České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra mikroelektroniky
Obor: Aplikovaná elektronika

Bezkontaktní identifikační přístupový systém se vzdálenou administrací

Contactless Identification Access Control System with Remote Administration

DIPLOMOVÁ PRÁCE

Vypracoval: Václav Hejný
Vedoucí práce: Ing. Vladimír Janíček, Ph.D.
Rok: 2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Hejný** Jméno: **Václav** Osobní číslo: **434849**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra mikroelektroniky**

Studijní program: **Elektronika a komunikace**

Studijní obor: **Elektronika**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Bezkontaktní identifikační přístupový systém se vzdálenou administrací

Název diplomové práce anglicky:

Contactless Identification Access Control System with Remote Administration

Pokyny pro vypracování:

1. Proveďte analýzu dostupných způsobů řešení identifikačních systémů pro evidenci přístupu do chráněného prostoru,
2. Zvolte optimální variantu a uvažujte řešení pro počítačovou učebnu,
3. Navrhněte a realizujte řešení celého systému na stadardu Mifare, vzdálený server bude sloužit pro monitoring a administraci karet.
4. Vytvořte GUI pro správu databáze.
5. Zhodnoťte dosažené výsledky a proveďte ekonomickou rozvahu zvoleného řešení a srovnání vlastností s komerčně dostupnými výrobky.

Seznam doporučené literatury:

1. Hrbáček Jiří : Komunikace mikrokontroléru s okolím I,II - BEN 2002,
2. Firemní dokumentace Philips MIFARE - Philips 2004,
3. Firemní dokumentace STM32,
4. Záhlava V. Návrh a konstrukce desek plošných spojů, BEN, Praha 2011

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Vladimír Janíček, Ph.D., katedra mikroelektroniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **28.01.2019** Termín odevzdání diplomové práce: _____

Platnost zadání diplomové práce: **20.09.2020**

Ing. Vladimír Janíček, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

7.2.2019 Datum převzetí zadání	Hejný Podpis studenta

Prohlášení

Prohlašuji, že jsem zadanou diplomovou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

V Praze dne ....

Václav Hejný

Název práce:
Bezkontaktní identifikační přístupový systém se vzdálenou administrací

Autor: Václav Hejný

Studijní program: Elektronika a komunikace
Obor: Aplikovaná elektronika
Druh práce: Diplomová práce

Vedoucí práce: Ing. Vladimír Janíček, Ph.D.

Abstrakt:
Cílem této diplomové práce je průzkum trhu s komerčně dostupnými identifikačními přístupovými systémy a na základě analýzy trhu navrhnout a zrealizovat bezkontaktní identifikační přístupový systém se vzdálenou administrací, který bude využívat karty Mifare jako identifikační medium. V navrženém systému bude možné použít více zařízení pro čtení karet najednou, která budou bezdrátově komunikovat se serverem. Důraz je kladen na co nejnižší cenu systému.

Klíčová slova: identifikační přístupový systém, RFID, ESP8266, mikrokontrolér, databáze, server

Title:
Contactless Identification Access Control System with Remote Administration

Author: Václav Hejný

Abstract:
The aim of this diploma thesis is to investigate the market with commercially available identification systems and to design and realize a contactless identification system with remote administration based on market analysis, where will be used Mifare identification card. In the system will be able to use multiple card readers at once to communicate wirelessly with the server. Emphasis is placed on the lowest price of the system.

Key words: access control system, RFID, ESP8266, microcontroller, database, server

Obsah

Seznam obrázků

Seznam použitých zkratek a symbolů

ASK Amplitude Shift Keying

CCD Charge Coupled Device

CLI Command Line Interface

FSK Frequency Shift Keying

GPIO General Purpose Input Output

GUI Graphical User Interface

MISO Master In Slave Out

MOSI Master Out Slave In

NFC Near Field Communication

NUID Non Unique IDentificator

PCB Printed Circuit Board

PIN Personal Identification Number

PLL Phase Locked Loop

RFID Radio Frequency Identification

Rx Reciever

SPI Serial Peripherial Interface

SQL Structured Query Language

TCP Transmission Controll Protocol

Tx Transmitter

UART Universal Asynchronous Receiver Transmitter

UDP User Datagram Protocol

UID Unique IDentificator

Úvod

Téma této diplomové práce jsem si zvolil z toho důvodu, že technologie RFID a systémy na ní založené jsou velmi moderní. Také jsem chtěl zjistit, jak přesně karty komunikují se čtečkami a jak toho využít při vlastním návrhu identifikačního přístupového systému pracujícího s RFID. Kromě toho jsem chtěl zjistit, jak by mohly mé čtečky karet komunikovat se serverem prostřednictvím internetu.
V dnešní době jsou již elektronické identifikační přístupové systémy natolik rozšířené a oblíbené, že je můžeme potkat téměř kdekoliv, kde je nutné dohlížet na to, aby do zabezpečených prostor vstupovaly pouze oprávněné osoby. Proto tyto systémy našly uplatnění v mnoha firmách, kde mohou sloužit například pro sledování docházky zaměstnanců, nebo jen jako náhrada již zastaralých kovových klíčů. Na rozdíl od klíčů mají tyto systémy mnoho výhod, mezi které patří to, že není nutné mít u sebe několik klíčů ke všem místnostem, ale stačí mít jen jedno přístupové medium v rámci celého systému, například RFID kartu, přívěšek nebo jiný způsob identifikace popsaný níže. V případě ztráty přístupové karty není potřeba vyhledat zámečníka, který by vyrobil nový klíč nebo vyměnil vložku zámku, v systému stačí pouze odebrat oprávnění k přístupu ztracené ke kartě a nahrát do systému novou. Další velkou výhodou je, že v databázi přístupů lze dohledat, kdo a kde byl v určitou dobu. Nevýhodou může být to, že tyto systémy potřebují být neustále napájeny a spotřebovávají elektrickou energii. Proto pro případ výpadku napájení z elektrické sítě je dobré při instalaci takového systému počítat se zálohou napájení. Existuje celá řada výrobců přístupových systémů, kteří mají široké portfolio svých produktů se zaměřením na specifické požadavky téměř všech zákazníků. Nejrozšířenější identifikační přístroje jsou založené na technologii RFID z důvodu jejich spolehlivosti a rychlosti přístupu. Ovšem existují i jiné metody identifikace, jako je číselný PIN zadávaný na klávesnici, sken otisků prstů, rozpoznání obličeje, a mnoho dalších metod. Po identifikaci oprávněné osoby je umožněn vstup do prostor například turniketem nebo elektronicky ovládanými dveřmi.

Kapitola 1

Analýza trhu dostupných řešení přístupových systémů

Na dnešním trhu je dostupné nepřeberné množství přístupových systémů různých výrobců. Tyto systémy lze charakterizovat mnoha parametry, jako je například množství uživatelů, kteří mohou systém využívat. Dále je možné volit systém podle způsobu identifikace osob. Některé sofistikovanější přístupové systémy mohou sloužit nejen jako přístupový systém, ale i zastupovat funkci docházkového systému, který z informací o době příchodů a odchodů spočítá dobu strávenou ve střeženém prostoru.

1.1 Typy systémů

Jedním z možných způsobů rozlišení přístupových systémů je rozlišení na systémy identifikační a systémy docházkové.

1.1.1 Identifikační přístupové systémy

Elektronický identifikační přístupový systém je systém, který umožní osobě po úspěšné identifikaci vstoupit do střežených prostor. Tento typ systému se volí tam, kde není nutné získávat informaci o době, kterou strávila osoba v daných prostorách. Aplikace tohoto typu systému je tedy možná například pro otevírání dveří jednotlivých školních učeben, hotelových pokojů a mnoha dalších prostor. Identifikační přístupové systémy lze rozdělit na systémy se vzdálenou administrací a na ty, které vzdálenou administraci nemají.
Systémy se vzdálenou administrací jsou koncepčně složitější z toho důvodu, že kromě autentizačního prvku, kterým je například čtečka karet, je potřeba i server s databází uživatelů. Velkou výhodou tohoto typu systému je to, že je možné v záznamech databáze dohledat, který uživatel byl v danou dobu v prostorách. Administrace tohoto typu systému je jednoduchá a provádí se pomocí GUI aplikace v počítači. Druhou

možností je systém bez vzdálené administrace, kdy se jedná o autentizační prvek, který má v paměti uložené pouze přístupové údaje všech uživatelů, například UID z RFID tagů.

Obrázek 1.1: Přístupový systém s lokální administrací [3]

Na obrázku 1.1 je přístupový systém s lokální administrací uživatelů. Tento systém obsahuje pouze RFID čtečku s klávesnicí pro zadávání PIN kódu, napájecí zdroj, elektromagnetický otevírač dveří a odchodové tlačítko.

1.1.2 Docházkové systémy

Jedná se o systémy, které slouží ke sledování správné docházky zaměstnanců do práce. U tohoto typu přístupového systému je nutné zaznamenávat každý průchod. Tím jsou myšleny všechny vstupy i výstupy z prostor. Tyto systémy obvykle mívají vstupní a výstupní identifikační zařízení. Z rozdílu času přístupu a odchodu se počítá čas strávený v prostorách. Docházkové systémy již našly své uplatnění v mnoha firmách.
Koncepčně bývají tyto systémy řešeny tak, že mají autentizační prvek, například čtečku RFID karet, a server, na kterém jsou v databázi uloženy informace o uživatelích daného systému. Do této databáze se ukládají časy každého průchodu. O výpočet doby strávené v prostorách se stará grafická počítačová aplikace, která je vzdáleně připojena k databázi na serveru.

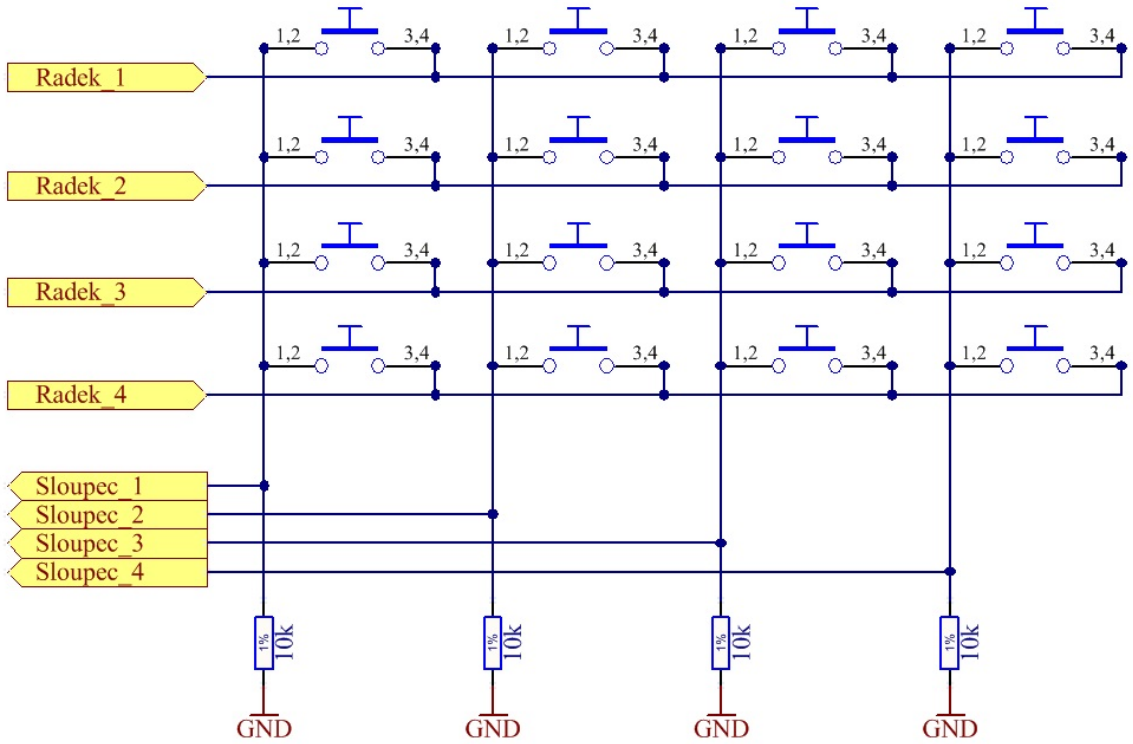
Další rozlišení elektronických identifikačních systémů je dle způsobu identifikace uživatelů.

1.2 Způsoby identifikace osob

Pokud vybíráme přístupový systém, je nutné zvážit, jaký způsob autentizace osob je pro daný objekt nejvhodnější. Autentizace je proces, při kterém dochází k identifikaci uživatele v daném systému.

1.2.1 PIN

PIN je nejjednodušším typem autorizace přístupu, ale také je nejméně pohodlný pro uživatele, protože si uživatel musí pamatovat několikamístné číslo. Při každém vstupu do zabezpečeného prostoru je nutné se autentizovat zadáním PINu na klávesnici u dveří. Pro zadávání čísel PINu se obvykle využívají maticové klávesnice, protože umožňují připojení všech tlačítek k mikrokontroléru s využitím nejmenšího počtu vstupně výstupních pinů.



Obrázek 1.2: Schéma zapojení maticové klávesnice

Nejjednodušší způsob, jak připojit maticovou klávesnici k mikrokontroléru, je znázorněn na obrázku 1.2. Všechny sloupce matice jsou připojeny přes Pull–Down rezistory k zemi, a tím je dána logická úroveň na výstupních signálech z klávesnice, když není stisknuto žádné tlačítko. Ve schématu jsou signály "Řádek_x" používány jako digitální vstupy do klávesnice, které jsou řízeny pomocí mikrokontroléru. Pro rozlišení toho, které tlačítko bylo stisknuté, je nutné posílat z mikrokontroléru na

vstupy klávesnice vždy jen na jeden řádek logickou jedničku. Všechny ostatní řádky musí být ve stavu vysoké impedance, aby při stisku více tlačítek nedocházelo ke zkratu vstupních signálů do klávesnice. Tuto logickou jedničku je nutné postupně přesouvat mezi všemi vstupy tak často, aby uživatel nemusel čekat do té doby, než bude stisk tlačítka vyhodnocen. Při stisku jednoho tlačítka dojde ke spojení mezi jedním řádkem a jedním sloupcem, tím se nám vstupní signál z řádku přenese na výstupní signál sloupce. Pokud je na jednom ze sloupců logická jednička, pak víme, že došlo ke stisku tlačítka v daném sloupci. Dále podle toho, v jakém řádku je nastavena logická jednička, poznáme přesně, které tlačítko je stisknuto.

Na obrázku 1.3 je autonomní přístupový systém od firmy Sebury. U tohoto systému lze pro autorizaci uživatele využít PIN nebo RFID technologii pracující na nosné frekvenci 125 kHz.

Obrázek 1.3: Autonomní přístupový systém od firmy Sebury [4]

Venkovní přístupový systém, který je na obrázku 1.3, lze využít tam, kde se očekává méně než 1000 uživatelů. Pro autorizaci je možné využít PIN kód, RFID tag, anebo kombinaci obojího. Tato jednotka obsahuje relé se spínacím i rozpínacím kontaktem, což umožňuje nejen ovládání elektromagnetických otevíračů dveří, ale i ovládání elektromagnetů, které slouží k držení uzavřených dveří. K napájení tohoto modulu je potřeba stejnosměrný zdroj napětí 12 V, který je schopen dodat proud až 2 A.
Přístupový systém s PIN kódem je vhodný tam, kde jsou nutné nízké náklady na přístupový systém, kde je méně uživatelů a kde se často neprochází přes zabezpečené dveře.

1.2.2 Biometrické autentizace

Biometrické metody autentizace jsou v dnešní době nejmodernějším způsobem, jak ověřit totožnost uživatele. Jelikož k autentizaci není potřeba znát PIN, a ani u sebe nosit nějaké přístupové médium, které se dá snadno ztratit, považuji tyto systémy za nejpohodlnější pro uživatele. Vzhledem k tomu, že jsou tyto systémy založeny na rozpoznávání jedinečných rysů uživatelů, stačí nám k autentizaci například jen otisk prstu. Díky mobilním zařízením se v posledních letech tyto způsoby autentizace velice rozšířily, a proto je dnes možné téměř všechny nové mobilní telefony odemykat pomocí otisků prstů, a dokonce i pomocí rozpoznávání obličeje, kdy stačí na svůj obličej zamířit přední kamerou a telefon se odemkne [6].

Sken otisku prstu

Jak jsem se již zmínil, tak mezi nejrozšířenější způsoby biometrické autentizace dnes patří sken otisku prstu.
Pro skenování otisků prstů se využívá mnoho různých senzorů. Tyto senzory se liší tím, na jakém fyzikálním principu je založena jejich činnost, a také cenou senzoru. Mezi běžně užívané senzory lze zařadit optoelektronické senzory a kapacitní senzory. Kromě těchto senzorů existuje mnoho dalších typů [5].

