Bezpečnost RFID technologií

Security of RFID technologies

Jan Grym

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Grym**
Osobní číslo:	**A13854**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnost RFID technologií**
Téma anglicky:	**The Security of RFID Technologies**

Zásady pro vypracování:

1. **Nastudujte a popište problematiku kopírování RFID.**
2. **Rozeberte příslušnou všeobecnou legislativu a normy.**
3. **Popište současně používané čipové technologie RFID(EMarin, MiFare Classic, MiFare DESFire EV1 apod.).**
4. **Diskutujte metody překonání zabezpečení RFID čipových technologií. Zaměřte se na možnosti jak docílit vyšší bezpečnosti systému ACS (identifikace,autentifikace).**
5. **Proveďte návrh maximálně zabezpečeného systému ACS.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RANKL, Wolfgang a Wolfgang EFFING. Smart card handbook. 4th ed. Překlad KennethCox. Chichester: John Wiley, 2010, xliv, 1043 s. ISBN 978-0-470-74367-6.**
2. **RANKL, Wolfgang a Wolfgang EFFING. Smart card applications: design models forusing and programming smart cards. 4th ed. Překlad Kenneth Cox. Chichester: JohnWiley, 2007, xviii, 217 s. ISBN 978-0-470-05882-4.**
3. **HUNT, V, Albert PUGLIA a Mike PUGLIA. RFID: a guide to radio frequencyidentification. 4th ed. Překlad Kenneth Cox. Hoboken, N.J.: Wiley-Interscience,c2007, xxiv, 214 p. ISBN 978-047-0107-645.**
4. **SHEPARD, Steven, Albert PUGLIA a Mike PUGLIA. RFID: radio frequencyidentification. 4th ed. Překlad Kenneth Cox. New York: McGraw-Hill, 2005, xvi, 256p. ISBN 00-714-4299-5.**
5. **JUŘÍK, Pavel, Albert PUGLIA a Mike PUGLIA. Platební karty: ilustrovaná historieplacení. 1. vyd. Překlad Kenneth Cox. Praha: Libri, 2012, 204 s. ISBN978-807-2774-982.**
6. **AHSON, Syed, Mohammad ILYAS a Mike PUGLIA. RFID handbook: applications,technology, security, and privacy. 1. vyd. Překlad Kenneth Cox. Boca Raton: CRCPress, c2008, xxi, 689 p. ISBN 14- 200-5499-6.**
7. **GLOVER, Bill a Bhatt HIMANSHU. RFID essentials. 1st ed. Beijing: O'Reilly, 2006,xiii, 260 s. ISBN 05-960-0944-5.**

Vedoucí diplomové práce: **doc. RNDr. Vojtěch Křesálek, CSc.**
Ústav elektroniky a měření

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
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

Diplomová práce Bezpečnost RFID technologií představuje v současnosti široce používané RFID technologie použité pro identifikaci osob především v systémech kontroly vstupu ACS. V této práci je uveden nejprve krátký úvod do problematiky identifikace, včetně spojených normativních a legislativních aspektů. Dále jsou popsány široce používané RFID technologie se zaměřením na jejich bezpečnost. Teoretická část práce je zakončena představením dosud známých metod překonání zabezpečení a možnostmi pro zdokonalení samotného procesu identifikace.

Praktická část se zabývá návrhem maximálně bezpečného systému ACS s využitím poznatků teoretické části. Návrh systému je aplikován na modelový objekt, včetně popisu integrace s ostatními poplachovými aplikacemi.

Klíčová slova: bezpečnost RFID, identifikace, elektronická identifikace, přístupový systém, ACS, systém kontroly vstupu SKV

ABSTRACT

This diploma thesis Security RFID technology present currently the widely used RFID technology for identification of persons especially in access control systems ACS. In this work we are given a brief introduction to the first issue of identification, including the related regulatory and legislative aspects. The following describes the widely used RFID technology focusing on their security. The theoretical part is concluded by presenting the known methods of overcoming security and possibilities for improving the identification process itself.

The practical part deals with the design maximum safe ACS system by using knowledge of the theoretical part. System design is applied to the object model, including a description of alarm integration with other applications.

Keywords: security of RFID, identification, electronic identification, access control system, ACS, Access

Poděkování

Rád bych poděkoval mému vedoucímu diplomové práce, panu doc. RNDr. Vojtěchu Křesálkovi, CSc. za odborné vedení a vstřícnost. Dále bych chtěl poděkovat svému rodinnému okolí, svým blízkým přátelům, ale i mému pracovnímu kolektivu za podporu ve studiu.

OBSAH

ÚVOD

Smyslem této diplomové práce je uvedení do problematiky bezpečnosti technologie RFID (Radio Frequency Identification – radiofrekvenční identifikace) s ohledem na provozování v systémech ACS (Access Control System – Systém kontroly vstupu).

V dnešní moderní době se denně setkáváme s potřebou identifikace osob, zvířat, nebo výrobků, kterou lze provést hned několika způsoby. Například na základě naší znalosti, po předložení uznávaného dokumentu sloužícího k identifikaci (občanský průkaz, cestovní pas, řidičský průkaz) nebo s využitím identifikátoru v elektronické podobě (číselný kód, čárový kód, magnetický proužek, RFID tag). Diplomová práce je zaměřena právě na technologii RFID, která je v současnosti stále více využívána pro mnohé aplikace a určitě bude v budoucnu pokračovat expanze této technologie i do dalších oblastí běžného života.

Ve vyspělých zemích je RFID používána prakticky v jakémkoliv oboru, kde je nutné zajistit ověření identity. Nejzávažnějším oborem pro potřeby identifikace je pak ověření identity osob. Vzhledem ke každodennímu využívání musí být identifikátor nejen bezpečný, ale i dlouhodobě spolehlivý. V současnosti je pro veřejné účely identifikace osob v České republice primárně využíván občanský průkaz, který je realizován na fyzickém médiu s vytištěnými daty a s použitými ochranami proti falzifikaci. Bohužel s vývojem technologií přichází možnost jednodušší výroby zdařilého falzifikátu, a proto je nutné zavést pro identifikaci nové technologie, které nelze falzifikovat. Při volbě bezpečného identifikátoru by měla být vyžadována bezpečnost i z dlouhodobého hlediska, neb při využití právě pro národní aplikaci, jako je občanský průkaz, musí být brán v úvahu minimálně průměrný věk osob. Tedy doba, po kterou by měla být zajištěna bezpečnost jak samotné technologie, tak i spolehlivost a odolnost fyzického média proti působení okolních vlivů. Naneštěstí lze velmi těžce předpokládat vývoj budoucích informačních technologií, které možná opět převrší míru zabezpečení v současnosti nepřekonatelných technologií. Jednou z možných ochran je například časové omezení platnosti identifikátoru, který je tím pádem nutné za danou periodu obměnit. Toto omezení však s sebou přináší ekonomické aspekty spojené se správou těchto identifikátorů.

Tato diplomová práce je však zaměřena především na využití RFID v systémech ACS, kde je mimo potřebné bezpečnosti identifikátoru, také nutné zajistit bezpečnost celého technologického celku a optimalizovat tak systém pro danou aplikaci.

I. TEORETICKÁ ČÁST

1 TECHNOLOGIE RFID

Pro účely identifikace objektů i subjektů je možné použít různé metody. V současnosti je například v mnoha zemích světa stále používána forma fyzického dokumentu pro identifikaci osob. Jedná se buď o klasickou papírovou knížku, popřípadě o kartičku z papíru, či plastu. Tyto různé formáty identifikačního dokumentu jsou chráněny proti falzifikaci, avšak vzhledem k své povaze a dostupným technologiím lze tyto dokumenty podvrhnout. Technologie RFID umožňuje mnohem bezpečnější proces identifikace pomocí elektronických zařízení. Identifikační data můžou být uloženy do paměti RFID čipu, kdy při použití bezpečnější technologie zůstávají chráněny pomocí různých moderních šifrovacích metod. V ideálním případě je pak tento identifikátor nemožné falzifikovat a je zaručena ochrana proti zneužití.

1.1 Historie RFID

Dle dostupných informací je považován za začátek využívání RFID technologie vojenský identifikační systém letadel využívaný během druhé světové války. Konkrétně se jednalo o systém IFF (Identification Friend or Foe – identifikace přítel nebo nepřítel). Po objevení RADARu (Radio Detection And Ranging – Rádiová detekce a měření) se naskytl problém s rozlišováním přátelských a nepřátelských letadel. Po vynálezu IFF již odpadl problém s identifikací letounů a tím došlo k zefektivnění samotného RADARu. Systém IFF pracoval na principu vyslání dotazu z vysílače (RADARu), který po dosažení letadla byl zpracován a na jehož základě odpovídač-transpondér vyslal signál zpět a tím došlo k předání informace o přátelském letounu. Signál z transpondéru mohl být zaslán zpět dvěma způsoby. Pasivní systém využíval odrazu původního signálu, kdy došlo k jeho úpravě tak, aby odražený signál obsahoval informaci pro identifikaci přátelského letounu. Princip pasivního systému je dnes nejvíce rozšířeným způsobem identifikace pomocí RFID. Druhá metoda tzv. aktivní systém nejprve přijal radarový signál, na který pomocí vysílače instalovaného přímo v letadle ihned odpověděl odpovídač, avšak ten již mohl vysílat signál na příklad na jiné nosné frekvenci apod. [7]

V šedesátých letech 20. století pokračoval výzkum bezdrátového přenosu dat pomocí radiové frekvence. Později se začal vyvíjet systém pro ochranu zboží, kdy na výrobky byl

nalepen tzv. 1 bitový RFID čip, který jednoduše určí, zda bylo za zboží zaplaceno, či se zloděj pokouší zboží ukrást. [7]

V 70. letech pak byl použit pasivní transpondér, který měl v paměti uloženo identifikační číslo, na jehož základě bylo umožněno první otevření dveří. Ve stejném období byl vyvíjen identifikační systém pro potřeby kontroly pohybu radioaktivních materiálů. Jednalo se o aktivní systém, který se skládal z brány a transpondéru ve vozidle. Brána byla v podstatě velká RFID čtečka, která po vjezdu kamionu přenesla radiový signál z brány do transpondéru, který zpět aktivně vyslal informace o převáženém materiálu, o konkrétním kamionu a popřípadě uložené ID číslo řidiče. Princip těchto bran je dnes využíván po celém světě jako tzv. mýtné brány. [7]

V 80. letech na žádost zemědělců byl vyvinut systém pro identifikaci zvířat. Zde byl již plně využit princip pasivního RFID systému. Postupně došlo ke standardizaci frekvence na 125 kHz. Tato frekvence se dodnes využívá, avšak postupně se přechází na standard 13,56 MHz. [7]

Od 90. let do současnosti byl vyvíjen RFID čip pro sledování zboží po celém světě. Zavedením EPC (Electronic Product Code – elektronický produktový kód) v kombinaci se standardním čárovým kódem došlo postupně k označování výrobků a k jejich automatickému sledování při cestování ke spotřebiteli. RFID čip zprvu obsahoval pouze produktové číslo z důvodu požadavku na co nejnižší cenu. Avšak postupem času docházelo vlivem vývoje technologií ke zlevnění výroby a tak bylo možné tyto čipy vybavit větší pamětí, která poskytovala úložný prostor pro více informací. Díky tomuto systému má dnes jakýkoliv zákazník možnost sledovat pohyb mezinárodní zásilky na cestě k odběrateli. [1]

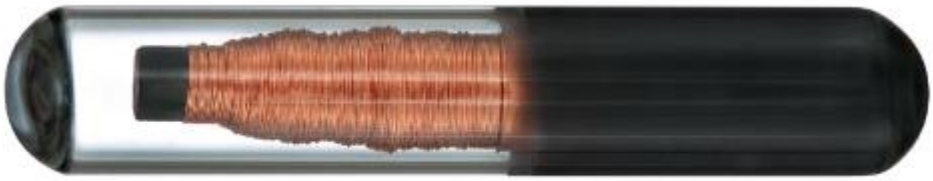
Obr. 1. Porovnání RFID čipu, čárového kódu a QR kódu, zdroj: http://www.inspectall.com

Jedním z dalších významných odvětví využívající technologii RFID je bankovnictví. Postupem času byly postupně vytlačeny finanční hodnoty fyzického charakteru v podobě vzácných kovů, minerálů, ale i později v podobě kupónů, šeků, bankovek, mincí, které jsou nahrazeny digitálními daty určujícími míru movitosti jedince. Samozřejmě odstraněním veškerých fyzických materiálů pro potřeby plateb se velmi zjednodušuje obchodní styk mezi subjekty. Ten je pak realizován právě pomocí RFID karty, díky které můžeme dnes platit bezkontaktně a bezhotovostně. U bankovních karet je kladen velmi vysoký důraz právě na bezpečnost, neb finanční otázka je velmi citlivá záležitost. [2]

1.2 Význam použití technologie RFID

Jak již bylo zmíněno v předchozí kapitole, RFID přináší bezpečnější variantu identifikace. Bohužel starší typy RFID technologie již byly v minulosti překonány a je tedy možné některé typy identifikátorů podvrhnout. Pokud není použitá RFID technologie bezpečná, rozhodně by neměla být používána v citlivých systémech, kde je kladen maximální důraz na bezpečnou a spolehlivou identifikaci. Nejčastěji takový případ nastává při identifikaci osob. V případě, že by například občanský průkaz měl být nahrazen RFID čipem, je nutné zabezpečit tuto technologii, aby nebylo možné v žádném případě vytvořit falzifikát, či neoprávněně použít identifikátor jinou osobou.

Jedna z futuristických představ je například implementace RFID čipu do lidského těla. Od realizace tohoto projektu nejsme technologicky vůbec vzdáleni. Stejně jako jsou označována zvířata pomocí RFID ve skleněné kapsli, která je zavedena pod kůži, je možné označit i osoby. Aplikace takového identifikátoru s sebou přináší mnoho aspektů psychologických, legislativních a medicínských. Při využití takovéhoto identifikátoru osob je opět nutné zajistit bezpečnost a spolehlivost na nejvyšší možnou míru.



Obr. 2. RFID tag ve skleněné ampuli, zdroj: http://www.lux-ident.com

V případě, že bychom dokázali vyvinout takovou RFID identifikaci, pak neopomínejme fakt, že pokud bylo něco vloženo do lidského těla, lze to zajisté i vyjmout a vložit do jiné osoby, která se pak může vydávat za původního majitele. Z tohoto důvodu je nutné zavést proces autentizace, díky kterému dojde k ověření osoby pomocí doplňujících informací. Příkladem těchto doplňujících informací může být například fotografie držitele čipu, tedy totožná informace, která je dnes standardně použita na občanských průkazech, cestovních pasech, řidičských průkazech apod.

Obr. 3. Potištěná RFID karta, zdroj: http://www.impro.net

Avšak metoda porovnání obličeje pouhým lidským okem není dokonalá a proto je vhodné doplnit fotografii biometrickými údaji. Při paranoidním náhledu na problematiku biometrického čtení, by těchto biometrických údajů muselo být více, neb plastická chirurgie v současnosti dokáže provést razantní úpravy jakékoliv části lidského těla. Naštěstí již dnes existuje více metod biometrického čtení, jako je například skenování rohovky, či duhovky, odraz zvuku v ušním boltci, sledování krevního řečiště v dlani, či celém těle, analýza řeči, analýza chůze apod.

