1. Introduction (Giới thiệu)

Tài liệu này được xây dựng nhằm mô tả các yêu cầu phần mềm và hệ thống cho dự án IOT-Smart-Doorlock-with-RFID-and-OTP-using-ESP32. Mục tiêu chính là định nghĩa rõ ràng các chức năng, đặc điểm kỹ thuật, ràng buộc và phạm vi của hệ thống, từ đó làm cơ sở cho việc thiết kế, lập trình, kiểm thử và triển khai.
Dự án hướng đến việc nâng cao tính bảo mật và tính tiện dụng của hệ thống khóa cửa truyền thống, thông qua cơ chế xác thực hai lớp.
Hệ thống sẽ cho phép người dùng mở khóa cửa thông qua hai cách:

- Xác thực RFID – quẹt thẻ RFID hợp lệ.
- Xác thực OTP – nhập mã OTP được gửi tới email hoặc ứng dụng di động.
- Xác thực PIN - nhập mã PIN đã được thiết lập từ trước

Nếu một trong ba cách được xác thực, cửa sẽ được điều khiển mở thông qua relay hoặc servo motor, sau đó tự động khóa lại sau một khoảng thời gian.

2. System Features (Các tính năng hệ thống / Functional Requirements)

ID	Requirement Description
R1	**Mở khóa bằng RFID**
R1.1	Hệ thống phải cho phép mở khóa bằng thẻ RFID hợp lệ.
R1.2	Hệ thống phải lưu trữ và quản lý danh sách thẻ RFID được phép sử dụng.
R1.3	Khi quét thẻ không hợp lệ, hệ thống phải từ chối và hiển thị cảnh báo.
R2	**Mở khóa bằng OTP (One-Time Password)**
R2.1	Hệ thống phải sinh OTP ngẫu nhiên và có thời hạn sử dụng (<60 giây).
R2.2	OTP phải được gửi đến người dùng qua ứng dụng di động/Telegram/email tùy cấu hình.
R2.3	Hệ thống chỉ mở khóa khi OTP nhập vào khớp và còn hiệu lực.
R3	**Mở khóa bằng PIN**
R3.1	Hệ thống phải cho phép người dùng nhập PIN cố định để mở khóa.
R3.2	Người dùng có thể thay đổi PIN thông qua giao diện quản lý.
R3.3	Khi nhập sai PIN nhiều lần liên tiếp, hệ thống phải khóa tạm thời và cảnh báo.
R4	**Quản lý mở khóa**
R4.1	ESP32 phải điều khiển khóa điện tử (servor) để mở hoặc đóng.
R4.2	Hệ thống phải có giao diện quản lý (Web/Mobile App) để thêm/xóa thẻ RFID, đổi PIN, tạo OTP.
R4.3	Hệ thống phải ghi lại log sự kiện (thẻ RFID được quét, OTP/PIN được nhập, trạng thái khóa).
R4.4	Hệ thống phải cho phép reset và cập nhật firmware qua OTA (Over-The-Air).

R1 – Mở khóa bằng RFID

R1.1. Hệ thống phải cho phép mở khóa bằng thẻ RFID hợp lệ.

- Thẻ RFID phải nằm trong danh sách đã đăng ký.
- Khi quét đúng thẻ hợp lệ, khóa phải mở trong ≤ 2 giây.
- Hệ thống phải phát tín hiệu xác nhận (LED xanh/buzzer).

R1.2. Hệ thống phải lưu trữ và quản lý danh sách thẻ RFID được phép sử dụng.

- Danh sách thẻ lưu trong bộ nhớ ESP32.

- Có thể thêm/xóa/sửa thẻ qua App/Web.
- Số lượng thẻ tối thiểu hệ thống lưu được ≥ 50.

