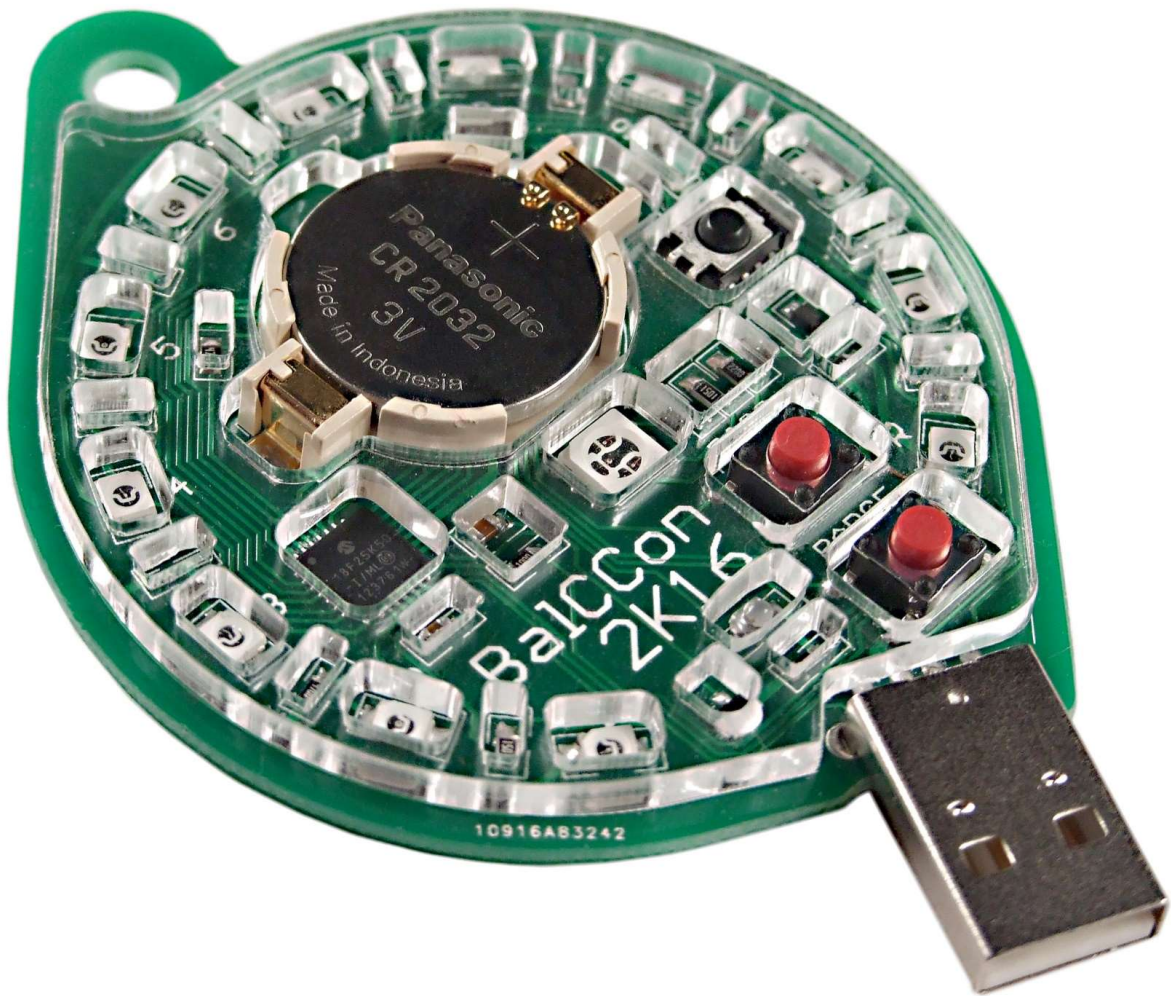
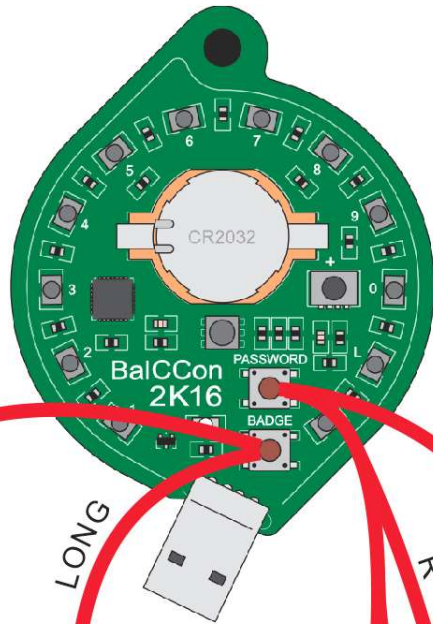


