FlexiPanel

OpenTooth™

Bluetooth device sensor for access control and personnel tracking

Summary

OpenTooth detects and recognizes Bluetooth devices within a 10m range, allowing OEMs to add Bluetooth capability to access control products.

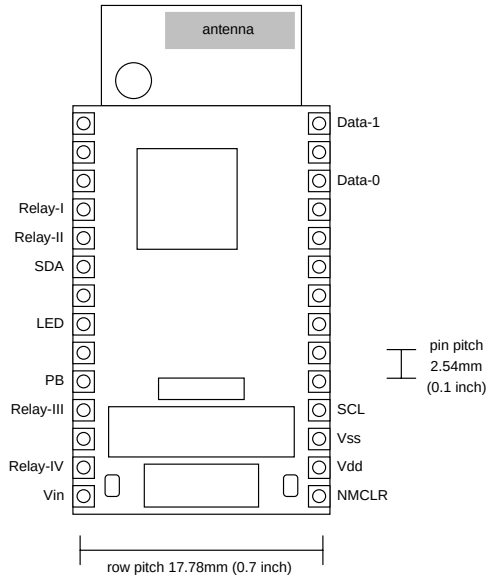
Applications

- ***Manual lock release*** – pulses relay when trusted device present and button pressed.
- ***Automatic lock release*** – pulses relay while trusted device present.
- ***Alarm deactivation*** – relay energizes while trusted device present.
- ***Wiegand "card reader"*** – if button pressed, sends Wiegand codes of all devices present.
- ***Personnel location tracker*** – sends Wiegand codes of all devices present at regular intervals.

Hardware Features

- FCC / CE / IC certified Class II Bluetooth V1.1 radio, 10m range, integral antenna.
- Relay, pushbutton and LED I/O pins for standalone operation.
- Weigand Data-0 and Data-1 outputs for networked access control.
- Real time clock with daylight savings time.
- Onboard power regulator, 5V – 10V supply.

phone and module not to scale



Firmware Features – Standalone

- New users can register their devices if they know the 'new user' PIN code.
- Up to 255 trusted devices.
- Registered devices can be managed from any Bluetooth-enabled Windows PC, Pocket PC, or high-end mobile phone.
- Trusted devices can be configured for time-of-day, day-of-week access and expiry date.
- On-board access log records recent access information.

Firmware Features – Networked

- 26-bit or 50-bit Weigand code of devices requesting access or all detected devices.

Customization

- Firmware C source code and customization services available.

Manufactured to ISO9001:2000

Ordering Information

Part No	***Description***
	OpenTooth 28-pin Dual-in-Line package Evaluation Version
	OpenTooth 28-pin Dual-in-Line package – Custom firmware xxx

Pin Descriptions

Pin Name	*Description*
Data-0	Weigand Data 0 output drives up to 25mA (see notes 2,4)
Data-1	Weigand Data 1 output drives up to 25mA (see notes 2,4)
LED	LED output, on while a trusted device is present. Pulses every 15 seconds to confirm correct operation. Active high and drives up to 25mA (see note 2)
NMCLR	50ms pulse low to reset. May be left unconnected.
PB	Pushbutton input for requesting access and/or entering setup modes. Active high.
Relay-I	Relay output I. Active high and drives up to 25mA (see notes 2,3)
Relay-II	Relay output II. Active high and drives up to 25mA (see notes 2,3)
Relay-III	Relay output III. Active high and drives up to 25mA (see notes 2,3)
Relay-IV	Relay output IV. Active high and drives up to 25mA (see notes 2,3)
SCL	To I2C external memory (customized versions only).
SDA	To I2C external memory (customized versions only).
Vdd	Regulated power +5V (see note 1,2)
Vin	Unregulated power input +5 to +10V (see note 1)
Vss	Power ground reference

