Laboratórna úloha s čítačkou NFC a modulom Arduino

Adrián Mikloši

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Adrián Mikloši**
Osobní číslo:	**A20347**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Laboratorní úloha s čtečkou NFC a modulem Arduino**
Téma práce anglicky:	**Laboratory Task with NFC Reader and Arduino Module**

Zásady pro vypracování

1. Seznamte se s programováním mikropočítače Arduino.
2. Nastudujte problematiku bezkontaktních identifikačních karet se zaměřením na karty Mifare.
3. Navrhněte program pro Arduino Uno, který bude komunikovat pomocí čipu PN532 (NXP) s kartami Mifare.
4. Sestavte laboratorní úlohu s použitím čtečky PN532 a otestujte ji na řadě karet Mifare a k úloze vypracujte vzorové řešení pro studenty a učitele.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. FINKENZELLER, K. RFID Handbook. 2010. Nakladatelství Wiley; Hoboken. ISBN 978-0-470-69506-7.
2. RANKL, W., EFFING, W. Smart card handbook – 4th edition. 1088 stran, 2010. Nakladatelství Wiley; Hoboken. ISBN 978-0-470-74367-6.
3. HEROUT, Pavel. Učebnice jazyka C. Koop. České Budějovice, 6.vydání, 2009. ISBN 978-80-7232-383-8
4. VODA, Zbyšek. Průvodce světem Arduina. Vydání druhé. Bučovice: Martin Stříž, 2017. ISBN 978-80-87106-93-8.
5. NFC Forum [online]. Dostupné z URL: <http://nfc-forum.org.
6. PINKER, Jiří. Mikroprocesory a mikropočítače. Praha: BEN – technická literatura, 2004. ISBN 80-7300-110-1.

Vedoucí bakalářské práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 16. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 5. 6. 2023

Adrián Mikloši

podpis studenta

ABSTRAKT

Bakalárska práca sa zaoberá využitím bezkontaktnej technológie NFC v prístupových zabezpečovacích systémoch a ďalej sa zameriava na karty Mifare ako pasívne nosiče údajov vstupujúcich do takýchto systémov. Výstupom praktickej časti je modelový prototyp simulujúci prístupový zabezpečovací systém, ktorý slúži ako laboratórna pomôcka a poskytuje základ pre laboratórnu úlohu. Základom modelu je platforma Arduino UNO, ku ktorej sú pripojené periférie ako čítačka NFC, maticová klávesnica a dvojriadkový LCD displej. V základnom režime model číta údaje z čipových kariet Mifare a vyhodnocuje udelenie prístupu na základe výsledku porovnania vyčítaných údajov s údajmi v databáze. V režime s vyšším oprávnením systém povoľuje manipuláciu s databázou a umožňuje administrátorovi pridávať alebo odoberať identifikačné čísla čipových kariet zo systému. Vstup do režimu s vyšším oprávnením je zabezpečený dvojfaktorovou autentifikáciou.

Kľúčové slová: NFC, RFID, Arduino, zabezpečovací prístupový systém, čipová karta, Mifare, maticová klávesnica, PN532

ABSTRACT

The bachelor's thesis deals with the use of contactless NFC technology in access security systems and further focuses on Mifare cards as passive data carriers entering such systems. The output of the practical part is a model prototype, simulating an access security system, which serves as a laboratory model and provides a basis for the laboratory task. The basis of the model is the Arduino UNO platform to which peripherals such as an NFC reader, a matrix keyboard and a two-line LCD display are connected. In the basic mode, the model reads data from Mifare smart cards and evaluates the granting of access based on the result of comparing the read data with the data in the database. In higher authority mode, the system allows manipulation of the database and allows the administrator to add or remove smart card identification numbers from the system. Access to the elevated security mode is secured by two-factor authentication.

Keywords: NFC, RFID, Arduino, security access system, smart card, Mifare, matrix keyboard, PN532

Rád by som poďakoval vedúcemu bakalárskej práce, pánovi Ing. Stanislavovi Goňovi, PhD., za odborné konzultácie, návrhy, rady a vedenie. Ďalej patrí moja vďaka rodine, priateľom a kolegom v práci za motiváciu a podporu.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Bezkontaktné technológie majú v súčasnosti široké uplatnenie naprieč rôznymi odvetviami. Pomáhajú zefektívniť procesy v skladovom manažmente a automatizácii, umožňujú pohodlné bezkontaktné platby, a v neposlednom rade prenikli a našli svoje využitie aj v bezpečnostných technológiách. Jeden z posledných počinov technologického vývoja v oblasti bezkontaktnej komunikácie je technológia NFC. NFC je skratka od názvu Near Field Communication a v preklade ide o komunikáciu blízkeho poľa.

Táto technológia sa postupne odvodila a vyvinula z technológie RFID (Radio Frequency Identification). NFC a RFID sú technológie bezdrôtovej komunikácie, ktoré umožňujú výmenu údajov medzi aktívnymi zariadeniami medzi sebou alebo medzi aktívnym zariadením a pasívnym elektrickým obvodom ako je čipová karta. Technológia NFC je postavená na princípoch RFID a zdieľa rovnaké základné koncepty používania rádiových vĺn na bezdrôtovú komunikáciu. Rozdiel spočíva v komunikačných protokoloch a pracovných frekvenciách. Technológia RFID zahŕňa celý rad frekvencií a protokolov, vrátane nízkofrekvenčných (LF), vysokofrekvenčných (HF) a ultravysokofrekvenčných (UHF), pričom každý má svoje výhody a účely použitia. NFC na druhej strane pracuje v rozsahu HF (13,56 MHz) a riadi sa špecifickými protokolmi definovanými organizáciou NFC Forum. Zariadenia NFC môžu tiež čítať a interagovať s určitými typmi pasívnych obvodov RFID, najmä s tými, ktoré pracujú v HF frekvenciách. Táto interoperabilita umožňuje čítačkám NFC komunikovať s mnohými staršími RFID štruktúrami rozšírenými po celom svete.

Táto bakalárska práca sa zameriava na technológiu NFC a jej využitie v bezpečnostných technológiách, konkrétne v zabezpečovacích prístupových systémoch. V praktickej časti popisuje vyhotovenie laboratórneho modelu prístupového systému na platforme Arduino. Jadrom systému je mikrokontrolér ATmega328P a pripojená čítačka NFC s označením PN532. Systém využíva spomínanú interoperabilitu na komunikáciu s RFID kartami Mifare, ktoré slúžia ako token pre identifikáciu predmetom. Ovládanie systému užívateľom umožňuje maticová klávesnica a dvojriadkový LCD displej pre navigáciu v užívateľskom rozhraní. To slúži najmä pre administrátorské funkcie akými sú registrácia nových prístupových kariet do systému, alebo naopak, ich zablokovanie. Režim administrátora je zabezpečený dvojfaktorovou autentifikáciou. Okrem priloženia karty s vyšším prístupom systém požaduje zadanie 4-miestneho pin kódu. Po úspešnej autentifikácií sú sprístupnené vyššie spomínané funkcie pre vykonávanie zmien v databáze.

Vytvorený model systému má slúžiť ako laboratórna pomôcka pre demonštráciu princípov fungovania zabezpečovacieho prístupového systému s využitím bezkontaktnej technológie. Hlavný zdrojový kód predstavuje vzorovú verziu programu a jeho konfigurácie. Sekundárny zdrojový kód je odľahčený o niektoré časti programu, celé funkcie alebo počiatočné definície. Účelom takéhoto kódu je priviesť programátora k využitiu svojich nadobudnutých vedomostí a použiť ich k dosiahnutiu plnej funkčnosti všetkých častí zostaveného modelu v požadovanej konfigurácií.

I. TEORETICKÁ ČASŤ

1 TECHNOLÓGIA RFID

Technológia RFID (Radio-Frequency Identification), ktorá sa zrodila z prvých experimentov s bezdrôtovou komunikáciou, má bohatú históriu, trvajúcu už niekoľko desaťročí. Jej korene možno vystopovať až do 20. storočia, pričom zásadným míľnikom boli objavy v radarovej technológii počas druhej svetovej vojny. Za pomoci radarových vĺn a pasívnych transpondérov vedeli spojenci rozlíšiť svoje lietadlá od nepriateľského letectva. Vynález pasívnych RFID transpondérov koncom 40-tych rokov minulého storočia položil základy moderným RFID systémom. Úsilie o štandardizáciu a príchod digitálneho veku ďalej poháňali integráciu RFID do rôznych priemyselných odvetví, čím spôsobili revolúciu v procesoch a umožnili bezproblémovú identifikáciu a sledovanie objektov vo výrobe alebo skladovom hospodárstve. [1]

1.1 Elektromagnetická indukcia

Základným fyzikálnym javom, na ktorom je založená technológia RFID je elektromagnetická indukcia. Elektromagnetická indukcia je jav, pri ktorom vo vodiči dochádza ku vzniku indukovaného elektromotorického napätia a indukovaného prúdu v dôsledku časovej zmeny magnetického indukčného toku. Objaviteľom tohto významného fyzikálneho javu v roku 1831 bol Michael Faraday. [2]

1.2 Rádio-Frekvenčná Identifikácia

Technológia RFID je systém, ktorý využíva rádiové vlny na automatickú identifikáciu a sledovanie objektov alebo osôb. Funguje prostredníctvom interakcie medzi dvoma hlavnými komponentmi: RFID štítky (tiež známe ako transpondéry alebo tagy) a RFID čítačky. RFID čítačka je zariadenie, ktoré komunikuje s RFID tagmi. Vysiela rádiofrekvenčné signály a zachytáva odpovede z tagov. Čítačka konvertuje prijaté signály na zmysluplné dáta a odovzdáva ich vyšším systémom na ďalšie spracovanie a analýzu. RFID tagy sú malé elektronické zariadenia, ktoré pozostávajú z mikročipu a antény. Po zachytení signálu z čítačky využijú tento signál na odoslanie odpovede vo forme dátovej informácie obsiahnutej v pamäti obvodu. [3]

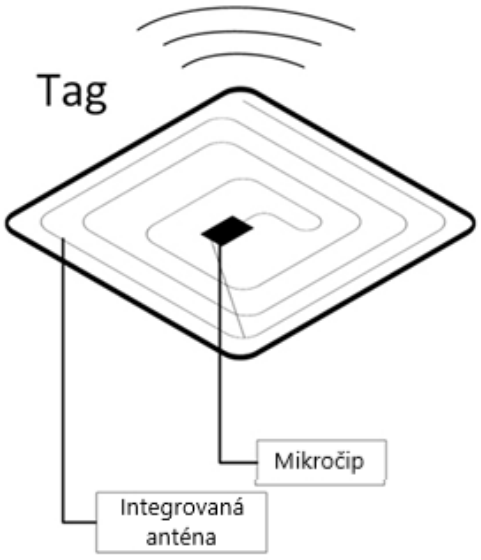
1.2.1 Aktívne tagy RFID

Aktívne štítky RFID majú svoj vlastný zdroj energie, zvyčajne batériu, ktorý im umožňuje aktívne prenášať signály. Tieto štítky neustále vysielajú signál a keď sa čítačka RFID

dostane do rádiusu ich dosahu, zaznamená signál a prečíta informácie z tagu. Aktívne tagy RFID majú dlhší dosah na čítanie a poskytujú možnosť sledovania v reálnom čase. Často sa používajú v aplikáciách ako je sledovanie majetku s vysokou hodnotou, sledovanie pohybu vozidiel a sledovanie personálu. [3]

1.2.2 Pasívne tagy RFID

Pasívne štítky RFID nemajú vlastný zdroj energie a pri aktivácii a napájaní štítku využívajú rádiové vlny vysielané čítačkou RFID. Keď čítačka vyšle signál, anténa štítku ho prijme a jeho energiu použije na napájanie mikročipu. Tag potom odošle späť odpoveď, ktorá obsahuje informácie o jeho unikátnom identifikátore (UID). Okrem identifikátora môže odoslať aj ďalšie dodatočné dáta uložené v pamäti obvodu. Tento proces využíva fyzikálny jav elektromagnetickej indukcie. Pasívne RFID tagy sú nákladovo efektívne, majú dlhšiu životnosť a sú menšie, vďaka čomu sú vhodné pre rôzne aplikácie, ako je riadenie zásob, sledovanie dodávateľského reťazca a kontrola prístupu. [3]



Obrázok 1. RFID pasívny tag [1]

1.3 Frekvenčné pásma v technológií RFID

Technológia RFID využíva rôzne frekvencie v závislosti od špecifických požiadaviek aplikácie, rozsahu a regulačných hľadísk. Dôležitou skutočnosťou je, že frekvencie používané v systémoch RFID podliehajú regionálnym predpisom a normám stanoveným regulačnými orgánmi, ako je Federálna komisia pre komunikácie (FCC) v Spojených štátoch a Európsky inštitút pre telekomunikačné normy (ETSI) v Európe. Tieto predpisy určujú špecifické frekvenčné pásma a limity výkonu, aby sa zabránilo rušeniu s inými bezdrôtovými zariadeniami. [3]

1.3.1 Nízka frekvencia (LF)

Nízkofrekvenčné pásmo využívané v RFID sa nachádza v rozsahu od 125 do 134 kHz a dosah komunikácie RFID v tomto pásme sa pohybuje približne okolo hodnoty 10 centimetrov. Svojimi charakteristikami má ideálne využitie v prostredí s početným výskytom kovov alebo veľkým objemom tekutín. Rádiové vlny v tomto pásme dokážu takýmito materiálmi bezproblémovo preniknúť. V bežnom prostredí sú nízkofrekvenčné RFID technológie používané napríklad pri označovaní zvierat a nesú údaje o vlastníkovi označenej zvery. [3]

1.3.2 Vysoká frekvencia (HF)

Vysokofrekvenčné pásmo využíva kmitočet rádiových vĺn vo výške 13,56 Mhz. Vzdialenosť komunikačnej schopnosti technológie sa v tomto pásme pohybuje v rozsahu okolo 30 centimetrov. S technológiou RFID je možné stretnúť sa najčastejšie práve v tomto vlnovom pásme. Využíva sa napríklad v kníhkupectvách, kde sú RFID tagy založené v jednotlivých knihách a upozornia na pokus o odcudzenie spustením zvukového alarmu pri prechode cez pole dosahu vysielacej antény, spravidla umiestnenej pri vstupe do predajne. Z hľadiska bezpečnostných systémov pracujú v tomto pásme aj prístupové karty alebo iné fyzické predmety určené k autentifikácií v systémoch kontroly prístupu. Hlavnou výhodou tohto frekvenčného pásma je, že je súčasťou mnohých globálnych štandardov a v neposlednom rade sa jedná práve o pásmo na ktorom je založená aj technológia NFC. [3]