# BalCCon 2K16 Badge



Instructions for use and schematic diagram



**BADGE**

OFF

**TV-B-GONE**

OFF

**SILENT**

**LONG**

**LONG**

**R**

**L**

1 2 3 4 5 6 7 8 9 0

**RETYPE**

**OFF**

**NEW PASSWORD**

**TYPE PASSWORD**

**OFF**

**PAUSE**

**OFF**

**RANDOM STRING**

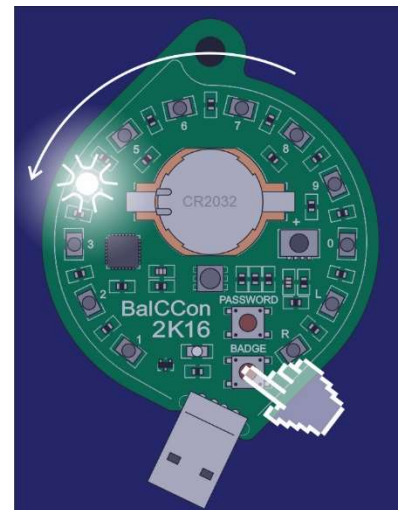
**PASSWORD LIST**

# 1. Badge

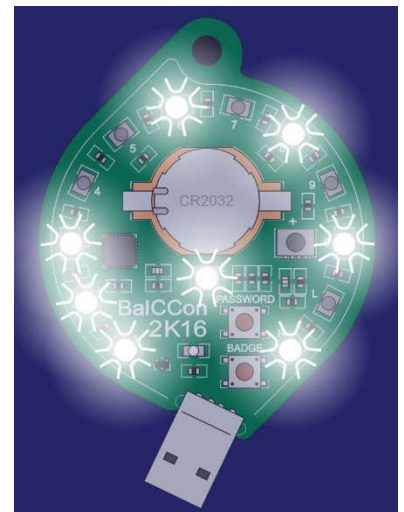
**SWITCH ON:** Press and release the lower button. Rotating LED pattern in CW direction signifies that the unit is ON.



**SWITCH OFF:** Press and release the lower button again. Rotating LED pattern in CCW direction signifies that the unit is OFF.



The unit is now in badge mode, where predefined LED patterns run at random. The badge will continuously seek other badges in the vicinity through infrared communication. When another badge is found and recognized, they will automatically synchronize and start playing an equal pattern in unison.



## 2. TV-B-Gone

**SWITCH ON:** Press the lower button and hold it until the slow RGB pattern on the central LED is replaced by a fast blinking sequence. This signifies TV-B-Gone is on and you may release the button.

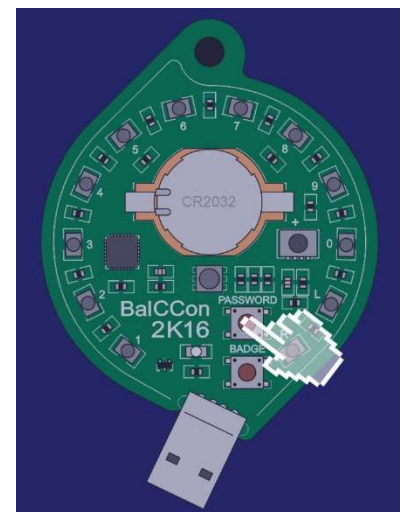


**SWITCH OFF:** The unit will automatically switch OFF after all of the TV codes have been transmitted. You can also switch the badge OFF at any moment by pressing the lower button. Rotating LED pattern in a CCW direction signifies that the unit is OFF.



The unit starts transmitting infrared TV codes when the fast sequence on the central RGB led is finished, and the slow sequence runs.

