Audyt i ćwiczenie DIY

Lista kontrolna audytu i czytnik kart na ESP32.

- Audyt fizyczny serwerowni i biura: lista kontrolna i własny czytnik kart

Audyt fizyczny serwerowni i biura: lista kontrolna i własny czytnik kart

Poziom: średnio

Dotyczy: obchód serwerowni i biura w Pamiątkowie, magazyn w Swarzędzu, ESP32, ESPHome, moduł RC522 albo PN532

Czas: ~90 min

Audyt fizyczny to obchód z listą w ręku: sprawdzamy drzwi, klucze, karty, kamery, czujki, sufity, szafy i biurka, a wynik zapisujemy w raporcie z terminami poprawek. Podajemy listę kontrolną, którą co kwartał odhaczamy my, a raz w roku pan Wojtek, oraz sposób raportowania. Na końcu budujemy czytnik kart na ESP32, który uczy, dlaczego numer karty nie jest hasłem.

Skróty użyte na tej stronie (28)

Skrót	Co znaczy
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
EM4100	układ firmy EM Microelectronic w najprostszych kartach 125 kHz, który po pobudzeniu tylko ogłasza stały, zapisany w fabryce numer
ESP32	Tani mikrokontroler z Wi-Fi i Bluetooth firmy Espressif: malutki komputer, z którego budujemy własne czujniki sieciowe
ESPHome	Oprogramowanie, które zamienia ESP32 w gotowy czujnik sieciowy bez pisania kodu od zera, a odczyty udostępnia przez sieć
HTTP	Hypertext Transfer Protocol: protokół stron WWW
I2C	Inter-Integrated Circuit: prosta dwuprzewodowa magistrala, którą mały układ (np. czujnik) rozmawia z mikrokontrolerem
IRQ	Interrupt Request: wyprowadzenie modułu, którym zgłasza on płytce zdarzenie, w naszym ćwiczeniu niepodłączone
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

Skrót	Co znaczy
MFRC522	układ firmy NXP w module RC522, który czyta karty 13,56 MHz zgodne z ISO/IEC 14443 A
MIFARE	marka kart zbliżeniowych firmy NXP: Classic ze złamanym szyfrem Crypto-1 i DESFire z szyfrowaniem AES
MISO	Master In Slave Out: przewód magistrali SPI, którym moduł wysyła dane do płytki
MOSI	Master Out Slave In: przewód magistrali SPI, którym płytka wysyła dane do modułu
NXP	NXP Semiconductors: producent układów do kart zbliżeniowych, w tym MIFARE i MFRC522
OSDP	Open Supervised Device Protocol: otwarty protokół rozmowy czytnika kart z kontrolerem, z nadzorem przewodów i szyfrowaniem, następca interfejsu Wiegand
PN532	układ i moduł firmy NXP do czytania kart NFC, z wyborem interfejsu I2C, SPI albo UART
RC522	popularny tani moduł z układem MFRC522 do odczytu numeru UID kart 13,56 MHz
RDM6300	tani moduł do odczytu kart 125 kHz EM4100, który przekazuje numer karty przez UART
RFID	Radio Frequency Identification: identyfikacja przez fale radiowe, bez konieczności widzenia znacznika
RST	Reset: wyprowadzenie modułu, którym płytka go restartuje, w ćwiczeniu podłączone do GPIO22
S3	Simple Storage Service: magazyn plików w chmurze AWS
SCK	Serial Clock: przewód zegarowy magistrali SPI, według którego płytka i moduł wymieniają bity
SDA	Serial Data: przewód danych magistrali I2C, którym czujnik i mikrokontroler wymieniają bity
UART	Universal Asynchronous Receiver Transmitter: łącze szeregowe z dwoma przewodami (nadawanie i odbiór), którym płytka rozmawia na przykład z czujnikiem pyłu PMS5003
UID	User ID: numer użytkownika w Linuksie
USB	Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS

Fiszka

Ta fiszka dotyczy ćwiczenia z czytnikiem kart z dalszej części strony. Instalację ESPHome i generowanie klucza API opisuje strona Kontaktrony i czujki ruchu w praktyce: wybór, montaż i własny moduł (DIY), a tutaj korzystamy z tych samych kroków.

TYLKO ODCZYT

Sprawdzenie pliku: esphome config esp08-czytnik.yaml

```
esphome config esp08-czytnik.yaml
```

Sprawdza składnię pliku i wypisuje, jak ESPHome go zrozumiał, a na końcu `Configuration is valid!`. Nic nie zmienia, więc sięgamy po tę komendę przed każdym wgraniem programu.

