Zabezpečení RFID tagů užívaných pro osobní identifikaci

Tomáš Stračinský

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš Stračinský**
Osobní číslo:	**A12167**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení RFID tagů užívaných pro osobní identifikaci**
Téma anglicky:	**Ensuring the Security of RFID Tags Used for Personal Identification**

Zásady pro vypracování:

1. **Prostudujte stávající RFID technologie používané pro osobní identifikaci a technologie vestavěné v běžných předmětech, např. platební karty, občanské průkazy a jiné.**
2. **Sestavte přehled dostupných RFID technologií použitelných pro osobní identifikaci.**
3. **U vybraných technologií uveďte úroveň a popis jejich zabezpečení.**
4. **Vytvořte přehled známých úspěšných útoků na tyto techlogie a popište, na které útoky jsou které technologie již zabezpečeny.**
5. **Sestavte porovnání vybraných tagů dle vhodně zvolených kritérií se zaměřením na jejich zabezpečení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **THORNTON, Frank. RFID Security. Rockland, MA: Syngress Publishing, 2006, 242 s. ISBN 1-59749-047-4. Dostupné také z: http://www.sciencedirect.com/science/book/9781597490474**
2. **GLOVER, Bill a Himamsu. BHATTA. RFID essentials. Sebastopol, CA: O'Reilly, 2006. ISBN 0596009445.**
3. **FIALOVÁ, Eva. Bezkontaktní čipy a ochrana soukromí. Praha: Leges, 2016. Praktik (Leges). ISBN 978-80-7502-150-2.**
4. **DOBKIN, Daniel Mark. The RF in RFID: UHF RFID in practice. Second edition. /. Amsterdam: Elsevier/Newnes, 2013, ix, 529 pages. ISBN 9780123945839.**
5. **SOMMEROVÁ, Martina. Základy RFID technologií. In: RFID všb Ostrava [online]. 2013 [cit. 2013-01-18]. Dostupné z: http://rfid.vsb.cz/miranda2/export/sites-root/rfid/cs/okruhy/informace/RFID_pro_Logistickou_akademii.pdf**

Vedoucí bakalářské práce: **Ing. Peter Janků**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **29. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně .....

podpis diplomanta

ABSTRAKT

Tato bakalářská práce se zabývá bezpečností RFID technologií používaných pro identifikaci osob. V práci je uveden nejprve krátký úvod do problematiky RFID technologie, včetně krátkého popisu funkce a rozdělení RFID čipů. Dále jsou popsány používané RFID technologie. Teoretická část práce je zakončena popisem zabezpečení dokladů pro identifikaci člověka.

Praktická část se zabývá přehledem možných útoků na RFID technologie. Dále zabezpečením vybraných RFID karet. Zakončena je hodnocením bezpečnosti jednotlivých RFID technologií.

Klíčová slova: RFID technologie, RFID čip, zabezpečení, kryptografie

ABSTRACT

This bachelor thesis deals with the security of RFID technologies used for personal identification. The paper presents a brief introduction to the issue of RFID technology, including a brief description of RFID functions and distribution of RFID chips. Below is the description of used RFID technologies. The theoretical part of the thesis ends with a description of security of ID's.

The practical part deals with an overview of possible attacks on RFID technology. Next, by security of selected RFID cards. Finally, it ends with an evaluation of the security of RFID technology.

Keywords: RFID technology, RFID tag, security, cryptography

Poděkování

Rád bych poděkoval mému vedoucímu bakalářské práce, panu ing. Peter Janků, za odborné vedení a vstřícnost. Dále bych chtěl poděkovat svému rodinnému okolí, svým blízkým přátelům, ale i mému pracovnímu kolektivu za podporu ve studiu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Smyslem této bakalářské práce je představení problematiky bezpečnosti RFID technologie (Radio Frequency Identification – radiofrekvenční identifikace) se zaměřením na identifikaci osob.

V dnešní době je každodenní potřebou identifikace osob, zvířat, nebo výrobků. Tuto lze provést několika způsoby. Například předložením dokumentu, ve tvaru plastové karty, sloužícího k ověření totožnosti (občanský průkaz, cestovní pas, řidičský průkaz) nebo s využitím dokladu, který je možné elektronicky číst (číselný kód, čárový kód, magnetický proužek, RFID tag). Tato práce se zaměřuje právě na elektronický způsob identifikace pomocí RFID. Tato technologie je v současnosti stále více využívána a dá se počítat s expanzí této technologie i do dalších oblastí normálního života.

V České republice s k identifikaci osob primárně používá občanský průkaz ve tvaru plastové karty, bez elektronického čipu, s ochranami proti falzifikaci. Bohužel s vývojem technologií je stále jednodušší vyrobit zdařilý falzifikát, a proto je nutné zavést bezpečnější ochrany proti kopírování. Tohoto může být docíleno například použitím zabezpečeného RFID čipu. Do budoucna lze však počítat s vývojem technologií, které opět dokážou překonat dnes nepřekonatelné ochrany. Díky časovému omezení dokladů, se tomuto dá částečně bránit.

I. TEORETICKÁ ČÁST

1 TECHNOLOGIE RFID

V mnoha zemích se v současnosti pro identifikaci osob používá forma fyzického dokumentu. Většinou se jedná o plastovou nebo papírovou kartičku, popřípadě o klasickou papírovou knížku. Tyto formáty identifikačního dokumentu jsou samozřejmě chráněny proti falzifikaci, avšak tyto dokumenty lze snadno falzifikovat. Technologie RFID umožňuje mnohem rychlejší a bezpečnější proces identifikace. Identifikační data můžou být uložena do paměti RFID čipu, kde zůstávají chráněna pomocí různých šifrovacích metod. V ideálním případě pak není možné tento identifikátor falzifikovat a zneužít.

1.1 Historie RFID

Identifikační systém letadel používaný během druhé světové války, je považován za počátek využívání RFID technologie. Jde o systém IFF (Identification Friend or Foe - identifikace přítel nebo nepřítel). Tento systém řešil problém s rozlišováním přátelských a nepřátelských letounů, což RADAR (Radio Detection And Ranging – Rádiová detekce a měření) nedokázal. Princip fungování systému spočíval v tom, že vysílač vyslal dotaz, který byl po přijmutí letadlem zpracován a poté vyslal signál zpět. Signál mohl být posílán pasivním nebo aktivním způsobem. U pasivního sytému dochází k úpravě původního signálu, tak aby odražený signál obsahoval požadovanou informaci. Tento princip je dnes nejvíce rozšířeným způsobem identifikace pomocí RFID. Na druhou stranu aktivní systém nejdříve přijme signál a poté na něj odpoví vysílač instalovaný v letadle. [1]

V šedesátých letech 20. století začaly obchodní společnosti vyvíjet systém pro ochranu zboží, který používal radiové vlny. Tento systém sloužil k rozpoznání, jestli bylo za výrobek zaplaceno nebo ne. K tomuto využívá 1bitový RFID čip, který má pouze dvě hodnoty (zapnuto, vypnuto). Defaultně je čip nastaven v poloze zapnuto. Po zaplacení, je pak čip přepnut do polohy vypnuto a osoba může opustit obchod. Pokud však zákazník za zboží nezaplatí, čip zůstává v poloze zapnuto. Při pokusu o krádež zboží, pak reaguje brána za pokladnou a vyvolá poplach. [1]

V roce 1973 obdržel Charles Walton patent pro pasivní transpondér, který použil k otevření dveří bez použití klíče. Karta se zapuštěným transpondérem komunikovala se čtečkou ve dveřích. Poté co čtečka rozpoznala validní číslo karty, odemknula dveře.

V 70. letech došlo k vývoji identifikačního systému pro potřeby kontroly pohybu radioaktivních materiálů. Tento aktivní systém se skládal z RFID čtečky umístěné v bráně a transpondéru umístěného ve vozidle. Když poté kamion projel branou, došlo k přenosu radiového signálu do transpondéru. Ten zpět vyslal informace o převáženém materiálu o konkrétním kamionu a popřípadě uložené ID číslo řidiče. Princip těchto bran se dnes využívá po celém světě jako tzv. mýtné brány. [1]

V 80. letech byl na žádost zemědělců vyvinut systém identifikace zvířat. Tento sytém již plně využíval princip pasivního RFID systému. [1]

Od 90. let byl vyvíjen RFID čip pro monitorování pohybu zboží po celém světě, zavedením EPC (Electronic Product Code – elektronický produktový kód). Tímto čipem v kombinaci se standardním čárovým kódem, byly postupně označovány výrobky. Toto umožnilo jejich automatické sledování na cestě ke spotřebiteli. Z důvodu požadavku co nenižší ceny, obsahoval RFID čip zprvu pouze produktové číslo výrobku. Postupem času vlivem vývoje technologie došlo ke zlevnění výroby čipů a bylo tak možné tyto čipy vybavit větší pamětí. Tento systém pak v dnešní době přináší možnost sledovat pohyb mezinárodní zásilky na cestě k odběrateli. [2]

1.2 Význam použití technologie RFID

Díky technologii RFID je identifikace věcí a osob mnohem rychlejší a bezpečnější. Bohužel starší typy RFID technologie již byly překonány a nejsou tedy bezpečné. Při využití RFID technologie například v obchodu, není kladen takový důraz na bezpečnost a je proto možné použít i tyto technologie. Pokud ale budeme mluvit například o identifikaci osob, měla by být používána technologie, u které je kladen maximální důraz na bezpečnost a spolehlivost. Pokud by se měl například občanský průkaz nahradit RFID tagem, je nutné tuto technologie zabezpečit tak, aby nebylo možné vytvořit padělek, či neoprávněně použít doklad jinou osobou. [6]

Jedna z futuristických představ je implementace RFID čipu pod kůži člověka. Obdobně jako jsou označována zvířata, kdy je RFID ve skleněné kapsli zavedeno pod kůži, je možné označit i osoby. V případě existence takové RFID identifikace, je potřeba nejen zabezpečit čip proti různým druhům radiových útoků a kopírování obsahu, ale také je třeba myslet na to, že čip lze z osoby vyjmout a vložit do jiné osoby. Z tohoto důvodu je potřeba RFID čip

doplnit o další informace. Příkladem může být například fotografie držitele čipu nebo biometrické údaje o osobě. Jako je například otisk prstu, sken rohovky, či duhovky apod. [6]

Od roku 2004 je v České republice k dispozici tzv. e-pas. V tomto dokladu jsou uloženy biometrické údaje držitele tohoto cestovního pasu. Tento e-pas je vydávaný v souladu s nařízením Rady Evropské Unie č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy. [4]

1.3 RFID architektura

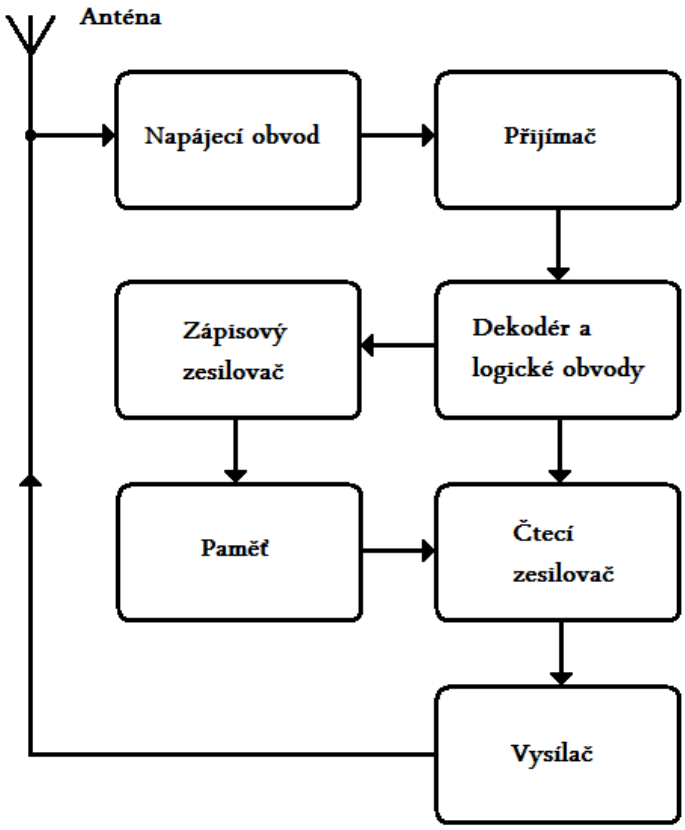
Systém RFID se skládá ze čtečky a čipu (někdy také RFID tag, RFID štítek atd.).

1.3.1 RFID čip

Zařízení RFID se řadí do kategorie rádiových zařízení, které se nazývají transpondéry. Transpondér je v podstatě kombinace přijímače a vysílače, který je navržený pro příjem specifického rádiového signálu a následné automatické odeslání odpovědi. Základní transpondéry pouze vyčkávají na rádiový impuls a poté vyšlou vlastní rádiový impuls jako odpověď.

RFID čipy obvykle obsahují následující části:

- napájecí obvod,
- přijímač,
- kódovací a dekódovací obvody,
- paměť,
- anténa,
- vysílač.



Obr. 1 Architektura RFID čipu [29]

1.3.2 RFID čtečka

Hlavní komponentou RFID čtečky je anténa, která může být u menších čteček integrovaná nebo oddělená, například u rámů v prodejnách.

RFID čtečky dále obsahují zařízení pro komunikaci, například: RS-232 sériový port, USB nebo Ethernetové připojení.

1.3.3 Middleware

Middleware je software řídící čtečky a zpracovávající načtená data. Tento systém dále předává data do koncových databázových systémů. Middleware je jakýsi prostředník, mezi čtečkou a koncovou databází.

1.4 Obecný princip RFID

RFID využívá princip elektromagnetický vln, pomocí kterých jsou přenášena data. Čtečka kolem sebe vytváří elektromagnetické pole. Toto pole je nastaveno na požadovanou frekvenci. Když je pak RFID tag vložen do elektromagnetického pole čtečky, využívá jeho energii pro napájení svých integrovaných obvodů. Vnitřní obvody RFID tagu pak vhodně upraví elektromagnetické pole. Na to reaguje čtečka, přečtením pole. Získaná data jsou v podobě binárního kódu. Tento kód je dále zpracován v mikrokontroléru, kde dojde k porovnání s pamětí identifikačních kódů a v případě shody dojde k vyvolání požadované akce.

1.5 Základní rozdělení RFID čipů

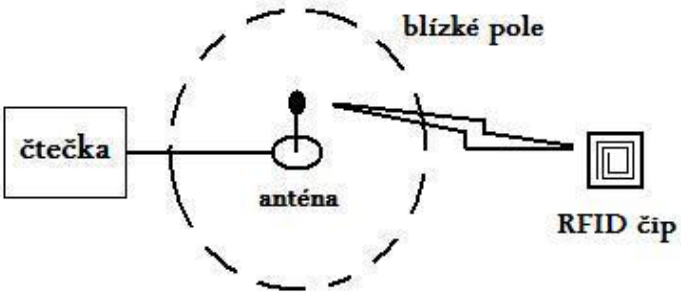
Základní rozdělení RFID čipů je na aktivní a pasivní, dále je můžeme dělit podle způsobu přenosu dat, dle pracovní frekvence, dle tvaru média a nebo podle metody šifrování.

1.5.1 Aktivní RFID čipy

Aktivní tagy jsou takové, které jsou napájené vlastní baterií, kvůli tomu jsou větší než ostatní tagy. V závislosti na čtečce, může baterie sloužit jako částečný nebo úplný zdroj energie. Některé baterie lze po uplynutí jejich životnosti vyměnit, některé ne, což může být problém aktivních tagů.

Výhodou aktivních tagů je možnost čtení na větší vzdálenosti. Vzhledem k tomu, že tag je napájen vlastním akumulátorem, pomáhá generovat napájení, které je schopno číst ve vzdálenosti několika desítek metrů.

Nevýhodou aktivních tagů je jejich větší velikost, kvůli integrované baterii. Baterie navíc nemusí být dobíjecí a tag se tak po vybití stává nefunkčním.



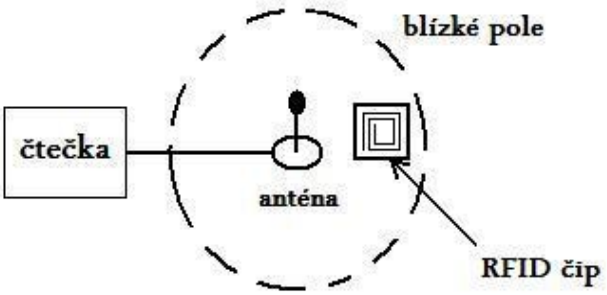
Obr. 2 Aktivní RFID čip [29]

1.5.2 Pasivní RFID čipy

Pasivní tagy jsou takové, které k napájení používají elektromagnetické pole čtečky. Neobsahují vlastní baterii, a proto nemohou nést tolik informací jako aktivní tagy.