Od roku 2004 je 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, k dispozici v České Republice tzv. e-pas, ve kterém jsou uloženy biometrické údaje obličeje a otisků prstů držitele tohoto cestovního pasu. [8]

1.3 Oblasti využití

RFID lze využít všude tam, kde je zapotřebí rozeznat jednotlivé subjekty a objekty. Tzn., že použití RFID je prakticky neomezené a je celosvětově široce rozšířené. [5]

RFID se využívá například pro identifikaci:

- Osob – veřejná správa (e-pasy, OP), ACS, nemocnice,
- Zvířat – očkování, podávání hormonů, plemenné kusy, určení dobytka na porážku
- Výrobků – obaly, ochrana proti krádeži v obchodech, ochrana proti neoriginální výrobě, načtení zboží v nákupním koši
- Vozidel – ACS, mýtné brány, imobilizační systémy, dálkové ovládání
- Platebních karet – bezkontaktní platby
- Dálkové ovládání privátních aplikací
- A v mnoha dalších aplikacích

1.4 Význam zneužití

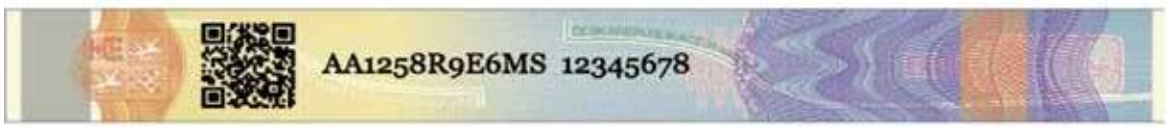
Používáme-li jakoukoliv technologii k identifikaci osob, je nutné zajistit ochranu proti falzifikaci na nejvyšší možnou míru z důvodu zachování věrohodnosti tohoto identifikátoru. Jsou-li dodrženy tyto podmínky, lze takovýto identifikátor používat pro

mnohem více sofistikovanější aplikace. Na využívání takového identifikátoru jsou pak závislé mnohem citlivější aplikace jako jsou bankovní systémy, registry veřejné správy, registry řidičů a automobilů atd. Při poskytnutí kvalitně falzifikovaného identifikátoru je možné získat úvěr na cizí osobu, popřípadě nechat si převést majetek na jinou osobu apod.

V momentu vývoje technologií na takovou úroveň, kdy je možné ne příliš složitým způsobem falzifikovat identifikátor, je pro zachování bezpečnosti nutné doplnit jej potřebnou ochranou na vyšší technologické úrovni, popřípadě nahradit jej novým řešením. Jako vhodným kandidátem se v dnešní době jeví právě technologie RFID v kombinaci s biometrickými údaji. Za předpokladu použití bezpečné nepřekonané RFID technologie je možné považovat takovýto identifikátor za velmi věrohodný.

Se zavedením technologie RFID je spjatá i otázka bezpečnosti celého technologického celku, jež bude zajišťovat spolehlivou funkci identifikace. RFID čip je nutné elektronicky detekovat a zajistit přenos identifikačních údajů do systému. Takovýto systém je založen především na softwarové aplikaci s využitím různých databází. V databázi jsou pak uloženy identifikační údaje subjektů, které musí korespondovat s identifikátorem. V případě, že nebude zajištěna bezpečnost tohoto softwarového celku, nelze takovýto systém považovat za věrohodný a tudíž nevhodný pro citlivé aplikace s velkým významem.

Identifikovat je možné nejenom osoby, ale i například zvířata, či zboží. RFID je možné využít například při výrobě alkoholu, či motorových olejů. Dle RFID čipu pak bude možné zjistit, jestli se jedná o falzifikovaný výrobek. Po přečtení RFID lze porovnat identifikační údaje například s on-line databází, čímž dojde k ověření pravosti výrobku. V závislosti na tzv. metanolové aféře je v současnosti pro identifikaci lahví alkoholických nápojů v České republice využíváno kontrolních pásků - kolků, kde mimo ochranných prvků je vytištěn QR (Quick Response – rychlá odpověď) kód, po jehož načtení můžeme ověřit certifikát pravosti výrobku. Tím lze spotřebiteli zajistit pravost výrobku bez obav újmy na zdraví. [9]

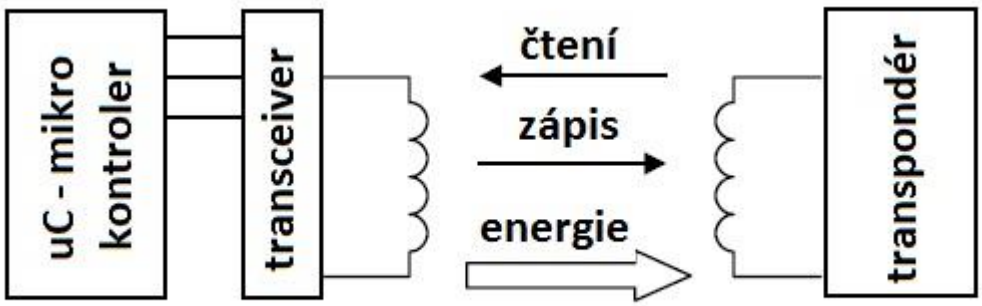


Obr. 4. Označovací pásek alkoholu, zdroj: http://www.pijbezpecne.cz

1.5 Obecný princip RFID

Jak už z významu zkratky vyplívá, RFID využívá princip elektromagnetický vln, které jsou využity pro přenos dat. Základními prvky RFID je transceiver neboli RFID čtečka (dále jen „čtečka“), která využívá simplexního, nebo poloduplexního přenosu dat. Dále transpondér, ve kterém jsou uloženy data v binární formě a mikro kontrolér, který zpracovává vysílaná, či přijímaná data. Základní prvky technologie RFID jsou patrné z obrázku níže. Označením transpondér máme na mysli tzv. RFID tag. Slovo tag lze přeložit jako přívěsek, cedulka, značka, etiketa, štítek. Spojení RFID tag univerzálně označuje RFID čip zapouzdřený do jakéhokoliv obalu, včetně antény. RFID tag může být vyrobený v podobě karty, přívěsku, dálkového ovladače apod. [1]

Čtečka v režimu snímání vytváří elektromagnetické pole, které je nastaveno na nosnou frekvenci. RFID tag po vložení do elektromagnetického pole generovaného čtečkou nejprve využije energii tohoto pole pro napájení integrovaných obvodů, které poté pomocí modulace ASK (Amplitude Shift Keying – klíčování amplitudovým posuvem) vhodně upraví vlastnosti elektromagnetického pole. Čtečka pak pomocí obvodu PLL (Phase Locked Loop – fázový závěs) získá přečtená data v podobě binárního kódu. Tento získaný kód je dále zpracován v mikro kontroléru, kde je porovnán s pamětí identifikačních kódů a v případě pozitivního výsledku dojde k vyvolání akce, jako je například zobrazení informací o osobě, otevření dveří, či k uskutečnění bankovní transakce.



Obr. 5. Obecné schéma přenosu RFID, zdroj: vlastní archiv autora

Režim zapisování pracuje analogicky stejně jako v režimu čtení, avšak zde dochází k přenosu dat z čtečky do paměti RFID čipu opět pomocí ASK modulace. [1]

Nejvíce rozšířenými pracovními frekvencemi používaných v RFID je 125 kHz, též nazývané jako RFID s nízkou frekvencí (low frequency) a vyšší frekvence 13,56MHz (high frequency). Tyto frekvence jsou využívány pro čtečky s malým dosahem do 10-30 cm nejčastěji se jedná o čtečky bezkontaktních proximity (proximity – těsná blízkost) tagů. Vzhledem k nastavenému limitu maximální vyzářené energie v rámci EMC (Electromagnetic Compability – elektromagnetické kompatibility) je zároveň vzdálenost 30 cm maximem při využití pasivního systému přenosu dat. Pokud jsou vyžadovány delší vzdálenosti pro přenos dat, jsou využívány jiné pracovní frekvence v pásmu UHF (Ultra High Frequency – ultra vysoká frekvence). Pro vzdálenější přenosy RFID jsou využívány frekvence 433,92 MHz a 868 MHz. Jedná se zpravidla o aktivní systémy, nejčastěji dálkové ovladače využívané v privátním sektoru.

Nosné frekvence se mohou různě lišit v mnohých částech světa, avšak vzhledem k vysoké míře standardizace se prakticky neliší a tím získávají tyto technologie na své univerzalitě. V ČR jsou úřadem pro telekomunikaci ČTÚ (Český telekomunikační úřad) spravovány jednotlivé frekvence, které jsou přidělovány jednotlivým subjektům, potažmo aplikacím. ČTÚ vydalo všeobecné oprávnění č.VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu, ve kterém jsou definována jednotlivé rozsahy frekvencí. Tyto pásma lze volně využívat bez nutnosti vlastnění licence provozování komunikace na daných frekvencích. [10]

2 LEGISLATIVNÍ RÁMEC A NORMY TÝKAJÍCÍ SE RFID

Tak jako všechny činnosti lidského snažení i RFID zařízení musí splňovat určité povinnosti definované v zákonech či normách. Aby bylo možné RFID využívat globálně je nutné zajistit standardizaci technologií používaných v RFID. Jedním z nejvyšších nároků mimo bezpečnosti karet je z technologického hlediska normalizace pracovních frekvencí a kompatibilita jednotlivých typů čipových technologií.

2.1 Legislativa

Systém ACS jako technologický celek musí splňovat základní podmínky platných norem a legislativních dokumentů. Vzhledem k faktu, že je ACS realizováno hardwarovými celky musí tyto splňovat následující legislativní dokumenty obecného charakteru, stejně jako zákony tykající se přímo řešené problematiky, které jsou uvedeny v následujících podkapitolách.

Legislativní dokumenty obecného charakteru:

- nařízení vlády č. 168/1997 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí
- nařízení vlády č. 173/1997 Sb., kterým se stanoví vybrané výrobky k posuzování shody
- nařízení vlády č. 291/2000 Sb., kterým se stanoví grafická podoba označení **CE**
- nařízení vlády č. 169/1997 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility
- nařízení vlády č. 18/2003 Sb. o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility

2.1.1 Vymezení pracovních frekvencí

Český telekomunikační úřad (dále jen „Úřad“) jako příslušný orgán státní správy podle § 108 odst. 1 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších

předpisů (dále jen „zákon“), a zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, na základě výsledků veřejné konzultace uskutečněné podle § 130 zákona, rozhodnutí Rady Úřadu podle § 107 odst. 9 písm. b) bod 2 a k provedení § 9 a § 12 zákona vydává opatřením obecné povahy ***všeobecné oprávnění č. VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu.*** [10]

Tímto všeobecným oprávněním ČTÚ stanovilo tzv. volné pásma, která jsou určena pro provozování bezdrátové komunikace bez nutnosti vlastnění oprávnění pro daný provoz. V tabulce č. 1 jsou uvedeny volné pásma, včetně frekvenčních hodnot a hodnot maximální intenzity elektromagnetických polí.

Článek 8 pak stanovuje konkrétní podmínky pro zařízení využívající indukční vazbu.

(1) Do kategorie indukčních zařízení patří rádiová zařízení, která používají magnetické pole a systémy s indukční smyčkou pro komunikaci na krátkou vzdálenost. Typická použití zahrnují imobilizéry automobilů, identifikaci zvířat, poplašné systémy, detekci kabelů, nakládání s odpady, identifikaci osob, bezdrátové hlasové spoje, řízení přístupu, senzory přiblížení, systémy ochrany proti krádeži včetně indukčních systémů ochrany proti krádeži využívajících rádiové kmitočty, přenos dat do kapesních zařízení, automatickou identifikaci zboží, bezdrátové řídicí systémy a automatický výběr mýtného.

(2) V případě vnější antény může být použita pouze indukční smyčka.

(3) Vyzařování stanic s indukční smyčkou v bezprostřední blízkosti od indukční smyčkyse nepovažuje za rušení podle zákona.

(4) Technické parametry stanic jsou:

Tab. 1. *Stanovené frekvenční pásma pro stanice s indukční smyčkou, zdroj: Všeobecné oprávnění č. VO/R/10/05.2014-3, dostupné z* http://www.ctu.cz

Ozn.	Kmitočtové pásmo	Intenzita magnetického pole	Další podmínky
a	9–90 kHz	72 dBμA/m ve vzdálenosti 10 m	
b	90–119 kHz	42 dBμA/m ve vzdálenosti 10 m	
c	119–135 kHz	66 dBμA/m ve vzdálenosti 10 m	
c1	135–140 kHz	42 dBμA/m ve vzdálenosti 10 m	
c2	140–148,5 kHz	37,7 dBμA/m ve vzdálenosti 10 m	
d	148,5–1600 kHz	–5 dBμA/m ve vzdálenosti 10 m	
e	1600–5000 kHz	–15 dBμA/m ve vzdálenosti 10 m	viz odst. 7
e1	1900–2100 kHz	5 dBμA/m ve vzdálenosti 10 m	
e2	3155–3400 kHz	13,5 dBμA/m ve vzdálenosti 10 m	
f	5–30 MHz	–20 dBμA/m ve vzdálenosti 10 m	viz odst. 7
g	6765–6795 kHz	42 dBμA/m ve vzdálenosti 10 m	viz odst. 8
h	7400–8800 kHz	9 dBμA/m ve vzdálenosti 10 m	
i	10,2–11,0 MHz	9 dBμA/m ve vzdálenosti 10 m	
j	13,553–13,567 MHz	42 dBμA/m ve vzdálenosti 10 m	viz odst. 8
j1	13,553–13,567 MHz	60 dBμA/m ve vzdálenosti 10 m	pouze zařízení elektronického dohledu nad zbožím[31]); viz odst. 8
k	26,957–27,283 MHz	42 dBμA/m ve vzdálenosti 10 m	

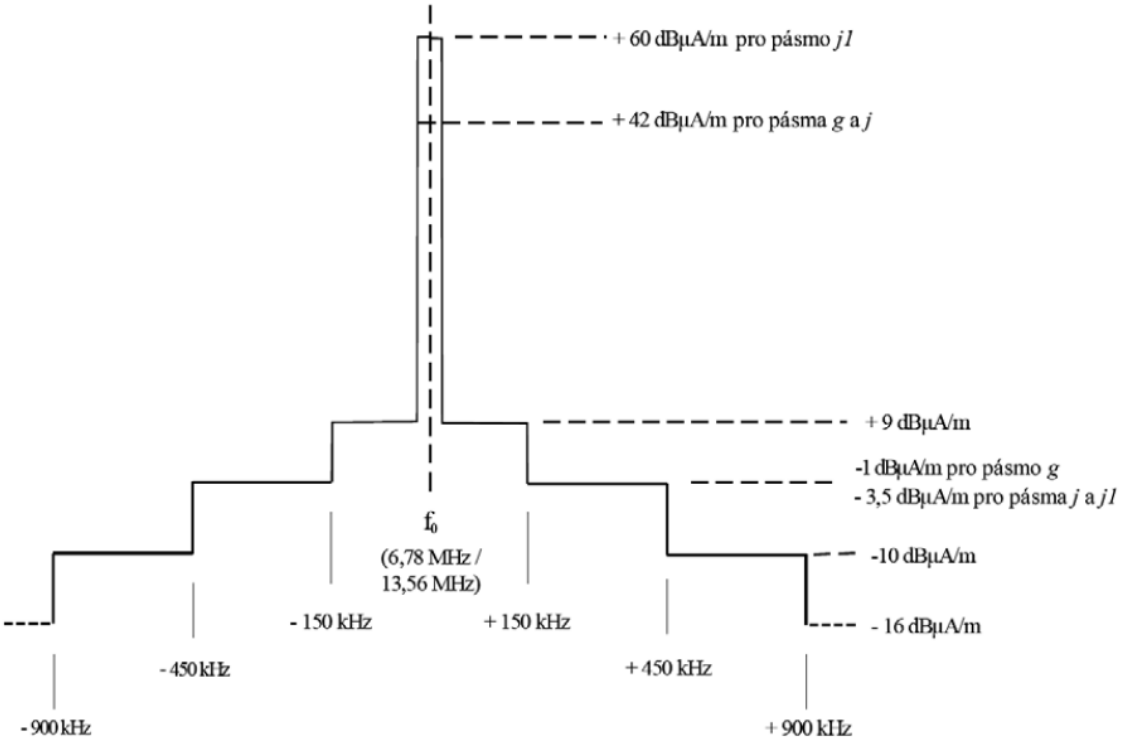
(5) *Kanálová rozteč není stanovena, může být použito celé příslušné pásmo.*

(6) V případě stanic s vestavěnou nebo výrobcem předepsanou smyčkovou anténou s plochou mezi 0,05 m2 a 0,16 m2 je uvedená intenzita magnetického pole zmenšena o 10 × log (plocha/0,16 m2); v případě plochy smyčkové antény menší než 0,05 m2 je uvedená intenzita magnetického pole zmenšena o 10 dB.

