# A Privacy Enhancing Architecture for Secure Wearable Devices

**Author**
Sonnino Alberto

**Supervisor**
Dr. Meiklejohn Sarah

Master Thesis
MSc Information Security

September 2016

# Introduction & Motivations

- **What** did I do ?

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

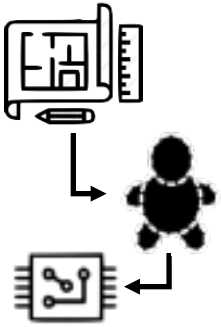
Wearable Devices / Using Anonymous Cred.

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

Wearable Devices / Using Anonymous Cred.

Architecture

Prototype

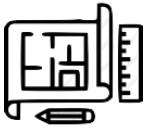
Industrial System

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

Wearable Devices / Using Anonymous Cred.

Architecture

Prototype

Industrial System

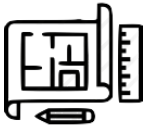
- **How** did I proceed ?

# Introduction & Motivations

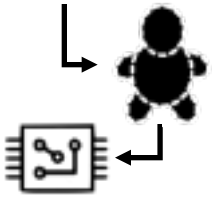
- **What** did I do ?

Flexible & Multi-Purpose PET

Wearable Devices / Using Anonymous Cred.

Architecture



Prototype

Industrial System

- **How** did I proceed ?

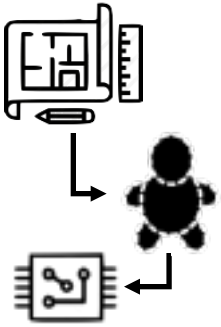

wearable

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

Wearable Devices / Using Anonymous Cred.

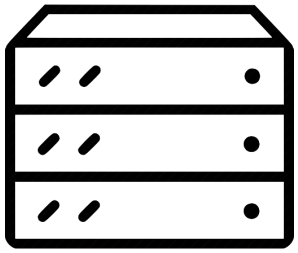



Architecture

Prototype

Industrial System

- **How** did I proceed ?



server

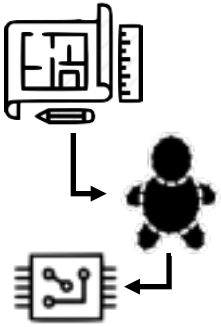

wearable

# Introduction & Motivations

- **What** did I do ?

Flexible & Multi-Purpose PET

Wearable Devices / Using Anonymous Cred.

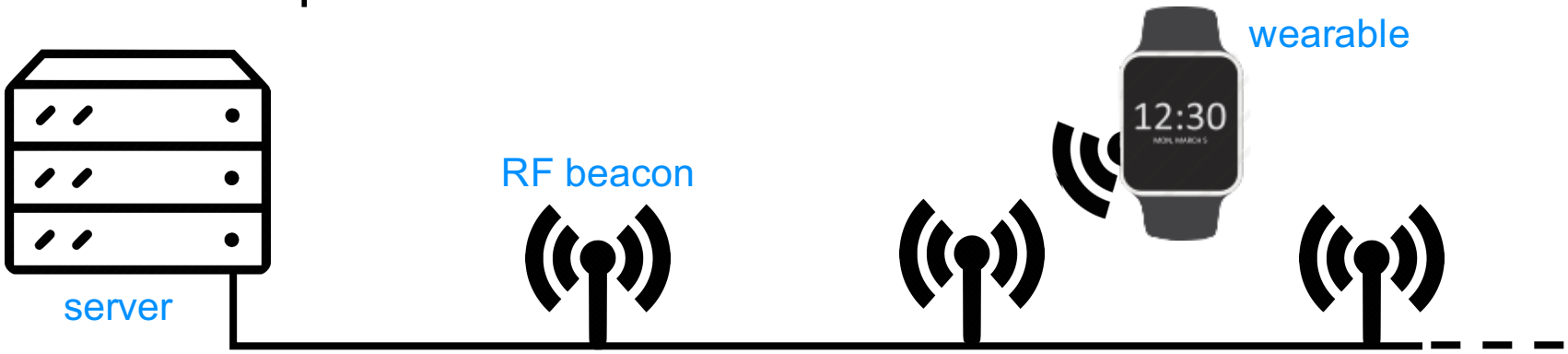



Architecture

Prototype

Industrial System

- **How** did I proceed ?



# Introduction & Motivations

- **Why** is it useful?

# Introduction & Motivations

- **Why** is it useful?
  - Wearable access many private information (more than others) [1]
  - Security often neglected on embedded systems [2]
  - Generally hard to include security on wearable devices [3] :

# Introduction & Motivations

- **Why** is it useful?
  - Wearable access many private information (more than others) [1]
  - Security often neglected on embedded systems [2]
  - Generally hard to include security on wearable devices [3] :

Very limited resources

Crypto is expensive

# Introduction & Motivations

- **Why** is it useful?
  - Wearable access many private information (more than others) [1]
  - Security often neglected on embedded systems [2]
  - Generally hard to include security on wearable devices [3] :

Very limited resources

Crypto is expensive

Huge devices' diversity

Rely on common architectures

# Introduction & Motivations

- **Why** is it useful?
  - Wearable access many private information (more than others) [1]
  - Security often neglected on embedded systems [2]
  - Generally hard to include security on wearable devices [3] :

Very limited resources

Crypto is expensive

Huge devices' diversity

Rely on common architectures

High connectivity

Sensitive data transfer

# Introduction & Motivations

- **Why** is it useful?
  - Wearable access many private information (more than others) [1]
  - Security often neglected on embedded systems [2]
  - Generally hard to include security on wearable devices [3] :