Výhodou pasivních tagů je, že fungují bez baterie, díky tomu mohou být používány déle, než aktivní tagy a po vybytí je není třeba vyhodit. Jelikož neobsahují baterii, jsou levnější a také menší.

Nevýhodou pasivních tagů je, že jsou menší a nemohou obsahovat tolik informací.



Obr. 3 Pasivní RFID čip [29]

1.5.3 Dle přenosu dat

- čtecí tagy (read tag) – jsou určeny pouze pro čtení a nelze do nich zapisovat. Identifikační data jsou při výrobě uložena do paměti ROM,
- čtecí\zapisovací tagy (read\write tag) – jsou v současnosti využívány pro složitější aplikace. Tyto RFID čipy lze nejenom číst, ale i do nich zapisovat. Díky tomu je

otevřena možnost využití v mnohem více aplikacích. Data jsou ukládána do paměti EEPROM.

1.5.4 Dle pracovní frekvence

Pracovní frekvencí rozumíme frekvence používané pro přenos dat mezi RFID tagem a čtečkou.

Dle frekvence se tagy dělí na čtyři používané frekvence:

- 125 – 134 KHz – LF pásmo, LF tag,
- 13,56 MHz – HF pásmo, HF tag,
- 860 – 960 MHz – UHF pásmo, UHF tag,
- 2,45; 5,8 GHz – mikrovlnné pásmo, microwave tag.

Vlastnosti a chování RFID tagů závisí na použité frekvenci.

LF tagy (nízké frekvence) mají dlouhou vlnovou délku a jsou schopnější pronikat tenkými kovovými látkami. Systémy LF RFID jsou navíc ideální pro čtení objektů s vysokým obsahem vody, jako je ovoce nebo nápoje, ale rozsah čtení je omezen na desítky centimetrů. Typické využití LF tagů zahrnuje přístupové systémy a označování zvířat.

HF tagy (vysoká frekvence) pracují poměrně dobře na objektech vyrobených z kovu a mohou pracovat kolem zboží se středním až vysokým obsahem vody. Typicky systémy HF RFID pracují v rozmezí od desítek centimetrů až do 1 metru. Typické využití HF tagů zahrnuje sledování knih v knihovně, sledování pohybu pacientů a jízdenky.

UHF tagy (velmi vysoká frekvence) typicky nabízejí mnohem lepší čtecí rozsah až desítky metrů (v závislosti na nastavení RFID systému) a mohou přenášet data rychleji (tj. Číst mnohem více tagů za sekundu) než LF a HF tagy. Protože však rádiové vlny UHF mají kratší vlnovou délku, je jejich signál slabší a nemůže procházet kovem nebo vodou. Vzhledem k vysoké rychlosti přenosu dat jsou UHF tagy vhodné pro mnoho položek najednou, například: boxy zboží, když projíždějí dveřmi do skladu nebo závodníky při překročení cílové čáry. Další typické využití UHF tagů zahrnuje elektronické vybírání mýtného a řízení přístupu k parkovištím.

V následující tabulce pak najdeme přesnější rozdělení společně s výhodami a nevýhodami při použití:

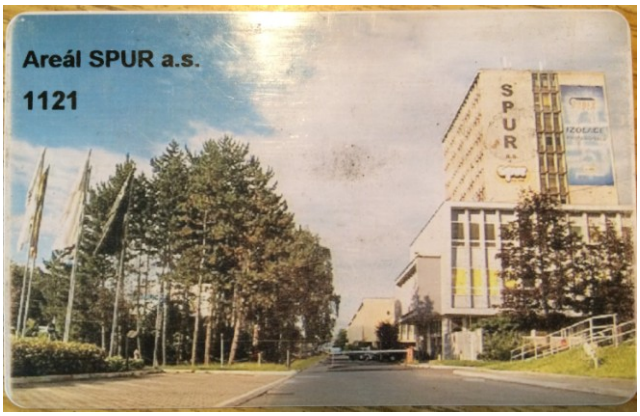
Komunikační frekvence	**Čtecí dosah**	**Vlastnosti - výhody**	**Vlastnosti - nevýhody**	**Použití**
125 - 134 kHz LW RFID (low frequency)	do 0,5 m	větší odolnost proti rušení	malý čtecí dosah	kontrola přístupu
		možnost upevnění v blízkosti vody (tekutiny)	malá komunikační rychlost	identifikace zvířat
		možnost upevnění na kovové podložce (např. na sudu)	velká anténa (solenoid) = velké a drahé provedení RFID tagu	imobilizéry automobilů
				identifikace kovových produktů (např. pivních kegů)
13,56 MHz HF RFID (high frequency)	do 1 m	menší rozměry antény = menší rozměry	kovové podložky a voda již významně snižují čtecí dosah a ruší komunikaci	chytré karty (Smart Cards)
		větší komunikační rychlost než LF		bezkontaktní placení
		větší čtecí dosah než LF		chytré etikety (Smart Labels)
		nízká cena RFID tagu - nejvíce rozšířené		označování zavazadel při přepravě
		celosvětově standardizovaná frekvence		záznam a přenos naměřených dat
				protokoly: ISO 14443, ISO 15693, Tag-IT, I-Code
				sledování identifikačních kódů palet a beden při přepravě a ve skladech
860 - 960 MHz UHF RFID (ultra high frequency)	do cca 3m	možnost i vzdáleného čtení = indentifikace průjezdem brány	nejsou čitelné přes kapaliny	současná identifikace více zabalených produktů
		velká přenosová rychlost = možná větší kapacity paměti RFID tagu	obtížné čtení na kovových podložkách	elektronické mýtné
		dipólová anténa	celosvětově nejednotná frekvence	parkovací karty
		levná výroba	problémy s odrazem od okolních kovových konstrukcí	sledování toku vratných obalů
				sledování skupinových balení (palet) při přepravě a ve skladech
				protokoly: ISO 18000-6A/B, EPC Class 0/1
2,4 GHz UHF RFID (ultra high frequency)	do 2 m	vysoká přenosová rychlost až 2 Mb/s	drahá a složitá konstrukce	elektronické mýtné
		malé rozměry dipólové antény = malé tagy	menší dosah než UHF RFID	identifikace zavazadel při letecké přepravě
			velký vliv rušení (kovu, kapalin apod.)	bezdrátový záznam a přenos dat v reálném čase

Tab. 1 Pracovní frenvence RFID čipů [7]

1.5.5 Dle tvaru média

Karty ID-1

Využívané v mnoha aplikacích, například zaměstnanecké karty, občanské průkazy, platební karty atd. Tyto karty jsou definovány normou ISO/IEC 7810. Samotná karta je pak potištěna identifikačním číslem, logem firmy, nebo fotografií držitele. Dále je možné aplikovat i ochranné holografické prvky.



Obr. 4 Příklad RFID zaměstnanecké karty

Přívěsky (klíčenky)

Určeny spíše pro soukromé účely. Většinou mají menší rozměry a zajímavý design.

Obr. 5 Příklad RFID klíčenky [19]

Dálkové ovladače

Využití v soukromých a firemních aplikacích. Většinou jsou určeny pro identifikaci a ovládání méně závažných aplikací (vrata, brány, závory, automobily, imobilizéry atd.).

Samolepky (labely)

Určeny především pro identifikaci zboží. Samolepka je většinou kombinována s čárovým kódem na povrchu. Velký důraz na cenu provedení.

Obr. 6 Příklad RFID samolepky [20]

Skleněné tagy (glass tags)

Slouží převážně k identifikaci zvířat.

Obr. 7 Příklad RFID skleněného tagu [21]

Tagy pro speciální aplikace

RFID tagy lze použít v podstatě použít pro jakoukoli aplikaci, například tzv. laundry tagy (tagy pro prádlo), tyto slouží pro identifikaci zboží v prádelnách, kde jsou kladeny vysoké podmínky na prostředí, kterému je tag vystaven. Dále je dnes RFID velmi často používáno v aquaparcích, kde jsou návštěvníkům rozdány RFID tagy ve formě různých náramků, hodinek apod.

Obr. 8 Příklad RFID hodinek

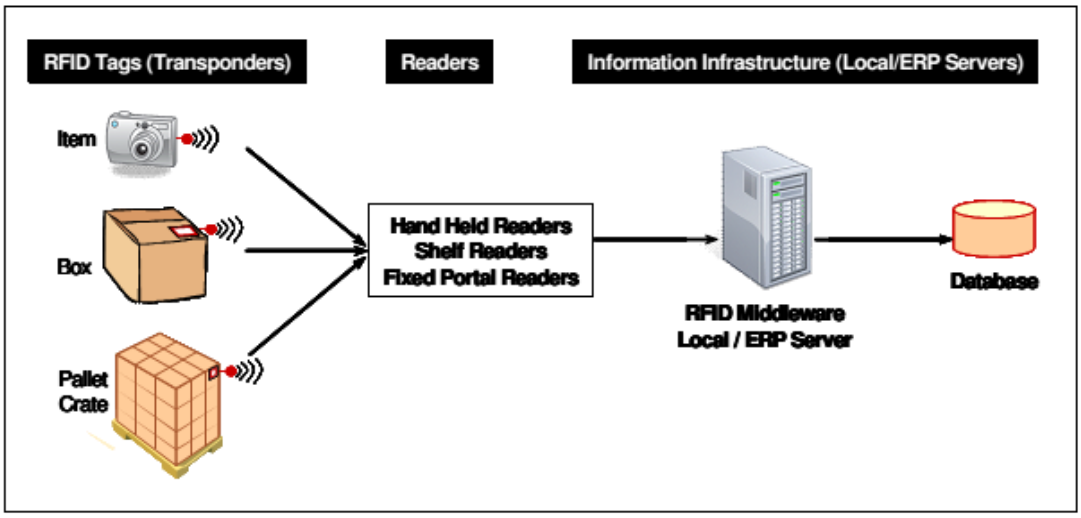
1.5.6 Dle použité metody šifrování:

- **Bez šifrování –** některé základní druhy tagů šifrování nepoužívají,
- **DES (Data Encryption Standard)** – symetrická bloková šifra, která již byla překonána. Pro šifrování se zde využívá klíče o délce 64 bitů. Z toho je pouze 56 bytů účinně používáno a zbylých 8 bitů slouží pro kontrolní součty. Jelikož je klíč docela krátký, je možné ho hrubou silou prolomit za méně než 24 hodin, [8]
- **3DES (někdy označován jako TDES, Triple DES)** – vychází ze šifrování DES, které se aplikuje třikrát. Délka klíče je tak rozšířena na 168 bitů (3x56 bitů), [8]
- **AES (Advanced Encryption Standard)** – symetrická bloková šifra s vysokou rychlostí zpracování. Velikost klíče je až 256 bitů. Útok na tuto šifru hrubou silou, by díky délce klíče trval i několik let. Tato metoda šifrování je využívána po celém světě, [8]
- **CRYPTO1** – symetrická proudová šifra. Jedná se o velmi rychlý proces šifrování, ale s nízkou bezpečností. Výrobce NXP semiconductors původně nechtěl prozradit algoritmus zpracování šifry. Díky reverznímu inženýrství byl však algoritmus odhalen a šifrování tak bylo překonáno, [8]
- **PKE (public key encryption – šifrování s veřejným klíčem)** – Jedná se o asymetrické šifrovací algoritmy. U asymetrických šifer je využíváno dvou typů klíčů. Privátní klíč, který slouží k dešifrování soukromé zprávy a veřejný klíč, k zašifrování zprávy pro příjemce. Oba klíče jsou navrženy tak, aby nebylo možné z jednoho spočítat druhý a obráceně. [8]

1.6 Oblasti využití RFID

RFID technologie naskýtá nespočet využití. Mezi ty největší a nejvyužívanější patří rozhodně použití v dodavatelských řetězcích.

Musíme mít na paměti, že RFID slouží k identifikaci objektu nebo člověka. Mezi jeho výhody patří, že k tomu nepotřebuje žádný lidský zásah, tagy mohou být obvykle přečteny i když nejsou natočeny přímo na čtečku a z větších vzdáleností. Informace je ihned posílána do počítače k dalšímu zpracování. Typicky jakmile čtečka přečte informace na čipu, posílá tři věci do počítače: ID čipu, ID čtečky a údaj o čase. Pokud organizace ví, kde se nachází která čtečka, má rychlý přehled o tom, kde se nachází které zboží a také, kde všude už bylo. [14]



Obr. 9 Jak funguje technologie RFID [22]

1.6.1 Sledování zboží

Není asi žádným překvapením, že sledování zboží patří k nejčastějšímu využití RFID technologie. Organizace mohou připevnit RFID tagy na zboží, které se často krade, ztrácí nebo je jenom těžko nalezitelné.

Například Air Canada šetří milióny dolarů každý rok tím, že sledují pohyb jídelních vozíků. Používají k tomu aktivní RFID čipy připevněné zespodu vozíku (pasivní bylo těžké přečíst přes železné vozíky) a čtečky na vstupech a výstupech z cateringových zařízení po celém světě. Nejenže jim to pomáhá zmenšit počet potřebných vozíků, ale navíc mohou lépe organizovat pohyb vozíků po letišti, tak že je vždy dostatek jídla pro cestující. [14]

1.6.2 Výroba

RFID je používáno ve výrobních továrnách už déle než desetiletí. Jeho úkolem je sledování součástek a postup práce, tak aby se omezil počet vad a zrychlila výroba. [14]

1.6.3 Maloobchod

Maloobchodní prodejny, jako je například Best Buy, Metro, Target, Tesco a WalMart jsou v popředí adopce RFID technologie. Tyto firmy se momentálně zabývají zefektivněním dodavatelských služeb a tím aby byl produkt v regálu v okamžiku, kdy ho chtějí zákazníci koupit.

Metro v Německu a Tesco ve Velké Británii podnikly několik studií, ke zjištění, jestli přidání RFID tagů na jednotlivé produkty, přispěje ke zmenšení počtu produktů, které nejsou skladem. Hewlett-Packard zase přidává tagy na tiskárny a elektroniku, které posílá do WallMartu. Ale vezmeme-li v úvahu stávající cenu RFID tagů, dá se předpokládat, že si budeme muset ještě pár let počkat, než bude využití RFID tagů v maloobchodě více relevantní.

Mezi nejvýce komentované aplikace patří schopnost automatického zaplacení za zboží, čímž se řetězce vyhnout velkým čekacím řadám u pokladen. Systém dále předpokládá s nasazením malých monitorů do nákupních košíků. Pokud by zákazník vložil do košíku například steak, na obrazovce se mu může zobrazit reklama na steakovou omáčku nebo víno, které je zrovna ve slevě. Při placení pak zákazník projde i s košíkem speciální tunelovou čtečkou, která automaticky načte všechny položky v košíku, pak už zbývá jen zaplatit za zboží. Tyto aplikace ale vyžadují nasazení RFID čipů na všechny položky v obchodě, čehož se asi v tomto desetiletí nedočkáme. [14]

1.6.4 Platební systémy

Jedním s oblíbených využití RFID technologie je placení mýtného bez potřeby zastavení. Tento aktivní systém využívá hodně zemí a některé fast foody se snaží experimentovat s využitím stejné technologie, pro placení za jídlo v jejich drive-through oknech.

Dalším využitím je jednoduché placení za cestu hromadnou dopravou. Hodně měst zavádí RFID karty namísto karet s magnetickým pruhem, protože RFID nabízí možnost rychlejšího nastupování vystupování pasažérů.

Hodně lyžařských středisek v Evropě používá RFID lístky. V Japonsku si zase může zákazník stáhnout do telefonu RFID lístek do kina. MasterCard a Visa také experimentují s RFID kartami a přívěsky na klíče pro menší platby. [14]

1.6.5 Příklady dalších zajímavých využití RFID systémů

Móda

Chytré zkušební kabinky. Někteří obchodníci začínají do zkušebních kabinek umisťovat RFID systémy. Po naskenování kódu se nakupujícímu zobrazí data o produktu a další podobné alternativy. Prodejci se na oplátku zvyšuje šance, že nakupující najde to, co hledá a navíc získá spolehlivý systém proti zlodějům. [5]

Zábavní parky

Lístky bez nutnosti skenování. Disneyland nedávno zavedl RFID technologii do svých vstupenek. Tyto vstupenky, ve tvaru platební karty, pak urychlují čekání v řadě, protože není potřeba skenovat čárový kód, nebo kontrola člověkem. Navíc tyto vstupenky nabízí operátorům parku důležitý zdroj informací o pohybu zákazníků a žádanosti jednotlivých atrakcí. [5]

Kasina

Kasina začínají do svých chipů implementovat RFID technologie. Tímto jsou schopna podchytit různé podvody týkajíce se sázek. Navíc okamžitě vidí, kdo vyhrává či prohrává a mohou tuto informaci použít k tomu, aby vás udržely déle ve hře, pomocí různých free drinků atd. [5]

Sport

Golfový míček. Na některých golfových hřištích se začínají objevovat míčky používající RFID technologii. Pokud se povede hráči zahrát míček mimo hřiště (například do lesa), nemusí pak strávit dlouhý čas hledáním místa, kam dopadl. [5]

Zbraně

RFID technologie se dostala už i do zbraní. Čipy se implementují jak do zbraní samotných, tak i do nábojů. Tohle má za úkol zlepšit kontrolu nelegálně držených zbraní. [5]

Půjčovny aut

Vrácení auta bez čekání. Přesto že spolu tyto dvě technologie normálně soupeří, V tomhle případě se RFID a GPS krásně doplňují. GPS slouží ke sledování půjčeného auta na velké vzdálenosti, zatímco RFID zabudované na parkovištích půjčoven slouží k vrácení vozidla. Zákazník tak může zaparkovat vozidlo a víc už se nestará. [5]

Zdravotní péče

Nemocnice nabízí celou řadu využiti pro RFID: vedení záznamů o lécích, distribuci léků a monitorování zařízení. Navíc se začínají objevovat speciální náramky pro doktory, které hlídají, aby si doktor nezapomněl umýt ruce. [5]

2 JEDNOTLIVÉ RFID TECHNOLOGIE

2.1 EM 4200

Společnost EM Microelectronic-Marin SA ze Švýcarska je jednou z mnoha firem vyrábějících RFID tagy. Jedním z nich je EM 4200. Tato technologie patří mezi LF tagy pracující na frekvenci 125kHz.

