Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences
Department of Engineering and Information Technology

# An inexpensive solution to some of your daily IT security problems

| Student/s | Tutor | Module Supervisor | Project proposed by |
|---|---|---|---|
| Noli Manzoni<br>Sandro Tiago Carlao | Dr. Simon Kramer | Prof. Marcel Pfahrer | Dr. Simon Kramer |

| Degree | Module | Year | Date |
|---|---|---|---|
| Bachelor of Science in Computer Science | BTI7301<br>Project 1 | 2016/2017<br>Spring semester | 13 June 2017 |


## Description

The risk of storing cryptographic keys on a hard disk is constantly increasing because, once the system where they are stored is compromised, the keys must be replaced. Therefore, to find a solution, new security modules such as smart cards or hardware security modules (HSM) were created. Unfortunately, these devices were designed only for commercial use and private users were abandoned with a few solutions. For this reason, the goal of this project is to find out which extent off-the-shelf Internet of Things module can be programmed to function as an HSM.

## Objectives

The main objective of the project is to pick, after researching and comparing, the Internet of Things device with the biggest and most complete API with the best compatibility with Java, to be able to use Google Keyczar (easy-to-use crypto toolkit). Once the device is chosen, it must be tested to find its limits as an HSM. Optionally, external functionalities like a Trusted Platform Module can be added. The secondary goal of this project is to give us freedom of will, this way we can be independent and able to learn what to prioritize to complete the project within the time frame that is at our disposal.

## Conclusion

As result we have created an UBS HSM on a Raspberry Pi 3 Model B, hence the name RPiHSM, it can be used in our daily life on the three major operation systems. The designed case with three leds has a captivating look that also helps the user for a higher productivity. Moreover, the RPiHSM can be used by an inexperienced user thanks to the graphical user interface application but also by the advanced ones thanks to the command line application. This HSM can perform all the basic cryptographic tasks like encryption, decryption, signature generation and signature verification.