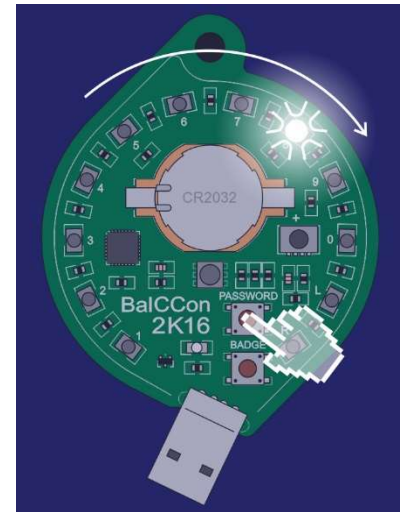
While the unit transmits TV codes, the central LED continuously rotates its colour. If you want to use it in "silent" mode, without displaying anything visible, you can switch OFF/ON the LED indicator by pressing the upper button. Just press and hold it until the LED is switched OFF. The infrared transmitter will continue to transmit TV-OFF codes normally.



TV-B-Gone is a universal remote control device for turning off a large majority — about 85% — of the currently available brands of television sets. It was invented by Mitch Altman, and is sold by his company Cornfield Electronics. *Mr. Altman kindly allowed to use his idea for the Balcon conference. Thanks, Mitch!*

### 3. Password manager

**SWITCH ON:** Press and release the upper button. A Rotating LED pattern in CW direction signifies that the unit is ON.

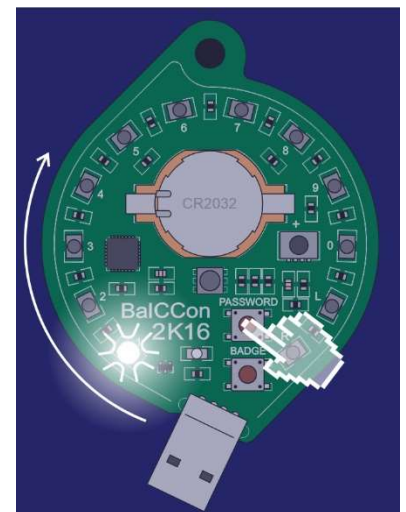


**SWITCH OFF:** The unit is automatically switched OFF after it is disconnected from the USB port. You can also switch it OFF at any moment by pressing the lower button. A Rotating LED pattern in CCW direction signifies that the unit is OFF.



Password manager is the unit which generates, holds and types up to 10 independent passwords, each of them 15...20 characters long. Computer sees it as a standard USB HID keyboard, so it works with every computer which has a USB port, and requires no extra software installation. When you are asked to type the password, simply switch the unit ON, select the desired password and plug it in the USB port.

When the unit is in Password Manager mode, only one LED is on ON. You can press the upper button repeatedly in order to select the desired password (autorepeat is active if you hold the button pressed long enough). LEDs **1, 2, 3... 9, 0** are for ten available passwords, and LEDs **L** and **R** will be described later.



**Note:** USB stack is open-source assembler software, by **Bradley A. Minch**. In the BalCCon Badge project, it was modified so that it accepts uppercase/lowercase characters, servicing <shift> bit in USB packet.

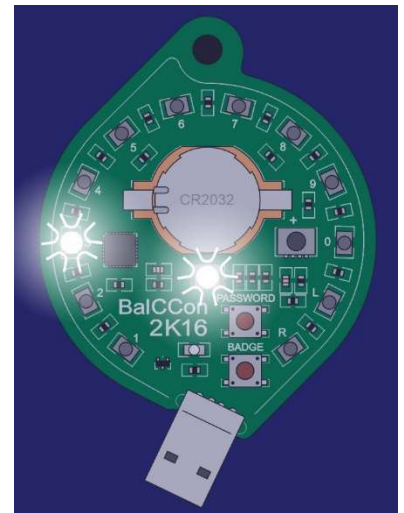
### 3.1 TYPING IN THE PASSWORD TO THE COMPUTER

All you have to do is switch the unit ON in Password Manager mode, select the password (1, 2, 3...9, 0) and plug it in the USB port. When the central LED stops blinking, enumeration process is finished and the password has been typed in the computer. You can retype the same password by pressing the upper button while the unit is plugged in the USB port. After the password has been typed in, you can unplug the unit from the USB port and it will be switched OFF automatically.



### 3.2 GENERATING A NEW PASSWORD

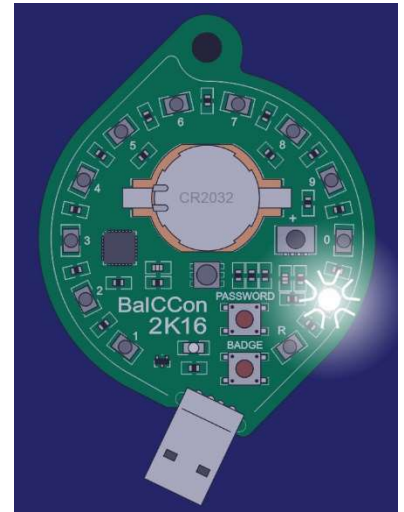
If the unit is switched ON by pressing and holding the upper button instead of releasing it shortly, the central LED lights up in red colour, and you can select the desired password in the same manner. Then you plug it in the USB port and, after the central LED stops blinking, press and release the upper button shortly to confirm that the old password is to be deleted and a new one generated (there is no undo). The new password will be automatically typed in. Unplug the unit from the USB port and it will be switched off automatically.