R1.3. Khi quét thẻ không hợp lệ, hệ thống phải từ chối và hiển thị cảnh báo.
- LED đỏ sáng và phát âm cảnh báo.
- Hiển thị thông báo "RFID không hợp lệ" trên App (nếu đang kết nối).
- Sau 3 lần quét sai liên tiếp, khóa tạm vô hiệu hóa trong 1 phút.

R2 – Mở khóa bằng OTP (One-Time Password)

R2.1. Hệ thống phải sinh OTP ngẫu nhiên và có thời hạn sử dụng (< 60 giây).
- OTP dài 6 chữ số.
- Mỗi OTP chỉ dùng một lần.
- Hết hạn sau 60 giây kể từ khi sinh ra.

R2.2. OTP phải được gửi đến người dùng qua ứng dụng di động/Telegram/email tùy cấu hình.
- OTP gửi thành công trong ≤ 5 giây.
- Có thông báo "OTP đã được gửi" trên App.

R2.3. Hệ thống chỉ mở khóa khi OTP nhập vào khớp và còn hiệu lực.
- OTP hết hạn sẽ bị từ chối.
- Sau 3 lần nhập sai OTP liên tiếp → khóa tạm thời trong 2 phút.
- Mở khóa thành công phải có log sự kiện lưu lại.

R3 – Mở khóa bằng PIN

R3.1. Hệ thống phải cho phép người dùng nhập PIN cố định để mở khóa.
- PIN dài 4–6 chữ số.
- Khi nhập đúng PIN, khóa mở trong ≤ 1 giây.
- Có tín hiệu xác nhận (LED xanh/buzzer).

R3.2. Người dùng có thể thay đổi PIN thông qua giao diện quản lý.
- Yêu cầu nhập PIN cũ hoặc OTP trước khi đổi.
- PIN mới không được trùng PIN cũ.
- Có thông báo xác nhận "PIN đã thay đổi thành công".

R3.3. Khi nhập sai PIN nhiều lần liên tiếp, hệ thống phải khóa tạm thời và cảnh báo.
- Sau 5 lần sai → khóa vô hiệu hóa trong 5 phút.
- Buzzer kêu ngắn 3 lần, LED đỏ nhấp nháy.
- Ghi log sự kiện sai PIN.

R4 – Quản lý mở khóa

R4.1. ESP32 phải điều khiển khóa điện tử (servo/relay) để mở hoặc đóng.
- Lệnh mở/đóng từ App → phản hồi trong ≤ 2 giây.
- Trạng thái khóa (mở/đóng) phải hiển thị trên App.
- Servo/relay phải hoạt động ổn định ≥ 50.000 chu kỳ.

R4.2. Hệ thống phải có giao diện quản lý (Web/Mobile App).
- Thêm/xóa thẻ RFID.
- Đổi PIN.
- Sinh OTP thủ công.
- Cấu hình kênh gửi OTP (SMS/Telegram/email).

R4.3. Hệ thống phải ghi lại log sự kiện.
- Log gồm: loại sự kiện (RFID/OTP/PIN), kết quả (thành công/thất bại), thời gian.
- Lưu tối thiểu 1000 sự kiện trong bộ nhớ.
- Có chức năng tải log xuống App.

R4.4. Hệ thống phải cho phép reset và cập nhật firmware qua OTA (Over-The-Air).
- Reset bằng nút cứng hoặc lệnh App.
- Firmware mới tải về phải được kiểm tra checksum.
- Khi cập nhật OTA, hệ thống vẫn đảm bảo an toàn (tự rollback nếu lỗi).

3. Non-Functional Requirements (Yêu cầu phi chức năng)

ID	Requirement Description
R5	Thời gian phản hồi khi quét RFID, nhập OTP hoặc PIN không vượt quá 2 giây.
R6	Hệ thống phải hoạt động liên tục 24/7 với tỉ lệ lỗi < 1%.
R7	Dữ liệu OTP/PIN phải được mã hóa khi truyền, và giao tiếp phải sử dụng HTTPS/TLS.
R8	Hệ thống phải tiêu thụ điện năng thấp, có thể dùng pin/UPS trong trường hợp mất điện.
R9	Hệ thống phải dễ mở rộng để tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa…).
R10	Giao diện người dùng phải thân thiện, hỗ trợ ít nhất tiếng Anh và tiếng Việt.