Very limited resources

Crypto is expensive

Huge devices' diversity

Rely on common architectures

High connectivity

Sensitive data transfer

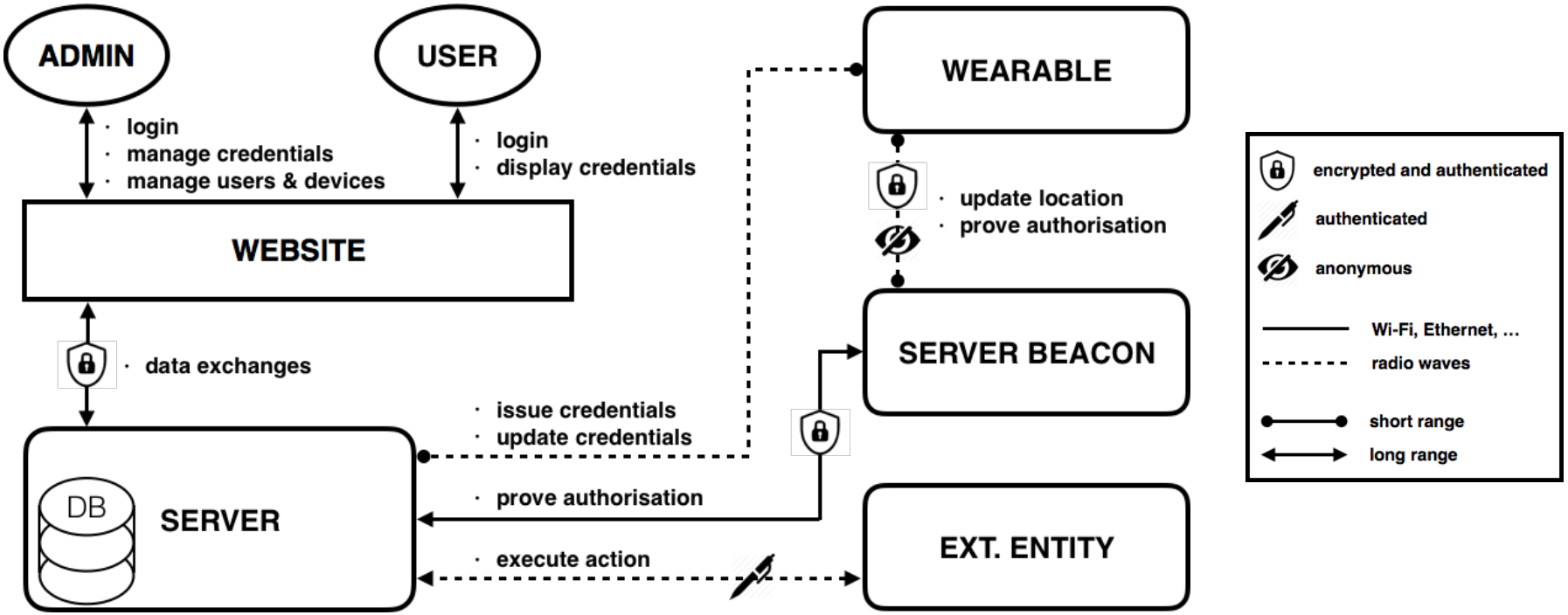
Emerging field

Risks' awareness, need for standards

# Contents

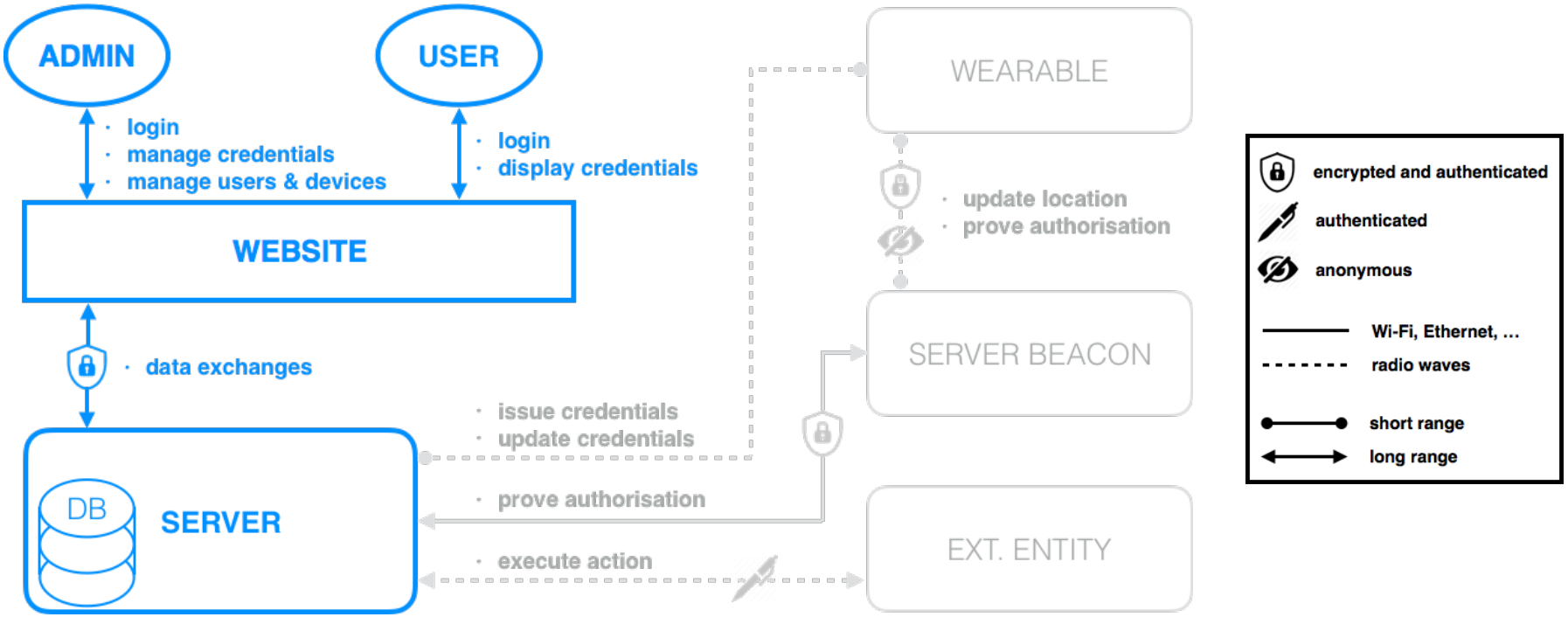
# System's Architecture

- The big picture



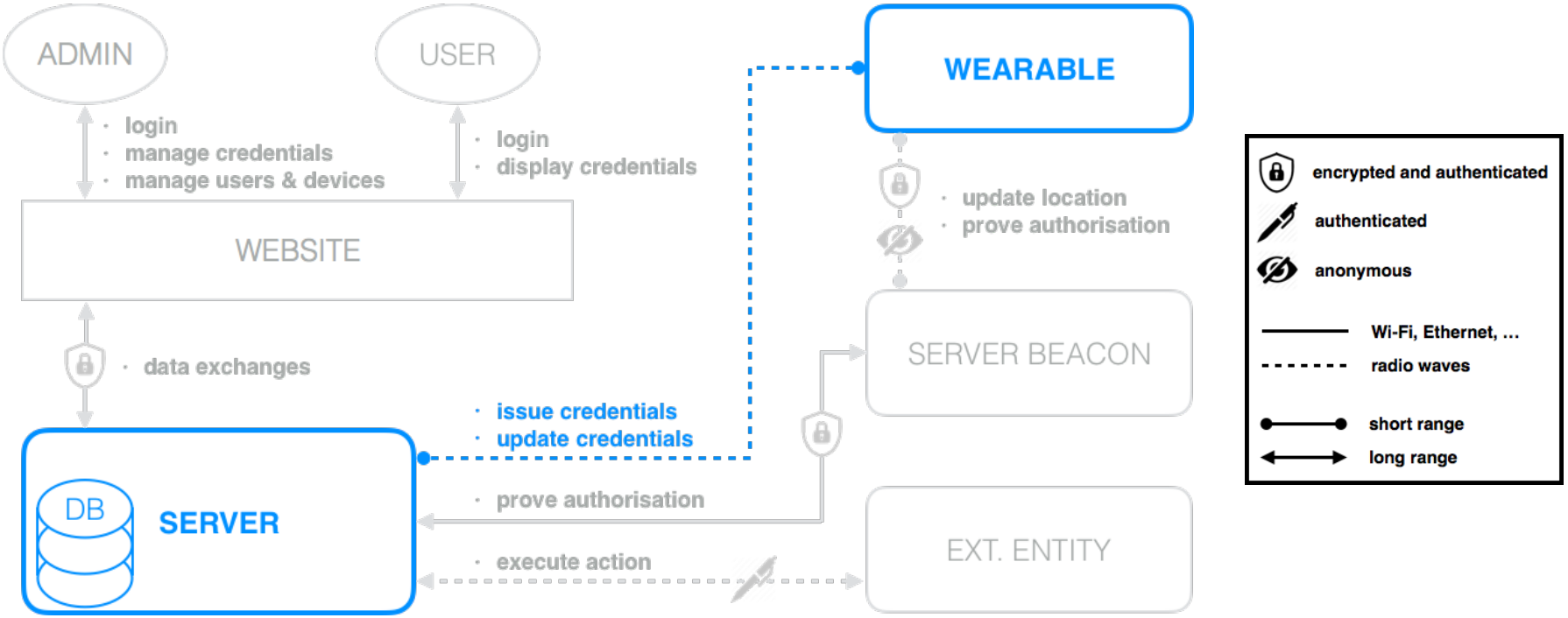