Optoelektronický senzor otisku prstu

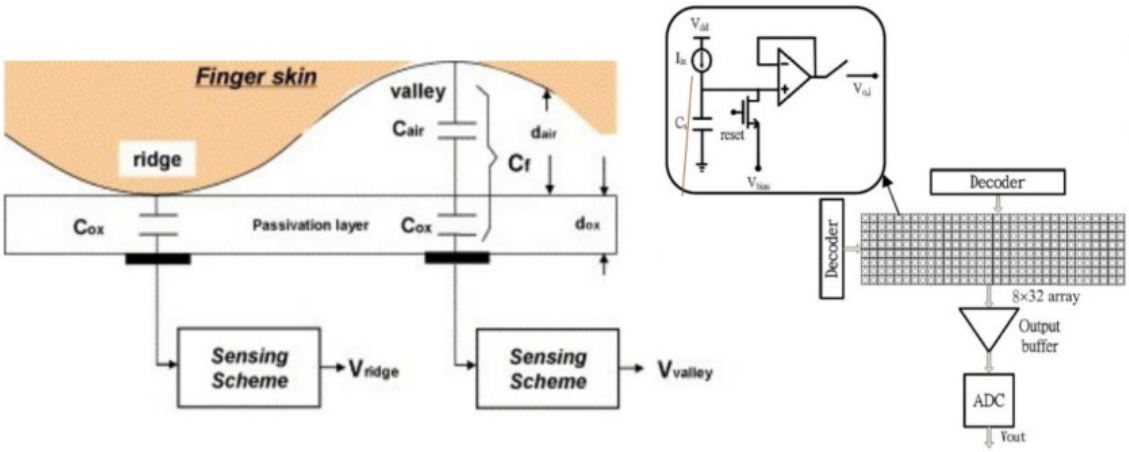
Obrázek otisku prstu se získává u tohoto typu senzoru tak, že se přiloží prst na snímač, který je osvětlen pomocí LED diod. Po přiložení prstu dojde k vyfotografování otisku CCD čipem. Následně dojde k vyhodnocení tmavých a světlých míst na fotografii [5].

Obrázek 1.4: Optický scanner otisku prstu [5]

Tento typ senzoru, který je na obrázku 1.4, patří k těm nejlevnějším a nejméně bezpečným. Přístupový systém s tímto typem senzoru lze oklamat například i vytištěným otiskem na papíru.

Kapacitní senzor otisku prstu

Kapacitní senzor je dnes nejpoužívanějším typem senzoru pro skenování otisku prstu. Proto se s tímto senzorem můžeme setkat i u mobilních telefonů a přenosných počítačů.
Namísto vytváření fotografie tento skener otisku prstu používá pro snímání pokožku prstu jako jednu společnou elektrodu a matici velmi malých elektrod, které jsou umístěné ve skeneru. Jelikož pokožka prstu je členitá, tak při dotyku senzoru jsou místa, kde se přímo dotýkáme senzoru. V těchto místech je kapacita větší než v místech, kde je vzduchová mezera. Jednotlivé kapacity je možné vypočítat podle vztahu $C = \epsilon_0 \epsilon_r \frac{S}{d}$, kde ϵ_0 je permitivita vakua, ϵ_r relativní permitivita materiálu, S je plocha elektrody kapacitoru a d je vzdálenost elektrod [7].



Obrázek 1.5: Kapacitní scanner otisku prstu [7]

Na obrázku 1.5 je znázorněna část otisku prstu dotýkající se části sensoru. Vlevo můžeme vidět papilární linii, která se přímo dotýká sensoru, a tak vzdálenost elektrod je malá a kapacita větší než v druhém případě v pravé části obrázku, kde je vzduchová mezera mezi prstem a povrchem senzoru. V tomto případě můžeme celkovou kapacitu rozdělit na dvě sériově řazené kapacity s různým dielektrikem. Z důvodu větší vzdálenosti elektrod je tato kapacita menší než v předchozím případě. Po změření všech kapacit v matici získáme digitální sken otisku prstu.
Oproti optickému scanneru je tento senzor mnohem bezpečnější.

Sken oční duhovky

Další metodou biometrické autentizace osob je sken oční duhovky. Tato metoda je mnohem bezpečnější než sken otisku prstu, protože je nižší pravděpodobnost nalezení dvou identických očních duhovek než pravděpodobnost výskytu dvou totožných otisků prstů.
Protože se oční duhovka po celou dobu lidského života nemění a není ji možné ani modifikovat chirurgickým zákrokem, dá se o ní říct, že je ideální prostředek pro autentizaci osob.
Jako skener oční duhovky je možné využít běžnou videokameru s dostatečným rozlišením. Kromě duhovky je možné pro autentizaci skenovat i sítnici, která se nachází v zadní části oka [6].

Rozpoznání obličeje

Tato metoda biometrické autentizace rozeznává uživatele na základě toho, že jsou vyfoceni kamerou, která je součástí přístupového systému. Ve fotografii jsou detekovány antropologicky významné body obličeje a ty jsou následně porovnávány s uloženými záznamy v databázi uživatelů. Tento způsob autentizace je relativně pomalý, protože vyhodnocení snímku potřebuje ze všech způsobů autentizace nejvyšší výpočetní výkon. Dále systémy s tímto způsobem autentizace nepatří mezi nejbezpečnější metody přístupu, neboť s časem se mění vzhled obličeje a barva kůže a je zřejmé, že systém musí umožnit pro autentizaci nemalou odchylku mezi pořízenou fotografií a starším záznamem v databázi. Některé systémy s tímto způsobem autentizace je možné oklamat například jen tím, že se před kameru umístí vytištěná fotografie někoho, kdo je uložen v databázi a má oprávnění ke vstupu [6].

Obrázek 1.6: Přístupový terminál SYSF203TP [8]

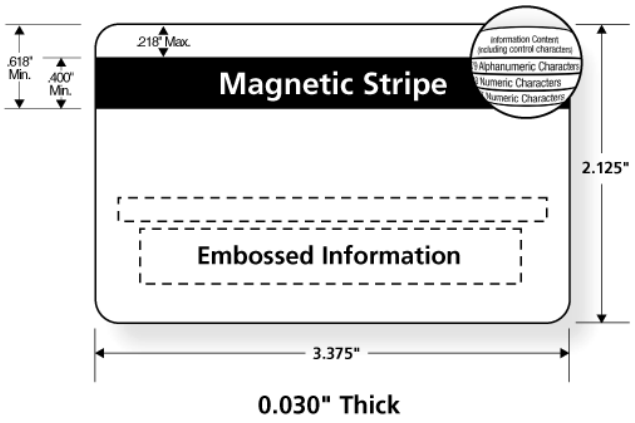
Na obrázku 1.6 je kombinovaný přístupový systém se vzdálenou administrací SYSF203TP, který pro autentizaci osob využívá z biometrických metod rozpoznávání obličeje a sken otisku prstu. Kromě toho je možné u tohoto systému využít k přístupu i RFID karty a PIN.

1.2.3 Přístupové karty

Přístupové karty jsou již delší dobu nejběžnějším médiem pro autentizaci osob, které chtějí vstoupit do zabezpečených prostor. Existuje celá řada typů karet, které je možné využít u přístupových systémů. Tyto karty se dají rozdělit podle jejich použití na kontaktní a bezkontaktní. Mezi kontaktní karty můžeme zařadit například karty s magnetickým pruhem nebo smart cards. Mezi bezkontaktní karty řadíme všechny typy RFID karet. Jediné, co mají tyto karty společné, jsou standardizované rozměry určené mezinárodní normou ISO/IEC 7810 [9]. V této normě je uveden tvar a rozměry karet. Dle normy jsou rozměry 85,60 x 53,98 mm.

Magnetické karty

Karta s magnetickým pruhem je nejstarším typem plastové karty s elektronicky přepisovatelným datovým záznamem. Tento typ karet existuje už od počátku sedmdesátých let minulého století. I přes stáří tohoto typu karet se s ním dnes můžeme běžně setkat například u platebních karet nebo u přístupových karet k hotelovým pokojům [29].



Obrázek 1.7: Magnetická karta [11]

Pro záznam dat je zde využit magnetický pruh s příměsí železa, který je znázorněn na obrázku 1.7.
Magnetické karty se dělí podle koercivity (intenzity magnetického pole), která je užita pro zápis dat do magnetické stopy.
HiCo karty [29] s tímto označením využívají vysokou koercivitu k přepisu záznamu na magnetickém proužku. Proto je záznam na kartě odolnější před poškozením než na kartách se slabým magnetickým polem. Tento typ magnetického proužku je vhodný k častému užívání, proto ho najdeme například na platebních kartách.

LoCo karty [29] s nízkou koercivitou využívají pro přepis dat slabší magnetické pole, což způsobuje, že záznam na kartě je citlivější na okolní magnetické pole.

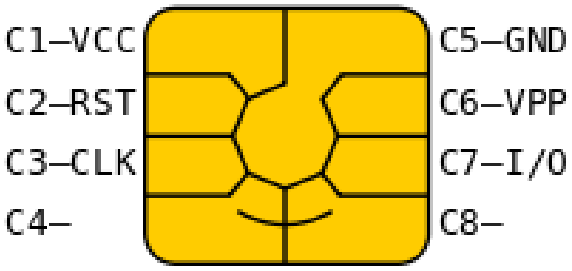
Vzhledem k tomu, že je poměrně snadné tyto záznamy na těchto kartách poškodit magneticky i mechanicky, bylo nutné vyvinout modernější způsob záznamu dat.

Smart cards

Smart karty byly nástupcem zastaralých karet s magnetickým proužkem. Jedná se o kontaktní typ karet, s pozlacenými kontakty, které jsou určeny k elektrickému propojení čipu v kartě se čtečkou. Pro komunikaci karet s terminálem je zde využit protokol APDU popsaný standardem ISO 7816 [10].

Obrázek 1.8: Smart card [12]

V kartě na obrázku 1.8 je umístěn polovodičový čip s řadičem a nevolatilní pamětí typu EEPROM [14]. EEPROM je elektronicky mazatelná programovatelná paměť, která uchovává data i po odpojení napájení. Řadič slouží k překladu instrukcí z protokolu ADPU a podle toho zapisuje nebo čte data z paměti. Paměťový čip má na kontakty karty vyvedené signály pro sériovou komunikaci se čtečkou a napájení.



Obrázek 1.9: Smart card pinout [12]

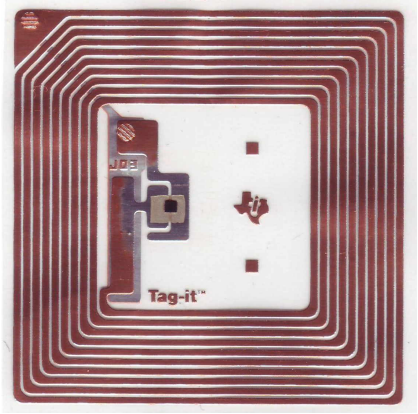
Na obrázku 1.9 je pinout kontaktů umístěných na přední straně smart card. Horní dva kontakty slouží k napájení paměťového čipu. VPP je programovací napětí pro EEPROM a zbylé kontakty slouží k sériové asynchronní komunikaci s čipem.

RFID karty

Radiofrekvenční identifikační karty jsou nejmodernějším typem elektronické karty. Jedná se o bezkontaktní typy karet, které pro přenos informací využívají modulované elektromagnetické pole [17].

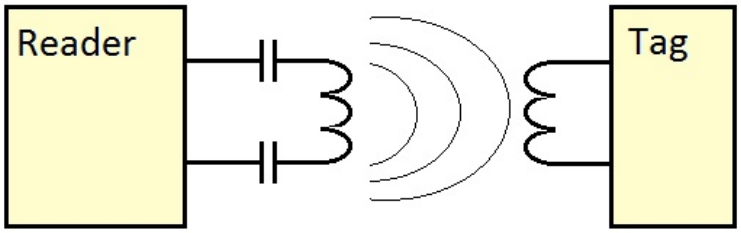
RFID transpondéry můžeme rozdělit na aktivní a pasivní.

Pasivní transpondér: Tento typ transpondéru neobsahuje žádnou baterii a napájení čipu je vyřešeno kondenzátorem, který se nabíjí z elektromagnetického pole generovaného čtecím zařízením. Po nabití kondenzátoru transpondér začíná komunikovat se čtečkou. Typickým zástupcem pasivních transpondérů jsou například bezkontaktní platební karty.



Obrázek 1.10: RFID tag [16]

Na obrázku 1.10 můžeme vidět vnitřek RFID tagu od firmy Texas Instruments, kde je vnější okraj pokryt několika závity cívky, která slouží jako anténa tohoto transpondéru. Ve středu transpondéru se nachází křemíkový čip.



Obrázek 1.11: Princip komunikace čtečky s tagem

Pro komunikaci čtečky s transpondérem je využito vzájemné vazby mezi indukčnostmi čtečky a tagu, jak je znázorněno na obrázku 1.11. Čtečka pro přenos dat k tagu využívá modulaci FSK, která funguje tak, že čtečka skokově mění nosnou frekvenci. Z důvodu, že pasivní transpondéry nejsou schopné vysílat vlastní signál,

tak je zpětná komunikace od tagu vyřešena s pomocí modulace ASK, kdy se ovlivňuje amplituda napětí na vysílací cívce zatížením přijímací cívky.

Aktivní transpondér: S těmito transpondéry se nesetkáme tak často jako s pasivními, protože se jedná o složitější a dražší systém. Na rozdíl od pasivních tagů obsahují zdroj napájení pro čip.
S tímto typem transpondérů se můžeme setkat například u NFC nebo mýtných systémů na českých dálnicích, kde transpondéry bývají zpravidla umístěné na čelním skle autobusů a kamionů.

RFID frekvence

V radiofrekvenční identifikaci se využívá více frekvencí, a to z toho důvodu, že určitá frekvence nemusí být vhodná pro každou aplikaci, protože na nosné frekvenci je závislý čtecí dosah a přenosová rychlost dat [17].

Pásmo nízkých frekvencí se pohybuje v rozmezí **125–134 kHz**. Čtecí vzdálenost v tomto frekvenčním pásmu je velmi krátká a přenosová rychlost je malá. Nejběžněji se tyto frekvence využívají u přístupových systémů. Tyto tagy bývají typicky pasivní a neobsahují přepisovatelnou paměť.

Pásmo vysokých frekvencí se pohybuje okolo **13,56 MHz**. Na této nosné frekvenci se můžeme setkat s pasivními i aktivními transpondéry. Pasivní tagy mají v porovnání s nízkofrekvenčními delší maximální čtecí vzdálenost a vyšší přenosovou rychlost. Systémy pracující s touto frekvencí jsou spolehlivé v blízkosti kovových předmětů a tekutin. Tagy mohou obsahovat i přepisovatelnou paměť. Běžné využití těchto tagů může být například v přístupových systémech nebo u bezkontaktních platebních karet.

Pásmo ultra vysokých frekvencí se pohybuje v rozmezí **860–960 MHz**. Čtecí vzdálenosti na těchto frekvencích dosahují až jednotek metrů. Své uplatnění našly v logistice pro označování palet se zbožím.

Mikrovlnná pásma jsou na frekvencích **2,4 a 8 GHz**. Tyto frekvence jsou určeny pro aktivní tagy. Systémy pracující na těchto frekvencích se vyznačují velkým čtecím dosahem a vysokou přenosovou rychlostí dat. Nevýhodou těchto frekvencí je nespolehlivost přenosu dat v blízkosti kovových předmětů a vody. Využití těchto tagů je možné například v dálničních mýtných systémech.

MIFARE

Mifare je obchodní označení RFID transpondérů firmy NXP. Tyto tagy pracují na frekvenci 13,56 MHz a jsou založené na specifikaci ISO/IEC 14443. Mifare je nejrozšířenějším typem RFID čipů. S různými typy transpondérů Mifare se můžeme setkat například u platebních karet, lítaček a ISIC karet.

Tyto bezkontaktní tagy se dělí do několika skupin podle velikosti vnitřní datové paměti a podle způsobu šifrování. Více o transpondérech MIFARE na [15].

1.3 Akční členy přístupového systému

Po autentizaci uživatele přístupovým systémem je nutné mu umožnit bezproblémový vstup do střežených prostor. Pro tento účel je možné vybrat a využít jedno z mnoha řešení, které vstup do prostor umožní. V následující části jsem se zaměřil na nejčastěji užívané akční členy.

1.3.1 Elektromagnetický otevírač dveří

S tímto otevíračem dveří je možné se setkat u běžných dveří, které se využívají například u školních učeben. Přidáním elektromagnetického otevírače do dveřní zárubně je umožněno elektronické ovládání dveří a zároveň není narušena funkce klasické dveřní vložky na klíče. Tento typ otevírače nepotřebuje stavební úpravy vchodu do místnosti, ani složité úpravy původních dveří. Jedná se o nejlevnější akční člen přístupových systémů.

Obrázek 1.12: Elektromagnetický otevírač FAB 2611MB [18]

Na obrázku 1.12 je znázorněn elektromagnetický otevírač, který se ovládá napěťovým impulzem zpravidla o velikosti 12 V, s maximálním proudem 1 A. Po dobu trvání napěťového impulzu je otevírač v otevřeném stavu. Mimo tuto dobu je otevírač aretován v uzavřené poloze.

1.3.2 Turniket

Dalším možným způsobem pro vpuštění osob do střeženého prostoru je turniket. Toto řešení je vhodné tam, kde se pohybuje větší množství lidí a je nutné provést autentizaci u všech uživatelů. S turniketem se dnes můžeme setkat téměř v každé kancelářské budově, kde jsou turnikety obvykle ovládány docházkovým systémem.

Obrázek 1.13: Turniket CYBERTRONIC CT-2.4 [19]

Na obrázku 1.13 je turniket CT-2.4 firmy Cybertronic. Tento turniket pro autentizaci osob využívá RFID karty a umožňuje až 45 průchodů za minutu. Jelikož tento turniket nemá zálohované napájení baterií, je možné ho při výpadku elektřiny manuálně odblokovat, a tím umožnit vstup do prostor.

1.3.3 Závora

Závora je vhodná pro vpouštění vozidel do chráněných prostor. Typické závory můžeme vidět na parkovištích, kde jsou kombinovány se systémem, který hlídá dobu parkování a na základě této doby vypočítává cenu parkovného.