1.3.3 Ultra vysoká frekvencia (UHF)

Frekvencie RFID komponentov pri UHF sú primárne 433 MHz alebo 860 až 960 MHz. Systémy UHF RFID umožňujú komunikáciu na veľké vzdialenosti s vysokou rýchlosťou prenosu dát. Často sa používajú pri riadení dodávateľského reťazca, sledovaní zásob,

maloobchode a logistike. UHF tagy ponúkajú výhodu hromadného čítania čo umožňuje identifikáciu viacerých tagov v dosahu čítačky súčasne. Dvojaké rozsahy frekvenčného pásma sú potrebné z dôvodu rozdelenia UHF tagov na pasívne a aktívne. Frekvencia 433 Mhz je využívaná pri aktívnom RFID. Aktívne RFID tagy majú vlastný zdroj napájania a nepotrebujú elektromagnetické vlny z prijímača k odoslaniu dát. To umožňuje komunikáciu až do vzdialenosti viac ako 100 metrov. Pasívne UHF RFID komunikujú v dosahu 25 metrov a prijímač nemá vlastný zdroj napájania. Rovnako umožňujú hromadné čítanie vysielačom a sú cenovo dostupnejšie. [3]

2 TECHNOLÓGIA NFC

Technológia Near Field Communication (NFC) sa prvý krát objavila v roku 2002, kedy bola prvýkrát predstavená ako bezkontaktný prenos dát. Jej vývoj bol do značnej miery poháňaný partnerstvom medzi Sony a NXP Semiconductors (predtým Philips) s cieľom vytvoriť štandard bezdrôtovej komunikácie na krátke vzdialenosti. V roku 2004 bola založená organizácia NFC Forum, ktorá vznikla za účelom štandardizácie technológie NFC a presadzovania jej širšej implementácie. NFC sa v priebehu rokov rozšírilo a získalo uplatnenie v rôznych oblastiach ako sú mobilné platby, dopravné systémy, kontrola prístupu a mnoho ďalších. [4]

2.1 Rozdiel medzi NFC a RFID

NFC vychádza z technológie RFID no nenahrádza ju ako technologicky dokonalejší nástupca ale môžeme povedať že ju dopĺňa alebo rozširuje. NFC pracuje vo frekvenčnom pásme 13,56 MHz, čo predstavuje oblasť vysokej frekvencie (HF). Vďaka tejto skutočnosti existuje kompatibilita medzi zariadeniami NFC a zariadeniami RFID pracujúcimi na frekvencii 13,56 MHz. [5] Zásadným rozdielom medzi NFC a RFID je bezpečnosť komunikácie. Vzhľadom na to, že NFC technológia komunikuje na vzdialenosti len niekoľkých centimetrov (1-3 cm), môže byť odcudzenie uložených dát nežiaducim čítacím zariadením komplikované. Väčšina NFC tagov naviac podporuje uloženie dát v kryptovanej forme. NFC technológia tým pádom poskytuje vlastnosti vhodné pre systémy a operácie kde je vyžadovaný vyšší dôraz na dátovú bezpečnosť. Takýmto operáciami sú napríklad finančné transakcie prostredníctvom POS terminálov alebo autentifikácia v systémoch zabezpečenia prístupu. [6]

2.2 Režimy komunikácie NFC

Zariadenia s podporou NFC sa v anglickom jazyku označujú v jednoduchosti tiež ako NFC-enabled zariadenia. Takéto zariadenie dokáže zastávať nie len funkciu čítačky alebo tagu, ale aj obe pozície súčasne. To akým spôsobom NFC-enabled zariadenie funguje určuje jeho aktuálny režim.

2.2.1 Read/Write režim

Režim zápis/čítanie znamená, že zariadenie s podporou NFC vystupuje ako čítačka (iniciátor) a získava údaje uložené v NFC alebo RFID tagu (pasívny prvok). Po priložení

NFC zariadenia získa pasívny prvok elektrickú energiu z rádiových vĺn. Takto napájaný obvod potom odpovedá odoslaním dát aktívnemu prvku. Na prepisovateľných NFC tagoch je v tomto režime možné dáta pomocou NFC zariadenia prepisovať alebo zapísať nové. [7]

2.2.2 Peer to Peer režim

V režime peer to peer komunikujú dve aktívne NFC-enabled zariadenia priamo medzi sebou. Prostredníctvom NFC môže prebiehať výmena dát napríklad medzi dvoma mobilnými telefónmi (vzájomná výmena kontaktov) alebo napríklad medzi smartfónom a GPS navigáciou s NFC, kedy stačí smartfón priložiť k navigácii a získať tak z nej všetky potrebné dáta. Vďaka NFC je v tomto režime tiež možné výrazne urýchliť proces spárovania zariadení pre inicializáciu komunikácie prostredníctvom technológie Bluetooth. [8]

2.2.3 Card Emulation režim

Card emulation režim umožňuje zariadeniu s podporou NFC vystupovať ako NFC tag. To znamená, že aktívne NFC zariadenie vystupuje ako pasívny NFC tag a odpovedá inému aktívnemu zariadeniu odoslaním požadovaných dát. Ideálnym príkladom je mobilný telefón vystupujúci ako banková karta pri priložení na POS terminál. NFC technológia umožňuje uložiť dáta bankových kariet do NFC čipu v mobilnom telefóne. Názov režimu teda opisuje NFC zariadenie v roli bezkontaktnej čipovej karty. NFC bolo vyvíjané práve za účelom bezkontaktných platieb platobnými kartami. V súčasnosti je využitie tejto technológie oveľa všestrannejšie. Smartfóny s podporou NFC sú v súčasnosti bežnou technologickou vymoženosťou a umožňujú emuláciu viacerých NFC tagov, ale aj niektorých RFID tagov pracujúcich vo vysokofrekvenčnom pásme. [8]

2.2.4 Wireless charging režim

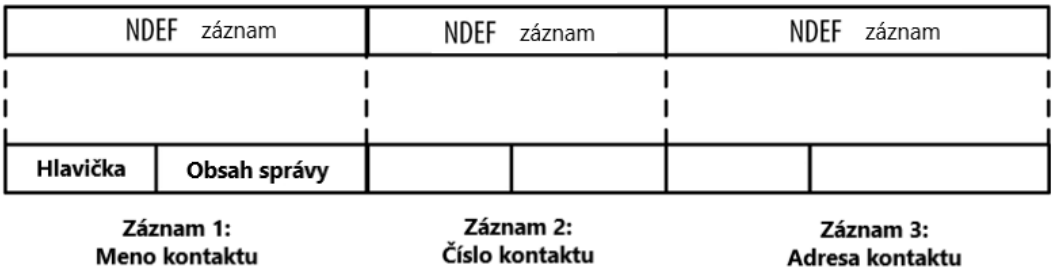
Okrem režimov slúžiacich na výmenu dát medzi zariadeniami, dokáže NFC technológia využiť komunikačný kanál aj na prenos elektrickej energie pre bezdrôtové dobíjanie menších zariadení. V režime bezdrôtového dobíjania je možné preniesť až 1W výkonu a dobíjať tak zariadenia s kondenzátorom alebo malou batériou, napríklad stylus alebo smart hodinky. [7]

2.3 NFC tag

NFC tag je pasívny elektrický obvod bez vlastného napájania. Aby čítačka NFC získala z pamäti takéhoto tagu potrebné dáta, musí mu dodať zdroj elektrickej energie. To sa deje prostredníctvom elektromagnetickej indukcie ku ktorej dochádza pri vysielaní rádiových vĺn

z čítačky vo frekvenčnom pásme 13,56 MHz. Čítačkou môže byť napríklad mobilný telefón. Konštrukcia NFC tagu pozostáva z medenej antény, kondenzátora, mikrokontroléra s pamäťou a zväčša plastového obalu. Anténa zachytáva elektromagnetické vlny vysielané čítačkou, ktoré vďaka vyššie spomínanému fyzikálnemu javu vytvárajú elektrickú energiu. Takto získaná elektrická energia sa ukladá v malom kondenzátore, ktorý slúži ako napájací zdroj pre samotný mikrokontrolér. Ten obsahuje riadiacu jednotku a pamäť. [9]

Dáta sú v NFC tagoch uložené v špecifickom formáte NDEF. NDEF (NFC Data Exchange Format) je štandardizovaný formát, definovaný organizáciou NFC Forum. NDEF podporuje rôzne typy záznamov, ako sú text, URL, email, alebo telefónne čísla, čím poskytuje konzistentnú štruktúru pre ukladanie a prenos údajov medzi rôznymi zariadeniami NFC. Výhodou NDEF formátu je, že zariadenie, ktoré tento formát rozpozná môže okamžite spustiť akciu korešpondujúcu so získaným záznamom. Napríklad zahájiť telefonický hovor po prečítaní tagu s telefónnym číslom. [10]



Obrázok 2. NDEF štruktúra dát

2.4 Typy NFC tagov

Organizácia NFC Forum definuje 5 rôznych typov NFC tagov, pričom stavia na existujúcich medzinárodných normách ISO z oblasti bezkontaktnej komunikácie. Podrobnejšie informácie k týmto normám sú uvedené v kapitole 4.

2.4.1 Typ 1 NFC Tag

Typ 1 je vhodný na ukladanie menšieho množstva dát. Vo svojej pamäti zvládne uchovať napríklad webovú adresu alebo vizitku s telefónnym číslom. Nevýhodou typu 1 je absencia antikolízneho mechanizmu. Veľkosť pamäte je v rozsahu od 93 B po 2 KB. Rýchlosť

prenosu dát je približne 106 kbit/s. Pamäť môže byť prepisovateľná aj uzamknutá, určená len na čítanie. Typ 1 je v súlade s normou ISO/IEC 14443A. [11]

2.4.2 Typ 2 NFC Tag

Typ 2 je vo väčšine špecifík totožný s typom 1. Je rovnako v súlade s normou ISO/IEC 14443A a prenosová rýchlosť je tiež identická. Rozdiel je vo veľkosti pamäte a mechanizme. Typ 2 má rozsah od 48 B po 2 KB a disponuje antikolíznym mechanizmom. [11]

2.4.3 Typ 3 NFC Tag

Typ 3 je už v rozdieloch signifikantnejší. Vyrába sa s v súlade s odlišnými normami ISO/IEC 18092 a JIS X 6319-4. Podporuje antikolízny mechanizmus a rýchlosť komunikácie prebieha v rozsahu od 212 kbit/s po 424 kbit/s. Pamäť má 2 KB a môže byť prepisovateľná alebo len na čítanie. [11]

2.4.4 Typ 4 NFC Tag

Typ 4 je zhodný s ISO/IEC 14443A aj s ISO/IEC 14443B. Je určený na uchovanie citlivejších dát a bez špecializovaného zariadenia neumožňuje ich prepis. Vyrába sa tiež k uchovaniu väčšieho objemu dát ako predchádzajúce typy a preto disponuje 32 KB pamäťou. Rýchlosti prenosu môžu byť 106 kbit/s, 212 kbit/s alebo 424 kbit/s. [11]

2.4.5 Typ 5 NFC Tag

Typ 5 je najnovšia špecifikácia, ktorú prijalo NFC Forum. Výroba je v súlade so štandardami ISO/IEC 15693. Podporuje antikolízny mechanizmus a rýchlosť komunikácie je 26,48 kbit/s. Veľkosť pamäte je až 64 KB. [11]

3 SMART KARTY MIFARE

MIFARE je typ technológie bezkontaktných čipových kariet, ktorá sa bežne používa v systémoch kontroly prístupu, systémoch verejnej dopravy, vernostných systémoch a mnohých iných aplikáciách, ktoré vyžadujú bezpečnú identifikáciu a autentifikáciu. Technológia bola vyvinutá spoločnosťou NXP Semiconductors (predtým Philips Semiconductors) na základe technológie RFID. Svoj prvý produkt, smart kartu Mifare Classic, uvidela na trh v roku 1994. Vďaka dobre vyváženému pomeru medzi cenou a funkciami sa za krátko stala jednou z najrozšírenejších čipových kariet. [12]

V roku 2002 spoločnosť Sony a NXP odprezentovali novú technológiu NFC na ktorej vývoji sa spoločne podieľali. Sony vo svojej vlastnej technológií smart kariet FeliCa a NXP v smart kartách Mifare. V roku 2004 vznikla za účelom štandardizácie v NFC organizácia NFC Forum, založená spoločnosťami NXP, Sony a Nokia. Štandardy NFC Forum vychádzali z už existujúcich ISO/IEC 14443 štandardov pre bezkontaktné čipové karty. [13]

Technológia MIFARE v súčasnosti používa proprietárne riešenia založené na štandardoch ISO/IEC 14443 a štandardoch organizácie NFC Forum. V portfóliu smart kariet Mifare je niekoľko rôznych typov, ktoré sa od seba líšia funkcionalitou, bezpečnosťou a cenou. Na základe preštudovania dokumentácií dostupných na stránkach NXP a NFC Forum je nutné zdôrazniť, že nie všetky smart karty Mifare spĺňajú špecifikácie ISO 14443 a NFC Forum Tag vlastnosti v plnom rozsahu. Napríklad smart karty Mifare Ultralight spĺňajú definované vlastnosti NFC Forum Tag Type2 zatiaľ čo Mifare Classic 1K/4K majú svoje vlastné proprietárne špecifiká. [14] Podobne je to aj s normami ISO 14443A a ISO 14433B. Niektoré smart karty Mifare spĺňajú normu v plnom rozsahu, iné zase len niektoré jej pod kapitoly. Typy smart kariet Mifare a ich vzťah k normám ISO 14443 sú rozpísané ďalej v tejto kapitole.

