Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

# IoT Hardware Security Module

NOLI MANZONI, SANDRO TIAGO CARLAO I2B

RPiHSM

# Outline

1. Summary
2. Hardware Security Module (HSM): concept
3. Internet of Things (IoT) devices: overview & choice
4. Our product design
5. Development: problems & solutions
6. Our final product
7. Demo

RPiHSM

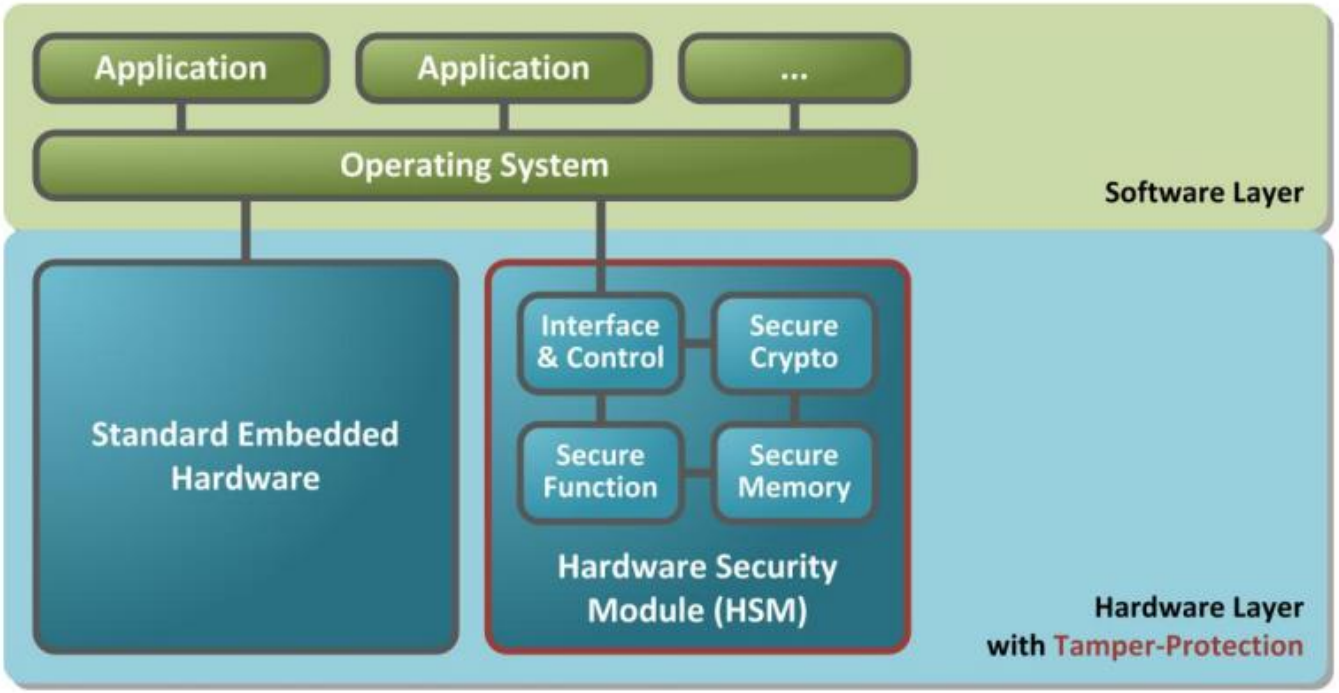
# Summary

**Goal:** create an **IoT HSM** for our personal use.

- **Task 1:** find the most suitable existing **IoT modules** to function as an HSM.
- **Task 2:** summarize the **state of the art** of HSM-capable IoT devices.
- **Task 3:** assess existing **Proofs of Concept**. Decide.