(7) V kmitočtových pásmech e, f se uvedená maximální intenzita magnetického pole vztahuje na šířku kmitočtového úseku 10 kHz. Pro systémy provozované v úseku širším než 10 kHz je při dodržení této podmínky celková maximální intenzita –5 dBμA/m ve vzdálenosti 10 m.

(8) Stanice vysílající v kmitočtových pásmech g, j, j1 mohou vyzařovat v úsecích

5,88–7,68 MHz a 12,66–14,46 MHz s hodnotami intenzity magnetického pole ve vzdálenosti 10 m takto: [10]



Obr. 6. Hodnoty intenzity magnetického pole, zdroj: Všeobecné oprávnění č. VO-R/10/05.2014-3, dostupné z http://www.ctu.cz

2.1.2 Ochrana osobních údajů

Při využívání technologie RFID v rámci identifikačních systémů je nutné zajistit maximální možnou bezpečnost uložených dat. Ochranou osobních údajů se v ČR zabývá Úřad pro ochranu osobních údajů, který byl zřízen na základě zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon“). Jsou- li pro účely identifikace využívány osobní údaje, či citlivé údaje je nutné zajistit splnění požadavků stanovených zákonem. [11]

Zákon stanovuje podmínky, za kterých je možné ukládat a zpracovávat osobní údaje včetně výjimek stanovených dalšími legislativními dokumenty. Jedním ze základních předpokladů pro provozování systému se správou osobních údajů je souhlas subjektu, jehož data budou ukládána.

Dále zákon stanovuje oznamovací povinnost subjektům, které zpracovávají osobní údaje nezávisle na typu aplikace. Pokud je takovýto systém provozován pak je nutné oznámit provoz tohoto systému Úřadu pro ochranu osobních údajů. Dle §16 zákona musí oznámení obsahovat: [11]

- Název správce systému (popřípadě jméno a příjmení), adresu jeho sídla, identifikační číslo
- Účel zpracování osobních údajů
- Kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají
- Zdroje osobních údajů
- Popis způsobu zpracování osobních údajů
- Místo nebo místa zpracování osobních údajů, jsou-li odlišná od sídla správce systému
- Příjemce, kterým mohou být zpřístupněny, či sdělovány osobní údaje
- Předpokládané přenosy osobních údajů do jiných států
- Popis opatření k zajištění požadované ochrany osobních údajů
- Propojení na jiné správce nebo zpracovatele

2.2 Standardizace

Aby identifikační systémy založené na technologii RFID byly opravdu spolehlivé, bezpečné a globálně dostupné je nutné normalizovat výrobu takovýchto zařízení po celém světě.

2.2.1 ISO/IEC 7816

ISO / IEC 7816 je řada norem, které stanovují využití karet s integrovanými obvody ICC (Integrated Circuits Cards – karty s integrovanými obvody) s přenosem informací přes fyzický kontakt pro účely identifikace. Tyto karty jsou určené pro výměnu informací mezi vnějším světem a integrovaným obvodem v kartě. Jako výsledek výměny informací, karta

poskytuje informace (výsledky výpočtů, uložená data) a nebo modifikuje svůj obsah (ukládání dat).

V normě nalezneme popis fyzikálních parametrů integrovaného obvodu, jako jsou například přípustné limity expozice okolních jevů. Takovým jevem můžou být rentgenové paprsky, elektromagnetické pole, UV (Ultra Violet – ultra-fialové) záření, statická elektrická pole, ale i překročení stanoveného limitu okolní teploty karty. ISO/IEC 7816 dále definuje charakteristiky vlastnosti karty při výskytu fyzické deformace plastové karty. Identifikační karty definované normou ISO/IEC 7816 využívají pro přenos kontaktního pole, jehož parametry jsou rovněž definovány. Norma definuje umístění, číslování, velikost kontaktního pole a materiálů z něhož je kontaktní pole vyrobeno. Součástí této normy je i popis přenosových protokolů. Typickým příkladem kontaktních karet je SIM (Subscriber Identity Module – účastnický identifikační modul) karta do mobilních telefonů, či kontaktní platební karty. [1]

2.2.2 ISO/IEC 7810

Norma určuje především rozměry a tvar identifikačních karet. Norma dále obsahuje specifikaci spolehlivosti karet při vystavení různým nestandardním prostředím.
ISO/IEC 7810 definuje 4 základní kategorie karet a 1 doplňkovou:

- ID-1 – rozměry 85,60 x 53,98 mm se zaoblenými rohy s poloměrem ohybu 2.88 – 3.48 mm. Tento rozměr karet je nejčastěji používaným typem především pro bankovní platební karty, řidičské průkazy, sociální karty, karty pro veřejnou dopravu, zaměstnanecké RFID karty.
- ID-2 – rozměry 105 x 74 mm (formát A7). Karty s formátem ID-2 jsou využívány například pro víza, nebo jako identifikační karty v evropských zemích, avšak pomalu se přechází na ID-1.
- ID-3 – rozměry 125 x 88 (formát B7). Využíváno především pro cestovní pasy.
- ID-000 – rozměry 25 x 15 mm s jedním mírně (3 mm) zkoseným rohem. Typické využití tohoto formátu jsou SIM karty do mobilních telefonů.

V návaznosti na tuto normu byla vytvořena ISO/IEC 7813, která je určena pro definici platebních a kreditních karet. Tato norma však doplnila parametry standardizace formátu karet, kdy stanovila tloušťku karty na 0,76 mm a zaoblení rohů s poloměrem 3,18 mm. [1]

Jako doplňkový formát norma definuje umístění karty formátu ID-000 v kartě formátu ID-1. ID-000 je umístěna na konkrétním místě pro čtení ve čtečkách pro ID-1, avšak vnitřní kartu ID-000 lze z původního většího formátu vyjmout bez nutnosti využití doplňkového nářadí. Toto uspořádání se označuje jako ID-1/000.

2.2.3 ISO/IEC 14443

ISO / IEC 14443 je mezinárodním standardem, používaným pro definici bezkontaktních karet používaných pro účely identifikace.

Norma se skládá z následujících částí:

- ISO / IEC 14443-1: 2008 Část 1: Fyzikální vlastnosti
- ISO / IEC 14443-2: 2010 Část 2: Napájení EM polem a signální rozhraní
- ISO / IEC 14443-3: 2011 Část 3: Inicializace a antikolize)
- ISO / IEC 14443-4: 2008 Část 4: Přenosový protokol

Někdy je norma označována jako ISO/IEC 14443 A, nebo B. Toto rozdělení vzniklo z neshody mezi výrobci, a tedy je možné se setkat s dvěma typy karet A a B, které obě pracují na frekvenci 13,56MHz. Hlavní rozdíly mezi těmito typy tkví v použité metodě modulace, v kódování a inicializačních protokolech. [1]

ISO / IEC 14443 zavádí termíny pro komponenty:

- PCD: Proximity Card Reader – Bezkontaktní čtečka karet
- PICC: Proximity Integrated Circuit Cards - Bezkontaktní čipová karta (popř. bezkontaktní karta s integrovanými obvody)

2.2.4 ČSN ETSI EN 302291

ČSN ETSI EN 302 291 – Elektromagnetická kompatibilita a rádiové spektrum – Zařízení krátkého dosahu (SRD – Short Range Devices) – Zařízení datových komunikací blízkého dosahu s induktivním přenosem, pracující na 13,56 MHz.

Tato norma stanovuje minimální potřebné vlastnosti pro dosažení optimální funkčnosti s využitím dostupného spektra volných frekvencí. Zařízení určené pro datovou komunikaci na blízký dosah s induktivním přenosem odpovídá definici pro zařízení krátkého dosahu SRD. Meze výkonu pro kmitočtová pásma lze nalézt v aktuální verzi doporučení CEPT/ERC 70-03, nebo v národních předpisech (viz. kapitola 2.1.1 – Vymezení

pracovních frekvencí). Toto normativum je závazné pro vysílače a přijímače datových komunikací blízkého dosahu s induktivním přenosem, pracující na 13,56 MHz. Požadavky na elektromagnetickou kompatibilitu jsou dále uvedeny v EN 301 489-1 a EN 301 489-3. V rámci normy jsou definovány zařízení jako pevné stanice, pohyblivé stanice a přenosné stanice. Tato norma je určena k pokrytí ustanovení článku 3.2 Směrnice 1999/5/EC (Směrnice R&TTE), který stanoví že "Rádiová zařízení musí být konstruována tak, aby efektivně využívala spektrum přidělené zemským/kosmickým radiokomunikacím a technické prostředky umístěné na oběžné dráze, aby se zabránilo škodlivé interferenci". Dále je pro účely elektromagnetické kompatibility zajištěna kompatibilita systémů ACS s následujícími normami:

- **ČSN EN 61000-6-1** Elektromagnetická kompatibilita (EMC) – Část 6-1: Kmenové normy – Odolnost – Prostředí obytné, obchodní a lehkého průmyslu
- **ČSN EN 61000-6-3** Elektromagnetická kompatibilita (EMC) – Část 6-3: Kmenové normy – Emise – Prostředí obytné, obchodní a lehkého průmyslu

2.2.5 Aplikační normy

S využitím RFID v různých jsou zavedeny normy určující požadavky pro konkrétní aplikace.

- ČSN EN 50 133 – Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
- ČSN EN 60839-11-1 – Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty (s účinností od 11.6.2016)
- ČSN ISO 18 186 – Kontejnery – Systém RFID tagů nákladních zásilek
- ČSN ISO 17 366 – Aplikace RFID v dodavatelském řetězci – Obaly výrobků
- ČSN ISO 17 367 – Aplikace RFID v dodavatelském řetězci – Označování výrobků
- ČSN EN 48 17 – Letectví a kosmonautika – Pasivní UHF RFID tagy, určené pro letecké použití
- ISO 11 784 a ISO 11 785 – Radiofrekvenční identifikace zvířat
- ČSN EN 60950-1 Zařízení informační technologie – Bezpečnost – Část 1: Všeobecné požadavky

3 SOUČASNĚ POUŽÍVANÉ ČIPOVÉ TECHNOLOGIE RFID

Na trhu existuje spousta výrobců RFID technologií. Vývojem jsou neustále objevovány nové bezpečnostní prvky a jejich využití. Díky těmto aspektům je k dispozici velké množství RFID čipů, které se mohou lišit ve spoustě parametrů. Níže jsou popsány používané technologie s majoritním podílem na celkovém počtu využití RFID po celém světě.

3.1 Základní rozdělení RFID tagů

Základní dělení RFID tagů je na aktivní a pasivní. Aktivní tagy jsou zpravidla vybaveny vlastním napájecím zdrojem, díky kterému je možné docílit delší vzdálenosti čtení. Pasivní tagy získávají energii z elektromagnetického pole vytvářeného čtečkou.

Druhým základním dělením je rozdělení podle typu přenosu dat a jejich uchování v paměti. [3]

- Čtecí tagy (read tag) – jsou určeny pouze pro čtení a nelze do nich zapisovat. Identifikační data jsou uložena do paměti ROM (Read Only Memory – paměť pouze pro čtení) při jejich výrobě. Z pohledu přenosu dat se pak jedná o simplexní přenos
- Čtecí\zapisovací tagy (read\write tag, někdy též označované jako R\W tag) – jsou v současnosti využívány pro sofistikovanější aplikace. Jak již z označení vyplývá, 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 (Electrically Erasable Programmable Read Only Memory – elektricky smazatelná programovatelná ROM). Přenos dat u R/W tagů probíhá poloduplexně.

RFID tagy dále dělíme následovně:

Dle pracovní frekvence: [4]

- 125 kHz – LW RFID (low frequency) – vhodné pro pasivní systémy, historicky více využívaná frekvence
- 13,56 MHz – HF RFID (high frequency) – vhodné pro pasivní systémy, v současnosti nejvíce používaná frekvence pro identifikaci
- 433,92 MHz – UHF RFID – vhodné pro aktivní systémy, přenos na delší vzdálenosti
- 868 MHz – UHF RFID – vhodné pro aktivní systémy, přenos na delší vzdálenosti

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

Dle tvaru média: [1]

- Karty ID-1 – definované normou ISO/IEC 7810 mají uplatnění v mnoha aplikacích jako jsou karty zaměstnanců, občanský průkaz, platební karty atd. Karty lze dále kombinovat například s technologií magnetického proužku či kontaktním čipem. Fyzická identifikace karty je pak zajištěna vytištěným identifikačním číslem, logem vydavatele, popřípadě fotografií držitele přímo na plastové kartě. Je také možné aplikovat i ochranné holografické prvky.
- Přívěsky (klíčenky) – určeny spíše pro privátní účely. Přívěsky mají většinou menší rozměry a zajímavý design. Přívěsky lze fyzicky identifikovat pomocí obrázku menších rozměrů, nebo pomocí vygravírování identifikačního čísla
- Dálkové ovladače – využití v privátních a firemních aplikacích. Ovladače jsou primárně určeny pro identifikaci a ovládání méně bezpečných aplikací (vrata, brány, závory, automobily, imobilizéry atd.). Vzhledem ke vzdálenému přenosu lze tyto identifikátory jednodušeji překonat, proto musí splňovat určité bezpečnostní požadavky.
- Samolepky (labely) – jsou určeny především pro identifikaci zboží. Je zde kladen velký důraz na nízké náklady. Samolepka bývá kombinována s čárovým kódem na povrchu.

- Skleněné tagy (glass tags) – slouží k identifikaci živých tvorů primárně zvířat. Při výrobě skleněného tagu je kladen velký důraz na jeho malé rozměry se zachováním velké čtecí vzdálenosti a také na hygienu. Jedná se o RFID čip zapouzdřený ve skleněné ampuli, která je vpravena pod kůži.
- Tagy pro speciální aplikace – díky moderním technologiím lze RFID čip umístit prakticky do jakéhokoliv pouzdra. Existují například tzv. laundry tagy (tagy pro prádlo), které slouží pro identifikaci zboží v prádelnách, kde jsou kladeny vysoké podmínky na prostředí, kterému je tag vystaven. Dále je dnes velmi často používáno RFID identifikace v aquaparcích, kde jsou návštěvníkům rozdány RFID tagy ve formě různých náramků, hodinek apod.

