMS</b>	<b>51</b>
7.1. Introduction	51
7.2. Basic functions	51
7.3. Advanced functions	51
7.4. Customer savings with Ingenico TMS solution	52
<b>8. Glossary</b>	<b>53</b>
<b>1. Document</b>	<b>7</b>
1.1. Document change history	7

1.2. Document sign off	7
<b>2. Equipment</b>	<b>9</b>
2.1. Introduction	9
2.2. General hardware description	9
2.2.1. Terminal's description	9
2.2.1.1. Dimensions & weight	9
2.2.1.1.1. With 25 mm paper roll	9
2.2.1.1.2. With 40 mm paper roll	10
2.2.1.2. Functional overview	10
2.2.2. Base description	12
2.3. Technical hardware characteristics	12
2.3.1. Processor	12
2.3.2. Memory capacity	13
2.3.3. Booster	13
2.3.4. Data security	13
2.3.4.1. Hardware design	13
2.3.4.2. Software design	14
2.3.4.3. Product activation	14
2.3.5. The isolation mechanism by electronic locking system	14
2.3.5.1. Isolation	14
2.3.5.2. MMU features	15
2.3.5.3. Inviolable memory protection	15
2.3.5.4. OS is inviolable and protected	15
2.3.5.5. The OS ensures the inter-violability of software application	15
2.3.6. Card readers	15
2.3.6.1. Main smart card reader	15
2.3.6.2. 2 <sup>nd</sup> card reader	16
2.3.6.3. Magnetic stripe reader	17
2.3.6.4. Contactless reader	17
2.3.6.4.1. Introduction to Contactless	18
2.3.6.4.2. What is Contactless card payment?	19
2.3.6.4.3. The advantages of Contactless technology	19
2.3.6.5. SAM readers	19
2.3.7. Keypad , navigation pad	20
2.3.8. Display	24
2.3.9. Printer	24



2.3.10. Audio	23
2.3.11. Battery	23
2.3.12. Power supply unit	23
<b>3. Connectivity</b>	<b>25</b>
3.1. On terminal	25
3.1.1. Wired Connectivity:	25
3.1.1.1. micro USB type A/B	25
3.1.1.2. Base Interface	25
3.1.2. Wireless Connectivity	26
3.1.2.1. GPRS	26
3.1.2.2. Bluetooth	26
3.2. On base	27
3.2.1. Base charger	28
3.2.2. USB	28
3.2.3. Bluetooth	29
3.2.4. Modem (PSTN)	29
3.2.5. Ethernet	30
<b>4. Standards</b>	<b>31</b>
4.1. Immunity characteristics	31
4.2. Disturbance produced by the equipment	31
4.3. Operating conditions	31
4.4. Storage conditions	31
<b>5. Norms and certifications</b>	<b>33</b>
<b>6. Software</b>	<b>35</b>
6.1. Software architecture	35
6.2. Memory space allocation	36
6.3. Software security management	37
6.4. Operating system	37
6.4.1. Bootstrap	37
6.4.2. Operating system (OS) characteristics	38




<b>6.5. Manager</b>	<b>39</b>
6.5.1. Terminal initialisation	39
6.5.2. Terminal maintenance	39
<b>6.6. Software downloading</b>	<b>41</b>
6.6.1. Downloading	41
6.6.2. LLT(Local Loading Tool)	41
6.6.3. Downloading by USB key	43
6.6.4. TMS (Terminal Management Server)	43
6.6.5. Downloading and managing memory allocation in the terminal	42
6.6.6. Improved software downloading	42
6.6.7. Starting the downloading	43
<b>6.7. Development workstation</b>	<b>44</b>
<b>7. TMS</b>	<b>45</b>
7.1. Introduction	45
7.2. Basic functions	45
7.3. Advanced functions	45
7.4. Customer savings with Ingenico TMS solution	46
<b>8. Glossary</b>	<b>47</b>



### Legend:

 This symbol indicates a process to follow.

 **This symbol indicates an important warning.**

 *Italic typeface in a frame indicates a piece of information.*



# 1. Document

---

## 1.1. Document change history

---

Version	Date	Changes	Author
V1	August 2010	Creation	L. LOMBARD
V2	Dec. 2010	Evolutions	C. JEANNEAU
V3	June 2012	Up-date 3G	G. ANDRE

## 1.2. Document sign off

---

Name	Title	Date	Signature
V. FILLAUD	Product Management Mobility		
C. LARINIER	R&D Product Manager		
G. ANDRE	Marketing Product Manager		



## 2. Equipment

---

### 2.1. Introduction

---

This document is aimed at describing from a technical perspective the Ingenico's new range of mobile terminals, the iWL series.

The iWL range has been developed to address all the mobility payment needs, even in the most demanding situations. From pay-at-table to taking payment on-the-move, all iWL terminals have been designed around the core of Ingenico's innovative technology and security expertise, bringing to the market the first pocket-sized wireless payment device and the most comprehensive portable range ever.

The iWL range is composed of 2 models:

- iWL220
- iWL250

**This Technical Guide is mainly geared to meet the needs of the regions when answering tenders. It can be used as a Reference Guide for any specification-related question.**

☞ This document is internal to Ingenico and should not be communicated to any customer.

For further information, you can refer to the sales guide and the user guide.