Kapitola 2

Návrh a realizace vlastního systému

Ze zadání práce vyplývá, že systém musí mít vzdálenou administraci, proto byl tento projekt rozdělen na více menších částí, a to na serverovou část, přístupové čtečky karet s otevírači dveří a databázi systému. Jako hardware, na kterém je spuštěna serverová aplikace a databázový server, byl využit malý počítač Raspberry PI. Dále je vhodné pro minimalizaci kabeláže využít nějaké z možných bezdrátových řešení pro komunikaci mezi čtečkami karet a serverem. Proto bylo využito malých a levných WiFi modulů ESP8266 od čínské firmy Espressif Systems. Dále je zadáno, že systém má být založen na přístupových médiích Mifare od firmy Philips semiconductors, dnes již NXP semiconductors. Pro čtení Mifare tagů bude využit jeden z nejpoužívanějších RFID modulů, který pro svou činnost využívá čip RC522 od NXP.

2.1 Čtečka karet

Čtečka karet slouží pro načtení přístupového tagu a následné otevření dveří v případě, že má načtený tag oprávnění vstoupit do daných prostor.

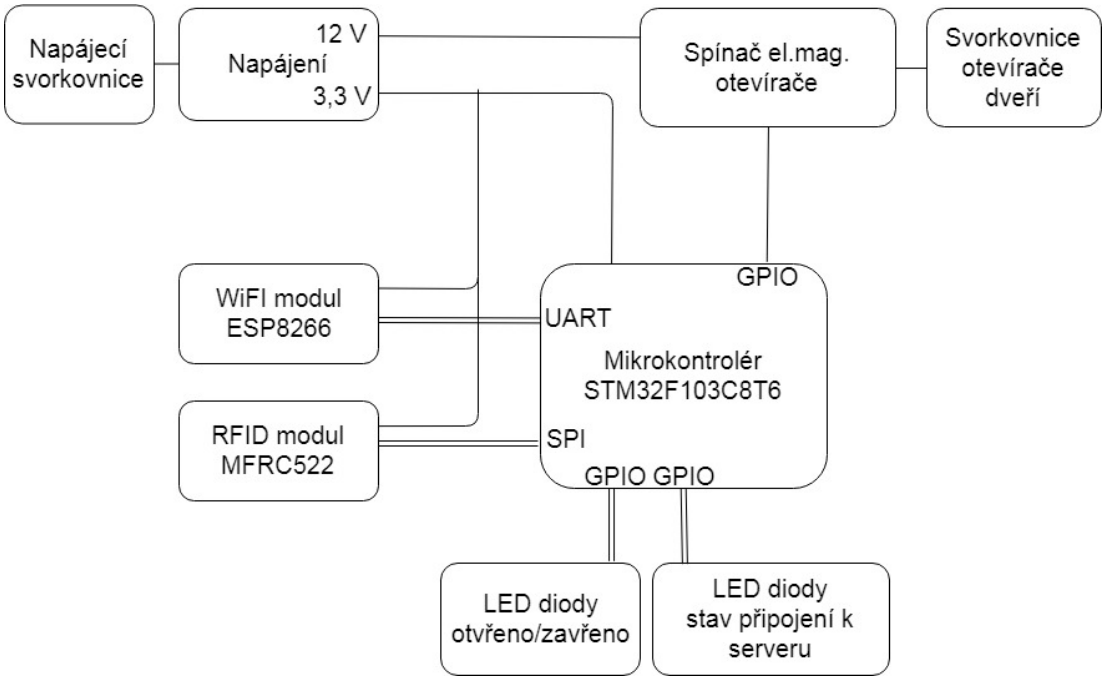
Obrázek 2.1: RFID čtečky firmy Honeywell [23]

Na obrázku 2.1 jsou zobrazeny komerčně prodávané čtečky přístupového systému firmy Honeywell.

2.1.1 Použité komponenty

Ve čtečce karet je využit WiFi modul ESP8266 [25] a RFID modul s čipem RC522 [24]. Oba tyto moduly jsou řízeny pomocí mikrokontroléru STM32F103C8T6 [27] od společnosti STMicroelectronics. Schémata použitých modulů jsou k nahlédnutí v příloze.

2.1.2 Blokové schéma čtečky karet

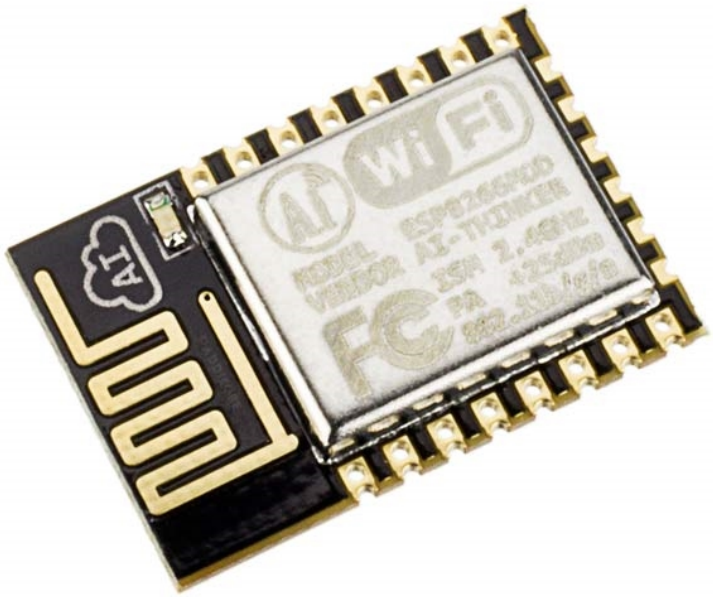


Obrázek 2.2: Blokové schéma navržené čtečky karet

Na obrázku 2.2 je znázorněno blokové schéma navržené čtečky karet. V blokovém schématu je vyobrazeno připojení modulů, LED diod a spínače elektromagnetického otevírače dveří k mikrokontroléru.

2.1.3 WiFi modul

WiFi modul ESP8266 [28] podporuje všechny standardy pro WiFi na frekvenci 2,4 GHz dle specifikací IEEE 802.11 b/g/n [26]. Po přeprogramování firmware lze tento modul využívat i jako 32bitový mikrokontrolér (NodeMCU), pracující s taktovací frekvencí v rozmezí 80–160 MHz s jedním analogově digitálním převodníkem a 17 vývody GPIO. WiFi modul je připojený k mikrokontroléru přes sériovou linku UART. Pro vzájemnou komunikaci je v modulu ESP8266 nahrán firmware, který umožňuje snadné ovládání pomocí implementovaných AT příkazů.

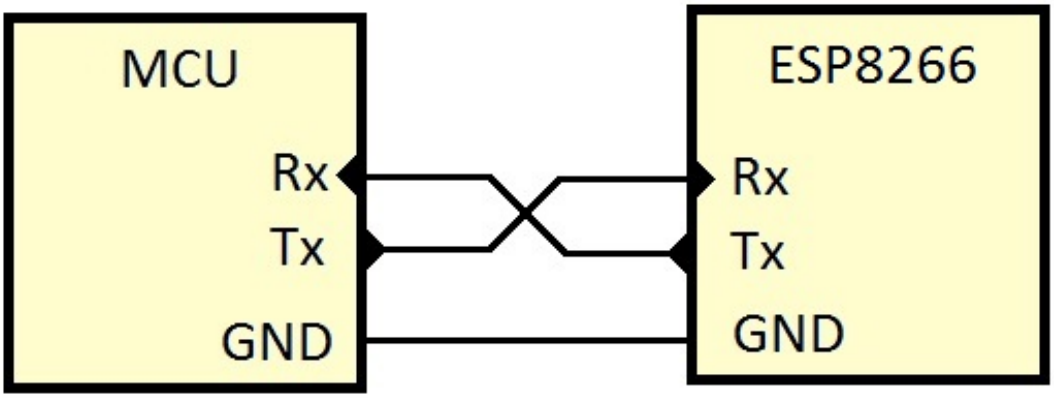


Obrázek 2.3: WiFi modul ESP8266 [28]

UART

UART je jeden ze základních periferních obvodů u všech mikrokontrolérů. Tento interface slouží pro obousměrný asynchronní seriový přenos dat. Z toho plyne, že u této seriové linky není potřeba žádný propojovací vodič pro přenos hodinového signálu. Oba obvody mají vlastní hodinový generátor, který se synchronizuje podle začátku zprávy. Proto UARTu stačí pouze dva signály, a to **Rx** (Reciever) – vstup přijímače a **Tx** (Transmitter) – výstup vysílače.

Na obrázku 2.4 je zobrazeno propojení dvou integrovaných obvodů pomocí UARTu.



Obrázek 2.4: Propojení signálů UARTu mezi mikrokontrolérem a ESP8266

UART má své napěťové úrovně vázané vůči zemní svorce GND, kde logické jedničce odpovídá napájecí napětí Ucc a logické nule přibližně 0 V. V případě, že mají oba obvody stejné napájecí napětí, je možné signály mezi čipy propojit přímo, ale pokud je napájení různé, je nutné využít převodníků úrovní.

Jelikož je přenos dat asynchronní, je nutné zprávu doplnit o start bit, podle kterého přijímač pozná, že bude následovat přenos dat. V klidovém stavu zůstává Tx signál v úrovni logické jedničky. Na start bit přijímač zareaguje tím, že zasynchronizuje hodiny, aby při přenosu dat nedošlo ke špatnému načasování čtení jednotlivých bitů. Časový průběh signálu Tx s přenosem jednoho bytu je pro názornost zobrazen na obrázku 2.5.

Obrázek 2.5: Časový průběh signálu UARTu pro přenos jednoho bytu [20]

Po start bitu následuje krátká zpráva o délce dle nastavení 5 až 9 bitů, typické nastavení je 8 bitů. Za zprávou podle nastavení může, ale nemusí následovat lichá nebo sudá parita sloužící k detekci chyby přenosu. Konec zprávy je dán stop bitem, který je možné nastavit na délku 1–2 bitů.

AT příkazy

AT příkazy [22] jsou standardizované jednoduché textové příkazy pro ovládání různých modemů, GSM, Bluetooth, WiFi a mnoha dalších modulů. Každý příkaz začíná sekvencí znaků **AT**, která je následována příkazem, co se má vykonat. Každý příkaz musí být ukončen znaky *CarriegeReturn* **CR** a *LineFeed* **LF**. Jsou to znaky s ASCII kódy **0x0D** a **0x0A**, po odeslání těchto znaků modulu dojde k vykonání příkazu.

AT příkazy pro ESP8266

V následujících několika řádcích je stručně popsáno několik základních AT příkazů pro ovládání modulu ESP8266 pomocí mikrokontroléru.

AT+RST Tento příkaz slouží pro softwarový restart modulu.

AT+CWMODE=x V případě, že **x** je '1', příkaz nastaví modul do režimu klient. Pokud je **x** '2', bude modul nastaven jako přístupový bod.

AT+CWJAP="ssid","pwd" Tento příkaz využijeme pro připojení k WiFi síti, kde **ssid** je název sítě, ke které se chceme připojit, a **pwd** je heslo.

AT+CIPSTAMAC? Tento příkaz využijeme, když potřebujeme zjistit fyzickou adresu **MAC** našeho modulu. Na tento příkaz by nám měl modul odpovědět zprávou ve tvaru +CIPSTAMAC:"cc:50:e3:4a:00:59", kde mezi uvozovkami je vypsána fyzická adresa modulu.

AT+CIPSTART="type","address",port Tento příkaz slouží pro připojení k TCP nebo UDP serveru. Syntaxe tohoto příkazu je taková, že místo **"type"** napíšeme název internetového protokolu, který chceme využít, a to **"TCP"** nebo **"UDP"**. Namísto **"address"** napíšeme IP adresu serveru, ke kterému se chceme připojit, a do části **"port"** zapíšeme číslo portu, který se bude využívat. Port nám slouží k tomu, aby server poznal, které aplikaci patří příchozí data ze sítě.

AT+CIPSEND=length Tento příkaz využijeme pro odeslání dat ve formě textového řetězce. Za **length** napíšeme číslo odpovídající počtu znaků, které chceme odeslat serveru. Po vykonání tohoto příkazu můžeme začít posílat znaky do modulu, kde se ukládají do vnitřního bufferu. Po přijetí celé zprávy modulem se odešle na server. Maximální délka jedné zprávy je 2 048 bytů.

Pro ukončení spojení se serverem slouží příkaz **AT+CIPCLOSE**.

2.1.4 RFID modul

Pro čtení z RFID karet jsem využil jeden z modulů pracujících na frekvenci 13,56 MHz, a to konkrétně modul s čipem RC522 od NXP [21]. Velkou výhodou je nízká cena a dobrá dostupnost.
Na obrázku 2.6 je fotografie použitého modulu.

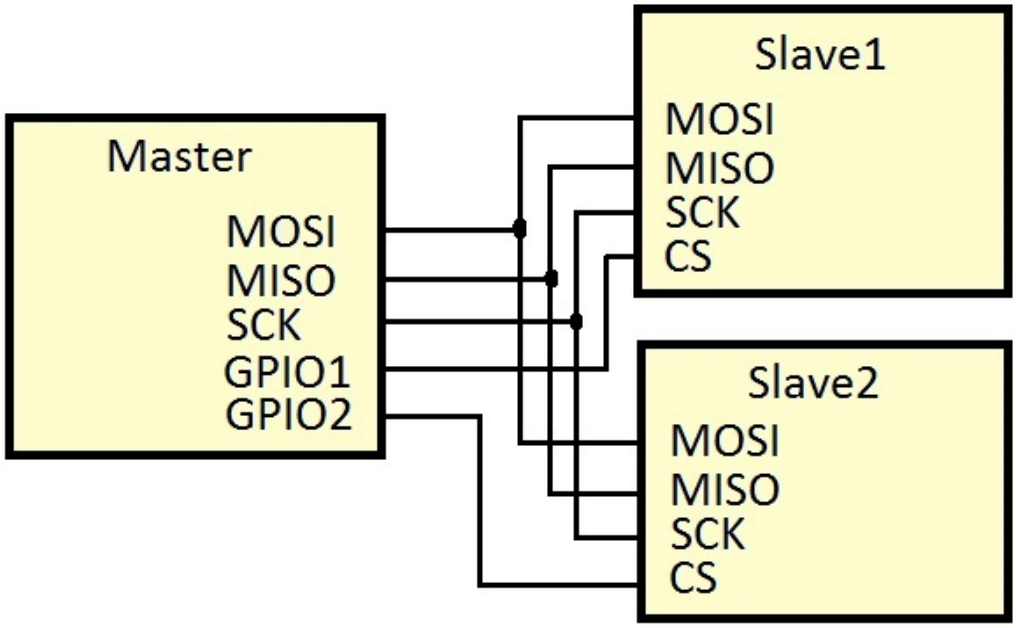
Obrázek 2.6: RFID modul RC522 [21]

Modul se připojuje pomocí 8pinového headeru, na kterém je vyvedeno napájení a **SPI** pro komunikaci s mikrokontrolérem.

SPI

SPI je jednou ze základních periferií v mikrokontrolérech pro synchronní sériovou komunikaci mezi mikrokontrolérem a ostatními integrovanými obvody na desce plošného spoje. Jako UART umožňuje SPI full duplexní komunikaci. Avšak na rozdíl od UARTu je u SPI vždy jeden z obvodů hlavní, takzvaný Master, který si sám řídí, s kterým obvodem bude komunikovat a generuje i hodinový signál. U SPI je možné k Masteru připojit více než jeden Slave. V případě, že Master je propojen s více Slavy, tak se pomocí signálu $\overline{SS}$ **S**lave **S**elect, popřípadě $\overline{CS}$ **C**hip **S**elect, aktivuje jeden Slave. V případě, že na tomto signálu je úroveň napětí odpovídající logické

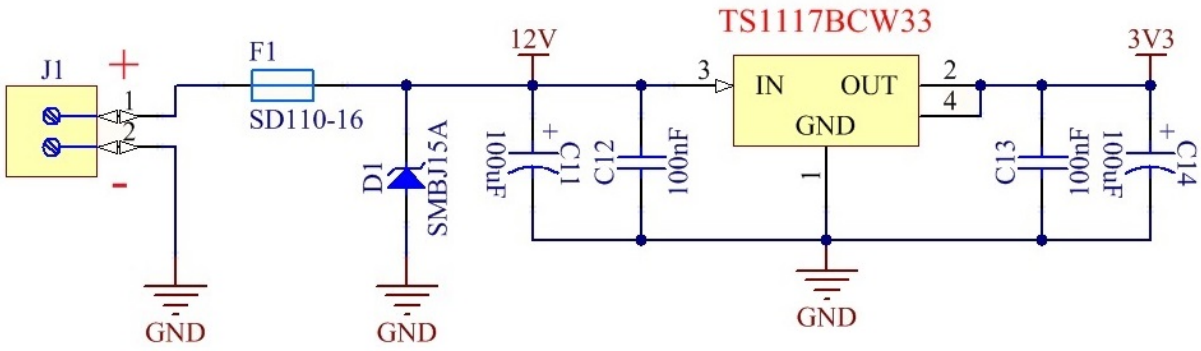
nule, je vybraný Slave aktivní. V případě, že je signál Chip Select v úrovni logické jedničky, přepne se výstup MISO z režimu push-pull do režimu vysoké impedance. SPI je ve své podstatě posuvný registr, do kterého z jedné strany vede vstup, a z druhé strany registru je výstup. Data se z registru vysouvají na výstup, v případě Masteru na signál MOSI. Vysouvání dat z registru je taktováno hodinovým signálem SCK. Datovým vstupem Masteru je signál MISO. Jelikož Slave nijak neřídí komunikaci s Masterem, nemůže po SPI vyvolat přerušení v mikrokontroléru, a tak bývají některé Slavy vybaveny i signálem pro vyvolání přerušení mikrokontroléru. Na obrázku 2.7 je propojení Masteru se dvěma Slavy.



