CRYPTAG ®

READER MANUAL

IDENTEC READER TYPES RL1 and RL3

IDENTEC LIMITED
Mercantile Road
Rainton Bridge Industrial Estate
Houghton-le-Spring
Co. Durham. DH4 5PH

Tel: +44 (0) 191 584 4084
Fax: +44 (0) 191 584 9077
Technical support: 0800 018 1661
Web site: www.identec.co.uk
e-mail: info@identec.co.uk

Last revised September 2000

This manual is provided for information purposes only. All information included in this manual is subject to change without notice. Identec is not responsible for any damages, direct or indirect, arising from or related to the use of this manual, or associated product.

WARNING NOTICE

This product uses radio frequency signals, and is therefore subject to possible interference. Any application should bear this in mind, and in particular it should not be possible for personal safety to be jeopardised by a failure to read.

This reader neither uses nor generates hazardous voltages. You should not connect any such voltage to it.

CE

This product complies with the following European Community directives

Low Voltage Directive. (73/23/EEC)
EMC Directive. (89/336/EEC)

FCC Regulations

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) this device must not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

FCC GRANT AUTHORISATION: JHDRL3-RL1

CONTENTS

1. CRYPTAG READERS RL1 and RL3

1.1 Introduction

Cryptag is a radio frequency tag identification system. Its multiple reading feature means that the reader can simultaneously identify and report one or more tags.

This combined manual covers the following reader types

RL1 Wiegand Output	RL1 RS232 Output	RL1 Clock/Data Output
RL3 Wiegand Output	RL3 RS232 Output	RL3 Clock/Data Output

RL3 readers contain an internal look-up table which modifies the way in which the tag's identity is reported, whereas RL1 readers report a number which is derived directly from the tag's identity. See Appendix A for details of output formats.

1.2 Unpacking

Check that the package contains

- Reader
- Magnet (if anti-tamper option fitted)
- Template/Installation Sheet
- Warning label
- 4 Security (front cover) screws

Each pack of up to 5 readers will contain one manual.

1.3 Getting started

(If you are new to Cryptag readers, just follow these simple instructions.)

1. Connect a 12V power supply to the reader.
   The positive connection goes to 12V on the main terminal block (see Figure 3) and the negative connection goes to 0V.

2. Bring a tag near to the reader.
   The reading range should be 90cm (35 inches) for a TM1 tag. Note how the range depends on the tag's orientation.

3. LED3 on the reader will flash regularly when a tag is being read. (LED3 is only visible when the cover is removed.)
   When no tag is present LED3 may flicker if noise is present. Learn to recognise the difference when a tag is being read.

4. The reader reports a tag only once.
   Although a tag is being read continuously, the reader will report it only once. To get another report the tag has to be removed completely first.

2. READER LOCATION

The reading range of the RL1/RL3 is such that some care is needed in selecting the reader's location.

Do not locate a Cryptag reader too close to another reader
If tags can pick up signals from two or more readers they respond to neither. The minimum separation is 1¼ times the combined reading range (i.e. 2½ times the range of two similar readers).

Do not mount the reader directly on to metal
This will reduce reading range and increase current consumption.
Do not place readers within 300mm (1 ft) of metal structures.
A reader can be mounted parallel to a metal surface with a minimum recommended spacing of 25mm (1 inch), but the metal must extend across the whole area of the reader..

Keep the reader away from possible interference sources
Interference (also referred to as noise) can reduce the reading range and make reading slower. Computer monitors can affect performance at up to 3.6m (12ft). Most monitors have less effect, but it does depend on the scan frequency.
A Site Survey (using an MS1 Site Survey Meter) is desirable.

When deciding where the reader is to be mounted, bear in mind where tags are to be worn. Think also of people in wheelchairs.

3. INSTALLATION AND COMMISSIONING

3.1 Tools and materials for installation

In addition to normal installation tools you will need a Security Screwdriver. (e.g. Cryptag Part No RL1-390) if you intend to use the security screws supplied. The normal cable is 6-core unscreened, unless another connection option has been selected. (See Appendix B).

For external mounting silicone rubber sealant is required.