RPiHSM

# HSM concept




Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

RPiHSM

# HSM concept

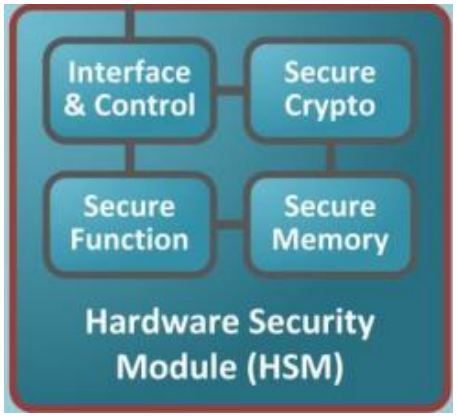
**Secure Memory:**
- Stores private & symmetric keys
- Side-channel attack protection

**Secure Cryptography:**
- Manages encryption, signature & hashing algorithms

**Tamper Protection:**
- Security against external attacks
- Special shielding or coatings

**Secure Function:**
- Physically protected clock
- True Random Number Generator

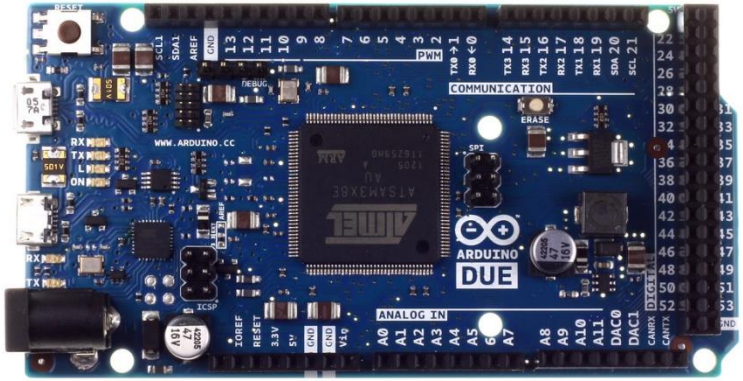
**Interface & Control:**
- Manages the access to the HSM
- Communication APIs