Obrázek 2.7: Propojení SPI mezi Masterem a Slavy

2.1.5 Schéma

Obvod je navržen tak, aby byl napájen stejnosměrným zdrojem o napětí 12 V, který je schopen dodat proud alespoň 1 A. Obvody jsou chráněny proti přepětí pomocí jednosměrného transilu SMBJ15A, který je ve schématu označen jako D1. Transil se zapojuje tak, aby byl závěrně orientován vůči správné polaritě napájení. V případě přepólování zdroje se transil chová jako klasická křemíková dioda a je na ní úbytek napětí 0,6 V. Pro ochranu diody proti vysokému proudu jsem využil vratnou pojistku PolyFuse, která při překročení proudu nad 1 A přestává vést. V případě správné orientace napájecího napětí nám transil ochrání obvody tak, že se chová v závěrné polarizaci stejně jako Zenerova dioda a při překročení napětí U_{br} začíná vést proud, a tím dojde k odpojení zdroje vratnou pojistkou. V tomto případě je využit transil s parametrem $U_{br} = 15$ V.

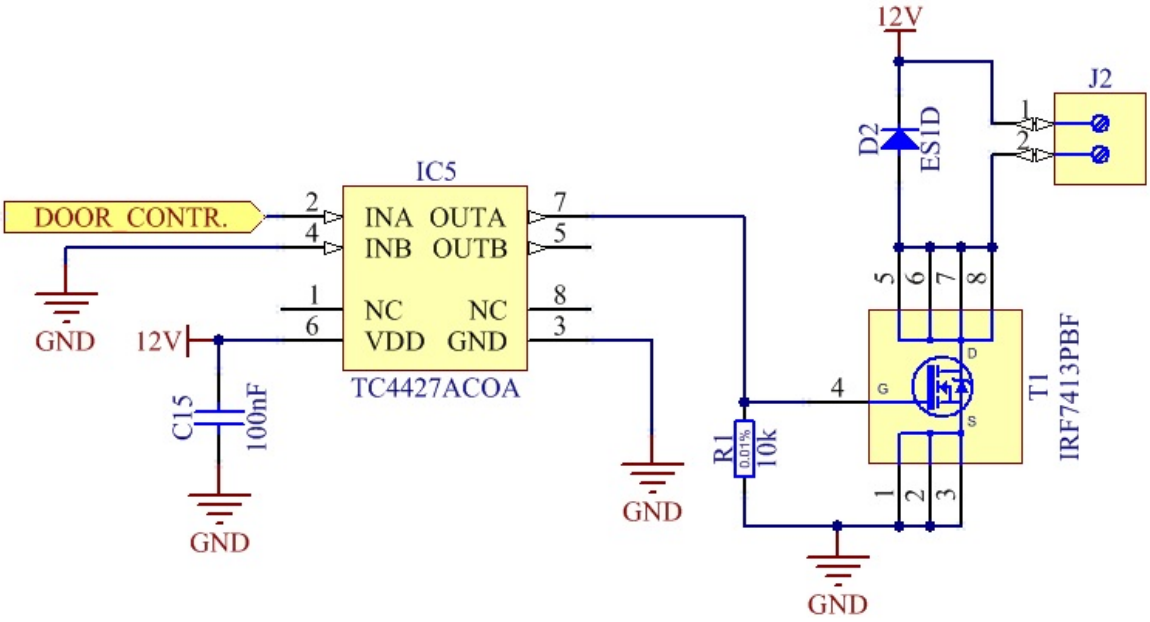


Obrázek 2.8: Napájení čtečky karet

Pro napájení elektromagnetického otevírače dveří je využito napětí v obvodu značené jako 12 V. Dále je pro napájení ostatních digitálních obvodů použito stabilizované napětí 3,3 V. Napětí 3,3 V je získané pomocí integrovaného lineárního regulátoru TS1117BCW33, který sice není nějak zvlášť účinný, ale pro tento účel je dostatečný, jelikož nebyl očekáván větší proudový odběr než 100 mA. Výkonová ztráta na LDO regulátoru je dle výpočtu $P = (12 - 3,3) * 0,1 = 0,87$ W. Z dokumentace regulátoru byl vyčten parametr tepelného odporu $\theta_{JA} = 130$ °C/W pro pouzdro SOT-223. Na základě toho bylo vypočteno, že by se obvod neměl ohřívat na teplotu větší než $T = \theta_{JA} * P = 130 * 0,87 = 113$ °C, což je méně než maximální provozní teplota regulátoru $T_{OPER} = 125$ °C. Spočtená teplota je dost vysoká, proto by bylo mnohem vhodnější použít spínaný buck regulátor pro snížení napětí na 3,3 V. LDO regulátor byl využit v této práci z důvodu jeho nízké ceny.

Pro spínání elektromagnetického otevírače byl použit MOSFET tranzistor IRF7413 s N kanálem. Tento výkonový tranzistor je v pouzdře SOIC-8, a tak oproti jiným zabírá méně prostoru na DPS. Tento tranzistor je možné napájet maximálním napětím $U_{DS} = 30$ V a v sepnutém stavu může tranzistorem trvale protékat proud $I_D = 13$ A. Z těchto parametrů plyne, že je tento tranzistor dostatečně naddimenzovaný pro

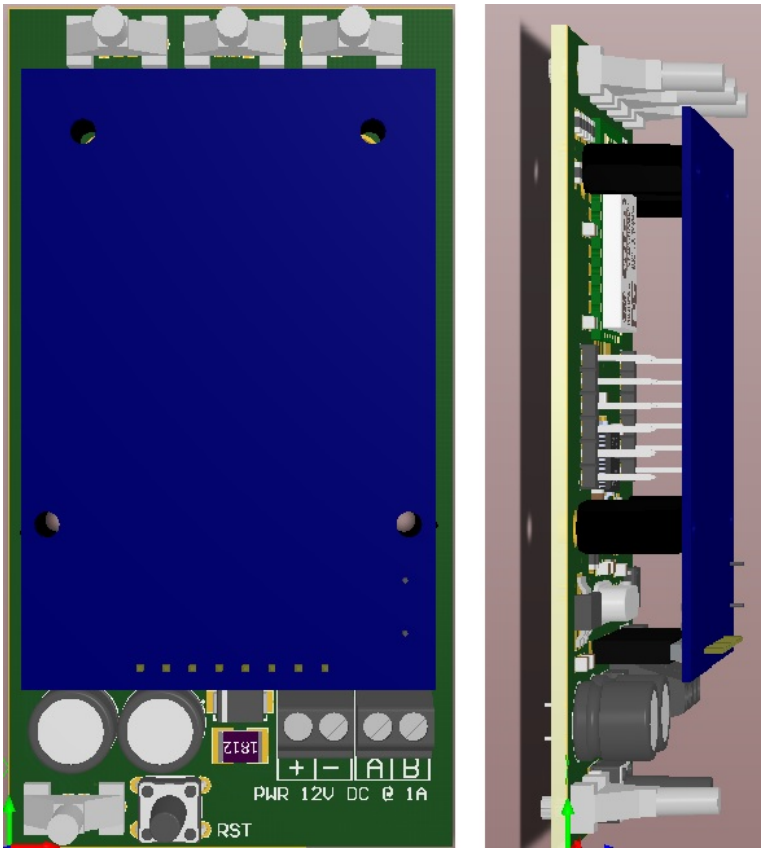
tento účel, kdy bude napájen ze zdroje 12 V a nepoteče jím proud větší než 1 A. Jelikož prahové napětí tohoto tranzistoru je dost vysoké $U_{GS(th)} = 3$ V, při buzení z GPIO pinu mikrokontroléru by netekl tranzistorem dostatečný proud pro sepnutí elektromagnetického otevírače. Proto je obvod doplněn budičem TC4427, který je schopen dostat tranzistor do saturace. Jedním budičem lze řídit až dva MOSFET tranzistory v zapojení se společným sourcem. Nepoužitý vstup INB je připojen na zem, aby měl na vstupu definovanou logickou úroveň. Mezi vývody tranzistoru gate a source je zapojen rezistor $R_1 = 10$ kΩ, aby byl tranzistor zavřený pro případ, že by byl nefunkční budič. Dioda D_2 slouží jako ochrana tranzistoru proti napěťovým špičkám, které vznikají při odpojování induktivní zátěže. Pro ochranu tranzistoru by bylo možné využít i RC nebo RCD snubber, ale vyžadují více komponent.



Obrázek 2.9: Spínání napájení magnetického otevírače

2.1.6 PCB

Ze zapojení ve schématu bylo nutné vytvořit desku plošného spoje, aby bylo možné sestrojit jednotlivé čtečky. Plošný spoj se navrhuje tak, že se začne vhodným rozmístěním komponent v prostoru a podle toho se navrhne obrys desky. Po vhodném rozmístění následuje propojení jednotlivých padů komponent tak, aby zapojení odpovídalo schématu. Při propojování je nutné volit správné šířky vodičů tak, aby odolaly proudům, které jimi potečou. Pro signálové vodiče je možné využít tenké propoje podle technologických možností výrobce.



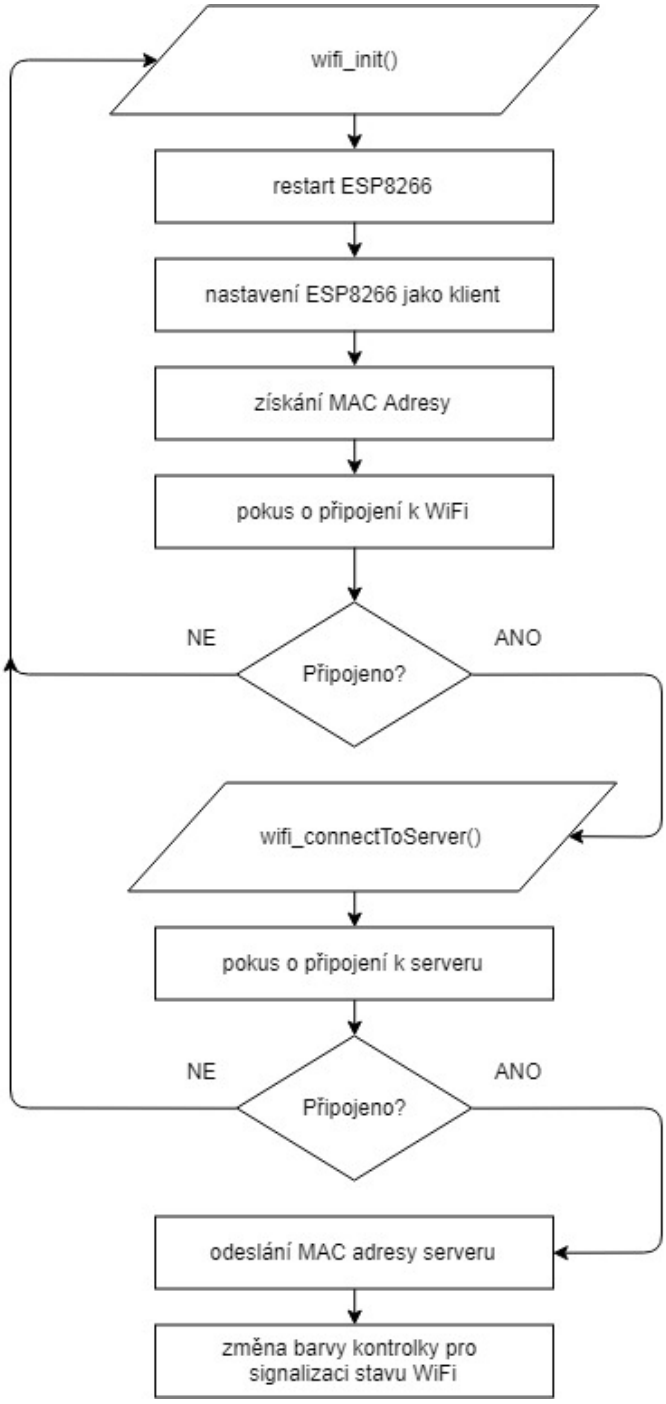
Obrázek 2.10: 3D model osazeného plošného spoje

Na obrázku 2.10 je 3D model osazený PCB. Vlevo je pohled na desku shora a vpravo pohled ze strany. V horní části čtečky jsou umístěny tři světlovody, které slouží k detekci toho, zda je místnost uzavřená nebo otevřená. Další světlovod je umístěn v levém horním rohu a slouží k signalizaci stavu připojení k WiFi síti. Uprostřed desky je umístěn modrý RFID modul MFRC522. V pravé dolní části PCB jsou umístěny dvě svorkovnice, levá slouží pro připojení napájení. Polarita napájení se připojuje dle popisků pod svorkovnicí.

2.1.7 Software

Software pro čtečku karet byl napsán v programovacím jazyce C ve vývojovém prostředí ARM Keil 5.
Pro nakonfigurování všech využitých periferií v mikrokontroléru byla použita aplikace STM32CubeMX, která slouží jako GUI pro nastavení všech periferií v mikrokontrolérech od STMicroelectronics. V této aplikaci byl nejprve nastaven generátor hodin tak, aby mikrokontrolér využíval externí mikrokontrolér 8 MHz. Tento vstupní kmitočet se ještě násobí dvěma v modulu PLL na frekvenci 16 MHz, kterou je taktováno jádro mikrokontroléru i se všemi periferiemi.
UART je nastaven tak, aby správně komunikoval s WiFi modulem ESP8266. UART musí mít nastaven stejný baudrate a stejný formát zprávy. Baudrate UARTu je nastaven na 115 200 baudů za sekundu a formát zprávy je ve tvaru 8 bitů bez parity a s jedním stop bitem. Dále bylo potřeba u UARTu povolit přerušení, aby mikrokontrolér mohl zpracovávat příchozí data z ESP8266.
Další používanou periferií je SPI. I u této periferie je nutné ohlídat stejný formát zprávy, která se posílá do RFID modulu, a tak je SPI nastaveno jako Master, a také tak, aby zprávy byly dlouhé 8 bitů. Ve zprávě se odesílá jako první bit s nejvyšší váhou. U SPI nezáleží na taktovací frekvenci, jelikož se jedná o synchronní přenos dat. Pro ovládání LED diod a řízení spínání elektromagnetického otevírače jsem si nakonfiguroval několik GPIO jako výstup v režimu push-pull.

Po zapnutí čtečky dojde k inicializaci všech používaných periferií v MCU. Rozsvítí se všechny červené LED diody. Horní červené LED diody signalizují, že místnost je uzavřena, a dolní červená LED signalizuje, že čtečka není připojena k WiFi síti. Dále se volá funkce wifi_init();, která se pokouší připojit k WiFi a serveru tak dlouho, dokud se jí to nepovede.



Obrázek 2.11: Diagram průběhu připojení k WiFi

Poté se program stará již jen o to, aby byla čtečka neustále připojena k serveru a aby probíhala komunikace s RFID modulem.
K ovládání WiFi modulu stačilo jen pár jednoduchých AT příkazů. Ale protože je ovládání RFID modulu mnohem složitější, byla využita knihovna pro jeho ovládání z [21]. Po zprovoznění této knihovny bylo zjištěno, že se z karet čte pouze čtyřbytový NUID. Proto byl kód upraven tak, aby vyčítal kompletní UID dle specifikace ISO/IEC-14443a. Pro čtení 7 a 10bytových UID bylo nutné upravit funkci, která zajišťuje průchod antikolizním systémem RFID karet.

```
uint8_t mfrc522_get_card_serial(uint8_t * serial_out){
                                        //funkce pro ziskani UID z tagu
 uint8_t UID[16];
 uint8_t comm[10];
 uint8_t  crc[2];
 uint8_t status,i;
 uint8_t serNumCheck=0;
 uint32_t unLen;

 mfrc522_write(BitFramingReg, 0x00);
 for(uint8_t i = 0; i < 16; i++){
  serial_out[i] = 0;
 }
 comm[0] = PICC_ANTICOLL;               //antikolizni smycka 1. kaskadni uroven
 comm[1] = 0x20;
 status = mfrc522_to_card(Transceive_CMD, comm, 2, serial_out, &unLen);
 serNumCheck = 0;
 if (status == CARD_FOUND){
  for (i=0; i < 4; i++){
   serNumCheck ^= serial_out[i];
  }
  if (serNumCheck != serial_out[i]){
   status = ERROR;
  }
 }
 comm[0] = PICC_ANTICOLL;               //ukonceni 1. kaskadni urovne
 comm[1] = 0x70;
 for(uint8_t j = 0; j < 5 ; j++){
  comm[j+2] = serial_out[j];
 }
 iso14443a_crc(comm, 7, crc);
 comm[7] = crc[0];
 comm[8] = crc[1];
 i = mfrc522_to_card(Transceive_CMD, comm, 9, comm, &unLen);
 if(serial_out[0] == 0x88){
 for(uint8_t i = 0; i < 3; i++){
  UID[i] = serial_out[i+1];
 }
 for(uint8_t i = 0; i < 16; i++){
  serial_out[i] = 0;
 }
 comm[0] = PICC_ANTICOLL2;               //antikolizni smycka 2. kaskadni uroven
 comm[1] = 0x20;
 status = mfrc522_to_card(Transceive_CMD, comm, 2, serial_out, &unLen);
 serNumCheck=0;
 if (status == CARD_FOUND){
  for (i=0; i<4; i++){
   serNumCheck ^= serial_out[i];
  }
  if (serNumCheck != serial_out[i]){
   status = ERROR;
  }
 }
 for(uint8_t i = 0; i < 4; i++){
  UID[i+3] = serial_out[i];
 }
 for(uint8_t j = 7; j < 16; j++){
  UID[j] = 0;
 }
 comm[0] = PICC_ANTICOLL2;              // ukonceni 2. kaskadni urovne
 comm[1] = 0x70;
 for(uint8_t j = 0; j < 5; j++){
  comm[j+2] = serial_out[j];
 }
 iso14443a_crc(comm, 7, crc);
 comm[7] = crc[0];
 comm[8] = crc[1];
 i = mfrc522_to_card(Transceive_CMD, comm, 9, comm, &unLen);
```

```
if(serial_out[0] == 0x88){
 for(uint8_t j = 0; j < 3; j++){
  UID[j+3] = serial_out[j+4];
 }
 comm[0] = PICC_ANTICOLL3;                //antikolizni smycka 3. kaskadni uroven
 comm[1] = 0x20;
 status = mfrc522_to_card(Transceive_CMD, comm, 2, serial_out, &unLen);
 serNumCheck=0;
 if (status == CARD_FOUND){
  for (i = 0; i < 4; i++){
   serNumCheck ^= serial_out[i];
  }
  if (serNumCheck != serial_out[i]){
   status = ERROR;
  }
 }
 for(uint8_t j = 0; j < 4; j++){
  UID[j+6] = serial_out[j];
 }
 comm[0] = PICC_ANTICOLL3;                //ukonceni 3. kaskadni urovne
 comm[1] = 0x70;
 for(uint8_t j = 0; j < 5; j++){
  comm[j+2] = serial_out[j];
 }
 iso14443a_crc(comm, 7, crc);
 comm[7] = crc[0];
 comm[8] = crc[1];
 i = mfrc522_to_card(Transceive_CMD, comm, 9, comm, &unLen);
 }
 for(uint8_t j = 0; j < 10; j++){
  serial_out[j] = UID[j];
 }
}
else{
 serial_out[4] = 0;
}
comm[0] = PICC_HALT;                      //vypnuti tagu
comm[1] = 0x00;
iso14443a_crc(comm, 2, crc);
comm[2] = crc[0];
comm[3] = crc[1];
i = mfrc522_to_card(Transceive_CMD, comm, 4, serial_out, &unLen);
return status;
}
```

Původní funkce obsahovala pouze první antikolizní smyčku pro čtení prvních 4 bytů NUID, proto byla doplněna i druhá smyčka pro čtení 7bytového UID a třetí smyčka pro 10bytové UID dle dokumentu ISO/IEC 14443a. Mikrokontrolér opakovaně posílá do čtečky požadavek ReqAll (0x52) nebo ReqIdl (0x26). Pokud je v dosahu alespoň jeden, nebo více RFID tagů, všechny odpoví řetězcem znaků nazývaným ATQA. Při odpovědi více karet dochází ke kolizi. Software čteček karet je naprogramován jen pro případ, kdy ke kolizi více karet nedochází, a to je v případě, kdy je ke čtečce přiložena pouze jedna karta. V odpovědi ATQA je zakódováno, o jaký typ karty se jedná.