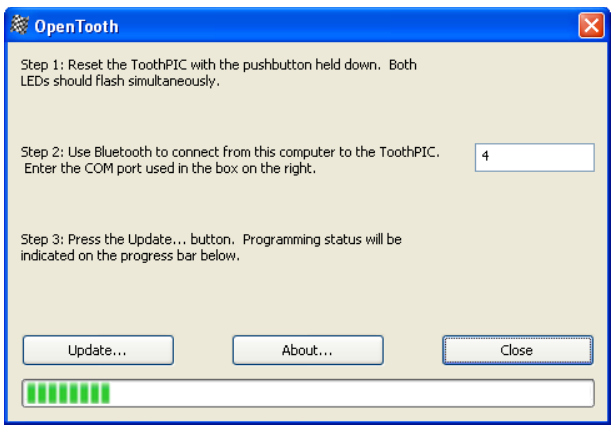
1. Either *(i)* regulated power should be provided on Vdd and Vin left unconnected or *(ii)* unregulated power should be provided on Vin and Vdd may be used as a regulated power output.
2. If on-board power regulator used, total current draw on all outputs (including Vdd if used as a regulated power output) shall not exceed 130mA.
3. Relay outputs I – IV act in unison and may be tied together to drive loads of up to 100mA.
4. Outputs are inverted (i.e. usually low, active high) so they are correct after drive transistors. Opposite polarity is a possible customized feature.

Initialization and Customization

OpenTooth is based upon the ToothPIC module from FlexiPanel Ltd. The Evaluation Version is intended for OEMs to use to evaluate the technology prior to customizing to their product lines.

The OpenTooth Evaluation Version is supplied as a ToothPIC module which must be 'Field Programmed'. This takes a few seconds and requires either a Windows PC or a Pocket PC with Bluetooth. This is not necessary for customized firmware versions. The procedure is as follows:

1. Download the ToothPIC Development Kit from *www.flexipanel.com* and locate the OpenTooth Service Pack `OpenToothWin.exe` (Windows) or `OpenToothPPC.exe` (Pocket PC).
2. Power-up the ToothPIC with the on-board pushbutton held down. The on-board LEDs will flash simultaneously.
3. Start running the OpenTooth Service Pack and connect from the computer to the ToothPIC using Bluetooth.
4. Enter the COM port used to connect to the ToothPIC in the box provided.



5. Press the Update button. Programming takes about 30 seconds. When the progress bar is full, field programming is complete.

Note: The OpenTooth Evaluation Version may be supplied with a Class I radio with 100m range. Since most phones *etc* are Class II devices, they will only be detected within a 10m range and operation will not be noticeably different. In production quantities, a Class II device is preferred to improve RF channel availability.

Operating Configurations

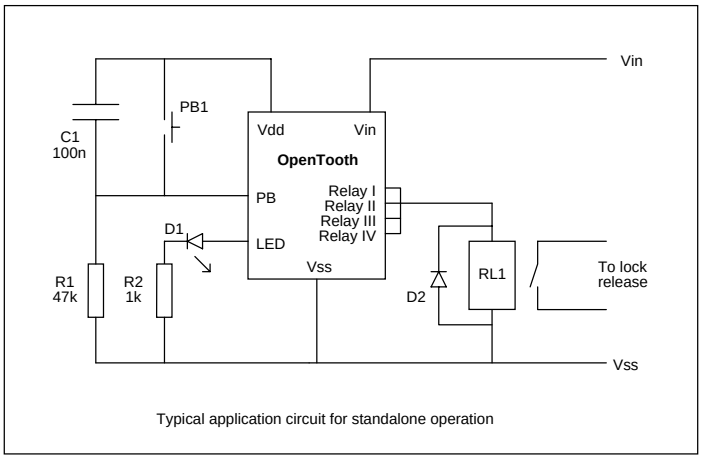
OpenTooth can be used as a standalone unit or as part of a networked access control system.