ESPHome = Oprogramowanie, które zamienia ESP32 w gotowy czujnik sieciowy bez pisania kodu od zera, a odczyty udostępnia przez sieć · **esphome** = ESPHome: buduje i wgrywa oprogramowanie na ESP32 z pliku YAML, pokazuje logi urządzenia

TYLKO ODCZYT

Wgranie programu przez USB: esphome run esp08-czytnik.yaml

```
esphome run esp08-czytnik.yaml
```

Buduje program, wgrywa go na płytkę przez USB i od razu pokazuje dziennik. Zmienia zawartość płytki, ale nie dotyka żadnego innego systemu.

USB = Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne · **esphome** = ESPHome: buduje i wgrywa oprogramowanie na ESP32 z pliku YAML, pokazuje logi urządzenia

TYLKO ODCZYT

Podgląd dziennika: esphome logs esp08-czytnik.yaml

```
esphome logs esp08-czytnik.yaml
```

Pokazuje na żywo komunikaty z płytki, w tym numer karty po każdym przyłożeniu. Przerywamy go skrótem Ctrl+C.

Przykład (kształt wyniku, bez znaczników czasu, nie z uruchomienia na hostach Zielonej):

```
[I][rc522]: Found new tag '74-10-37-94'
[I][czytnik]: UID karty: 74-10-37-94
```

esphome = ESPHome: buduje i wgrywa oprogramowanie na ESP32 z pliku YAML, pokazuje logi urządzenia

TYLKO ODCZYT

Plik z hasłami: secrets.yaml

```
# secrets.yaml, obok pliku esp08-czytnik.yaml
wifi_ssid: "NazwaSieciBiurowej"
wifi_haslo: "HasloWifi"
api_klucz: "Tu wklejamy klucz z openssl rand -base64 32"
ota_haslo: "HasloOta"
web_uzytkownik: "nazwa_usera"
web_haslo: "HasloWebServera"
```

Wartości są placeholderami do podmiany. Hasła trzymamy w tym pliku, a w pliku konfiguracyjnym odwołujemy się do nich przez `!secret`.

PLIK KONFIGURACYJNY

Plik konfiguracyjny ESPHome: esp08-czytnik.yaml

```
esphome:
  name: esp08
  friendly_name: Czytnik kart, ćwiczenie

esp32:
  board: esp32dev
  framework:
    type: esp-idf

logger:

# Ćwiczenie stoi na biurku, więc wystarczy Wi-Fi. Moduł w serwerowni dostałby Ethernet z
PoE.
wifi:
  ssid: !secret wifi_ssid
  password: !secret wifi_haslo

api:
  encryption:
    key: !secret api_klucz
```

```
  reboot_timeout: 0s

ota:
  - platform: esphome
    password: !secret ota_haslo

web_server:
  port: 80
  auth:
    username: !secret web_uzytkownik
    password: !secret web_haslo

# Magistrala SPI: SCK, MOSI i MISO modułu RC522
spi:
  clk_pin: GPIO18
  mosi_pin: GPIO23
  miso_pin: GPIO19

# Czytnik RC522: SDA modułu to wejście wyboru układu (CS)
rc522_spi:
  cs_pin: GPIO5
  reset_pin: GPIO22
  update_interval: 1s
  on_tag:
    - lambda: |-
        ESP_LOGI("czytnik", "UID karty: %s", x.c_str());
        id(ostatni_uid).publish_state(x);

text_sensor:
  - platform: template
    id: ostatni_uid
    name: "ostatni_uid"

# Własna karta testowa: UID wpisujemy po odczycie z dziennika (poniżej wartość
przykładowa)
binary_sensor:
  - platform: rc522
    uid: 74-10-37-94
    name: "karta_testowa_1"
```

```
    filters:
      - delayed_off: 3s
```

Plik sprawdziliśmy poleceniem `esphome config` i zwrócił `Configuration is valid!`. Wartość `74-10-37-94` pochodzi z dokumentacji ESPHome i jest przykładowa, a własny UID odczytujemy z dziennika po pierwszym przyłożeniu karty [1].

ESPHome = Oprogramowanie, które zamienia ESP32 w gotowy czujnik sieciowy bez pisania kodu od zera, a odczyty udostępnia przez sieć · **UID** = User ID: numer użytkownika w Linuksie · **id** = pokaż użytkownika, jego numer UID oraz grupy, do których należy

PLIK KONFIGURACYJNY

Wariant z modułem PN532: pn532_i2c

```
i2c:
  sda: GPIO21
  scl: GPIO22

pn532_i2c:
  update_interval: 1s
  on_tag:
    - lambda: |-
        ESP_LOGI("czytnik", "UID karty: %s", x.c_str());
```

Ten fragment zastępuje w pliku powyżej bloki `spi`, `rc522_spi` oraz `binary_sensor` z platformą `rc522`. Moduł PN532 ma przełączniki wyboru interfejsu, więc przed podłączeniem ustawiamy go na I2C zgodnie z opisem modułu [2]. Pełny plik z tym wariantem także przeszedł `esphome config`.