Dle použité metody šifrování:

- DES (Data Encryption Standard) – symetrická bloková šifra, která je již překonána. Pro šifrování využívá klíč o délce 64 bitů, avšak pouze 56 bytů je efektivně používáno a zbylých 8 bitů je použito pro kontrolní součty. Díky této krátké délce klíče, lze šifrování prolomit hrubou silou za méně než 24 hodin. [12]
- 3DES (někdy označován jako TDES, Triple DES) – vychází ze základního šifrování DES. Pro zvýšení bezpečnosti byla délka klíče rozšířena na 168 bitů (3x56 bitů). Prodloužením bitové délky klíče se zvýšila bezpečnost šifry, avšak s dnešními výkonnými zařízeními lze i tuto šifru překonat hrubou s rozumnou dobou trvání. Šifrování pomocí 3DES je poměrně pomalé a proto se využívá dokonalejších kryptografických nástrojů. [12]
- AES (Advanced Encryption Standard) – symetrická bloková šifra s vysokou rychlostí zpracování. Velikost klíče dosahuje délky až 256 bitů. Šifra je považována za bezpečnou, protože její bezpečnost zatím nebyla zpochybněna. Díky délce klíče až 256 bitů by útok hrubou silou trval několik let. Tato metoda šifrování je využívána masově po celém světě. Například americký úřad pro standardizaci NIST (National Institute of Standards and Technology – Národní Institut Standardů a Technologie) schválil AES jako bezpečnou metodu pro šifrování neutajovaných

dokumentů. V roce 2003 pak americká vláda uvedla, že AES může být použita i pro ochranu utajovaných dokumentů. [12]

- CRYPTO1 – symetrická proudová šifra vytvořena primárně pro potřeby MiFare Classic technologie. Jedná se o velmi rychlé šifrování, avšak s velmi nízkou bezpečností. Původně výrobce NXP semiconductors neprozradil algoritmus zpracování šifry, avšak reverzním inženýrstvím byl algoritmus odhalen a šifrování bylo tak překonáno. [13]
- PKE (public key encryption) - neboli šifrování s veřejným klíčem je označení pro asymetrické šifrovací algoritmy. Nejznámější varianty PKE jsou pak algoritmy RSA (Rivest, Shamir, Adleman), Diffie-Hellman, nebo ECC (Elliptic curve cryptography- kryptografie nad eliptickými křivkami). V asymetrickém šifrování je využíváno dvou typů klíčů. Privátní slouží k dešifrování soukromé zprávy a veřejný k zašifrování zprávy pro příjemce. Oba klíče jsou matematicky podobné, ale jsou navrhnuté tak, aby nebylo možné ze znalosti veřejného klíče spočítat soukromý klíč a obráceně. [12]

3.2 EM Marin

Společnost EM Microelectronic-Marin SA ze Švýcarska vyrábí od roku 1970 miniaturní integrované obvody se zaměřením na minimální napětí a energetickou spotřebu. Jinými slovy vyrábí právě RFID tagy. Na světovém trhu je technologie EMmarin značně rozšířená i přes minimální bezpečnost těchto čipů.

Technologie EM Marin (někdy též uváděno EMarin, EMmarin) pracuje na frekvenci 125kHz, avšak v současnosti společnost vyrábí i RFID pracující na 13,56MHz, popřípadě i na odlišných frekvencích. Jednotlivé typy RFID čipů jsou pak označovány písmeny EM a čtveřicí čísel. Dříve toto označení bylo místo písmen EM pouze H. Jedna z prvních široce používaných karet byla EM4001, která byla postupně nahrazena typem EM4100 a EM4102. Dnes je vyráběn čip EM4200, které je plně kompatibilní s předchozími typy. [14]

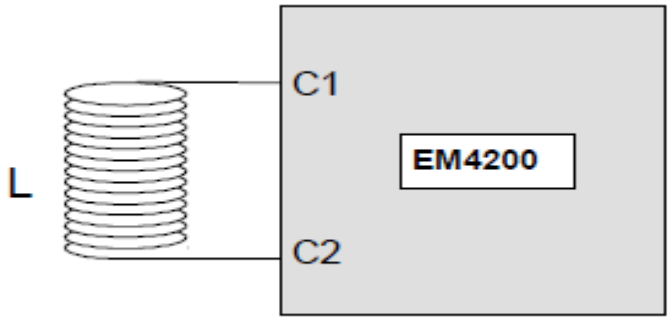
EM 4200 je integrovaný obvod typu CMOS (Complementary Metal Oxid Semiconductor – doplňující se polovodič kov-oxid) určený pouze pro čtení. V porovnání s předchozími typy nabízí EM 4200 vyšší čtecí rozsah a větší paměť. V paměti ROM je pomocí laseru uloženo

unikátní 128 bitové UID (Unique Identification – unikátní identifikační číslo) již při výrobě. [14]

Integrované obvody jsou plně napájeny z externí antény, která je buzena elektromagnetickým polem. Modulací OOK (On-Off Keying) čip posílá zpět unikátní kód obsažený v ROM paměti. [14]

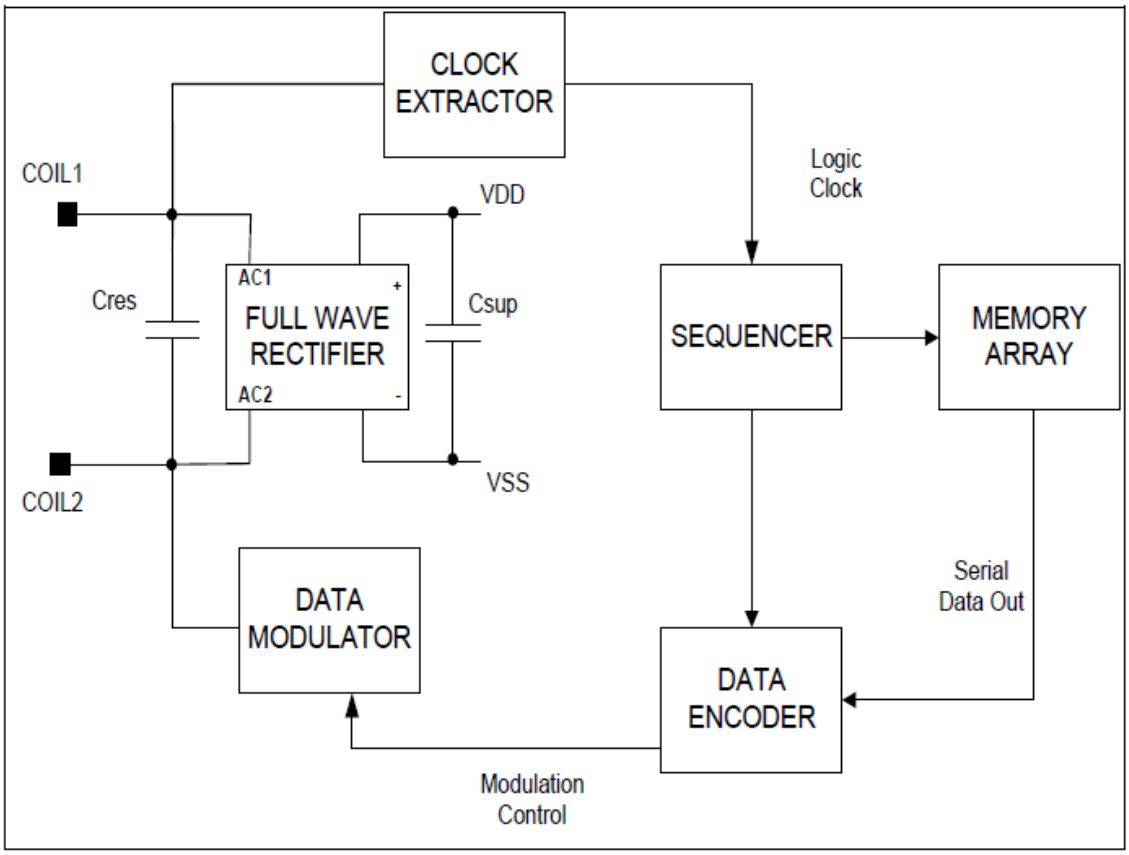
EM 4200 nabízí:

- Plnou kompatibilitu s předchozími typy EM 4100\4102 a EM4005\4105
- 128 bitovou laserově programovanou ROM paměť
- Několik možností přenosových rychlostí a typu kódování
    - Manchester 32 a 64 RF period na přenesený 1 bit
    - Biphase 32 a 64 RF period na přenesený 1 bit
    - PSK 16 RF period na přenesený 1 bit
    - FSK2 50 RF period na přenesený 1 bit
- Několik rezonančních kondenzátorů integrovaných v čipu (0 pF, 75 pF nebo 250 pF)
- Frekvenční rozmezí 100 až 150 kHz



Obr. 7. Obecné znázornění RFID čipu s anténou, zdroj: 4200-DS.doc, Version 3.2, 8-Nov-13,EM Microelectronic-Marin SA, dostupné z http://www.emmicroelectronic.com

Technologie EM 4200 bohužel nenabízí žádnou ochranu proti falzifikaci. Pro překonání této technologie postačí přečíst UID čipu a dále ho už stačí jenom zkopírovat do jiného čipu.



Obr. 8. Vnitřní schéma čipu EM4200, zdroj: 4200-DS.doc, Version 3.2, 8-Nov-13,EM Microelectronic-Marin SA, dostupné z http://www.emmicroelectronic.com

Na trhu jsou dnes k dispozici kopírovací zařízení, které lze pořídit v cenové relaci 1000 až 2000 Kč, které jednoduše zkopírují UID a nahrají ho do nenaprogramované karty.

Vzhledem k minimální bezpečnosti této technologie je však poměrně rozšířena. Díky menším ekonomickým nákladům při pořízení systému, ale i samotných karet nalézá tato technologie využití dodnes. Tuto technologii je možné použít pro aplikace, kde není kladen důraz na vysokou bezpečnost. Jedná se například o identifikaci zvířat, odpadové hospodářství, přístupové systémy pro méně bezpečné aplikace (vstupy na kulturní akce, vjezdy na parkoviště atd.), automatická logistika, průmyslová identifikace, jednoduchá ochrana proti padělání výrobků.

Mimo výše popsaný typ je k dispozici i čtecí a zapisovací čip EM4450, který nabízí paměť 1K (1024bitů) realizovaný pamětí EEPROM. Úložný prostor může být chráněn 32 bitovým heslem. Heslo je možné změnit, ale nelze ho přečíst. Čip je standardně vybaven 64 bitovou ROM pamětí, kde je opět uloženo UID. [1]

3.3 HITAG

Další společností, která se zabývá výrobou RFID čipů je NXP semiconductors N.V. (dříve Philips Semiconductors). Společnost je špičkou ve svém oboru a mimo RFID technologie vyvíjí spoustu jiných aplikací s využitím polovodičů. NXP je výrobcem technologií ICC čipů HITAG, ICODE, NTAG a UCODE. Pro účely přístupových systémů je využíváno technologie HITAG, která je dnes vyráběna již ve své druhé variantě HITAG 2. Tato společnost je rovněž výrobcem dalších čipových technologií, které jsou popsány dále. [15]

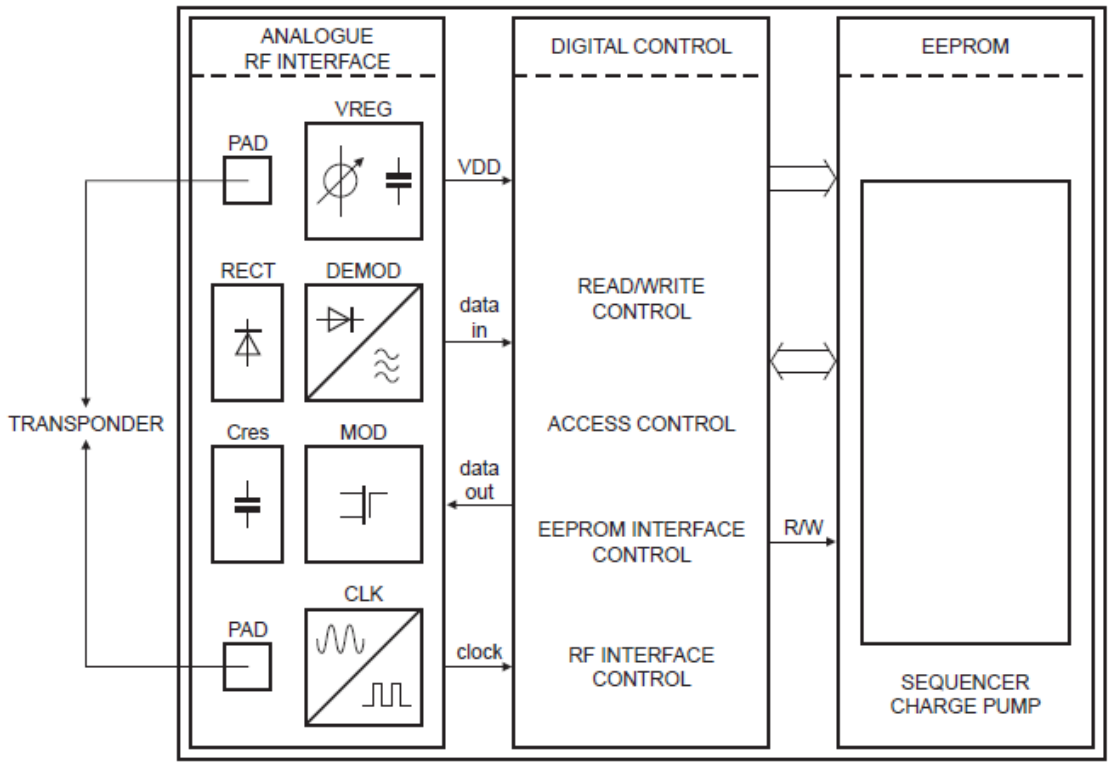
RFID čip HITAG 2 je pasivní technologie s pracovní frekvencí 125kHz. Data jsou přenášena poloduplexně a mohou být pro bezpečnostní účely přenášena zašifrované. HITAG 2 je vybaven 256 bitovou pamětí, která může být chráněna proti čtení či zápisu nastavením tzv. paměťových flagů (vlajek, značek). Tento čip nabízí možnost nastavení hesla, šifrovací mód a 3 módů pro pouhé čtení. [15]

HITAG 2 nabízí možnosti:

- Identifikace pro použití v bezkontaktních aplikacích
- Pracovní frekvence 125 kHz
- Přenos dat a napájení je zajištěno z elektromagnetického pole čtečky
- 256 bitovou EEPROM paměť (128 bitů pro uživatelská data a 128 bitů pro kontrolní data a chráněnou paměť)
- Uchování dat v paměti až 10 let
- 100 000 cyklů mazání a zápisu
- Výběr ochrany pro čtení a zápis paměti
- Dva typy kódování:
    - Manchester

- Biphase

- Efektivní komunikační protokol s kontrolou integrity dat
- Čtecí a zapisovací mód umožňuje:
  - Přenos neupravených dat chráněných heslem
  - Přenos šifrovaných dat



Obr. 9. Vnitřní schéma čipu HITAG 2, zdroj: HT2x HITAG 2 transponder IC, Rev. 3.1 – 3 November 2014, 210431, dostupné z http://www.nxp..com

HITAG 2 využívá pro přenos stejně jako ostatní RFID modulaci ASK. Karta je opět vybavena pamětí ROM, kde je uloženo 32 bitové UID. Přístup do paměti může být chráněn 24 bitovým heslem, nebo může být obsah paměti šifrován pomocí 48 bitového klíče.