### 2.2. General hardware description

---

#### 2.2.1. Terminal's description

##### 2.2.1.1. Dimensions & weight

###### 2.2.1.1.1. With 25 mm paper roll

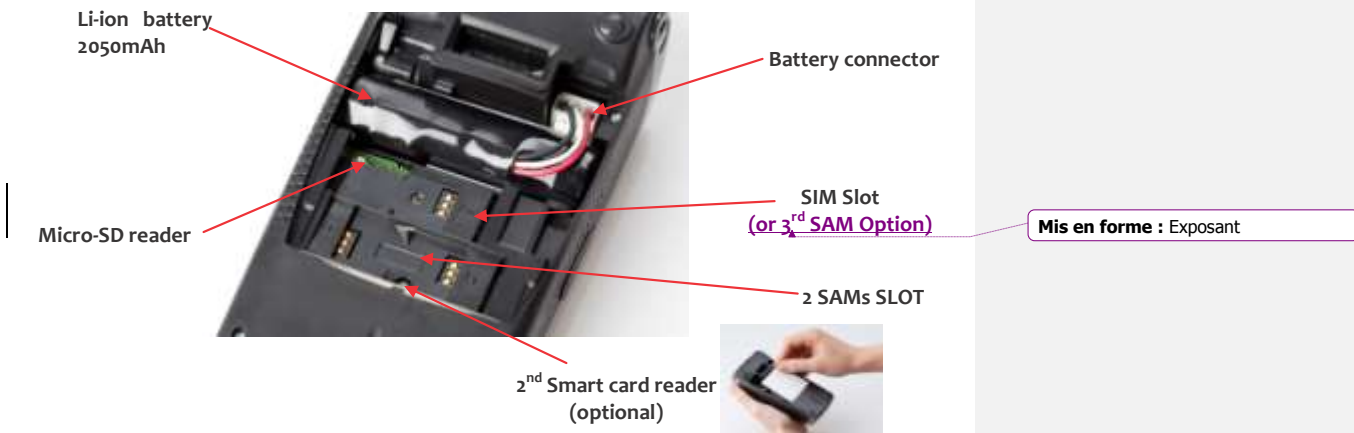


2.2.1.1.2. With 40 mm paper roll



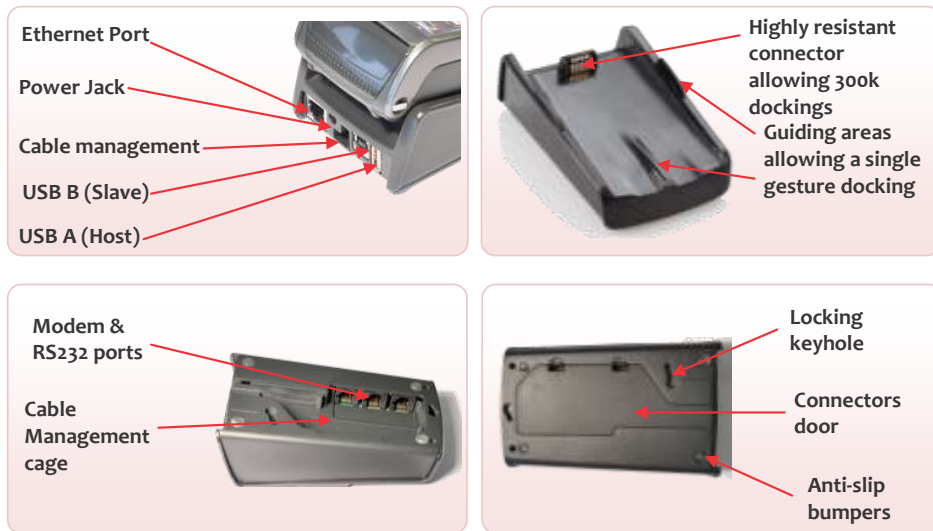
2.2.1.2. Functional overview





Model	iWL220/250 with 25mm paper roll	iWL220/250 with 40 mm paper roll
Type	Monochrome	Color
Display area	2.51" 56,3 x 31,3 mm	2.81" 57,1 x 42,8 mm
Number of pixels	128 x 64	320 x 240 (QVGA)
Number of keys	15 keys	15 keys
Function & navigation keys	7 keys	7 keys
Keyboard	Backlit	Backlit
Buzzer	Up to 60 dB	Up to 60 dB
Audio speaker	-	Optional
External dimensions	150 (l) x 44 (H) x 78 (W) mm	165 (l) x 54 (H) x 78 (W) mm
Weight	285g	300g
Casing material	Baked in ABS-PC	Baked in ABS-PC

### 2.2.2. Base description



Connector	Description
Terminal interface	USB link between Base and Terminal
Jack female (Ø 3,5 – 1,3mm)	PSU connector
USB-A (Host)	Host port
USB-B (Slave)	Slave port
RJ11	Up to 2 RS232 ports for serial links
RJ11	Dial-up Modem
RJ45	Ethernet 10/100 Base T

## 2.3. Technical hardware characteristics

### 2.3.1. Processor

Main CPU	RISC 32-bits ARM9 processor
Clock frequency	380 MHz
Capacity	450 MIPS



<b>CRYPTO CPU (booster)</b>	RISC 32-bits ARM7 processor with flash and RAM memory
<b>Clock frequency</b>	57 MHz
<b>Capacity</b>	50 MIPS

<b>Calendar</b>	Leap-year management
-----------------	----------------------

The power of the iWL2xx's processors gives the following performance:  
 $3DES \rightarrow$  less than 10 $\mu$ s.

Keys \ Algorithm	RSA	SDA	DDA
1024 exp 3	0,4 ms	1 ms	1,5 ms
1024 exp $2^{16} + 1$	3 ms	8 ms	13 ms
2048 exp 3	1,1 ms	3 ms	4,5 ms
2048 exp $2^{16} + 1$	9 ms	24 ms	38 ms

### 2.3.2. Memory capacity

Memory	iWL220	iWL250
Internal SDRAM	16MB up to 32MB	32MB
Internal Flash	16MB up to 128MB	128MB
$\mu$ SD card reader	Optional	Standard

### 2.3.3. Booster

The booster is a secured ASIC (crypto processor) including all the secured functions which protect the device against various attacks.  
The booster embedded has an impact on security personalization.

### 2.3.4. Data security

#### 2.3.4.1. Hardware design

The terminal was designed to be tamper sensitive, in order to preserve the sensitive data (keys or confidential code) and to delete this data as soon as a tamper attempt is detected.

- Tamper detection
  - Protection against tampering:
    - By micro switches
    - By temperature monitoring

- By voltage monitoring
- By CPU clock monitoring

- Tamper evidence

When tampering occurs, the terminal reacts:

- The crypto-processor deletes sensitive data
- A message is displayed to alert the user
- The crypto-processor locks
- The keypad locks with display of the message “unauthorized” or “irruption”

#### 2.3.4.2. Software design

Application software loading is made secure. Only authenticated, signed and certified software can be loaded into the terminal .

The application software identification scheme is based on:

- Asymmetric encryption algorithm with the public and private keys
- Certified RSA cards
- Software signature tool (SST)

Software intended to be loaded into the secure terminal must first be signed by software signature tool. It can be downloaded or loaded using a LLT (local loading tool).

Once the software is loaded, the crypto-processor checks the loaded software’s certificate and signature. The operation constitutes the authentication. If the loaded software is authentic, it is accepted.

If this condition is satisfied, the downloading of a software application into an iWL2xx using a local or remote tool operates the same way as for other products in Ingenico’s range.

#### 2.3.4.3. Product activation

The product has to be activated before any use. Once activated the terminal is operational. Activation enables:

- authorization of application software loading and product security.

### 2.3.5. The isolation mechanism by electronic locking system

#### 2.3.5.1. Isolation

Read/write isolation is obtained by user confinement in the application software memory space, inter-software isolation is controlled by an MMU (memory management unit) .

### 2.3.5.2. MMU features

- Hardware protection
- Total inter-software protection (read/write)
- Code protection

### 2.3.5.3. Inviolable memory protection

The controller **checks each access** to the memory.

### 2.3.5.4. OS is inviolable and protected

The processor distinguishes two execution environments:

- USER environment: software domain
- SUPERVISOR environment: OS domain

No software running in the USER environment can access the SUPERVISOR environment. This exclusion mechanism is ensured by the processor itself. Therefore the operating system (OS) is tamper-proof, even in the case of an application software bug. This system tamper protection ensures that the isolation mechanism monitoring by the OS remains.

### 2.3.5.5. The OS ensures the inter-violability of software application

The OS can decide the access rights of the USER environment at any time.

The MMU used by the processor enables the software application's addressable space to be defined. A software application can only write to the memory space corresponding to the extent of its data field. Any attempt **to write or read** in another space is immediately "trapped" by the controller, generating an exception. Thus the operating system keeps a track of this incident for future use with remote diagnostics. The other software application remain tamper-proofed and operational. Furthermore, the software in question cannot even self destruct, because its write access to code is denied.

## 2.3.6. Card readers

### 2.3.6.1. Main smart card reader

The smart card reader is located at the front of the terminal.

It allows easy introduction and removal of the card, and leaving the card visible to the user.



It can detect cards presence and resist to IK04 impact.