Kódy označující typ vybraných karet:
0x4403 – Mifare DesFire
0x4400 – Mifare Ultralight
0x0400 – Mifare Classic 1k
0x0800 – Mifare Classic 4k

Po zjištění typu karty se pokračuje vyčtením UID nebo NUID. To se získá tak, že mikrokontrolér odpoví na ATQA řetězcem se znaky SEL a NVB. Pro kaskádní level 1 je tvar zprávy:

SEL = 0x93	NVB = 0x20

Na tento řetězec karta odpoví zprávou dlouhou 5 bytů. V případě, že 1. byte není roven hodnotě 0x88, získali jsme kompletní NUID. Pak víme, že zpráva má tvar:

NUID0	NUID1	NUID2	NUID3	BCC

Ve zprávě jsou první čtyři byty NUID karty a pátý byte je BCC. BCC slouží k tomu, aby se dalo poznat, zda při přenosu dat nevznikla chyba. BCC je spočten jako: $BCC = NUID0$ xor $NUID1$ xor $NUID2$ xor $NUID3$.

V případě, že 1. byte zprávy má hodnotu 0x88, víme, že se nejedná o NUID, ale o kartu, která má UID. Také víme, že jsme zatím získali jen první 3 byty z UID. Hodnota 0x88 na prvním bytu se nazývá CT. Zpráva má tvar:

CT	UID0	UID1	UID2	BCC

I v tomto případě je BCC spočten jako xor všech předchozích bytů ve zprávě.

Pro ukončení první kaskádní úrovně je nutné odeslat kartě zprávu ve tvaru:

SEL = 0x93	NVB = 0x70	B0	B1	B2	B3	BCC	CRC-A

SEL je pro první kaskádní úroveň roven hodnotě 0x93. Byte NVB je v tomto řetězci roven hodnotě 0x70. B0-BCC je zpráva přijatá od RFID tagu a CRC-A je 16bitový kontrolní součet ze všech předchozích částí zprávy a slouží k detekci chyb během přenosu dat mezi čtečkou a RFID tagem. Výpočet tohoto CRC-A je definován standardem ISO/IEC 14443a. Funkci pro výpočet CRC-A v jazyce C je možné nalézt a zkopírovat na konci dokumentu ISO/IEC 14443a.

Ukázka kódu pro výpočet CRC-A:

```
void iso14443a_crc(uint8_t *pbtData, size_t szLen, uint8_t *pbtCrc){
 uint32_t wCrc = 0x6363;
 do {
  uint8_t  bt;
  bt = *pbtData++;
  bt = (bt ^ (uint8_t)(wCrc & 0x00FF));
  bt = (bt ^ (bt << 4));
  wCrc = (wCrc >> 8) ^ ((uint32_t) bt << 8) ^ ((uint32_t) bt << 3) ^ ((uint32_t) bt >> 4);
 } while (--szLen);
 *pbtCrc++ = (uint8_t)(wCrc & 0xFF);
 *pbtCrc = (uint8_t)((wCrc >> 8) & 0xFF);
}
```

[13]

Pokud bylo z tagu získáno NUID, tak pro přístupový systém již není nutné s tagem dále komunikovat.

V případě, že byly vyčteny jen první tři byty z UID, pokračuje se do další kaskádní úrovně, kde získáme buď zbylé 4 byty do 7bytového UID, nebo jen 3 byty a zbylé 4 byty do 10bytového UID jsou možné získat v 3. kaskádní úrovni. V druhé kaskádní úrovni se posílá kartě zpráva ve formátu:

SEL = 0x95	NVB = 0x20

Na tuto zprávu nám karta odpoví podobně jako v první kaskádní úrovni.

UID3	UID4	UID5	UID6	BCC

V případě 7bytového UID nám karta dává zbylé 4 byty UID.

Nebo nám karta odpoví ve formátu:

CT	UID3	UID4	UID5	BCC

CT má opět hodnotu 0x88. Z toho je patrné, že jde o kartu s 10bytovým UID a že bude nutné pokračovat do třetí kaskádní úrovně po dokončení druhé úrovně.

Pro ukončení druhé kaskádní úrovně je nutné odeslat kartě zprávu ve tvaru:

SEL = 0x95	NVB = 0x70	B0	B1	B2	B3	BCC	CRC-A

Tato zpráva je téměř stejná jako u první úrovně. Liší se jen tím, že SEL má jinou hodnotu.

V třetí kaskádní úrovni je téměř vše stejné jako v předchozí úrovni. Rozdíl je jen v tom, že se použije SEL s hodnotou 0x97. V této úrovni čtečka získá poslední 4 byty UID.

Pro názornost jsou dále uvedeny zprávy od karty pro jednotlivé typy ID.

4bytové NUID:

CL1	NUID0	NUID1	NUID2	NUID3	BCC

7bytové UID:

CL1	CTag	UID0	UID1	UID2	BCC
CL2	UID3	UID4	UID5	UID6	BCC

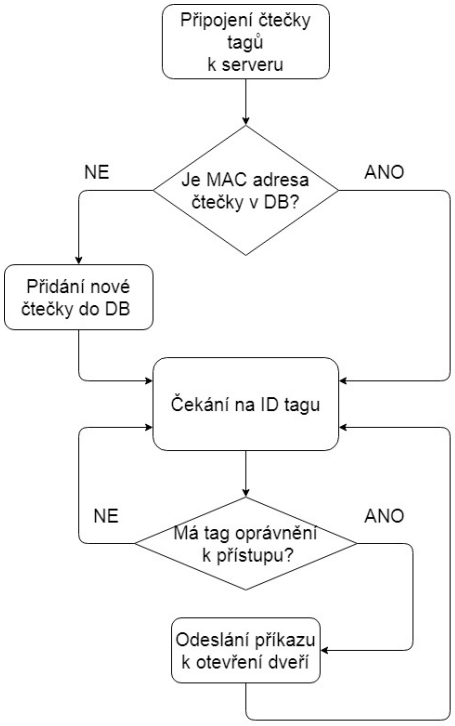
10bytové UID:

CL1	CTag	UID0	UID1	UID2	BCC
CL2	CTag	UID3	UID4	UID5	BCC
CL3	UID6	UID7	UID8	UID9	BCC

Po získání kompletního identifikátoru tagu čtečka přes WiFi modul odešle identifikátor serveru, kde dojde k vyhodnocení, zdali má daný tag oprávnění k přístupu. V případě, že tag má přístup, server pošle příslušné čtečce karet zprávu s řetězcem "OPEN", na kterou čtečka zareaguje tak, že rozsvítí zelené LED diody v horní části čtečky a sepne buzení pro elektromagnetický otevírač dveří po dobu pěti sekund. Až uplyne doba, po kterou bylo otevřeno, zhasnou zelené LED a rozsvítí se červené.

2.2 Server

Jako hardware serveru v této práci byl využit miniaturní počítač Raspberry PI 3B+ [30], který obsahuje integrovaný WiFi modul. Na Raspberry PI je uložena systémová MySQL databáze a serverová aplikace naprogramovaná v jazyce Python.
Server je aplikace v počítači, která se stará o obsluhu požadavků od klienta. V tomto případě bylo nutné využít možnosti vícevláknového běhu programu za účelem obsluhy více klientů najednou. Každé vlákno serveru náleží jednomu klientovi. Připojení klienta k serveru probíhá tak, že se klient pokusí připojit k serveru pomocí protokolu TCP s příslušnou IP adresou a portem. Po připojení klienta si server vytvoří nové vlákno pro komunikaci s tímto klientem. V první zprávě klient pošle svoji fyzickou adresu a server se podívá v databázi do tabulky DOOR, zda obsahuje adresu tohoto klienta. V případě, že tato fyzická adresa je v databázi, uloží si server číslo ze sloupce ID. Toto číslo využije později při autorizaci přístupu do místnosti. Když MAC adresa čtečky není známa, vytvoří se v databázi nový záznam, kde čtečce bude přiřazeno ID a název místnosti ve tvaru "Nova ctecka x", kde x značí, o kolikátou čtečku v systému jde. Tímto je nová čtečka přidána do tohoto systému. Když server přijme zprávu od čtečky s informacemi vyčtenými z RFID tagu, server se podívá do databáze na DOOR_ID (identifikátor čtečky) a USER_ID (identifikátor uživatele) a vyhledá záznam v tabulce AUTHORIZATION podle DOOR_ID a USER_ID. Pokud je v tabulce záznam obsahující oba identifikátory, víme, že má tento tag oprávnění pro vstup do místnosti. Dále se uloží záznam do tabulky ENTRY s informacemi, kdo, kdy a kam vstoupil. Nakonec server pošle dané čtečce řetězec znaků "OPEN".

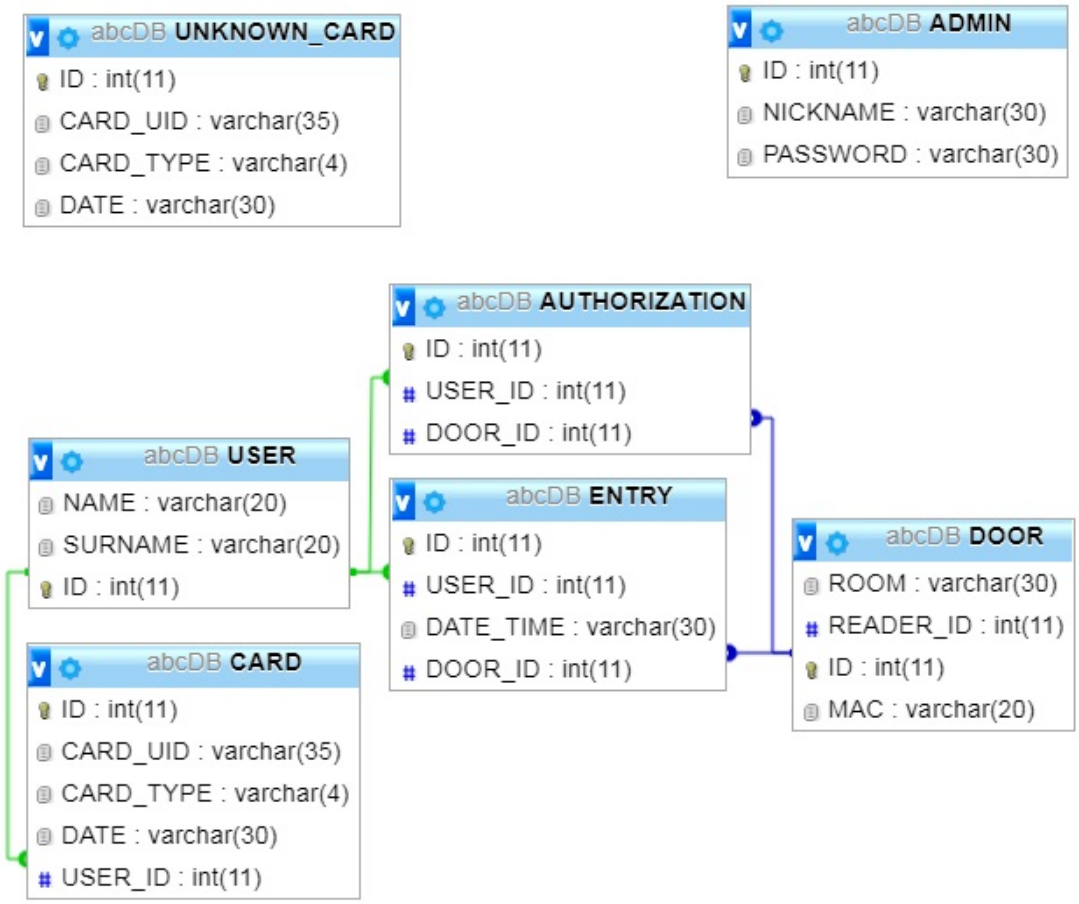


Obrázek 2.12: Zjednodušený diagram činnosti serveru

2.3 Systémová databáze

Databáze slouží ke strukturovanému ukládání dat. Struktura databází se dělí na tabulky. Tabulka obsahuje sloupce pro záznamy dat. Například tabulka "uživatel" bude obsahovat sloupce "jméno" a "příjmení". Tyto sloupce se již nesmí objevit v jiné tabulce, aby nedocházelo k duplicitně ukládaným informacím. V relačních databázích je možné vytvořit vazby mezi tabulkami tak, aby záznam z jedné tabulky byl přiřazen k jednomu nebo více záznamům z jiné tabulky. Vazby mezi tabulkami mohou být typu 1:1, kde jeden záznam z první tabulky souvisí jen s jedním záznamem z druhé tabulky, 1:N. V tomto případě odpovídá jednomu záznamu N záznamů z druhé tabulky a posledním typem vazby je vazba N:M, která se vytvoří pomocí dvou vazeb 1:N a vazební tabulky. Vazba tabulek se vytváří mezi takzvanými klíči. Na primární klíč je možno navázat jeden nebo N záznamů určených cizím klíčem. Primární klíče v tabulkách bývají obvykle pojmenovány ID.
Pro zápis, čtení a veškerou administraci relačních databází se využívají standardizované dotazy SQL.

Systémová databáze je vytvořena v databázovém systému MySQL a je uložena na serveru. Tato databáze má strukturu dle obrázku 2.13.



Obrázek 2.13: Struktura systémové databáze

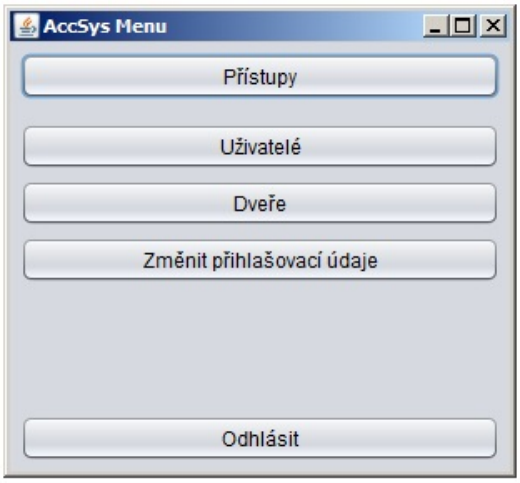
Systémová databáze je navržena tak, aby každý uživatel mohl mít více než jeden přístupový tag. Dále je možné mít přístup do více místností dle nastavených oprávnění. Do databáze se ukládá každý povolený přístup.
Tabulka USER slouží k ukládání základních informací o uživateli, jako je jméno a příjmení. Tabulka USER je spojena vazbou 1:N s tabulkou CARD, ve které se ukládají informace o kartě, a to její UID/NUID, typ karty a datum přidání do systému. Informace o kartě se nezadávají ručně, ale kopírují se z tabulky UNKNOWN_CARD, kam server ukládá informace o neznámých kartách. Další tabulkou je tabulka DOOR, která obsahuje informace o čtečkách dveří. Každý záznam v této tabulce obsahuje název místnosti a fyzickou MAC adresu čtečky. Mezi tabulkami USER a DOOR jsou vytvořeny pomocí vazebních tabulek dvě vazby typu M:N, kde tabulka AUTHORIZATION slouží k ukládání oprávnění pro přístup do dveří jednotlivým uživatelům a tabulka ENTRY slouží k ukládání všech povolených přístupů. V tabulce ENTRY se jen ukládá čas ID uživatele a ID čtečky. Poslední nepopsanou tabulkou je tabulka ADMIN, která obsahuje jen jeden záznam s přístupovými údaji do GUI počítačové aplikace.