3.1 Bezpečnostné funkcie smart kariet

Bezkontaktné čipové karty využívajú rôzne bezpečnostné mechanizmy na zabezpečenie dôveryhodnosti, integrity a pravosti údajov. Na ochranu citlivých dát využívajú rôzne kryptografické algoritmy. Taktiež používajú bezpečné postupy správy kľúčov, vrátane ich diverzifikácie a bezpečného ukladania, aby zabránili neoprávnenému prístupu. Bezkontaktné čipové karty navyše implementujú protokoly vzájomnej autentifikácie na overenie legitimity karty aj čítačky kariet, čím poskytujú robustnú ochranu proti klonovaniu, manipulácii a neoprávnenému použitiu. [13]

3.1.1 Kryptovacie algoritmy

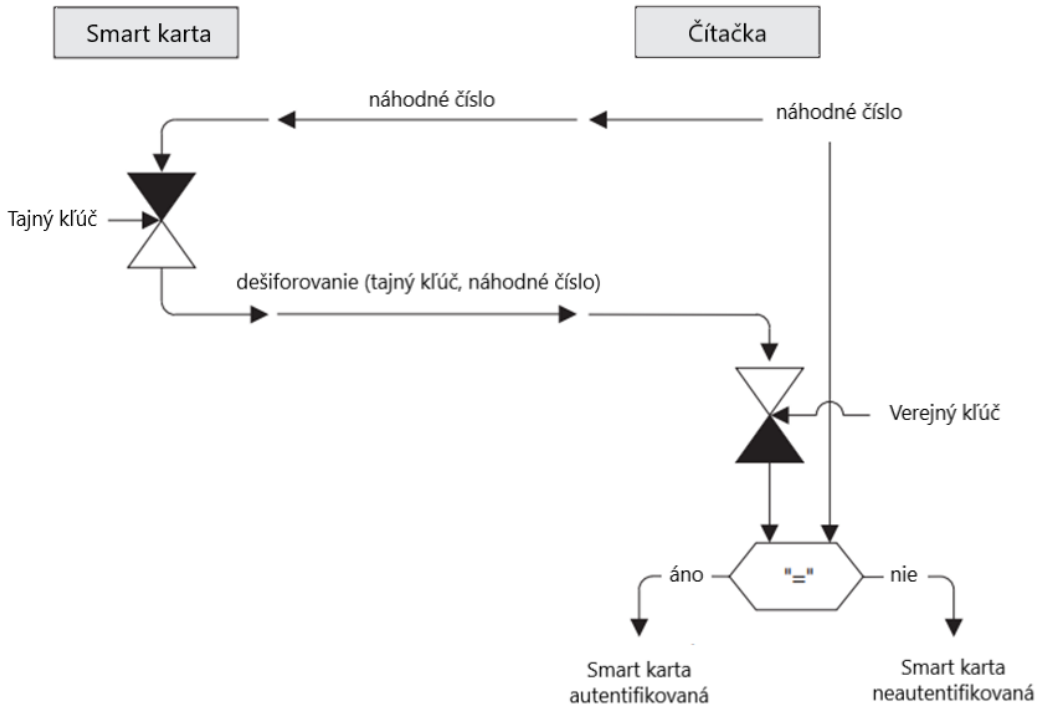
K ochrane dát uložených v pamäťovej jednotke smart karty sa najčastejšie používajú algoritmy AES, DES a 3DES. AES je moderný a často používaný symetrický šifrovací algoritmus známy svojou silnou bezpečnosťou a efektívnosťou. DES je starší algoritmus, ktorý sa v súčasnosti stále používa, no bol do značnej miery nahradený kvôli nedostatočnej veľkosti šifrovacieho kľúča. Jeho vylepšená verzia 3DES poskytuje vyššiu bezpečnosť ale v porovnaní s AES je pomalší. Kľuč sa používa na vykonávanie operácií šifrovania a dešifrovania a pozná ho iba karta a oprávnené subjekty (napríklad čítačka a zodpovedný administrátor). [13]

Názov	Nešifrovaná správa	Šiforovaná správa	Veľkosť kľúča
DES	8 bytes	8 bytes	56 bits
Triple DES with two keys	8 bytes	8 bytes	112 bits (2 × 56 bits)
Triple DES with three keys	8 bytes	8 bytes	168 bits (3 × 56 bits)
IDEA	8 bytes	8 bytes	128 bits
AES	16 bytes	16 bytes	128 bits (16 bytes) 192 bits (24 bytes) 256 bits (32 bytes)

Obrázok 3. Parametre šifrovacích algoritmov [13]

3.1.2 Autentifikácia

Na zabezpečenie legitimity karty aj čítačky prebieha proces vzájomnej autentifikácie. Tento proces prebieha spôsobom výzva-reakcia. Čítačka kariet vygeneruje náhodnú výzvu alebo číslo a odošle ju na kartu. Karta použije svoje uložené kryptografické kľúče na dešifrovanie výzvy a odošle súvisiacu zašifrovanú odpoveď späť do čítačky. [13]



Obrázok 4. Proces vzájomnej autentifikácie karty a čítačky [13]

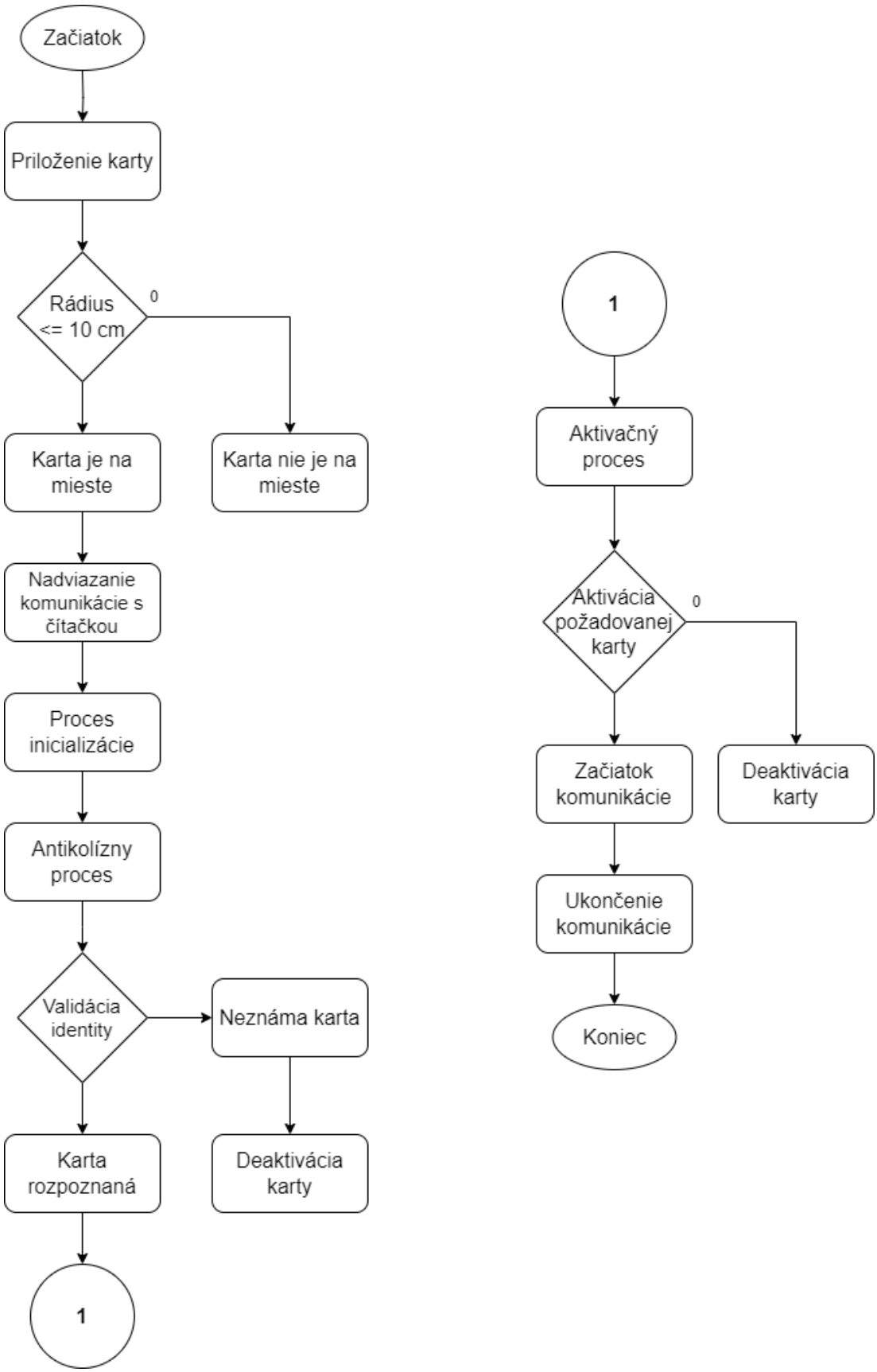
3.1.3 Antikolízny mechanizmus a inicializácia

Antikolízny mechanizmus v bezkontaktných smart kartách sa používa na efektívne rozlišovanie medzi viacerými kartami v dosahu čítačky. Inicializačný proces začína odoslaním príkazu protikolíznej slučky z čítačky kariet, aby sa karty aktivovali. Každá karta v dosahu odpovedá svojim unikátnym identifikátorom (UID). UID je sériové číslo, ktoré je pre každú kartu odlišné (unikátne). Čítačka kariet analyzuje reakcie a deteguje kolízie, ak súčasne reaguje viacero kariet. V tomto bode sa aktivuje bitový antikolízny algoritmus. Čítačka kariet spúšťa sériu príkazov, selektívne vysiela jednotlivé bity UID a žiada karty, aby odpovedali iba vtedy, ak sa ich UID zhoduje s prenášaným vzorom. Antikolízny proces iteratívne zužuje rozsah možných UID tým, že ho rozdeľuje na základe prijatých odpovedí. Tento proces pokračuje až kým nezostane jednoznačne identifikovaná iba jedna karta. Tá je následne zvolená pre ďalšiu komunikáciu a antikolízny proces je dokončený. To umožňuje efektívnu identifikáciu a komunikáciu s viacerými kartami a zaisťuje ich spoľahlivé a presné rozpoznanie. [13]

3.2 Priebeh komunikácie medzi kartou a čítačkou

1. Inicializácia: Čítačka odošle na kartu požiadavku na začatie komunikácie. Táto požiadavka obsahuje informácie, ako je typ karty, komunikačný protokol a podporované príkazy.
2. Antikolízna detekcia: Karta reaguje na požiadavku čítačky odoslaním svojho unikátneho identifikačného čísla. Ak sa v dosahu čítačky nachádza viacero kariet, na vyriešenie konfliktov sa aktivuje antikolízny mechanizmus vysvetlený v predchádzajúcej podkapitole.
3. Výber: Čítačka vyberie konkrétnu kartu s ktorou chce ďalej komunikovať, zvolením jej UID.
4. Autentifikácia: Čítačka odošle na zvolené UID overovaciu správu. Karta správu dešifruje, spracuje odpoveď a zašifrovanú ju odosiela čítačke.
5. Prenos dát: Po dokončení autentifikácie môže čítačka komunikovať s kartou princípom príkaz-reakcia. Čítačka odošle príkaz na kartu a karta odpovie požadovanými údajmi alebo stavovým kódom.
6. Ukončenie: Po ukončení každého procesu príkaz-reakcia dochádza k vzájomnej výmene správy o ukončení.

Presný proces komunikácie sa môže líšiť v závislosti od konkrétneho typu použitej karty alebo čítačky, ako aj od použitých príkazov a komunikačných protokolov. [13]



Obrázok 5. Priebeh komunikácie čítačky s čipovou kartou

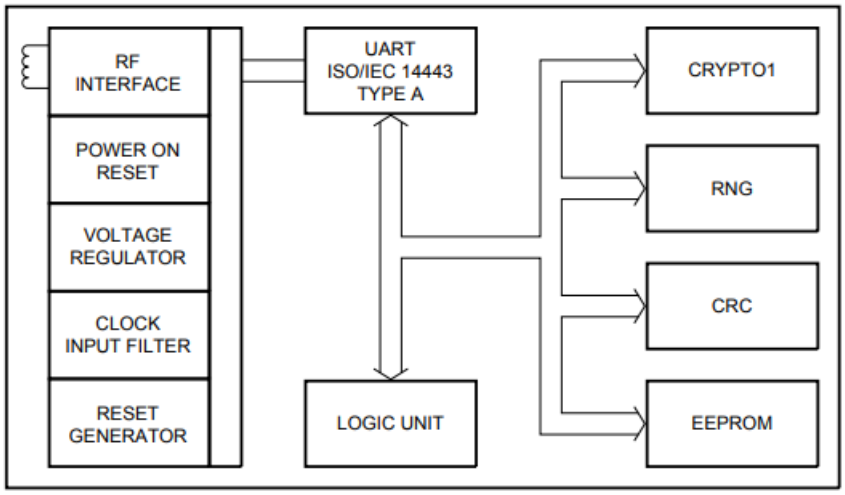
3.3 Typy bezkontaktných smart kariet MIFARE

Karty MIFARE existujú v rôznych variantoch a každá z nich ma rozdielny účely použitia.

3.3.1 MIFARE Classic

Classic je najstarší typ karty Mifare a široko používaná technológia bezkontaktných čipových kariet do roku 2008. V tom roku boli zaznamenané významné narušenia v jej bezpečnosti. Výskumníci a hekeri objavili chyby v šifrovacom algoritme Crypto1 používanom kartami Mifare Classic. To im umožnilo prelomiť kryptografické kľúče karty a získať prístup k údajom v pamäti. Crypto1 je proprietárny algoritmus organizácie NXP a jeho problémom bola malá veľkosť kryptovacieho kľúča. To umožnilo útoku hrubou silou v relatívne krátkom čase zistiť jeho podobu. V tom čase už 18 rokov starý kryptovací algoritmus DES vyžadoval o 256 pokusov o útok hrubou silou viac ako Crypto1. Tieto udalosti poukázali na potrebu prísnejších bezpečnostných opatrení v systémoch čipových kariet a viedli k vývoju vylepšených verzií kariet Mifare. [12]

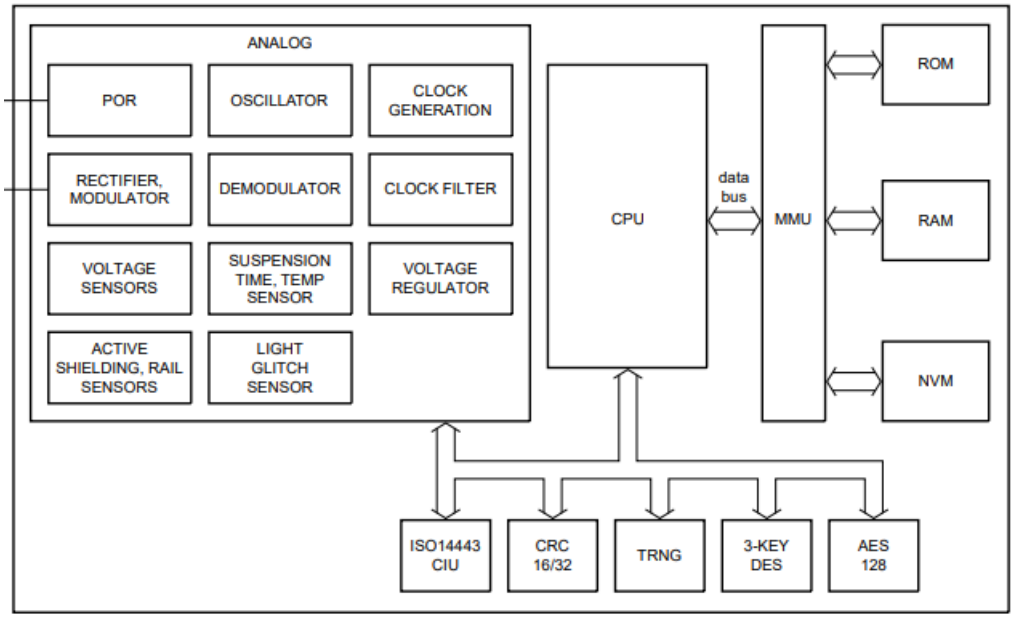
Napriek vyššie uvedeným udalostiam sa karty Mifare Classic používajú v niektorých oblastiach aj v súčasnosti. Vzhľadom na cenovú dostupnosť majú stále svoje uplatnenie v systémoch s nižšími nárokmi na bezpečnosť. Okrem toho sú na trhu k dispozícii aj v zmodernizovanej verzii Mifare Classic EV1, ktorá používa vylepšený algoritmus Crypto1 a pridáva dodatočný level autentifikácie. Obe verzie majú kapacitu pamäte 1 KB alebo 4 KB a z normy ISO/IEC 14443A spĺňajú časť 3, ktorá definuje antikolízny mechanizmus. Karty Classic sú vhodnejšie skôr do oblastí s nižšími požiadavkami na bezpečnosť. [15]



Obrázok 6. Blokový diagram integrovaného obvodu MIFARE Classic [15]