Feature	Description
<b>Conformity with ISO standard</b>	- ISO/IEC 7816-1, 2, 3 standard - EMV specifications
<b>Protocol handled</b>	Synchronous and Asynchronous T=0 & T= 1
<b>Clock frequency</b>	4,76MHz (double choice by SW, with PPS management)
<b>Protection</b>	Detection of short-circuit or over-consumption Detection of accidental removal
<b>Programming voltage Vpp</b>	Not connected
<b>Grip</b>	8 friction contacts (middle chip) Contact for card presence and removal
<b>Synchronous cards</b>	Separate logical outputs on contacts 4 and 8 Possibility of specific drivers development on request.
<b>Power supply voltage</b>	Vcc 5V or 3V or 1.8V (transition by software)
<b>Read head lifespan</b>	300 000 cycles

### 2.3.6.2. 2<sup>nd</sup> card reader

On the iWL2xx the second card reader is an optional device. It is located at the rear side of the terminal. The card is hidden under a removable trapdoor.



Featu	Description
<b>Conformity with ISO standard</b>	ISO7816-2
<b>Cards format</b>	ID1 format
<b>Synchronous cards</b>	Don't manage 4 and 8 contacts
<b>Read head lifespan</b>	<ul style="list-style-type: none"> <li>• Resist to foreign object insertion IP30</li> <li>• Resist to card insertion in a wrong way</li> <li>• Up to 5000 card operations (insertion /withdrawal)</li> </ul>

### 2.3.6.3. Magnetic stripe reader

The reader is located on the right side of the terminal and a drawing indicates card position and swiping direction.

The MSR is able to read the 3 tracks simultaneously.



Feature	Description
Reader type	Manual
Tracks read	Tracks ISO 1, 2, 3
Cards format accepted	ISO7810 and 7811 and 7813 standards
Card swipe speed	From 0.1m/s to 1m/s with typical cards
Read direction	Bi-directional
Read head lifespan	500 000 reads

### 2.3.6.4. Contactless reader

The contactless reader is located around the display.



Feature	Description
Reader type	Contactless

<b>Cards format accepted</b>	ISO/IEC 14443-2 Type A&B standard EMV specifications Mifare: <ul style="list-style-type: none"> <li>• Mifare classic 1k / classic 4k</li> <li>• Mifare mini</li> <li>• Mifare Ultralight /Ultralight C  “Ultralight C” managed as “Ultralight” (DES authentication not implemented)</li> <li>• Mifare DESFire 2k/4k/8k</li> <li>• Mifare Smart MX (Type A)</li> <li>• ISO 14443 Type B</li> </ul> NFC Master , passive mode Felica (scheduled for 2011) Calypso
<b>Information processing</b>	4 indicator lights
<b>Communication speed</b>	106 / 212 kb/s
<b>Operating volume</b>	Up to 4 cm
<b>Optional</b>	Yes (factory setting)

#### 2.3.6.4.1. Introduction to Contactless

“Contactless” is the term that was invented and widely adopted by the Smartcard industry to characterize a new way to read smartcards. By using radio signal, it is possible to read cards at a short distance, without inserting a card in the reader, thus the name “contactless”.

Contactless technology is sometimes mixed with Radio Frequency Identification (RFID), which is partly true since both use the same principles: a reader (sometimes called a coupler) sends a radio frequency (RF) wave through a card or a tag containing a coil and a small chip RF power energizes the coil, giving enough current to power the chip and allows data transmission both way.

It should be noted however that RFID is mostly used for identification of objects and animals, and is based on a wide range of frequencies (from 125 kHz to 5 GHz). On the contrary, contactless allows the use of microprocessor smartcards with more security and is preferred for the identification of persons (for ID, payment and others uses). Contactless uses only one frequency: 13,56 MHz.

#### 2.3.6.4.2. What is Contactless card payment?

The contact payment allows a cardholder to make a purchase without having to hang over, swipe or dip a payment card. To make payment the cardholder simply present the payment card in front of the contactless landing zone of the terminal, defined by the logo:



A payment contactless will normally be an offline authorized chip transaction, the card can be removed 500 milliseconds (ms) and the transaction will be completed in less than one second.

In certain local markets and for international may be required after the card has been removed.

#### 2.3.6.4.3. The advantages of Contactless technology

Contactless technology offers several advantages:

- **Short transaction time:** the ease of card to reader presentation and a high speed of data transfer reduce considerably the transaction time. Because the transaction time is reduced, business can increase speed and generate more revenue.
- **Reliability and lower costs:** there is no mechanical contact between the card and the reader so the damages of both card and reader are reduced. Thus, contactless technology is reliable and reduces the maintenance cost of reader.
- **Vandal protection:** Contactless technology increases protection against vandalism. Whereas the contact slot of contact reader is often the target of vandalism acts, contactless reader will not be exposed to these problems.
- **Security:** The use of contactless smart cards with a microprocessor allows for a high level of transaction security and these cards are very difficult to duplicate.

#### 2.3.6.5. SAM readers

The access to the SAMs is protected. It is located under a removable trap. SAMs are identified by marking on casing “1” and “2”.

[An optional third SAM is available. A SAM3 label identifies this option on the right of the reader.](#)

2 SAM readers

2 SAM readers  
Optional third SAM readers



Feature	Description
Conformity with ISO standard	ISO7810
Cards format	ID-000 format
Synchronous cards	Don't manage 4 and 8 contacts
Lifespan	1000 SAM operations (insertion/withdrawal)

### 2.3.7. Keypad , navigation pad



Feature	Description
Number of keys	15+ up/down/OK navigation keys+ 4 function keys F1-F2-F3-F4
Type	Elastomer membrane



<b>Number of operations</b>	2 000 000 operations
<b>Pressing force</b>	80g to 200g
<b>Backlit</b>	White by LED

### 2.3.8. Display



Feature	iWL220	iWL250
<b>Type</b>	Monochrome	Color
<b>Display area</b>	2.53" 56,3 x 31,3 mm	2.81" 57,1 x 42,8 mm
<b>Number of pixels</b>	128 x 64	320 x 240 (QVGA)
<b>Technology</b>	FSTN	TFT
<b>Frame frequency</b>	40Hz	70Hz
<b>Number of colors</b>	NA	4096 colors
<b>Serviceability</b>	Screen replaceable in repair center only	Screen replaceable in repair center only

### 2.3.9. Printer

iWL2xx printer allows a fast printing: up to 30 lines/s. It is very silent:  $\leq 52$ dB.



Technical manual\_iWL220/250  
ICO\_MKP\_009\_GU\_EN\_V4

Feature	Printer's description
Type	Thermal printing
Paper loading	Easy paper loading without paper axis
Printing speed	Up to 30 lines/s – 90mm/s
Noise level	≤52dB
Paper presence detection	Paper sensor at the end of the roll
Definition	200 DPI
Lifespan	200 000 transactions , 400 000 cuts with reference paper
Graphic mode	200 DPI in two directions
Printing color	Black
MTBF	Printer Annual Failure Rate for printer estimation : 2% (printer MTBF : 50 years estimated)

Feature	Paper roll's description
Paper type	Paper color White – JUJO AF50ks or equivalent
Width	56 mm
Length	9 m (for 25 mm diameter roll), around 17 m (for other rolls)
Diameter	25 mm / 40 mm

### 2.3.10. Audio

2 modes available:  
- buzzer

Feature	Buzzer's description
Noise level	Up to 60 dB, at 1 m all directions (adjustable by software)

- audio speaker (option for iWL250)

### 2.3.11. Battery

---

Technical manual\_iWL220/250  
ICO\_MKP\_009\_GU\_EN\_V4

• 26/60



Copyright © 2010 Ingenico  
All rights reserved

The iWL2xx has a lithium-ion easy-to-set-and-remove battery.