2.4 GUI pro správu databáze

Již delší dobu v počítačové technice existují dva způsoby ovládání počítačových programů. Jedním z nich je CLI, kde se všechny programy ovládají pomocí složitých textových příkazů s různými parametry. Tyto textové příkazy se zapisují do terminálu, který je vykoná. Druhou a dnes více rozšířenou možností je využití GUI grafického rozhraní počítačových aplikací, kde pro ovládání aplikace slouží různá tlačítka a mnoho dalších objektů v okně dané aplikace. GUI může být webová stránka nebo počítačová aplikace.
Při rozmýšlení, v jakém programovacím jazyce bude GUI vytvořeno, bylo zvažováno více možností. Jednou z možností by bylo PHP, kdy by GUI bylo webovou stránkou. Další možností bylo využít programovací jazyky C♯ nebo Java. Po důkladném zvážení všech výhod a nevýhod bylo vytvořeno GUI v jazyce Java. Hlavní výhodou Javy je to, že ji lze použít v každém operačním systému.
Po spuštění GUI se nám jako první zobrazí přihlašovací okno.

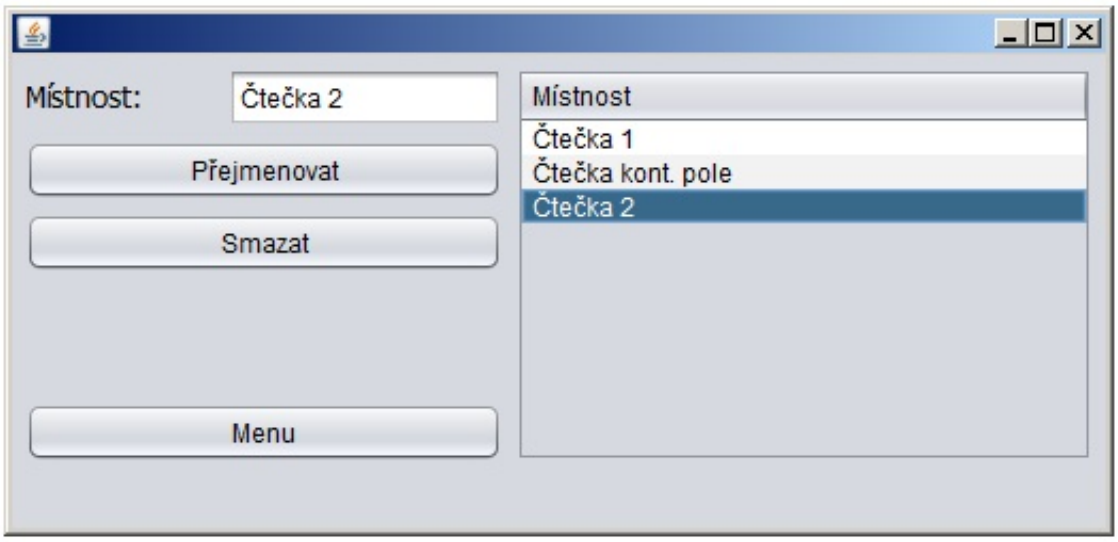
Obrázek 2.14: Přihlašovací okno v GUI

Pro úspěšné přihlášení je nutné zadat správné přístupové údaje, které se shodují s databázovým záznamem v tabulce ADMIN. Po zadání jména a hesla se přihlásíme pomocí tlačítka login. Po přihlášení do systému se nám zobrazí okno s menu.



Obrázek 2.15: Okno s menu

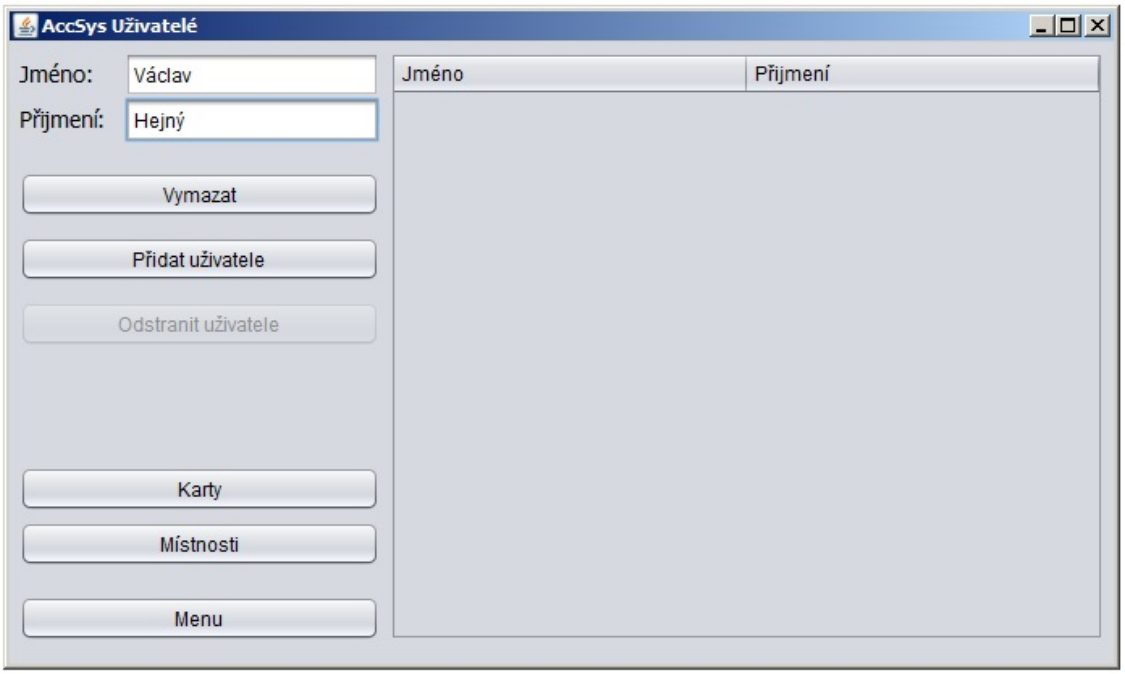
V menu na obrázku 2.15 máme několik tlačítek, pomocí kterých si můžeme vybrat, co chceme spravovat. K zobrazení přístupů je možné použít tlačítko "Přístupy". Pro administraci uživatelů a jejich přístupových práv nám slouží záložka "Uživatelé". Pro administraci čteček máme tlačítko "Dveře". Tlačítko "Změnit přihlašovací údaje" nám ukáže okno, kde je možné nastavit nové přihlašovací údaje do GUI. Tlačítko "Odhlásit" nás přesměruje zpět na přihlašovací okno.
Po kliknutí na tlačítko "Dveře" se nám zobrazí okno, které je na obrázku 2.16.



Obrázek 2.16: Okno pro administraci čteček

V okně pro administraci čteček, které je znázorněno na obrázku 2.16, je možné čtečku přejmenovat, anebo ji smazat ze systému. Upravovanou čtečku zvolíme tak, že na ni klikneme myší v seznamu místností. V případě, že chceme čtečku přejmenovat, přepíšeme její název v textovém poli nad tlačítkem "Přejmenovat". Přejmenování místnosti potvrdíme kliknutím na tlačítko "Přejmenovat". Po nastavení názvů místností klikneme na tlačítko "Menu".

Pro administraci uživatelů v systému klikneme na tlačítko "Uživatelé", které nám zobrazí okno, které je na obrázku 2.17.

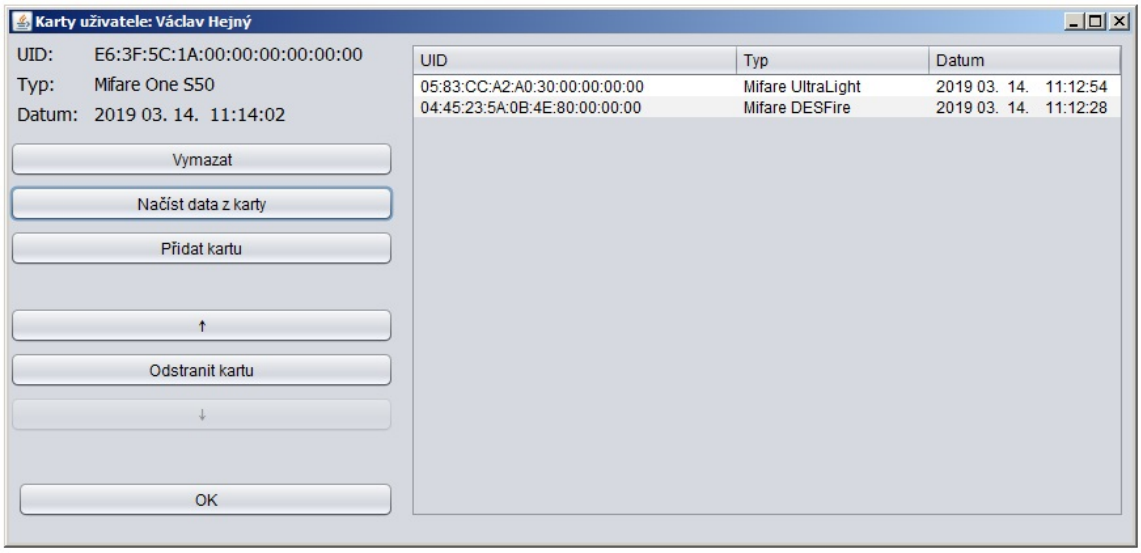


Obrázek 2.17: Okno pro administraci uživatelů

V okně, které je na obrázku 2.17, je možné přidávat a odstraňovat uživatele. Pokud chceme přidat nového uživatele, napíšeme do textových polí jméno a příjmení uživatele a potvrdíme tlačítkem "Přidat uživatele". V případě odebírání uživatele můžeme jeho jméno napsat do textových polí, nebo ho najít v seznamu uživatelů v pravé části okna, kde na vybraného uživatele klikneme myší a jeho jméno se překopíruje do textových polí. Když je vybrán uživatel, můžeme ho odstranit kliknutím na tlačítko "Odstranit uživatele".

V okně jsou také tlačítka "Karty" a "Místnosti". Pomocí těchto tlačítek můžeme zobrazit okna pro přidávání karet a oprávnění k přístupům.

Když vybereme jednoho uživatele ze seznamu a klikneme na tlačítko "Karty", tak se nám otevře okno, které je zobrazeno na obrázku 2.18.

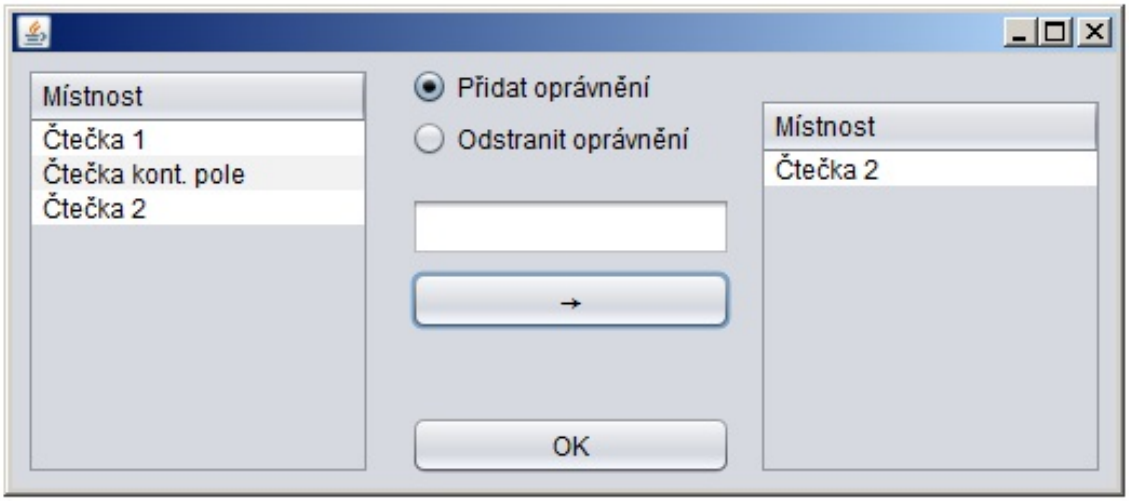


Obrázek 2.18: Okno pro administraci tagů uživatele

V pravé části okna je vidět seznam přidaných tagů uživateli. V seznamu tagů jsou zobrazovány informace o tagu, jako jsou UID a typ tagu. Dále se zobrazuje datum a čas přidání tagu do systému. Nahrání nového tagu do systému se provádí tak, že přiložíme tag, který ještě není zaznamenaný v systému k libovolné čtečce karet. Čtečka karet načte identifikátor karty a pošle ho serveru. V případě, že tag v systému ještě není, je identifikátor tagu uložen v databázi do tabulky UNKNOWN_CARD. Z této tabulky se načtou data v případě, že v GUI klikneme na tlačítko "Načíst data z karty". Po načtení informací o tagu z databáze ho můžeme přiřadit uživateli stisknutím tlačítka "Přidat kartu".
V případě, že potřebujeme odstranit ztracený tag uživatele, vybereme ho kliknutím do řádku v seznamu tagů, nebo pomocí tlačítek se šipkami nahoru a dolů. Parametry vybraného tagu se zobrazují nad tlačítky. Poté, co jsme si jisti, že chceme vybraný tag smazat, můžeme kliknout na tlačítko "Odstranit kartu". Po kliknutí na tlačítko "OK" se toto okno zavře a můžeme pokračovat v administraci uživatelů.

Po přidání tagu uživatel stále nemá možnost vstoupit do žádné místnosti, jelikož nemá oprávnění a žádná čtečka karet ho do uzavřených prostor nevpustí. Proto je nutné uživateli přidělit oprávnění k přístupu do vybraných místností. To se provede tak, že se v okně pro administraci uživatelů klikne na tlačítko "Místnosti".

Po kliknutí na tlačítko "Místnosti" se otevře okno, které je zobrazeno na obrázku 2.19.

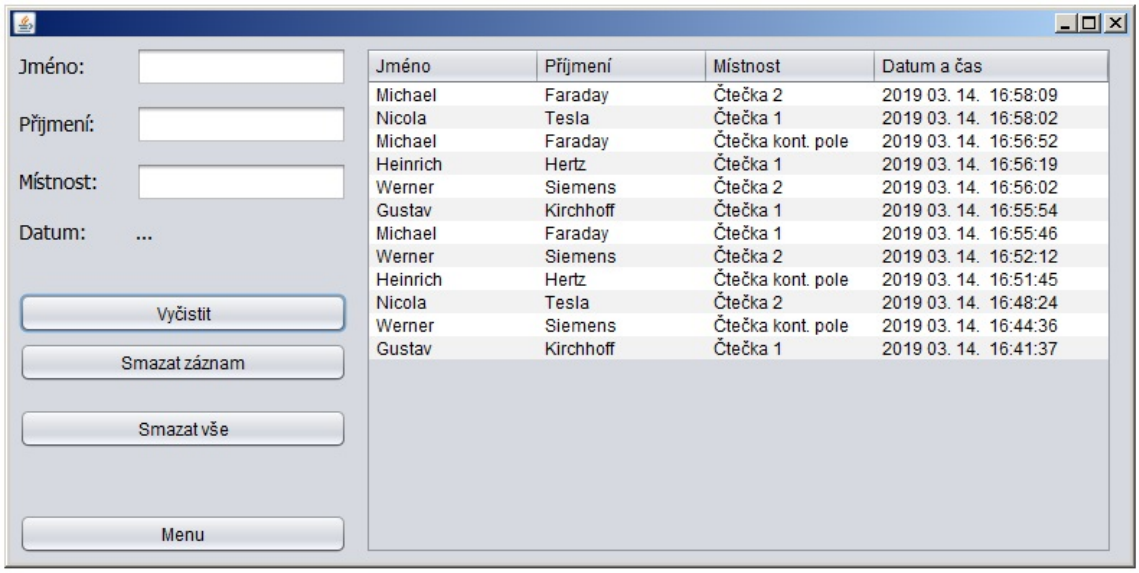


Obrázek 2.19: Okno pro administraci oprávnění k přístupu

V tomto okně je možné přidávat i odebírat oprávnění k přístupu do místností pro uživatele. V levé části okna je seznam všech čteček v systému. V pravé části je seznam čteček, u kterých má uživatel oprávnění k přístupu. V případě, že potřebujeme přidat oprávnění, zaškrtneme políčko "Přidat oprávnění". Poté v levém seznamu vybereme čtečku tagů místnosti, do které chceme povolit přístup, a klikneme na ni myší. Tím se nám název místnosti překopíruje do textového pole uprostřed okna. Volbu potvrdíme kliknutím na tlačítko se šipkou mířící doprava, a název místnosti se nám objeví i v pravém seznamu. Tím je oprávnění přidáno.
Odebrání oprávnění se provádí podobně, jen se zaškrtne políčko "Odstranit oprávnění", ale místnost tentokrát vybíráme z pravého seznamu. Název místnosti se opět překopíruje do textového pole uprostřed okna a volbu potvrdíme tlačítkem se šipkou doleva.

Kliknutím na tlačítko "OK" se opět vrátíme zpět k administraci uživatelů.
Po přidání uživatelů a veškerých výše popsaných nastavení se můžeme vrátit do menu kliknutím na tlačítko "Menu".

Pro zobrazení tabulky s přístupy je možné kliknout v menu na tlačítko "Přístupy". Poté se nám otevře nové okno, které je zobrazeno na obrázku 2.20.