3.4 MiFare Classic

S RFID technologií MiFare přecházíme do řady HF RFID, tedy s využitím pracovní frekvence 13,56MHz. MiFare je označovaná jako Smart Card IC (chytrá karta s integrovanými obvody). MiFare je vyráběna v 4 řadách Classic, DESFire, Plus a Ultralight. Nejrozšířenějšími jsou právě řady Classic a DESFire, které jsou níže popsány.

MiFare Classic je první typem z řady MiFare technologie. Čipy jsou dále označovány přívlastkem S50 a S70, které označují velikost paměťového prostoru. S 50 byla vybavena 1K pamětí a S 70 4K. Dnes se již vyrábí pouze varianta S70. Karta plně vyhovuje normě ISO/IEC 14443-A. Technologie MiFare Classic byla již v minulosti překonána a proto se ustupuje od jejího použití a nahrazuje se novějším typem DESFire. Výrobce NXP Semiconductors doporučuje tuto kartu využívat například pro jízdenky ve veřejně přepravě, pro mýtné brány, jako studentské karty, přístupové karty, parkovací karty, zaměstnanecké karty a pro mnoho dalších aplikací. Vzhledem k překonání technologie nemůžeme tuto kartu považovat za bezpečnou a stejně jako výše popsané technologie EM marin lze tyto karty používat pouze pro aplikace, kde nejsou kladeny vysoké požadavky na bezpečnost. Nicméně technologii MiFare Classic lze určitě považovat za bezpečnější než EM marin, avšak na trhu jsou k dispozici rovněž kopírovací zařízení, které jednoduše zkopírují obsah paměti do jiné karty. [16]

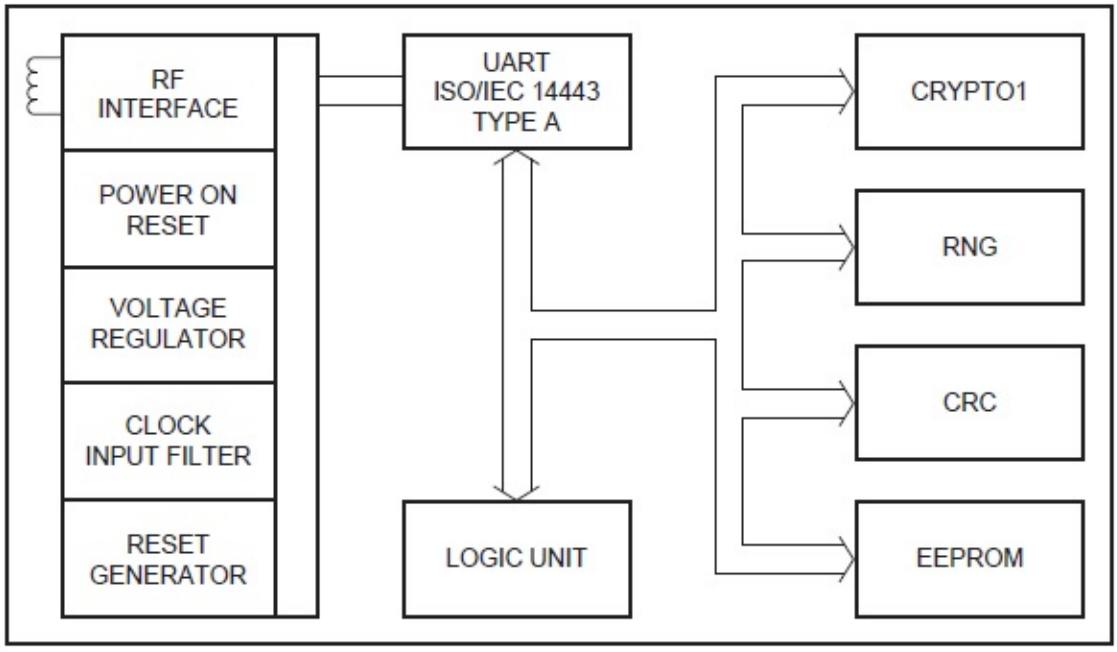
MiFare Classic S70 využívá inteligentní anti kolizní mechanismus, který zajišťuje spolehlivý přenos dat mezi čtečkou a jedním RFID tagem i za situace, že je v elektromagnetickém poli přítomno více RFID tagů. Mechanismus pracuje na principu přečtení UID čipu, se kterým pouze udržuje spojení právě pomocí identifikace UID.

Čip má ve výrobě naprogramován 7 bajtový UID nebo 4 bajtový NUID (Non-Unique ID – neunikátní identifikační číslo). Dále nabízí možnost nastavení tříprůchodové autentizace dle standardu ISO/IEC 9798-2. V čipu lze nastavit dva rozdílné šifrovací klíče A a B na jeden sektor paměti v rámci podpory multi-aplikací. [16]

MiFare Classic S70 nabízí:

- Bezkontaktní přenos dat a energie

- Pracovní frekvenci 13,56 MHz
- Integritu dat zajištěnou 16 bitovým CRC (Cyclic Redundancy Check – cyklický redundantní součet) obvodem, kontrolu paritních a kódovacích bitů
- Pracovní čas potřebný pro zpracování čipu menší než 100 ms
- Podpora generátoru náhodného ID (pouze i 7 bajtové UID verze)
- Čtecí vzdálenost do 100 mm (záleží na tvaru a nastavení transceiveru)
- Přenosovou rychlost 106 kbit\s
- Paměť EEPROM 4K organizovanou do 32 sektorů s 4 bloky a do 8 sektorů s 16 bloky (jeden blok obsahuje 16 bajtů)
- Životnost dat v paměti 10 let a 200 000 zapisovacích cyklů
- Uživatelsky nastavitelný přístup k jednotlivým paměťovým blokům
- Aplikaci proudové šifry CRYPTO1



Obr. 10. Vnitřní schéma čipu MiFare Classic, zdroj:MF1S70yyX/V1, MiFare CLassic EV1 4K, Rev. 3.1 – 8 Septemeber 2014, 279331, dostupné z http://www.nxp.com

Jak již bylo zmíněno pro zabezpečení uložených dat je využíváno tzv. tříprůchodové autentizace. Princip této ochrany tkví v ověření pravosti daného RFID čipu. Po přiložení karty dojde pomocí anti kolizního protokolu k zahájení komunikace. Během této inicializace probíhá komunikace v nešifrované podobě a dojde k přenosu typu karty a UID. Bohužel mnoho aplikací využívá pouze UID pro identifikaci a proto tyto aplikace je poměrně jednoduché překonat pouhým přečtením UID a vložením do jiné karty. V případě, že aplikace využívá plně potenciál zabezpečení, pak je nutné k identifikaci karty přečíst některý z bloků v paměti, který může být chráněn šifrovacím klíčem. Dochází k výměně data, které mají za úkol ověření správnosti šifrovacích klíčů na obou stranách. Postup probíhá následovně:

1. Čtečka vyšle žádost o přístup do konkrétního sektoru.
2. Čip z tohoto sektoru přečte data a zvolí náhodný vzorek, který zašle čtečce aby došlo k ověření znalosti klíče.
3. Čtečka přijme vybraná data a v případě, že je schopná data dešifrovat, tedy zná správný klíč zašle odpověď, ve které bude zároveň obsažen další vzorek dat zašifrovaných dle klíče čtečky.
4. Čip po příjmu odpovědi dešifruje data pomocí vlastních výpočtů a zašle čtečce potvrzení znalosti klíče.
5. Čtečka pomocí vlastního výpočtu ověří odpověď a v případě kladného výsledku je autentizace úspěšně dokončena. [6]

Po dokončení autentizace probíhá již komunikace šifrovaně pomocí jednoho z klíčů. V tomto režimu může dále docházet ke čtení nebo zápisu dat. Každý datový blok paměti může byt šifrován pomocí klíče A, nebo klíče B. Použití jednoho z klíčů je definováno v přístupových bitech bloku. Pro proces autentizace a šifrování přenášených dat je využívána proudová šifra CRYPTO1. [6]

3.5 MiFare DESFire EV1

Po překonání technologie MiFare Classic došlo ze strany výrobce NXP k vývoji nové technologie MiFare DESFire. Ta již obsahuje více bezpečnostních prvků, avšak v roce 2011 byla technologie překonána týmem vědeckých pracovníků z německé univerzity v městě Bochum. NXP však ještě před překonáním DESFiru zavedla modifikaci MiFare DESFire EV1, která je v současnosti stále považována za nepřekonatelnou a tudíž dostatečně bezpečnou a to při zachování poměrně nízkých ekonomických nákladů. [18]

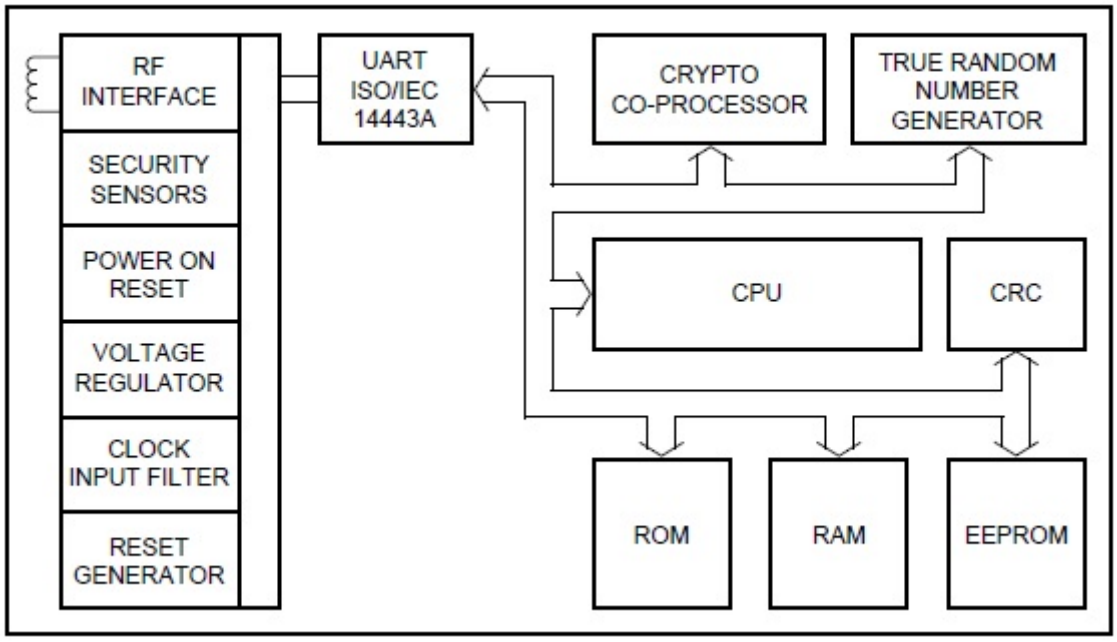
MiFare DESFire EV1 je vyráběna s třemi velikostmi paměti 2K, 4K a 8K. Technologie je certifikována bezpečnostním certifikátem Common Criteria EAL4+, což svědčí o jejím zabezpečení. Díky tomu je tato technologie vhodná ve spoustě aplikacích jako je veřejná přeprava, přístupové systémy, nebankovní platební karty atd. Karta nabízí vyšší přenosovou rychlost dat, větší bezpečnost přenosu a více flexibilní organizaci paměťového prostoru. MiFare DESFire EV1 je plně založena na standardu ISO/IEC 14443-A. Karta nabízí integrovaný zálohovací systém a tříprůchodovou autentizaci. Jediná karta může obsahovat až 28 nezávislých aplikací, kdy každá aplikace může využívat až 32 souborů uložených v paměti. Přenosová rychlost je navýšena až na 848 kbit\s a umožnuje velmi rychlý přenos dat. [17]

Hlavním rysem těchto DESFire karet je využití vysoce bezpečných šifrovacích metod 3DES a AES. Šifrování probíhá v hardwarovém modulu, díky čemuž je zajištěna vysoká rychlost šifrování dat. Další výhodou je podpora multi-aplikačního systému, kdy může být karta využívána pro více aplikací, jako jsou bezhotovostní platby, knihovní systémy, přístupové systémy atd., a to při zachování vysoké bezpečnosti a spolehlivosti v jedné kartě.

MiFare DESFire EV 1 nabízí:

- Bezkontaktní přenos dat a napájení
- Čtecí vzdálenost do 100 mm (záleží na tvaru a nastavení čtečky)
- Pracovní frekvenci 13,56 MHz
- Rychlé datové přenosy 106 kbit\s, 212 kbit\s, 424 kbit\, 848 kbit\
- Vysokou integritu dat zajištěnou 16\32 bitovým CRC obvodem, kontrolu paritních a kódovacích bitů
- 7 bajtové UID
- Pamět EEPROM 2K, 4K, nebo 8K
- Životnost dat v paměti 10 let a 500 000 zapisovacích cyklů
- Až 28 aplikací v jedné PICC a 32 souborů na jednu aplikaci
- Certifikaci Common Criteria EAL4+

- Možnost vytvoření 1 master klíče a 14 aplikačních šifrovacích klíčů
- Hardwarový DES šifrovací obvod s možností využití 56\112\168 bitového klíče
- Hardwarový AES šifrovací obvod se 128 bitovým klíčem
- Šifrování RF přenosu
- Anti-kolizní mechanismus



Obr. 11. Vnitřní schéma čipu MiFare DESFire EV1, zdroj: MF3ICDx21_41_81,MiFare DESFire EV1, Rev. 3.1 – 21 December 2010, 145631,dostupné z http://www.nxp.com

Vzhledem k využití 7 bajtového UID je zvýšena základní bezpečnost. Naneštěstí je UID stejně jako u verze MiFare Classic přenášeno během tříprůchodové autentizace nezašifrované a je možné jej tak přečíst a dále falzifikovat. Při procesu autentizace pak dochází již k šifrování pomocí některého z hardwarových šifrovacích modulů (DES, 2K3DES, 3DES, nebo AES).