3.3.2 MIFARE Plus EV2

Karta Mifare Plus EV2 je už výraznejšie aktualizovaná verzia Classic kariet, ktorá ponúka vylepšené bezpečnostné funkcie. Má kapacitu pamäte 2 KB alebo 4 KB a na ochranu údajov využíva bezpečnejšie 128 bitové šifrovanie Advanced Encryption Standard (AES). Spĺňa všetky 4 časti normy ISO/IEC 14443. Je plne spätne kompatibilná so systémami Mifare Classic a teda môže používať aj šifrovanie algoritmom Crypto1. Nastavenie úrovne bezpečnosti tejto karty je možné prispôsobiť rôznym bezpečnostným požiadavkám systému v škále troch stupňov. S ohľadom na tieto vlastnosti má svoje uplatnenie aj v systémoch kontroly prístupu alebo systémoch verejnej dopravy s kreditnými transakciami. [16]



Obrázok 7. Blokový diagram integrovaného obvodu MIFARE Plus [16]

3.3.3 MIFARE DESFire

Karta Mifare DESFire je vysoko zabezpečená karta, ktorá používa na ochranu údajov šifrovacie algoritmy DES, 3DES a AES. Má kapacitu pamäte v najvyššej variante až 8 KB a je možné ju použiť pre širokú škálu aplikácií s požiadavkou na maximálnu bezpečnosť v ochrane dát. [17]

3.3.4 MIFARE SAM

Modul Mifare SAM (Secure Access Module) je samostatný modul, ktorý sa používa v kombinácií s inými kartami Mifare na poskytovanie dodatočných bezpečnostných funkcií. Obsahuje kryptografický koprocesor a používa sa v aplikáciách kde je vyžadovaná dodatočná úroveň kryptografického zabezpečenia. [18]

3.3.5 MIFARE Ultralight

Karta Mifare Ultralight je lacná možnosť, ktorá sa často používa na jednorazové lístky alebo iné aplikácie, kde sa vyžaduje len obmedzená pamäť a žiadne zabezpečenie. Má kapacitu pamäte 512 bitov a nemá zabudované žiadne bezpečnostné prvky. Spĺňa časť 3 z normy ISO/IEC 14443, ktorá definuje antikolízny mechanizmus. [19]

3.3.6 MIFARE Ultralight C

Karta Mifare Ultralight C je podobná karte Ultralight ale obsahuje vstavaný autentifikačný mechanizmus pre vyššiu bezpečnosť. Má kapacitu pamäte 512 bitov a využíva algoritmus 3DES, čo ju robí odolnejšou voči klonovaniu. Používa sa prevažne v systémoch verejnej dopravy. [20]

4 ŠTANDARDY V BEZKONTAKTNEJ KOMUNIKÁCII

Near Field Communication (NFC) je bezkontaktná komunikačná technológia, ktorá bola prvýkrát štandardizovaná spoločnosťou Ecma (ECMA 340) a neskôr prijatá organizáciou ISO/IEC (ISO/IEC 18092). NFC je kompatibilné aj so staršími systémami bezkontaktných čipových kariet založených na štandardoch ISO/IEC 14443 a FeliCa (JIS X 6319-4). Normalizácia v oblasti NFC sa tiež zamerala aj na zvýšenie kompatibility so štandardom ISO/IEC 15693. ISO/IEC 15693 je medzinárodná norma, ktorá popisuje fyzické, fyzikálne a informačno-technické charakteristiky bezkontaktných čipových kariet a iných objektov a príslušných čítacích zariadení. [21]

Okrem štandardizácie prostredníctvom normatívnych orgánov ako ISO/IEC a Ecma, existuje aj štandardizácia vychádzajúca z organizácie NFC Forum. Cieľom NFC Forum je ďalšia špecifikácia dátových formátov, protokolov, požiadaviek na interoperabilitu a tiež certifikácia zariadení a aplikácií NFC.

4.1 ISO/IEC 14443

ISO/IEC 14443 je široko uznávaný medzinárodný štandard pre bezkontaktné čipové karty a RFID/NFC tagy, ktorý definuje fyzické parametre a vrstvy dátového spojenia komunikačného protokolu. Norma je rozdelená na 4 časti v ktorých špecifikuje frekvenčný rozsah, modulačnú schému a ďalšie parametre komunikácie, ako aj dátový formát a protokol pre výmenu informácií medzi kartou a čítačkou. [22]

Norma ISO/IEC 14443 používa pre komponenty nasledujúce výrazy:

PCD: proximity coupling device (čítačka RFID kariet)

PICC: proximity integrated circuit card (karta RFID)

4.1.1 ISO/IEC 14443-1:2018

Popisuje fyzikálne charakteristiky, špecifikuje fyzické rozmery, ohybnosť, odolnosť voči prostrediu (ultrafialové a röntgenové žiarenie) alebo rušeniu elektromagnetických podmienok pre garantovanú funkčnosť. Norma popisuje aj potrebný súlad s ďalšími normami a to s ISO/IEC 7810 alebo ISO/IEC 15457-1. [22]

4.1.2 ISO/IEC 14443-2:2020

Popisuje rádiofrekvenčné napájanie (elektromagnetická indukcia) a signálové rozhranie (interface), ktoré špecifikuje charakteristiku polí poskytnutých pre napájanie a obojsmernú komunikáciu medzi zariadeniami PCD (RFID čítače) a bezdotykovými kartami alebo objektmi PICC (RFID karty alebo predmety). [22]

4.1.3 ISO/IEC 14443-3:2018

Predmetom normy je inicializácia a antikolízny mechanizmus. Definuje dotazovanie pre bezdotykové karty alebo objekty (PICC), ktoré vstupujú do poľa aktívneho zariadenia (PCD). Ďalej popisuje rámce a časovanie používané počas počiatočnej fázy komunikácie medzi PCD a PICC, bajtový formát, stavy karty alebo iných PICC predmetov a kódovanie dotazov a odpovedí. [22]

4.1.4 ISO/IEC 14443-4:2016

Špecifikuje prenosový protokol a funkcie pre špeciálne potreby bezkontaktných podmienok a definuje sekvencie aktivácie a deaktivácie protokolu (naviazanie a ukončenie komunikácie medzi PICC a PCD). [22]

4.1.5 Typ „A“ a typ „B“

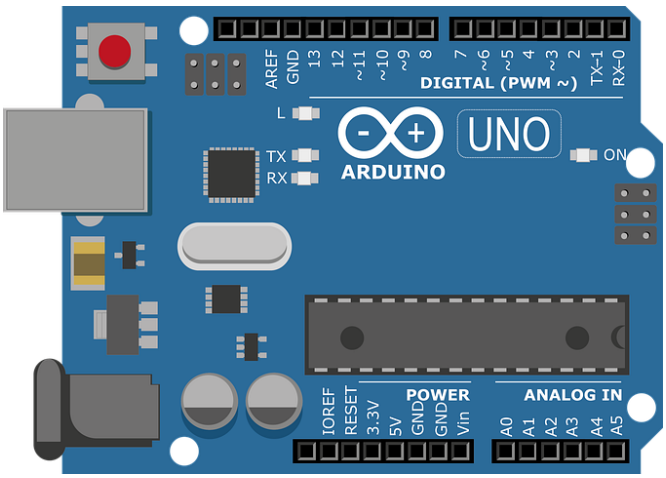
Podľa normy ISO/IEC 14443 existujú dva typy PICC kariet alebo predmetov. Typ „A“ a typ „B“, pričom oba komunikujú prostredníctvom rádiových vĺn pri 13,56 MHz. Hlavné rozdiely medzi týmito dvoma typmi sa týkajú modulačných metód, schém kódovania (ISO/IEC 14443-2) a postupov inicializácie protokolu (ISO/IEC 14443-3). Oba typy RFID kariet sa riadia rovnakým prenosovým protokolom (opísaným v časti ISO/IEC 14443-4). [22]

5 PLATFORMA ARDUINO

Arduino je licenčne otvorená (open-source) elektronická vývojová doska. Nadšenci do elektrotechniky ale aj profesionálny výrobcovia môžu použiť Arduino na navrhovanie a vytváranie elektronických zariadení, ktoré interagujú s fyzickým svetom.

Platforma Arduino bola vytvorená v roku 2005 v Interaction Design Institute Ivrea (IDII) v Taliansku. V tom čase boli dosky mikrokontrolérov viac určené pre profesionálne použitie a študenti na IDII potrebovali jednoduchší aj cenovo dostupnejší spôsob vytvárania svojich projektov. Skupina ľudí z univerzitného prostredia sa napokon rozhodla, že vytvoria svoju vlastnú vývojovú dosku. To sa im podarilo a zakrátko bol záujem o Arduino rozšírení po celom technologickom svete. Neskôr dospeli k rozhodnutiu poskytnúť technické podklady k jeho výrobe pod otvorenou licenciou a dali tak školám aj elektrotechnickým nadšencom ešte viac možností. Zaujímavosťou je, že názov Arduino je podľa názvu baru v ktorom sa zakladajúci členovia stretávali počas jeho vývoja. [23]

V technikom slova zmysle je Arduino obvod s mikrokontrolérom, čo je v podstate celý jednoduchý počítač na malej doske. Mikrokontroléry sú vo väčšine modelov 8-bitové a ich výrobcom je firma Atmel. Majú procesorové jadro, pamäť, vstupné a výstupné ovládacie prvky, bity pre správu napájania, moduly časovania, vstupné a výstupné hlavičky atď.. Vďaka otvorenej licencií je dostupné veľké množstvo softvérových knižníc a hardvérových rozšírení. [23]



Obrázok 8. Arduino doska model UNO

5.1 Mikrokontrolér

Najdôležitejším komponentom dosiek Arduino je mikrokontrolér. Mikrokontrolér je kompaktný integrovaný obvod (IC), ktorý obsahuje mikroprocesorové jadro, pamäť a periférne rozhrania na jednom čipe. Je navrhnutý tak, aby vykonával špecifické úlohy a ovládal externé zariadenia na základe inštrukcií uložených v jeho pamäti. [24]

5.1.1 Pamäť

Programová pamäť (Flash) uchováva programové inštrukcie, ktoré mikrokontrolér vykonáva. Inak povedané, obsahuje zdrojový kód programu.

Dátová dynamická pamäť (RAM) uchováva dočasné údaje ako sú premenné, zásobník a hodnoty registrov, počas behu programu.

Pamäť EEPROM slúži na ukladanie dát, ktoré je potrebné uchovávať aj po odpojení napájania. [24]

5.1.2 Mikroprocesorové jadro

Pozostáva z aritmeticko-logickej jednotky (ALU) na vykonávanie matematických a logických operácií, riadiacej jednotky na riadenie toku inštrukcií a registrov na dočasné ukladanie dát. Jadro získava inštrukcie z pamäte, dekóduje ich a vykonáva požadované operácie. [24]

5.1.3 Periférne rozhrania

Periférne rozhrania rozširujú funkčnosť a všestrannosť mikrokontroléra a umožňujú mu komunikovať s externými zariadeniami. Príklady periférií mikrokontrolérov sú vstupné/výstupné (I/O) porty na pripojenie k senzorom a akčným členom, časovače a počítadlá pre presné časovacie operácie, sériové komunikačné rozhrania ako UART, SPI a I2C pre výmenu dát s inými zariadeniami, digitálne prevodníky (ADC) na konverziu analógových signálov na digitálne a moduly s pulzne šírkovou moduláciou impulzov (PWM) na generovanie analógových signálov. [24]

5.1.4 Slučka a prerušenia

Slučka je základný princíp, ktorým mikrokontrolér vykonáva inštrukcie. Začína načítaním inštrukcie z pamäte, pokračuje dekódovaním a končí vykonaním inštrukcie. Tento cyklus sa neustále opakuje, čo umožňuje mikrokontroléru sekvenčne spracovávať inštrukcie a

vykonávať naprogramované úlohy. Počas tohto cyklu sa môžu vyskytnúť prerušenia, ktoré dočasne pozastavia normálny tok vykonávania inštrukcii. Keď dôjde k prerušeniu, mikrokontrolér uloží svoj aktuálny stav a preskočí na službu prerušenia (ISR). ISR vykoná špecifickú akciu alebo úlohu spojenú s udalosťou prerušenia, ako je čítanie hodnoty senzora alebo spracovanie externého vstupu. Po dokončení ISR sa mikrokontrolér vráti k prerušenej úlohe a obnoví normálne vykonávanie slučky. Prerušenia sú kľúčové pre zvládnutie časovo kritických udalostí, zabezpečujú včasnú odozvu a efektívny multitasking. [24]

5.2 Typy dosiek Arduino

Modely Arduina obsahujú množstvo rôznych elektronických komponentov na jednej doske plošných spojov. Základom každej z nich je mikrokontrolér od firmy Atmel. Dizajn a zloženie závisí od konkrétneho modelu. Tých je v súčasnosti pomerne mnoho a každý z nich má svoje špecifické vlastnosti a využitie. V nasledujúcich podkapitolách sú popísané niektoré najznámejšie Arduino modely. [23]

5.2.1 Arduino Nano

Arduino Nano je kompaktná a všestranná doska založená na mikrokontroléry ATmega328P (16 MHz). Nano má 14 digitálnych I/O pinov, 8 analógových pinov a 6 pinov s PWM moduláciou. Disponuje tiež vstavaným USB rozhraním pre programovanie a komunikáciu s počítačom. Vďaka svojej malej veľkosti sa Arduino Nano bežne používa v projektoch kde je obmedzený priestor alebo je požadovaný kompaktnejší dizajn. [23]

5.2.2 Arduino Uno

Arduino Uno doska je založená na mikrokontroléry ATmega328P. Je to jeden z najobľúbenejších modelov Arduino vďaka svojej jednoduchosti a všestrannosti. Arduino Uno má 14 digitálnych I/O pinov, z toho 6 PWM pinov a ďalších 6 analógových vstupných pinov. To umožňuje pripojenie a ovládanie rôznych senzorov, akčných členov a ďalších komponentov z jednej dosky. Súčasťou je aj USB rozhranie pre programovanie a komunikáciu s počítačom. Arduino Uno sa bežne používa na prototypové projekty, vďaka čomu je vhodnou voľbou pre začiatočníkov ale aj skúsených výrobcov. [23]

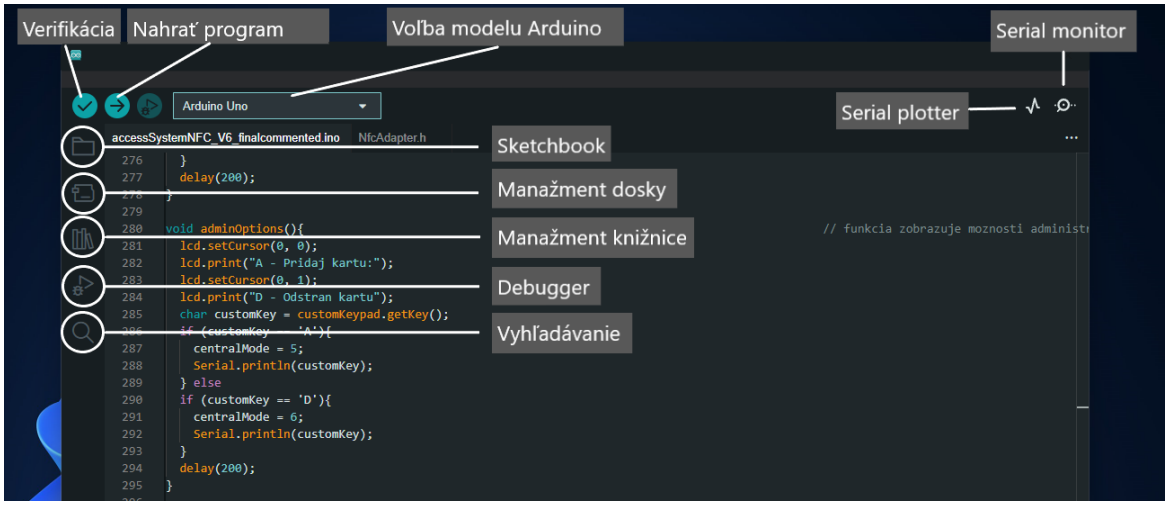
5.2.3 Arduino Mega

Arduino Mega je pokročilá doska, ktorá ponúka výrazne viac vstupných/výstupných pinov a pamäte v porovnaní s inými modelmi Arduino. Je založená na mikrokontroléry