EM 4200 je integrovaný obvod CMOS určený pro použití v elektronických transpondérech. 128b jedinečný kód je uložen v laserově naprogramované paměti ROM. K dispozici je několik možností velikostí paměti 64, 96 nebo 128b ROM.

EM 4200 nabízí:

- několik možností modulace dat: Manchester, Biphase, PSK a FSK,
- 128b programovaná paměť ROM (nebo 64 a 96b),
- frekvenční rozsah 100 až 150 kHz,
- on-chip usměrňovač a omezovač napětí,
- teplotní rozsah -40 ° C až + 85 ° C. [9]

2.2 EM 4333

Dalším tagem od společnosti EM Microelectronic-Marin SA je EM 4333.

EM4333 je bezkontaktní čipová karta, která integruje blízké i bezdrátové protokoly do jednoho čipu pomocí stejné antény. Díky tomu je použitelná v široké škále aplikací.

Karta podporuje ISO/IEC 15693 rozhraní s vysokou úrovní zabezpečení datových přenosů. EM 4333 je zabezpečena proudovou šifrou Grain128a s klíčem délky 128b. Šifra podporuje tří průchodovou autentizaci a MAC funkci (Message Authentication Code – Kód ověřování zpráv) pro zajištění zabezpečení datových přenosů.

Současně podporuje protokol ISO14443 typu A, který může komunikovat až 848 kb/s v obou směrech, vhodný pro bezdrátové aplikace s vysokorychlostními a vysoce zabezpečenými přenosy.

EM 4333 nabízí:

- 4kB uživatelského prostoru pro data, sdíleného mezi oběma ISO protokoly,
- 64kB kódové paměti pro zákaznický operační systém,
- 3kB XRAM and 256B iRAM,
- ISO/IEC14443A zabezpečené šiframi DES/3DES a AES-128,
- ISO/IEC15693 zabezpečené proudovou šifrou Grain128A. [39]

2.3 NTAG 413 DNA

Další společností zabývající se výrobou RFID čipů je NXP semiconductors N.V. (dříve Philips Semiconductors). Jejich RFID čip NTAG 413 DNA je nabízí bezpečnostní funkce, jako je kryptografická autentizace a jedinečná autentizace s každým použitím, což umožňuje pokročilejší ochranu produktu a dynamičtější uživatelské zkušenosti.

NTAG 413 DNA nabízí:

- ISO/IEC14443 typu A,
- 160 B uživatelské paměti,
- uchování dat v paměti až 10 let,
- 100 000 cyklů mazání a zápisu,
- pracovní frekvence 13,56 MHz,
- operační vzdálenost až 100 mm,
- zabezpečení šifrou AES128. [10]

2.4 MiFare Classic

Technologie MiFare je další z řady výrobků společnosti NXP semiconductors. Pracuje na frekvenci 13,56 MHz. Vyrábí se ve 4 řadách Classic, DESFire, Plus a Ultralight. Nejrozšířenějšími jsou právě řady Classic a DESFire.

MiFare Classic je prvním typem z řady MiFare technologie. Karta plně vyhovuje normě ISO/IEC 14443-A. Technologie MiFare Classic byla již v minulosti překonána a proto se ustupuje od jejího používání, nahrazuje se novějším typem DESFire.

Přesto že byla tato technologie překonána a nelze ji tak považovat za bezpečnou, lze stále říct, že je bezpečnější než EM Marin.

Čip má z výroby naprogramován 7 bajtový UID nebo 4 bajtový NUID (Non-Unique ID – neunikátní identifikační číslo). Dále nabízí možnost nastavení tří průchodové autentizace dle standardu ISO/IEC 9798-2. V rámci podpory více aplikací, lze v čipu nastavit dva rozdílné šifrovací klíče A a B.

MiFare Classic S70 nabízí:

- ISO/IEC 14443 typu A,
- pracovní frekvenci 13,56 MHz,
- podpora generátoru náhodného ID (pouze i 7 bajtové UID verze),
- operační vzdálenost až 100 mm,
- přenosovou rychlost 106 kbit/s,
- 1kB – 4kB paměť EEPROM,
- 200 000 cyklů mazání a zápisu,
- uživatelsky nastavitelný přístup k jednotlivým paměťovým blokům,
- aplikaci proudové šifry CRYPTO1. [11]

2.5 MiFare DESFire EV1

Další technologie je MiFare DESFire. Tato obsahuje více bezpečnostních prvků, přesto byla v roce 2011 překonána. Nepodařilo se překonat šifru 3DES, ale zabezpečení bylo prolomenu pomocí postranních kanálů. NXP však zavedla modifikaci MiFare DESFire EV1, která je stále považována za nepřekonatelnou a to i při zachování poměrně nízkých výrobních nákladů.

Tato technologie je použitelná ve spoustě aplikací, jako je veřejná přeprava, přístupové systémy, nebankovní platební karty atd. Tento čip nabízí větší bezpečnost přenosu a vyšší přenosovou rychlost dat. MiFare DESFire EV1 je plně založena na standardu ISO/IEC 14443-A. Karta nabízí integrovaný zálohovací systém a tří průchodovou autentizaci.

Technologie využívá vysoce bezpečných šifrovacích metod 3DES a AES. Šifrování probíhá v hardwarovém modulu, díky čemuž je zajištěna vysoká rychlost šifrování dat.

MiFare DESFire EV 1 nabízí:

- čtecí vzdálenost až 100 mm,
- pracovní frekvenci 13,56 MHz,
- rychlé datové přenosy 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s,
- 7 bajtové UID,
- paměť EEPROM 2K, 4K, nebo 8K,
- životnost dat v paměti 10 let a 500 000 zapisovacích cyklů,
- certifikaci Common Criteria EAL4+,
- hardwarový 3DES šifrovací obvod s možností využití 56/112/168 bitového klíče,
- hardwarový AES šifrovací obvod se 128 bitovým klíčem,
- šifrování RF přenosu,
- anti-kolizní mechanismus. [12]

2.6 SmartMX2

Další technologií, kterou lze považovat za poměrně bezpečnou je SmartMX2. Jedná se o Kartu ICC s duálním rozhraním pro komunikaci. Výrobcem je společnost NXP semiconductors. Technologie je vhodná pro prožití v aplikacích v oblasti eGovermentu, tzn. bankovnictví a veřejné dopravy.

SmartMX2 nabízí:

- paměťový prostor EEPROM až 144 KB,
- minimální životnost dat v paměti 25 let a 500 000 zapisovacích cyklů,
- paměť ROM: 384 KB,
- paměť RAM: 8.125 KB (8320 B),
- procesor SmartMX2 CPU (Central Processing Unit),

- koprocesor PKI(Public Key Infrastructure) s využitím RSA, ECC,
- hardwarové koprocesory pro šifrování 3DES a AES,
- generátor pravých náhodných čísel dle AIS-31,
- kontrolní koprocesor s podporou 16 a 31 bitové CRC,
- reálné časování podporující kontrolu časových komunikačních limitů,
- kompatibilita s normami ISO/IEC 7816 - kontaktní přenos (rozhrání UART) a ISO/IEC 14443A - bezkontaktní přenos (rozhraní CIU),
- možnost implementace podpory pro technologii MiFare Classic a MiFare DESFire EV1. [13]

2.7 ATC1024

Čip ATC1024-MV010 od společnosti LEGIC je dalším z mnoha produktů RFID technologie. Čip nabízí vysokou bezpečnostní úroveň za nízké ceny. Je to perfektní čip pro velké projekty, jako jsou městské karty, e-lístky apod.

Kombinace větší čtecí vzdálenosti, vysoké transakční rychlosti a vícevrstvého zabezpečení činí tyto čipy ideální volbou pro bezpečné a konkurenceschopné aplikace s velkým objemem.

ATC1024 nabízí:

- ISO/IEC 15693,
- 912 B paměti,
- 8 bajtové UID,
- čtecí vzdálenost do 70cm,
- šifrování datového přenosu pomocí šifry 3DES,
- šifrování dat (každá aplikace zvlášť) pomocí šifer AES128, AES256, 3DES, LEGIC encryption,
- až 59 různých aplikací,
- minimální životnost dat v paměti 10 let a 100 000 zapisovacích cyklů. [24]

3 BEZPEČNOSTNÍ PRVKY IDENTIFIKAČNÍCH DOKLADŮ

3.1 Elektronický občanský průkaz – e-OP

Tento průkaz je vydávaný od 2. 1. 2012. Věnuje se mu novela zákona č. 328/1999 Sb., o občanských průkazech. Další podrobnosti stanoví vyhláška č. 400/2011 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech. V roce 2018 začne být vydáván pouze e-OP, který splňuje podmínky nařízení eIDAS s novým typem čipu. Každý držitel občanského průkazu bude muset znát svůj bezpečnostní osobní kód, PIN kód k online přístupu, PUK kód k případné deblokaci a PIN kód k digitálnímu podpisu. [15]

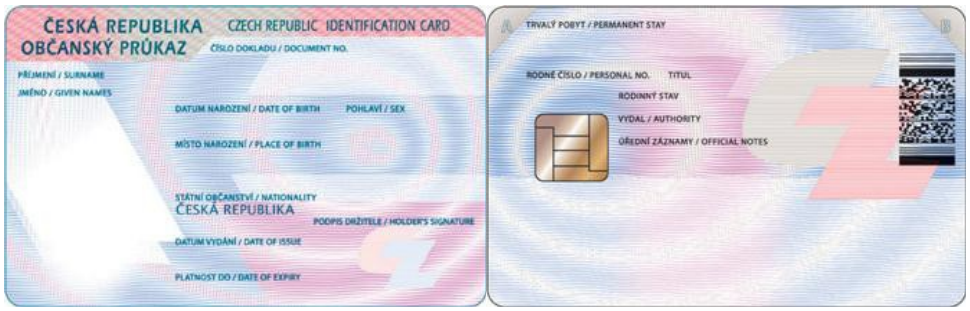
3.1.1 Varianty a vzhled

Existují dvě varianty elektronického občanského průkazu:

- se strojově čitelnými údaji bez kontaktního elektronického čipu,
- se strojově čitelnými údaji s kontaktním elektronickým čipem.

Varianta s čipem se vydává pouze na žádost občana. Na čipu je uložena informace o čísle občanského průkazu a dalších údajích. Dále je v budoucnu v plánu do dokladu zapisovat informace o řidičském průkazu, zbrojním průkazu apod. Poplatek za vydání nového dokladu je 500,- Kč. Varianta bez čipu je běžnou formou OP. Vydání tohoto průkazu je bezplatné.

Grafické vyobrazení vzorů se nachází ve vyhlášce 400/2011 Sb. [15]



Obr. 10 Vzor eOP dle vyhlášky č. 400/2011 [15]

Obr. 11 Specimen eOP [15]

3.1.2 Údaje uložené v čipu

Zákon stanoví údaje zapisované do e-OP:

1. jméno (popřípadě jména), příjmení, pohlaví, rodné číslo, občanství, datum narození, místo narození a adresa trvalého pobytu,
2. číslo e-OP, datum vydání dokladu, skončení platnosti dokladu a označení úřadu, který jej vydal,
3. digitální fotografii občana a jeho zdigitalizovaný podpis,
4. strojově čitelná zóna (obsahuje jméno, příjmení, pohlaví, státní občanství, datum narození, datum platnosti dokladu, číslo a kód dokladu),
5. 2D kód (obsahuje číslo OP).

3.1.3 Bezpečnostní osobní kód

Podle §8a zákona o občanských průkazech platí:

- bezpečnostní osobní kód (BOK) slouží k autentizaci při elektronické identifikaci držitele OP při komunikaci s informačními systémy veřejné správy,
- BOK je kombinace 4 – 10 číslic,
- občan zvolí BOK povinně při převzetí OP. [15]

3.1.4 Základní kryptografické zabezpečení dokladů - BAC

BAC je protokol sloužící k vygenerování dočasných klíčů s nízkou entropií pro vybudování bezpečného komunikačního kanálu mezi čipem a terminálem (SM). Odvozuje přístupové klíče z vybraných údajů, vytištěných v strojově čitelné zóně dokladu (MRZ) – číslo dokladu (9 znaků), datum narození držitele dokladu (6 znaků) a datum konce platnosti dokladu (6 znaků). Všechny tyto údaje jsou chráněny kontrolní číslicí, která umožňuje detekovat chyby při optickém čtení údajů. [15]

Obr. 12 MRZ dokladu [15]

3.1.5 Kryptografické zabezpečení dokladů - PACE

PACE je protokol sloužící k vygenerování dočasných klíčů s vysokou entropií pro vybudování bezpečného komunikačního kanálu mezi čipem a terminálem (SM) na základě znalosti sdíleného tajemství (hesla sdíleného mezi personalizovaným čipem a tělem dokladu nebo držitelem). Heslo není většinou spojeno s hodnotami, které může útočník odhadnout (datum narození, konec platnosti dokladu):

- Card Access Number (CAN) logické číslo, které může být statické, nebo dynamické. Statická forma může být vytištěna na dokladu, dynamická zobrazena na displeji dokladu,
- Personal Identification Number (PIN) krátké heslo, které je známé výhradně držiteli dokladu,
- Machine Readable Zone (MRZ) heslo odvozené z MRZ , které je možné použít pro PACE i BAC (pro zpětnou kompatibilitu). [15]

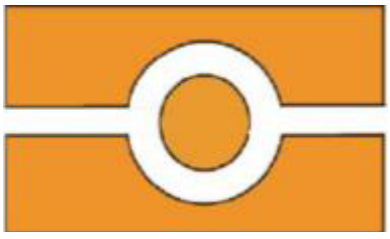
Metoda	Výhoda	Nevýhoda
PA	Autenticita LDS	Neodstraňuje klonování a substituci čipu
AA	Zabraňuje klonování a výměně čipu	Vyžaduje kryptografický čip, neodstraňuje sémantiku výzvy
BAC	Zabraňuje neoprávněnému čtení a odposlouchávání komunikace mezi čipem a oprávněným terminálem	Vyžaduje kryptografický čip, klíče mají nízkou entropii (34 – 73 bitů)
PACE	Náhrada BAC, odvozuje klíče s vysokou entropií na základě sdíleného hesla	Vyžaduje kryptografický čip s podporou PACE
EAC/EACv2	Zabraňuje neoprávněnému přístupu k citlivým biometrickým údajům, zabraňuje klonování čipu	Vyžaduje komplexní infrastrukturu PKI

Tab. 2 Kryptografické zabezpečení dokladů [15]

3.2 Elektronický pas - e-Pas

Organizace ICAO (International Civil Aviation Organization – Mezinárodní organizace pro civilní letectví) čerpá specifikace pro tzv. e-pasy z normy ISO 14443. Tato norma specifikuje frekvenci použitou pro RFID čipy na 13.56MHz. Použité čipy jsou pasivní a vzdálenost, na kterou lze čip přečíst je cca 10cm.

Zatím co americký obchodní řetězec WalMart používá jednoduché čipy jejichž jediným bezpečnostním prvkem je tzv. příkaz „kill“, který učiní tag permanentně nefunkčním. U e-pasů se používá tagů se zabezpečením, jako je například odolnost proti manipulaci s čipem, nebo šifrování. [16]



Obr. 13 Označení elektronického pasu [16]

3.2.1 Data uložená na čipu

Podle standardu ICAO pro e-pasy s biometrickou identifikací, byla zavedena logická struktura uložení dat na čipu. Konkrétně specifikuje, že data, která jsou již vytištěna na papírovém pase, jsou povinná a biometrie obličeje (fotka s vysokým rozlišením ve formátu JPEG 2000), otisky prstů a čočky jsou nepovinné.