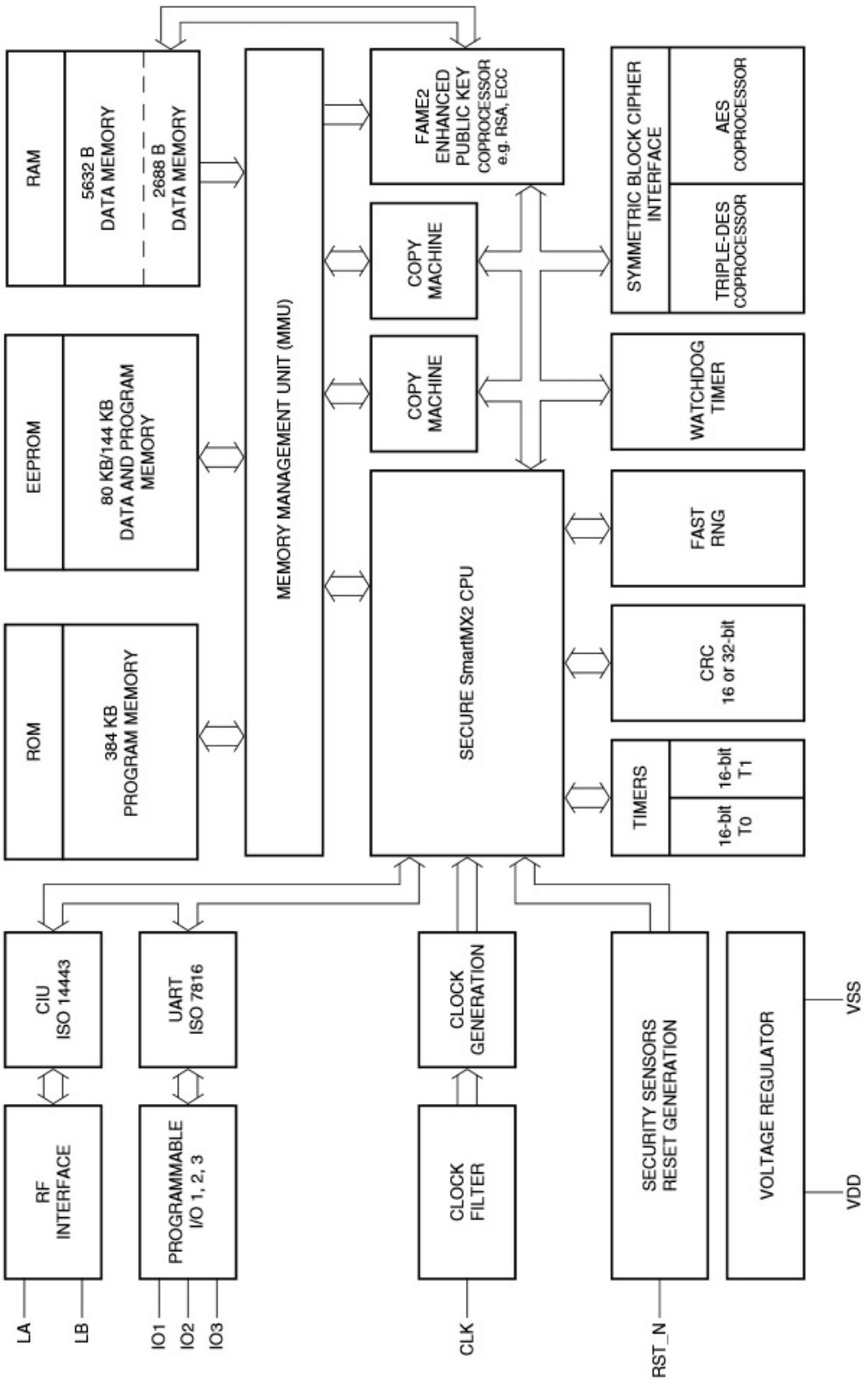
Tuto technologii můžeme považovat za bezpečnou za předpokladu, že je využito šifrované čtení paměti.

3.6 SmartMX2

Technologie SmartMX2 lze považovat za poměrně novou a velice bezpečnou technologii. Jedná se o vysoce výkonnou ICC kartu s duálním rozhraním pro komunikaci. Výrobcem je společnost NXP semiconductors a je to jedna z celosvětových vysoce bezpečnostních technologií. SmartMX2 je funkční platforma pro bezpečné a rychlé datové transakce realizované kontaktně, či bezkontaktně. Technologie je vhodná pro aplikace v oblasti elektronické správy vládních aplikací tzv. eGovernmentu, bankovnictví a veřejné dopravy. SmartMX2 nabízí pokročilou odolnost proti útoku a vysoký výkon podporovaný silnými kryptografickými koprocesory s minimální spotřebou energie. SmartMX2 patří do kategorie karet smart karet, které v sobě kombinují vysoce bezpečnostní šifrovací mechanismy s poměrně velkým paměťovým prostorem s možností výpočtů dat integrovaným mikroprocesorem. [19]

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
- Kopírovací mechanismy pro vnitřní přenosy dat z registrů a pamětí bez nutnosti zásahu CPU
- 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)
- Podpora současného přenosu dat pomocí obou rozhraní
- Možnost implementace podpory pro technologii MiFare Classic a MiFare DESFire EV1



Obr. 12. Vnitřní schéma čipu SmartMX2, zdroj: SmartMX2 family P60D080 and P60D144, Rev.1 – 1 September 2010, 197210, dostupné z http://www.nxp.com

RFID technologie SmartMX2 je vybavena bezpečnostním certifikátem Common Criteria EAL6+. Výrobce doporučuje využití této technologie především pro potřeby eGovernmentu, pod kterými si lze představit především e-pasy, elektronické občanské průkazy, zdravotní karty, elektronické řidičské průkazy. Využití je dále doporučeno pro bankovní aplikace (kontaktní a bezkontaktní platební karty), pro velmi bezpečné přístupové systémy na logické i fyzické úrovni, pro potřeby autentizace zařízení, popřípadě pro různé potřeby veřejné dopravy. [19]

4 METODY PŘEKONÁNÍ ZABEZPEČENÍ RFID A ACS

Tak jako v ostatních oborech je vývoj RFID technologií doprovázen i vývojem technologií k jejich překonání. Je možné a velice pravděpodobné, že časem dojde k prolomení i technologie MiFare DESFire EV1. V případě, že chceme zachovat naši RFID aplikaci bezpečnou je nutné neustále sledovat vývoj a aktualizovat bezpečnostní opatření.

4.1 Překonání zabezpečení technologie RFID

V následujících podkapitolách jsou uvedeny metody pro překonání samotné RFID technologie. Jedná se zpravidla především o falzifikaci originálního RFID tagu získáním UID, nebo šifrovacího klíče, či algoritmu, na jehož základě může být vyroben falzifikát nerozeznatelný od originálu.

4.1.1 Zkopírování UID

Nejjednodušší metoda překonání bezpečnosti RFID je zkopírování UID čísla čipu. Zůstává otázkou zda-li se vůbec jedná o překonání bezpečnosti, neb technologie EM4100 není vybavena žádnou ochranou proti kopírování.

Po přečtení UID z originálního tagu lze toto číslo zapsat do nenaprogramované karty, která se posléze tváří jako karta originální. Bohužel neustálým vývojem technologií dochází výrobě více sofistikovanějších zařízení a to při zachování nízké pořizovací ceny. Takovým příkladem jsou kopírovací zařízení RFID karet. Ty lze dnes jednoduše objednat přes Internet za náklady 1000 až 2000Kč. RFID kopírovací zařízení je většinou kompatibilní s jedním formátem karet nejčastěji EM4100.

Obr. 13. Kopírovací zařízení EM marin karet, zdroj: http://www.ebay.com

Bezpečnost EMmarin aplikací je tak snížena na absolutní minimum. V ČR je většina společností zabývající se kopírováním klasických mechanických klíčů vybavena těmito kopírovacími zařízeními a tím se možnost zkopírování stává velice dostupnou. V přístupovém systému nelze po zkopírování nijak rozeznat, že se jedná o zkopírovanou kartu, avšak vždy je jednoznačně stanoven držitel originální karty. Tím lze poměrně úspěšně dospět k osobě, která kartu nechala zkopírovat.

Při vhodné úpravě čtecí antény kopírovacího zařízení lze pak vytvořit nástroj na nenápadné zkopírování RFID karty, kdy nic netušícímu držiteli je karta zkopírována, aniž by muselo dojít k fyzickému kontaktu, popřípadě k blízkému přiblížení. Takové zařízení pracuje na baterie a je tedy mobilní. V případě požadavku na delší čtecí vzdálenosti lze například i modifikovat některou z vyráběných čteček s dlouhým dosahem.

Obr. 14. Mobilní kopírovací čtečka s dlouhým dosahem, zdroj: http://www.proxclone.com

V případě nenápadného zkopírování karty pak může docházet k jejímu zneužití po velice dlouho dobu bez menšího povšimnutí.

Jako vhodnou ochranu volíme nahrazení technologie s čtením UID vyspělejším technologickým celkem, který identifikuje subjekt na základě dalších dat uložených v paměti RFID tagu.

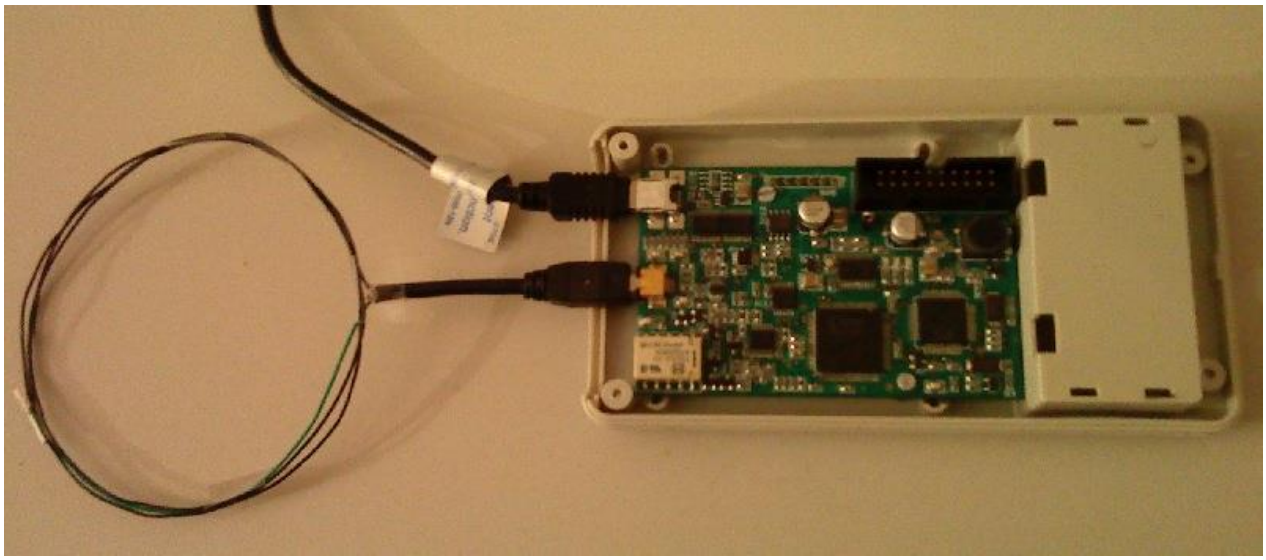
4.1.2 Prolomení klíče pomocí postranních kanálů

Tato metoda je založena na sledování fyzikálních veličin vyskytujících se v blízkosti karty. Jedná se o složitější metodu, kde není jejím cílem získání dat, ale odhalení vnitřních pochodů integrovaných obvodů, na jejichž základě lze zpětně sestavit algoritmus pro odhalení šifrovacích klíčů. Po účely této metody je využívána časová analýza, odběrová analýza, analýza elektromagnetického pole, nebo útoku zaváděním chyb.
Při časové analýze je měřenou veličinou čas, který je potřebný pro vyslání odpovědí zpět v závislosti na typu prve vyslaných dat. Odběrová analýza je měřena poměrně jednoduše v závislosti na stavu elektromagnetického pole čtečky, protože RFID čip je napájen přímo

z tohoto EM pole. Jedním z dalších možností jak zjistit informace o RFID technologii je úmyslné zavádění chyb, které mohou poodhalit slabiny technologie. To lze například způsobit překročením různých fyzikálních limitů stanovených výrobcem jako je vystavení čipu extrémním teplotám, přepětím nebo podpětím atd. To vše může způsobit nestandardní vnitřní pochody integrovaných obvodů, které mohou mnohé prozradit. [20].
Této metody bylo právě využito pro překonání technologie MiFare DESFire v roce 2011, kdy došlo k odhadnutí vnitřních pochodů šifrovacího čipu pomocí sledování elektromagnetického pole kolem karty a za 7 hodin byly šifrovací klíče odhaleny. To vše za pomoci vybavení za 50 tisíc korun. I přesto výrobce tvrdí, že opakování této metody prolomení je velice náročné, a tedy technologii MiFare DESFire lze považovat za vysoce bezpečnou.

4.1.3 Prolomení klíče pomocí odečtení z čtečky a karty

Tento typ překonání se anglicky nazývá Key Recovery Attack a je určena především pro překonání technologie MiFare Classic. Principem této metody je postupné odečítání přenášených dat mezi čtečkou a kartou. V případě přečtení RFID tagu získáme informaci o vnitřním stavu a za předpokladu znalosti principu posuvného registru použitého pro šifrování CRYPTO1 jsme schopni odhalit šifrovací klíč. Pro odchycení komunikace je zapotřebí speciální čtečka například Proxmark 3 s propojením do počítače, který musí být vybaven odpovídajícím softwarem. Po dostatečném přečtení dat je možné odhalit šifrovací klíč. [21]



Obr. 15. Čtečka Proxmark 3 s externí anténou, zdroj: https://code.google.com/p/proxmark3

4.1.4 Překonání proudové šifry CRYPTO1

Proudová šifra CRYPTO1 byla využita pro zabezpečení přenosu dat u technologie MiFare Classic. Jak se později ukázalo, toto zabezpečení se stalo naopak slabinou. Společnost NXP drží přesný algoritmus stále v tajnosti, avšak metodou reverzního inženýrství již došlo k odhalení procesu šifrování. Postupně docházelo k dalším odhalení, které vedly ke stále časově efektivnějším útokům na toto zabezpečení. Pseudonáhodný generátor čísel obsažený v čipu pracuje pouze s 16 bity, díky čemuž dochází k neustálému opakování čísel během necelé minuty při běžné přenosové rychlosti. Při každém zapnutí registru pak dochází k resetování generátoru na počáteční stav, čímž dochází ke ztrátě náhodnosti čísel. Tím lze vycházet vždy z počátečního stavu a kontrolovat tak čas mezi zapnutím generátoru a autentizací [20]

Posuvný 48 bitový registr používaný pro generování bitového proudu šifrovacího klíče využívá pouze bity č. 9 až 47. Rozdělením na sudé a liché bity dostaneme dvě skupiny čísel, které jsou použity pro generování 2 nových bitů. Pokud známe hodnoty těchto nových dvou bitů, můžeme vyloučit bity, které negenerují správné proudové bity klíče. Takto můžeme postupně odhalit klíč z každého paměťového sektoru. Dle normy musí být každý přenášený bajt doplněn o lichý paritní bit. Bohužel tento paritní bit je vypočítán z otevřeného textu a nikoliv ze zašifrovaného. Díky tomu nedochází k posunu registru a tím dojde k zašifrování předchozího paritního bitu a prvního bitu následujícího bajtu stejným bitem proudového klíče. Po následné kontrole může dojít ke zjištění nesprávně nastaveného paritního bitu a tím dojde k zablokování karty pomocí příkazu HALT. Jestliže jsou však všechny bity v pořádku, ale odpověď čtečky je nesprávná, neb není znám šifrovací klíč, dojde k zaslání odpovědi NACK z čipu. Tato odpověď je již zašifrovaná a tím můžeme získat až 4 bity proudového klíče. Takto můžeme postupně zrekonstruovat celý klíč a překonat tak šifrování CRYPTO1.

Metod pro překonání MiFare Classic potažmo proudové šifry CRYPTO1 je více. Většina metod je založena na matematických operacích a znalosti principu algoritmu tohoto šifrování. O objevení těchto metod se zasloužili především Flavio D. Garcia a Nicolas T. Courtois.