ATmega2560 a poskytuje rozšírené možnosti pre väčšie a komplexnejšie projekty. Arduino Mega má až 54 digitálnych I/O pinov (z toho 15 s PWM) a 16 analógových vstupných pinov. Obsahuje tiež 256 KB flash pamäte pre ukladanie programov a 8 KB dynamickej pamäte. Vďaka rozšíreným I/O a pamäťovým zdrojom je Arduino Mega obzvlášť vhodné pre projekty, ktoré vyžadujú vysoký počet pripojení alebo väčší výpočtový výkon. [23]

5.3 Arduino IDE

Arduino IDE je užívateľsky prívetivé vývojové prostredie vyvinuté priamo pre programovanie dosiek Arduino. Doska Arduino je pripojená k počítaču cez USB, kde sa prepojí s vývojovým prostredím Arduino (IDE). IDE je napísané v jazyku Java a vychádza z výukového prostredia Processing. Ponúka editor kódu so zvýrazňovaním syntaxe a automatickým dopĺňaním, správcu knižníc pre jednoduchú integráciu do vlastného kódu a zjednodušený proces nahrávania skompilovaného kódu na dosku Arduino. Poskytuje tiež príklady a návody, ktoré používateľom pomáhajú naučiť sa a implementovať rôzne funkcie Arduina. IDE je open-source a je dostupné pre viacero operačných systémov zdarma. [23]



Obrázok 9. Arduino IDE – popis vývojového prostredia

5.3.1 Jazyk prostredia Arduino IDE

Kód pre Arduino je napísaný v programovacom jazyku C alebo C++ ale častejšie sa vyžíva písanie pomocou knižnice Wiring. Wiring predstavuje akúsi nadstavbu jazyka C++ no nejedná o plnohodnotný programovací jazyk. Súbor do ktorého sa v Arduino IDE píše zdrojový kód sa v tomto prostredí nazýva sketch (náčrt). Napísaný zdrojový kód v náčrtoch sa na pokyn užívateľa skompiluje a nahrá do pamäte pripojeného Arduina. Kompilácia je

proces pri ktorom sa program napísaný užívateľom v programovacom jazyku prekladá do strojového jazyka, ktorému rozumie procesor. [23]

5.3.2 Knižnice

Knižnice sú súbory funkcii pre riešenie špecifických úloh a problematík. Podobne ako v iných programovacích prostrediach, aj pre Arduino existujú vstavané knižnice, ktoré poskytujú základné programové funkcie. Okrem toho je možné importovať ďalšie knižnice a rozšíriť možnosti a funkcie dosky Arduino. Vďaka open-source licencovaniu a obrovskej komunite existuje množstvo knižníc zameraných na rôzne oblasti. Poskytujú napríklad základný zdrojový kód pre ovládanie pripojených zariadení ako je čítačka RFID kariet alebo maticová klávesnica.

5.3.3 Štruktúra programu

Každý program pre Arduino musí obsahovať sekciu *setup()*. Táto funkcia definuje počiatočný stav programu pri štarte a spustí sa iba raz. Vo funkcií *setup()* sú definované nasledovné stavy a procesy:

- Funkcionalita pinov na doske (pinMode)
- Počiatočný stav pinov na doske
- Inicializácia tried
- Inicializácia premenných

Druhá nevyhnutná sekcia programu je sekcia *loop()*. Táto sekcia vojde do réžie v momente skončenia sekcie *setup()*. Sekcia *loop()* beží v nekonečnej slučke a odohráva sa v nej hlavná logika programu. Skončí len v prípade vypnutia alebo reštartovania a to na úrovni softvérovej alebo hardvérovej. [23]

6 PRÍSTUPOVÝ SYSTÉM

Prístupový systém, tiež známy ako systém kontroly prístupu, slúži na reguláciu a riadenie vstupu na fyzické miesta alebo digitálne priestory. Primárnym účelom prístupového systému je zabezpečiť, aby bol prístup povolený iba oprávneným jednotlivcom alebo subjektom, a neoprávnenému vstupu zabrániť. Existujú dva typy riadenia prístupu: fyzické a logické. Riadenie fyzického prístupu obmedzuje prístup do areálov, budov, alebo miestností. Logická kontrola prístupu obmedzuje pripojenia k počítačovým sieťam a digitálnym súborom či údajom. Na reguláciu a monitorovanie prístupu využíva kombináciu elektronických zámkov, prístupových kariet, biometrických čítačiek, čítačiek kariet a ovládacích panelov prístupu. Oprávneným osobám je povolený vstup na základe ich autentifikačných a identifikačných prostriedkov ako sú napríklad čipové karty, PIN kódy, biometrické snímky, heslá alebo ich kombinácie. [25]

6.1 Autentifikácia

V prístupových systémoch je autentifikácia proces overovania identity jednotlivcov alebo subjektov, ktorí vyžadujú prístup do fyzických priestorov, digitálnych systémov alebo k digitálnym zdrojom. Je to základný krok v kontrole prístupu, ktorý má zabezpečiť, aby bol povolený vstup len oprávneným osobám alebo subjektom. Autentifikácia môže prebiehať niekoľkými spôsobmi. [25]

6.1.1 Autentifikácia heslom

Autentifikácia založená princípe znalostí. Je to metóda overenia identity používateľa spoliehaním sa na informácie, ktoré pozná. Je často používaná ale má bezpečnostné riziká ako sú slabé heslá alebo zraniteľnosť voči útokom hrubou silou. Táto zraniteľnosť sa dá zmierniť presadzovaním zásad silných hesiel alebo kombináciou s ďalšou metódou autentifikácie. [25]

6.1.2 Autentifikácia predmetom

Autentifikácia založená na vlastníctve je metóda overenia identity používateľa prostredníctvom niečoho, čo vlastní. To môžu byť napríklad prístupové karty, kľúčenky, hardvérové tokeny alebo mobilné zariadenia s digitálnymi certifikátmi. Autentifikácia založená na vlastníctve poskytuje ďalšiu úroveň zabezpečenia, pretože vyžaduje od jednotlivca aby fyzicky vlastnil autorizovanú položku. V súčasnosti patria

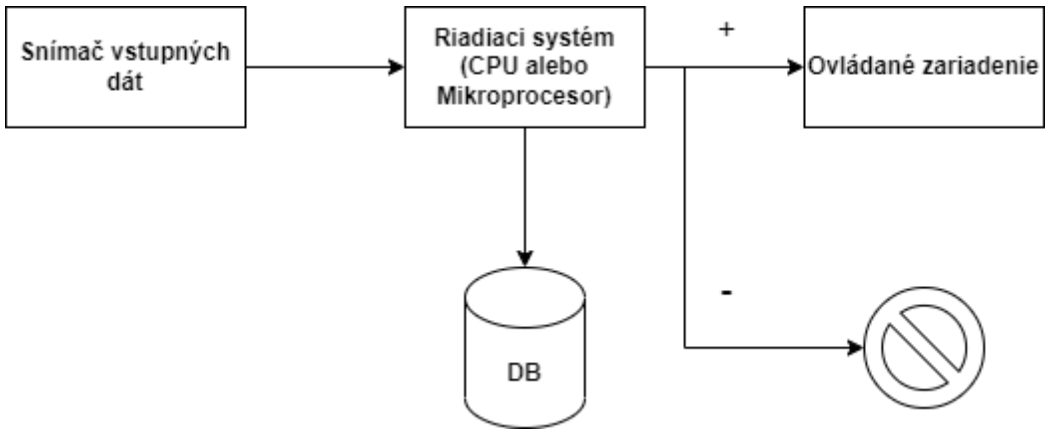
k najpoužívanejším predmetom tejto autentifikácie bezkontaktné čipové karty, založené na technológií RFID. Okrem klasickej formy v podobe plastovej karty môžu byť zabudované do rôznych predmetov ako sú sklenené tyčinky, prívesky na kľúče alebo plastové disky. [25]

6.1.3 Biometrická autentifikácia

Biometrická autentifikácia je metóda overovania identity osoby na základe jej unikátnych fyziologických vlastností. Zahŕňa zachytávanie a analýzu biometrických údajov, ako sú odtlačky prstov, vzory dúhovky, črty tváre, hlas alebo žilové riečisko na ruke. Získané biometrické údaje sa porovnávajú s uloženými šablónami biometrie jednotlivca. Ide o vysoko bezpečnú a spoľahlivú formu identifikácie, ktorú je ťažké sfalšovať alebo replikovať. Biometrická autentifikácia eliminuje potrebu hesiel alebo fyzických tokenov avšak potrebný výkon systému pre matematickú analýzu biometrie sa premieta do vyšších obstarávacích nákladov. [25]

6.2 Princíp

Princíp prístupového systému spočíva v procese overenia vstupných dát, poskytnutých užívateľom, na základe ktorého následne dôjde k odpovedajúcej akcií. Na základe analýzy a porovnania vstupných dát s údajmi v databáze, systém urobí rozhodnutie podľa ktorého buď udelí alebo zamietne prístup. Ak je prístup povolený, systém vyšle signál pripojenému podsystému. Takýmto podsystémom môže byť napríklad servo mechanizmu pre ovládanie mechanickej zábrany. Počas celého procesu sa môžu zaznamenávať relevantné dáta na účely monitorovania pohybu osôb cez prístupové body v reálnom čase alebo pre účely auditu v dátach histórie. [25]



Obrázok 10. Diagram prístupového systému

II. PRAKTICKÁ ČASŤ

7 MODEL PRÍSTUPOVÉHO SYSTÉMU

Súčasťou tejto bakalárskej práce je vytvorenie modelovej verzie prístupového systému, ktorý je zameraný na autentifikáciu predmetom. Tento model sa špecificky zameriava na bezkontaktné čipové karty Mifare od spoločnosti NXP. Riadiacou jednotkou modelu je platforma Arduino s pripojenou bezkontaktnou čítačkou NFC. Užívateľské rozhranie tvorí maticová klávesnica a jednoduchý LCD displej. V tejto kapitole sú popísané konkrétne komponenty použité pre zostavenie modelu, ako aj ich konfigurácia a výsledné zapojenie.

7.1 Použité komponenty

Hlavnú funkciu prístupového systému tvorí riadiaca jednotka a čítačka bezkontaktných kariet. V prípade tohto modelu je to Arduino UNO a čítačka PN532. Čítačka je vstupom do systému, ktorý získava potrebné dáta z čipových kariet a posiela ich ďalej na spracovanie do programovej časti. Model je doplnený o dvojriadkový LCD displej a maticovú klávesnicu so 16 tlačidlami. Všetky komponenty sú pomerne ľahko dostupné a ich obstarávacia cena nepredstavuje zásadné obmedzenia. Nasledujúca tabuľka predstavuje zoznam všetkých použitých komponentov a ich orientačný cenový rozpis.

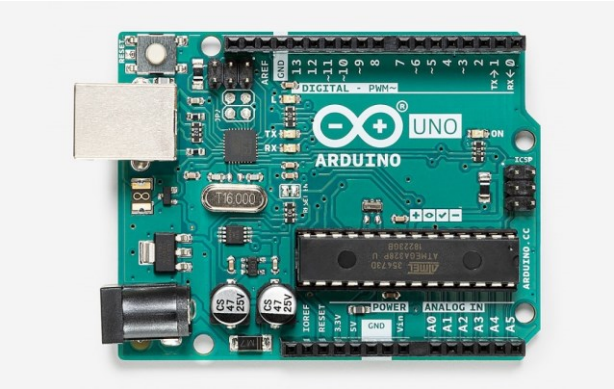
Tabuľka 1. Zoznam komponentov

Komponent	Počet kusov	Cena (EUR)
Arduino UNO R3	1	27.95
PN532	1	9.80
Klávesnica 4×4 AVR	1	1.50
LED display 16×2 s I2C	1	4.60
PCF8574 expandér I2C	1	2.30
LED dióda	2	0.06
Kontaktné pole	1	2.00
Sada káblov na prepoj	2	3.00
Výsledná cena: 54, 27 eur		

7.1.1 Arduino UNO

Riadiacou jednotkou modelu je Arduino UNO s mikrokontrolérom ATmega328P. Arduino je napájané cez USB port pripojením k počítaču alebo z 9V batérie. Doska tiež poskytuje 5V

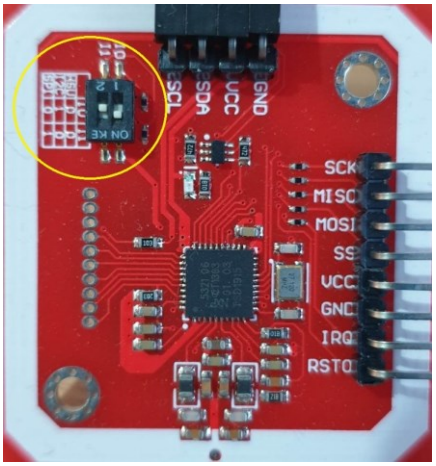
alebo 3,3V napájanie pre pripojené komponenty. Všetky pripojené komponenty v tomto modely využívajú 5V logiku.