PN532 = układ i moduł firmy NXP do czytania kart NFC, z wyborem interfejsu I2C, SPI albo UART · **I2C** = Inter-Integrated Circuit: prosta dwuprzewodowa magistrala, którą mały układ (np. czujnik) rozmawia z mikrokontrolerem · **UID** = User ID: numer użytkownika w Linuksie

PLIK KONFIGURACYJNY

Wariant dla kart 125 kHz: rdm6300

```
uart:
  rx_pin: GPIO16
  baud_rate: 9600
```

```
rdm6300:
  on_tag:
    - lambda: |-
        ESP_LOGI("czytnik", "ID karty 125 kHz: %d", (int) x);
```

To jest inny moduł niż RC522, bo karty 125 kHz mają inną częstotliwość niż karty 13,56 MHz. Czytnik RDM6300 obsługuje karty EM4100 i przekazuje identyfikator przez UART [3]. Przed podłączeniem sprawdzamy w opisie modułu napięcie zasilania i poziom logiczny wyjścia danych, bo płytka ESP32 pracuje na 3,3 V.

RC522 = popularny tani moduł z układem MFRC522 do odczytu numeru UID kart 13,56 MHz · **RDM6300** = tani moduł do odczytu kart 125 kHz EM4100, który przekazuje numer karty przez UART · **EM4100** = układ firmy EM Microelectronic w najprostszych kartach 125 kHz, który po pobudzeniu tylko ogłasza stały, zapisany w fabryce numer · **UART** = Universal Asynchronous Receiver Transmitter: łącze szeregowe z dwoma przewodami (nadawanie i odbiór), którym płytka rozmawia na przykład z czujnikiem pyłu PMS5003 · **ESP32** = Tani mikrokontroler z Wi-Fi i Bluetooth firmy Espressif: malutki komputer, z którego budujemy własne czujniki sieciowe

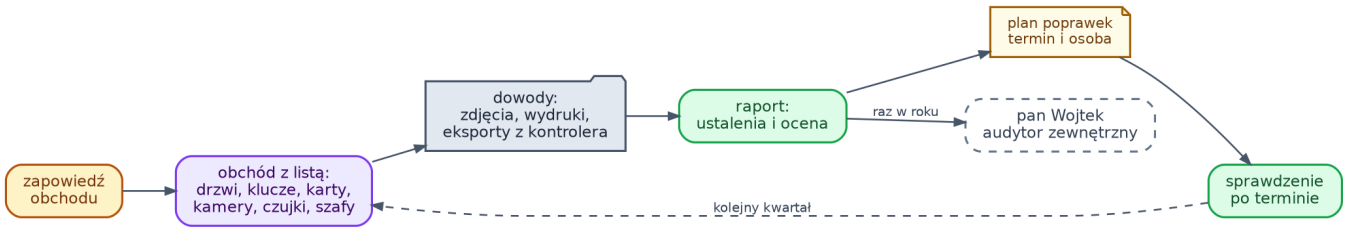
Z życia wzięte

Z ŻYCIA WZIĘTE

Wtorek, 10:00. Pan Wojtek wchodzi na obchód z kartką w ręku i zaczyna od korytarza IT, a nie od serwerowni. Unosi płytę sufitu podwieszanego nad drzwiami D3, świeci latarką w górę i pokazuje Tomkowi, że ściana serwerowni kończy się na wysokości sufitu podwieszanego, a nad nią biegnie otwarta przestrzeń przez cały korytarz. Dalej znajduje klucz tkwiący w zamku szafy R3 i drzwi D2 podparte klinem z tektury, bo „sprzątaczka tak wolała”.

Jak przebiega audyt

Audyt fizyczny jest obchodem wszystkich stref według tej samej listy, z dowodami i raportem. Robimy go w dwie osoby: jedna sprawdza, druga zapisuje, a role zamieniamy przy kolejnym kwartale, żeby osoba, która instalowała zamek, nie oceniała go sama. Raz w roku tę samą listę wypełnia pan Wojtek, zewnętrzny audytor, który nie zna naszych skrótów, więc pytania na liście piszemy tak, żeby rozumiał je bez objaśnień.