Standardní formát pro fotku obličeje, pokud je použita, zahrnuje celou hlavu vycentrovanou s vlasy nepřekážejícími v obličeji a oči otevřené ve stejné horizontální výšce. Krk a ramena by taky měly být součástí fotky, společně s jednobarevným pozadím a bez stínů.

Data uložená na čipu by měla být stejná jako data vytištěná na papírovém pasu. Toto je důležité ze dvou důvodů. Pokud by z nějakého důvodu čip selhal, může cestovatel stále použít svůj papírový doklad a navíc si je schopný kdykoliv ověřit data uložená na čipu, bez jakéhokoli speciálního vybavení.

V roce 2011 ICAO navíc navrhovalo možnost zahrnutí cestovní historie, víz a aplikace pro automatizované odbavení. [17]

Biometrická data

Biometrií rozumíme měřitelné biologické nebo behaviorální aspekty člověka, které mohou být použity k automatickému rozpoznávání.

Jsou to velice silné identifikátory a většinou představují nevyvratitelný důkaz o identitě osoby, které zvyšují bezpečnost a efektivitu přístupových systémů, jelikož jsou jen stěží duplikovatelné nebo sdílené.

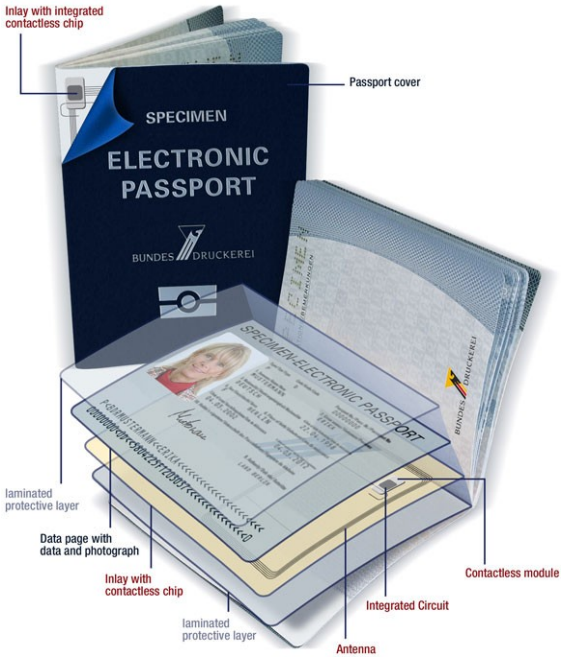
Biometrická data mohou být použita dvěma způsoby: pro identifikaci a pro autentizaci.

V případě identifikace, porovnává počítač biometrická data člověka (např. otisk prstu) se všemi biometrickými vzorky uloženými v databázi. Pokud se shodují s jedním z nich, je osoba identifikována. Tomuto se říká shoda one-to-many (jeden-k-mnoha).

V případě autentizace, předkládá osob živé biometrické údaje a ty jsou porovnávány s uloženými údaji předloženými dříve. Pokud se shodují, je autentizace u konce. Tomuto se říká shoda one-to-one (jeden-k-jednomu). Biometrická data zde nejsou uložena v databázi, ale osoba je předkládá uložené na čipu, který vlastní a je za něj odpovědná.

Nicméně informace, které biometrie poskytuje, jsou velice citlivé a nesou s sebou vážná bezpečnostní rizika.

V případě e-pasů jsou biometrická data použita k autentizaci a jsou uložena v RFID čipu. [17]

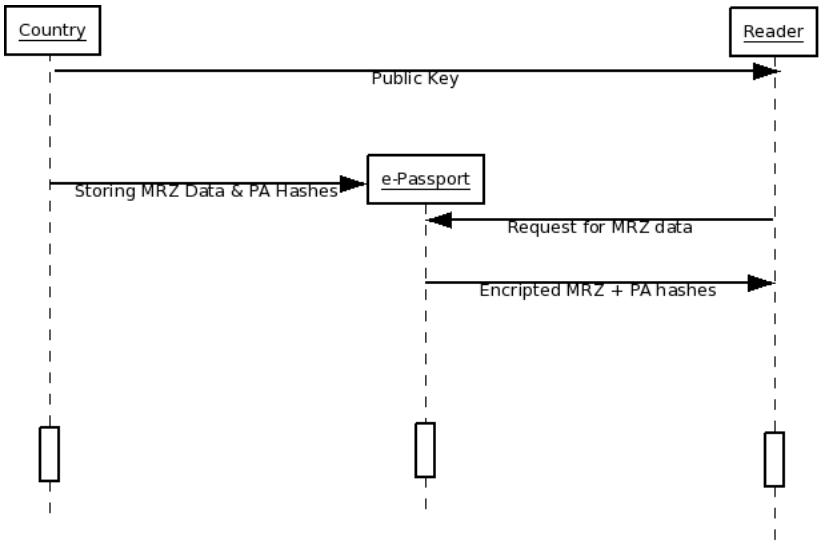


Obr. 14 Struktura elektronického pasu [23]

3.2.2 Kryptografie použitá v e-pasech

Specifikace ICAO

Norma ICAO specifikuje jednu povinnou šifrovací funkci a to **pasivní autentizaci**. Data uložená na čipu jsou podepsána příslušným státem. Povolené algoritmy pro podpisy jsou RSA, DSA a ECDSA. Jak uvádí standard ICAO, pasivní autentizace zaručuje pouze to, že data na čipu jsou pravá, nedokáže už ale zajistit pravost samotného čipu. [23]



Obr. 15 Pasivní autentizace [23]

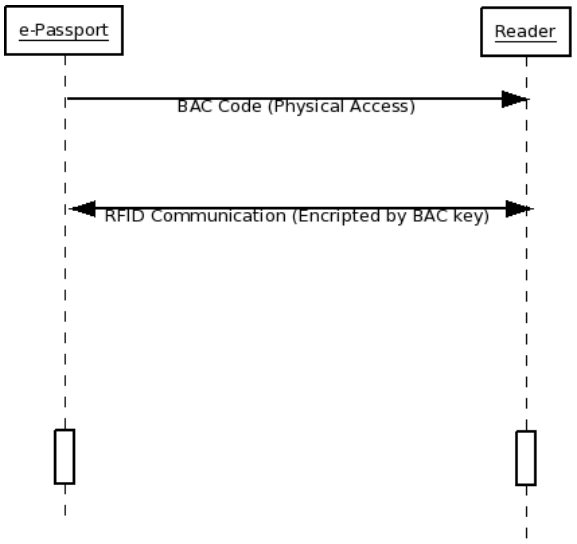
Dále standard ICAO specifikuje dvě volitelné šifrovací funkce a to **Basic Access Control** (základní kontrola přístupu) a **Secure Messaging** (bezpečné zpracování zpráv). Aby se zabezpečilo, že data může přečíst pouze povolená čtečka, jsou do čipu uloženy speciální šifrovací klíče (K_{ENC}, K_{MAC}). V okamžiku kdy se čtečka pokouší přečíst čip, dojde ke spuštění protokolu výzva-odpověď, který prokáže, že čtečka zná dvojici klíčů, a odvozuje tzv. relační klíč. Pokud je autentizace úspěšná, tak čip uvolní přístup ke svým datům, na druhou stranu není-li autentizace úspěšná, zůstává čtečka považována za neautorizovanou a čip nepovolí přístup k datům. Klíče K_{ENC} a K_{MAC} se odvozují z dat vytištěných na čipu:

- číslo pasu, běžně 9 číslic,
- datum narození držitele pasu,
- datum vypršení platnosti pasu.
- 3 čísla kontroly, pro každý předcházející údaj.

Záměr použití základní kontroly přístupu je jasně popsán přímo v ICAO standardu:

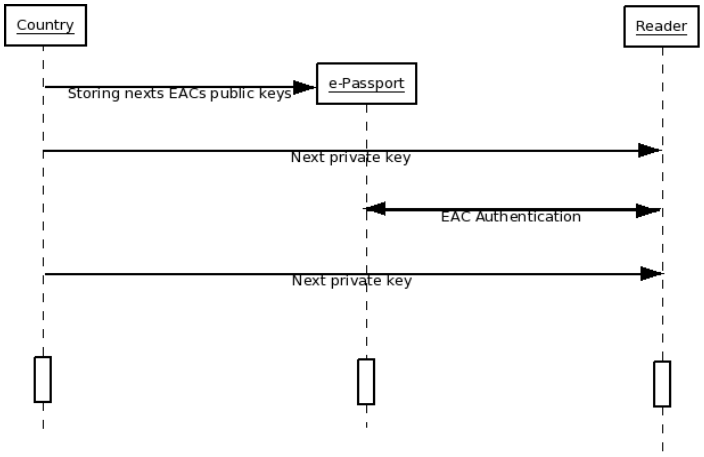
Schopnost přečíst údaje uložené v pasu, by měla být dostupná pouze v okamžiku, kdy chce majitel tohoto pasu prokázat svou totožnost.

Toto bohužel není pravda, kvůli dvěma důvodům. Zaprvé entropie klíčů je příliš malá, 56 bitů. Zadruhé klíče jsou fixní a používané po celou životnost pasu. Což znamená, že jakmile byl jednou čip přečtený, je nemožné odmítnout přístup čtečky. [23]



Obr. 16 Basic Access control (základní kontrola přístupu) [23]

ICAO dále standardizuje autentizaci nazývanou **Extended access control** (rozšířená kontrola přístupu). Ta se skládá ze sady podpisů terminálů uložených na čipu. Jednotlivé země tyto podpisy periodicky mění, aby se zabánilo ukradení podpisů, kvůli velkému používání terminálů. [23]

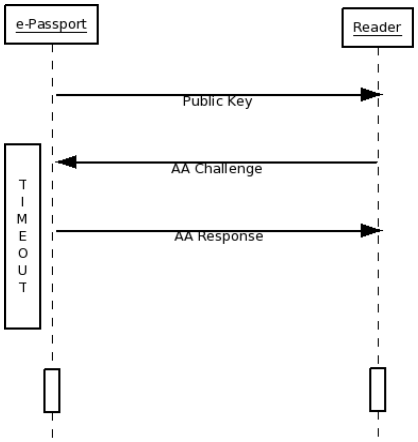


Obr. 17 Extended access control (rozšířená kontrola přístupu) [23]

Aktivní autentizace

Zatím co Basic access control zaručuje pravost dat na čipu, aktivní autentizace slouží k zabezpečení čipu proti klonování. Aktivní autentizace spoléhá na šifrování veřejným klíčem. Na čipu je společně s dalšími podepsanými daty uložen také privátní klíč. K autentizaci čipu dochází tak, že čtečka vyšle k čipu 8 bytový dotaz, ten ho digitálně podepíše svým privátním klíčem a vrátí výsledek. Čtečka pak ověří odpověď pomocí veřejného klíče pro tento pas.

Veřejný klíč používaný pro aktivní autentizaci musí být svázaný se specifickým e-pasem a jeho biometrickými daty. Jinak by mohlo dojít k útoky man-in-the-midle. Mimoto pro zefektivnění, by neměl privátní klíč, používaný pro aktivní autentizaci, nikdy opustit konkrétní čip. [23]



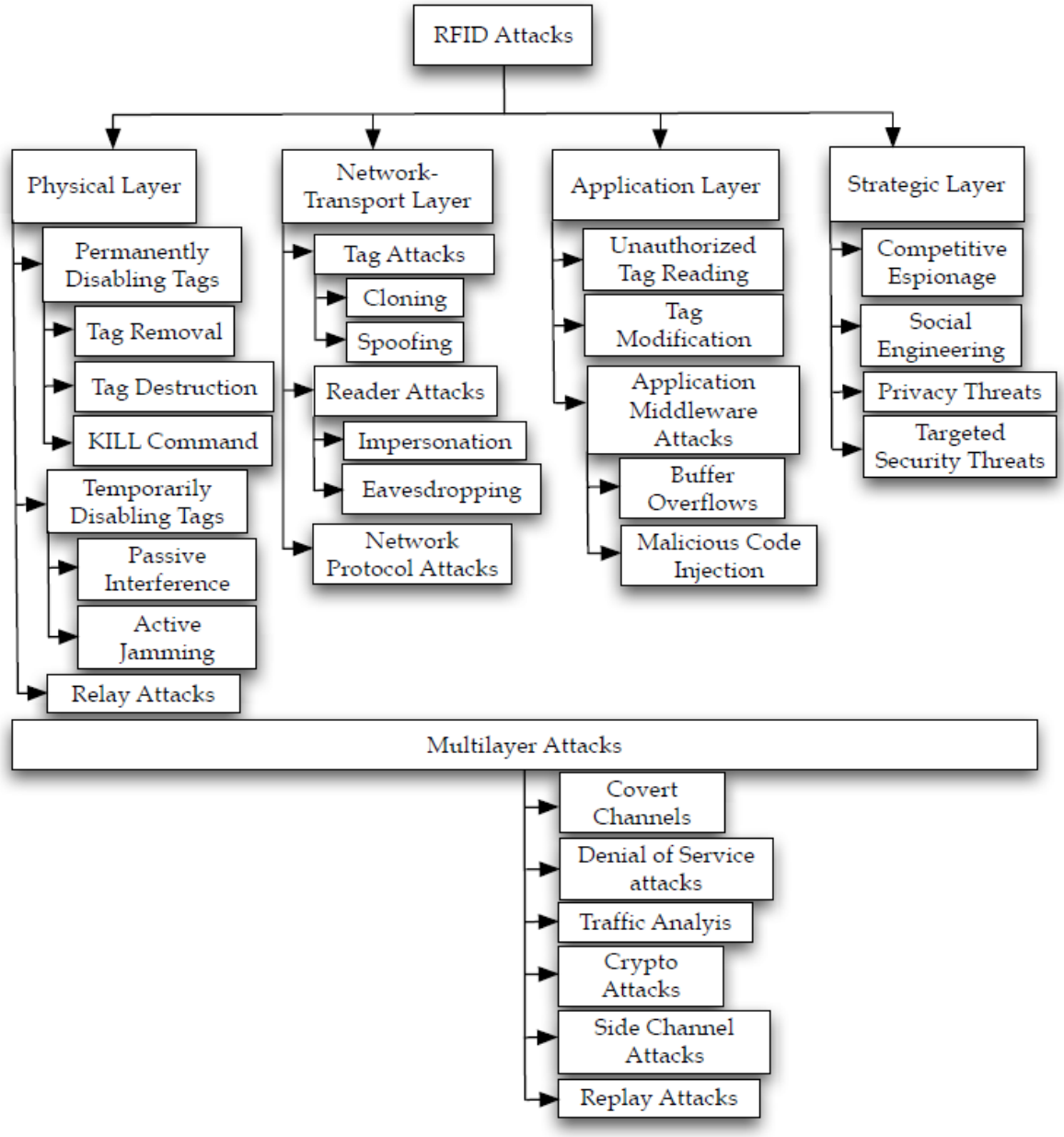
Obr. 18 Aktivní autentizace [23]

II. PRAKTICKÁ ČÁST

4 PŘEHLED MOŽNÝCH ÚTOKŮ NA RFID

Stejně jako jiné informační systémy, tak i RFID jsou náchylné na útok a můžou být ohroženy během různých fází použití.

Útoky na RFID systémy se dají rozdělit do 5 základních úrovní: útok na fyzické úrovni, síťové a přenosové úrovni, aplikační úrovni, strategické úrovni a víceúrovňoví útok.