R5 – Thời gian phản hồi
- RFID/OTP/PIN phải được xử lý trong ≤ 2 giây.
- Nếu vượt ngưỡng thì hệ thống phải ghi log sự kiện lỗi.

R6 – Độ tin cậy hệ thống
- Hệ thống phải hoạt động liên tục 24/7 với uptime ≥ 99%.
- Có cơ chế tự khởi động lại khi treo.

- Khi mất mạng, RFID/PIN vẫn hoạt động offline.
- Tuổi thọ phần cứng tối thiểu 2 năm.

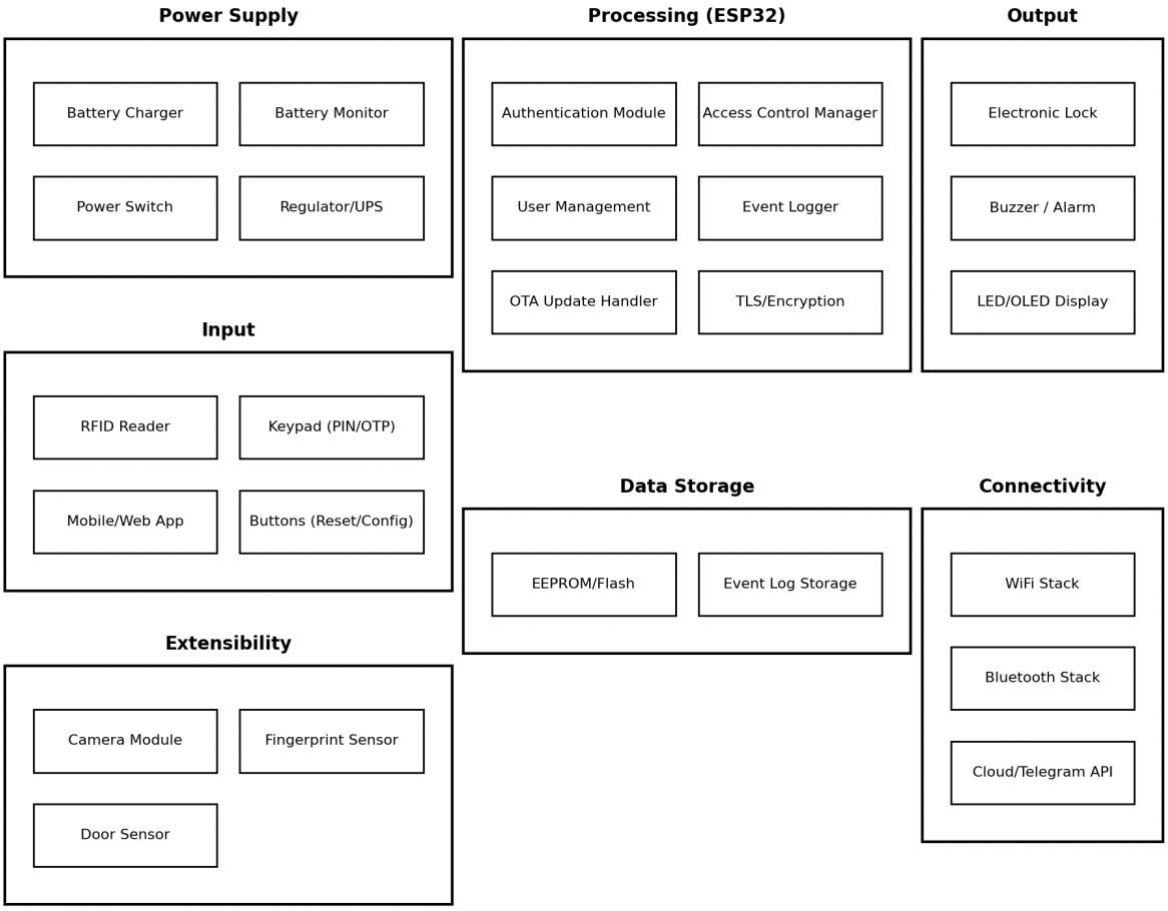
R7 – Bảo mật dữ liệu
- OTP/PIN phải được mã hóa (AES-128 trở lên).
- Giao tiếp sử dụng HTTPS/TLS.
- Không được lưu OTP dưới dạng plaintext.