### 3.3 TYPING OUT THE PASSWORD LIST

Same as typing one password, but with LED "L" selected. When you plug it in the USB port, all passwords will be typed out. The column on the right shows how many times each password was invoked.

You can use this function to print out your passwords and store them in the safe place.



```
Untitled - Notepad
File Edit Format View Help

Password list          13
0 DKLm2iT7wUZnFgSGr  117
1 Kz8p0dU7uA4fR0sWJy7m  10
2 fw030Gyq6QJLVf3     22
3 qEGj8sAvUSC6Xd8ETA   6
4 S20eVMpsf7ZebcYPNVmo 1
5 62FUyU6NLGPtFuTodVM 5
6 OkoqtbESEJfMGXC7z    2
7 TnaX9zGldG1Axsj      1
8 isEAdDr6yA4wpbGvd    31
9 Aee9qcISTPNncBo5k4S  1
```

### 3.4 TYPING OUT RANDOM NUMBERS

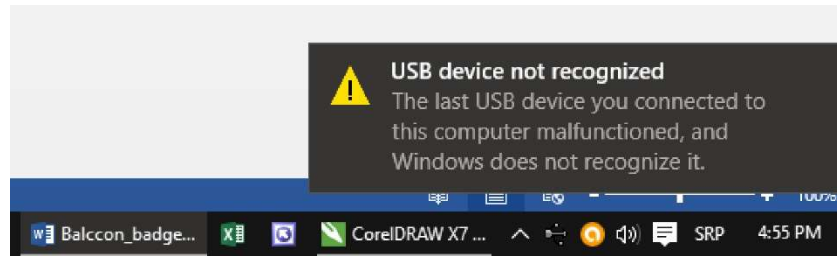
In some cases, you may need a string of random numbers. To print the infinite list, switch the unit ON in password manager mode and select the LED "R". When you plug the unit in the USB port, the infinite list of random 5-digit numbers will be typed out. You can pause/resume by pressing the upper button.



```
Untitled - Notepad
File Edit Format View Help

94796 28278 18731 76786 17288 16618 46382 92096 37347 28245 78125 08606
84782 65403 35367 22549 19698 34597 51481 50779 36562 61513 43770 80206
20825 80243 65203 49068 33950 35256 67516 26179 98234 31416 74879 66095
```

**Important:** USB interface requires at least 3 V to operate correctly. If the battery is exhausted, the voltage may drop and in that case the computer may report the error:



## 3.5 RANDOM NUMBER GENERATOR

Internal Random Number Generator (RNG) combines three techniques to create high quality randomness, using no external hardware. Those are:

### 3.5.1. UNINITIALIZED RAM CONTENTS

This technique is fully described at <http://hackaday.com/2015/06/29/true-random-number-generator-for-a-true-hacker/>. There you will also find a detailed analysis of randomness quality, which employed *Diehard* and *ENT* tests. The output from this process is used as the 32-bit SEED number in the following step.

### 3.5.2. 32-BIT PSEUDORANDOM NUMBER GENERATOR (PRNG)

The firmware of the Password Manager contains a 32-bit linear congruential generator. The main principle is described at [https://en.wikipedia.org/wiki/Linear\\_congruential\\_generator](https://en.wikipedia.org/wiki/Linear_congruential_generator)

Seed number is initialized once after the RESET process (when the battery is inserted) and all other PRNG steps are performed executing the algorithm  $X_{n+1} = (X_n * 0x41c64e6d + 0x00006073) \text{ mod } 32$ . The output contains 8-bit, created by ADDing/XORing the newly generated SEED contents.

### 3.5.3. UNIFORM CYCLIC COUNTER

The firmware also uses the internal module TIMER0 as the uniform counter with 15 Hz increment rate. In the moment when the button is pressed (which is randomness generated by a human), the 8-bit content of this counter (TMR0L) is copied to the memory location, which is used to further increase the entropy of the RNG.