Obr. 19 Klasifikace útoků na RFID [27]

4.1 Útok na fyzické úrovni (Physical layer)

Fyzická vrstva v RFID se skládá z fyzického rozhraní a samotného zařízení RFID. Útočník zde využívá bezdrátové komunikace technologií RFID, jejich špatné fyzické bezpečnosti a jejich nedostatečné odolnosti proti fyzické manipulaci. Tyto typy útoků zahrnují útoky, které trvale nebo dočasně zničí RFID tagy a také Relay útoky. [27]

4.1.1 Trvalé zničení tagu

Trvalým zničením RFID tagu rozumíme všechna možná rizika nebo hrozby, které mohou mít jako výsledek úplné zničení nebo podstatné zhoršení provozu tagu. Možné způsoby, jak tohoto docílit jsou: odstranění tagu, zničení tagu nebo použití příkazu KILL. [27]

Tag Removal (odstranění tagu). Vzhledem k tomu, že TFID tagy používají špatné fyzické zabezpečení, mohou být tagy, které nejsou pevně přichyceny k produktům, lehce odstraněny nebo připevněny k jinému výrobku. Jednoduchým příkladem může být zloděj v supermarketu, který prohodí tagy mezi drahým a levným produktem. Tento druh útoků je poměrně jednoduchý a není k němu potřeba žádných velkých zkušeností, naštěstí ho nelze použít ve větším měřítku. [27]

Tag Desruction (zničení tagu). Vzhledem k již zmíněné špatné fyzické bezpečnosti RFID tagu, může dojít k úmyslnému zničení, přesto že to pro útočníka nemusí představovat žádný konkrétní zisk. Vandal, který se zajímá jen o znepříjemnění života lidí nebo narušení provozu, může snadno zničit RFID tag. I když RFID tag unikne zničení vandaly, stále existuje možnost zničení kvůli vystavení extrémním podmínkám prostředí. Jako jsou například příliš vysoké nebo příliš nízké teploty. Kromě toho mohou být aktivní RFID tagy zničeny odebráním baterie, nebo vystavením velkému elektrostatickému výboji. [27]

KILL Command (příkaz KILL). Výrobce EPC Global vytvořil speciální příkaz zvaný KILL, který je naprogramovaný do jeho tagů. Tento příkaz je schopný permanentně umlčet RFID tag. Každý tag má jednoznačné heslo, jehož použití způsobí trvalou nefunkčnost RFID tagu. Ačkoli toto může být použito z důvodů ochrany soukromí, je zřejmé, že to může být zneužito útočníkem. [28]

4.1.2 Dočasné zničení tagu

K dočasnému vyřazení RFID tagu, lze použít tzv. Faradayovi klece, kdy útoční obalí RFID tag do alobalu a ten je pak stíněný před čtečkou. RFID tagy mohou být také dočasně zničeny pomocí radiového rušení, ať už aktivního nebo pasivního. [27]

Passive Interference (pasivní rušení). RFID tagy fungují v nestabilním a hlučném prostředí, jejich komunikace je považována za náchylnou na možné rušení a srážky z jakéhokoli zdroje rádiového rušení, jako jsou hlučné elektronické generátory a napájecí zdroje. Je tedy jasné, že toto rušení zabraňuje přesné a efektivní komunikaci. [27]

Active Jamming (aktivní rušení). Pasivní rušení je většinou nechtěný jev, kterého ovšem může využít útočník. RFID tag totiž „poslouchá“ bez rozdílu všechny radiové signály ve svém dosahu. Útočník tudíž může vytvořit elektromagnetický rušící signál ve stejném rozsahu jako čtečka, k zabránění komunikace tagů se čtečkami. [27]

4.1.3 Relay Attacks (přeposílání komunikace)

U útoku relay se útočník chová jako prostředník. Rušící zařízení je tajně vloženo mezi RFID tag a čtečku. Toto zařízení je schopné zachytit a upravit vysílaný rádiový signál. Legitimní čtečka a tag jsou oklamány, aby si myslely, že komunikují výhradně mezi sebou. Následná komunikace je pak přemostěna pomocí rušícího zařízení. Velmi znepokojivý je pak fakt, že tento útok může být proveden ze značných vzdáleností. [30]

4.1.4 Obrana proti útokům na fyzické úrovni

Za účelem zabezpečení systémů RFID proti jednoduchým útokům, jako jsou trvalé nebo dočasné zneškodnění tagů, by se měly používat tradiční protiopatření, například zvýšená fyzická bezpečnost s ochrannými kryty, ploty, brány, zamčené dveře a kamery. Díky tomu může být, úmyslné i neúmyslné fyzické zničení, stejně jako použití hliníkové tašky s fólií, zmírněno. [30]

Odebrání tagu by také mohlo být zabráněno přijetím této politiky fyzické ochrany nebo použitím silnějších prostředků proti snadnému odstranění (např. silnější lepidlo, tag zabudovaný do produktu atd.).

Rušení radiového přenosu se dá zabránit použitím zdí, které jsou nepropustné pro určité frekvence.

Pro zabránění neoprávněného použití příkazů KILL je možné použít účinnou správu hesel. Například příkaz KILL pro tag Class-1 Gen-2 EPC standartu vyžaduje 32-bitové heslo. Pro ochranu před útoky relay, je možné použít šifrování komunikace RFID nebo přidání druhé formy ověřování, jako je heslo, PIN nebo biometrická informace. Tento požadavek však definitivně eliminuje pohodlí a výhody komunikace RFID. Dalším možným způsobem, jak potlačit útoky relay, je použití tzv. distance-bounding protokolu (protokol ohraničení vzdálenosti) založený na ultra-širokopásmové pulzní komunikaci navržené společností Hancke a kol [32]. Další zajímavý přístup, který lze použít k ochraně RFID systémů proti útokům navrhl Bolotnyy a kol [31]. Přesněji řečeno, navrhli hardwarově založený přístup, který se opírá o fyzicky neklonovatelné funkce, které poskytují zabezpečení a soukromí. Tyto funkce poskytují exponenciální řešení problému distribuce klíčů a mohou chránit před klonováním, i když má útočník fyzický přístup k RFID tagům. [27]

4.2 Útok na síťové a přenosové úrovni (Network-Transport Layer)

V této úrovni jsou zahrnuty všechny útoky, které jsou založeny na způsobu komunikace RFID systémů a způsobu přenosu dat mezi subjekty RFID sítě (tagy, čtečky). Tyto útoky rozdělujeme na útok na tagy, útok na čtečky a útok na síťový protokol. [27]

4.2.1 Útok na tagy

Cloning (Klonování). Dokonce i nejdůležitější a charakteristický rys RFID systémů, jejich jedinečný identifikátor, je náchylný k útokům. Ačkoli teoreticky nemůžete požádat výrobce RFID, aby vytvořil klon RFID tagu, v praxi se ukázalo, že vytvoření repliky RFID tagu nevyžaduje spoustu peněz ani odborných znalostí vzhledem k široké dostupnosti zapisovatelných a reprogramovatelných tagů. [33]

Spoofing (Imitování). Spoofing je v podstatě variantou klonování, která fyzicky nereplikuje RFID tag. V tomto typu útoků se protivník vydává za platný tag, aby získal své oprávnění. Toto zosobnění vyžaduje úplný přístup ke stejným komunikačním kanálům jako původní tag. Patří sem znalost protokolů a tajemství používaných při ověřování. [27]

4.2.2 Útok na čtečky

Impersonation (zcizení identity). S ohledem na skutečnost, že komunikace RFID je v mnoha případech neověřená, mohou útočníci snadno padělat identitu legitimní čtečky k získání citlivé informace nebo úpravě dat na RFID tagu. [27]

Eavesdropping (odposlouchávání). Kvůli bezdrátové povaze RFID je odposlouchávání jednou z nejzávažnějších a nejrozšířenějších hrozeb. Při odposlechu neoprávněná osoba používá anténu k zaznamenání komunikace mezi legitimní RFID čtečkou a tagem. Tento typ útoku lze provádět v obou směrech: tag-čtečka a čtečka-tag. Vzhledem k tomu, že čtečky vysílají informace o mnohem vyšší síle než tagy, jsou citlivější na tento druh útoků ve větší míře a na mnohem větší vzdálenosti. Zaznamenané informace mohou být použity k provádění pozdějších složitějších útoků. Účinnost tohoto útoku závisí na mnoha faktorech, jako je například vzdálenost útočníka od legitimních zařízení RFID. [27]

4.2.3 Útok na síťový protokol

Systémy RFID jsou často spojeny s back-end databázemi a síťovými zařízeními na podnikové páteři. Nicméně tato zařízení jsou náchylná ke stejným zranitelnostem univerzálních síťových zařízení. Chyby v operačním systému a síťových protokolech mohou být použity škodlivými útočníky ke spuštění útoků a ohrožení infrastruktury back-end databáze. [27]

4.2.4 Obrana proti útokům na síťové a přenosové úrovni

Pomocí vhodného sběru dat je možné detekovat klonované RFID tagy. Alternativně mohou být klonovací útoky zmírněny pomocí ověřovacích protokolů reakce na výzvu. Ty by měly rovněž podporovat mechanizmy proti útokům hrubou silou. Nicméně vnitřní omezení zdrojů RFID tagů, vedou k slabým autentizačním protokolům, které jsou neúčinné vůči odhodlaným útočníkům. Existují techniky pro posílení odolnosti EPC tagů před klonovacími útoky pomocí přístupu založeném na PINu. Veřejné povědomí o bezpečnostních důsledcích spojených s klonovacími útoky by mělo být klíčovou politikou, proti které je potřeba se bránit.

To však ne vždy platí. Například žádná ze zemí, které vydávají e-pasy, nemá mechanismy proti klonování, jak navrhuje standard ICAO 9303 [33]. Abychom mohli bránit útokům pasivního odposlechu, mohly by být použity šifrovací mechanismy k šifrování komunikace

RFID. Se Spoofingem lze bojovat pomocí ověřovacích protokolů nebo druhé formy ověřování, jako jsou jednorázová hesla, PIN či biometrie. [27]

4.3 Útok na aplikační úrovni (Application layer)

Tato úroveň zahrnuje všechny útoky zaměřené na informace týkající se aplikací a vazby mezi uživateli a tagy RFID. Takové útoky využívají nepovolené čtení tagů, úpravy údajů tagů a útoky v aplikačním middlewaru. [27]

4.3.1 Unauthorized Tag Reading (nepovolené čtení tagu).

Protože ne všechny značky RFID podporují protokoly pro ověření operace čtení, útočníci mohou snadno číst obsah značek RFID (i z velkých vzdáleností), aniž by zanechali stopu. [27]

4.3.2 Tag Modification (úprava údajů tagu).

Vzhledem k tomu, že většina RFID tagů, které jsou dnes rozšířené, využívá zapisovatelnou uživatelskou paměť, může útočník tuto možnost využít k úpravě nebo vymazání cenných informací. Je třeba si uvědomit, že snadnost, s jakou může být takový útok proveden, je velmi závislá na používaném standardu a použité ochraně READ/WRITE. [27]

4.3.3 Middleware Attacks (útok na Middlwware)

Buffer Overflows (Přetečení vyrovnávací paměti). Přetečení vyrovnávací paměti představuje jednu z hlavních hrozeb a patří k největším bezpečnostním problémům v softwaru. Přetečení vyrovnávací paměti využívá data úložiště nebo kód mimo meze vyrovnávací paměti s pevnou délkou. Útočníci mohou použít tagy RFID k zahájení přetečení vyrovnávací paměti na back-end RFID middlewaru. I když to nemusí být triviální vzhledem k paměťovému ukládání RFID tagů, stále existují příkazy, které umožňují, aby RFID tag opakovaně odesílal stejný datový blok, aby došlo k přetečení vyrovnávací paměti v middleware RFID. Další možnosti zahrnují použití dalších zařízení s více zdroji, jako jsou čipové karty nebo zařízení, která jsou schopna napodobit více RFID tagů nebo pomocí tagu s větší pamětí, než je očekávaná. [34]

Malicious Code Injection (Injekce škodlivého kódu). RFID tagy mohou být použity k šíření nepřátelského kódu, který by následně mohl infikovat jiné subjekty sítě RFID (čtečky a propojovací sítě). V tomto scénáři útočník používá paměťový prostor značek RFID k uložení a šíření virů. Ačkoli tento typ útoků není široce rozšířený, laboratorní experimenty ukázaly, že jsou proveditelné.

Vzhledem k tomu, že middleware aplikace používají více skriptovacích jazyků, jako je Javascript, PHP, XML atd., může útočník tuto možnost využít a vložit škodlivý kód, který ohrozí middleware systémy. Konkrétněji mohou být RFID tagy použity ke vložení kódu do RFID aplikací, které používají webové protokoly a zachycují skriptovací jazyky. Stejným způsobem lze také provádět SQL vložení, speciální útok na vkládání kódu založený na nečekaných příkazech SQL, které mohou vést k neoprávněnému přístupu k databázím back-end a následně odhalit nebo dokonce změnit data uložená v back-end RFID Middleware. [34]

4.3.4 Obrana proti útokům na aplikační úrovni

Abychom se mohli bránit před neoprávněným čtením a úpravou tagů, měli bychom se zaměřit na kontrolu přístupu k RFID tagům. Jedním z navrhovaných postupů je použití hliníkových peněženek na ochranu platebních karet RFID a ochranu proti neoprávněnému čtení. Mnoho společností toto řešení přijalo a prodávalo tento typ výrobků. Nicméně v okamžiku skutečného používání je karta mimo tohle pouzdro a může být provedeno čtení důvěrných údajů. Šifrovací techniky, autentizační protokoly nebo seznamy řízení přístupu mohou poskytnout alternativní a lepší řešení. Konkrétně byly navrženy přístupy založené na šifrování symetrického klíče, šifrování veřejného klíče, funkce hash, vzájemná autentizace nebo dokonce nekryptografické řešení, jako jsou pseudonymy. Důležitým omezením využívání těchto schémat v systémech RFID je však to, že tyto systémy mají přirozené zranitelnosti, jako jsou možné přerušení napájení nebo narušení bezdrátových kanálů.

S přetečením vyrovnávacích pamětí a zaváděním škodlivého kódu v middleware lze bojovat s jednoduchými protiopatřeními. Prováděním pravidelné kontroly kódu, aby se zajistila bezpečnost systému proti zranitelnosti a chybám. U databází pomůže použití nejmenších možných oprávnění k zabezpečení systému. Dále vypnutí nepotřebných funkcí middleware, jako je back-end skriptování, podporuje integritu systému. Dalšími jednoduchými opatřeními je izolace middleware serveru RFID tak, že v případě, že je ohrožen, nebude poskyt-

nut přístup do zbytku sítě, kontrola vstupních dat middleware RFID a odstranění zvláštních a podezřelých znaků. [27]

4.4 Útok na strategické úrovni (Strategic layer)

Tato úroveň zahrnuje útoky, které cílí na organizaci a podnikové aplikace, a využívají tak bezstarostný návrh infrastruktury a aplikací. Konkrétně jde o konkurenční špionáž, sociální inženýrství, soukromí a cílené bezpečnostní hrozby. [27]

4.4.1 Konkurenční špionáž

Útočníci často mají jako cíl své obchodní nebo průmyslové konkurenty. Využívají schopnost sledovat a detekovat označené položky, mohou shromažďovat kritické a důvěrné informace, k sabotování svých konkurentů. Tyto informace mohou zahrnovat strategie a postupy týkající se změny cen, plánů výroby nebo marketingových scénářů. Takovýchto útoků lze dosáhnout odposloucháním nebo získáním neautorizovaného přístupu k databázím back-end atd. [27]

4.4.2 Sociální inženýrství

Útočník může dokonce využít dovednosti sociálního inženýrství k ohrožení systému RFID a získání neoprávněného přístupu k důvěrným místům nebo informacím. Místo toho, aby procházel náročným procesem hackování/prolomení komunikace RFID, útočník jednoduše použije důvěryhodný trik k manipulaci s lidmi, aby odhalili důvěrné informace. Útočník může využít jednoduchých činů lidské laskavosti, jako je podržení otevřených dveří (načež je možné vstoupit bez RFID karty, do jinak zakázané oblasti) nebo půjčení RFID karty (načež je možné získat všechny její důvěrné informace). [27]

4.4.3 Ohrožení soukromí

RFID štítky reagují na libovolnou čtečku, autorizovanou nebo neautorizovanou, aniž by o tom informovali své majitele. Tuto funkci mohou útočníci zneužít ke sledování a profilování jednotlivce. Potenciální shromažďování osobních informací od nákupních návyků až po lékařské informace je jedním z největších rizik v systémech RFID a vedlo k nárůstu kampaní proti využívání RFID. [35]

4.4.4 Cílené bezpečnostní hrozby

Protivník může použít informace shromážděné sdružením nebo lokalizační hrozbou ke spuštění škodlivé události a/nebo fyzického nebo elektronického útoku. Typickým příkladem tohoto útoku je zaměřování a okradení lidí, kteří shromažďují cenné předměty (např. hodinky nebo šperky) nebo lodě, které nesou cenné nebo kritické položky. [27]

4.4.5 Obrana proti útokům na strategické úrovni

Útoky na tuto úroveň je možné bránit pomocí opatření používaných v obraně ostatních úrovní. Přesněji, pro ohrožení soukromí a cílené bezpečnostní hrozby byla navržena široká škála technických řešení, včetně „usmrcení“ nebo dočasného vypnutí tagů, blokování přístupu k neautorizovaným čtečkám, používání pseudonym, měření vzdálenosti a šifrovacích technik.

Nicméně abychom efektivně čelili strategickým hrozbám, musíme je konfrontovat jako problém, který vyžaduje dlouhodobé úsilí. Společnosti a organizace, které používají systémy RFID, by měly zavést a udržovat politiku ochrany soukromí a údajů a provádět hodnocení rizik s cílem definovat hrozby a rizika spojená s využívanou RFID infrastrukturou. Je důležité obdržet pokyny od důvěrníka pro ochranu soukromí a právního poradce týkajícího se přijatých strategických scénářů a otázek souvisejících s ochranou soukromí. Bezpečnostní politika by měla být přiměřeně oznámena všem zaměstnancům. Neustálé školení a vzdělávání zaměstnanců organizace v oblasti bezpečnosti a ochrany osobních údajů v oblasti RFID je nezbytné, neboť podporuje informovanost a dohled nad kritickými informacemi.