R8 – Tiêu thụ năng lượng
- Có pin/UPS dự phòng ≥ 4 giờ trong trường hợp mất điện.
- Cảnh báo pin yếu hiển thị trên App.

R9 – Khả năng mở rộng
- Hỗ trợ tích hợp thêm cảm biến (camera, vân tay, cảm biến cửa).
- Cho phép giao tiếp mở rộng qua UART/I2C/SPI.
- Có thể quản lý cảm biến bổ sung qua App/Web.

R10 – Giao diện người dùng
- Giao diện App/Web phải trực quan, thao tác mở khóa tối đa 2 bước.
- Hiển thị rõ ràng trạng thái khóa (mở/đóng).
- Hỗ trợ song ngữ Anh/Việt, cho phép đổi ngôn ngữ trong cài đặt.

4. System architecture (Kiến trúc hệ thống)



5. Use case modelling

Use Case Name	**Unlock with RFID**
Use Case ID	UC01
Scope	IoT Smart Doorlock (hardware + mobile/web app)
Primary Actor(s)	User
Stakeholders and Interests	User: muốn mở khóa nhanh chóng bằng thẻ RFID. System Owner: muốn đảm bảo chỉ thẻ hợp lệ mới mở được khóa.
Preconditions	Người dùng có thẻ RFID hợp lệ đã được đăng ký.
Postconditions	Khóa mở nếu thẻ hợp lệ. Log sự kiện được ghi lại.

Main Flow of Events	1. Người dùng quẹt thẻ RFID. 2. Hệ thống đọc ID thẻ. 3. Hệ thống so sánh với danh sách thẻ hợp lệ. 4. Nếu hợp lệ → điều khiển khóa mở.
Alternative Flow	Nếu thẻ không hợp lệ → hệ thống từ chối, hiển thị cảnh báo, ghi log.
Exception Flows	RFID reader bị lỗi phần cứng → báo lỗi cho người dùng.
Includes	UC07 (Điều khiển khóa điện tử), UC05 (Ghi log sự kiện).
Extends	None
Special Requirements	Thời gian phản hồi < 2s (R5).
Assumptions	Thẻ RFID đã được add vào hệ thống.
Notes	Có thể mở rộng với nhiều loại thẻ RFID khác nhau.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**Unlock with OTP**
Use Case ID	UC02
Scope	IoT Smart Doorlock (hardware + mobile/web app)
Primary Actor(s)	User
Stakeholders and Interests	User: muốn mở khóa từ xa bằng OTP/ System Owner: đảm bảo OTP hợp lệ và an toàn.
Preconditions	Người dùng đã đăng ký tài khoản, có app/Telegram/email.
Postconditions	Nếu OTP hợp lệ → khoá mở. Nếu OTP sai hoặc hết hạn → từ chối, ghi log.
Main Flow of Events	1. Người dùng yêu cầu OTP qua app. 2. Hệ thống sinh OTP và gửi qua kênh cấu hình (Telegram/email/app). 3. Người dùng nhập OTP trên app.