Obrázek 2.20: Okno pro kontrolu přístupů

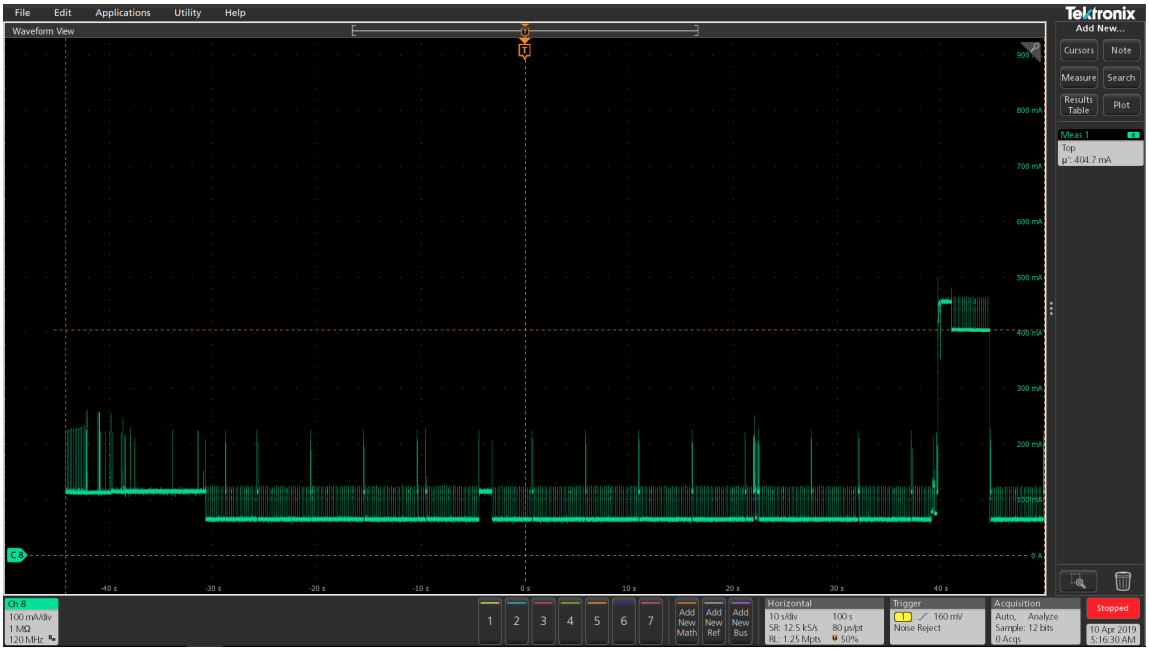
V pravé části okna je tabulka se všemi přístupy. V tabulce jsou záznamy se jménem a příjmením osoby, která byla vpuštěna do místnosti. Dále se zobrazuje, kdy a kam byl vstup umožněn. V záznamech je možné vyhledávat podle jména, příjmení nebo názvu místnosti. Vyhledávání se provádí tak, že se zapíše hledaný výraz do textových polí v levém horním rohu. Stisknutím tlačítka "Vyčistit" se vyprázdní levá textová pole. V případě, že máme vyhledaný jeden záznam ze seznamu, můžeme ho smazat pomocí tlačítka "Smazat záznam". Pro smazání všech záznamů o příchodech můžeme použít tlačítko "Smazat vše".

Kapitola 3

Test zrealizovaného systému a ekonomické zhodnocení

3.1 Test čtečky karet

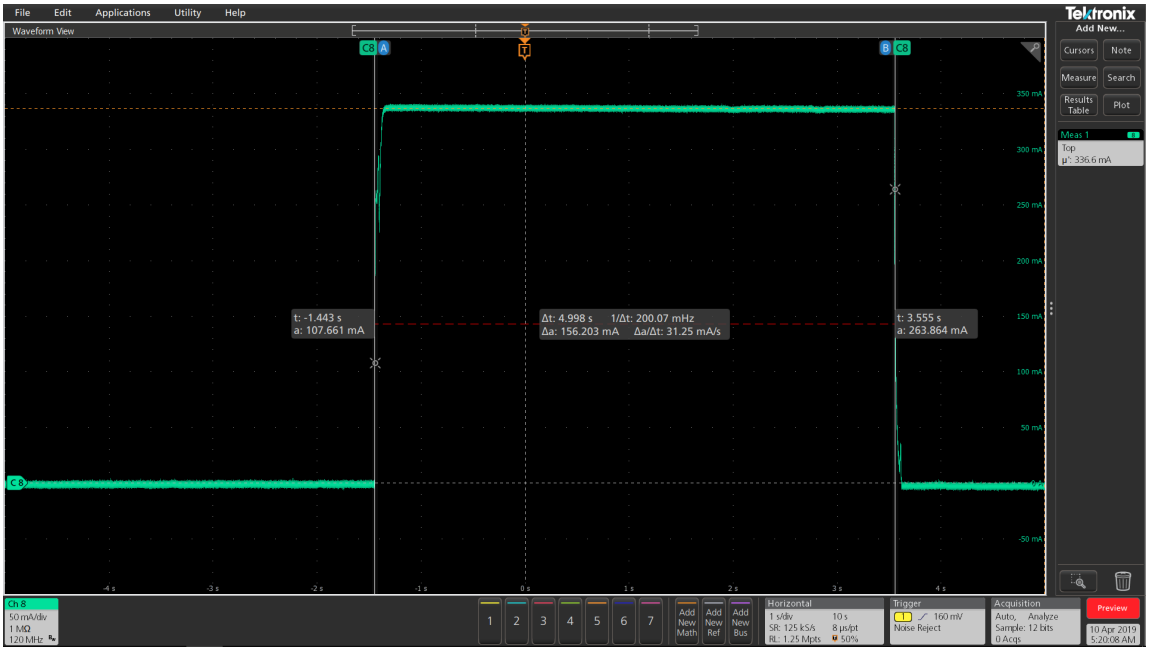
Během testování čtečky karet se ukázalo, že proudový odběr čtečky se pohybuje okolo 100 mA, což odpovídá předpokladu.



Obrázek 3.1: Proudový odběr čtečky karet

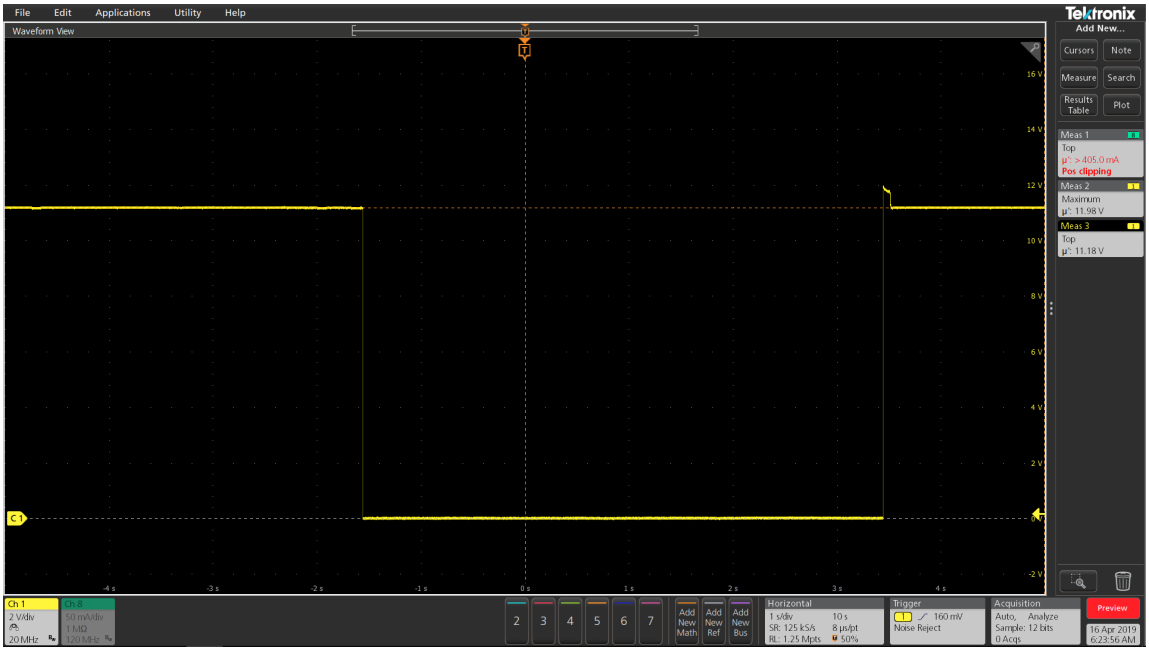
Na obrázku 3.1 je zaznamenán průběh proudu na osciloskopu, který byl měřen proudovou sondou. Proud byl měřen od okamžiku připojení čtečky k napájení. V tu chvíli měla čtečka proudový odběr přibližně 115 mA po dobu 15 sekund. Po připojení k WiFi proud klesl na 70 mA. V pravé části průběhu je zaznamenán impulz dlouhý 5 sekund. V té době byl sepnut elektromagnetický otevírač dveří. Špičky na průběhu

proudu jsou způsobeny WiFi a RFID modulem.



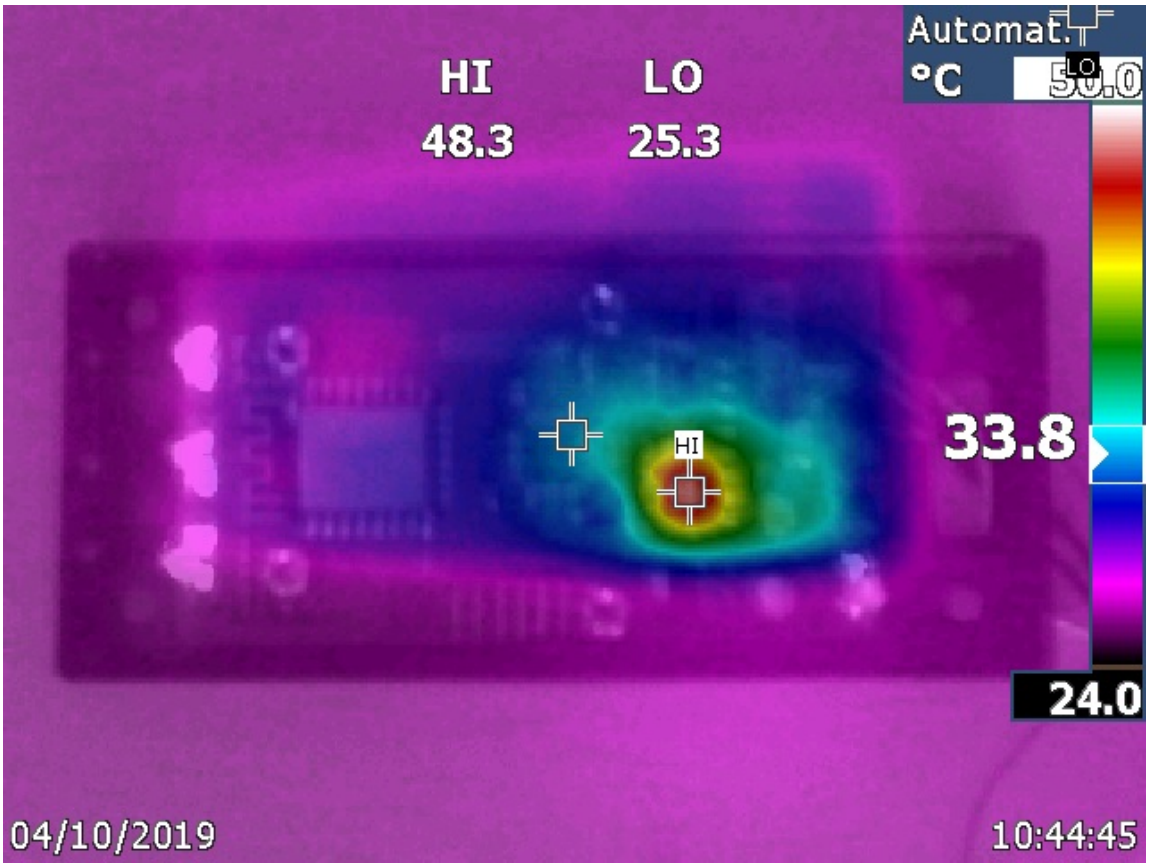
Obrázek 3.2: Proudový odběr elektromagnetického otevírače

Na obrázku 3.2 je zobrazen průběh proudu indukčností elektromagnetického otevírače dveří. Z průběhu je patrné, že délka pulzu je 5 sekund, což odpovídá době nastavené v softwaru čtečky. Maximální hodnota proudu, tekoucího skrze použitý elektromagnetický otevírač dveří, je 336,6 mA.



Obrázek 3.3: Průběh napětí na spínacím tranzistoru T1

Na obrázku 3.3 je zaznamenán průběh napětí na spínacím tranzistoru T1. Při rozpínání tranzistoru vzniká napěťový překmit, který je diodou D2 omezen na velikost 0,8 V.



Obrázek 3.4: Termo snímek čtečky karet

Termo snímek, který je na obrázku 3.4, byl pořízen tehdy, kdy byl demontován RFID modul, aby bylo vidět na PCB se součástkami. Na tomto snímku je vidět, že jedinou součástkou, která je tepelně namáhaná, je LDO regulátor, u kterého to bylo očekáváno. Teploty, které jsou napsány na snímku, neodpovídají skutečnosti z toho důvodu, že termokamera nebyla zkalibrována. Kalibrace termokamery není možná pro snímek s více prvky, které mají různou emisivitu povrchu.

3.2 Ekonomické zhodnocení

V ekonomickém zhodnocení systému jsou sepsány pouze komponenty pro čtečky karet, a to z toho důvodu, že server může být nastaven na jakémkoliv počítači, na kterém je nainstalován MySQL server a Python.

Desky plošného spoje pro čtečky karet byly vyrobeny u čínského výrobce ALLPCB, kde výroba 10 ks DPS vyšla na 5 USD. Tedy plošný spoj pro jednu čtečku karet stál 50 centů, což odpovídá cca 13 Kč.

Moduly a mikrokontrolér byly objednány z internetového portálu Aliexpress.com.
RFID modul MFRC522 stál 90 centů, (cca 23 Kč).
WiFi modul ESP8266 stál 1,5 USD, (cca 28 Kč).
Mikrokontrolér STM32F103C8T6 stál 93 centů, (cca 23 Kč).

Ostatní komponenty byly objednány u prodejce TME. Vzhledem k tomu, že se jednalo většinou o položky řádově v několika desítkách haléřů nebo jednotek korun, byly ceny těchto položek sloučeny.
Ostatní komponenty vyšly po zaokrouhlení na 62 Kč.

Náklady na jednu čtečku jsou tedy 149 Kč. V ceně není zahrnuta krabička pro čtečku karet.

Závěr

Navržený a zhotovený bezkontaktní identifikační přístupový systém se vzdálenou administrací je plně funkční. Všechny čtečky karet v systému správně komunikují se serverem. Pro daný systém je databáze navržena správně a umožňuje každému uživateli vlastnit neomezené množství RFID tagů. Oprávnění k přístupu do jednotlivých místností lze všem uživatelům nastavit tak, jak je potřeba. Vytvořené GUI umožňuje snadné ovládání systému.
V navrženém systému jsou části, které by se daly vyřešit i lépe. Například 3,3 V napájení ve čtečkách je řešeno s využitím lineárních regulátorů, na kterých dochází k velkému poklesu napětí a při odebíraném proudu hlavně WiFi modulem ESP8266 dochází na regulátoru k velkým výkonovým ztrátám, a tím i k přehřívání tohoto integrovaného obvodu. Tento problém by se dal spolehlivě vyřešit použitím spínaného step–down měniče. Druhou záležitostí, která by se dala řešit lépe, je to, že ve čtečkách nejsou uloženy UID tagů používaných v systému. To zapříčiňuje to, že odezva elektromagnetického otevírače po přiložení RFID tagu není okamžitá, ale čeká se, než čtečka pošle identifikátor tagu na server a pak se ještě čeká na odpověď od serveru. Z pozorování tohoto jevu jsem zjistil, že nám čtečka karet sepne elektromagnetický otevírač se zpožděním přibližně dvou sekund.

Literatura

[1] Hrbáček Jiří. *Komunikace mikrokontroléru s okolím I, II*. Praha. BEN. 2002.

[2] Záhlava V. *Návrh a konstrukce desek plošných spojú*. Praha. BEN. 2011.