3.2. Preparation

Open the Reader by removing the 4 front screws.
Loosen the terminal blocks

CAUTION
Take care not to move or damage internal components

3.3 Connections

For most installations using Wiegand format, the connections will be

0V	Power supply –ve (and data reference)
12V	Power supply +ve (10.8V to 14V, 150mA typical)
D0	Wiegand D0 line
D1	Wiegand D1 line
LED	LED control (high or floating for red, low for green)

The HOLD line can be used to buffer the output data, if there is a suitable signal available.

For details of other output formats refer to Appendix A. This includes the relay connections which are only provided on RS232 output readers.

The reader has the option of an isolated output section. For details of how to use this refer to Appendix B.

*3.4 **Mounting***

3.4.1 Select a convenient position at a suitable height for the Reader. Bear in mind how Cryptags will be worn.

3.4.2 Using the template supplied drill the fixing holes and cable entry hole. The cable entry hole should be 13mm (½ inch) diameter. The holes for the fixings will depend on the surface to which the Reader is to be fixed.

3.4.3 If the Reader has the anti-tamper option fitted, the wall mounting magnet must also be fitted at the location shown on the template.

3.4.4 Run the Cable. If there is any possibility of tension on the cable remove the PCB from the back-plate and fit a suitable clamp on the cable, before refitting the board.

3.4.5 Mount the Reader Assembly to the wall, bringing the cable through the hole in the reader.

3.4.6 Connect the cable to the terminal block. The cable should not be run across the back of the Reader itself. Also, as the Reader will normally be on the insecure side, the cable should not be accessible from that side.

3.4.7 If the Reader is not to be commissioned immediately replace the cover on the Reader.

*3.5 **Commissioning***

If any problems are experienced during commissioning, refer to the Trouble-shooting Section (Section 4)

3.5.1 If necessary remove the cover. Check the following-

Wiring is correct and secure

Links are correctly positioned

If there is no wire to 5V(W) then LK1 and LK2 should be in. There need be no wire to 0V(W), which is connected to 0V.

If there is a wire to 5V(W) but no wire to 0V(W) then LK1 should be in and LK2 should be out.

If there are wires to 5V(W) and 0V(W) then both links should be out.

Potentiometers are fully clockwise.

A range of suitable **Cryptags** is available.

If the anti-tamper option is being used it is best to short the terminals for the time being.

For **RL3** readers, ensure that the **look-up table** has been loaded. (Appendix C.)

3.5.2 Apply power to the system. The red indicator LED (LED1) should come on. Green (on LED2) means that the LED input is being pulled low.

3.5.3 Ensure that there are no Cryptags close to the Reader

If the internal LED (LED3) is on at all, turn RV3 anticlockwise until LED 3 is permanently off. (If there are no Cryptags present LED 3 will only light if there is external interference. Reducing receiver sensitivity using RV3 will eliminate interference, but it may also affect the range.)

3.5.4 Bring a Cryptag towards the Reader from the front with its face parallel to the Reader. When LED 3 starts to flash the Cryptag is being read. This indicates the range of the reader.

3.5.5 If the range is greater than desired, reduce the transmitter power output using RV2 until the desired range is achieved.

3.5.6. RV3 should be adjusted for best performance. Repeat 3.5.3. and note the position of RV3.

Now position a Cryptag at the desired range and reduce RV3 until LED3 ceases to flash. Note this position, which should be anticlockwise of the position noted above. Set RV3 approximately halfway between the two positions.

3.5.7. Now carry out system checks with the equipment to which the Reader is connected. (In the Fault Finding this is referred to as the controller)

3.5.8 If the anti-tamper option is fitted, remove the shorting links. Check that the circuit is closed when the cover is placed on the reader.

3.5.9 Replace the cover and fit the 4 screws. If Security Screws are to be used, now is the time to fit them.

If the reader is mounted externally cover the screw heads with silicone rubber sealant. Also use silicone rubber sealant to seal the gap between the Reader and the wall, but leave a small section unsealed on the bottom edge to allow for drainage.

*3.6 **Warning Labels***

Each Reader is supplied with a Warning Label which identifies a Cryptag Control Zone and advises against loitering. These labels are particularly recommended for situations where Active Cryptags might be left in the vicinity of a reader.

4. TROUBLE-SHOOTING

The equipment to which the reader is connected is referred to here as the controller. The controller is expected to receive the output signal (Wiegand, RS232 or Clock/Data as applicable). It should also control the external LEDs.