Rysunek 1. Obieg audytu: zapowiedź obchodu, obchód z listą, dowody, raport z ustaleniami i oceną, plan poprawek z terminem i osobą oraz sprawdzenie po terminie, a raz w roku raport trafia do pana Wojtka. Warto zauważyć, że ostatni krok wraca do obchodu w kolejnym kwartale, więc audyt jest pętlą, a nie jednorazowym zdarzeniem. (kliknięcie otwiera pełny rozmiar)

Zapowiadamy obchód prezesowi i osobie z agencji, jeśli alarm będzie rozbrajany, ale nie zapowiadamy go całej firmie, bo część kontroli polega na zobaczeniu stanu zwykłego dnia. Nie testujemy kart i kodów pracowników i nie próbujemy obejść zabezpieczeń na siłę. Próbę wejścia „za plecami” innej osoby, czyli tailgating, przeprowadzamy tylko za zgodą pana Zbigniewa i bez zaskakiwania konkretnych osób.

Lista kontrolna

Każdy wiersz ma wynik: zgodne, uwaga albo niezgodne. Przy uwagach i niezgodnościach robimy zdjęcie, jeśli nie ma na nim osób, i zapisujemy miejsce.

Drzwi i zamki

Co sprawdzamy	Jak	Dobry wynik
Drzwi D1, D2, D3 zamykają się same	otwieramy i puszczamy, patrzymy na samozamykacz	drzwi zamykają się i zatrzaskują
Drzwi nie są podparte	obchód o różnych porach	żaden klin, tektura ani stojak
Zawiasy i ościeżnica	oglądamy od strony zewnętrznej	zawiasy od strony chronionej albo zabezpieczone przed wyjęciem
Kontaktron drzwi serwerowni	otwieramy drzwi i patrzymy w Zabbixie	zdarzenie w ciągu kilku sekund
Alarm drzwi otwartych dłużej niż 5 minut	otwieramy drzwi na ponad 5 minut	powiadomienie dociera do zespołu IT
Wyjście bez karty	sprawdzamy klamkę i przycisk wyjścia	wyjść można z każdej strony bez karty

Klucze i karty

Co sprawdzamy	Jak	Dobry wynik
Spis kluczy mechanicznych	porównujemy spis z kluczami w sejfie i u osób	wiadomo, ile kluczy istnieje, kto je ma i gdzie
Klucze awaryjne	oglądamy miejsce przechowywania	zamknięte, z wpisem wydania
Karty aktywne a lista zatrudnionych	porównujemy eksport z kontrolera z listą z kadr i grupami AD	brak kart osób, które odeszły
Karty niewykorzystane od 90 dni	eksport z kontrolera	zablokowane albo potwierdzone przez właściciela strefy
Karty tymczasowe i zgubione	sprawdzamy rejestr	wszystkie rozliczone, zgubione zablokowane
Dziennik wejść	przeglądamy ostatnie 30 dni, szukamy wejść w nocy i w weekendy	każde wejście wyjaśnione, godziny zgodne z kamerami

Szczegóły kwartalnego audytu uprawnień opisuje strona Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień.

Kamery i alarm

Co sprawdzamy	Jak	Dobry wynik
Obraz z cam01, cam02, cam03	oglądamy podgląd na żywo	ostry, kąt na przejście, bez zasłonięcia
Data i godzina na nagraniu	porównujemy z zegarem	zgodne z `dc01`
Okres przechowywania	sprawdzamy najstarsze nagranie	zgodne z przyjętym okresem, nie dłuższe niż 3 miesiące
Oznaczenie monitoringu i informacja dla pracowników	oglądamy tablice, pytamy o pisemną informację	tablice widoczne, potwierdzenia pracowników zebrane
Pomieszczenia, w których kamer nie wolno mieć	obchód	brak kamer w toaletach, szatniach, stołówkach i palarniach
Test chodzenia po czujkach alarmu	idziemy przez każdą strefę przy uzbrojonym alarmie i patrzymy, czy czujka zgłasza ruch	każda czujka reaguje
Sabotaż czujek i centrali	otwieramy pokrywę czujki w trybie testowym	centrala zgłasza sabotaż
Lista osób do powiadomienia w agencji	pytamy agencję o aktualną listę	tylko osoby, które pracują i odbierają telefon
Akumulator centrali	sprawdzamy datę wymiany i test zaniku zasilania	w terminie, test zaliczony