# System's Architecture

- Web Administration



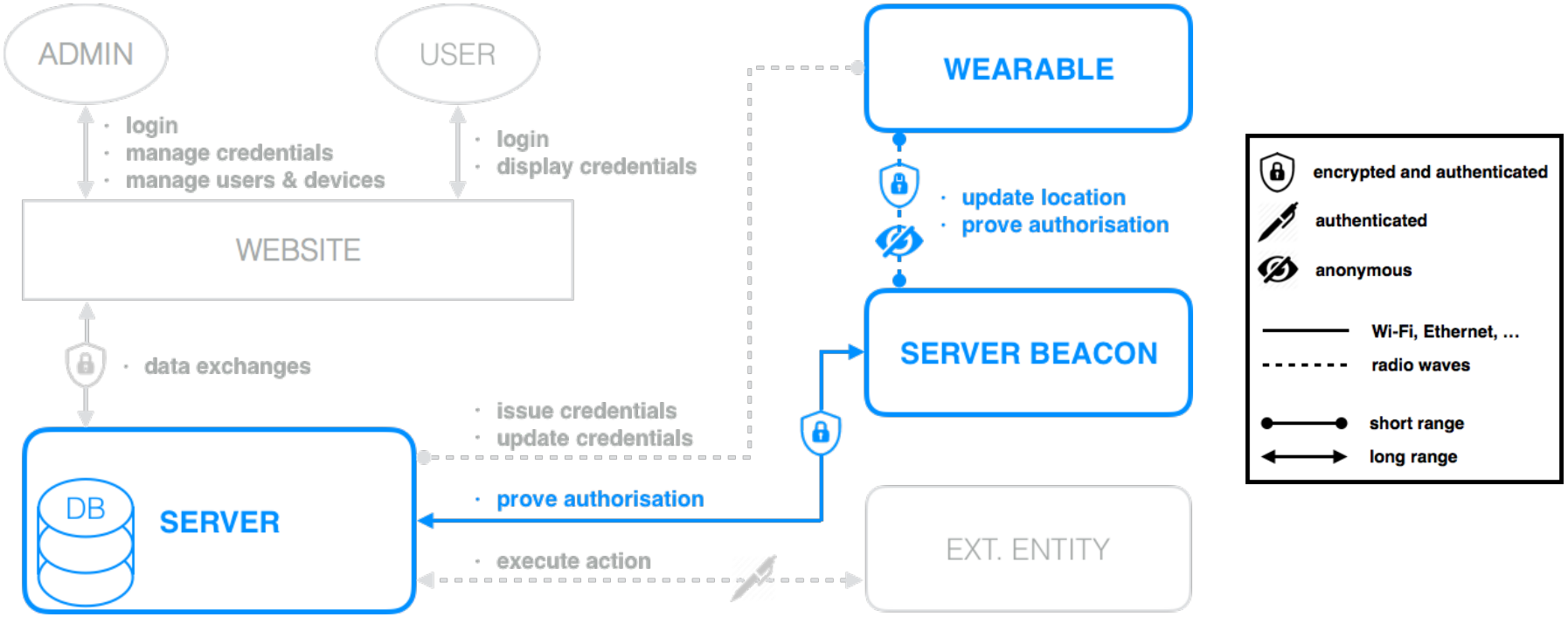
# System's Architecture

- Credentials' Issuance



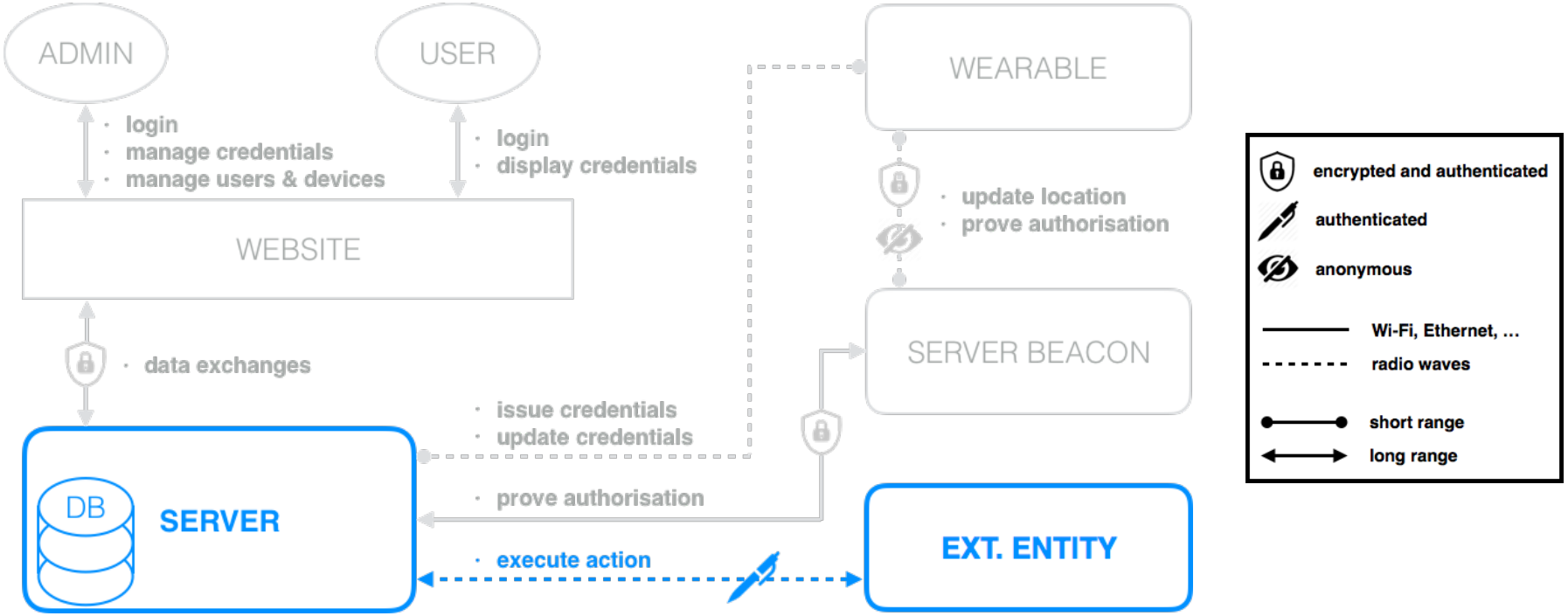
# System's Architecture

- Credentials' Presentation



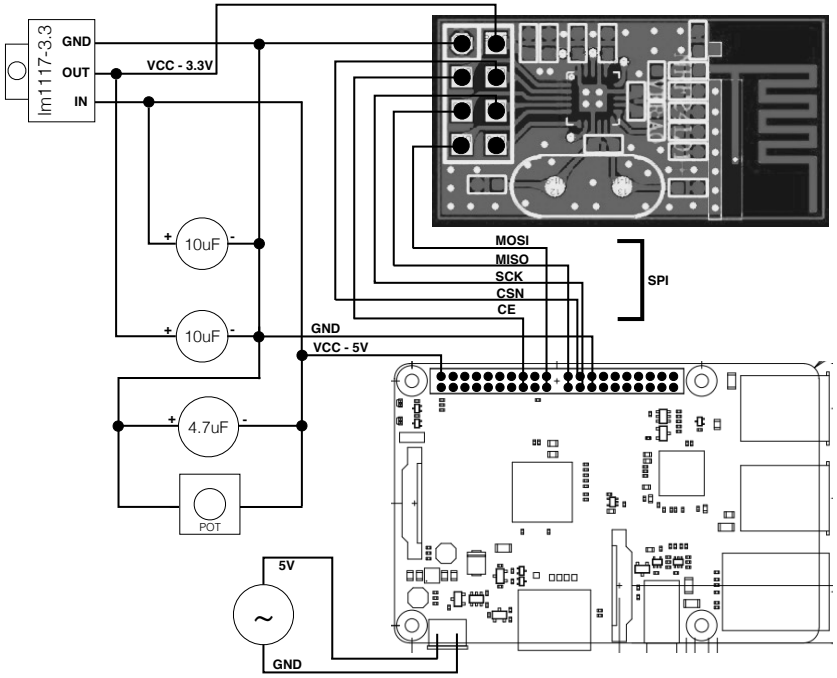
# System's Architecture

- Action's Execution

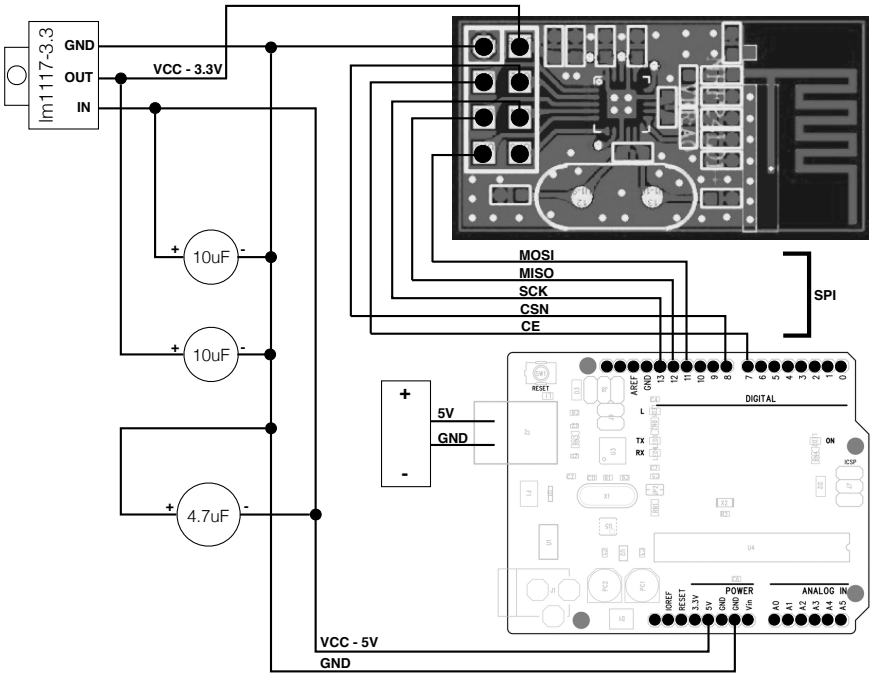


# Prototype

- Hardware Implementation