The external LED indicators will either indicate red or green. If one goes out the other should come on. It may be possible for them both to appear to be lit, if an a.c. waveform is transmitted.

4.1 **No indicating LED on** (both LED1 and LED2 off when power applied)

Check: +5V(W) with respect to 0(W).

If 5V is not present - Check wiring and links LK1, LK2

If 5V is present - Replace Reader

4.2. **LED3 does not come on when Cryptag presented**

Check: +12V with respect to 0V (not 0V(W)).

If 12V is not present - Check wiring to Reader

If 12V is present - Either Cryptag or Reader is faulty

Check: Adjustment of RV2 and RV3 (See Commissioning section.)

4.3 **LED3 permanently flickering**

Re-adjust RV3 (See Commissioning Section)
If LED3 is beating steadily, look for a tag within range of the reader.

4.4 **LED3 responds to tag but no response by Controller**

Check: Cryptags are valid for this Reader (refer to Appendix A for RL1 and Appendix C for RL3.)

Check: Wiring to Reader and correct if necessary.

Check: Is Hold line high. If it is low (<2.5V) the Reader will not transmit data .

NOTE: The presence of pulses could be tested with a Logic Probe or oscilloscope.

4.5 **Indicating Red/Green LEDs not operating** (always in the same state)

Check: Voltage on LED input

If voltage is +5V - red LED should be on

If voltage is 0V - Green LED should be on.

The operation of the LEDs can be checked by removing the connection to the LED input. The red LED should be on. Now short the LED input to 0V(W). The green LED should come on (and the red LED go off).

4.6 **Range insufficient**

Check: Is the Reader mounted on metal?

If so then range can be improved by lifting the Reader off the metal

Try connecting GND to the metal (only helps sometimes).

Check: Adjustment of RV2 and RV3 (See Commissioning Section)

Check: Tag orientation is correct (including rotation in its own plane)

4.7 **Unreliable or Slow Reading**

Check: Adjustment of RV3 (See Commissioning Section)

Try connecting GND to metal.

Check: Tag orientation is correct (including rotation in its own plane)

4.8 **Anti-tamper circuit open circuit.**

Check: Micro-switch is operated when cover put on Reader

Check: Reed Switch is closed. Is the magnet correctly located on the wall behind the reed switch?

5. TECHNICAL

5.1 Principles of operation

The reader contains a transmitter and a receiver, both under the control of a processor.

The transmitter sends out signals that will be picked up by any Cryptag in its vicinity. Each Cryptag will respond and a dialogue takes place which identifies the Cryptag. The nature of the dialogue is well disciplined so that more than one Cryptag can be interrogated and correctly read without interaction.

After the interrogation dialogue the Reader communicates the identity of valid tags it has seen. Tag transmissions are buffered.

5.2 Reading Range

The reading range with an active Cryptag (TM1) is 900mm (35 inches). Range quoted is typical under optimum conditions and with the 12V supply at nominal. Normal variation is $\pm$ 10%.

The range at which a Cryptag will be identified is affected by -

Cryptag orientation - Figures quoted assume optimum orientation. Rotating through 45^0 reduces the range by about 15%. At exactly 90^0 tags will not be read at all. The optimum orientation varies around the reader.

Presence of metal - The Reader should not be mounted directly on or near a metal surface. As well as reducing range metal will increase power consumption.

Electrical interference - The transmission from Cryptag to Reader is at low power and may be affected by sources of electrical interference such as computer monitors.

The range of the Reader can be deliberately reduced. There is a potentiometer to reduce the power of transmissions to the tag and therefore reduce range. Another potentiometer reduces the input sensitivity of the receiver. This eliminates interference, and in some cases reducing the sensitivity may increase the range.

5.3 Dimensions

Height 232mm (9.1 inches)

Width 232mm (9.1 inches)

Depth 39mm (1.5 inches)

Weight 1.3kg (2.9lb)

5.4 ***Environmental***

Temperature	-20^0 to + 60^0C (-4^0F to 140^0F)
Housing Material	Glass filled plastic (Flame Retardant)
Mounting	Normally vertical on internal or external walls. When used externally the reader should be sealed using silicone rubber as described in the installation section.