Jedná se o tyto následující metody:

- Courtoisův útok – vyžaduje přibližně 335 autentizačních pokusů spojených s výpočty matematických operací. Pro odhalení klíče je využito malé variability

proudového klíče s využitím diferenční kryptoanalýzy. Courtoisovou metodou lze odhalit až 42 bitů vnitřního stavu šifry, avšak zbylých 6 bitů je nutné odhalit pomocí hrubé síly. [20]

- Garciův útok s konstantním Nt – pro účely této metody je potřeba využívat přesného časování a udržování konstantní výzvy RFID čipu. K získání klíče je opět nutná znalost vnitřního stavu posuvného registru, který můžeme vždy, vzhledem k lineární závislosti, posunout do výchozího stavu. Dále je pak hledán každý 8 bit, který ovlivňuje proudovou šifru. F.D. Garcia uvádí, že pro překonání šifrování CRYPTO1 touto metodou je nutné využít 28 500 dotazů k nalezení množiny bitů, po jejichž odhalení je nutné dále provést $436 \cdot 2^{24}$ kombinací vnitřních stavů šifry za využití zpětného posouvání registru. [21]
- Garciův útok s konstantním Nr – obdobná metoda jako předchozí, avšak zde předpokládáme neměnnou hodnotu paritních bitů a Nr. Vytvořením tabulky všech možných vnitřních stavů šifry s nastavením paritních bitů na nulu. Poté zkoušíme provést autentizaci, dokud neobdržíme odpověď zašifrovanou klíčem odpovídajícím nulovým hodnotám paritních bitů. Dále pak předpokladem zpětného posunu registru hledáme klíč. Nevýhodou této metody je, že vytvořená tabulka obsahuje až 384 GB dat. Další matematicko – logickou úpravou však můžeme získat tabulku o velikosti 96MB.

Vzhledem k více možným metodám překonání, které byly již několikrát ověřeny, společnost NXP Semiconductors přestala využívat technologii šifrování CRYPTO1 a přešla na jiné šifrovací algoritmy DES, 3DES a AES, využité v technologii MiFare DESFire EV1,

4.1.5 Prolomení hrubou silou

V souvislosti se zabezpečením RFID a jejích aplikací získává metoda prolomení hrubou silou více významů. V rámci ACS, nebo jakýchkoliv prvků MZS (Mechanické zábranné systémy) můžeme hovořit o jejich fyzickém překonání. Avšak metodu překonání hrubou silou máme na mysli především v oblasti informatiky. Jedná se o metodu, která slouží k odhalení hesla, šifrovacího klíče a jiných bezpečnostních datových řetězců.

Metoda je založena na vyzkoušení všech různých možných kombinací dané délky. V případě, že využíváme v rámci ACS nezabezpečené RFID EM marin (např. EM4100) pak je obsažena 64bitová paměť, ze které je použito 40 bitů pro UID. Tzn., že je k dispozici 2^{40} kombinací což je 1 099 511 627 776 možností UID. Pro vyzkoušení všech kombinací by bylo nutné vytvořit generátor UID, který postupně vyzkouší všechny možné kombinace. Jednoduchým výpočtem zjistíme, že při předpokladu doby testování 1ms jedné kombinace by doba pro vyzkoušení všech kombinací trvala 34 let.

V případě bezpečnějších technologií MiFare DESFire je využito šifrování DES, 3DES a AES. DES nabízí délku klíče 56bitů, tzn. 2^{56} kombinací. 3DES je pak šifrován klíčem o délce 168 bitů. AES využívá 128 bitů. Díky delší bitové délce je metoda hrubé síly neefektivní, neb prolomení bezpečnosti klíče, či kódu zabere poměrně dlouhou dobu. U více bezpečnostních aplikací je pak možné tyto klíče za danou periodu obměnit a tím pádem znemožnit překonání hrubou silou. Doba obměny klíče musí být menší než teoretická potřebná doba pro překonání hrubou silou.

4.2 Metody překonání systému ACS

Bezpečnost RFID technologie zajišťuje pouze přenos a uchování dat v paměti tagu. RFID tag však musí spolupracovat se systémem, který s ním dokáže komunikovat a generovat akci v závislosti na průběhu identifikace. Překonání zabezpečení se pak nemusí týkat pouze samotné technologie RFID, ale i dalších částí identifikačního systému.

4.2.1 Fyzické zcizení

Zcizení vlastního RFID tagu nelze jistě považovat za samotné překonání RFID technologie, avšak je důležité si připomenout, že i sebe lepší RFID technologie, které využívá různé „nepřekonatelné“ metody, má stále slabé stránky. Odcizení RFID tagu má primárně za cíl jeho zneužití v konkrétním typu aplikace. Používáme-li tag v systému kontroly vstupu, pak pachatel získá přístup do zabezpečeného prostoru, kde může napáchat škody. V případě citlivých aplikací jakou jsou ACS v jaderných elektrárnách může mít zcizení RFID tagu nedozírné následky. Takovýchto velmi citlivých aplikací ACS je celá řada například objekty bankovního sektoru, vědecké ústavy, vojenské objekty, vládní objekty atd.

Je-li RFID používáno pro bezhotovostní platby, pak je opět nasnadě zneužití po zcizení. Dnešní bankovní ústavy nabízí využívání tzv. bezkontaktních karet, kde je většinou nastaven limit platby 500 Kč bez nutnosti zadávání autentizačního PIN (Personal Identification number – osobní identifikační číslo) kódu. Takto lze pak jednoduše vyčerpat peněžní obnos na daném bankovním účtu.

Ve výsledku je tedy nutné jistě využívat RFID s maximální možnou mírou bezpečnosti, avšak je rovněž velmi důležité přizpůsobit celou aplikaci bezpečnostním požadavkům, které nesmí být opomíjeny. V případě zcizení je nutná co nejrychlejší detekce ztráty RFID tagu, oznámení správci aplikace a jeho okamžitá reakce v podobě zamezení oprávnění dané karty v systému.

4.2.2 Sociální inženýrství

Dalším důležitým aspektem, který je nutný brát v potaz, je fakt, že aplikované režimové bezpečnostní opatření jsou vždy založeny na předpokladu užívání uživateli. Uživatel jakékoliv aplikace je poměrně slabou stránkou celého systému. Metoda sociálního inženýrství je v dnešní době velice často používána, aniž bychom si to uvědomovali. Obecně lze říci, že se jedná o psychické ovlivnění subjektu na základě přenosu informací od druhého subjektu.

Typickým příkladem v rámci ACS je instalace zabezpečení objektu bytového domu pomocí ACS, kde je provedena integrace se systémem domácích telefonů DT. Základní integrace spočívá v možnosti ovládání bezpečnostního elektronického zámku ze systému DT. Vydáváním se za jinou osobu je pak možné přesvědčit obyvatele domu, aby otevřel zámek a vpustil tuto osobu do chráněného prostoru. Bohužel se jedná o velice častý případ narušení bezpečnosti domu, zvláště u seniorů, kteří jsou více důvěřivý. Z tohoto hlediska je pak vhodná ochrana objektu odpojením ovládání zámku ze systému DT. Obyvatelé pak v případě nutnosti musí fyzicky dojít na místo požadovaného vstupu a na základě své úvahy umožnit vstup.

Další možností využití sociálního inženýrství je například pro účely zkopírování RFID karty, zapůjčení svazku klíčů, kde rovněž bývá často samotný RFID tag v podobě přívěsku. Svazek klíčů si lze zapůjčit za jakoukoliv jinou záminkou a pak již lze v případě využití

méně bezpečné RFID jednoduše zkopírovat UID, aniž by majitel měl tušení o pravém smyslu zapůjčení svazku klíčů.

Příkladů pro metodu sociálního inženýrství by asi šlo nalézt nespočet. Důležitým faktem proč si tuto metodu připomínáme, je opět pohled na celou bezpečnostní aplikaci včetně započítání lidského faktoru, popřípadě snížení chybovosti lidského faktoru na minimální úroveň. V případě, že chráníme velice citlivé statky, je nutné zavést pak i různá pravidla a režimová opatření.

4.2.3 Zachycení přenášených dat

Další možností jak překonat identifikační systém založený na RFID je tzv. odposlech vedení. Tato metoda je založena na zachycení dat z přenosové trasy mezi čtečkou a kontrolerem a jejich opětovném vyslání do systému.

V závislosti na hierarchii použitého systému lze použít více přenosových tras pro zachycení dat. Základní přenosovou trasou je spojení mezi samotnou čtečkou a terminálem pro zpracování dat. V současnosti je v systémech ACS využíváno přenosového protokolu Wiegand, který vzhledem ke své době zavedení není nijak zabezpečen. Protokol je přenášen datovými vodiči D0 a D1, kde jednoduše dochází ke změně stavu podle přenášeného řetězce. Čtečka přečte bitový kód UID a převede jej na signály DO a D1. Zachycení přenášeného řetězce lze pak pomocí speciálního zařízení jednoduše zaznamenat a poté tento řetězec znovu vyslat do systému. Kontroler pak v závislosti na přijímaných datech provede akci. V případě simulace prezence oprávněné karty v systému ACS dojde například k otevření zámku apod. Některé systémy ACS používají pro zabezpečení této komunikace šifrování AES se 128 bitovým klíčem se systémem výměny klíčů Diffie-Hellman.

Další možností zachytávání dat je přenos dat po sběrnici RS 485, která je zpravidla využívána pro komunikaci dveřních terminálů s kontrolerem. Přenosové protokoly těchto sběrnic dnes využívají rovněž různých ochranných prvků. S masovým využitím datových sítí přichází také přenos dat mezi terminálem a kontrolerem po Ethernetu. V takovém případě je pak nezbytné využití šifrovacích metod, neb při zapojení hardwaru do místní sítě LAN může kdokoliv získat přístup k přenášeným datům.

Na druhou stranu metoda zachycení přenosu dat je založena na předpokladu fyzického připojení odposlechového zařízení k přenosové sběrnici. Realizace tohoto připojení je poměrně obtížná, neb při dodržení bezpečnostních pravidel pro instalaci poplachových systémů, musí být veškerá kabeláž vedena skrytě a vhodně chráněna proti manipulaci. Základním pravidlem je pak vedení kabeláže ve vnitřních chráněných prostorách. Pokud je již narušitel v prostoru, který má být napaden, pozbývá smyslu připojení se na komunikační sběrnici pro získání přístupu do objektu. V případě odposlechu Wiegand přenosu ze čtečky je připojení mnohem snazší, neb čtečku lze většinou demontovat z venkovní strany. Demontáží čtečky jsou odhaleny vodiče, na které se lze připojit. Aby mělo smysl komunikaci zachytávat, je nutné čtečku nainstalovat zpět, aby procházející uživatelé vytvořili několik transakcí, které jsou vhodné pro zachycení. Z tohoto důvodu musí být odposlechové zařízení instalované nenápadným způsobem. Moderní systémy ACS využívají tamper ochranu čteček, kdy po demontáži čtečky dojde k přenosu informace o poškození krytu. V závislosti na této poplachové transakci může být zaslána notifikační zpráva prostřednictvím emailu nebo SMS, popřípadě může dojít k sepnutí relé výstupu a aktivaci akustického, či optického indikátoru.

4.3 Zvýšení bezpečnosti identifikace osob

Vzhledem k výše popsaným metodám překonání stávajícího zabezpečení identifikačních systémů je vhodné tyto systémy neustále zdokonalovat a využívat tak stále modernější metody ochrany dat. Nicméně i při sebe lepším zabezpečení samotné RFID je možné RFID tag ztratit, poškodit, či jej zcizit. Po úmyslném zcizení tagu získá neoprávněná osoba možnost falzifikace identity. Pro tyto případy je vhodné zavést proces ověření identity.

4.3.1 Identifikace – autentizace

Po přiložení RFID tagu ke čtečce dojde k přenosu informace, která má za následek identifikaci subjektu. Jak již bylo naznačeno, v případě, kdy z jakéhokoliv důvodu bude vlastnit RFID tag neoprávněná osoba dochází k podvržení identity a možnosti zneužití. Ochrana před takovým zneužitím spočívá v zavedení doplňkového procesu ověření identity tzv. autentizace. Při zavedení procesu autentizace je po prvotní identifikaci vyžadována doplňující informace, která zajistí pravost subjektu. Autentizace je vhodná pro chráněné objekty s vysokou mírou bezpečnosti.

Autentizace v ACS lze provést několika způsoby:

- **PIN kódem** – v databázi systému je vedle čísla tagu uložen i PIN kód, který je vyžadován po přiložení karty, jinak nedojde k ověření identity. Ačkoliv je autentizace PIN kódem účinný nástroj k ověření identity, nelze zaručit, že PIN kód nebude prozrazen. Například při zadávání kódu uživatelem, lze při nesprávném krytí klávesnice kód vypozorovat a pak ověření ztrácí účinnost.
- **Druhým RFID tagem** – po přiložení RFID karty uživatele musí dojít k jejímu ověření přiložením druhé oprávněné karty. Takovýto režim lze například nastavit, je-li na konkrétním vstupu přítomna fyzická ostraha, která může svou oprávněnou kartou autentizovat vstupující osoby. Pro ověření identity může sloužit fotografie držitele karty, kterou lze buď vytisknout přímo na RFID kartu, popřípadě může být uložena v databázi systému. V případě druhé možnosti je pak po přiložení karty ke čtečce zobrazena fotografie na monitoru. Autentizace zde plně závisí na rozpoznávacích schopnostech ostrahy. Při využití umění vyzážistů je však možné upravit vzhled za účelem falzifikace identity. Tedy ani tato metoda autentizace není 100% účinná.
- **Biometrickými údaji** – nejúčinnějším nástrojem pro ověření identity je doplnění biometrických údajů držitele karty. Pomocí některého z principů biometrického čtení popsaných v další kapitole, lze velice účinně ověřit identitu a zajistit tak vysokou bezpečnost identifikačního systému. Tohoto principu plně využívají současné e-pasy, kde jsou v paměťové části tagu uloženy biometrické údaje, které jsou v případě kontroly přečteny a porovnány s biometrickými údaji právě kontrolovaného subjektu.

Tyto uvedené metody lze samozřejmě kombinovat mezi sebou a je tak možné vytvořit velmi bezpečný přístup v kombinaci RFID tagu, PIN kódu a biometrických údajů.

4.3.2 Biometrické čtení

Pod pojmem biometrické čtení rozumíme jakékoliv opakovatelné měření fyzikálních veličin na lidském těle. Spolu s vývojem technologií v oblasti elektroniky, se dnes biometrické čtečky stávají denní součástí běžného života. Nejčastěji používaným typem biometrické čtečky je čtečka otisku prstu. S ní se můžeme setkat například na mobilních telefonech, noteboocích a samozřejmě v systémech ACS.

V rámci ACS u objektů s nižší mírou bezpečnosti je proces autentizace biometrickými údaji vynechán a rovnou je zavedena identifikace pomocí biometrických údajů. U aplikací s vyšší mírou bezpečnosti je pak plně využíván principu autentizace popsaný v předchozí kapitole. Samozřejmě je i možné provést identifikaci i autentizaci pomocí biometrických údajů bez využití RFID.

Namátkově jsou uvedeny jednotlivé typy biometrického čtení:

- otisku prstů
- krevního řečiště prstu
- krevního řečiště dlaně
- oční rohovky, či duhovky
- 3D skener obličeje
- dynamiky chůze
- odrazu zvuku v ušním boltci
- dynamiky hlasu

Pro biometrické údaje lze použít prakticky jakýkoliv fyzikální jev vytvářený lidským tělem, který musí splňovat podmínky jedinečnosti. V budoucnu bude možné provést identifikaci osob na základě DNA (Deoxyribonucleic acid – kyselina deoxyribonukleová). V současnosti lze provést DNA identifikaci, avšak délka procesu je značně zdlouhavá a tedy absolutně nevhodná pro okamžitou identifikaci.