Feature	Description
Type	Lithium-ion
Power	2050 mAh
Battery life	<ul style="list-style-type: none"> <li>- 1 000 transactions with fully charged battery and without energy consumption related to backlit or radio link</li> <li>- Can remain powered ON up to 300 hours in <u>sleeping state</u> starting with fully charged battery and without energy consumption related to backlit or radio link</li> <li>- Can remain powered ON up to 200 hours with connected GPRS/3G link and terminal in sleeping state starting with fully charged battery and without energy consumption related to backlit or radio link</li> </ul>
Saving power mode	Automatic sleeping mode and backlight power off (time can be user defined)
Charge	With 5V-1A power supply
Recharge time	4 hours from empty to full charge
Powering mode	<ul style="list-style-type: none"> <li>- Putting the terminal on the base</li> <li>- Directly connecting the micro USB port</li> </ul>
MTBF	According to battery supplier : 80% of the initial capacity (i.e. 1700 mAh) still available after 500 charging cycles, under nominal conditions.
Back-up battery	Lithium cell 3V-220mAh

Please note that these data are approximate.

### 2.3.12. Power supply unit

Two main types of PSU are offered:

- Multi PSU with adapter for different countries (Australia, UK...) allowing either to deliver a solution compatible with several standards or to provide a solution for countries not covered by CE, UK or US standards
- Monoplug PSU CE or US or UK type

Character	Description
Input voltage	100-240V , 50/60 Hz
Output voltage	5V, 1A

<b>Protection</b>	Against surges: thermal fuse placed on primary Against conducted interference: integral filter
<b>Standards</b>	Class II double-isolation
<b>Mechanical Interface</b>	Power supply jack with safety catch Straight flexible cable: about 3 meters long between base and power supply unit , plug in on base side
<b>Weight</b>	Approximately 100 g

## 3. Connectivity

---

### 3.1. On terminal

---

#### 3.1.1. Wired Connectivity:

##### 3.1.1.1. micro USB type A/B



Characteristic	Micro USB type A / B
Electronic interface	USB Host & Slave
Life duration	Up to 1000 operations
Mechanical interface	A-B micro-USB receptacle
Logical interface	Low speed: 1.5 Mbps Full speed: 12 Mbps USB2.0
Functionnalities	- Battery recharge - Software upgrade - Terminal to be used as a USB device

##### 3.1.1.2. Base Interface

The iWL2xx has a connection interface allowing to create a USB link between the Terminal (HOST) and the base (SLAVE).



### 3.1.2. Wireless Connectivity



#### 3.1.2.1. GPRS

The GPRS connection is optional in iWL2xx.

The access to the GPRS SIM connector is protected; it is located under a removable trap. GPRS SIM is identified by marking on casing "SIM".

Characteristics	GSM/ GPRS
Frequency	Quad band: GSM (850, 900Mhz) DCS (1800Mhz) PCS (1900Mhz)
Transit power	Class 4 (2W) for GSM850 / EGSM900 Class 1 (1W) for DCS1800 / PCS1900
Communication feature	Multi slot Class 10 ( 4+1, 3+2) Stay connect feature
GPRS baudrates	Downlink up to 85.6 kbps, Uplink up to 42.8 kbps

#### 3.1.2.2. 3G - HSDPA

The 3G-HSDPA connectivity is one of the connectivity options available for iWL250.

The access to the 3G SIM connector is protected; it is located under a removable trap.

The 3G SIM is identified by marking on casing "SIM". It is the same slot than the GPRS SIM.

Characteristics	HSDPA 3,6Mbps and EDGE/GPRS/GSM Class 12
Frequency	Triple bands WCDMA 900/1900/2100 MHz or 850/1900/2100 MHz Full Quad band support GSM/GPRS/EDGE 850/900/1800/1900 MHz
Transmit power	Class 4 (2W) for GSM850 / EGSM900 Class 1 (1W) for DCS1800 / PCS1900 Class E2 EDGE 900 / 1800 Class 3 for UMTS 900/1900/2100

<b>Com. feature</b>	GPRS SMG 31bis, Multi slot class 12, class B terminal, PBCCH support, 3 PDP contexts, CS1 to CS4.
	EDGE Multi slot class 12
	Class E2, Voice and Data in parallel for UMTS/HSDPA, 4 logical channels
<b>HSDPA baudrate</b>	Downlink up to 3.6 Mbit/s Uplink up to 0.384 Mbit/s

### 3.1.2.3. Bluetooth

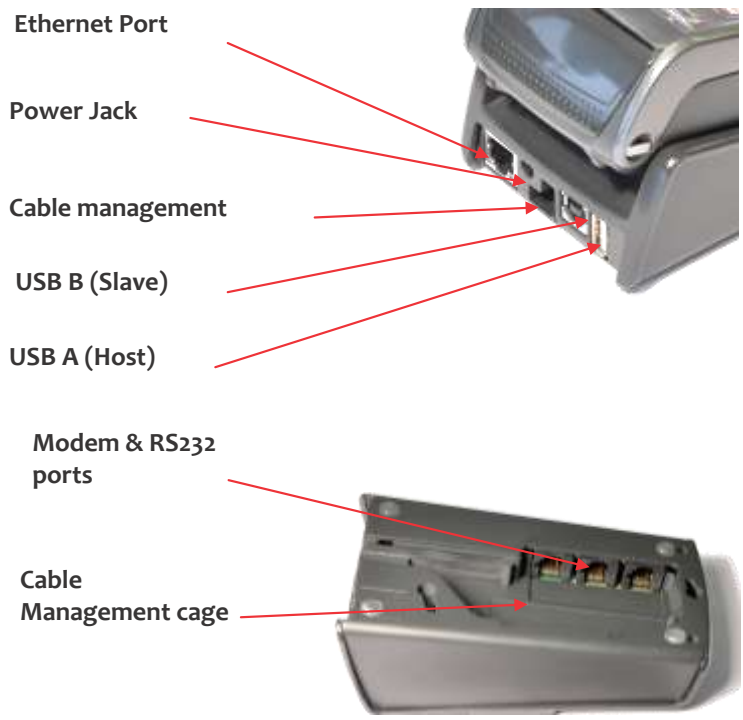
Characteristic	Bluetooth V2.0
<b>Chipset</b>	Bluecore 6
<b>Standard compliance</b>	Bluetooth v2.1 EDR (enhanced data rate) – Class 1
<b>Profile</b>	SPP Other profile to be analysed on request
<b>Radio transfer rate</b>	1 Mbit/s 2Mbit/s (EDR)
<b>Number of supported links</b>	7 slaves to 1 base
<b>Range</b>	Indoor: 70m typical Bluetooth Class 1 – mini 100m in free sight