5.5 ***Electrical***

5.5.1 Power Input	12V nominal (10.5V to 14V) 150mA typical, 175mA maximum including 15mA interface circuit current. (Current measured at nominal supply voltage, maximum transmitter power, no tags present and with the reader on a non-metallic surface.) If the reader is mounted 1cm from a metal surface, the current consumption can rise to 250mA maximum.

5.5.2 Outputs (see Figure 2 for interface circuits)

Data Output	DATA0 and DATA1 lines. Normally high (+5V), pulsing to low 0.4V. Format - See Appendix A. 1k ohms pull-up to 5V(W). In Wiegand and Clock/Data readers the data lines **cannot handle more than 5mA maximum**.
LED	Input impedance 100k ohms pull-up to + 5V(W) High or floating for RED Low for GREEN Nominal switching level 2.5V.
HOLD	Input impedance 100k ohms pull-up to 5V(W) Input capacitance 1nF High or floating for Data output Low to freeze data output transmission Nominal switching level 2.5V (**NOTE**. If HOLD goes low during a transmission, that transmission will continue to completion.)
Data Buffer	Up to 10 tags can be stored. This limits the number of tags that can be identified simultaneously.
Max Voltage	The + 5V(W) input must never exceed 6.5V Other data lines (DATA0, DATA1, LED, HOLD) must not fall below - 0.3V or above 6.5V. Protection circuits are incorporated to prevent damage from transient spikes (above normal EMC limits).

Cable Length	Wiegand and Clock/Data - 100m (300 ft) maximum. (**NOTE**. Cable length may also be limited by the equipment at the other end.) RS232 - 20m (60 ft) maximum (9600 baud)
Output Timing	When the Cryptag has been read its identity is stored. The identity data is buffered to ensure that there is a minimum inter-burst period between a pair of data transmissions. The inter-burst time is configurable, and the standard value is 100ms. (See Appendix A).
Interrogation Time	230ms maximum per Cryptag. This may increase in the presence of interfering signals.
Transmission Time	Nominally 1ms per bit, but can be altered on request. (See Appendix A.)
Pulse Width	Nominally 50 µs.

5.5.3. Radio Transmissions

Reader to tag	132kHz carrier Magnetic field, <40db µA/m at 10m
Tag to reader	66kHz (Phase locked to 132kHz) Magnetic field, <-10db µA/m at 10m.

5.5.4 EMC

Emission	Exempt according to MPT1337 (Dept of Trade and Industry)
Susceptibility	Not affected by 4kV, 150ns pulses (such as defined by IEC Standard 801-4, 1988)

Screened cable is not normally required, but may be used. (Tested without screened cable.)

5.5.5 Anti-Tamper Option

The reader can be supplied with an anti-tamper loop containing a micro-switch to detect cover removal, and a reed switch to detect removal from wall. A magnet is supplied, for wall fixing, to operate the reed switch. Contacts are shorted in the secure state.

5.6 ***Cryptags***

Current Cryptag types are:

TM1 personnel tag
TA1 article tag
TK3 keyfob tag (replaceable battery)

All of these are active (battery powered) tags.

All Cryptags have a Public Identity (PID) of 16 bits and a Hidden Identity (HID) which is theoretically 16 bits, but in practice one bit cannot be identified and the useful size is 15 bits. The identity of the Cryptag is a total of 31 bits giving 2 billion possible identities.

Current production tags are programmed by Identec and can be supplied with sequential numbers. Once the identity has been programmed it cannot be altered, and tag identities are not duplicated.

Older (pre 1999) tags had a fixed identity. In order to obtain sequential numbering with older tags it is necessary to use an RL3 reader with its look-up table, as described in Appendix C.