Obrázok 11. Arduino UNO R3

7.1.2 Čítačka PN532

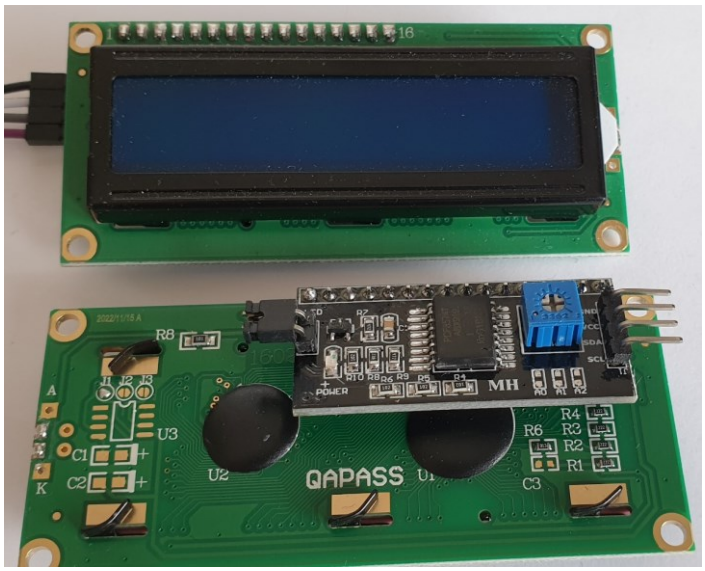
Bezkontaktné čítanie z kariet zabezpečuje NFC čítačka s označením PN532. Čítačka disponuje troma rôznymi spôsobmi komunikácie. Je možné použiť zbernicu SPI, UART alebo I2C. Pre zostavenie modelu som zvolil zbernicu I2C, pretože zaberá len 2 analógové piny na doske Arduino a ľahko sa s ňou pracuje. Pre porovnanie SPI a UART by zabrali až 6 pinov na doske. Nevýhodou I2C oproti ostatným dvom menovaným je pomalšia rýchlosť prenosu dát. V tomto modely však nepredstavuje žiaden problém a rýchlosť prenosu cez I2C je postačujúca. Nastavenie režimu komunikácie sa vykonáva pomocou kombinácie dvoch malých prepínačov vyznačených na obrázku nižšie. Tabuľka vedľa prepínača informuje o pozícií prepínačov pre každý z troch možných režimov.



Obrázok 12. PN532 a prepínač režimov komunikácie

7.1.3 LCD displej

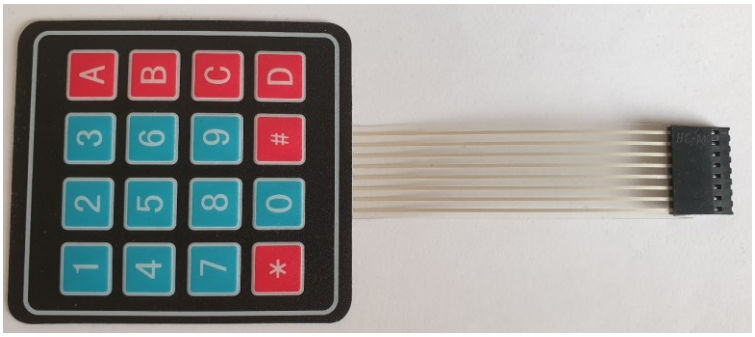
Výstupné zariadenie užívateľského rozhrania tvorí jednoduchý LCD displej. Pozostáva z dvoch riadkov a 16 stĺpcov na jeden riadok pre zobrazovanie znakov. Rovnako ako pri čítačke, aj tu som zvolil pripojenie cez zbernicu I2C. Natívny režim komunikácie takýchto zobrazovacích jednotiek je SPI. Je však možné použiť špeciálny prevodník alebo zakúpiť displej s už spájkovaným prevodníkom z SPI na I2C ako je možné vidieť na obrázku nižšie. V tomto prípade som zvolil pre rýchlosť a jednoduchosť druhú spomínanú variantu.



Obrázok 13. LCD displej s prevodníkom na I2C zbernicu

7.1.4 Klávesnica 4x4

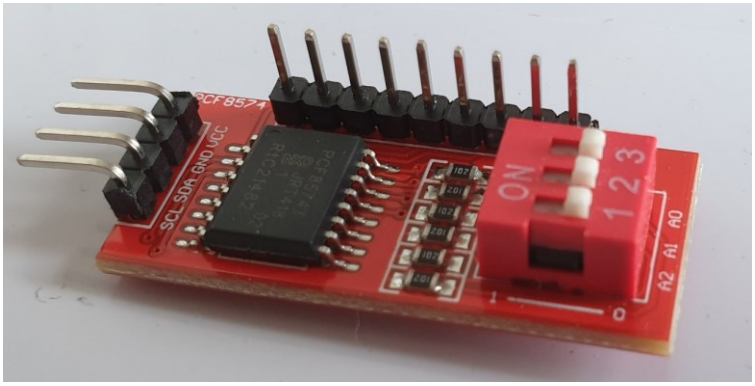
Vstupné zariadenie užívateľského rozhrania predstavuje maticová 4x4 klávesnica. Klávesnica slúži najmä pre zadávanie pin kódov a navigáciu v softvérovej časti systému. Počet pinov pre pripojenie, ktoré táto klávesnica vyžaduje, je až 8 digitálnych. Vzhľadom na skutočnosť, že Arduino model UNO má takýchto pinov len 14, bolo nutné vyhľadať alternatívne riešenie. Tým bola opäť zbernica I2C a expandér PCF8574 špecifikovaný v nasledovných riadkoch.



Obrázok 14. Maticová klávesnica 4x4

7.1.5 PCF8574

Pri hľadaní riešenia ako zredukovať počet pinov, ktoré vyžaduje maticová klávesnica, som narazil na komponent s označením PCF8574. Ten umožňuje pripojenie ôsmich pinov klávesnice do svojej dosky plošných spojov a preposielať z nich signály do Arduina cez I2C zbernicu. [26]



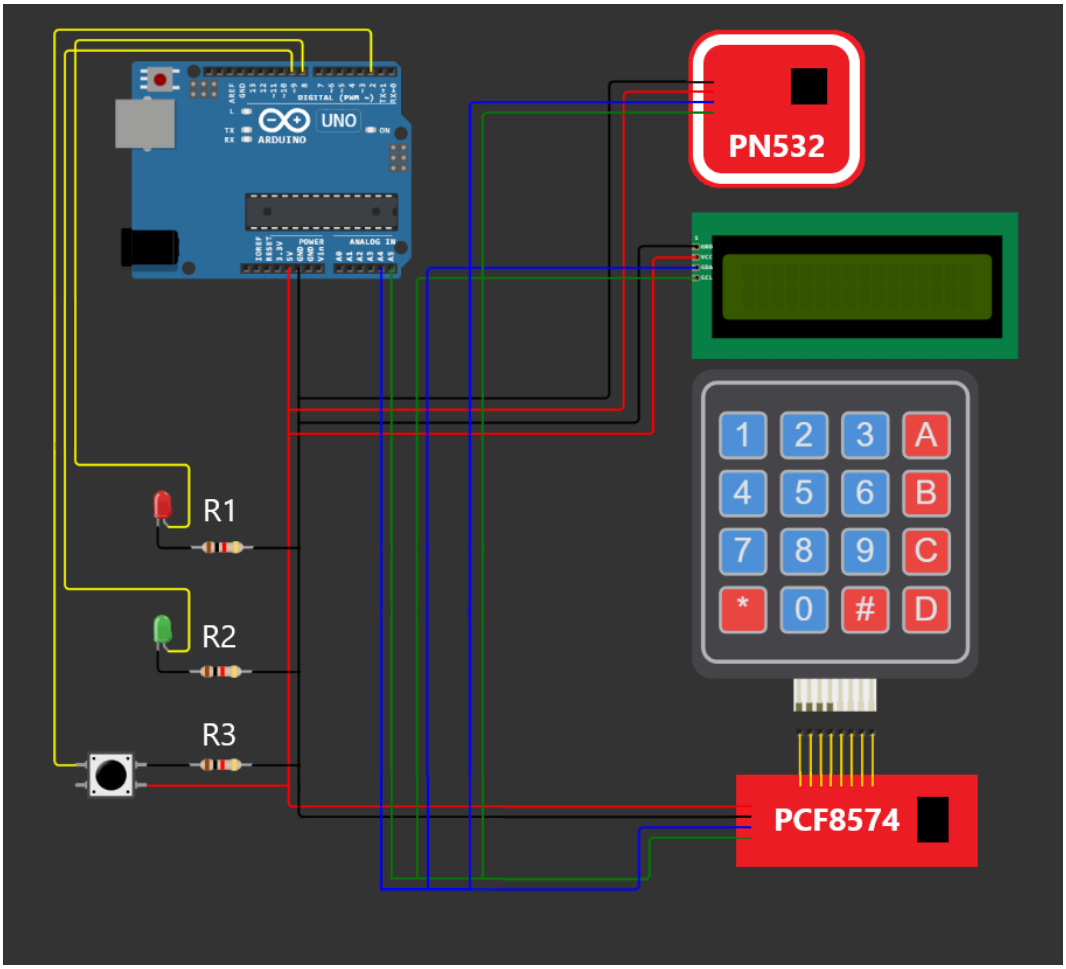
Obrázok 15. PCF8574 expandér

7.1.6 Ostatné komponenty

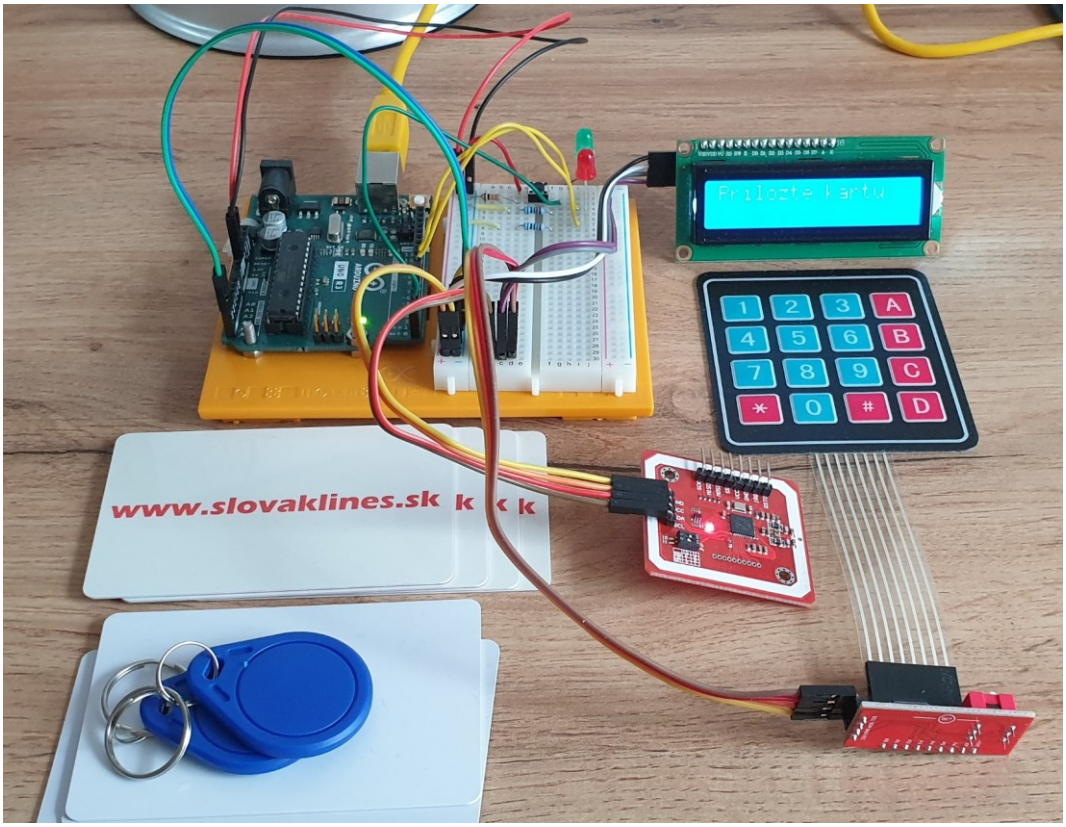
Pre zapojenie finálnej podoby modelovej verzie prístupového systému boli použité niektoré ďalšie súčasti, nevyhnutné pre konečné zapojenie. Okrem prepojovacích káblikov a kontaktného poľa, nazývaného tiež breadboard, boli použité aj LED diódy a jednoduché mechanické tlačidlo. LED diódy pre indikáciu úspešnej alebo neúspešnej autentifikácie a mechanické tlačidlo pre prepínanie medzi režimom čítania karty a režimom klávesnice.

7.2 Prepojenie komponentov

Na obrázku nižšie je grafická schéma vzájomného prepojenia všetkých komponentov. V zapojení sa nachádzajú 220 ohmové rezistory R1 a R2 a 10000 ohmový rezistor R3. Mechanické tlačidlo je zapojené na digitálny pin 2 na ktorom sa podľa dokumentácie Arduina UNO nachádza funkcia prerušenia. Vedenie vyznačené modrou a zelenou farbou znázorňuje zbernicu I2C (SCL zelená farba a SDA modrá farba). LED diódy sú prepojené na digitálne piny 8 a 9. Z týchto pinov bude prichádzať napájanie v závislosti od programovej časti modelu. Vedenie stáleho napájania je vyznačené červenou a čiernou farbou. Takto zapojená schéma predstavuje finálne vyhotovenie hardvérovej časti modelu prístupového systému.



Obrázok 16. Schéma celkového zapojenia modelu.



Obrázok 17. Zrealizované zapojenie

8 APLIKÁCIA PRE ZOSTAVENÝ MODEL

V tejto kapitole je popísaná logika programovej časti zostaveného modelu, knižnice použité pri jeho tvorbe, ako aj komplikácie s ktorými som sa v procese vývoja musel vysporiadať. V závere kapitoly je návrh laboratórnej úlohy, vychádzajúci zo zdrojového kódu programu pre model prístupového systému. Zdrojový kód programu zároveň predstavuje vzorové riešenie pre navrhnutú úlohu.

8.1 Použité knižnice

Pre ovládanie pripojených zariadení, akými sú čítačka NFC, LCD displej alebo maticová klávesnica, sú v programe použité knižnice. Knižnica je súbor špecializovaných funkcii pre špecifické účely.

8.1.1 LiquidCrystal_I2C

Knižnica pre Arduino, ktorá umožňuje komunikáciu medzi doskou Arduino a displejom LCD, prostredníctvom protokolu I2C. Poskytuje jednoduché ovládanie a zobrazovanie informácií na displeji.

8.1.2 Keypad_I2C

Obsahuje súbor funkcií pre uľahčenie procesu čítania vstupu z maticovej klávesnice. I2C v názve označuje, že táto verzia knižnice Keypad je modifikovaná pre použitie komunikačného protokolu I2C.

8.1.3 Wire

Vstavaná knižnica pre Arduino, ktorá mu umožňuje komunikovať s pripojenými zariadeniami cez zbernicu I2C. Rovnako ako predošlé knižnice zamerané na I2C protokol, poskytuje jednoduchú inicializáciu komunikačného rozhrania.

8.1.4 PN532

Knižnica určená pre Arduino, ktorá uľahčuje komunikáciu s modulom PN532 NFC. Modul PN532 umožňuje doskám Arduino interakciu s NFC tagmi, kartami a ďalšími zariadeniami s podporou NFC. Knižnica poskytuje potrebné funkcie a pomôcky pre zjednodušenie procesu čítania a zápisu údajov pomocou technológie NFC.

8.1.5 PN532_I2C

Doplňuje knižnicu PN532 o možnosť komunikácie cez protokol I2C. Je súčasťou rovnakého balíka knižníc pre čítačku NFC. Importovanie doplňujúcich balíkov pre odlišné komunikačné protokoly je voliteľné z dôvodu úspory pamäte Arduina.

8.1.6 NfcAdapter

Model systému sa zameriava na čipové karty Mifare. Táto knižnica poskytuje potrebné ovládače pre čítačku PN532, ktoré umožňujú komunikáciu s kartami Mifare Classic a Mifare Ultralight.