In ***Standalone Operation***, OpenTooth lights an LED when a trusted device is present. While the trusted device is present, a relay can be *(i)* pulsed to provide access immediately (default), *(ii)* pulsed to provide access if a pushbutton is pressed, or *(iii)* energized to disable an alarm. New users register by pairing using a secret PIN code. Settings are managed by connecting to OpenTooth from a Windows PC or Pocket PC (or certain high-end phones).

In ***Networked Operation***, OpenTooth transmits information about the detected Bluetooth devices to a central computer using the industry standard Weigand data format. Proprietary formats can be provided as a customization feature. In access control applications, detected devices are be transmitted to the central computer when a pushbutton is pressed, just like a standard Weigand card reader except that no card is required. The central computer decides whether or not to provide access. For personnel tracking applications, detected devices are transmitted to the central computer at regular intervals. This allows the central computer to track users within a building using an existing Weigand security network

Standalone Operation

A typical application circuit for standalone operation is shown in the adjacent figure. D1 is an LED which pulses briefly every 15 seconds during normal operation. Pushbutton PB1 is de-bounced by C1 and R1.



Typical application circuit for standalone operation

To register, for example, a new phone, press the pushbutton repeatedly until the LED flashes. Use the Bluetooth on your phone to search for OpenTooth and pair with it. Pairing may be called *bonding* or *trusted devices* depending on the phone. You will need to enter the New User PIN code (the initial setting is 1234). Once pairing is complete you may delete OpenTooth from the phone's list of paired devices – OpenTooth will still remember it. New users registered in this way stay registered for six months and are then automatically deleted. If you do not pair with any device within five minutes, or if you press the button again, OpenTooth will reset.

Once a new device is registered, LED1 will light whenever it is present and, by default, relay RL1 will trigger once every 15 seconds to provide access. If, for some reason, the user wishes stay in range, they may temporarily disable the relay by pressing the button. Normal service will resume when the user is no longer present or the relay is pressed again.

To configure OpenTooth in a more detailed manner it is necessary to connect to it using FlexiPanel Client software. This is available for Windows PCs, Pocket PCs and high-end mobile phones. It is freely distributable and may be downloaded from www.FlexiPanel.com. To connect to OpenTooth, press and hold the button for five seconds until the LED flashes. Then search for and connect to OpenTooth from the computer running FlexiPanel Client software. A Configuration PIN must be entered. This can be different from the New User PIN. The initial setting is 0000.

Once connected, the Registered Users screen will list the registered users. Press Add to add a new user and the Add User screen is displayed.

The Add User screen shows a list of the Bluetooth devices most recently detected. Choose one and press Select. The new user will be added to the list of users and the Modify User screen will be displayed for the new user.

The Modify User screen is also displayed from the Registered Users screen if you select a user and press Modify. Pressing Delete will remove the user from the list.

The Modify User screens allow the registered user's name to be changed and also the date when they will be automatically removed from the user list. Note that users added using the FlexiPanel Client rather than the New User PIN do not expire for 50 years by default. It is also possible to specify the time of day and/or week when the user is allowed access.

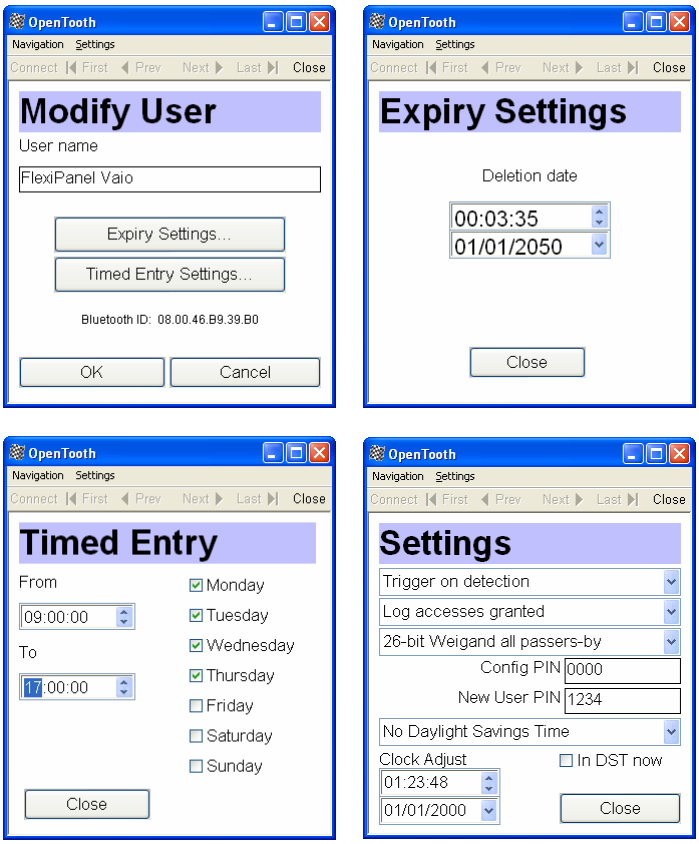
From the Registered Users screen, press Settings to show the Settings screen, which allows the following to be configured:

Automatic Lock Release: Where the relay is triggered when a trusted device is present.

Manual Lock Release: Where the relay is triggered when a trusted device is present and the button is pressed.

Alarm Deactivation: Where the relay is energized while a trusted device is present.

Access Log: Records accesses granted, all devices detected or nothing at all.



Weigand Card Reader Mode: The Weigand code of all devices present is transmitted when the button is pressed.

Personnel Tracking Mode: The Weigand code of all devices present is transmitted regularly.

PIN Codes: For configuration from a FlexiPanel Client and for registering new users.

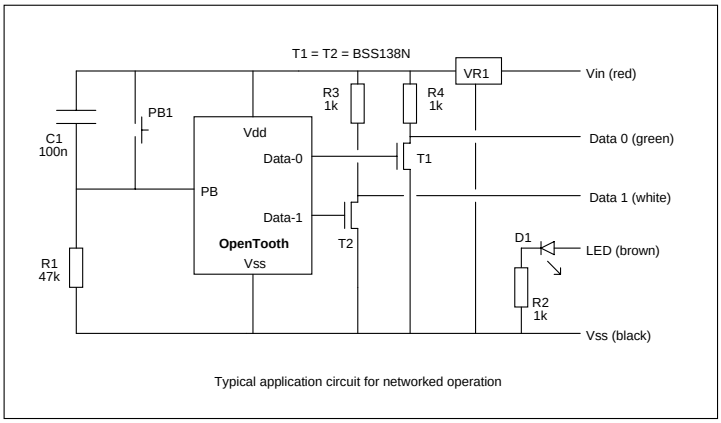
Clock Settings: For adjusting the time, date and daylight savings time.

From the Registered Users screen, pressing Access Log will show the list of users recently granted access. Pressing Manual will upload an instruction manual in HTML format to the computer running FlexiPanel Client. (This is possible with some FlexiPanel Clients only.) Since the files are stored on OpenTooth, no internet connection is required. However, if the manual is large, external memory may need to be added. This is a relatively simple customization procedure.

Networked Operation

A typical application circuit for networked operation is shown in the adjacent figure. Pushbutton PB1 is de-bounced by C1 and R1. Configuration from a FlexiPanel Client is the same as with Standalone Operation.

The red, green, white, brown and black connections shown are standard Weigand connections as defined by the Security Industry Association (*www.SIAOnline.org*). The green line could be anything from 5V to 24V so voltage regulator VR1 should be appropriate for the supply in use. Some 5V Weigand systems don't have sufficient current rating and a local power supply will be required.



Typical application circuit for networked operation

If Weigand Card Reader Mode is selected, the Data 0 and Data 1 lines transmit the Weigand codes of all devices present when the button is pressed. If Personnel Tracking Mode is selected, all devices detected will be transmitted at regular intervals. If open collector outputs are required, omit resistors R3 and R4.