RPiHSM

# IoT Devices: overview

Start with **two proofs of concept**

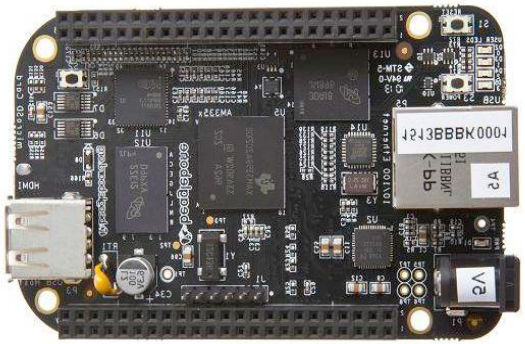



Arduino DUE


Raspberry Pi 3 model B

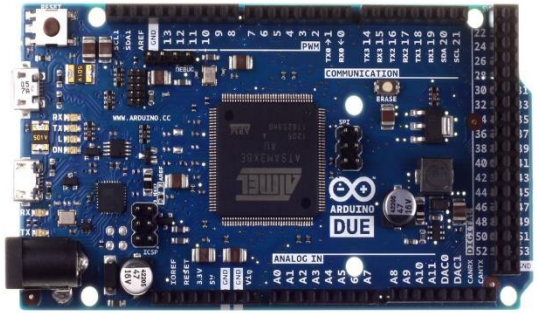
RPiHSM

# IoT Devices: overview

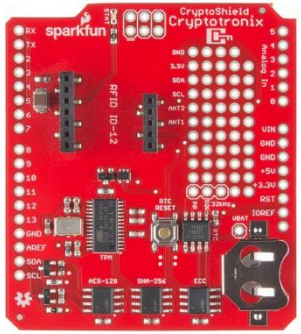


Beaglebone Black

CryptoCape



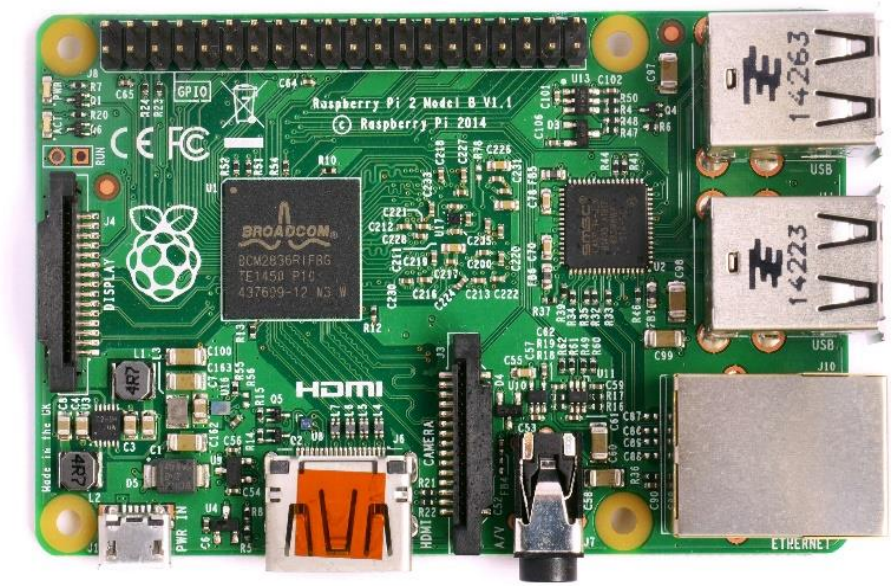

Arduino DUE




Crypto shield

RPiHSM

# IoT Devices: choice

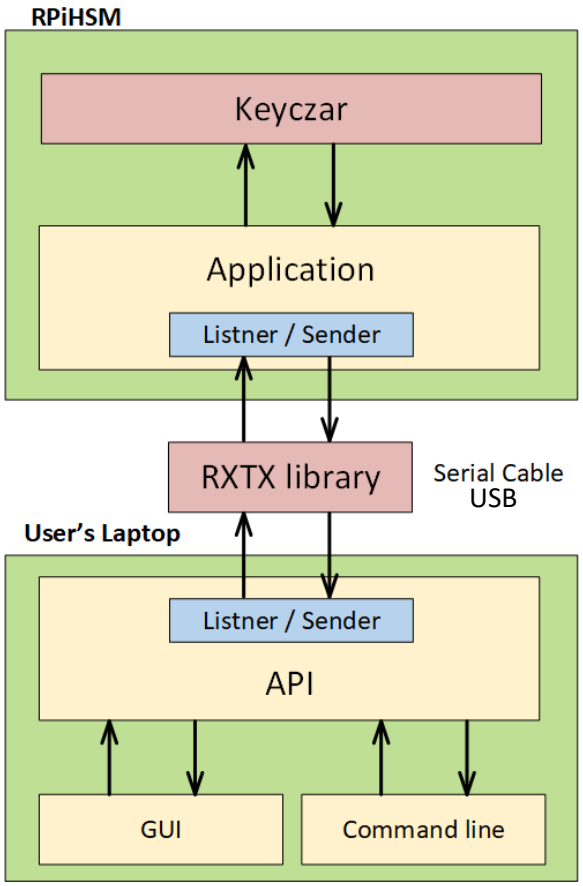



Raspberry Pi 3 model B

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

RPiHSM

