
# Nymi Band: Secure Fingerprint Template Storage

June 24, 2020

nymi™

# Overview

1. Fingerprint template generation and matching
2. Secure storage of sensitive data
3. Encryption
4. Fingerprint biometric performance





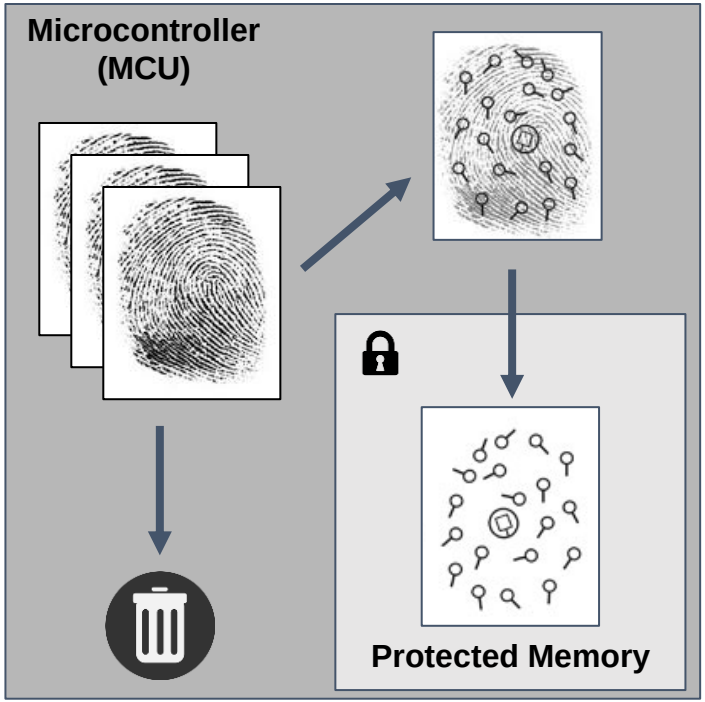
nymi™

# Fingerprint Template Generation

**Fingerprint Sensor**

**1.** Fingerprint images are analyzed by the sensor and sent to the MCU

**4.** Fingerprint images are discarded from memory upon enrollment completion




**2.** Unique features are extracted from fingerprint images to create a mathematical template

**3. Fingerprint template** is stored within protected memory on the MCU and is **never transmitted outside the MCU**





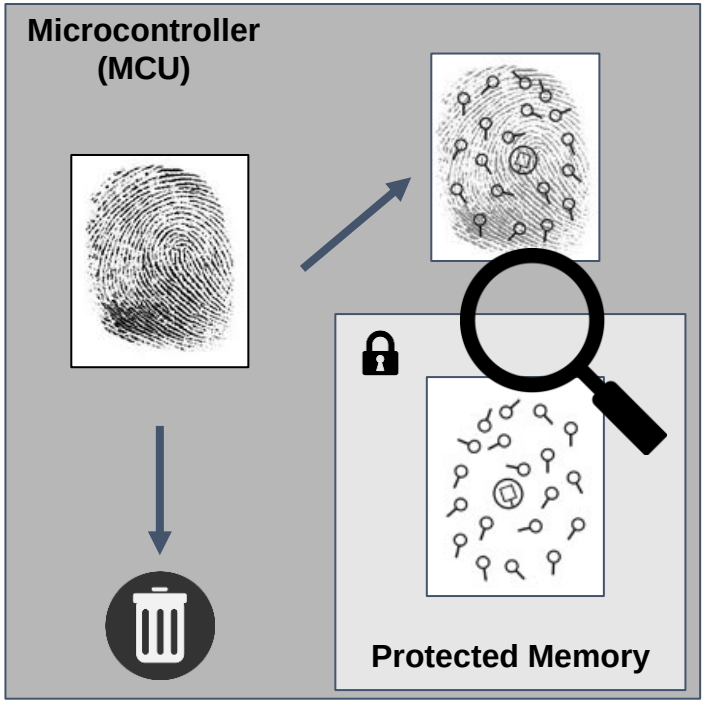
nymi™

# Fingerprint Match Process

**Fingerprint Sensor**

**1.** A fingerprint image is analyzed by the sensor and sent to the MCU

**4.** Fingerprint image is discarded from memory upon match completion




**2.** Unique features are extracted from the incoming fingerprint image

**3.** Features are compared against the stored template to determine if they match





nymi™

# Nymi Band Secure Storage

**How is sensitive data protected in the Nymi Band?**

- Fingerprint templates are generated and stored in protected memory inside the MCU
- Sensitive data cannot leave the MCU protected memory space