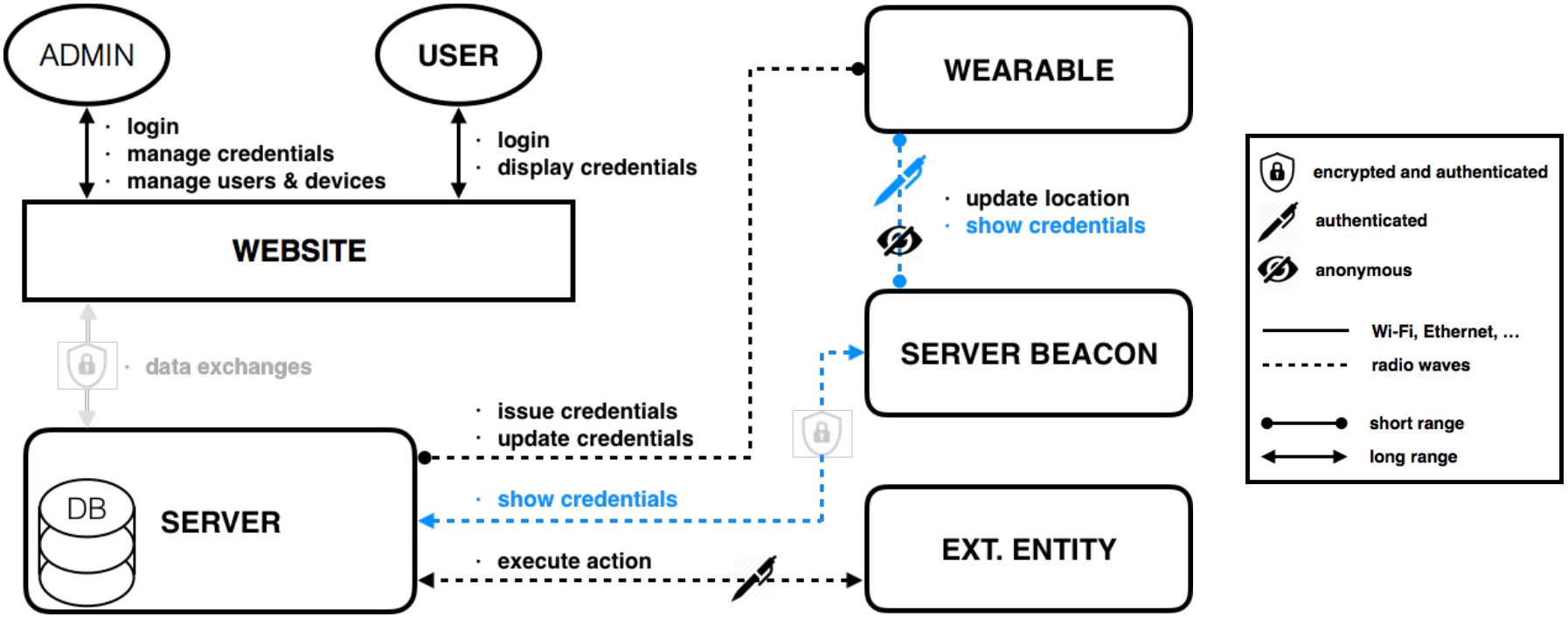

Server Implementation




Wearable & Beacon Implementation

# Prototype

- What has actually been built



# Prototype

- Performances & Resource Analysis

| Server | Wearable | Beacon |
|---|---|---|
| £33.25 | £4.89 | £4.89 |

Financial Cost

| | Program Memory | Dynamic Memory |
|---|---|---|
| Wearable | 20.080 KB | 284 B |
| Beacon | 14.422 KB | 196 B |