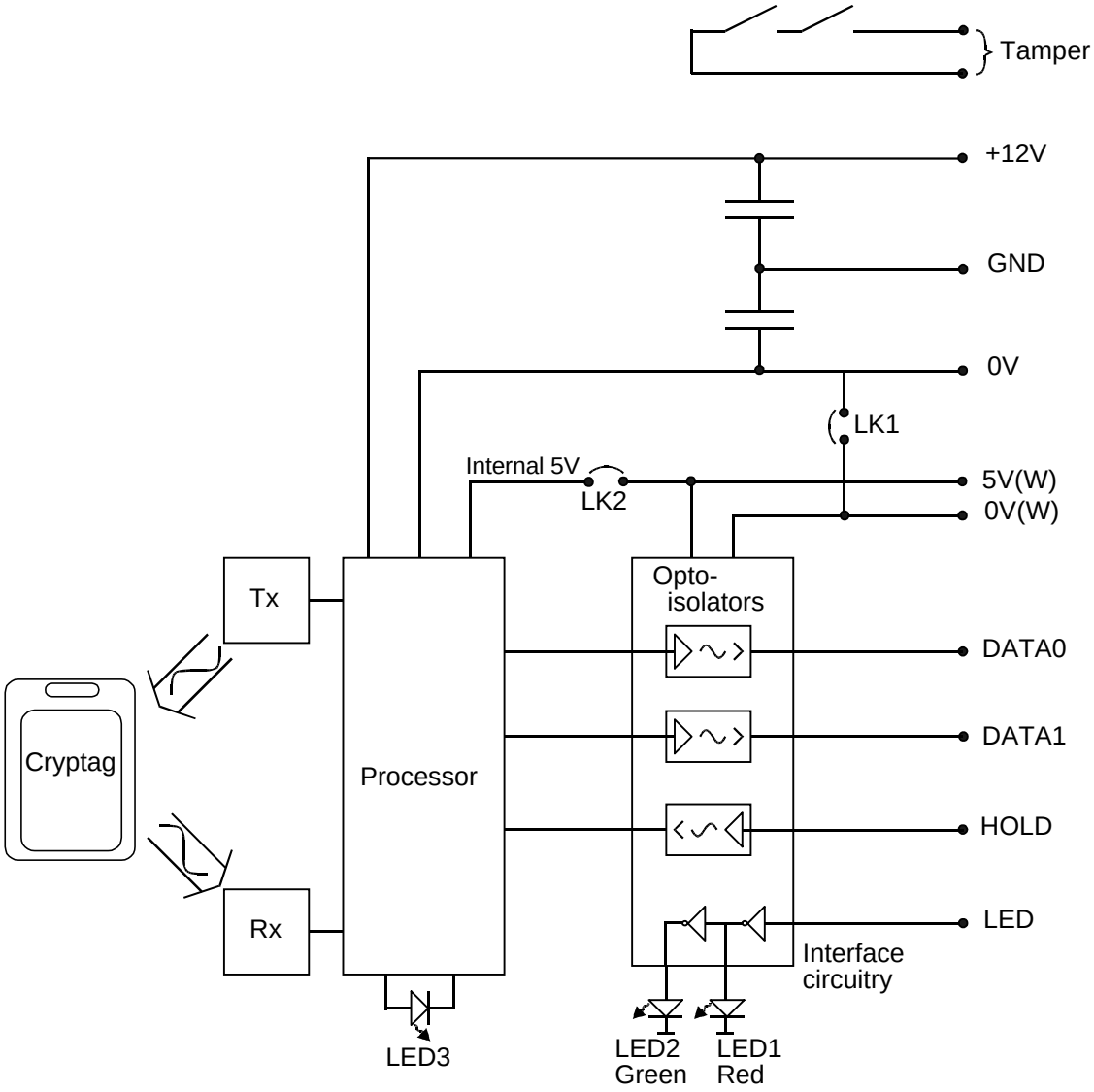
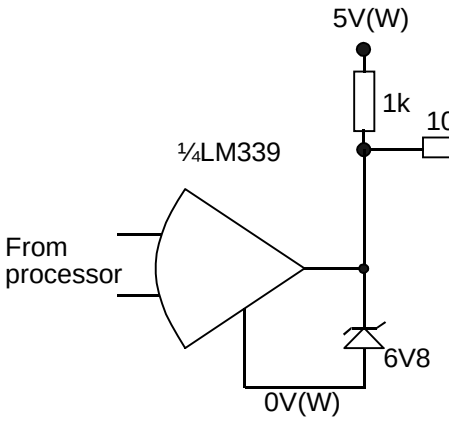