Okna, ściany, sufity i podłogi

Co sprawdzamy	Jak	Dobry wynik
Okna biura i świetliki	oglądamy zamknięcia, kontaktrony, kraty	zamknięte, zabezpieczone, pod nadzorem alarmu
Serwerownia bez okien	oglądamy ściany i otwory	brak otworów poza przepustami
Ściana serwerowni do stropu	unosimy płytę sufitu podwieszanego w korytarzu IT i patrzymy w górę	ściana sięga stropu właściwego, a nie sufitu podwieszanego
Podłoga i dolna krawędź ścian	serwerownia ma podłogę zwykłą, więc oglądamy szczeliny przy ścianach i drzwiach	brak szczelin ani otworów, przez które da się wsunąć rękę
Przepusty kablowe i rura skroplin	oglądamy miejsca, gdzie kable i rury przechodzą przez ściany	zaślepione, bez wolnych otworów

Szafy i sprzęt

Co sprawdzamy	Jak	Dobry wynik
Szafy R1 do R5 zamknięte	sprawdzamy drzwi z przodu i z tyłu	zamknięte, klucze nie tkwią w zamkach
Klucze do szaf	porównujemy z listą wydania	każdy klucz ma właściciela
Porty USB i konsole serwerów	oglądamy zaślepki i podłączone urządzenia	brak niepodpisanych pendrive i adapterów
Konsola KVM lub sesja administratora	sprawdzamy blokadę ekranu	zablokowana po krótkim czasie bezczynności
Wolne gniazda sieciowe poza strefami S2 i S3	sprawdzamy, które gniazda są aktywne	gniazda w poczekalni i salach spotkań nieaktywne lub w osobnej sieci
Nośniki do zniszczenia	oglądamy pojemnik i ewidencję	zamknięty pojemnik, wpisy zgodne z liczbą nośników

Zasady dla szaf opisuje strona Szafa 19 cali: jednostka U, wymiary, nośność i rozplanowanie szaf R1 do R6, a nośniki przeznaczone do zniszczenia strona Niszczenie nośników: DIN 66399, kasowanie dysków i protokół.

Biuro: ekrany i czysty stół

Co sprawdzamy	Jak	Dobry wynik
Ekrany widoczne z korytarza, recepcji i okien	stajemy w miejscu gościa	żaden ekran z danymi nie jest widoczny
Blokada ekranu	sprawdzamy kilka stanowisk po godzinach pracy	zablokowane

Co sprawdzamy	Jak	Dobry wynik
Hasła na karteczkach	oglądamy monitory i biurka	brak haseł w miejscach widocznych
Dokumenty i nośniki na biurkach	obchód po godzinach pracy	niczego poufnego na wierzchu, szafki zamknięte
Tablica po spotkaniu	oglądamy sale spotkań	wyczyszczona
Goście i serwisanci	porównujemy listę wizyt z kartami tymczasowymi	każda wizyta zapisana, opiekun wskazany

Jak raportujemy

Raport powstaje tego samego dnia, bo po tygodniu nikt nie pamięta, co widział. Zawiera nagłówek (data, osoby, zakres), tabelę z wynikami według powyższej listy, zdjęcia, ocenę ważności każdego ustalenia i plan poprawek z terminem i osobą odpowiedzialną. Raport trafia do zbioru dokumentów audytowych, a pan Wojtek raz w roku dostaje cztery ostatnie.

Ważność ustalamy według skutku. Wysoka dotyczy takich rzeczy jak ściana serwerowni otwarta nad sufitem albo karta byłego pracownika z dostępem do S3, i ma termin 7 dni, jak w kwartalnym audycie uprawnień. Średnia, na przykład klucz w zamku szafy, ma termin 30 dni, a niska, na przykład brak podpisu na pokwitowaniu, 90 dni albo następny obchód. Po terminie sprawdzamy, czy poprawka naprawdę została zrobiona, i dopiero wtedy zamykamy ustalenie.

Przykład wpisu w raporcie (ilustracja, nie z prawdziwego audytu):

Nr	Obszar	Ustalenie	Ważność	Poprawka	Osoba	Termin
1	Ściany	ściana serwerowni kończy się na suficie podwieszanym, nad korytarzem jest wolna przestrzeń	wysoka	dokończyć ścianę do stropu właściwego	pan Zbigniew, wykonawca	7 dni
2	Szafy	klucz tkwi w zamku szafy R3	średnia	klucze wracają do sejfu, wpis wydania	zespół IT	30 dni
3	Drzwi	drzwi D2 podparte tekturą	średnia	rozmowa z firmą sprzątającą, samozamykacz	zespół IT	30 dni

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: wypełniona strona raportu z obchodu w dokumencie audytowym, widoczne nagłówek, tabela wyników z trzema ustaleniami i kolumna terminów, bez danych osobowych.