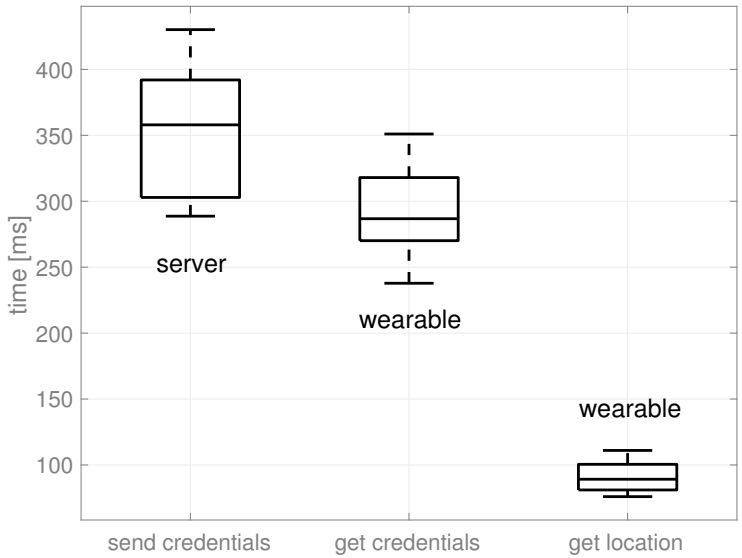
Memory Usage

| Server | Wearable | Beacon |
|---|---|---|
| ~ 1 W | < 150 mW | < 150 mW |

Power Consumption

# Prototype

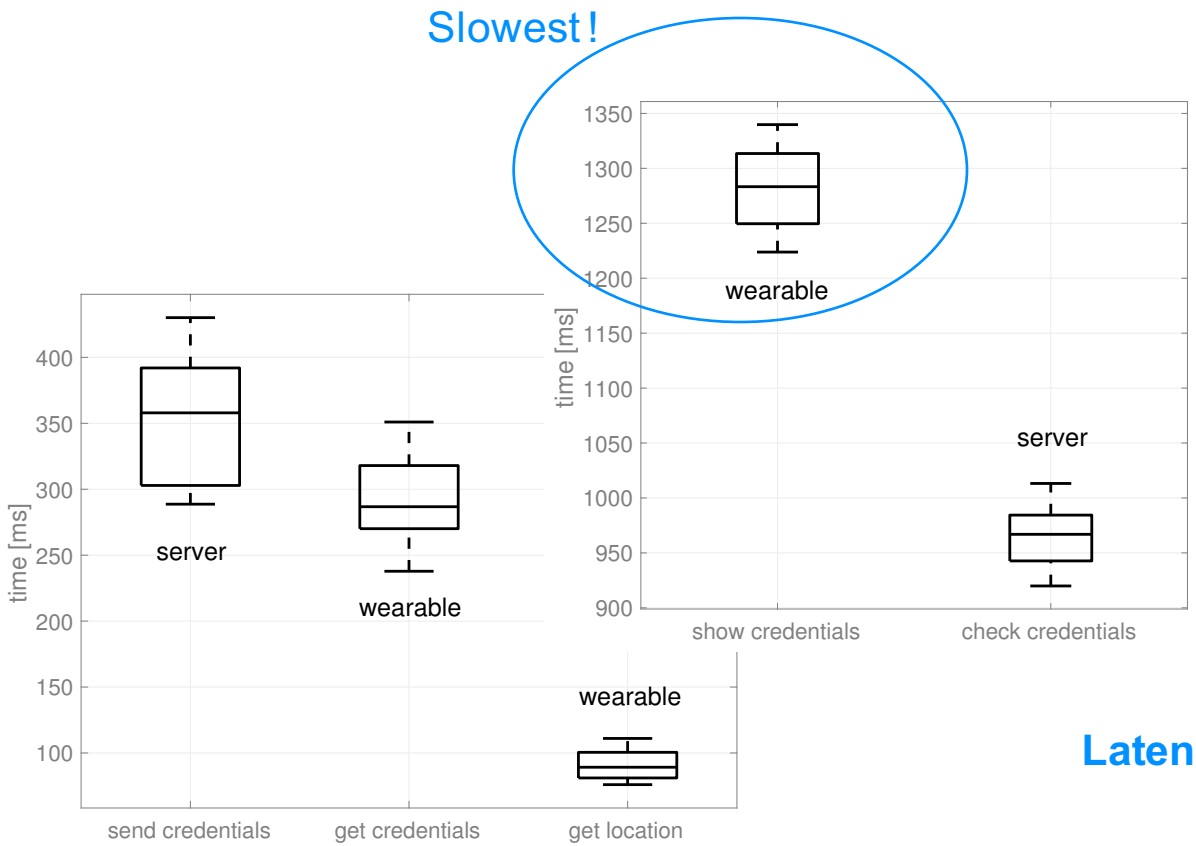
- Performances & Resource Analysis




**Latency Analysis**

# Prototype

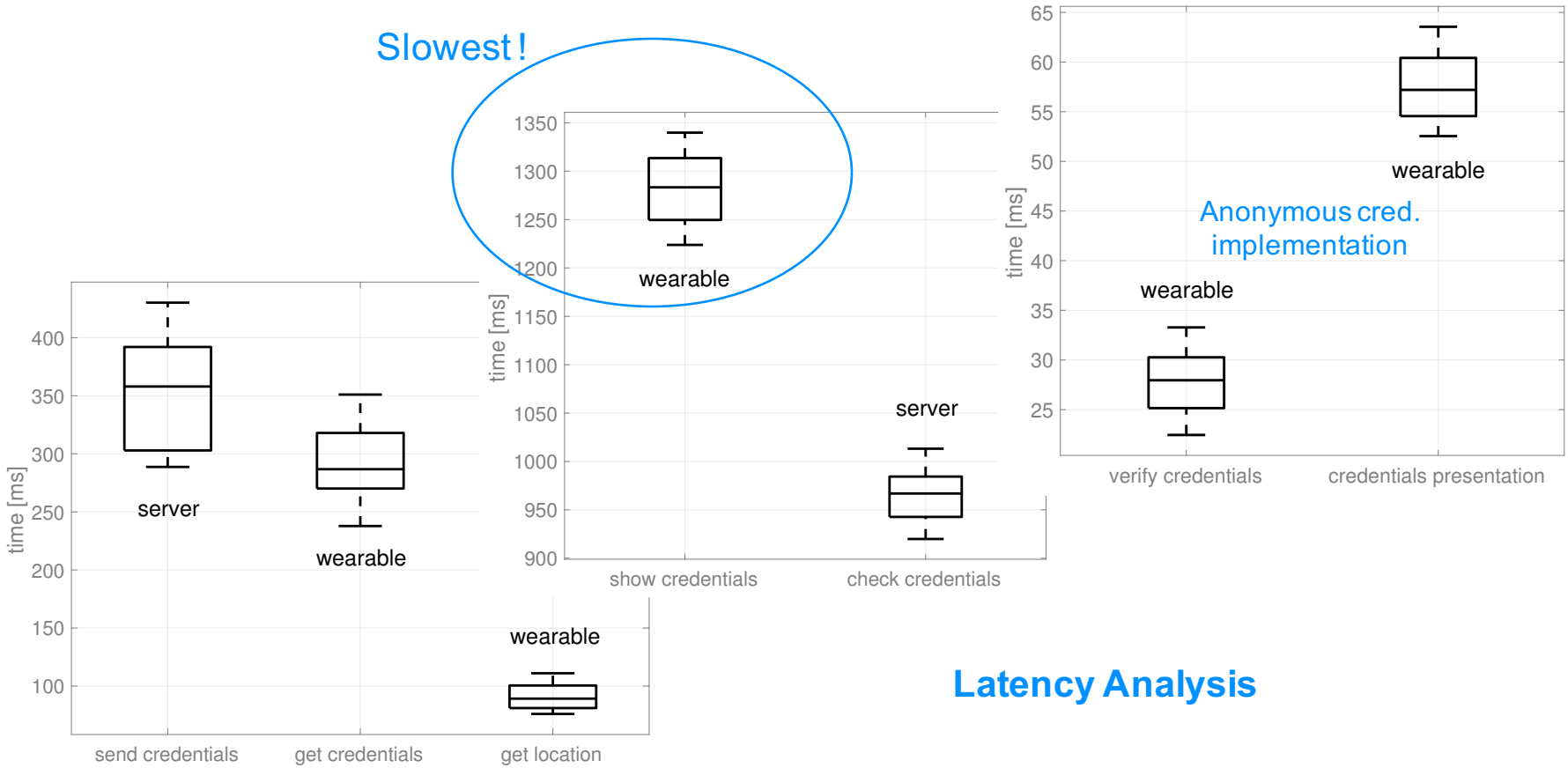
- Performances & Resource Analysis




**Latency Analysis**

# Prototype

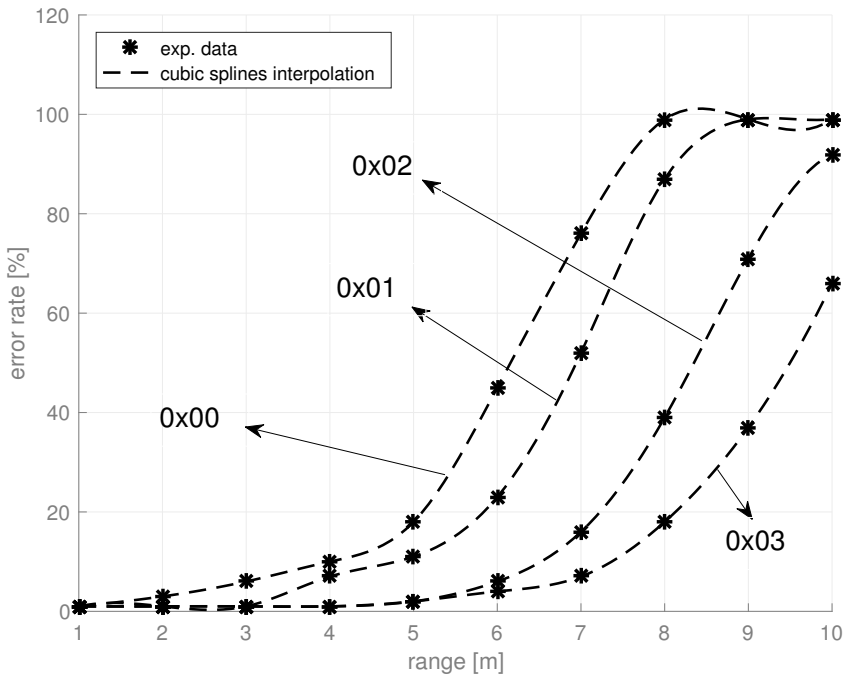
- Performances & Resource Analysis



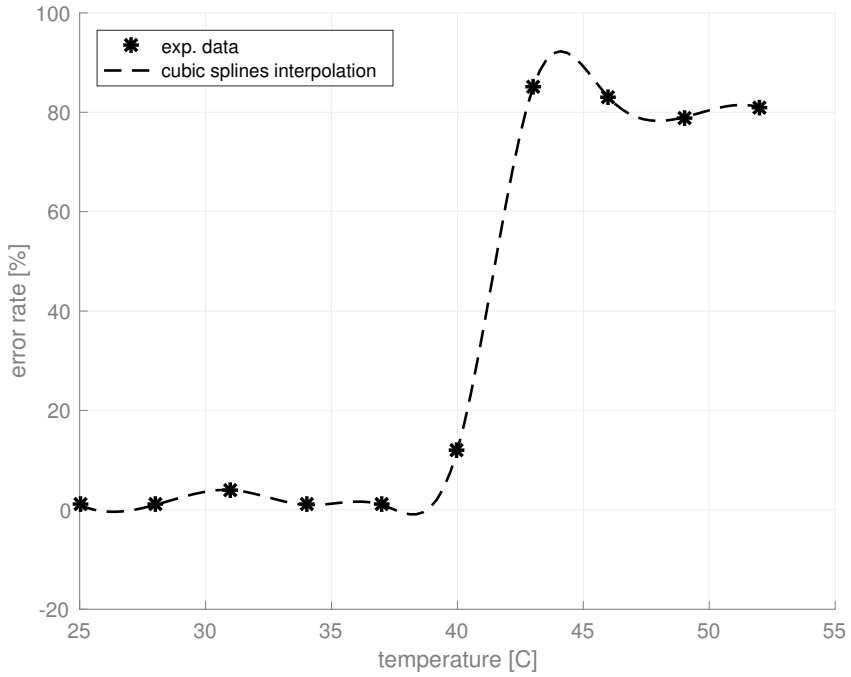

**Latency Analysis**

# Prototype

- Performances & Resource Analysis



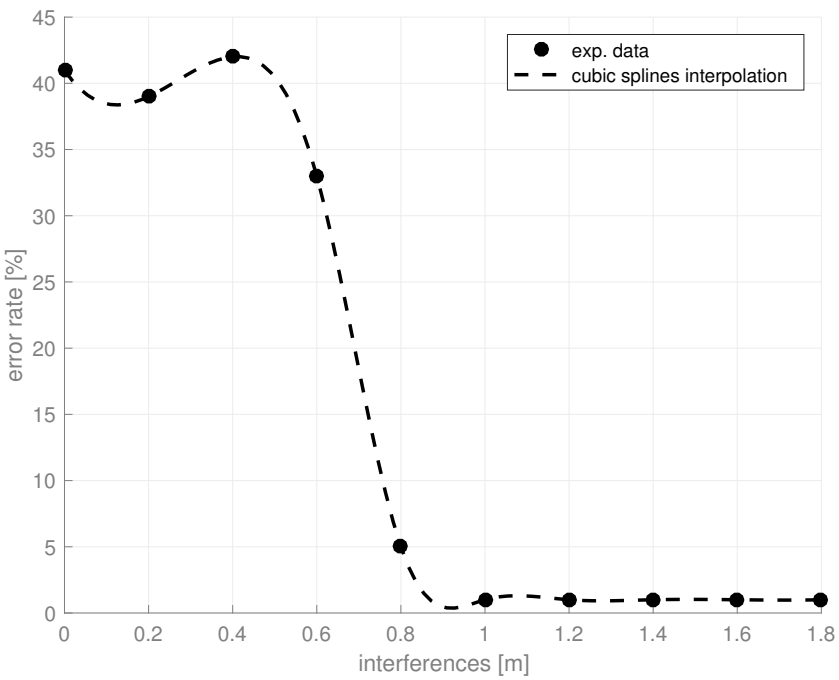

**Operational Range**

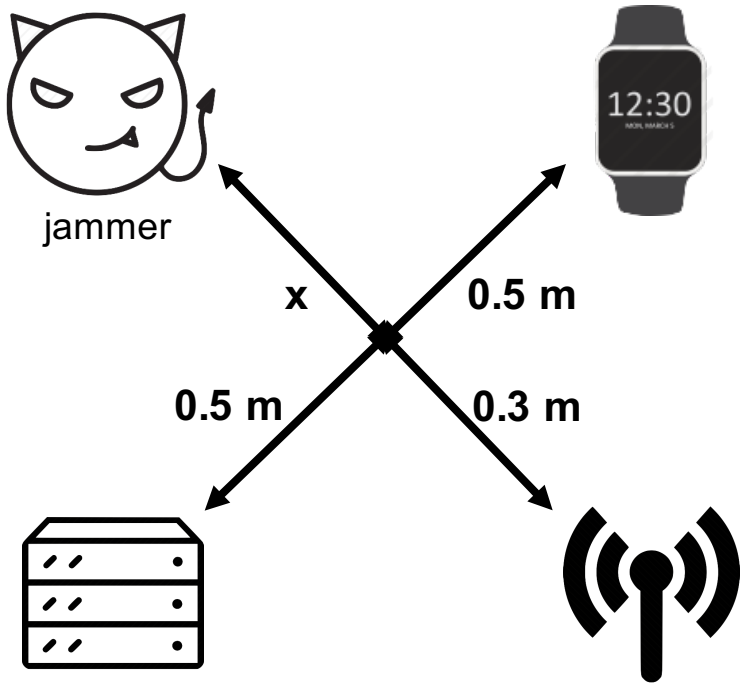



**Temperature Dependency (wearable)**

# Prototype

- Performances & Resource Analysis




**Sensibility to Radio Interferences**

# Towards an Industrial System

- Microchip PIC32MZ

# Towards an Industrial System

- Microchip PIC32MZ

# Towards an Industrial System

- Microchip PIC32MZ

**Embedded WolfSSL**

# Towards an Industrial System

- Microchip PIC32MZ

**Embedded WolfSSL**



**Compatible with the Prototyped Code**

# Towards an Industrial System

- Microchip PIC32MZ

**Embedded WolfSSL**



**Compatible with the Prototyped Code**

**Hardware Implementations**

1. SHA-2,
2. PNG & RNG
3. AES and DES (CBC, ECB, CTR, CFB, OFB)
4. AES-GCM
5. OTP-array with restricted memory access

# Towards an Industrial System

- Microchip PIC32MZ

**Embedded WolfSSL**



**Compatible with the Prototyped Code**

**Hardware Implementations**

1. SHA-2,
2. PNG & RNG
3. AES and DES (CBC, ECB, CTR, CFB, OFB)
4. AES-GCM
5. OTP-array with restricted memory access

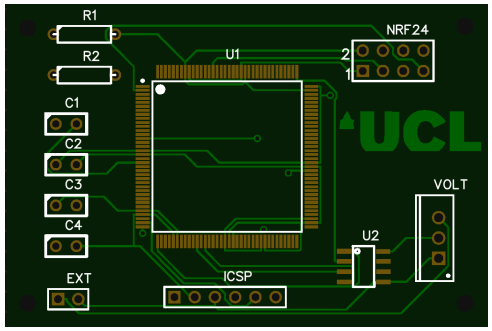
**Very Cheap**

**From less than**

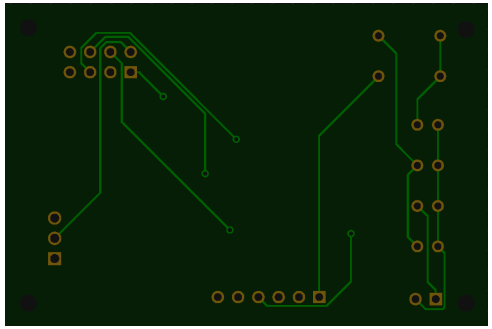
**£10**

# Towards an Industrial System

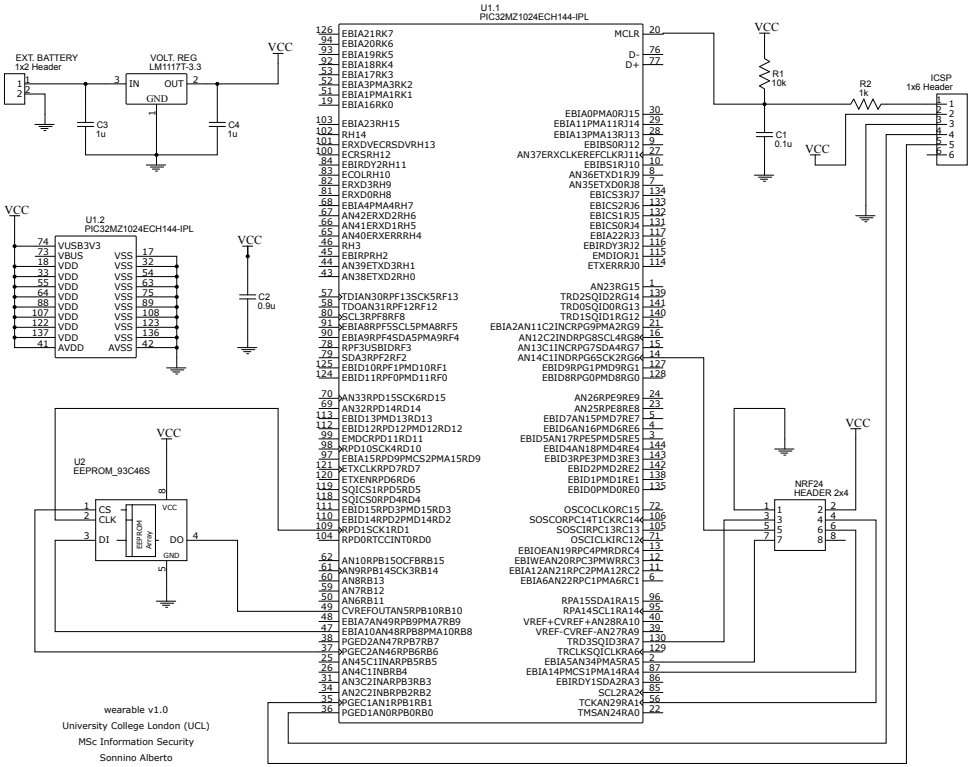