	4. Hệ thống xác thực OTP. 5. Nếu đúng → mở khóa.
Alternative Flow	OTP hết hạn (<60s) → báo lỗi, yêu cầu nhập lại.
Exception Flows	Mạng lỗi → OTP không gửi đi được.
Includes	UC07 (Điều khiển khóa điện tử), UC05 (Ghi log sự kiện).
Extends	None
Special Requirements	OTP phải mã hóa khi truyền (R7).
Assumptions	Người dùng có kết nối mạng.
Notes	OTP chỉ dùng một lần.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**Unlock with PIN**
Use Case ID	UC03
Scope	IoT Smart Doorlock keypad input
Primary Actor(s)	User
Stakeholders and Interests	User: muốn mở khóa bằng PIN cá nhân. System Owner: đảm bảo an toàn, khóa khi sai nhiều lần.
Preconditions	PIN đã được đăng ký.
Postconditions	Khóa mở nếu PIN đúng. Nếu sai nhiều lần → hệ thống khóa tạm thời, cảnh báo.
Main Flow of Events	1. Người dùng nhập PIN. 2. Hệ thống so khớp với PIN lưu trữ. 3. Nếu đúng → mở khóa.
Alternative Flow	1. PIN sai → báo lỗi, ghi log.

	2. Nhập sai liên tiếp → khóa tạm thời.
Exception Flows	Keypad bị hỏng → báo lỗi.
Includes	UC07 (Điều khiển khóa điện tử), UC05 (Ghi log sự kiện).
Extends	None
Special Requirements	Thời gian phản hồi < 2s (R5).
Assumptions	Người dùng nhớ PIN.
Notes	Có thể đổi PIN qua UC04.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**Manage Access (RFID, PIN, OTP)**
Use Case ID	UC04
Scope	IoT Smart Doorlock web/mobile app
Primary Actor(s)	Admin
Stakeholders and Interests	Admin: muốn thêm/xóa thẻ RFID, đổi PIN, tạo OTP. System Owner: muốn quản lý tập trung, bảo mật.
Preconditions	Admin đã đăng nhập.
Postconditions	Thay đổi được áp dụng, log sự kiện ghi lại.
Main Flow of Events	1. Admin mở giao diện quản lý. 2. Admin thêm/xóa thẻ RFID hoặc đổi PIN. 3. Hệ thống cập nhật dữ liệu.
Alternative Flow	Nếu thẻ đã tồn tại → báo lỗi.
Exception Flows	Mất kết nối server → thao tác thất bại.
Includes	UC05 (Ghi log sự kiện).

Extends	None
Special Requirements	Giao diện thân thiện, đa ngôn ngữ (R10).
Assumptions	Admin có quyền hợp lệ.
Notes	Có thể tích hợp thêm xác thực đa yếu tố.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**Log Events**
Use Case ID	UC05
Scope	IoT Smart Doorlock system
Primary Actor(s)	System
Stakeholders and Interests	System Owner: muốn biết ai mở khóa, lúc nào, bằng phương thức gì.
Preconditions	Hệ thống hoạt động bình thường.
Postconditions	Sự kiện được lưu trữ vào log.
Main Flow of Events	1. Hệ thống ghi lại mọi hành động mở khóa, thêm/xóa user. 2. Log lưu vào EEPROM/Flash.
Alternative Flow	None
Exception Flows	Bộ nhớ đầy → báo lỗi.
Includes	None
Extends	None
Special Requirements	Log phải bền vững, không mất khi mất điện (R8).
Assumptions	Bộ nhớ khả dụng.

Notes	Có thể đồng bộ log lên cloud.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**System Update and Maintenance**
Use Case ID	UC06
Scope	IoT Smart Doorlock OTA update
Primary Actor(s)	Admin
Stakeholders and Interests	Admin: muốn cập nhật firmware từ xa. System Owner: muốn đảm bảo hệ thống luôn an toàn
Preconditions	Thiết bị có kết nối internet.
Postconditions	Firmware được cập nhật, hệ thống khởi động lại.
Main Flow of Events	1. Admin chọn “Cập nhật OTA” trên app. 2. Hệ thống tải firmware mới. 3. ESP32 cập nhật và khởi động lại.
Alternative Flow	Người dùng chọn “Reset” hệ thống.
Exception Flows	Kết nối mạng lỗi → OTA thất bại.
Includes	UC05 (Ghi log sự kiện).
Extends	None
Special Requirements	Quá trình OTA phải an toàn, có TLS (R7).
Assumptions	Firmware hợp lệ.
Notes	Có thể rollback nếu OTA thất bại.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