8.1.7 MemoryFree

Posledná z použitých knižníc slúži pre sledovanie stavu pamäte Arduina. Dôvod importovania tejto knižnice do programu zapríčinili komplikácie v závere vývoja programu. Umožňuje priebežne sledovať stav dynamickej pamäte, čo považujem za užitočné aj v prípade laboratórnej úlohy. Z toho dôvodu som sa rozhodol ponechať ju v záverečnej verzii programu.

8.2 Počiatočná konfigurácia

Pred spustením programu v slučke musí najskôr prebehnúť inicializácia všetkých objektov z použitých knižníc, inicializácia konštánt, premenných programu a nastavenia režimu pre použité digitálne a analógové piny (vstup alebo výstup). V tejto fáze sa alokuje priestor v dynamickej pamäti Arduina pre každú premennú a objekty z použitých knižníc. V modely je väčšina komponentov pripojená cez zbernicu I2C. Aby komunikácia fungovala správne, musí mať každý z nich odlišnú I2C adresu. Tá je nastavená výrobcom a každý typ komponentu má svoju vlastnú. Zistiť túto adresu je možné buď v dokumentácií komponentu alebo pomocou funkcie z knižnice Wire. Nájdenú adresu je potrebné dosadiť ako parameter do definície objektu pre príslušný komponent. Premenná *centralMode* má východziu hodnotu 0 a zastáva dôležitú funkciu v spôsobe, akým prebieha hlavná slučka programu. Ďalšie definované premenné sú polia znakov pre uloženie unikátnych identifikátorov čipových kariet Mifare.

8.3 Logika programu

Program pre zostavený model prístupového systému sa po zapnutí Arduina spustí v natívnom režime kontroly prístupu. To znamená, že čaká na priloženie čipovej karty

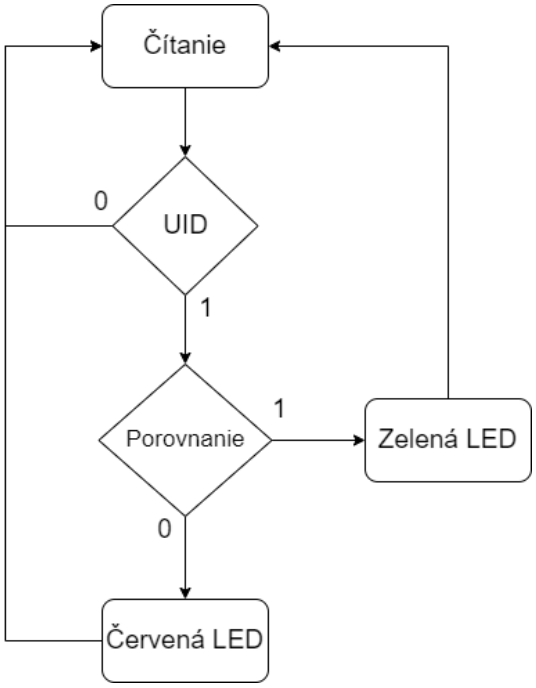
k čítačke, aby následne porovnal vyčítané UID karty s databázou a podľa výsledku porovnania rozhodol o udelení alebo zamietnutí prístupu. Rozhodnutie je interpretované prostredníctvom LED diód, kde zelená predstavuje udelenie prístupu a červená naopak zamietnutie. Okrem režimu kontroly prístupu je možné spustiť aj režim administrátora alebo režim informácie o karte. Pre zmenu z natívneho režimu do jedného z menovaných je nutné stačiť mechanické tlačidlo, ktoré následne vyšle signál pre spustenie prerušenia. Vyvolané prerušenie spôsobí, že program prestane bežať v natívnej slučke čítania karty a spustí pridruženú funkciu. Táto funkcia zmení hodnotu premennej *centralMode* na hodnotu, ktorá zodpovedá režimu čítania z maticovej klávesnice. Systém v tomto režime prestane čakať na priloženie karty k čítačke a namiesto toho zobrazí na LCD displeji ponuku možností pre ďalšiu akciu. V tomto stave program čaká na signál z maticovej klávesnice na základe ktorého opäť vykoná príslušnú zmenu režimu. Opätovným stlačením mechanického tlačidla prerušenia sa program vráti späť do režimu kontroly prístupu. V prípade, že užívateľ zvolil prostredníctvom maticovej klávesnice vstup do režimu administrátora, program zobrazí výzvu na priloženie čipovej karty. Ak je UID priloženej karty zhodné s aspoň jedným UID v databáze administrátorov, zobrazí na LCD displeji ďalšiu výzvu. Zobrazený text informuje užívateľa o nutnosti zadať k rozpoznanej karte príslušný pin kód. Ak je vstup z klávesnice vyhodnotený ako správny, užívateľ úspešne prešiel dvojfaktorovou autentifikáciou. Program teraz beží v režime s vyšším oprávnením a umožňuje spustiť funkcie pridania a odstránenia čipových kariet z databázy.

Celá logika hlavnej slučky je teda založená na globálnej premennej *centralMode,* ktorej hodnotu program kontroluje na začiatku každého cyklu. Mechanické tlačidlo prerušenia a maticová klávesnica umožňujú ovládanie systému prostredníctvom zmeny hodnoty práve tejto premennej. V nasledujúcich podkapitolách sú bližšie popísané jednotlivé režimy do ktorých môže byť program uvedený.

8.3.1 Bežný režim kontroly prístupu (0)

Základný režim po spustení cyklicky vyhľadáva prítomnosť čipovej karty v dosahu čítačky. V prípade, že sa v signálovom poli nachádza funkčná čipová karta, prebudí svoj integrovaný obvod a odošle svoje UID. Prijatý identifikátor sa uloží do premennej *rfidString* a tá je následne porovnávaná s prvkami dvojrozmerného znakového poľa *knownCards*, ktoré reprezentuje databázu užívateľov s povoleným prístupom. Ak pri niektorom z prvkov poľa nastane zhoda, program vyšle signál na výstupný pin 9, ktorý na dobu jednej sekundy poskytne napájanie pre zelenú diódu udelenia prístupu. Ak nenastala zhoda pri žiadnom

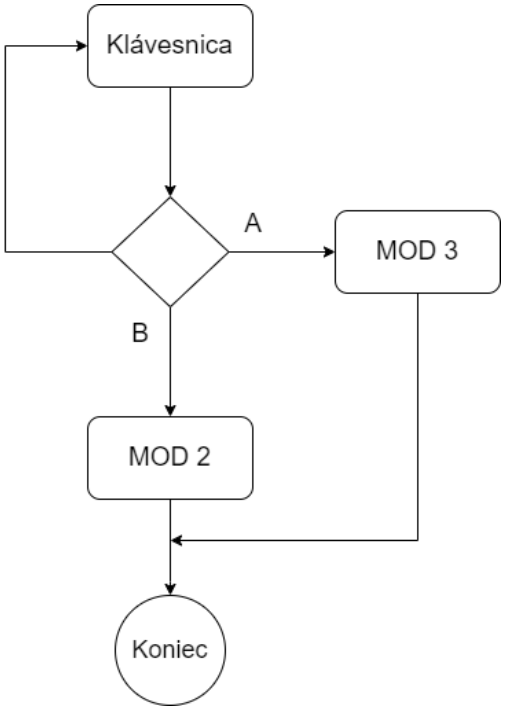
z prvkov poľa *knownCards*, signál príde na výstupný pin 8 pre červenú diódu zamietnutia prístupu. V každom z prípadov sa program na konci vráti späť do stavu čítania priložených kariet.



Obrázok 18. Bežný režim kontroly prístupu.

8.3.2 Režim čítania z maticovej klávesnice (1)

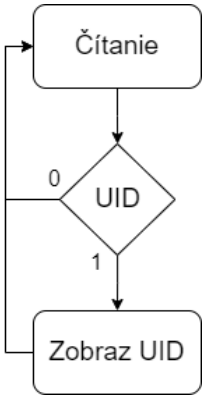
Po stlačení mechanického tlačidla prerušenia je program uvedený do režimu čítania vstupu z klávesnice. Na LCD displeji zobrazí ponuku režimov do ktorých môže používateľ program ďalej uviesť. Informácia na displeji tiež zobrazuje aký znak na maticovej klávesnici je nutné stlačiť pre žiadaný režim. Po stlačení klávesy „A“ sa nastaví hodnota premennej *centralMode* na hodnotu 3. Ak je stlačená klávesa „B“, hodnota *centralMode* bude nastavená na 4. Po nastavení tejto premennej sa slučka v tomto režime ukončí a pri novom cykle bude prebiehať v novo zvolenom režime podľa premennej *centralMode*.



Obrázok 19. Režim čítania z klávesnice

8.3.3 Režim informácie o karte (2)

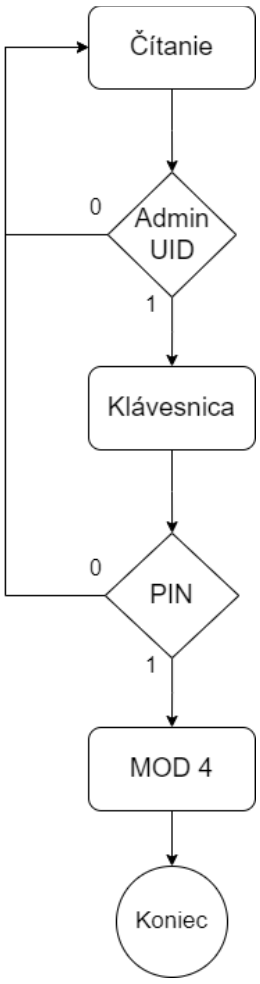
V režime informácie o karte program funguje podobne ako v režime 1. Čítanie prebieha rovnakým spôsobom a v prípade získania UID priloženej karty uloží toto číslo v hexadecimálnej podobe do premennej *rfidString.* Tieto znaky postupne posiela na LCD displej, ktorý používateľovi zobrazí identifikačné číslo priloženej karty. Ukončenie slučky v tomto režime sa vykoná stlačením mechanického tlačidla prerušenia. Prerušenie vyvolá funkciu *switchMode()* a tá vráti program do režimu bežného čítania karty.



Obrázok 20. Režim informácie o karte

8.3.4 Režim dvojfaktorovej autentifikácie (3)

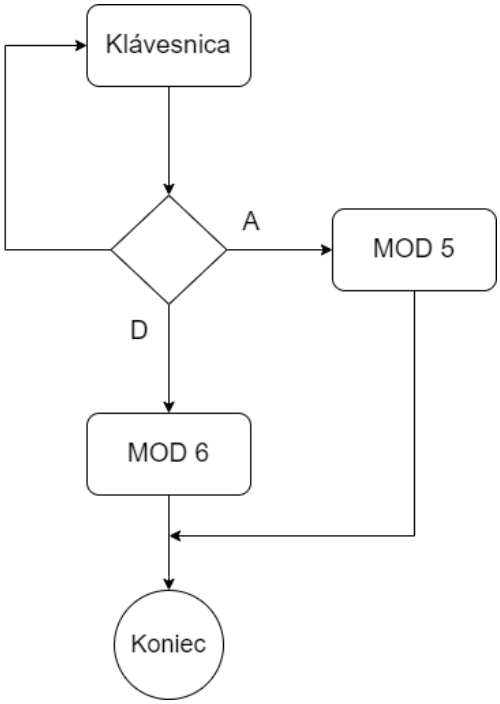
Dvojfaktorová autentifikácia nasleduje po tom ako sa používateľ rozhodol pre vstup do režimu administrátora. Pred tým, ako program sprístupní funkcie s vyšším oprávnením, musí používateľ úspešne splniť podmienky procesu v tomto režime. V úvode slučky zobrazuje LCD displej výzvu na priloženie karty s administrátorským oprávnením. Vyčítané UID priloženej kary sa uloží do premennej *rfidString*. Následne prebieha porovnávanie s prvkami poľa *adminCards* a hľadá sa zhoda. Ak sa vyčítané UID v databáze nenájde, program zobrazí hlášku s upozornením, že karta nemá oprávnenie pre vstup do tohto režimu. V opačnom prípade zobrazí výzvu pre zadanie pin kódu a čaká na vstup z klávesnice. Znaky postupne ukladá do premennej *pin*. Po stlačení štvrtého znaku v poradí sa spustí kontrola zadaného pin kódu. Tá prebieha spôsobom, že program si pamätá index pozície overenej karty administrátora v poli *adminCards* a porovnáva zadaný pin kód s pin kódom v poli *adminPinns* pod rovnakým indexom. Úspešná zhoda zmení premennú režimu na hodnotu 4 a ukončí cyklus dvojfaktorovej autentifikácie. V opačnom prípade sa vráti na jeho začiatok.



Obrázok 21. Režim 2FA

8.3.5 Režim čítania z klávesnice pre administrátora (4)

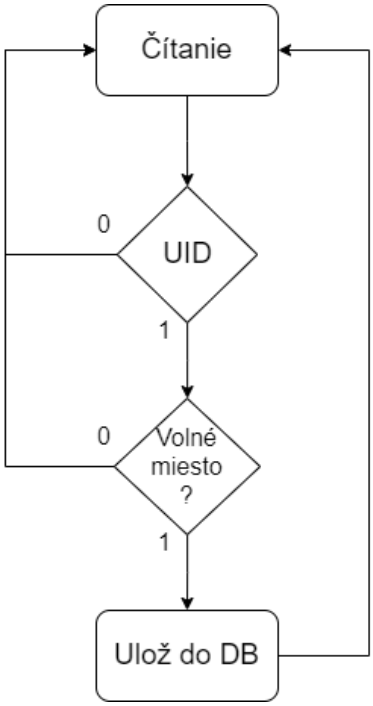
Po úspešnej verifikácií údajov administrátora systém sprístupní navigačné menu funkcie na modifikáciu databázových záznamov. LCD displej zobrazuje možnosti pridania alebo odstránenia čipovej karty s príslušným symbolom pre spustenie akcie. Klávesa „A“ uvedie program do režimu pridávania kariet do databázy, zatiaľ čo klávesa „B“ sprístupní režim odoberanie uložených kariet.



Obrázok 22. Režim klávesnice pre administrátora

8.3.6 Režim pridávania karty do databázy (5)

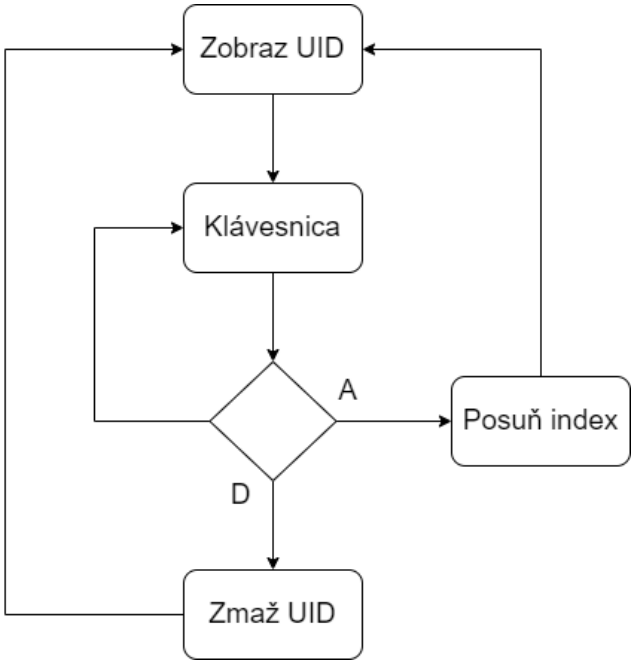
Slučka v tomto režime číta kartu a ukladá jej UID do premennej *rfidString* rovnako ako pri ostatných režimoch s čítaním. Následne prebehne overenie voľného miesta v premennej *knownCards*, reprezentujúcej databázu. Maximálny počet uložených UID je definovaný premennou *maxNumberOfUsers*. Program overí či sa na pozícii *maxNumberOfUsers – 1* nachádza nejaké UID. Ak áno, informuje prostredníctvom LCD displeja o maximálnom stave a uloženie nevykoná. V opačnom prípade uloží hodnotu z *rfidString* do prvej voľnej pozície v poli *knownCards*.