### 3.1.2.4. Wifi

Characteristic	2.4Ghz and 5Ghz wifi
<b>Chipset</b>	TI wilink 8 base
<b>Standard compliance</b>	802.11 a,b,g,n / SISO / 20-40MHz bandwidth
<b>Radio transfer rate</b>	From 1 Mbit/s to 135Mb/s
<b>Range</b>	Indoor: 30m typical mini 100m in free sight
<b>Home security</b>	OPEN, WEP, WPA, WPA2
<b>Enterprise security</b>	EAP-TLS, EAP-TTLS, EAP-PEAPv0

Mis en forme : Anglais (États Unis)

## 3.2. On base



Terminal bases available for the iWL2xx series:

Base's name	Power supply	Line in	1 USB Host	1 USB Slave	1 x RS232	2 x RS232	Ethernet	Power Over Ethernet (POE)
Charger Base	•							
Modem- 1RS Base	•	•	•		•			
Modem- 2RS base	•	•	•			•		
Ethernet Modem- Base	•		•	•		•	•	(•)
Bluetooth - Ethernet- Modem Base	•	•	•	•		•	•	(•)

(x): optional feature

Brief technical descriptions of the base's options:





	Modem	COMo or COM1	Host USB	Slave USB	Ethernet
Electronic interface		Simplified RS232	Host USB	Slave USB	IEEE 802.3
Number of wires		CTS RX TX GND RTS	5v-D+ GND	5v-D+ GND	RX+ RX- TX+ TX-
Mechanical interface	V34, V32b, V32, V42, V42b, MNP4&MNP5 V22b, V22, full duplex, asynchronous, synchronous	Modular jack 6 points RJ11 1=Ground 3=Rx 4=Tx 5=CTS 6= RTS		Type USB socket 1=5V 2=D- 3=D+ 4=GND	Modular jack 8 points RJ 45 Standard interface
Logical interface	Operation from 0 to -43dBm Software configured	300-115kbps Software – configured framing	Low speed: 1.5 Mbps High speed: 480 Mbps USB 2	12Mbps max USB 1.1	10 Mbps and 100 Mbps compatible Full duplex
Connection examples	AT compatible Connection to network by RJ11	Cash register Check editor/reader Computer External modem RS 485 converter unit	Check-reader External-modem dongle External ISDN dongle, ...	POS integration	LAN

### 3.2.1. Base charger

Characteristic	
Endurance	300 000 dockings with the terminal supported
Type	110-230 V +/- 10%, 50-60 Hz
Insulation	Class II
Charge	With 5V-1A power supply

The connector is a power supply jack.

### 3.2.2. USB

	USB Host A	USB Slave B
Electronic interface	USB HOST	USB slave
Number of wires	1= vBus 2= D- 3= D+ 4= GND	1= vBus Slave 2= D- 3= D+ 4= GND

<b>Mechanical interface</b>	USB type A jack	USB type B jack
<b>Logical interface</b>	Low speed : 1,5 Mbps High speed : 12 Mbps	CDC Class only
<b>Connection examples</b>	- Check reader equipped with USB - PP30S, P30 - Fingerprint sensor - Contactless target, external modem, ...	- Local downloading tool - Point of sale integration

### 3.2.3. Bluetooth

Characteristic	Bluetooth V2.0
<b>Chipset</b>	Bluecore 6
<b>Standard compliance</b>	Bluetooth v2.1 EDR (enhanced data rate) – Class 1
<b>Profile</b>	SPP Other profile to be analysed on request
<b>Radio transfer rate</b>	1 Mbit/s 2Mbit/s (EDR)
<b>Number of supported links</b>	7 slaves to 1 base
<b>Range</b>	Indoor: 70m typical Open space: up to 250m

### 3.2.4. Modem (PSTN)

- Modem V22, V22b , V32, V32b ( respectively 1 200, 2 400, 9 600, 14400 bauds)
- Full software configuration
- AT compatible
- Communicates with the STN
- Responder, initiator, busy line detection
- Fast connect

Characteristic	PSTN
<b>Modulation / Compression</b>	V34, V32b, V32, V42, V42b, MNP4& MNP5 V22b, V22, full duplex, asynchronous, synchronous
<b>Emission levels</b>	Software configured – 0 to 15dBm
<b>Reception levels</b>	Operation from 0 to -43dBm

<b>Insulation</b>	Line differential security: 250V non-destructive Galvanic isolation between line interface and modem: 2.500 volts/1min
<b>Logical</b>	AT-compatible command set
<b>Cable</b>	Plug-in cable, length 3m, fitted with RJ11 at both ends Connection to network by RJ11 socket + T/RJ11 adapter if necessary

### 3.2.5. Ethernet

Characteristics	Ethernet
<b>Electronic interface</b>	IEEE 802.3
<b>Number of wires</b>	RX+ RX- TX+ TX-
<b>Mechanical interface</b>	Modular jack 8 points RJ 45 Standard interface
<b>Logical interface</b>	10 Mbps and 100 Mbps compatible Full duplex
<b>Speeds</b>	100 MHz
<b>Protocol</b>	- IPv4 - FTP SSLv3 (Open SSL layer embedded. Security profiles management. Single / dual authentication possible. Conforms to Mastercard PTS program) SNMP SMTP
<b>Connections examples</b>	LAN



## 4. Standards

### 4.1. Immunity characteristics

Tests of immunity to:	Standards
Electrostatic discharges	IEC/EN 61000-4-2
Radio-frequency electromagnetic fields	EN 61000-4-3 (2002 + A1/2002)
Electrical fast transients/bursts	IEC/EN 61000-4-4
Surges	EN 61000-4-5 (2005)
Radio disturbances	EN 61000-4-6 (2003+A1/2004+A2/2006)
Magnetic fields	EN 61000-4-8 (1993+A1/2000)
Voltage dips, short interruptions and voltage variations	EN 61000-4-11 (2004)

### 4.2. Disturbance produced by the equipment

	Standards	Details
Conducted disturbance	EN 55022 éd. 1998 / A1-2000 / A2-2003	Class B
Radiated disturbance	EN 55022 éd. 1998 / A1-2000 / A2-2003	Class B
Limits for harmonic current emissions	EN 61000-3-2 (2000+A2/2005)	
Limitation of voltage fluctuations and flicker	EN 61000-3-3 (1994+A1/2001)	

### 4.3. Operating conditions




	Details
Operating Temperature	-10°C to +45°C
Charging temperature	+5°C to +40°C
Max relative humidity (no condensation)	85%HR at +40°C

### 4.4. Storage conditions

	Details
Temperature	-20°C - +55°C
Max relative humidity (no condensation)	85% HR +40°C



## 5. Norms and certifications

Certifications	
	Approved LOA 124350910400 21 FIM, 9/6/2010
	Approved v.2 LOA 4-20161, 9/27/2010
 <small>Associação Brasileira das Empresas de Cartões de Crédito e Serviços</small>	Approved Manual ABECS Rev. 5