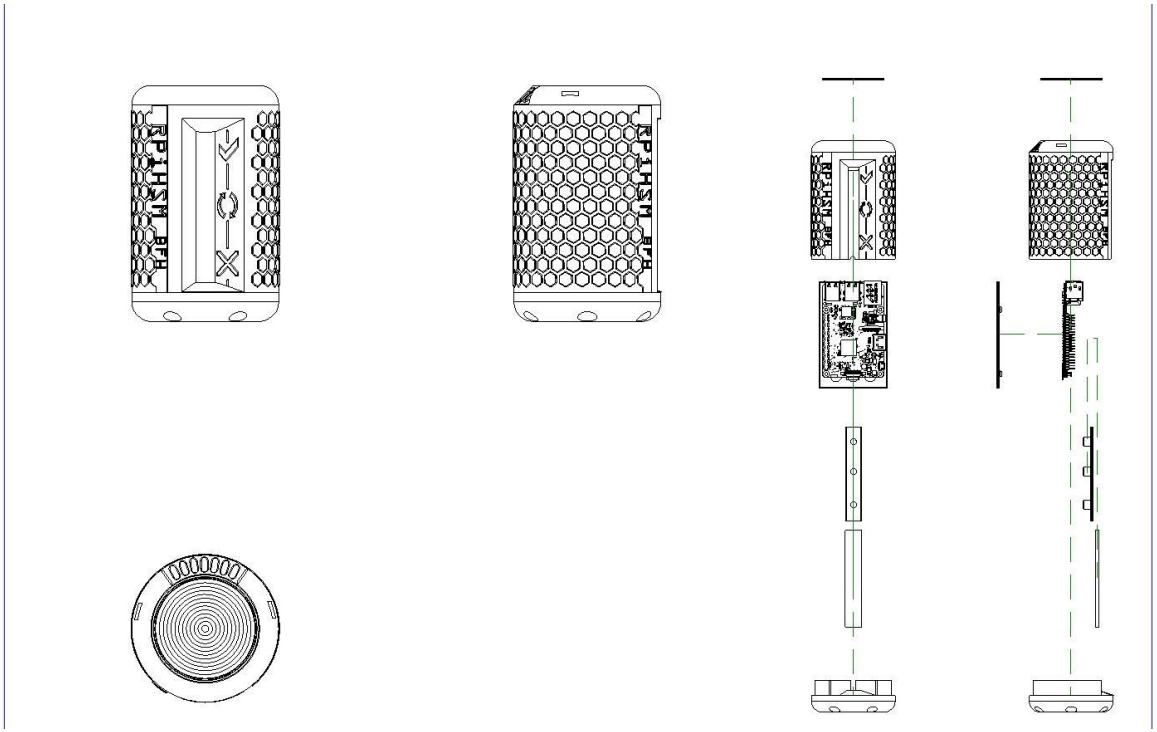
# Our product design



RPiHSM

# Our product design

**Synergy** with the **Micro and Medical Technology** department



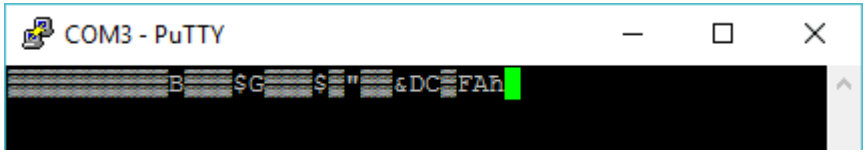

Designed by **Kevin Thomas** (kevinalexander.thomas@students.bfh.ch)

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

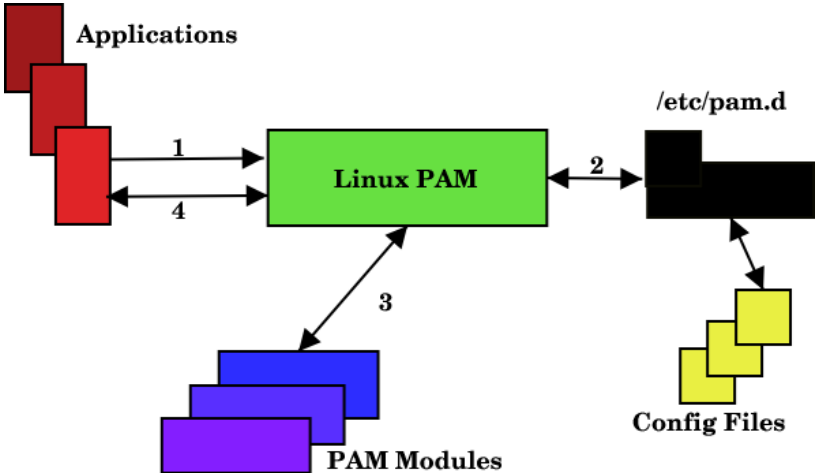
RPiHSM

# Development: problems & solutions

Serial connection generated **strange characters**




Authentication with **PAM** (Pluggable authentication module)