Czytnik RFID na ESP32: ćwiczenie z UID

Budujemy czytnik, żeby zobaczyć na własne oczy, co czytnik widzi, kiedy przykładamy kartę. Wynik jest prosty: czytnik odczytuje numer karty, czyli UID, i nic więcej. Ten numer ogłasza każdemu czytnikowi, który się do niej zbliży, dlatego sam nie może być hasłem.

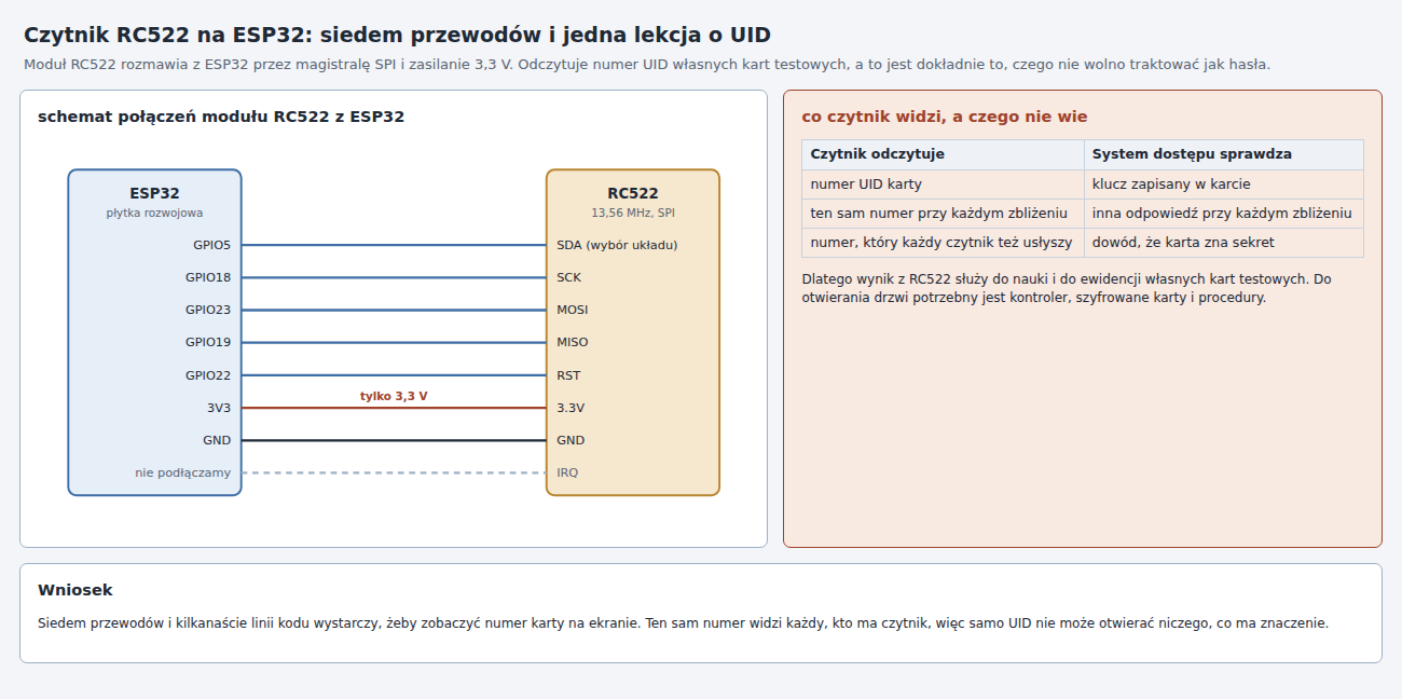
> Ćwiczenie dotyczy wyłącznie własnych kart testowych. Nie odczytujemy kart współpracowników i gości, nie zapisujemy ich numerów i nie podłączamy naszego czytnika do żadnych drzwi. To nie jest system kontroli dostępu i go nie zastępuje.

Lista części

Część	Po co	Uwagi
Płytka ESP32 z ESPHome (typ `esp32dev`)	procesor z Wi-Fi	taka sama jak w pozostałych ćwiczeniach
Moduł RC522 (13,56 MHz)	odczyt UID kart ISO/IEC 14443 A	układ MFRC522 pracuje z zasilaniem od 2,5 do 3,3 V [4]
Siedem przewodów połączeniowych	połączenie modułu z płytką	żeńsko-żeńskie, jeśli piny są wlutowane
Własne karty lub breloki 13,56 MHz	próbki do odczytu	kilka różnych, najlepiej o różnym wyglądzie
Własna karta 125 kHz (opcjonalnie)	pokazanie, że RC522 jej nie czyta	wymaga innego modułu, na przykład RDM6300
Kabel USB	zasilanie i wgranie programu	dane, nie tylko ładowanie

Moduł RC522 działa według układu MFRC522, który pracuje na 13,56 MHz, obsługuje karty ISO/IEC 14443 A i rodzinę MIFARE oraz czyta na odległość do 50 mm [4]. Dlatego czyta karty MIFARE Classic i DESFire, ale karty 125 kHz z EM4100 ignoruje, bo to zupełnie inna technika radiowa.