Otázky ochrany soukromí související s komunikací pomocí RFID by měly být také předmětem pozornosti zákonodárců a orgánů, které mohou poskytnout pokyny, které by měly následovat organizace a společnosti, které používají systémy RFID. [27]

4.5 Víceúrovňové útoky (Multilayer attacks)

Mnoho útoků zaměřených na komunikaci RFID není omezeno pouze na jednu úroveň. V této kategorii jsou zahrnuty útoky, které postihují více úrovní včetně fyzické, přenosové, aplikační a strategické úrovně. Jde zejména o skryté kanály, odmítnutí přístupu, analýza provozu, kryptografické útoky a útok na postranní kanály. [27]

4.5.1 Skryté kanály

Útočníci mohou využívat RFID tagy k vytvoření neoprávněných komunikačních kanálů pro tajné přenášení informací. Útočníci mohou využívat nevyužitou paměť více RFID tagů ke skrytému přenášení dat způsobem, který je obtížně rozpoznatelný. Například sada RFID štítků implantovaných do lidských těl, jejichž normálním účelem je identifikace osoby, může tajně hlásit soukromé informace týkající se lékařských dat nebo společenských aktivit. [36]

4.5.2 Denial od Service Attack (Odmítnutí přístupu)

Normální provoz RFID tagů může být přerušen záměrným blokováním přístupu. Záměrné blokování přístupu a následné odmítnutí služby pro RFID tagy může být způsobeno škodlivým používáním "blokovacích tagů" nebo použitím tzv. TFID guardianu. Oba přístupy byly navrženy k zabezpečení komunikace RFID proti ohrožení soukromí. Nicméně, mohli by být také použity útočníky k úmyslnému odmítnutí přístupu. Dalším způsobem odmítnutí služby je neoprávněné použití příkazů LOCK. Příkazy LOCK jsou zahrnuty v několika normách RFID, aby se zabránilo neoprávněnému zapisování do paměti RFID tagů. V závislosti na použitém standardu je příkaz LOCK aplikován předdefinovaným heslem a může mít trvalé nebo dočasné efekty. Navíc, jelikož middleware RFID obsahuje síťová zařízení, může útočník využít omezených zdrojů systému a způsobit odmítnutí služby v middlewaru RFID. Například posílání streamu paketů do middleware, takže síť nebo zpracovatelská kapacita je zaplavena a následně popírá přístup k běžným klientům. [36]

4.5.3 Analýza provozu

Komunikace pomocí RFID je také náchylná k útokům na analýzu provozu. Odposlouchávatel je schopen zachytit zprávy a získat informace z komunikačního kanálu. I když je komunikace RFID chráněna šifrovacími a ověřovacími technikami, je stále citlivá na útoky na analýzu provozu. Čím větší počet zpráv je zachycen, tím efektivnější bude tento útok. [27]

4.5.4 Kryptografické útoky

Když jsou důležité informace uloženy na RFID tazích, používají se šifrovací techniky, aby byla zachována celistvost a důvěrnost chráněných dat. Odhodlaný útočník pak používá šifrovací útoky k prolomení použitých kryptografických algoritmů a odhalení nebo manipu-

laci s citlivými informacemi. Například v Holandsku bezpečnostní firma s názvem Riscure prokázala, že klíč použitý v holandském cestovním pasu lze snadno rozluštit pomocí standardního PC, který provádí útok hrubou silou po dobu dvou hodin. [37]

4.5.5 Útok na postranní kanály

Útoky po postranních kanálech využívají fyzické implementace kryptografického algoritmu spíše než jeho teoretické zranitelnosti. Tento druhu útoků obvykle využívá informace o časování, spotřebě energie nebo dokonce elektromagnetické pole. Účinné nasazení útoků postranních kanálů vyžaduje hluboké znalosti vnitřního systému, na kterém jsou implementovány kryptografické algoritmy. Časové útoky jsou prováděny zkoumáním kolísání rychlosti výpočtu, zatímco jednoduchá analýza výkonu zachycuje informace o výkonech na základě změn spotřeby energie. Diferenciální analýza je speciální typ útoků, který je založen na elektromagnetických změnách vytvořených například během komunikace mezi čtečkou RFID a značkou. Přesněji, varianty elektromagnetického pole, kdy RFID tag provádí šifrovací operaci, mohou být použity k odhalení tajných kryptografických klíčů.

Například německým vývojářům se podařilo prolomit šifrovací algoritmus, který se používá na bezkontaktních kartách Mifare DESFire. Doposud byly tyto karty považovány za bezpečné, jelikož dříve nebyla zveřejněná hrozba, která by dovolovala ohrozit obsah karty či jej zkopírovat. Vědcům z německé University Ruhr se podařilo klíče z karty dostat za sedm hodin s vybavením asi za 50 tisíc korun. Celý útok je založen na technice postranních kanálů, kdy je sledováno elektromagnetické pole kolem karty, podle kterého jsou následně odhadnuty pochody uvnitř šifrovacího čipu. [27]

4.5.6 Útok replay

Běžným obranným mechanizmem k útokům, je použití protokolu reakce na výzvu. RFID tagy a čtečky obvykle používají protokol výzva-odpověď k ověření jejich totožnosti. Přesto je tento přístup velmi často vystaven útokům replay. Při replay útoku vysílá útočník odpověď tagu, která byla zaznamenána z minulé transakce pro imitování validního tagu pro čtečku. Typickým příkladem tohoto útoku je neoprávněný přístup do vyhrazených oblastí vysláním přesného záznamu rádiového signálu odeslaného z legitimního tagu čtečce, která udělí přístup. [27]

4.5.7 Obrana proti víceúrovňovým útokům

Útoky skrytých kanálů je velmi těžké odhalit a bránit. Majitelé a uživatelé RFID tagů nemají žádnou informaci o tom, že jejich tagy byly ohroženy a že se používají k útokům skrytých kanálů. Odstraňování těchto útoků je otevřenou otázkou výzkumu. Nicméně možný mechanismus, který by měl proti nim bojovat, by se měl zaměřit na snížení dostupnosti paměťových prostředků v RFID tagu (např. vymazání nevyužité paměti každých pár sekund nebo náhodného kódu a umístění dat).

Denial of Service útoky a analýza provozu jsou závažnými bezpečnostními hrozbami ve všech typech sítí, včetně kabelových. Zatímco teoreticky mohou být tyto typy útoků potírány, nedostatečné zdroje RFID tagů činí jejich obranu problematickou a zůstávají otevřeným problémem výzkumu. Kryptografické útoky mohou být eliminovány použitím silných kryptografických algoritmů po otevřených kryptografických standardech a použitím klíče s dostatečnou délkou. Mohou se proto vyhnout případům, jako je odhalení bezpečnostních chyb Mifare smart card. Útoky postranních kanálů lze chránit tím, že se omezí elektromagnetické emise systému. Nicméně toto obvykle znamená omezení provozního rozsahu.

Za účelem ochrany RFID před replay útoky existují některá jednoduchá protiopatření, jako je použití časových značek, jednorázových hesel a kryptografické výzvy. Nicméně tyto systémy jsou nepohodlné a s pochybnou účinností vzhledem k zranitelnosti, vůči nimž jsou protokoly citlivé. Dalším přístupem je použití RF stínění na čtecích zařízeních k omezení směrovosti rádiových signálů. Jiný přístup je založen na vzdálenosti mezi žadatelem o informace a vlastníkem informací. Poměr signálu k šumu čtecího signálu v systému RFID dokáže dokonce odhalit vzdálenost mezi čtečkou a tagem. Tyto informace je možné použít k rozlišení mezi autorizovanými a neautorizovanými čtečkami nebo tagy a následnému zmírnění útoků replay. [27]

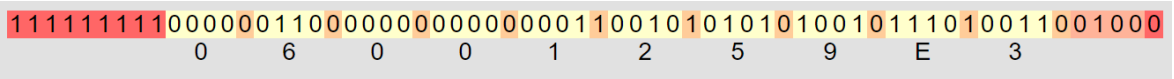
5 ZABEZPEČENÍ A SLABINY VYBRANÝCH TECHNOLOGIÍ

5.1 EM 4200

V současnosti lze tyto karty velmi jednoduše zkopírovat pomocí zařízení, které není nijak vysoce nákladné. Při kopírování karty dochází k přečtení čísla a zapsání do jiné karty. Nová karta se pak v systému ACS tváří jako originální. Kopii lze rozeznat pouze podle fyzického prozkoumání média – karty, přívěsku apod. Tato technologie pracuje na frekvenci 125kHz. [38]

5.1.1 Komunikace EM 4200

Po vložení do elektromagnetického pole RFID čtečky, začne tag vysílat data. Prvních 9 bitů je logická 1. Tyto bity se používají jako pro označení začátku řetězce. Tato sekvence 9 jedniček se pak nevyskytne v žádné jiné části řetězce, díky tomu, že se zde využívá sudá parita. Následuje 10 skupin po 4b s daty a 1 sudým paritním bitem. Nakonec se posílají 4 paritní bity a jeden stop bit (0). Tag pak pokračuje v opakování tohoto řetězce, do té doby než mu dojde energie. [38]



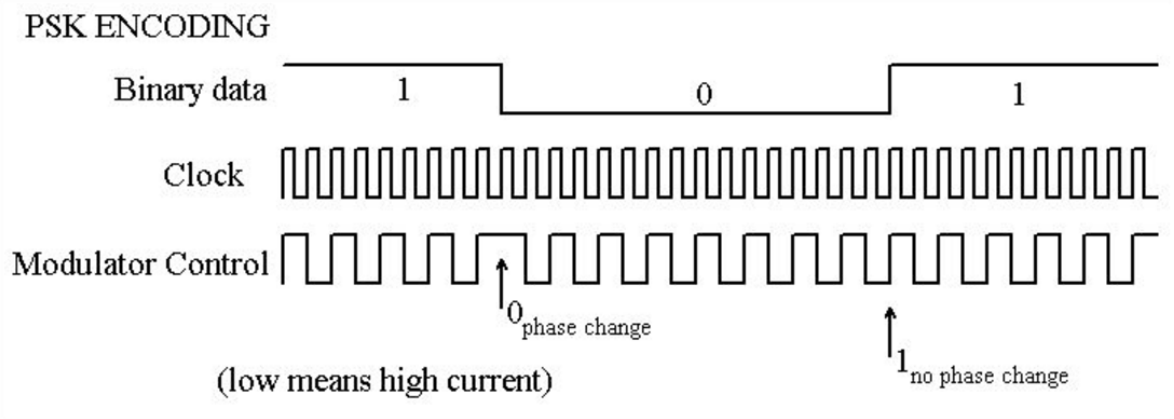
Obr. 20 Příklad posílaného řetězce [38]

5.1.2 Modulace dat

Pro modulování signálu mezi tagem a čtečkou se u EM 4200 nejčastěji používá modulace PSK – Phase Shift Keying.

PSK modulace

Pomocí PSK modulace, je RF pole je upraveno tak, aby došlo k přechodu s každým hodinovým signálem. To znamená, že každých 64, 32 nebo 16bitů v závislosti na délce bitů, které tag používá, může dojít ke změně fáze. Dojde-li ke změně fáze, objeví se na výstupu 0, pokud se nezmění, zůstává 1. [38]



Obr. 21 PSK modulace [38]

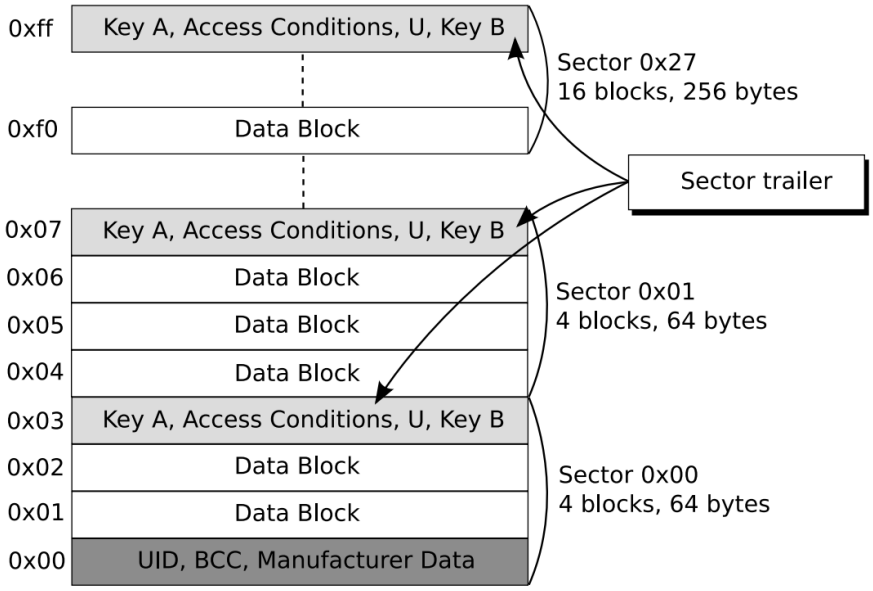
5.2 MiFare Classic

S více než miliardou prodaných karet pokrývá Mifare Classic více než 70% trhu bezkontaktních čipových karet. Mifare Classic splňuje požadavky částí 1 až 3 normy ISO 14443A, které specifikují fyzikální vlastnosti, rádiové rozhraní a protokol proti kolizím. Mifare Classic neimplementuje část 4 normy, která popisuje přenosový protokol, ale místo toho používá svou vlastní zabezpečenou komunikační vrstvu. V této vrstvě Mifare Classic používá proudovou šifru CRYPTO1, která zajišťuje důvěrnost dat a vzájemnou autentizaci mezi kartou a čtečkou. Tato šifra byla nedávno překonána pomocí reverzního inženýrství. [25]

5.2.1 Datová struktura karty MiFare Classic

Značka Mifare Classic je v podstatě paměťový čip se zabezpečenou bezdrátovou komunikační schopností. Paměť tagu je rozdělena do sektorů, z nichž každá je dále rozdělena na bloky šestnácti bajtů. V posledním bloku každého sektoru jsou uloženy dva tajné klíče a přístupové podmínky pro tento sektor.

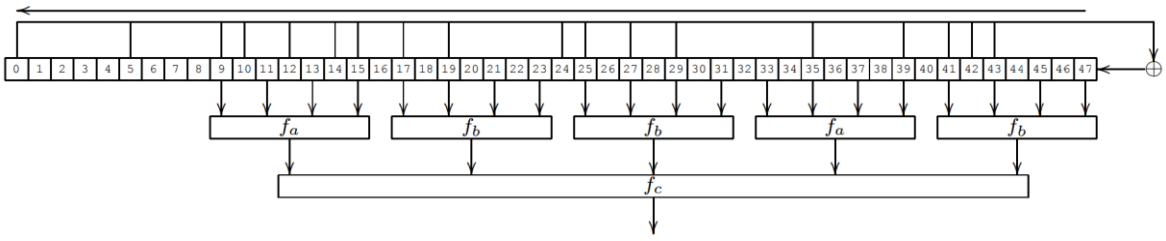
Chcete-li provést operaci na určitém bloku, čtečka musí nejprve autentikovat sektor, který tento blok obsahuje. Podmínky přístupu určují, který z obou klíčů musí být použit. [25]



Obr. 22 Rozložení paměti MaFare Classic [25]

5.2.2 KRYPTO1

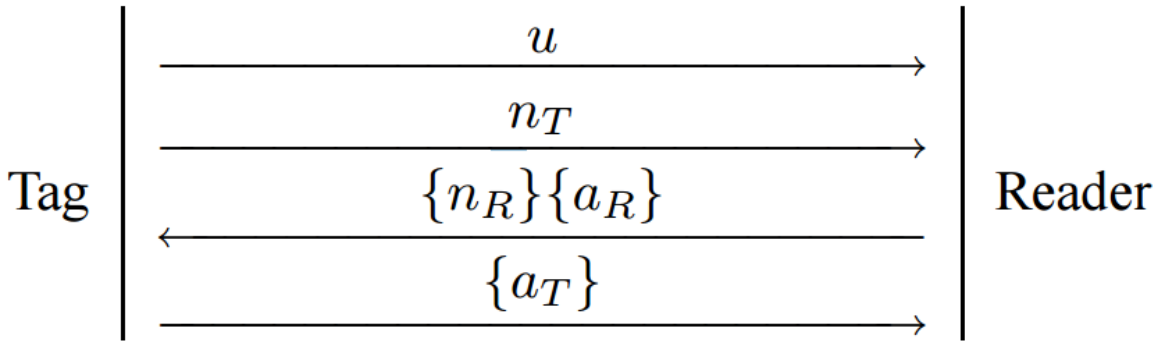
Po ověření je komunikace mezi tagem a čtečkou zašifrována proudovou šifrou CRYPTO1. Tato šifra se skládá ze 48-bitového posuvného registru s lineární zpětnou vazbou s generujícím polynomem $x^{48} + x^{43} + x^{39} + x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{29} + x^{24} + x^{23} + x^{21} + x^{19} + x^{13} + x^{9} + x^{7} + x^{6} + x^{5} + 1$ a nelineární filtrační funkcí f. S každým tiknutím hodin je dvacet bitů registru posunuto přes filtrační funkci, čímž se generuje jeden bit klíče. Potom registr posune jeden bit doleva a pomocí generujícího polynomu vygeneruje nový bit vpravo. [25]



Obr. 23 struktura proudové šifry KRYPTO1[25]

5.2.3 Autentizační protokol a inicializace

Během anti-kolizní fáze vysílá tag své UID ke čtečce. Čtečka pak požádá o ověření pro určitý sektor. Tag odesílá dotaz n_T. Od tohoto okamžiku je komunikace zašifrována. Čtečka reaguje svým vlastním dotazem n_R a odpovědí $a_R := suc^{64}(n_T)$ na dotaz tagu; tato výměna končí odpovědí tagu $a_T := suc96(n_T)$. [25]



Obr. 24 Autentizační protocol MiFare Classic [25]

5.2.4 Slabiny MiFare Classic

Mezi hlavní slabiny MiFare Classic patří paritní bity a vnořené autentizace.