RPiHSM

# Our final product

**USB HSM**

- Store keys
- Encrypt/Decrypt files
- Sign files
- Verify signature
- Public key export
- Multiple users
- Internationalization


ON BUSY ERROR

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

RPiHSM

# Our final product

**Use our API for your application!**

Select C:\Windows\system32\cmd.exe

```
C:\Workspace\rpihsm>java -jar RPiHSM-CommandLine-0.1.jar encrypt -n test -f C:\Users\nolti\Desktop\test.docx
```

Key set: test

File: Select file to encrypt

C:\Users\nolti\Desktop\test.docx

Encrypt

```
EncryptDecrypt ed = new EncryptDecrypt(serialHelper, userPath, keySetName, filePath);
if (ed.encrypt()) {
    return ENCRYPT_SUCCESS;
} else {
    return ENCRYPT_ERROR;
}
```

RPiHSM

# Our final product

| | |
|---|---|
| ch.bfh.ti.project1.RPiHSM.IoT.Commands | 96% |
| ch.bfh.ti.project1.RPiHSM.IoT.Utils | 89% |

| | |
|---|---|
| ch.bfh.ti.project1.RPiHSM.API | 73% |
| ch.bfh.ti.project1.RPiHSM.API.Exception | 67% |

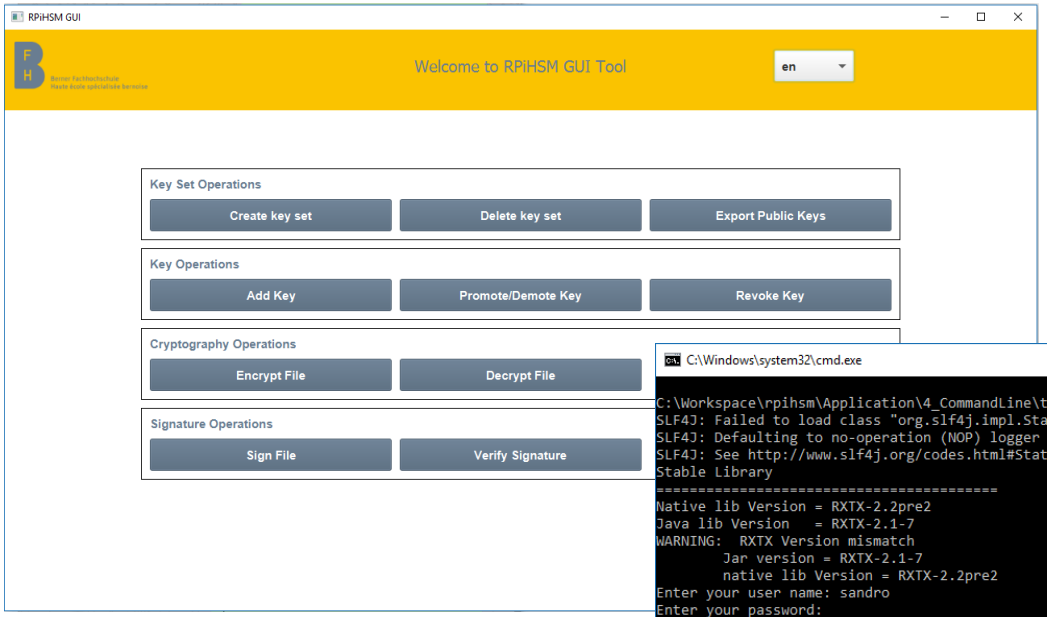
| | Classes | Jar Size | Lines of Code | Lines of JavaDoc | Total Code |
|---|---|---|---|---|---|
| IoT | 20 | 1901 KB | 486 | 318 | **804** |
| API | 16 | 749 KB | 348 | 310 | **658** |
| GUI | 15 | 3982 KB | 1111 | 205 | **1316** |
| CommandLine | 18 | 4027 KB | 537 | 294 | **831** |
| **Total** | **69** | **9849 KB** | **2482** | **1127** | **3609** |