- Wearable's Printed Circuit Board




PCB Front Side



PCB Back Side




PCB Schematics

# Conclusion & Further Directions

- What did we talked about ?
  - An architecture for secure wearable devices
  - Prototype and extensive testing
  - How to build industrial system from prototype

# Conclusion & Further Directions

- What did we talked about ?
  - An architecture for secure wearable devices
  - Prototype and extensive testing
  - How to build industrial system from prototype

- The main things I learnt :
  - Security is expensive – This is not a joke !
  - Do test (a lot) your prototype
  - Really consider the target hardware

# Conclusion & Further Directions

- What did we talked about ?
  - An architecture for secure wearable devices
  - Prototype and extensive testing
  - How to build industrial system from prototype
- The main things I learnt :
  - Security is expensive – This is not a joke !
  - Do test (a lot) your prototype
  - Really consider the target hardware
- What's next ?
  - Build an industrial system from the prototype
  - Add a revocation mechanism

# Bibliography

[1] **V. Mott, K. Caine**. *Users' Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected*. Springer, 8976 (Lecture Notes in Computer Science): 231-244, 2015.

[2] **H. Modares, R. Salleh, A. Moravejosharieh**. *Overview of Security Issues in Wireless Sensor Networks*. IGI Global, PeerReviewed, 2010.

[3] **D. K. Yadav, B. Ionascu, S. V. K. Ongole, A. Roy, N. Memon**. *Design and Analysis of Shoul- der Surfing Resistant PIN Based Authentication Mechanisms on Google Glass*. Springer, 8976 (Lecture Notes in Computer Science): 281-297, 2015.

[4] ***IconFinder.*** Search through 1,130,755 icons or browse 24,517 icon sets. *Visited on the 23rd of Aug. 2016 *. https://www.iconfinder.com.*