Schemat połączeń



Rysunek 2. Schemat połączeń modułu RC522 z ESP32: SDA na GPIO5, SCK na GPIO18, MOSI na GPIO23, MISO na GPIO19, RST na GPIO22, zasilanie 3,3 V i masa, IRQ niepodłączone. Warto zauważyć, że prawa strona schematu pokazuje, czego czytnik nie wie: nie sprawdza żadnego klucza zapisanego w karcie. (kliknięcie otwiera pełny rozmiar)

Pin modułu RC522	Pin płytki ESP32	Uwagi
SDA	GPIO5	wybór układu (CS)
SCK	GPIO18	zegar SPI
MOSI	GPIO23	dane do modułu
MISO	GPIO19	dane z modułu
RST	GPIO22	reset
3.3V	3V3	tylko 3,3 V, nie 5 V
GND	GND	masa wspólna
IRQ	niepodłączony	nie używamy

Pierwsze uruchomienie

Przygotowujemy `secrets.yaml` i `esp08-czytnik.yaml` z fiszki, sprawdzamy plik poleceniem `esphome config`, wgrywamy go przez USB poleceniem `esphome run` i obserwujemy dziennik. Po przyłożeniu

karty do modułu w dzienniku pojawia się linia z jej numerem, a w interfejsie web serwera płytki wartość `ostatni_uid`. Odczytany numer wpisujemy do pliku w miejsce przykładowego `74-10-37-94`, jeśli chcemy, żeby czujnik `karta_testowa_1` zapalał się dla tej karty.

Co z tego widać

Przykładamy kolejno trzy karty testowe i za każdym razem kilka razy tę samą. Numer każdej karty jest za każdym razem taki sam, co oznacza, że karta ogłasza go każdemu czytnikowi bez pytania o cokolwiek. Karta 125 kHz przyłożona do tego modułu nie daje żadnej odpowiedzi, bo moduł jej nie słyszy.

Wniosek dla kontroli dostępu jest ten sam co w opisie kart na stronie Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień: system, który sprawdza sam UID, otwiera drzwi każdemu, kto numer powtórzy. Bezpieczny system zadaje karcie losowe wyzwanie i sprawdza odpowiedź podpisaną kluczem, którego karta nie ujawnia, jak robią to karty DESFire.

Ograniczenia i bezpieczeństwo

UID nie jest zabezpieczeniem. Układ nie sprawdza żadnego klucza, a numer da się usłyszeć i powtórzyć, więc nie wolno zbudować na nim drzwi, szafy ani logowania. Czytnik nie rozmawia z kartą szyfrowanym kanałem, więc o kartach DESFire dowiaduje się tylko tego, co każda karta ogłasza. *Numer karty przypisany do osoby to dane osobowe, więc własne karty testowe opisujemy nazwą „karta testowa", a nie nazwiskiem.* Płytka na biurku ma hasło do aktualizacji i do strony WWW, a serwer HTTP ESPHome domyślnie korzysta z uwierzytelniania podstawowego, więc nie wystawiamy go poza sieć biurową. *Moduł stoi poza serwerownią i nie trafia do VLAN 40 ani do sieci serwerów.* Moduł zasilamy z pinu 3,3 V, bo układ MFRC522 ma zakres zasilania od 2,5 do 3,3 V, a podanie 5 V grozi jego uszkodzeniem [4].

> Więcej możliwości albo gotowe rozwiązanie od ręki (out of the box): kontroler dostępu z czytnikami DESFire i OSDP, szafa serwerowa z elektronicznym zamkiem zapisującym, kto ją otworzył, oraz system rejestracji obchodów z punktami kontrolnymi RFID, który zapisuje, kto i o której sprawdził daną strefę. W dużych centrach danych stosuje się całodobową ochronę z recepcją, śluzy osobowe, kontrolę dostępu z kilkoma czynnikami w każdej strefie, kamery z zapisem zdarzeń powiązanym z dziennikiem wejść oraz regularne audyty zewnętrzne.