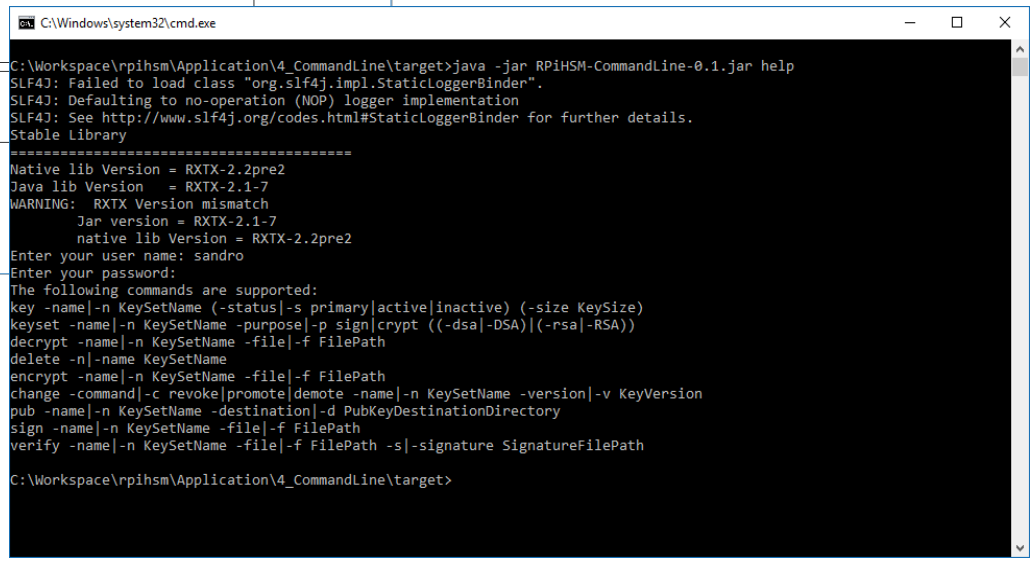
| | |
|---|---|
| Case | ~ 6 CHF |
| Hardware (digitec.ch) | ~ 65 CHF |
| **Total** | **~ 71 CHF** |

Search **RPiHSM** on www.github.com

## RPiHSM

# Demo


RPiHSM GUI
Welcome to RPiHSM GUI Tool
en
Key Set Operations
Create key set
Delete key set
Export Public Keys
Key Operations
Add Key
Promote/Demote Key
Revoke Key
Cryptography Operations
Encrypt File
Decrypt File
Signature Operations
Sign File
Verify Signature


C:\Windows\system32\cmd.exe
C:\Workspace\rpihsm\Application\4_CommandLine\target>java -jar RPiHSM-CommandLine-0.1.jar help
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
Stable Library
==========
Native lib Version = RXTX-2.2pre2
Java lib Version = RXTX-2.1-7
WARNING: RXTX Version mismatch
Jar version = RXTX-2.1-7
native lib Version = RXTX-2.2pre2
Enter your user name: sandro
Enter your password:
The following commands are supported:
key -name|-n KeySetName (-status|-s primary|active|inactive) (-size KeySize)
keyset -name|-n KeySetName -purpose|-p sign|crypt ((-dsa|-DSA)|(-rsa|-RSA))
decrypt -name|-n KeySetName -file|-f FilePath
delete -n|-name KeySetName
encrypt -name|-n KeySetName -file|-f FilePath
change -command|-c revoke|promote|demote -name|-n KeySetName -version|-v KeyVersion
pub -name|-n KeySetName -destination|-d PubKeyDestinationDirectory
sign -name|-n KeySetName -file|-f FilePath
verify -name|-n KeySetName -file|-f FilePath -s|-signature SignatureFilePath
C:\Workspace\rpihsm\Application\4_CommandLine\target>