## 3.6 RULES FOR PASSWORDS

- All passwords are 15...20 character in length (which is random).
- At least one lowercase, one uppercase character and one digit is guaranteed in each password.
- There are no punctuation marks or special characters.

### By the way...

...someone asked me: "Why don't you have a PIN code that would be required to unlock the device itself", to keep your passwords safe in case your unit gets stolen? This is a good point, but the 2 button interface of the device wouldn't make for a comfortable typing experience. Instead, you could secure your device with a trick : manually type in an extension to the existing passwords. So, when you generate a new password, use the PC keyboard to type your "pin" before and/or after it, and then store the extended password (there will be no conflict between USB keyboards on the computer). Now the password will need the extra "pin" typed in manually every time you use the password. This can be the same sequence of (say 4, or so) characters for all passwords.

### One more remark...

...the password manager operates like a keyboard and is as such subject to the currently selected keyboard language



in your operating system. For example, if you registered your password while using the English keyboard setting in Windows, using the password while having the Russian language selected for your keyboard will not produce the same password.

**So...**

- ...no manual password typing...
- ...no driver installation...
- ...no password keeping on your computer...
- ...no crackable PRNG password creation...
- ...no spying over your shoulder while you type the password...

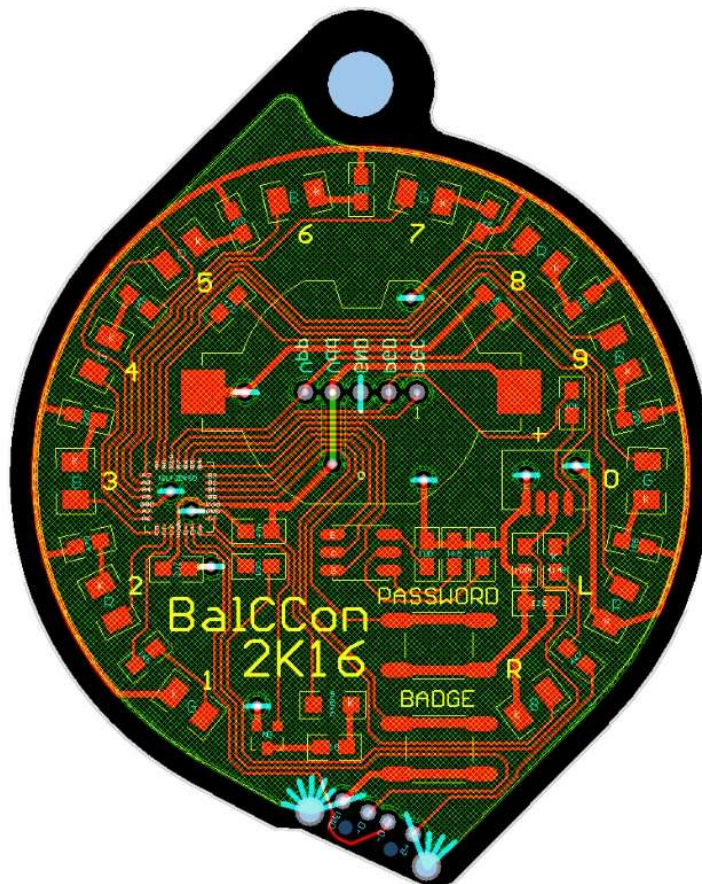
## 4. Hardware

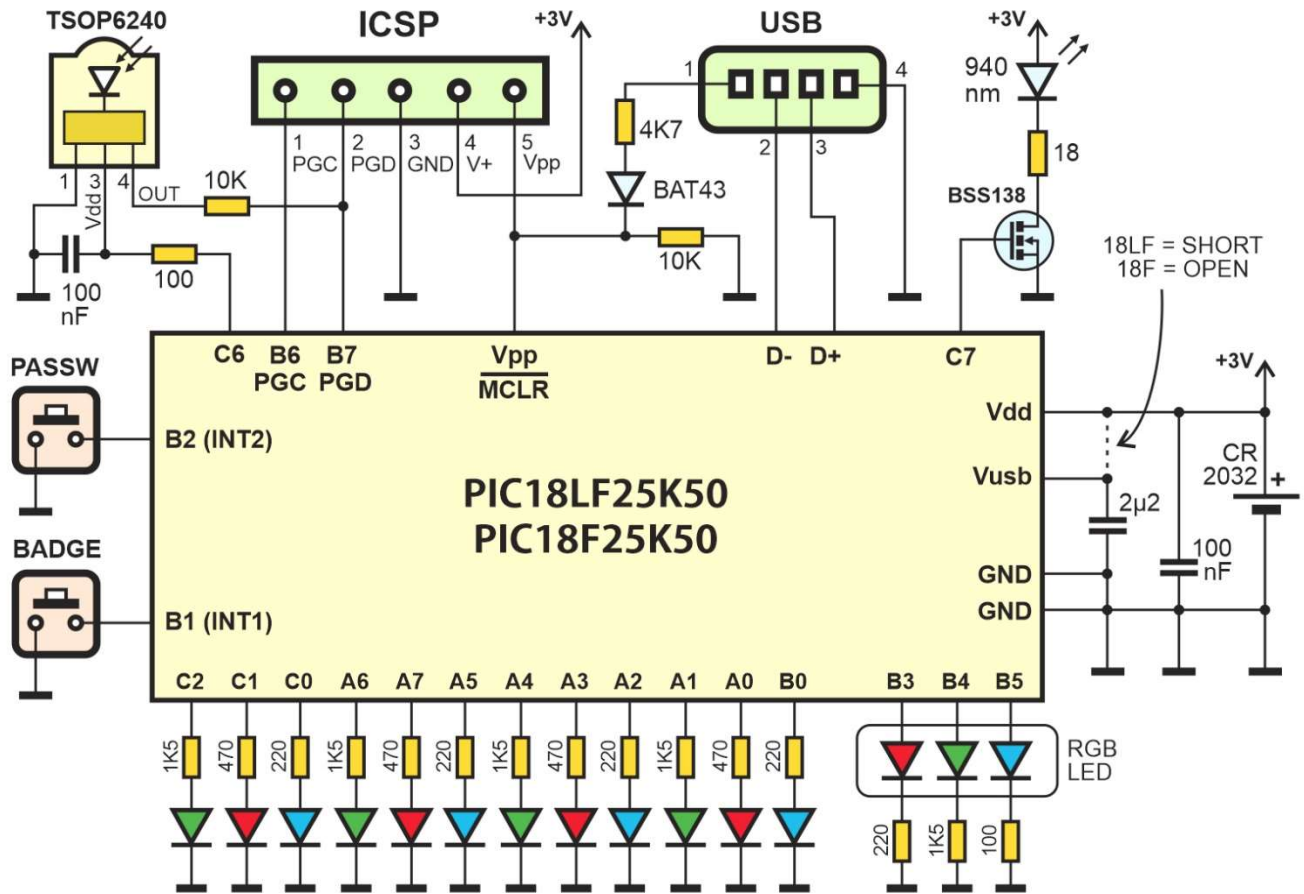