Paritní bity

Standard ISO 14443-A specifikuje, že každý odeslaný byte je následován paritním bitem. Mifare Classic vypočítává paritní bity nad prostým textem místo nad zašifrovaným textem. Dále bit kódu, používaný k šifrování paritních bitů, se znovu použije k šifrování dalšího bitu prostého textu. Toto narušuje důvěryhodnost šifrovacího schématu.

Existuje ještě další slabost týkající se paritních bitů. Během ověřovacího protokolu, když čtečka odešle $\{n_R\}$ a $\{a_R\}$, tag zkontroluje paritní bity ještě před odpovědí čtečky. Pokud je alespoň jeden z osmi paritních bitů špatný, tag neodpovídá. Je-li všech osm bitů parity správných, ale odpověď a_R je nesprávná, tag odpoví 4bitovým chybovým kódem 0x5, který oznamuje neúspěšnou autentizaci (chyba přenosu). Je-li všech osm paritních bitů správných a odpověď a_R je také správná, tag samozřejmě reaguje na odpověď a_T. Dále v případě, že čtečka odešle správnou paritu, ale špatnou odpověď, je 4bitový chybový kód 0x5 odeslán zašifrovaně. K tomu dochází, i když se čtečka sama neověřila, a proto nelze předpokládat, že je schopna zprávu dešifrovat. [25]

Vnořené autentizace

V Mifare Classic, existuje slabina, která dovoluje útočníkovy získat další klíče, jakmile zná jeden sektorový klíč. Pokud čtečka již komunikuje (zašifrovaně) s tagem, musí být následující příkaz pro nový sektor zaslán také zašifrovaně. Po tomto ověření je vnitřní stav šifry nastaven na klíč pro nový sektor a autentizační protokol se znovu spustí. Tentokrát se však

dotaz tagu také posílá zašifrovaně. Protože existuje pouze 2^{16} možností, může se útočník jednoduše pokusit odhadnout a objevit všech 32 bitů klíče.

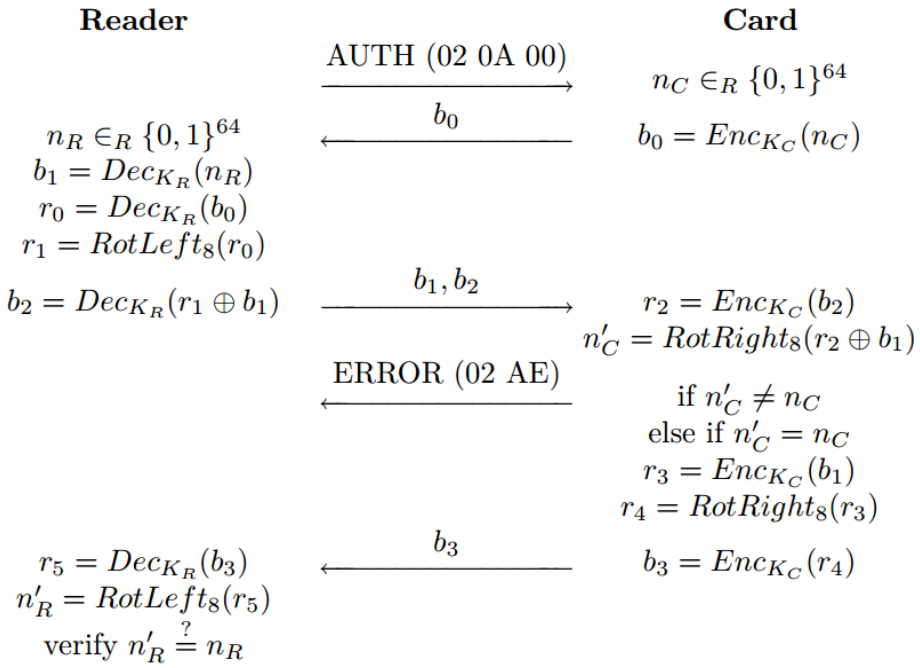
Informace které unikají pomocí paritních bytů, zde lze použít k urychlení útoku. [25]

5.3 Mifare DESFire a DESFire EV1

Karty Mifare DESFire a Mifare DESFire EV1 vyhovují částem 1 až 4 normy ISO 14443A. Jejich UID je sedm bajtů dlouhé a podporuje vysokou přenosovou rychlost až 848 kBit/s. Komunikace s kartou může být pomocí otevřené MAC funkce nebo pomocí úplného šifrování dat. Karty MiFare DESFire nabízejí 4 kByte uložiště a šifrování dat pomocí hardwarové šifry DES a 3DES. Karty Mifare DESFire EV1 navíc poskytují šifrování dat pomocí AES-128 a jsou prodávány ve třech variantách s pamětí 2 kByte, 4 kByte a 8 kByte. Každá karta obsahuje až 28 různých aplikací s až 14 různými klíči za aplikaci. Pro DESFire může každá aplikace obsahovat až 16 souborů, zatímco u DESFire EV1 je maximální počet souborů 32. [26]

5.3.1 Autentizační protokol a inicializace

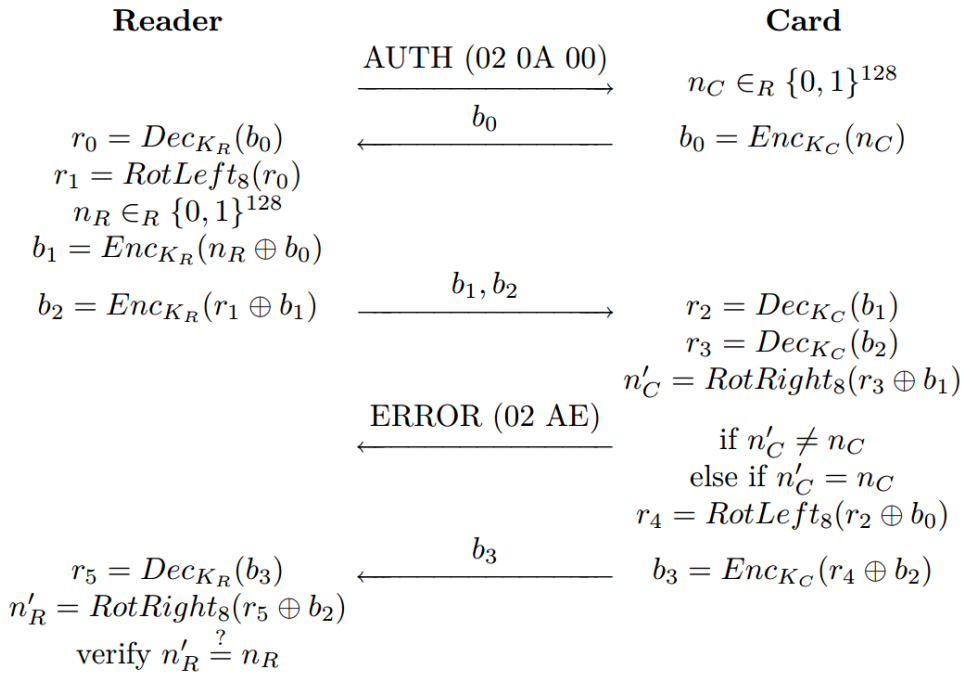
Stejně jako u karet Mifare Classic je UID v době výroby bezprostředně naprogramován do karty. V závislosti na přístupových právech pro každou aplikaci musí být před čtením a manipulací s údaji dokončen protokol vzájemného ověřování, který zajišťuje shodu symetrického klíče karty a čtečky.



Obr. 25 Autentizační protokol MiFare DESFire [26]

Před autentizací je vybrána aplikace reprezentovaná identifikátorem aplikace. Čtečka spustí autentizační protokol, pomocí příkazu authenticate spolu s klíčovým číslem, které má být použito při autentizaci. Pozor na to, že karty Mifare DESFire provádějí pouze (3)DES šifrování $E_{ncK}(\cdot)$, které používají tajný klíč K, proto čtecí zařízení DESFire vždy musí používat dekódování (3)DES $D_{ecK}(\cdot)$.

Karta DESFire reaguje na ověřovací příkaz se šifrovaným 64bitovým náhodným n_C. Čtečka také zvolí 64bitovou náhodné n_R, dešifruje přijaté n_C, otáčí je o osm bitů nalevo a dešifruje n_R stejně jako otočené n_C. Karta ověřuje, zda se otočená hodnota rovná n_C po obnovení otočení. Pokud tomu tak je, karta zašifruje první hodnotu pro získání n_R, otočí ji o osm bitů napravo a zašifruje výsledek, který pak bude odeslán čtečce. Otočené a šifrované číslo pak ověřuje čtečka, pokud je tento konečný krok úspěšný, obě strany jsou vzájemně ověřené.



Obr. 26 Autentizační protokol MiFare DESFire EV1[26]

5.3.2 Zabezpečení MiFare DESFire / EV1

Neinvazivní útoky na postranní kanály na zařízeních RFID, umožňují extrahovat tajné informace z bezdotykových karet měřením elektromagnetických vyzařování karty, během provádění kryptografické operace. Důraz je kladen na zařízení, která využívají DES nebo 3DES, a první úspěšný útok k získání klíčů na takových zařízeních byl uskutečněn německými vývojáři. Autoři tohoto útoky tvrdí, že útoky byly od té doby vylepšeny a jsou použitelné pro karty Mifare DESFire. S přibližně 1 000 000 měřeními jsou plně schopni obnovit klíč 3DES uložený na kartě Mifare DESFire. Útok po postranních kanálech se v současné době nevztahuje na DESFire EV1, který byl certifikován podle Common Criteria EAL 4+. Účinné útoky však mohou v budoucnu přicházet, nebo by se klíč mohl získat jinými prostředky, např. využitím slabých míst systému backend. [26]

6 BEZPEČNOST VYBRANÝCH RFID TAGŮ

Abychom byli schopni mezi sebou porovnat jednotlivé RFID technologie, musíme si nejprve vymezit kritéria, podle kterých je budeme hodnotit.

6.1 Vymezení kriterií hodnocení

U hodnocení RFID tagů nemůžeme pomýšlet jenom na jejich zabezpečení, ale také na jejich další vlastnosti.

Vlastnosti, které budeme posuzovat, jsou:

- kryptografické zabezpečení,
- rychlost komunikace,
- délka uchování dat,
- čtecí vzdálenost,
- komplexnost,
- ekonomičnost.

6.2 Hodnocení RFID technologií

Kritéria budeme hodnotit na stupnici od 1 do 10, kdy vyšší hodnoty znamenají lepší vlastnosti.

- **kryptografické zabezpečení** – hodnotíme podle rychlosti útoků. Pokud tag není nijak zabezpečený, dostane hodnotu 0, pokud ještě nebyl překonán, dostane hodnotu 10. Ostatní ohodnotíme podle doby potřebné k vykonání úspěšného útoku,
- **rychlost komunikace** – tagy budeme hodnotit podle rychlosti komunikace. Čím rychlejší tím vetší ohodnocení,
- **délku uchování dat** – hodnotíme podle doby uchování údajů na čipu. Občanské průkazy jsou většinou vydávány s platností 10 let. Tagy, které dokážou uchovat data minimálně dvojnásobnou dobu, nebo déle dostanou hodnotu 10, ostatní poměrně menší hodnotu,

- **čtecí vzdálenost** – u čtecí vzdálenosti budeme hodnotit menší pracovní vzdálenost jako bezpečnější,
- **komplexnost** – komplexností, myslíme možnost využití tagu na více aplikací zároveň. Čím více možných aplikací, tím větší ohodnocení,
- **ekonomičnost** – poslední faktorem, který budeme hodnotit je cena. Čím levnější je tag, tím větší dostane ohodnocení.

	Kryptografické zabezpečení	rychlost komunikace	délka uchování dat	čtecí vzdálenost	komplexnost	ekonomičnost
EM 4200	0	8	5	5	1	10
EM 4333	3	8	10	5	1	9
NTAG 413 DNA	4	7	10	8	1	6
MiFare Classic	6	7	5	8	3	8
MiFare DESFire EV1	10	6	5	8	6	5
SmartMX2	9	7	10	8	8	6
ATC1024	9	7	5	3	6	6

Tab. 3 Vstupní tabulka hodnocení jednotlivých RFID čipů

Dále je potřeba určit váhu jednotlivých kritérií.

Pro určení kritérií použijeme metodu stanovení preferenčního pořadí kriterií. Tato metoda určuje hodnotu významnosti kriterií od nejvýznamnějšího až k nejméně významnému.

Pro stanovení nenormované váhy se uplatňuje vztah:

$$k_j = n + 1 - p_j$$

k_j – nenormovaná váha kriteria v j sloupci

n – počet kriterií

p_j – pořadí kriteria v j sloupci v jeho preferenčním uspořádání

Dále je třeba tyto váhy normovat (součet normovaných vah souboru kriterií je roven jedné). Normování vah kriterií se provádí podle vztahu:

$$v_j = \frac{k_j}{\sum_{j=1}^{n} k_j}$$

v_j – normovaná váha kriteria v j sloupci

k_j – nenormovaná váha kriteria v *j* sloupci

n – počet kriterií

V tabulce 4 jsou pak uvedeny průměrné hodnoty vah jednotlivých kritérií hodnocení.

	Kryptografické zabezpečení	rychlost komunikace	délka uchování dat	čtecí vzdálenost	komplexnost	ekonomičnost
Váha	0,29	0,24	0,19	0,14	0,1	0,05

Tab. 4 Váhy jednotlivých kritérií

Úlohu budeme řešit dvěma způsoby:

- metodou celkového zisku,
- metodou WSA (Weighted Sum Approach).

6.2.1 Metoda celkového užitku

U této metody nejprve musíme upravit vstupní tabulku hodnocení. To provedeme tak, že na základě bodového hodnocení v rozmezí 1 až 10, přiřadíme variantám hodnotu v rozmezí 0 až 1.

	Kryptografické zabezpečení	rychlost komunikace	délka uchování dat	čtecí vzdálenost	komplexnost	ekonomičnost
EM 4200	0,0	0,8	0,5	0,5	0,1	1,0
EM 4333	0,3	0,8	1,0	0,5	0,1	0,9
NTAG 413 DNA	0,4	0,7	1,0	0,8	0,1	0,6
MiFare Classic	0,6	0,7	0,5	0,8	0,3	0,8
MiFare DESFire EV1	1,0	0,6	0,5	0,8	0,6	0,5
SmartMX2	0,9	0,7	1,0	0,8	0,8	0,6
ATC1024	0,9	0,7	0,5	0,3	0,6	0,6

Tab. 5 Transformovaná tabulka hodnocení

Nyní můžeme použít následující vzorec:

$$U(a_i) = \sum_{j=1}^{n} u_{ij} \cdot v_j$$

$U(a_i)$ – celkový užitek varianty v *i* řádku

v_j – normovaná váha kriteria v *j* sloupci

u_{ij} – normalizovaný prvek v *i* řádku a *j* sloupci

V následující tabulce je pak provedeno vyhodnocení podle metody celkového užitku.

SmartMX2	0,841
MiFare DESFire EV1	0,726
ATC1024	0,656
NTAG 413 DNA	0,626
MiFare Classic	0,619
EM 4333	0,594
EM 4200	0,417

Tab. 6 Hodnocení pomocí metody celkového užitku

Varianta, která dosáhne nejvyšší hodnoty celkového užitku $U(a_i)$ je metodou vyhodnocena jako nejlepší.

6.2.2 Metoda WSA

principem této metody je maximalizace užitku variant váhami ohodnocených kritérií.

Určíme ideální varianty H a bazální varianty D ze vstupní tabulky hodnocení.