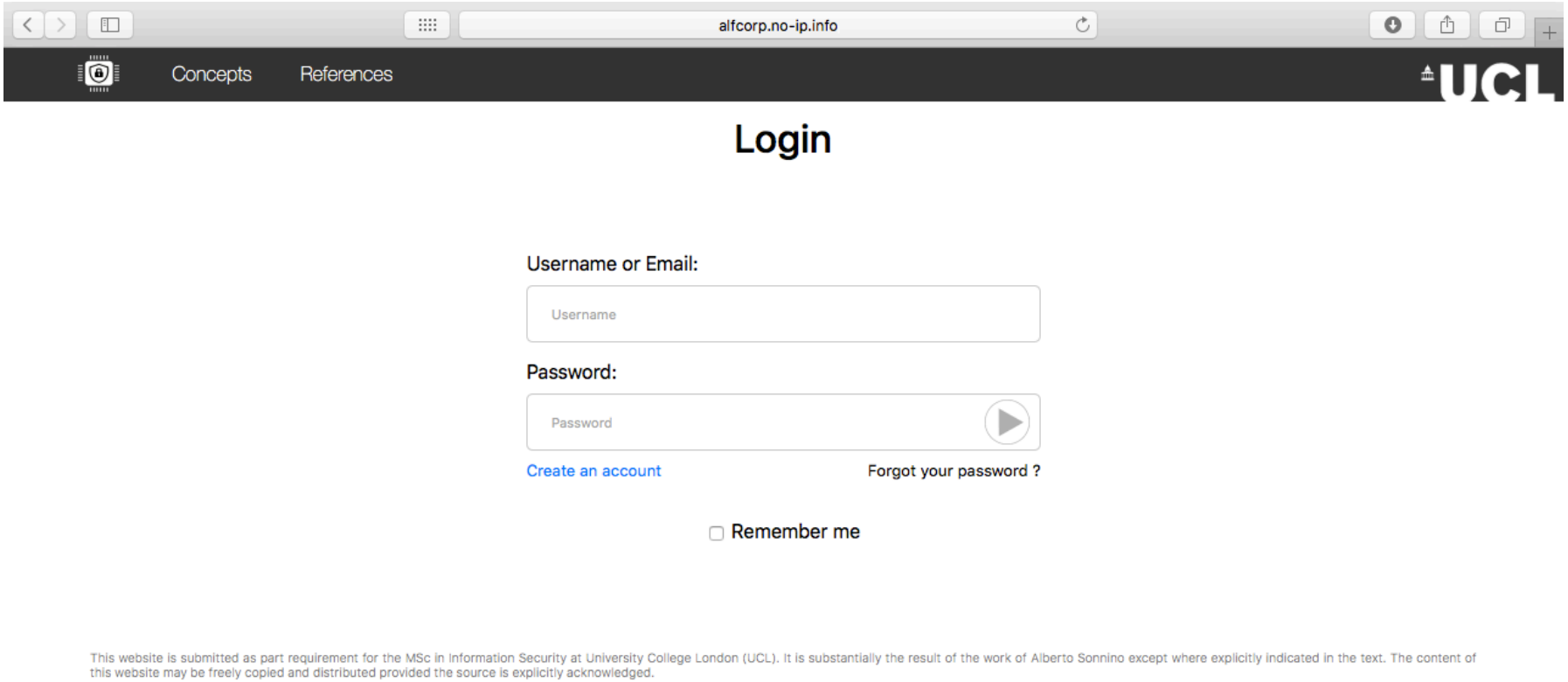
---

** All figures in this presentation come from reference [4].*

# Thank you for your attention

# Extras. Web Interface

- Login



# Extras. Web Interface

- Admin Panel

alfcorp.no-ip.info

Concepts References

## Welcome admin4test !

| User | Attributes | Admin | Edit |
|---|---|---|---|
| **user4test**<br>*alberto.sonnino@skynet.be* | m1 = 5<br>m2 = 15 | No | |
| **admin4test**<br>*alberto.sonnino@gmail.com* | m1 = 10<br>m2 = 20 | Yes | - |

Log Out Edit User Data

# Extras. Web Interface

- User Panel

alfcorp.no-ip.info

Concepts References

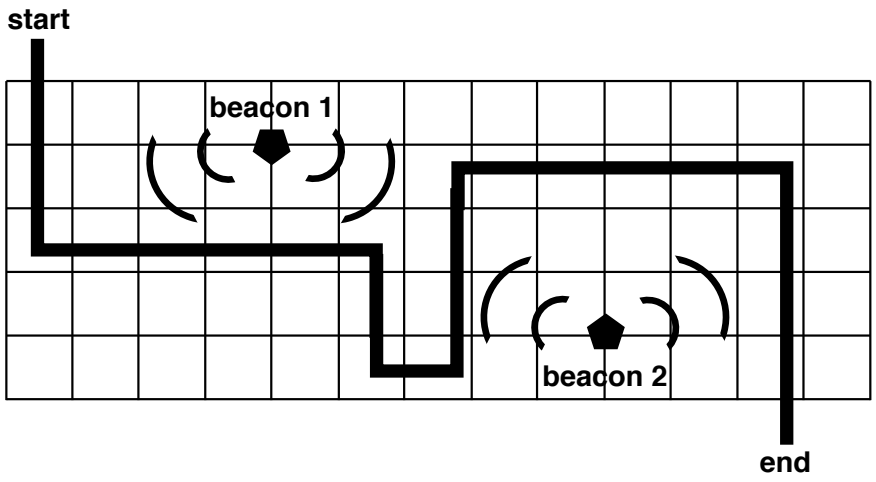
## Welcome user4test !

| User | Attributes | Admin |
|---|---|---|
| **user4test**<br>*alberto.sonnino@skynet.be* | m1 = 5<br>m2 = 15 | No |

Log Out Edit User Data

# Extras. RF Positioning System

- How does it works ?
  - Each beacon emits a signal with its name
  - The user detects it
  - localisation within a map

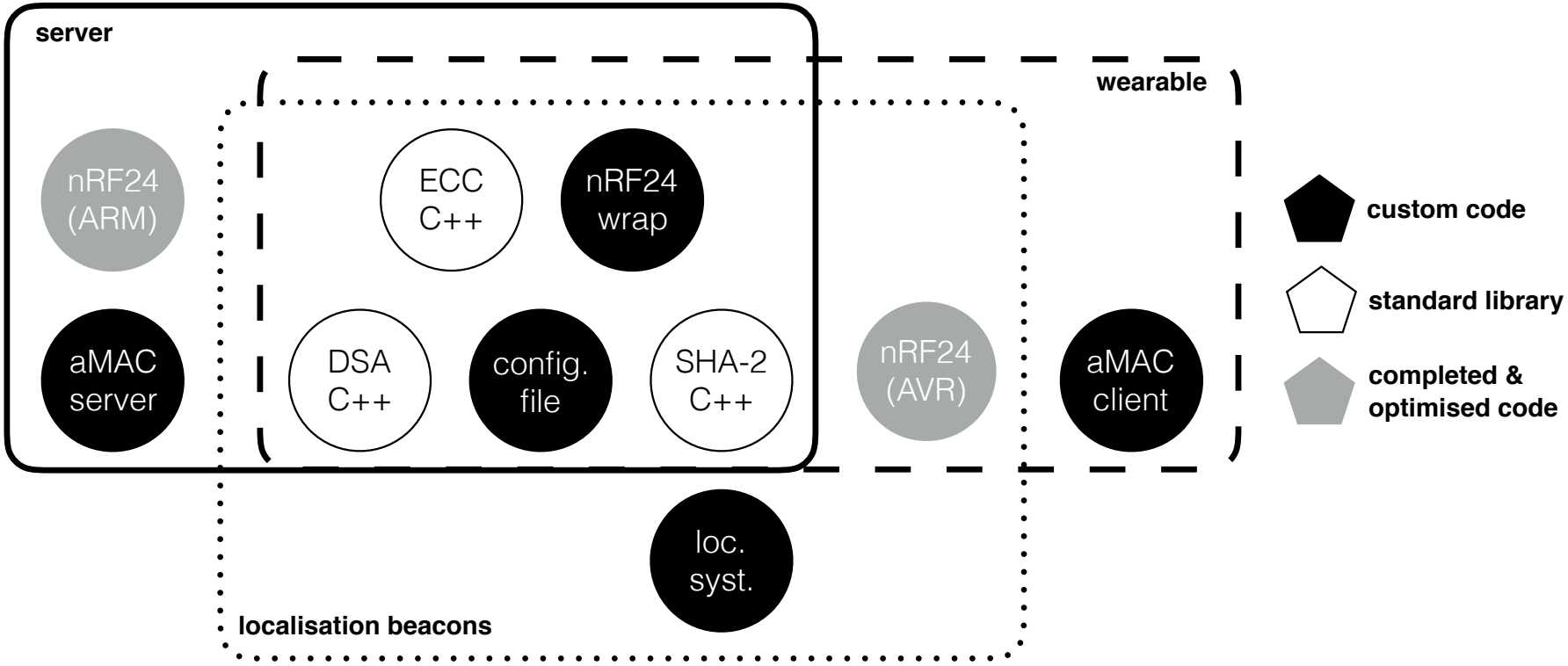



- Advantages :
  - Cost-effectiveness
  - Unremarkable hardware
  - Flexible
  - Works where other systems do not have signals

- Drawback:
  - Need security measures (signed messages, …)

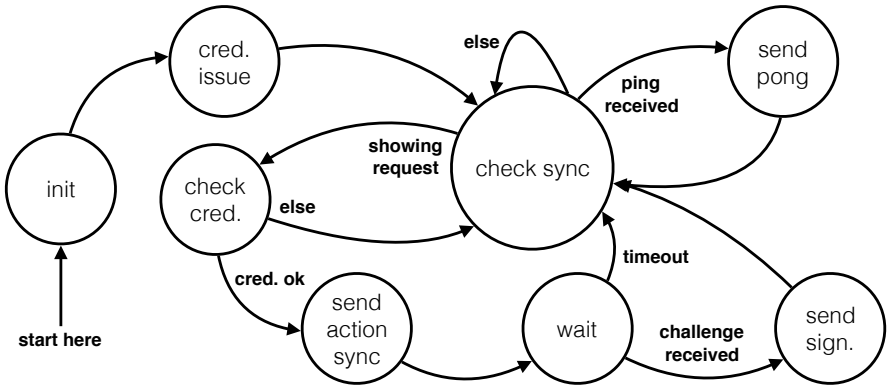
# Extras. Prototype Implementation (Details)