Bluetooth unique device IDs are 48 bits long. Therefore to transmit absolutely unique Weigand codes, a 50-bit custom Weigand code is used. The first bit is an even parity bit over the first 24 bits of the Bluetooth ID; the last bit is an odd parity bit over the last 24 bits of the Bluetooth ID.

If standard 26-bit Weigand codes are required, these can be selected. While the IDs will not be absolutely unique, the Bluetooth ID is compressed in such a way that there are 16 million possible combinations so duplication is exceedingly unlikely.

Customization

OEMs will probably wish to customize OpenTooth to suit their specific applications. The source code is detailed in the documentation for ToothPIC, available from *www.FlexiPanel.com*. FlexiPanel Ltd can in some cases offer customization services provided the OEM can commit to a minimum order quantity. The 14 unused pins may be configured for custom I/O including analog and counter inputs and PWM outputs.

OpenTooth uses the FlexiPanel Clients for creating user interfaces on remote devices. If you want to change the appearance of the user interface, the FlexiPanel Client software does not need to be modified. This is because user interface is stored on the OpenTooth device itself and transmitted to the client when needed.

Frequently Asked Questions

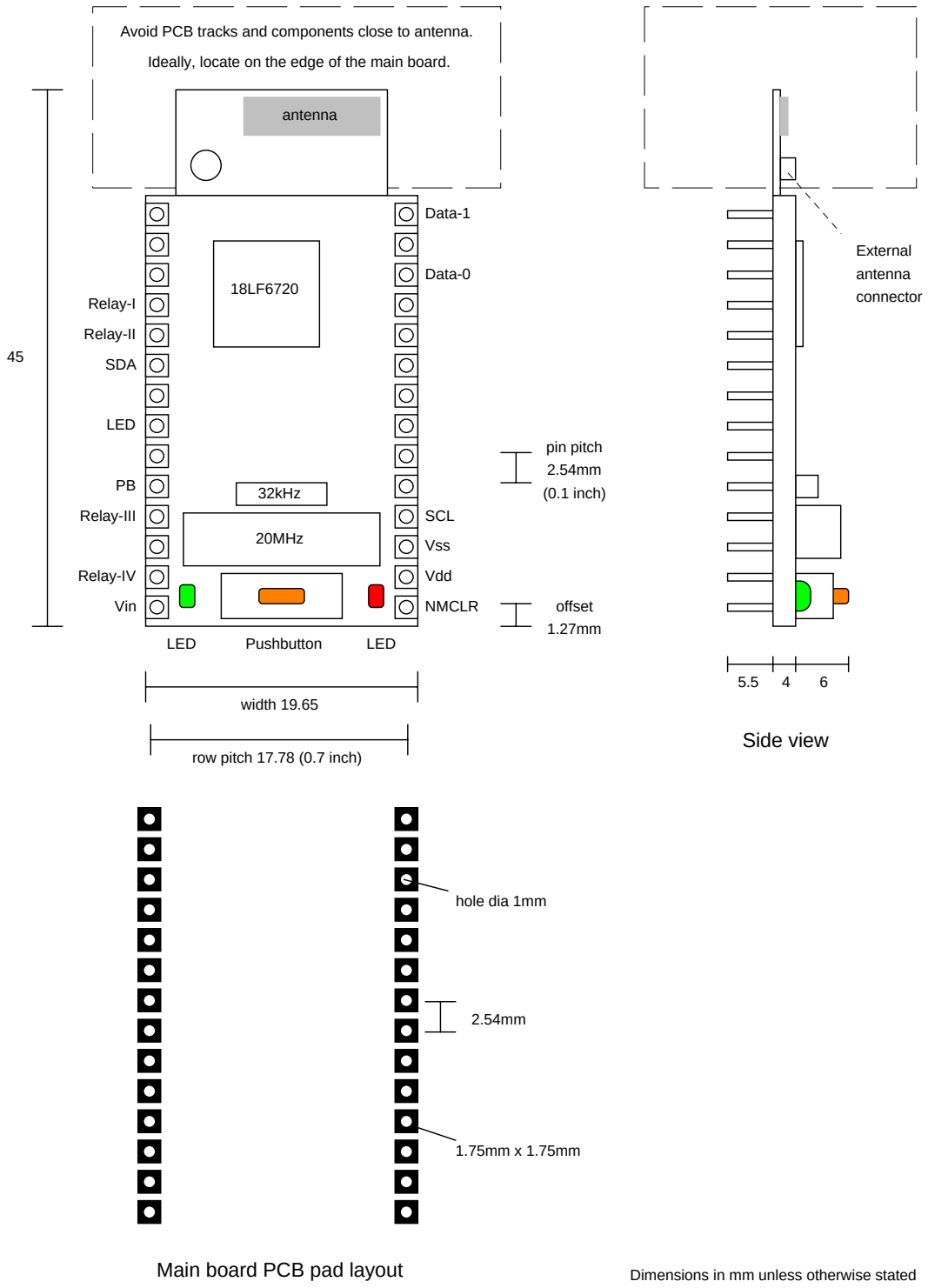
Will it drain the batteries on mobile phones etc? For access control applications, communication with OpenTooth is infrequent and the battery drain will be negligible. For personnel tracking applications, OpenTooth should be configured to scan for devices with a frequency of once per minute or less in order to moderate the drain on permanently present devices.