The badge is based on Microchip's microcontroller PIC18(L)F25K50. All LEDs are driven directly via MCU parallel ports, and the dimming is obtained by software controlled PWM. Infrared interface consists of IR LED and IR receiver TSOP6240. Wavelength is 940 nm, and the carrier frequency 40 KHz. Custom PCM is used for command coding.

There is a 5-pin In-Circuit Serial Programming Port (ICSP), which can be used for unit reprogramming. It is available at the back side of the unit.

Source code (in assembly language) and PCB project (in Protel 98) are available at [www.voja.rs](http://www.voja.rs)

There is a brief demo at <https://www.youtube.com/watch?v=IFifeMkfp8>





Here is the current consumption table, measured with the full 3V battery voltage:

|                         | Min.   | Typ.              | Max.   | Hours *(1)    |
|-------------------------|--------|-------------------|--------|---------------|
| <b>Badge</b>            | 3.2 mA | 6 mA              | 9.7 mA | 31.7          |
| <b>TV-B-Gone</b>        | 4.4 mA | 6.5 mA            | 9.0 mA | 29.2          |
| <b>Password Manager</b> | 4.0 ma | 4.3 mA            | 5.2 mA | 44.2 *(2)     |
| <b>OFF</b>              |        | 115 nA/12 µA *(3) |        | 1.6M/16K *(3) |

Notes:

\*(1) Battery life is based on 190 mAh capacity. However, the real life may be shorter, as the average current is higher than recommended for lithium battery

\*(2) This is the hypothetical value, real battery life for password manager is shorter, as the USB interface will not work at low voltages, when the battery is exhausted for more than approx. 50%

\*(3) Values are for 18LF25K50 and 18F25K50, respectively. The value for 18LF25K50 is the hypothetical value, real current consumption is affected by battery self-discharge