**Can data on the MCU be accessed through external communication lines?**

- **NO** - Physical communication lines (USB, serial) are disabled on the MCU
  - Even if the MCU were physically removed from the Nymi Band, physical communication lines remain disabled ensuring no access to MCU memory
- **NO** - Wireless communication (BLE, NFC) is restricted from protected memory access

**Can malicious firmware be loaded to gain wireless access to MCU memory?**

- **NO** - only encrypted firmware signed by Nymi can be loaded onto the Nymi Band
- **NO** - JTAG programming ports are permanently disabled during secure manufacturing

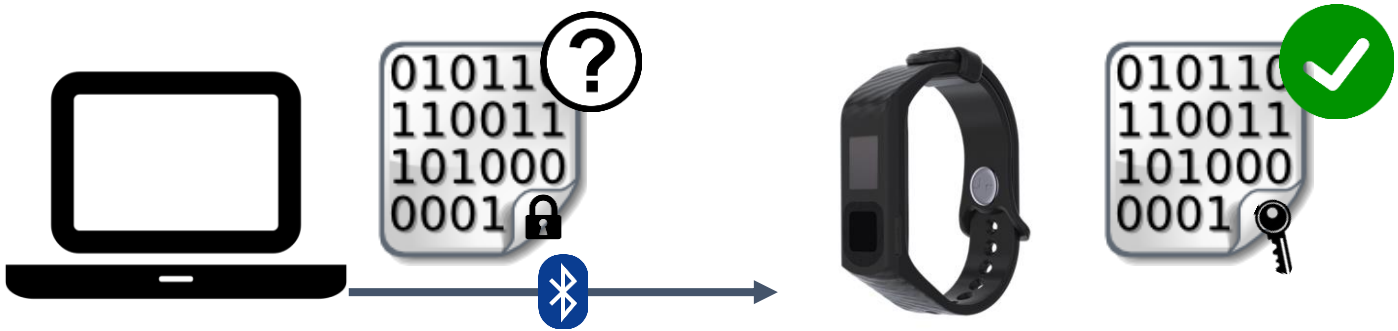
# Protecting Data

**Encryption** is used to protect information during communication from being read

**Signing** ensures information being communicated is from a legitimate source

**Why does Nymi encrypt and sign firmware?**

- Firmware is communicated to the Nymi Band
- Signing is used to ensure incoming firmware is legitimate and has not been externally compromised, encryption is used to ensure confidentiality







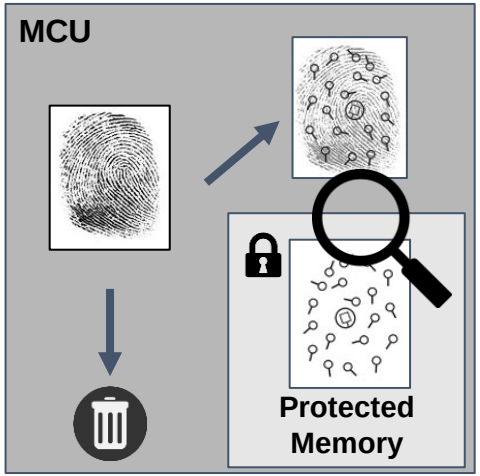

nymi™

# Protecting Data

## Encryption is used to protect sensitive information during communication

### What is a fingerprint template?

- A mathematical representation of distinct fingerprint features




### When are fingerprint templates encrypted?

- When they are stored and processed in different locations (servers, hard drives, external memory, etc.)

### Why does Nymi not encrypt fingerprint templates?

- Fingerprint templates are generated and read only in the MCU
- There is no data communication to be encrypted
- Templates are protected by making them inaccessible
- Nymi takes the same approach to protecting our sensitive key material on the Nymi Band

# Fingerprint FAR Performance

**What are the chances of another individual being able to match their fingerprint to the enrolled template?**

- Nymi Band 2.0 has a false acceptance rate (FAR) of 3.1 in 50,000
- Updated software in Nymi Band 3.0 will have an FAR of 1 in 500,000
- ECG liveness detection is used to mitigate the use of fake fingerprints





nymi™