Figure 1 Reader Block Diagram

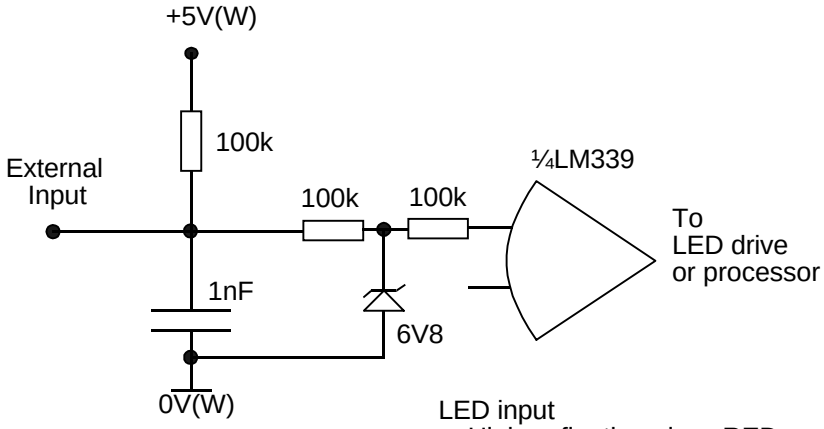
Wiegand outputs (also Clock/Data, but not RS232)



Wiegand output
- Normally high
- Pulses low on relevant line for each bit
- Each pulse is 50µs long
- Typical pulse separation 1ms

Clock/Data output
- Clock on Data 1 line pulses for each bit
- Data (Data0 line) is inverted
- Data is valid while Clock low
- Card Present (on Relay NO) is low throughout the transmission

LED and Hold inputs



LED input
- High or floating gives RED
- Low gives GREEN

HOLD input
- High or floating has no effect
- Low inhibits output data
- If HOLD goes low during a transmission the transmission will be completed.

Fig 2: Interfaces

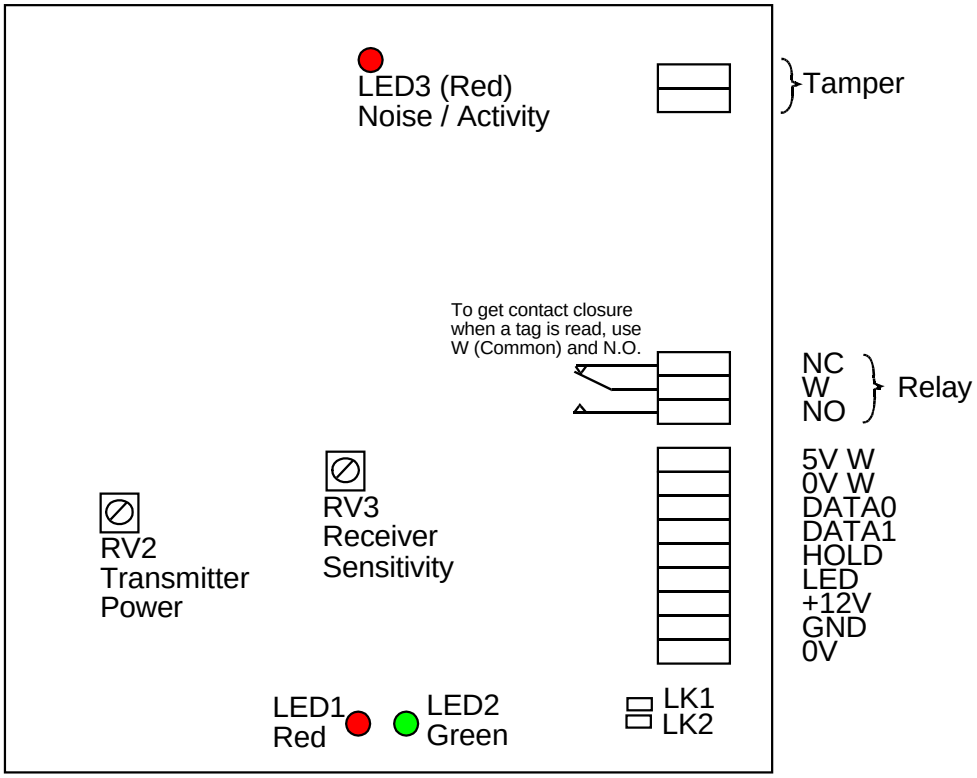


Figure 3: Connections etc.

APPENDIX A

Output Formats and Data connections

The output format of the reader is configurable. This appendix gives some typical formats and the terminal connections to use.

*A.1 **Wiegand output***

The number of bits and their allocation is usually customer specific, but some RL1 readers are supplied with a standard 26 bit format.

