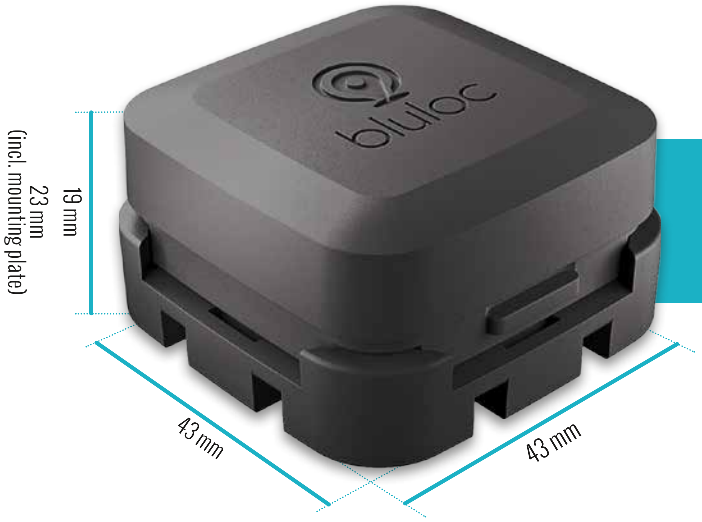
bluloc

BLACKWELL BEACON - SMALL



Bluloc GmbH
Lauterenstraße 37
55116 Mainz

Phone: +49 6131 3272 280
Email: kontakt@bluloc.com
Web: www.bluloc.com

20 g

PROCESSOR	Main	8051 based CC2541 by Texas Instruments
	Memory	256 KB flash, 8 KB RAM
COMMUNICATIONS	Bluetooth	2.4 GHz Bluetooth Low Energy wireless technology
TRANSMISSION POWER	Bluetooth	-23 dBm / -6 dBm / 0 dBm
SENSITIVITY	Bluetooth	-94 dBm
BATTERY AND POWER	Model	CR 2477
	Nominal voltage	3 V
	Nominal capacity	1000 mAh
	Standard load	0.2 mA
	Type	Cell, replaceable
	System	Lithium Manganese
BATTERY LIFE	730 days*	1000 ms Interval, 0 dBm, 0.057 mA
	1736 days*	2000 ms Interval, 0 dBm, 0.024 mA
CASING	Material	Flame resistance
	Color: Anthracite	For custom color please inquire individually.
	Protection	IP 64
ENVIRONMENTAL	Temperature	-30° C / +60° C
	Humidity	from 0 % up to 100 %

* $(C_{nom}/I_{avg})/24$ at 20° C

YOU MIGHT NOT KNOW - BUT YOUR INFRASTRUCTURE CAN ALREADY BE UNDER ATTACK!

BLULOC BEACONS KEEPS YOUR DATA ENCRYPTED

You might think that a Beacon is just a simple device constantly emitting a radio signal that triggers any kind of action inside the fitting App. But as Beacons are rapidly becoming gateways to more & more complicated interactions with financial motivation it is of utmost importance to focus on data security. Take note: All communication with conventional Beacons happened "in the clear" and was not encrypted yet. We changed that.

WE SHOW YOU WHY

There are several ways to attack a beacon infrastructure. And sure there are several reasons to attack.

1. PIGGYBACKING

Piggybacking means that an attacker listens to your beacon and captures your beacons' UUIDs, Majors, and Minors and adds them to his or her application without your consent. You sure do not want your competitor to fare-dodge on your infrastructure. While Piggybacking is just annoying but is not damaging your app or harming your customers cloning is way more dangerous.

2. CLONING

Cloning means that an attacker captures and copies your beacon information and configures another beacon with the captured information. This is extremely dangerous on beacons that triggers any in-app payments or any actions with financial motivation. Also it might make all your analytics on customer data unusable and enable way finding services.

3. HIJACKING

Using unencrypted communication enables hacker to read out the password you use to connect to the beacon. Having read-out the password the Hacker is able to change the password and take control over your infrastructure.

4. CRACKING

Since this a "physical" attack on your infrastructure – and theft – it might seem as a low-probability event and a very special case: It means to remove the beacon, open it and probe the memory or flash the firmware directly. bluloc offers embedded beacons to avoid any physical attacks on your infrastructure.

BLULOC'S CRYPTO-BEACONS FIX YOUR SECURITY LOOPHOLES

Besides all positive facts describing the bluloc standard beacon the Crypto-Beacon sends encrypted information for authorized applications only. While many competitors work on encrypting their Beacon signals bluloc is the only supplier already offering an encryption on a rolling key basis.

Not only the Majors and Minors of your beacons change on a random basis but also the MAC-address of you device. Also the rolling key technology enables you to give your customers access to your infrastructure for limited time without logging them in and out manually.

This works on- and offline making blulocs rolling key technology even more flexible than the new Google EID. Furthermore the bluloc Crypto-Beacons are password secured. The end-to-end-encrypted password is set via maintenance-app.

This innovative solution is vital to protect from the attacks above and to secure confidential information, protecting user against unrequested proximity marketing and to protect you against guerrilla campaigns caused by competitors.