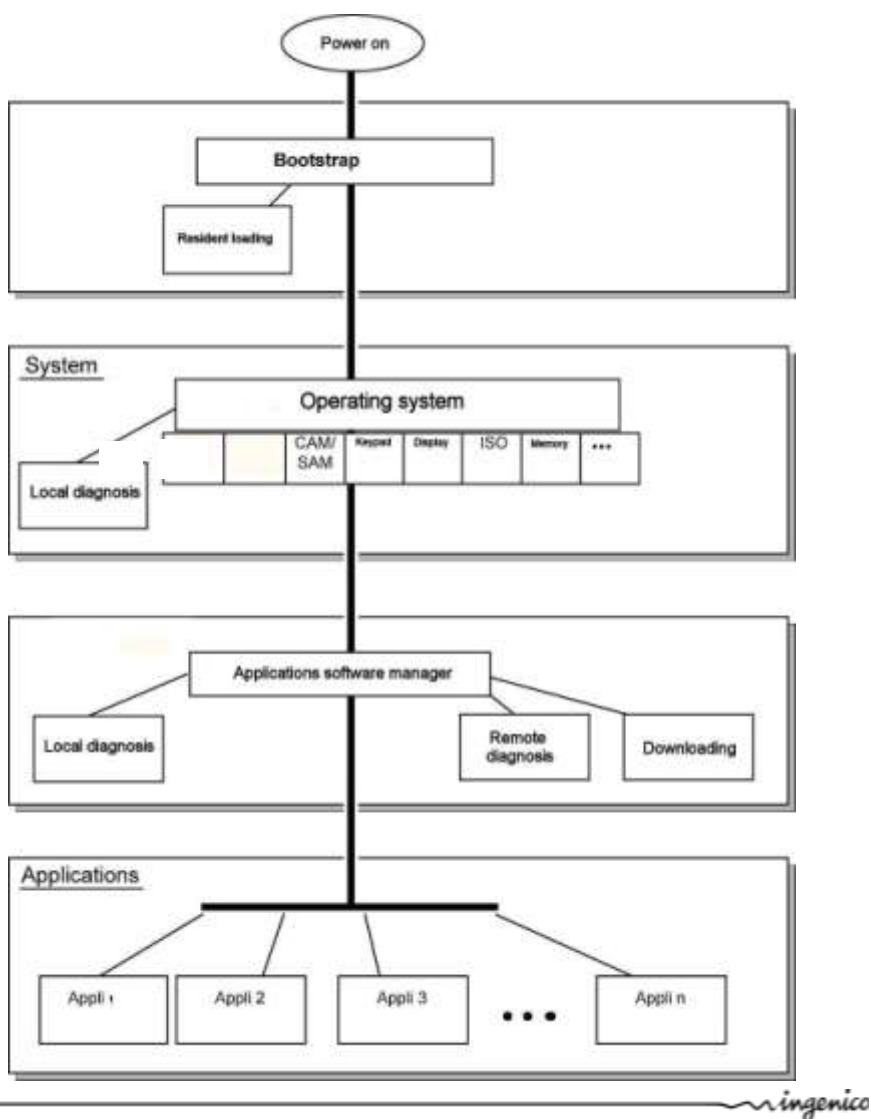


## 6. Software

The terminal has a software architecture that supports several applications coexisting without mutual interference.

The OS is multitask, real-time and pre-emptive. The inputs/outputs are managed under interruptions. This means the peripherals can be processed simultaneously, and thus improves the terminal's performance. It can be downloaded to FLASH memory.

### 6.1. Software architecture



The software architecture is divided into three levels:

- System
- Multi-application manager
- Independent applications

The system manages access to all the terminal's peripherals. Access is completed via standard C primitives for all the input/output peripherals (keypad, printer, etc.) and via specific primitives for other peripherals (smart cards and magnetic stripe cards). Further, the system takes charge of memory management. It allocates memory space to the software applications and controls access.

The multi-applications manager is the entity that calls on the various applications downloaded in the terminal in response to the various events that occur in the terminal.

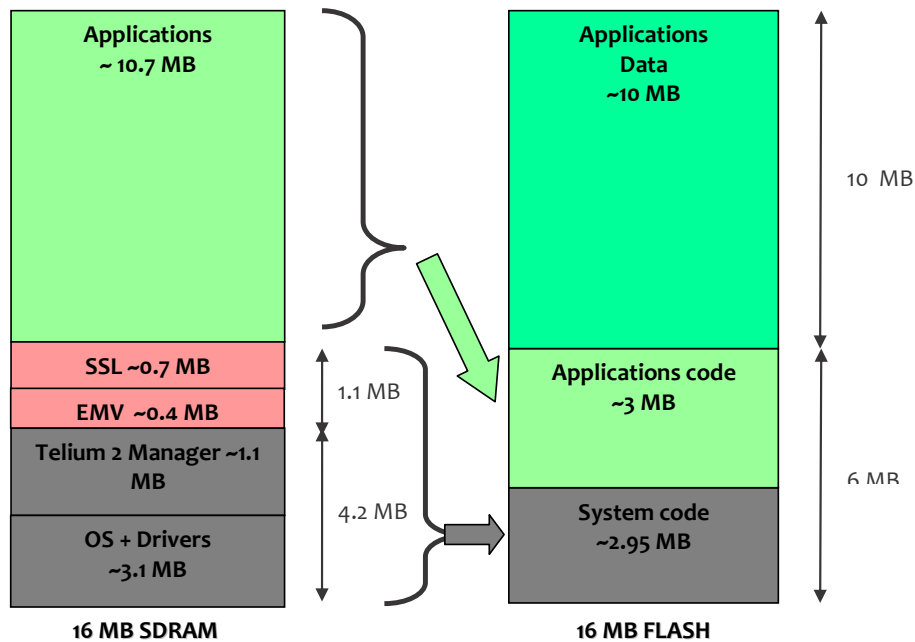
The applications are modeled around the demands made by the multi-applications manager. Each request or input point represents a processing operation to be performed. Each application manages the execution of these processing operations according to its specifications. This standardization based on input points simplifies the implementation of the applications on terminals. The iWL2xx provides natural access to the modularity concepts and improves the maintainability and quality of the applications.

## 6.2. Memory space allocation

---

This part describes the memory usage as it is known at the present moment, this is subject to change.

Example of a rough memory space allocation for a 16MB Flash + 16MB SDRAM configuration.



## 6.3. Software security management

The terminal is designed to execute authentic software only and to this in a ranked context.

The terminal performs the following checks

- During a software download, the terminal checks:
  - Its authenticity, by checking its signature with the RSA algorithm with RSA-2048 algorithm.
- Before loading a software from Flash to SDRAM, the terminal checks:
  - Its authenticity, by checking its signature with the RSA algorithm with RSA-2048 algorithm.

## 6.4. Operating system

### 6.4.1. Bootstrap

Bootstrap is resident.

The bootstrap very briefly takes control of the terminal following each powering up to perform the initialization and the self-test. Then it automatically runs the OS which in turn starts the applications manager.

Thus the Bootstrap provides the following functionalities:

- Memory and checksum self-test;
- Local download of the OS if absent;
- OS authenticity check and start-up.

### 6.4.2. Operating system (OS) characteristics

The OS is downloaded (locally or remotely) into the memory. It is upgradeable. After a few fractions of a second following powering up, it takes control. It checks the presence, integrity and authenticity of the system components and application present in the terminal.

The maintenance subsystem takes control in the following cases:

- if no authentic application is present;
- or if a manual action by the operator is made when powering up;
- or if it is activated by application.

The maintenance subsystem ensures, among other things, the downloading of the applications.