Use Case Name	**Control Electronic Lock**
Use Case ID	UC07
Scope	IoT Smart Doorlock hardware
Primary Actor(s)	ESP32 (System)
Stakeholders and Interests	User: muốn khóa mở nhanh chóng. System Owner: muốn an toàn, không mở ngoài ý muốn.
Preconditions	Yêu cầu mở khóa hợp lệ từ RFID/OTP/PIN.
Postconditions	Khóa điện tử mở hoặc đóng.
Main Flow of Events	1. Hệ thống gửi tín hiệu điều khiển servo. 2. Servo mở hoặc đóng khóa.
Alternative Flow	None
Exception Flows	Servo bị kẹt → báo lỗi.
Includes	None
Extends	None
Special Requirements	Phản hồi < 2s (R5), tiêu thụ điện thấp (R8).
Assumptions	Nguồn điện đủ.
Notes	Có thể mở rộng với nhiều loại khóa điện tử.
Author	[Your Name]
Date	[Date of Use Case Creation or Modification]

6. Use Case-Requirement Traceability Matrix

	UC01	UC02	UC03	UC04	UC05	UC06	UC07
R1.1	X						X
R1.2				X			

R1.3	X				X		
R2.1		X					
R2.2		X					
R2.3		X					X
R3.1			X				X
R3.2				X			
R3.3			X		X		
R4.1							X
R4.2				X			
R4.3					X		
R4.4						X	
R5	X	X	X				X
R6		X				X	X
R7						X	
R8							X
R9				X			X
R10				X			

7. External Interface Requirements (Yêu cầu giao diện ngoài)

7.1. Giao diện người dùng (User Interface)

- **Ứng dụng di động/Web**:
  - Hiển thị trạng thái cửa (mở/đóng).
  - Cho phép nhập OTP để mở khóa.
  - Quản trị viên có thể thêm/xóa thẻ RFID, thay đổi PIN, xem nhật ký truy cập.
  - Hỗ trợ ngôn ngữ: Tiếng Việt, Tiếng Anh.
- **Màn hình LCD/OLED**:
  - Hiển thị hướng dẫn: "Quét thẻ RFID", "Nhập OTP/PIN", "Thành công/Thất bại".
  - Đèn LED và còi báo trạng thái (Xanh = thành công, Đỏ = thất bại, Vàng = đang xử lý).
- **Keypad**: nhập OTP và PIN.

7.2. Giao diện phần cứng (Hardware Interface)

- ESP32 kết nối với:
  - RFID RC522 (SPI/I2C).
  - Relay/Servo motor (GPIO).
  - Keypad (GPIO).
  - LCD/OLED (I2C/SPI).
  - Buzzer + LED (GPIO).
- Nguồn cấp 5V–12V, có pin dự phòng.

7.3. Giao diện phần mềm (Software Interface)

- **Firmware trên ESP32**: Arduino C++, thư viện WiFi, HTTPClient, MFRC522, Keypad, ArduinoJson.
- **Server/Cloud**: Backend (Node.js/Flask/Django), cơ sở dữ liệu MySQL/MongoDB.
- **Ứng dụng di động/Web**: React Native/Flutter/ReactJS, kết nối server qua REST API (HTTPS, JSON).

7.4. Giao diện truyền thông (Communication Interface)

- Wi-Fi 802.11 b/g/n.
- Giao thức HTTP/HTTPS hoặc MQTT giữa ESP32 và server.
- Giao tiếp UART/I2C/SPI/GPIO giữa ESP32 và các module.