Output bit	
1	Even parity on Bits 1-13
2-9	Hidden Identity (least significant byte)
10-25	Public Identity
26	Odd parity on Bits 14-26

The most significant part of the Hidden Identity (HID) is ignored. (On some RL1 readers, it will be checked so only tags with some HIDs will be reported.)
Tags are reported when they are first seen, and then only if the tag has been out of the field for at least 2 seconds.

Timing 1 ms bit period
50µs bit low pulse for each bit

Buffering The reader ensures a minimum period (100ms) between transmissions. This ensures that the controller does not confuse the two transmissions.

With current Cryptags the tag numbers are programmed to suit customer requirements. If older tags (pre 1999) are present on the site there is a possibility of numbering problems if the Access Control system is not sufficiently flexible. Two ways to avoid these are

a) Use RL3 readers, as described in Appendix C.

b) Make the user number as long as possible (ideally 31bits) and derive the tag number from the tag's identity

Tag number = HID * 65536 + PID

*A.2 **RS232 output***

The standard output format is 9600 baud, 8 data bits, no parity and one stop bit. The data transmitted is

HID:HHHH PID:PPPPP<LF><CR>

Where HHHH is the Hidden Identity in hexadecimal, and PPPPP is the Public Identity in decimal, <LF> is line feed and <CR> is carriage return.

The RS232 output is on the D0 terminal. The D1 terminal is not used. RS232 readers have a single pole relay fitted, as shown in Figure 3. The HOLD input has no effect on RS232 readers.

A.3 ***Clock/Data output***

This format emulates magnetic stripe card readers, and is supplied to conform to specific customer requirements. For details of the encoding format, contact Identec.

Terminals for Clock/Data output readers

D0	Data output (inverted data)
D1	Clock output (Data output is valid while Clock is low)
Relay NC	Card Present (low throughout data transmission)

APPENDIX B

Power Supplies and Earthing

This Appendix explains the options available, when they should be used, and how to implement them.

*B.1 **Circuitry***

Refer to Figure 1 (Block Diagram).

The reader has two sets of Circuitry, which are electrically isolated using opto-isolators.

Reader Electronics -	Connected to 0V
	+12V
Output Interface -	Connected to 0V(W)
	+5V(W)

The ground connection (GND) is connected via 1nF capacitors to 0V and +12V.

The other connections (DATA 0, DATA 1, LED, and HOLD) are connected to the Interface Circuitry, and must be referenced to 0V(W)

The Reader electronics contain a 5V regulator. This can also be used to supply the Interface Circuitry

There are two links related to the power supplies -

LK1 connects 0V and 0V(W)
LK2 connects 5V(W) to the Reader's own 5V

*B.2 **Normal Arrangement** (Interface powered internally)*

In this arrangement the external connections are -

0V	LK1 In
+12V	LK2 In
DATA 0	
DATA 1	
LED	
HOLD	

0V and 0V(W) are connected by LK1
5V and 5V(W) are connected by LK2

All outputs are referenced to 0V (and to 0V(W)).

This arrangement will be used when the Controller (the unit to which the Reader is connected) can provide a 12V supply with sufficient current.

The 12V supply must be capable of supplying 175mA. If the Reader is mounted on metal the current can rise to 250mA. The current requirement is reduced if the range is reduced using RV2.

B.3. ***Separate 12V supply*** *(non-isolated, with interface powered externally***)**

This arrangement is used when the controller cannot provide the required 12V power and an external supply is used. The 12V supply must not be grounded except through the Reader.

Connections are -

0V	LK1 In
+12V	LK2 Out
+5V (W)	
DATA 0	
DATA 1	
LED	
HOLD	

0V and 0V(W) are connected by LK1. It is best to use the 0V connection.
5V(W) is supplied separately by the controller so LK2 is out.

The outputs are referenced to 0V (and to 0V(W)).

The 12V supply must be capable of supplying 165mA. If the Reader is mounted on metal the current can rise to 240mA. The current requirement is reduced if the range is reduced using RV2.

The 5V Interface Circuitry supply current (taken from the controller) will be 15mA.

B.4 ***Totally Isolated***

This arrangement is used when the Reader and/or its 12V supply must be totally isolated from the interface to the controller. A typical case will be when the 12V supply is shared, and the other use must itself ground the 0V line.