The OS ensures the start of the multitask core and then runs of the application by making a set of services available to them:

- **Multitask management:** Availability of a pre-emptive real-time environment, based on interruptions, events and mail boxes. This management enables simultaneous processing, which improves the terminal's performance.
- **Input/output management:** This is carried out under interruptions, generally in buffered mode. Thus, the applications developer enters a "conventional" C context.
- **System alarms management:** Certain incidents (e.g. swipe card reading error) detected by the OS are recorded. They can be used later by the maintenance subsystem during remote or local diagnostics.
- **Application alarms management:** A number of incidents detected by the applications can be saved by the OS at their request. This recording is used later as in the case of system alarms.
- **Application isolation management:** The OS provides the mechanisms described in the section on software isolation and memory protection. Between software isolation is managed by an **MMU** (Memory Management Unit).

- **Applications download management:** The OS offers the downloading services described in the section "Software download"

## 6.5. Manager

---

The main functions offered by the manager are the following:

- Application management;
- Terminal initialisation;
- Terminal maintenance;
- Card recognition and routing to the application.

When EMV DC module is present, it selects the application:

- EMV applications (conform with EMV level 2);
- non EMV applications.

### 6.5.1. Terminal initialisation

#### 6.5.1.1. Operating requirements

To function, the terminal has to be equipped with its OS, the applications manager and at least one application. If one of the three components is missing, the terminal warns the operator who has to load it.

If no application is initialized, the applications manager displays a message asking for an application to be initialized.

If at least one application is initialized, the terminal is operational. The applications manager then awaits an event to poll the software applications loaded in the terminal.

#### 6.5.1.2. Common parameters Initialization

The applications manager is used to initialize the common parameters:

Date, time, message display language, phone network configuration data, Pin-pad connection, local downloading of remote diagnostics.

### 6.5.2. Terminal maintenance

The terminal has maintenance functions for:

- Properties;
- Local downloading;
- Diagnostics.

#### 6.5.2.1. Properties

The properties function is used to print the following tickets:

---

Technical manual\_iWL220/250  
ICO\_MKP\_009\_GU\_EN\_V4

- List of applications downloaded into the terminal: version number, checksum, etc. The applications manager prints this information for itself and for the operating system;
- Applications call time: remote collect, download, etc;
- Total number of transactions in each application file contained in the terminal.

### 6.5.2.2. Download

The downloading function uses the parameters downloaded during the initialization of the application manager.

The program update function is used to update the terminal by:

- Using a special local downloading tool connected to the terminal;
- Using a remote downloading tool;
- Using a USB key.

### 6.5.2.3. Diagnostics

The diagnostic is used for:

- **Local diagnostics**

saving consists of two groups of items:

- Incident counters: used for repetitive-type incidents, when only the number of occurrences is of use, e.g. the number of incorrect swipe readings.
- Exceptional events. The information content depends on the type of incident. Generally this is the date and time, and then information on the incident itself. These events are saved in a revolving file where the most recent are kept.

- **Remote diagnostics**

This allows the operator to make a call to the server to transfer information saved in the terminal. The server can thus enrich a database for ensuring efficient monitoring of equipment, propose preventive maintenance services, operating statistics, etc.

## 6.6. Software downloading

---

### 6.6.1. Downloading

Software can be downloaded:

- Locally via the serial port (COM or USB).
- Remotely via
  - the switched telephone network (PSTN)
  - X25
  - Ethernet
  - TCP/IP network.
- By a USB key.

The techniques used:

- data compression;
- authenticity checking;
- memory allocation management, etc.

best optimize the downloading operations.

Hence savings in downloading time, use security, ease of upgrade, and number of software programs installed in the terminal.

### 6.6.2. LLT(Local Loading Tool)

The LLT is used for local software downloading.

The LLT is comprised of:

- PC running Windows XP/ 2000 / NT4, Vista;
- Ingenico downloading software;
- PC-terminal connection cable.

Local downloading is carried out:

- Using the PC with the LLT installed, on the USB slave port;
- Automatic switching to the local loader of the OS.

Possible connection by USB slave port: speed about 8 Mbps.

Selection of the software to download is guided on the PC screen using an Explorer-type windowing system (Windows Loader).

The downloading time of a 1Mo application is 4s by USB port.

### 6.6.3. Downloading by USB key

Downloading by USB key allows the downloading without any other tool.  
Downloading time is equal to USB.

### 6.6.4. TMS (Terminal Management Server)

See “Terminal management system– TMS” Chapter.

### 6.6.5. Downloading and managing memory allocation in the terminal

- Before the downloading, the system checks that the memory space is available.
- Software downloading (possibly compressed) is done into flash.
  - If software is deleted, the system frees the space.
  - If software is upgraded, the system downloads the new software, checks it and then deletes the old.
- The whole memory zone remains used and usable. No zone is reserved for upgrades.
- When the terminal starts up (power up or reset) the applications are decompressed and the code copied into RAM.

### 6.6.6. Improved software downloading

Includes the following characteristics:

- Downloading via FTP TCP/IP and PPP for optimized downloading.  
V32b downloading performance is:
  - about 14.4 kbps on the original files.Once the connection has been made with the V32b modem, the downloading of a **120 Kb** application takes about **1 min**.
- Downloading can be done by IP via Ethernet on a SSL secured channel.
- Data compression according to algorithm based on the Lempel-Ziv method ensuring compression rates of about 40%.
- For downloading, only the improved application will be downloaded. In addition, the terminal manages this and not the remote server, which offers operating security during multiple sources downloading.
- Recall management in case of communication breakdown. This service enables an interrupted downloading to be resumed at the same place where it had lost connection and only to downloading the unfinished part.
- The downloaded software is executed securely, using the authenticity check.



### 6.6.7. Starting the downloading

The downloading can be made:

- **Manually:** The applications manager at the merchant request Launch a downloading. This is especially the case of a program update or the addition of new software into the terminal's memory. In this case the procedure is simplified to the maximum.

Thus, the user starts the call **from the applications manager** by choosing the upgrade function from the dialogue menus and keys. Dial-up and connection to the server are automatic.

- For an upgrade, the user has nothing to enter.
  - For a new software request, the user is guided on screen to make the choice. The business's ID is not requested. The ID saved in the terminal is automatically transmitted to the server.
- 
- **Through management application:** The application at the request of the centre or the merchant. In this case, the downloading is fully automatic. The downloading ticket lets the business know.
  - **Through call scheduling:** terminal can be set to call at schedule date and time to regularly check of the content is up to date.

## 6.7. Development workstation

---

### Introduction

The software is written in high level C language in a multi-applications environment. Ingenico makes available all the software and equipment required for development. This includes the documentation. Also, training sessions are offered.

### Required configuration

The development workstation executes on a Pentium PC running under Windows 2000/XP/Vista.

Integrated environment (Eclipse) takes care of the software development phases:

- Project creation,
- edition,
- compilation/edition of links under GNU,
- signature,
- downloading,
- simulation,
- remote debugger.

### Supply

The development workstation comprises:

- M<sup>2</sup>OS software licence which includes:
  - Operating system
  - Applications software manager
  - Libraries
  - Related documentation in PDF files.
- User licence of SAT (Software Authentication Tool);
- User licence of LLT (Local Loading Tool);
- RSA Card and smart card reader for signing applications software.

### Related services

- Technical support

Lasts 6 months following the training.

It includes access to the hot-line, and to the updates of the documentation and software during this period.

- Software terminal package

Software packages are available allowing easy development for applications (EMV level 2 ...)