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę

Audyt fizyczny to sprawdzenie, czy drzwi są zamknięte	Obejmuje klucze, karty, kamery, alarm, sufity, szafy, biurka i procedury
Wystarczy raz w roku, kiedy przychodzi audytor	Karty, kody i klucze zmieniają się szybciej, więc obchód robimy co kwartał, a audytor sprawdza raz w roku
Numer karty z czytnika to jej hasło	UID to numer, który karta ogłasza każdemu czytnikowi
Własny czytnik zastąpi kontrolę dostępu	Nie ma kontrolera, szyfrowanych kart, dziennika ani nadzoru nad zamkiem
Ściana do sufitu podwieszanego to ściana do sufitu	Ściana ma sięgać stropu właściwego, bo sufit podwieszany da się unieść

Częste błędy

Objaw	Przyczyna	Co robimy
Lista jest wypełniona w całości na „zgodne”	obchód robi osoba, która sama instalowała zabezpieczenia	zamieniamy role i dodajemy zdjęcia
Ustalenia wracają co kwartał	brak terminu i osoby w raporcie	przypisujemy termin i osobę, a po terminie sprawdzamy poprawkę
Raport powstaje po tygodniu	brak szablonu	wypełniamy raport w dniu obchodu
Moduł RC522 nie czyta karty	karta 125 kHz albo zbyt duża odległość	sprawdzamy typ karty i przykładamy ją płasko do modułu
W dzienniku brak numeru karty	luźny przewód SPI albo zasilanie 5 V	sprawdzamy połączenia według tabeli i zasilanie 3,3 V
`esphome config` zgłasza błąd składni	złe wcięcia w YAML	porównujemy z plikiem z fiszki, kontrolujemy spacje
Płytka restartuje się co 15 minut	brak klienta API i ustawiony `reboot_timeout`	zostawiamy `reboot_timeout: 0s` jak w pliku
Numer karty ląduje w opisie czujnika z nazwiskiem	wygoda	zostawiamy nazwę „karta testowa”

□□ Ćwiczenia

1. Dlaczego przy audycie unosimy płytę sufitu podwieszanego nad drzwiami serwerowni?

Odpowiedź

Ściana serwerowni może kończyć się na suficie podwieszanym, a nad nim biegnie wolna przestrzeń, którą da się przejść z korytarza. Drzwi z kartą i PIN-em nic wtedy nie dają, bo wejście jest nad nimi.

1. Jak ustalamy ważność ustalenia i termin poprawki?

Odpowiedź

Według skutku: wysoka (otwarta droga do serwerowni, aktywna karta byłego pracownika) ma termin 7 dni, średnia (klucz w zamku szafy, drzwi podparte) 30 dni, a niska 90 dni lub następny obchód. Po terminie sprawdzamy, czy poprawka naprawdę działa.

1. Przykładamy do modułu RC522 kartę, która działa w naszych drzwiach, i nic się nie dzieje. Jaką mamy hipotezę?

Odpowiedź

Karta może być kartą 125 kHz, której moduł 13,56 MHz nie czyta. Sprawdzamy typ karty u producenta kontrolera, a jeśli to 125 kHz, do ćwiczenia potrzebny jest moduł RDM6300.

1. Czy możemy podłączyć nasz czytnik RC522 do zamka w drzwiach pomieszczenia gospodarczego, skoro karty testowe działają?

Odpowiedź

Nie. Czytnik zna tylko UID, który każdy czytnik też usłyszy i powtórzy, więc zamek otwierałby się dla każdej kopii numeru. Kontrolę dostępu budujemy na kartach z szyfrowaniem i kontrolerze z dziennikiem, a nie na UID.

1. Pan Wojtek pyta, jak udowodnimy, że usterki z poprzedniego raportu zostały naprawione. Co pokazujemy?

Odpowiedź

Plan poprawek z terminem i osobą oraz wpis o sprawdzeniu po terminie, z datą i zdjęciem lub eksportem z systemu. Dobrze, gdy ten wpis jest w następnym raporcie z obchodu, a stare ustalenie jest oznaczone jako zamknięte.

Powiązane: Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień · Monitoring wizyjny: kamery IP, ONVIF, rejestrator i RODO · Alarm i ochrona: centrala, czujki, strefy i połączenie z agencją · Niszczenie nośników: DIN 66399, kasowanie dysków i protokół · Serwerownia Zielonej: gdzie stoją czujniki i dokąd płyną alarmy

Źródła:

1. ESPHome, komponent RC522 (rc522_spi, rc522_i2c, on_tag, format UID): esphome.io
2. ESPHome, komponent PN532 (pn532_spi, pn532_i2c): esphome.io
3. ESPHome, komponent RDM6300, czytnik 125 kHz i karty EM4100: esphome.io
4. NXP, karta katalogowa MFRC522, 13,56 MHz, zasilanie 2,5 do 3,3 V, zasięg do 50 mm: nxp.com