Connections are -

0V	LK1 Out
+12V	LK2 Out
0V(W)	
+5V(W)	
DATA 0	
DATA 1	
LED	
HOLD	

Interface circuitry connections are referenced to 0V(W) and not 0V.

The 12V supply must be capable of supply 165mA. If the Reader is mounted on metal the current can rise to 240mA. The current requirement is reduced if the range is reduced using RV2.

The 5V Interface Circuitry supply current will be 15mA max.

B.5. ***Ground***

The GND connection can be connected to local metal objects. This may improve range if the Reader is affected by some types of interference.

APPENDIX C

RL3 Look-up Table

This section applies to RL3 readers only. RL1 readers report the tag's identity number.

C.1 Introduction

Cryptags have a unique identity number. In current production Cryptags this is programmed into tags before they are shipped, but in earlier (pre 1999) Cryptags the number was put in at an earlier stage. This meant that it was not possible to supply tags with particular numbers. Many Access Control systems do not have the flexibility to handle what are effectively random numbers, and the RL3 reader was introduced to provide sufficient flexibility for those applications.

The RL3 reader contains a look-up table in non-volatile memory. This stores the identities of tags which are valid for that site, together with the number that is to be reported for that tag. The numbers are reported as a Site Code (fixed for the site) and a User Number which is normally sequential.

The look-up table can be programmed into the RL3 reader in two different ways.

1. using ENCODER STATION LE1
2. using MASTER TAG MT1

Normally readers are configured initially using an LE1 Encoder Station, and the MT1 is a portable "encoder" used for updating installed readers.

C.2 ***Operation of Encoder LE1*** *(for full instructions see LE1 Operational Manual)*

The LE1 Encoder is used before a batch of tags and RL3 readers is shipped. The tags within the shipment are loaded into the encoder. Each tag is then given a small label which identifies its User Number.

The look-up table is downloaded into each of the readers for that shipment. Only readers that have the correct look-up table downloaded into them will report the tags correctly.

The look-up table can also be downloaded into an MT1 Master Tag. The look-up table can then be downloaded into existing readers on site.

C.3 ***Operation of Master Tag MT1***

The MT1 Master Tag is most commonly used to upgrade an existing installation, for instance to add more tags. This will only work if the MT1 Master Tag is correctly programmed for that reader, so that a Master Tag is site specific. It is not necessary to remove the reader's cover before using the Master Tag..

Master Tag Operations during upload

	Master Tag indications RED	GREEN
Initially	OFF	OFF
Present in field, power up and data integrity test	ON	ON
Test Passed	OFF	ON for 5 seconds maximum If this state persists the Site Code is incorrect. Contact Identec.
Loading	OFF	Flashing (on & off equal times)
Load Finished	OFF	Flashing (on 3 times more than off) (Continued for 10 seconds after leaving field)
Red Led – Error message	RED	GREEN
Power up test failed	ON	OFF
Battery Low	ON	Flashing (on & off equal times)
Loading (Bad Frames)	ON OFF (Alternating)	OFF ON
Load Failed	FLASHING (on 3 times longer than off)	OFF

Power Up Test Failed

Remove Master Tag from field and wait till no LEDs are on.
Reintroduce to field

If it fails again try a different Reader. Failure again means:-

a) Wrong Master Tag
b) Fault in Master Tag
c) Very low battery
d) Reader transmit power set close to minimum

Battery Low
OK for one reader upload but replace battery before next reader. Disconnecting the battery will not affect the stored data.

Bad Frame
This is OK but not recommended. Your master Tag will keep trying if it loads a bad frame. The more red light you see in general the harder it is finding it to upload so try a different position of the Master Tag relative to the Reader.

Load failed
Try again after removing the tag from the field.

Try a different Reader to see if the fault is in the Tag or the Reader

Report any difficulty to your supplier

*C.4 **Example of Look Up Table.***

Tag number		User number
HID (Hexadecimal)	**PID (Decimal)**	**(Decimal)**
000D	00100	0001
0AAF	64436	0002
BDCE	37000	0003
000A	00010	0004
OA01	01952	0005
881F	26534	0006
6654	32212	0007
1010	11414	0008
		0009

Next Tag will be 0009