What if someone does not want to be tracked and/or detected? They can place their phone in its non-discoverable mode where OpenTooth cannot detect it.

Will a metal case reduce the RF range? Yes, but unpredictably. A metal front panel alone should not noticeably reduce the range, but testing is advisable.

How secure are the Bluetooth ID codes? Bluetooth ID codes are very difficult to replicate without reprogramming a Bluetooth transmitter chip. The level of security is greater than cylindrical locks, for example, which most people use to secure their homes.

Mechanical Data



Main board PCB pad layout

Dimensions in mm unless otherwise stated

Notes: Ensure the area where the module is mounted has a solid ground plane. To remove the module from an IC socket or breadboard, lever it out using a screwdriver against the pin headers at the sides. Levering from either end may damage components.

Technical Specifications

Max operating temperature	-20ºC to +75 ºC
Max storage temperature	-30ºC to +85 ºC
Dimensions L × W × H	45mm × 20mm × 10mm excluding pins

Electrical

Supply Voltage (unregulated)	5V to 10V
Supply Voltage (regulated)	4.5V to 5.5V
Peak power requirement excluding draw on I/O pins	270mA
Maximum current on any I/O pin	25mA
Maximum total current on all I/O pins	200mA
Max voltage on I/O pins	-0.5V to +5.5V

Radio

Max RF output power	Class II = 2.5mW = +4dBm (see note 1)
RF frequency range	2402MHz to 2480MHz
RF channels / frequency hop rate	79 / 1600 Hz
Range	10m nominal
Pairing method	Unit link key

1. Evaluation versions may be supplied with Class I radios (100mW).

FCC, CE and IC modular approval

The radio has 'modular approval' for USA, Canada and certain European countries, provided the existing integral antenna is used. The CE mark on the module indicates that it does not require further R&TTE certification. The exterior of the product should be marked as follows:

Contains Transmitter Module FCC ID: CWTUGPZ2
Contains Transmitter Module IC:1788F-UGPZ2

Ordering Contact Details

OpenTooth is manufactured and distributed by

R F Solutions Ltd
Unit 21, Cliffe Industrial Estate,
Lewes, E. Sussex, BN8 6JL, United Kingdom
email : sales@rfsolutions.co.uk
http://www.rfsolutions.co.uk
Tel: +44 (0)1273 898 000, Fax: +44 (0)1273 480 661

Technical Information and Customization Contact Details

OpenTooth is owned and designed by FlexiPanel Ltd:

FlexiPanel

FlexiPanel Ltd
Suite 120, Westbourne Studios
242 Acklam Road
London W10 5JJ, United Kingdom
Tel +44 (0) 20 7524 7774
email: support@flexipanel.com