	Kryptografické zabezpečení	**rychlost komunikace**	**délka uchování dat**	**čtecí vzdálenost**	**komplexnost**	**ekonomičnost**
Ideální varianta	10	8	10	8	8	10
Bazální varianta	0	6	5	3	1	5

Tab. 7 Ideální a bazální varianta vstupní tabulky hodnocení

Dále transformujeme vstupní tabulku hodnocení podle následujícího vzorce:

$$r_{ij} = \frac{y_{ij} - D_j}{H_j - D_j}$$

rij – normalizovaný prvek v i řádku a j sloupci

yij – prvek v i řádku a j sloupci

Dj – bazální varianta j prvku

Hj – ideální varianta j prvku

	Kryptografické zabezpečení	rychlost komunikace	délka uchování dat	čtecí vzdálenost	komplexnost	ekonomičnost
EM 4200	0,000	1,000	0,000	0,400	0,000	1,000
EM 4333	0,300	1,000	1,000	0,400	0,000	0,800
NTAG 413 DNA	0,400	0,500	1,000	1,000	0,000	0,200
MiFare Classic	0,600	0,500	0,000	1,000	0,286	0,600
MiFare DESFire EV1	1,000	0,000	0,000	1,000	0,714	0,200
SmartMX2	0,900	0,500	1,000	1,000	1,000	0,200
ATC1024	0,900	0,500	0,000	0,000	0,714	0,200

Tab. 8 Transformovaná normalizovaná vstupní tabulka hodnocení

Nyní vypočítáme vážený užitek varianty a_i dle vztahu:

$$u(a_i) = \sum_{j=1}^{n} v_j . r_{ij}$$

$u(a_i)$ – užitek varianty v *i* řádku

v_j – normovaná váha kriteria v *j* sloupci

r_{ij} – normalizovaný prvek v *i* řádku a *j* sloupci

SmartMX2	0,821
EM 4333	0,613
NTAG 413 DNA	0,576
MiFare DESFire EV1	0,501
MiFare Classic	0,493
ATC1024	0,462
EM 4200	0,346

Tab. 9 Hodnocení pomocí metody WSA

Varianta, která dosáhne nejvyšší hodnoty celkového užitku $u(a_i)$ je metodou vyhodnocena jako nejlepší.

6.3 Dílčí závěr

Nejlepší variantou by pak byla taková, která by získala hodnotu rovnou 1. Vliv na výsledek celého výpočtu pak mají zejména hodnoty vstupní tabulky hodnocení

	Metoda celkového užitku	Metoda WSA
SmartMX2	0,841	0,821
MiFare DESFire EV1	0,726	0,501
ATC1024	0,656	0,462
NTAG 413 DNA	0,626	0,576
MiFare Classic	0,619	0,493
EM 4333	0,594	0,613
EM 4200	0,417	0,346

Tab. 10 Porovnání výsledků jednotlivých metod

Jak znázorňuje tabulka 10, použité metody (celkového užitku a WSA) se v pořadí jednotlivých variant více či méně shodují. Jako nejbezpečnější technologie pak byla vyhodnocena SmartMX2.

ZÁVĚR

Cílem této práce bylo seznámení se z RFID systémy a jejich využitím v oblasti identifikace osob. Byly prostudovány stávající RFID technologie používané pro osobní identifikaci. Dále byl popsán princip fungování RFID technologií a jejich základní dělení.

V práci jsou představeny dostupné RFID tagy, které se používají k identifikaci. Dále bylo popsáno zabezpečení identifikačních dokladů.

Praktická část se zaměřuje na přehled možných útoků na tyto technologie a na možné způsoby ochrany proti těmto útokům. Byly prostudovány útoky na všechny možné úrovně RFID systému, ve všech fázích použití.

V závěru práce je vypracováno hodnocení uvedených technologií s ohledem na jejich zabezpečení. Z tohoto hodnocení vyplývá, že karty fungující na frekvenci 125kHz, které jsou dnes běžně používané například jako studentské karty, nejsou nijak zabezpečeny a jejich zkopírování je jen otázkou několika vteřin. Na druhou stranu tagy, jako jsou MiFare DESFire EV1 a SmartMX2, mají docela silná zabezpečení, které se zatím nepodařilo prolomit. Tyto tagy jsou teda vhodné pro použití ve státních aplikacích, jako je například elektronický občanský průkaz.

V současnosti nejbezpečnější RFID technologie, však nemusí být bezpečné navždy. Je jen otázkou času, kdy dojde k objevení metody, které překoná pokročilé metody šifrování. Je ale potřeba doufat, že s příchodem nových technologií, dojde i k objevení nových lepších kryptografických metod, které mohou zaručit dočasnou, či snad trvalou ochranu identifikačních technologií.

Vzhledem k tomu, že lidstvo spěje k maximálnímu zjednodušení života, se dá předpokládat nasazení RFID čipu pevně umístněného do lidského těla. Tady ovšem vyvstává velká filozofická otázka, jestli je vážně potřebné a žádoucí takto permanentně značit lidi. I když to zní jako sci-fi myšlenka, už dnes je toho technologicky možné dosáhnout.

SEZNAM POUŽITÉ LITERATURY

[1] *The History of RFID technology* [online]. [cit. 2015-02-04]. Dostupné z: http://www.rfidjournal.com/articles/view?1338

[2] HUNT, V, Albert PUGLIA a Mike PUGLIA. *RFID: a guide to radio frequency identification*. Hoboken, N.J.: Wiley-Interscience, 2007, xxiv, 214 p. ISBN 978-047-0107-645. D

[3] JUŘÍK, Pavel. *Platební karty: ilustrovaná historie placení*. 1. vyd. Praha: Libri, 2012, 204 s. ISBN 978-807-2774-982.

[4] *Cestovní doklady s biometrickými prvky* [online]. [cit. 2015-05-21]. Dostupné z: http://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx?q=Y2hudW09MQ%3d%3d

[5] 7 unexpected and awesome uses of RFID tags. *RFID Arena* [online]. 2014 [cit. 2016-05-18]. Dostupné z: http://rfidarena.com/2014/3/4/7-unexpected-and-awesome-uses-of-rfid-tags.aspx

[6] SPONSORED BY IEEE-USA, the IEEE New Technology Directions Committee and IEEE Region 5. *IEEE RFID 2007 welcome to the first IEEE RFID Conference*. [Piscataway, NJ: IEEE, 2007. ISBN 1424410134.

[7] Používané RFID frekvence a jejich vliv na čtení a zápis tagu. *Automatizace.hw.cz: rady a poslední novinky z oboru* [online]. Praha: Vojáček, 2015 [cit. 2016-05-25]. Dostupné z: http://automatizace.hw.cz/komponenty-prumyslove-sbernice-a-komunikace/vice-i-mene-bezne-rfid-frekvence-a-jejich-vliv-na-vlastnosti-tagu.html

[8] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín, 2013. Scriptum. Univerzita Tomáše Bati Zlín.

[9] EM4200: 128 bit Read Only, Low Frequency Contactless Identification Device. *EM Microelectronic* [online]. [cit. 2017-05-28]. Dostupné z: http://www.emmicroelectronic.com/products/rf-identification-security/lf-animal-access-ics/em4200

[10] HTx2: HITAG 2 transponder IC. *NXP Semiconductors: Automotive, Security, IoT* [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.nxp.com/documents/short_data_sheet/HT2X_SDS.pdf

[11] MIFARE Classic. *NXP Semiconductors: Automotive, Security, IoT* [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.nxp.com/products/identification-and-security/smart-card-ics/mifare-ics/mifare-classic:MC_41863

[12] MIFARE DESFire EV1 4K: MIFARE DESFire EV1 contactless multi-application IC. *NXP Semiconductors: Automotive, Security, IoT* [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.nxp.com/products/identification-and-security/smart-card-ics/mifare-ics/mifare-desfire/mifare-desfire-ev1-contactless-multi-application-ic:MIFARE_DESFIRE_EV1_4K

[13] SmartMX2-P60. *NXP Semiconductors: Automotive, Security, IoT* [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.nxp.com/products/identification-and-security/smart-card-ics/smartmx2-p60:MC_71471

[14] RFID Business Applications. *RFID Journal* [online]. 2005 [cit. 2016-05-25]. Dostupné z: http://www.rfidjournal.com/articles/view?1334/

[15] EOP s čipem: Porovnání realizace v ČR a Německu. *2012.smartcardforum.cz* [online]. Smart Cards & Devices Forum 2012, 2012 [cit. 2016-05-25]. Dostupné z: http://2012.smartcardforum.cz/prezentation/ke_stazeni/01_Rosol.pdf

[16] RFID chips and EU e-passports: the end of privacy? *Conferences.ionio.gr* [online]. [cit. 2016-05-25]. Dostupné z: http://conferences.ionio.gr/icil2012/download.php?f=papers/027-nikita-full_text-en-v001.pdf

[17] Machine Readable Travel Documents: Part 3: Specifications Common to all MRTDs. *International Civil Aviation Organization (ICAO): A United Nations Specialized Agency* [online]. 2015 [cit. 2016-05-25]. Dostupné z: http://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

[18] *RFID Technology, Security Vulnerabilities, and Countermeasures* [online]. 2008 [cit. 2016-05-25]. Dostupné z: http://cdn.intechopen.com/pdfs/6177.pdf

[19] *RFID keyring* [obrázek online]. [cit. 2016-05-26]. Dostupné z: http://www.yxcard.com/en/ShowProducts.asp?id=29

[20] *RFID smart label* [obrázek online]. [cit. 2016-05-26]. Dostupné z: http://www.indianbarcode.com/pimages/387_rfidlabel.jpg

[21] *RFID glass capsule* [obrázek online]. [cit. 2016-05-26]. Dostupné z: https://www.rfidcanada.com/wp-content/uploads/2012/09/Glass-tag3.jpg

[22] *How RFID technology boosts WalMart's supply chain management* [online]. [cit. 2016-05-26]. Dostupné z: http://www.jitbm.com/24th%20Volume%20JITBM/3%20Supply%20Chain%20Management.pdf

[23] The ePassport Standard and it's Cryptographic Scheme. *CodeCereal* [online]. 2011 [cit. 2016-05-26]. Dostupné z: http://codecereal.blogspot.cz/2011/06/epassport-standard-and-its.html

[24] Identification in a new dimension: Modern with high cost efficiency. *LEGIC* [online]. [cit. 2017-05-19]. Dostupné z: http://www.legic.com/media/1400912/v3/File/legic-atc256-and-1024-en.pdf

[25] Wirelessly Pickpocketing a Mifare Classic Card. *Institute for Computing and Information Sciences* [online]. [cit. 2017-05-19]. Dostupné z: http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf

[26] Cloning Cryptographic RFID Cards for 25$. *Proxmark* [online]. [cit. 2017-05-19]. Dostupné z: http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20DESFire/Cloning_Cryptographic_RFID_Cards_for_25USD-WISSEC_2010.pdf

[27] MITROKOTSA, Aikaterini, Melanie R. RIEBACK a Andrew S. TANENBAUM. *Classification of RFID Attacks* [online]. [cit. 2017-05-24]. Dostupné z: http://visionlab.tudelft.nl/sites/default/files/IWRT08.pdf

[28] CENTER, A.I. *900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification* [online]. 2003 [cit. 2017-05-24]. Dostupné z: www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf

[29] ČEHOVSKÝ, Jaroslav. RFID čipy a jejich zabezpečení. In: *Portál UTB* [online]. 2009 [cit. 2017-05-25]. Dostupné z: htt-

ps://portal2.utb.cz/StagPortletsJSR168/PagesDispatcherServlet?pp_destElement=%23ssSouboryStudentuDivId_13295&pp_locale=cs&pp_reqType=render&pp_portlet=souboryStudentuPagesPortlet&pp_page=souboryStudentuDownloadPage&pp_nameSpace=G3400&soubidno=10991

[30] KARYGIANNIS, T., B. EYDT, G. BARBER, L. BUNN a T. PHILLIPS. Guidelines for Securing Radio Frequency Identification (RFID) Systems: Recommendations of the National Institute of Standards and Technology. In: *National Institute of Standards and Technology: NIST Special Publication 800-98* [online]. [cit. 2017-05-25]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf

[31] BOLOTNYY, L. a G. ROBINS. Physically Unclonable Function -Based Security and Privacy in RFID Systems. In: *Department of Computer Science: University of Virginia* [online]. 2007 [cit. 2017-05-25]. Dostupné z: http://www.cs.virginia.edu/~robins/papers/percom2007_published.pdf

[32] HANCKE, Gerhard P. a Markus G. KUHN. An RFID Distance Bounding Protocol. In: *Computer Laboratory: University of Cambridge* [online]. [cit. 2017-05-25]. Dostupné z: http://modsec.zimmerle.org/wireless-sec-papers/An%20RFID%20Distance%20Bounding%20Protocol.pdf

[33] LAURIE, A. Practical attacks against RFID. In: *Network Security: Vol. 2007, No. 9.* [online]. 2007 [cit. 2017-05-25]. Dostupné z: http://opac.vimaru.edu.vn/edata/E-Journal/2007/Network_Sercurity/Network%20Security.Vol%202007.Issue%209.A%204.pdf

[34] RIEBACK, Melanie R., Bruno CRISPO a Andrew S. TANENBAUM. Is Your Cat Infected with a Computer Virus? In: *Computer Systems Group: Vrije Universiteit Amsterdam* [online]. [cit. 2017-05-25]. Dostupné z: http://www.rfidvirus.org/papers/percom.06.pdf

[35] AYOADE, J. Roadmap to solving security and privacy concerns in RFID systems: Privacy and RFID Systems. *Computer Law & Security Review*. 2007, **23**(6), 555-561.

[36] KARYGIANNIS,, A., A. TSIBERTZOPOULOS, a T. PHILLIPS,. RFID Security: A Taxonomy of Risk. *Roc. of China'Com '06*. 2008, , 1-8.

[37] *Riscure: Privacy Issues with New Digital Passport* [online]. In: . [cit. 2017-05-25]. Dostupné z: http://www.riscure.com/2 news/passport.html

[38] Priority 1 Design [online]. 2007 [cit. 2011-04-28].EM4100 Protocol description. Dostupné z: http://www.priority1design.com.au/em4100_protocol.html.

[39] EM4333: Dual ISO/IEC 15693 and ISO 14443 Contactless Smart Card IC. *EM Microelektronic* [online]. [cit. 2017-05-28]. Dostupné z: http://www.emmicroelectronic.com/products/rf-identification-security/nfc-high-frequency-ics/em4333

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	3-Data Encryption Standard; bloková šifra aplikovaná třikrát po sobě
AA	Aktivní autentizace
AES	Advanced Encryption Standard; symetrická bloková šifra s vysokou rychlostí zpracování
ASK	Amplitude-shift keying; klíčování amplitudovým posuvem
BAC	Basic access control; základní kontrola přístupu
Bit	Binary digit; nejmenší jednotka informace používané především v číslicové a výpočetní technice
CRC	Cyclic redundancy check; cyklický redundantní součet
CRYPTO1	symetrická proudová šifra
DES	Data Encryption Standard; symetrická bloková šifra
DOS	Denial of Servise; odmítnutí přístupu
DSA	Digital Signature Algorithm; algoritmus digitálního podpisu
EAC/EACv2	Extended Access Control; rožšířená kontrola přístupu
ECC	Elliptic Curve Cryptography; kryptografie nad eliptickými křivkami
ECDSA	Elliptic Curve Digital Signature Algorithm; protokol digitálního podpisu s využitím eliptických křivek
EEPROM	Electrically Erasable Programmable Read-Only Memory; elektronicky mazatelná programovatelná pamět určená pouze pro čtení
EPC	Electronic Product Code; elektronický produktový kód
FSK	Frequency-shift keying; klíčování frekvenčním posuvem
GPS	Global Positioning System; globální polohovací systém
ICAO	International Civil Aviation Organization; mezinárodní organizace pro civilní letectví
ID	Identification; identifikace

IFF	Identification Friend or Foe; identifikace přítel nebo nepřítel
ISO	International Organization for Standardization; Mezinárodní organizace pro normalizaci
JPEG	Formát počítačového souboru, většinou obrázek
MRZ	Machine readable zone; strojově čitelná zóna
NIST	National Institute of Standards and Technology; Národní Institut Standardů a Technologie
NUID	Non-Unique ID; neunikátní identifikační číslo
OP	Občanský průkaz
PA	Pasivní autentizace
PACE	Password Authenticated Connection Establishment; Heslem ověřené navázání spojení
PKE	Public Key Encryption; šifrování s veřejným klíčem
PSK	Phase-shift keying; klíčování fázovým posuvem
RADAR	Radio Detection And Ranging; rádiová detekce a měření
RFID	Radio Frequency Identification; identifikace na rádiové frekvenci
ROM	Read-Only Memory; paměť určená pouze pro čtení
RS232	Sériový port
RSA	Rivest, Shanim, Adleman algoritmus podpisu
UID	Unique ID; univerzální identifikační číslo
USB	Universal Serial Bus; univerzální sériová sběrnice
ZoEP	Zákon o elektronickém podpisu

SEZNAM OBRÁZKŮ

SEZNAM TABULEK