- Software & Libraries



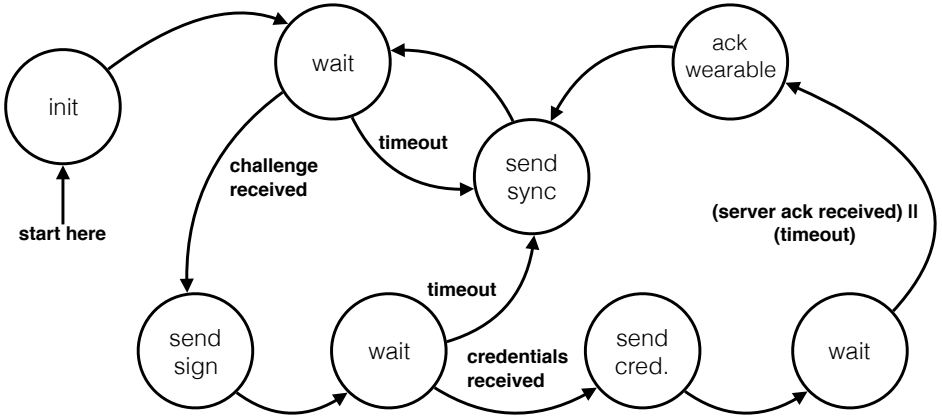
# Extras. Prototype Implementation (Details)

- Server & Beacon Implementation



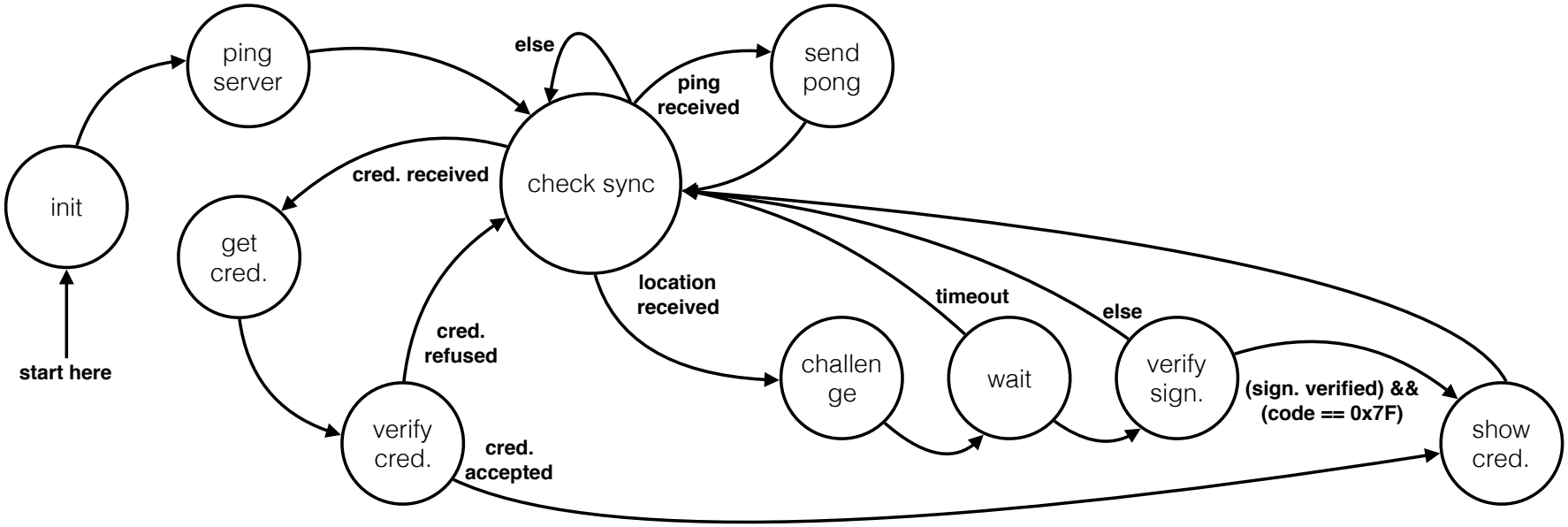

**Server**

**Beacon**



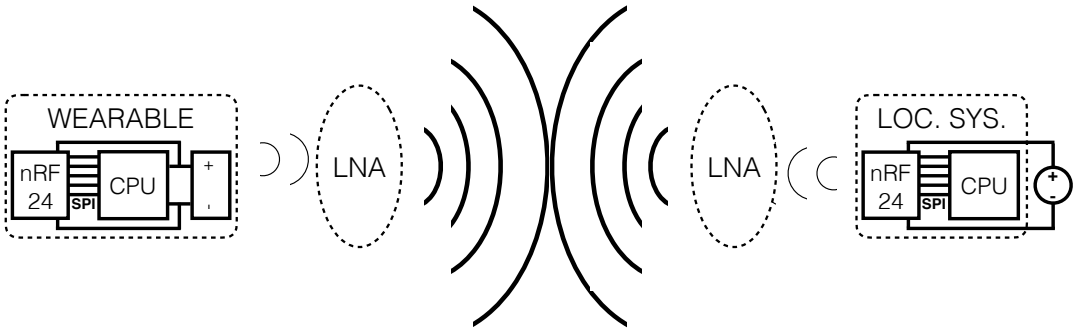
# Extras. Prototype Implementation (Details)

- Wearable Implementation

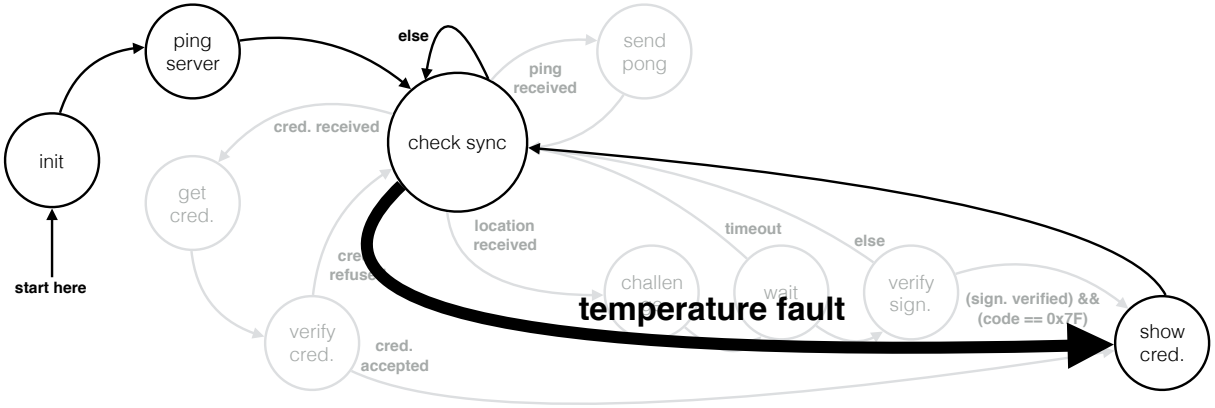


# Extras. Potential Attacks

- LNA Based Attack

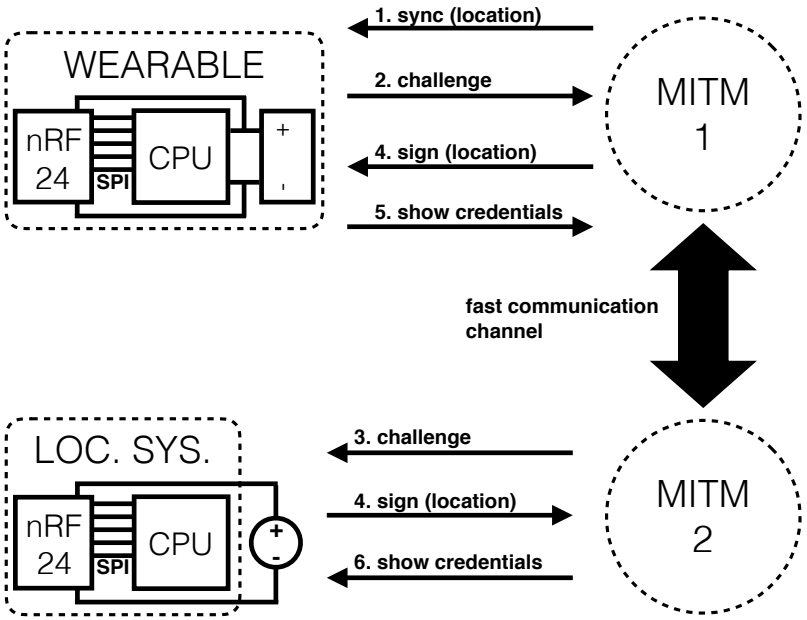



- Exploiting the Temperature Fault



# Extras. Potential Attacks

- Man-In-The-Middle




- Denial of Service (DoS)

## Vulnerable Pseudo-code

```
while (not RX_TIMEOUT)
    if (first load received)
        while (not RX_TIMEOUT)
            if (second load received)
            {
                [perform some actions]
                return
            }
return
```

## Mitigation

$$\text{RX\_TIMEOUT} = \frac{Q_3}{n_{RX}}$$