Obrázok 23. Režim pridávania karty

8.3.7 Režim odstránenia karty z databázy (6)

Na LCD displeji v prvom riadku je zobrazené UID uložené na prvej pozícií v poli *knownCards.* Druhý riadok informuje o možnostiach pre používateľa. V prípade stlačenia klávesy „A“ sa inkrementuje hodnota premennej *actualId* a program zobrazí v prvom riadku displeja UID z nasledovnej pozície v poli *knownCards.* Klávesa „D“ spôsobí odstránenie zobrazeného UID a to takým spôsobom, že vynuluje záznam na pozícií *actualId* v poli *knownCards*. Následne popresúva všetky nasledujúce položky o jednu pozíciu nižšie. Na LCD displeji sa zobrazí v prvom riadku ďalšie UID, ktoré zabralo pozíciu *actualId* po predošlom prvku.



Obrázok 24. Režim odstránenia karty

8.4 Limitácie modelu Arduino UNO

Vývoj programu sa nezaobišiel bez vzniknutých komplikácií. Súčasťou modelu prístupového systému mala byť pôvodne aj perzistentná databáza uložená na SD karte a história udelených prístupov. Výzvou bola už hardvérová časť implementácie perzistentnej databázy, ktorá si vyžadovala pripojenie modulu pre SD kartu. Tento modul je možné zapojiť len použitím zbernice SPI a tá potrebuje až 6 digitálnych pinov. V čase riešenia tohto problému mala verzia fyzického zapojenia obsadených 8 pinov maticovou klávesnicou, 2 piny obsadené LED diódami a 1 pin funkciou prerušenia. To je 11 obsadených digitálnych pinov a zostávali voľné už len 3. Najväčšie obmedzenie predstavovala maticová klávesnica, na ktorú som sa zameral pri hľadaní riešenia vzniknutej situácie. Riešenie sa nájsť úspešne podarilo a bola ním súčiastka PCF8574, ktorá umožnila pripojenie maticovej klávesnice na zbernicu I2C, čím sa uvoľnilo všetkých 8 digitálnych pinov. I2C zbernica využíva analógové piny 4 a 5. Následne vznikol priestor pre zbernicu SPI a pripojenie modulu pre SD kartu. Výsledné zapojenie sa javilo pri jednoduchom teste zápisu a čítania z SD karty ako funkčné. Po implementácii do zdrojového kódu programu pre prístupový systém, začalo byť jeho správanie nepredvídateľné a nezodpovedalo stavu pred pridaním funkcií pre prácu s SD kartou. Vyhľadávanie otázok a riešení s podobnou situáciou na známych fórach ma naviedlo na možnú príčinu. Arduino IDE informuje o spotrebe statickej a dynamickej pamäte pri

nahrávaní programu do Arduina. Spotreba dynamickej pamäte dosiahla úroveň 97% a voľných tak zostalo len niekoľko desiatok bajtov. 97 % spotrebovali importované knižnice a globálne premenné, ako sú napríklad polia pre ukladanie UID kariet. Keď sa program spustil a začal pracovať s dátami lokálnych premenných, takmer okamžite došlo k maximálnemu využitiu pamäte, čo malo za následok jeho nepredvídateľné správanie. Po postupnej analýze som zistil, že knižnica pre prácu s SD kartou spotrebuje približne 30% z celkovej dynamickej pamäte Arduina UNO. Alternatívna knižnica sdFat má približne rovnaké nároky na dynamickú pamäť. Vzhľadom na skutočnosť, že ostatné použité knižnice zohrávajú dôležitú rolu pri kľúčových funkciách zostaveného modelu, nebolo možné žiadnu z nich vynechať a uvoľniť tak miesto pre knižnicu SD. Perzistentná databáza tak musela byť z finálnej verzie prístupového systému vynechaná. Výsledkom tejto práce je teda aj zistenie, že prístupový systém v tejto podobe, doplnený o databázu, predstavuje príliš komplexné riešenie, ktoré presiahlo možnosti Arduina, konkrétne modelu UNO.

8.5 Laboratórna úloha

Záverečnou časťou tejto bakalárskej práce je návrh laboratórnej úlohy k zostavenému modelu prístupového systému. Účelom tejto úlohy je praktické precvičenie znalostí zo základov programovania v spojení s pochopením základného princípu na ktorom pracujú zabezpečovacie prístupové systémy a technológia NFC. Úloha je rozdelená na dielčie pod-úlohy, ako je napríklad doplnenie kódu do funkcie pre rozsvietenie LED diód alebo uloženie identifikačného čísla prístupovej karty do databázy.

```
if (centralMode == 5){
  int freePosition = numOfUsers();
  if (freePosition < maxNumberOfUsers) {
    strcpy(knownCards[freePosition], rfidString);
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Karta pridana");
    delay(2000);
  } else {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Maximalny pocet");
    lcd.setCursor(0, 1);
    lcd.print("ulozenych kariet");
  }
}
```

```
// DOPLN KOD TAK ABY PRIDAL UID PRECITANEJ KARTY DO DATABAZY
// ALEBO VYPISAL NA LCD DISPLEJ IFNORMACIU O PLNEJ DATABAZE
// *DATABAZA JE PREMENNA knownCards[][]
if (centralMode == 5){
  int freePosition = numOfUsers();
  if (freePosition < maxNumberOfUsers) {

    // PRIDAJ UID DO DATABAZY

  } else {

    // INFORMUJ NA LCD DISPLEJ ZE DATABAZA JE PLNA

  }
}
```

Obrázok 25. Ukážka časti laboratórnej úlohy a vzorového riešenia

Príloha k tejto bakalárskej práci obsahuje dve verzie programu. Verzia pre laboratórnu úlohu obsahuje prázdne časti v kóde s inštrukciami k doplneniu. Úplná verzia programu je

hlavným výstupom tejto práce a zároveň ponúka vzorové riešenia jednotlivých častí laboratórnej úlohy.

ZÁVER

Cieľom tejto bakalárskej práce bolo zostavenie modelu zabezpečovacieho prístupového systému s technológiou NFC. Tento cieľ sa splniť podarilo a výsledkom je funkčné softvérové aj hardvérové riešenie. Model má slúžiť ako laboratórna pomôcka a jeho účelom je demonštrácia princípov, na ktorých sú tieto systémy postavené. Poskytuje náhľad do spôsobu programovania prístupových systémov, ako aj do možnosti vzájomného prepojenia a komunikácie jednotlivých komponentov systému medzi sebou. Obstarávacia cena súčastí pre zostavenie modelu je približne 55 eur. Vďaka tejto cenovej dostupnosti predstavuje riešenie vhodné pre experimentovanie a testovanie rôznych konfigurácii. Nijak sa tým však nevylučuje ani možnosť využiť model ako základ pre skutočný prístupový systém.

Základ vyhotoveného modelu tvorí Arduino UNO a čítačka NFC. Spolu poskytujú základnú funkcionalitu modelu, ktorou je kontrola prístupu. Maticová klávesnica a LCD displej tvoria používateľské rozhranie, ktoré poskytuje systému ďalšie možnosti. Jednou z nich je dvojfaktorová autentifikácia za účasti čipovej karty a pin kódu. Tá poskytuje prístup k ďalším funkciám s vyšším oprávnením, ako sú pridávanie alebo odoberanie čipových kariet z databázy systému. Zamýšľanou súčasťou bola pôvodne aj perzistentná databáza kariet na SD karte. Túto časť sa podarilo čiastočne zrealizovať, avšak postupne som narazil na limity Arduina UNO. Prístupový systém s vlastnou perzistentnou databázou predstavuje pre Arduino UNO prílišnú komplexnosť a pre nedostatok dynamickej pamäte musela byť v závere perzistentná databáza z modelu vynechaná. Možným riešením v takomto prípade je prechod na výkonnejší model Arduino MEGA so štvornásobnou kapacitou dynamickej pamäte.

Záverečnou časťou práce bolo navrhnúť laboratórnu úlohu pre zostavený model. Navrhnutá úloha spočíva v doplnení chýbajúcich častí zdrojového kódu v pripravenom súbore. Ten vychádza z hlavného programu pre model systému, ktorý predstavuje jeho vzorové riešenie. Cieľom úlohy je uviesť model do funkčného stavu. Vyriešenie úlohy vyžaduje základné znalosti programovania a pochopenia princípu, na ktorom funguje prístupový systém.

ZOZNAM POUŽITEJ LITERATÚRY

[1] ROBERTI, Mark. The History of RFID Technology. *RFID journal* [online]. 16 Jan 2005 [cit. 2023-03-04]. Dostupné z: https://www.rfidjournal.com/the-history-of-rfid-technology

[2] MICHAEL FARADAY OBJAVITEĽ ELEKTROMAGNETICKEJ INDUKCIE. *Elektrolab.eu* [online]. [cit. 2023-03-04]. Dostupné z: https://www.elektrolab.eu/blog/michael-faraday-objavitel-elektromagnetickej-indukcie

[3] What is RFID? | The Beginner's Guide to How RFID Systems Work. *Atlasrfidstore* [online]. [cit. 2023-03-04]. Dostupné z: https://www.atlasrfidstore.com/rfid-beginners-guide/?utm_source=Quick-Start&utm_medium=Link&utm_campaign=Content&utm_content=What-is-RFID

[4] The History of NFC. *Tragging* [online]. [cit. 2023-03-07]. Dostupné z: https://tragging.com/blog/the-history-of-nfc/

[5] THRASHER, James. RFID versus NFC: What's the difference between NFC and RFID?. *Atlasrfidstore* [online]. [cit. 2023-03-07]. Dostupné z: https://www.atlasrfidstore.com/rfid-insider/rfid-vs-nfc/

[6] TARDI, Carla. Near Field Communication (NFC) Definition. *Investopedia* [online]. 13 Dec 2022 [cit. 2023-03-07]. Dostupné z: https://www.investopedia.com/terms/n/near-field-communication-nfc.asp

[7] Operating Modes. *NFC Forum* [online]. [cit. 2023-03-07]. Dostupné z: https://nfc-forum.org/learn/nfc-technology/

[8] Near Field Communication (NFC) Explained: Working and Applications. *Utmel* [online]. 24 Maj 2021 [cit. 2023-03-07]. Dostupné z: https://www.utmel.com/blog/categories/rf/near-field-communication-nfc-explained-working-and-applications

[9] WANKHEDE, Calvin. How do NFC tags and readers work? Here's everything you need to know. *Android Authority* [online]. 17 Maj 2023 [cit. 2023-04-02]. Dostupné z: https://www.androidauthority.com/nfc-tags-explained-271872/

[10] Tags. *NFC Forum* [online]. [cit. 2023-03-07]. Dostupné z: https://nfc-forum.org/learn/nfc-technology/

[11] How Does NFC Work?. *Blue Bite* [online]. 17 Maj 2023 [cit. 2023-05-21]. Dostupné z: https://www.bluebite.com/nfc/how-does-nfc-work

[12] *The MIFARE Classic story* [online]. 2010. [cit. 2023-06-04]. ISSN 1363-4127.

[13] RANKL, W. *Smart card handbook*. 4th ed. Chichester, West Sussex, U.K.: Wiley, 2010. ISBN 978-0-470-74367-6.

[14] NFC Forum Type Tags: White Paper V1.0. *NFC Forum* [online]. 1 April 2009 [cit. 2023-05-04]. Dostupné z: https://members.nfc-forum.org/resources/white_papers/NXP_BV_Type_Tags_White_Paper-Apr_09.pdf

[15] MF1S50YYX_V1: MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development. *NXP* [online]. 23 Maj 2018 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf

[16] MF1P(H)x2: MIFARE Plus EV2. *NXP* [online]. 9 Aug 2021 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF1P(H)x2_SDS.pdf

[17] MF3D(H)x3: MIFARE DESFire EV3 contactless multi-application IC. *NXP* [online]. 15 Maj 2020 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF3DHx3_SDS.pdf

[18] MF4SAM3: MIFARE SAM AV3 secure access module. *NXP* [online]. 2 Aug 2019 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF4SAM3_SDS.pdf?pspll=1

[19] MF0ULX1: MIFARE Ultralight EV1 - Contactless ticket IC. *NXP* [online]. 9 Apr 2019 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF0ULX1.pdf

[20] MF0ICU2: MIFARE Ultralight C - Contactless ticket IC. *NXP* [online]. 30 Jul 2019 [cit. 2023-05-04]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF0ICU2.pdf

[21] MINIHOLD, Roland. *NFC Technology and Measurements: White Paper: White Paper* [online]. Jun 2011 [cit. 2023-05-04]. Dostupné z: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5E_NFC_WHITE_PAPER.pdf

[22] ISO/IEC 14443. *ISO* [online]. [cit. 2023-05-15]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-4:ed-3:v1:en

[23] VODA, Zbyšek. *Průvodce světem Arduina*. Vydání druhé. Bučovice: Martin Stříž, 2017. ISBN isbn978-80-87106-93-8.

[24] PINKER, Jiří. *Mikroprocesory a mikropočítače*. Praha: BEN - technická literatura, 2004. ISBN isbn80-7300-110-1.

[25] KOLAJA, M. *Využití přístupových systémů v průmyslu komerční bezpečnosti*. Zlín, 2006. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky.

[26] A Keypad + LCD with only 2 Pins?! No problem with the I2C Protocol!. *Brainy Bits* [online]. 25 Okt 2020 [cit. 2023-05-31]. Dostupné z: https://www.brainy-bits.com/post/a-keypad-lcd-with-only-2-pins-no-problem-with-the-i2c-protocol

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

RFID Radio Frequency Identification

NFC Near Field Communication

LCD Liquid Crystal Display

LF Low Frequency

HF Hight Frequency

UHF Ultra High Frequency

POS Point Of Sale

ISO International Organization for Standardization

IEC International Electrotechnical Commission

PICC Proximity Integrated Circuit Card

PCD Proximity Coupling Device

I/O Input/Output

PWM Pulse width modulation

IDE Integrated Development Environment

SPI Serial Peripheral Interface

I2C Inter-Integrated Circuit

UART Universal asynchronous receiver-transmitter

LED Light emitting diode

SCL Serial Clock

SDA Serial Data

2FA Two factor authentication

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: OBSAH PRILOŽENÉHO USB KĽÚČA

accessSystemNFC_final.ino

accessSystemNFC_labtask.ino

fulltext.pdf