[3] Obo Hands: *Rfid Keypad Door Access Control System*.
https://www.epicworldstore.com/products/obo-hands-rfid-keypad-door-access-control-system-kit-electric-magnetic-electronic-door-lock-power-supply-5pcs-key-fobs-full-set

[4] Sebury BC2000: *Autonomní kódová klávesnice s čtečkou*.
https://www.zabezpecovaci-zarizeni.cz/klavesnice-a-ovladace/kodove-klavesnice/autonomni-kodova-klavesnice-s-cteckou-bc2000

[5] Wikipedia: *Čtečka otisků prstů*.
https://cs.wikipedia.org/wiki/%C4%8Cte%C4%8Dka_otisk%C5%AF_prst%C5%AF

[6] Biometric: *Biometriky*.
http://www.biometricke-ctecky.cz/biometriky/

[7] Robert Triggs: *Capacitive scanners*. březen 2019
https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

[8] Eurosat: *Přístupový terminál SYSF203TP*.
hhttps://www.eurosat.cz/12485-2/

[9] ISO/IEC: *ISO/IEC 7810*. 2003.
https://www.iso.org/standard/31432.html

[10] ISO/IEC: *ISO/IEC 7816*. 2006.
https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-3:en

[11] ISO/IEC 14443: *Identification cards*. leden 2001
http://www.icedev.se/proxmark3/docs/ISO-14443-3.pdf

[12] Wikipedia: *Čipová karta*.
https://cs.wikipedia.org/wiki/%C4%8Cipov%C3%A1_karta

[13] Wikipedia: *EEPROM*.
https://cs.wikipedia.org/wiki/EEPROM

[14] Wikipedia: *Mifare*.
https://en.wikipedia.org/wiki/MIFARE

[15] electronicwings: *Sensors & Modules*.
https://www.electronicwings.com/sensors-modules/rfid-reader-em18

[16] Wikipedia: *RFID*.
https://en.wikipedia.org/wiki/Radio-frequency_identification

[17] FAB: *Elektromagnetický otevírač*.
http://www.fab.cz/produkt/1904

[18] CYBERTRONIC: *Turniket*.
http://www.cybertronic-labs.cz/turniket-model-ct-2-4-kit-nerez-i94c2

[19] Wikipedia: *Universal asynchronous receiver-transmitter*. listopad 2010.
https://en.wikipedia.org/wiki
/Universal_asynchronous_receiver-transmitter

[20] Asif Mahmud Shimon: *MIFARE RFID with AVR*. leden 2016.
https://github.com/asif-mahmud/MIFARE-RFID-with-AVR

[21] ESP8266: *AT Instruction set*.
https://www.espressif.com/sites/default/files/documentation
/4a-esp8266_at_instruction_set_en.pdf

[22] Honeywell: *Omniclass 2.0*.
https://www.security.honeywell.com/product-repository/omniclass

[23] NXP: *MFRC522*.
https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

[24] Espressif Systems: *ESP8266*. 2018.
https://www.espressif.com/sites/default/files
/documentation/0a-esp8266ex_datasheet_en.pdf

[25] Wikipedia: *IEEE 802.11*.
https://cs.wikipedia.org/wiki/IEEE_802.11

[26] STMicroelectronics: *STM32F103*.
https://www.st.com/resource/en/datasheet/cd00161566.pdf

[27] Wikipedia: *ESP8266*.
https://en.wikipedia.org/wiki/ESP8266

[28] ID cards: *Magnetic Stripe Card*.
https://www.idwholesaler.com/learning-center/magstripe-card-coercivity/

[29] q-card: *ISO Magnetic Stripe Card Standards*.
https://www.q-card.com/about-us/iso-magnetic-stripe-card-standards/
page.aspx?id=1457

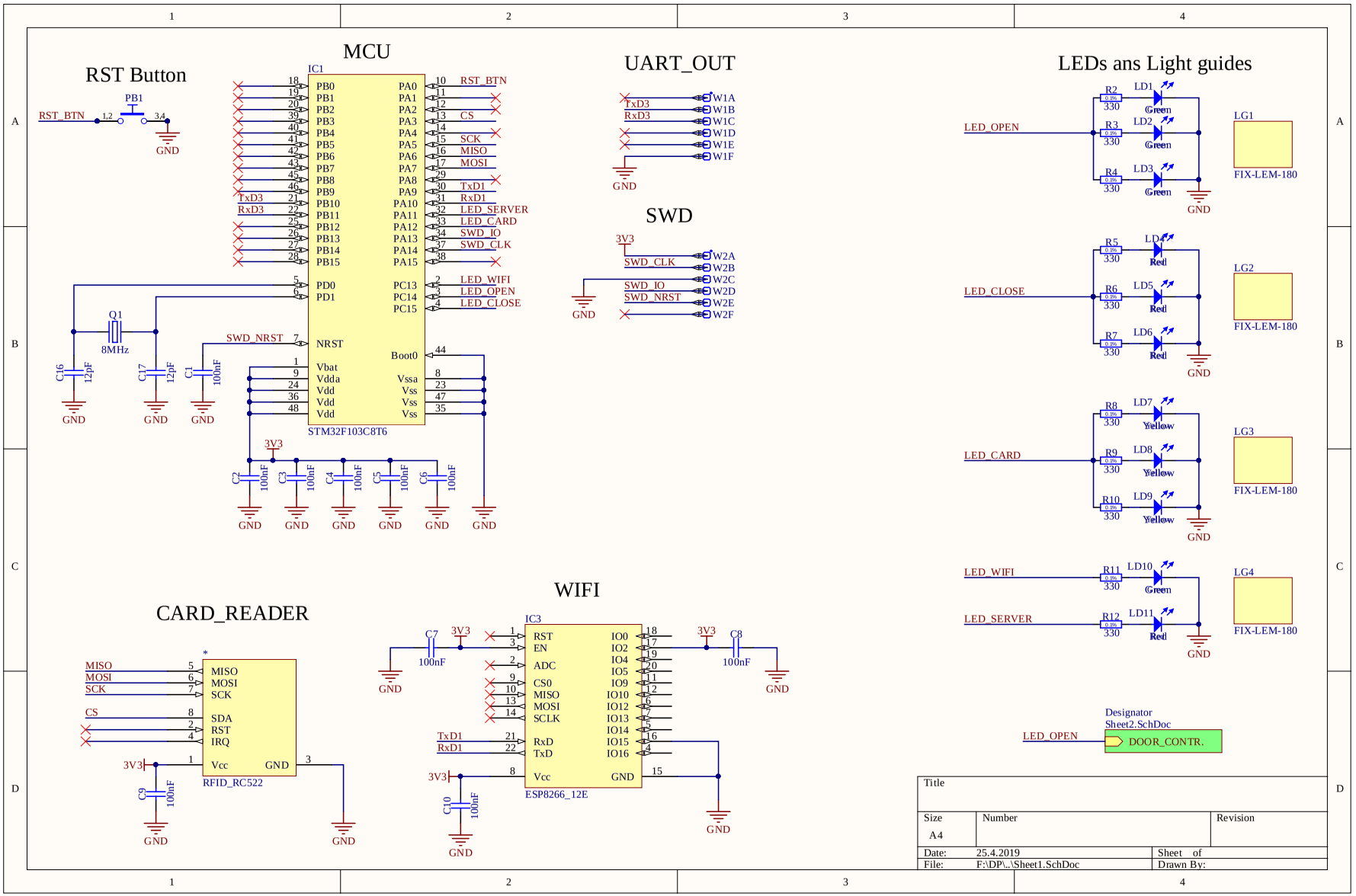
[30] Raspberry PI: *Raspberry PI*.
https://www.raspberrypi.org/

[31] ESP8266: *Schematic*.
http://wiki.sunfounder.cc/index.php?title=File:ESP8266SCHEMATIC.png

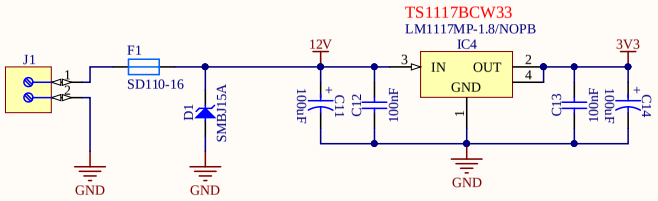
[32] MFRC522: *Schematic*.
https://easyeda.com/gerrychen/RFID_MFRC522-lHBSasmEW

Příloha A

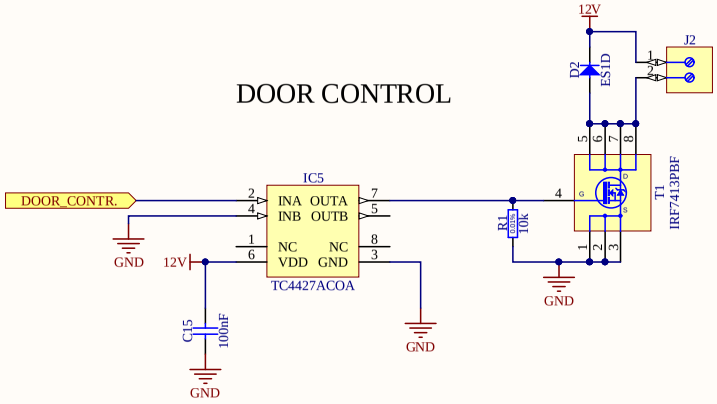
Úplné schéma čtečky karet


MCU
RST Button
UART_OUT
SWD
LEDs ans Light guides
CARD_READER
WIFI
STM32F103C8T6
RFID_RC522
ESP8266_12E
LED_OPEN
LED_CLOSE
LED_CARD
LED_WIFI
LED_SERVER
DOOR_CONTR.
Designator
Sheet2.SchDoc
Title
Size
A4
Number
Revision
Date: 25.4.2019
File: F:\DP\..\Sheet1.SchDoc
Sheet of
Drawn By:

Power supply



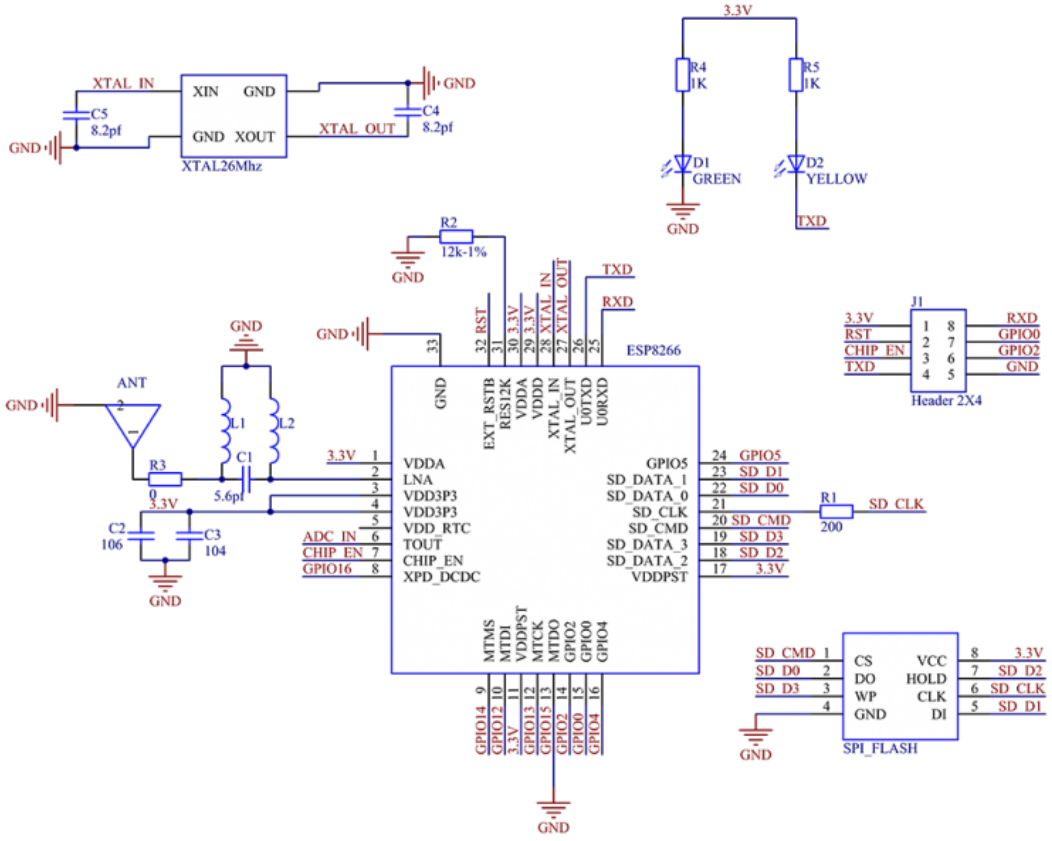
DOOR CONTROL



Title			
Size A4	Number		Revision
Date: 25.4.2019		Sheet of	
File: F:\DP\..\Sheet2.SchDoc		Drawn By:	

Příloha B

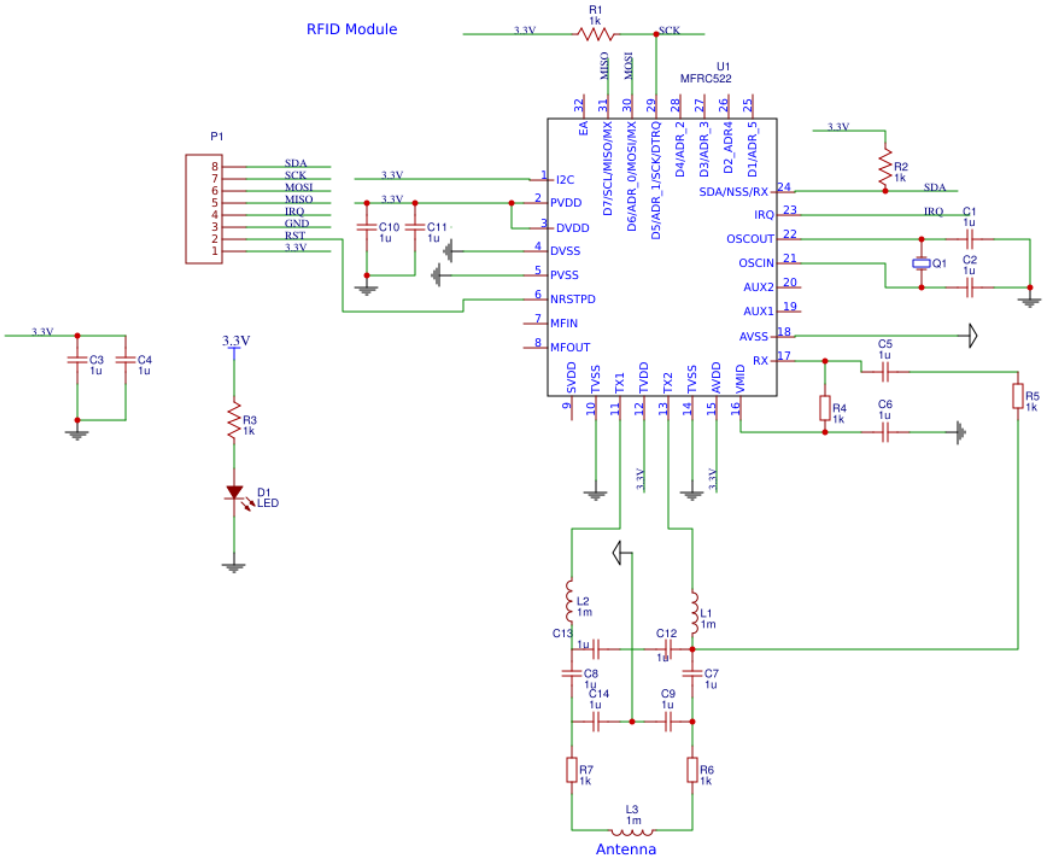
Schéma WiFi modulu



Obrázek B.1: Schéma modulu ESP8266 [31]

Příloha C

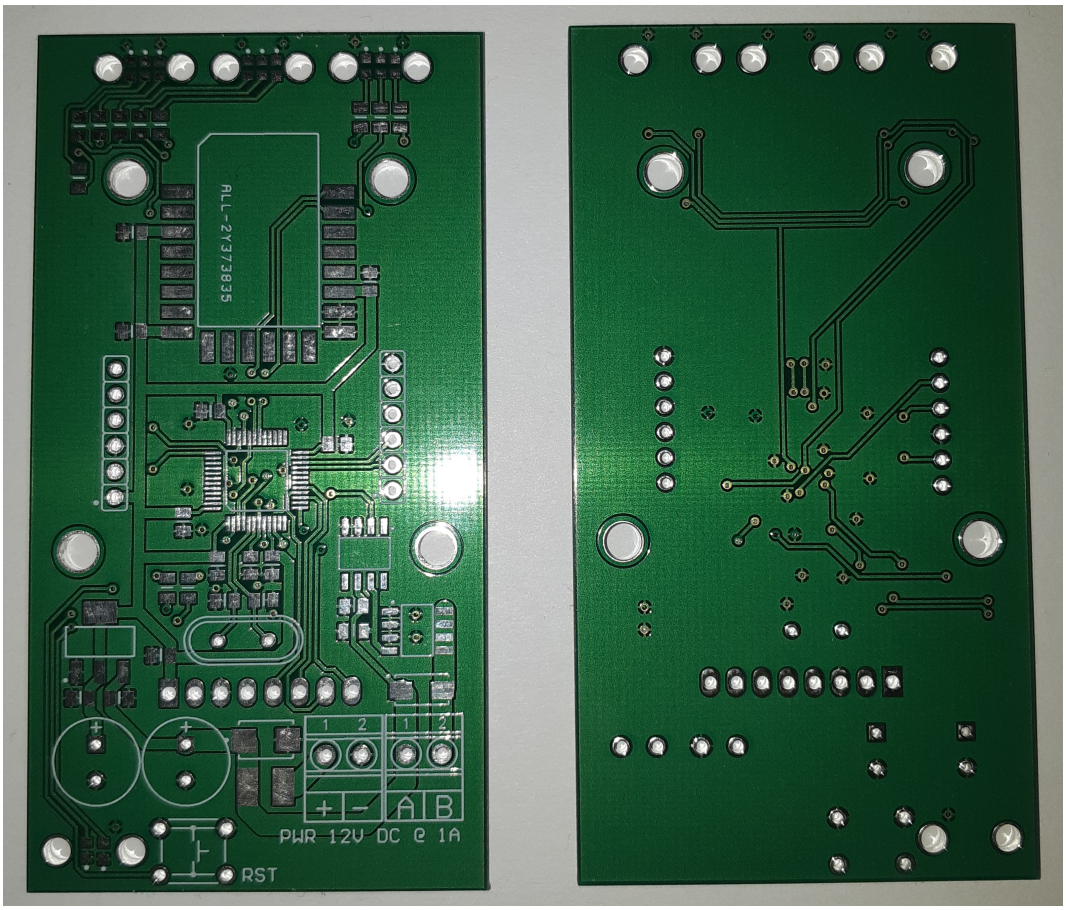
Schéma RFID modulu



Obrázek C.1: Schéma modulu MFRC522 [32]

Příloha D

Fotografie plošného spoje



Obrázek D.1: Plošný spoj čtečky karet

Příloha E

Fotografie čtečky karet

Obrázek E.1: Čtečka karet

Obrázek E.2: Čtečka karet bez krytu