## 7. TMS

---

### 7.1. Introduction

---

Ingenico developed its own Terminal Estate Management System called IngEstate. It is a link between an organisation with an estate of payment terminals and their merchants. It allows users to remotely manage payment terminals, modify their software content and interact with merchants.

### 7.2. Basic functions

---

The basic functions are:

- be able to locally download software on a terminal using a direct cable link (usually RS232)
- be able to remotely download software on a particular terminal using modems and IP connections
- be able to remotely download applications and configuration updates to a large estate of terminals
- be able to upload terminal configurations and check software status
- be able to inform merchants when terminals are out of use during maintenance periods

### 7.3. Advanced functions

---

The advanced functions are extremely various, with new ones being requested frequently:

- draw statistics and reports about terminal configurations
- optimise automatic call scheduling/download balancing for large estates of terminals
- be able to display written messages on the terminal, using the display or the printer
- be able to easily configure a complete terminal (i.e. several applications) and to download it in one operation
- be able to analyse the status of terminal software and do only delta downloads (i.e. only the parts that are damaged or need updates)
- be able to download to either a PIN Pad or a terminal when connected;
- Customise the system easily
- Integrate with systems such as SAP easily
- ... and many others

## 7.4. Customer savings with Ingenico TMS solution

---

The most obvious cost saving is not having to send a technician to service the terminal at the merchant location. Many other costs savings are derived from the ability to have a “clean” estate; better diagnostics and remote software repairs mean less shipping of replacement terminals, less downtime, less mail and phone communication costs, more efficient update campaigns, etc.

## 8. Glossary

---

### B

**Bluetooth**: Short-range wireless connection standards

**Bps (Bits per second)**: The unit of measurement for the rate at which data is transmitted

### C

**CDMA (Code division multiple access)**: A spread-spectrum approach to digital transmission. With CDMA, each conversation is digitized and then tagged with a code. The mobile phone is then instructed to decipher only a particular code to pluck the right conversation off the air.

**Cryptography**: Information security (encryption and decryption of data)

### D

**DES**: Data encryption standard, a symmetrical encryption algorithm

### E

**EAP: Authentication protocol used with Radius server.**

**EAP-TLS : EAP with TLS authentication (require client and optional root certificate)**

**EAP-TTLS : EAP with Tuneled TLS authentication (require optional root certificate only)**

**EAP-PEAP : EAP with tunneled authentication (required optional root certificate)**

**EAP-MD5 : non secured EAP protocol mainly used for Ethernet only.**

**EMV**: EMV stands for Europay Mastercard Visa and is the new EFTPOS standard that enables with chips to be accepted anywhere in the world. It offers increased security by allowing information identifies the cardholder to be stored on the chip.

**EMV Level 1**: EMV approval level for mechanical and electrical processing (and driver software), which guarantees interoperability between card and terminals.

**EMV Level 2**: EMV approval level for software layer (or kernel), which allows a transaction to be carried out an EMV card.

**Encryption**: The transformation of data, for the purpose of privacy, into a unreadable format until reformatted with a decryption key.

**Ethernet**: A network cabling system.

## F

**Flash:** Non-volatile memory.

**Frequency:** A measure of the energy, as one or more waves per second, in an electrical or light-wave information signal. A signal's frequency is stated in either cycles-per-second or Hertz (Hz).

## G

**GSM:** Global system for mobile communication, a world standard for digital wireless transmissions. GSM is the most widely used standard in the world today with more than 150 million users worldwide.

## I

**ISDN:** Integrated services digital network

**ISO:** International organization for standardization is a global network that identifies what international standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts the by transparent procedures based on national input and delivers them to be implemented worldwide.

**ISO-8583:** International standard covering EFT messaging.

## L

**LAN:** Local area network, a data communication network, typically within a building or campus, to link computers and peripherals devices under some form of standard control.

**LCD:** Liquid crystal display.

**LED:** Light emitting diode.

**LLT:** Local loading tool

## M

**Modem:** Modulator/DEModulator, a hardware device which converts digital data into analog and vice versa to enable digital signals from computers to be transmitted over analog telephones lines.

**MSR:** Magnetic stripe reader

## O

**Operating system:** A software program that manages the basic operations of a computer system. These operations include memory apportionment, the order and method of handling tasks, flow of information into and out of the main processor and to peripherals, etc.

## P

**PCI PED:** Payment card industry PIN entry device, a security specification for EFT terminals, designed to secure the PIN information stored in a terminal from fraudulent activity.

**PED:** PIN entry device, the secure customer interface module of a payment terminal.

**PIN:** Personal identification services, it is used as a security device on payment cards requiring this code to be entered for further verification.

**Protocol:** Set of rules for organizing the transmission of data in a network.

**PSTN:** Public switching telephone network

## R

**RAM:** Random access memory

**RS-232:** RS-232 is the serial connection found on IBM-compatible PCs. It's used it for many purposes, such as connecting a mouse, printer, external modem, and various peripheral devices to a PC.

## S

**SAM:** Secure authentication module.

**Smart card:** A credit card-sized card with a microprocessor and memory.

**SRAM:** Static random access technology.

## T

**TCP/IP:** (Transmission control protocol/ internet protocol) the standard set of protocols used by the internet for transferring information between computers, handsets, and other devices.

## U

**USB:** USB is a plug-and-play interface between a computer and add-on devices (such as keyboards, printers and other peripheral devices). With USB, a new device can be added to your computer without having to add an adapter card or having to turn the computer off.

## W

**Wifi:** Wireless fidelity, Wireless network.

[Wifi 802.11 a : wifi on 5GHz band](#)

[Wifi 802.11 b : wifi on 2.4GHz band / 11Mb/s max](#)

[Wifi 802.11g : wifi on 2.4GHz band / 54Mb/s max](#)

[Wifi 802.11n : wifi up to 130Mb/s \(in SISO mode\) on 2.4GHz or on 5Ghz](#)

[Wifi SISO mode : single in, single out mode. Meaning 1 antenna only.](#)







#### NON CONTRACTUAL DOCUMENT

This Document is Copyright © 2010 by INGENICO Group. INGENICO retains full copyright ownership, rights and protection in all material contained in this document. The recipient can receive this document on the condition that he will keep the document confidential and will not use its contents in any form or by any means, except as agree beforehand, without the prior written permission of INGENICO. Moreover, nobody is authorized to place this document at the disposal of any third party without the prior written permission of INGENICO. If such permission is granted, it will be subject to the condition that the recipient ensures that any other recipient of this document, or information contained therein, is held responsible to INGENICO for the confidentiality of that information.

Care has been taken to ensure that the content of this document is as accurate as possible. INGENICO however declines any responsibility for inaccurate, incomplete or outdated information. The contents of this document may change from time to time without prior notice, and do not create, specify, modify or replace any new or prior contractual obligations agreed upon in writing between INGENICO and the user.

INGENICO is not responsible for any use of this device, which would be non consistent with the present document.

All trademarks used in this document remain the property of their rightful owners.

Your contact

Ingenico  
192 avenue Charles de Gaulle  
92200 Neuilly sur Seine - France  
Tél.: + 33 1 46 25 82 00 - Fax: + 33 1 47 72 56 95  
[www.ingenico.com](http://www.ingenico.com)

DIVxxxxA