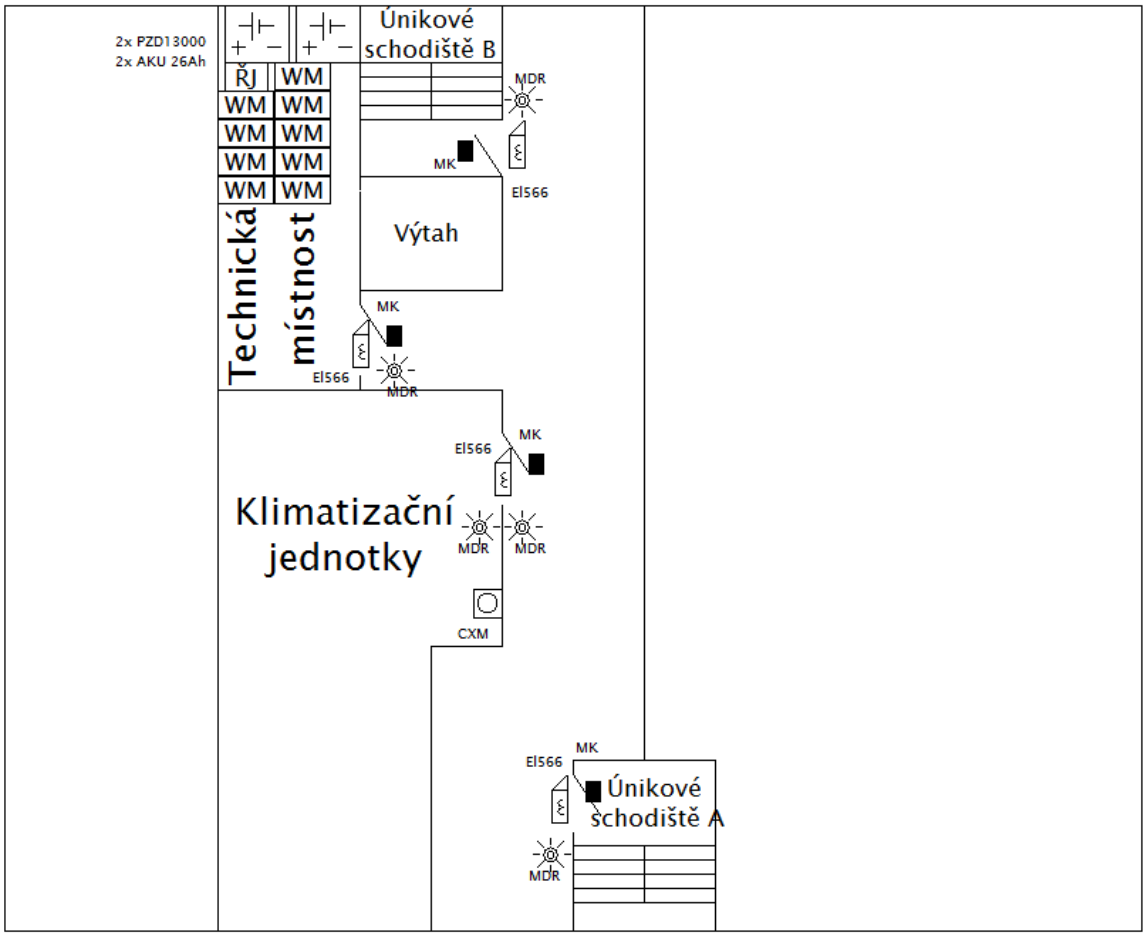
II. PRAKTICKÁ ČÁST

5 NÁVRH BEZPEČNÉHO SYSTÉMU ACS

Při navrhování systému ACS je nutné brát v úvahu jaké hodnoty jsou zabezpečované celky a jakou možnou ztrátu může způsobit jejich krádež, poškození, nebo jejich ovlivnění. Tyto údaje by měly být patrné z bezpečností analýzy zabezpečovaného objektu. V případě bytového domu není cílem zajistit maximální bezpečnost nýbrž optimální bezpečnost na rozumné úrovni. Při návrhu systému je také samozřejmě vytvářen tlak na ekonomickou stránku věci, takže je většinou nutné volit kompromis mezi dostupnými technologiemi, smyslem zabezpečení a ekonomickými náklady.

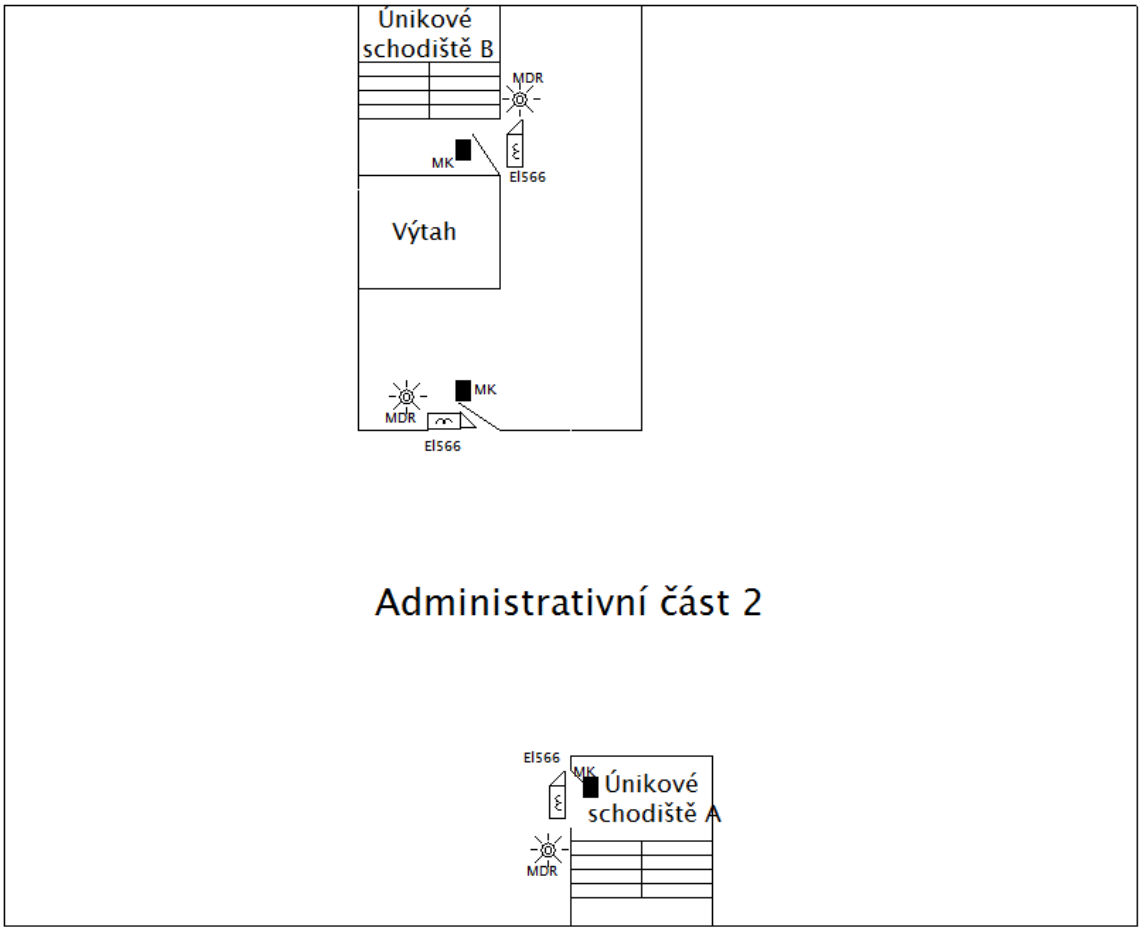
5.1 Popis objektu

Pro účely návrhu maximálně bezpečného systému ACS vytvoříme modelovou situaci objektu s vysoce hodnotnými statky. Účel modelového objektu bude datové centrum s administrativní částí splňující podmínky pro zavedení pod chráněné objekty krizové infrastruktury, kde je nutné zajistit maximální bezpečnost jak z pohledu ochrany dat, výpočetního hardwaru, ale i ochrany objektu.

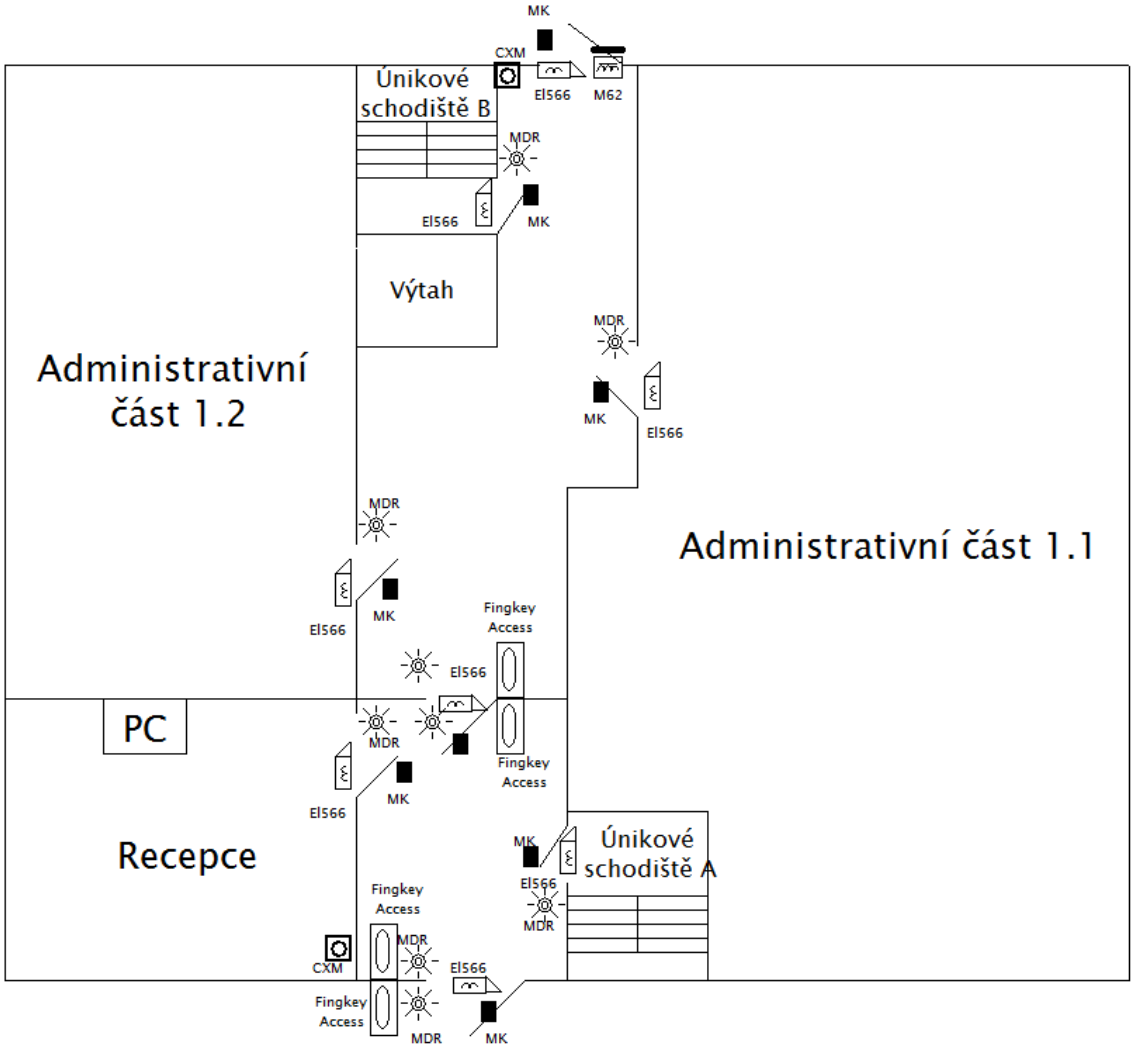


Obr. 16. Schéma rozmístění komponent ACS v 3.NP, zdroj: vlastní archiv autora

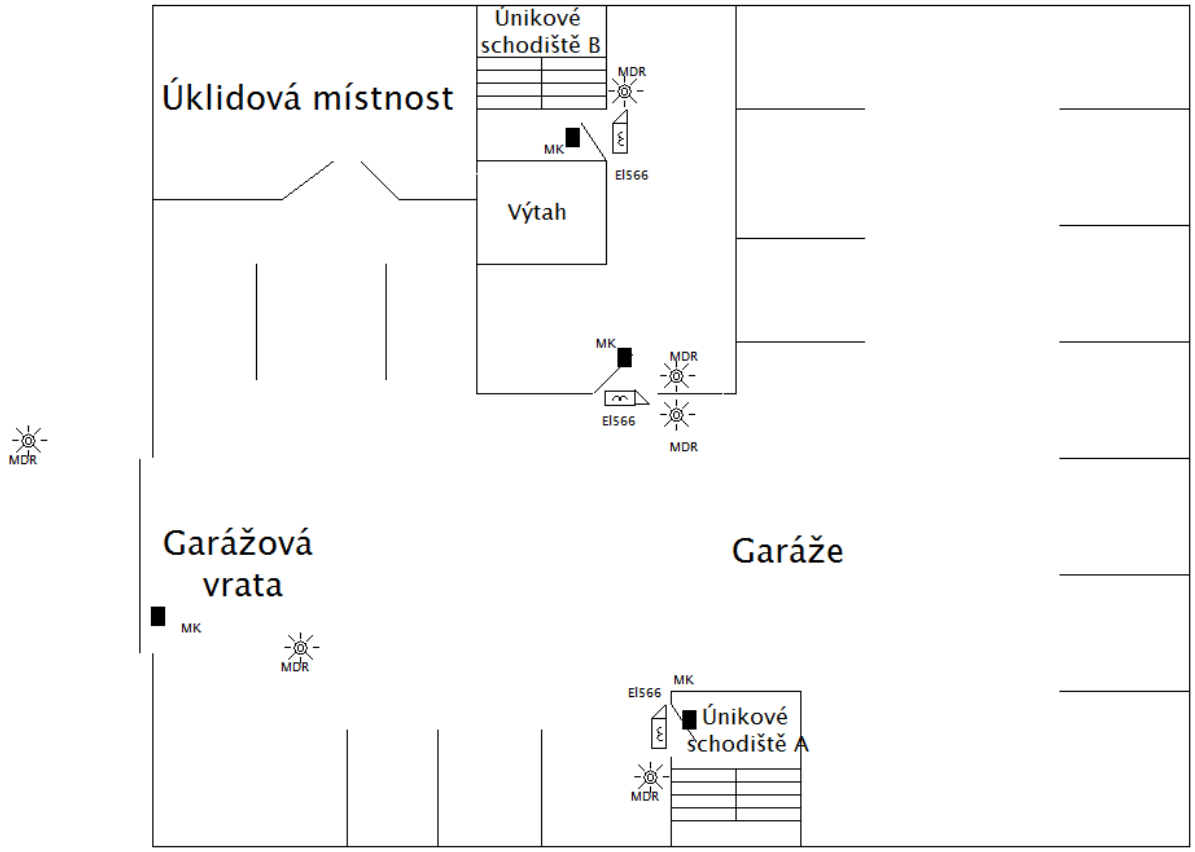
Objekt je šesti podlažní dům s třemi podzemními a třemi nadzemními podlažími. V nadzemní části je obsažena administrativní část budovy, kde jsou kancelářské prostory a v nejvyšším patře jsou klimatizační jednotky. V 1.PP jsou garáže, v 2.PP samotné datové centrum a v 3.PP jsou sklady, rozvodna elektrické sítě a prostory pro záložní napájecí zdroje UPS (Uninterruptible Power Supply – nepřerušitelný zdroj energie).



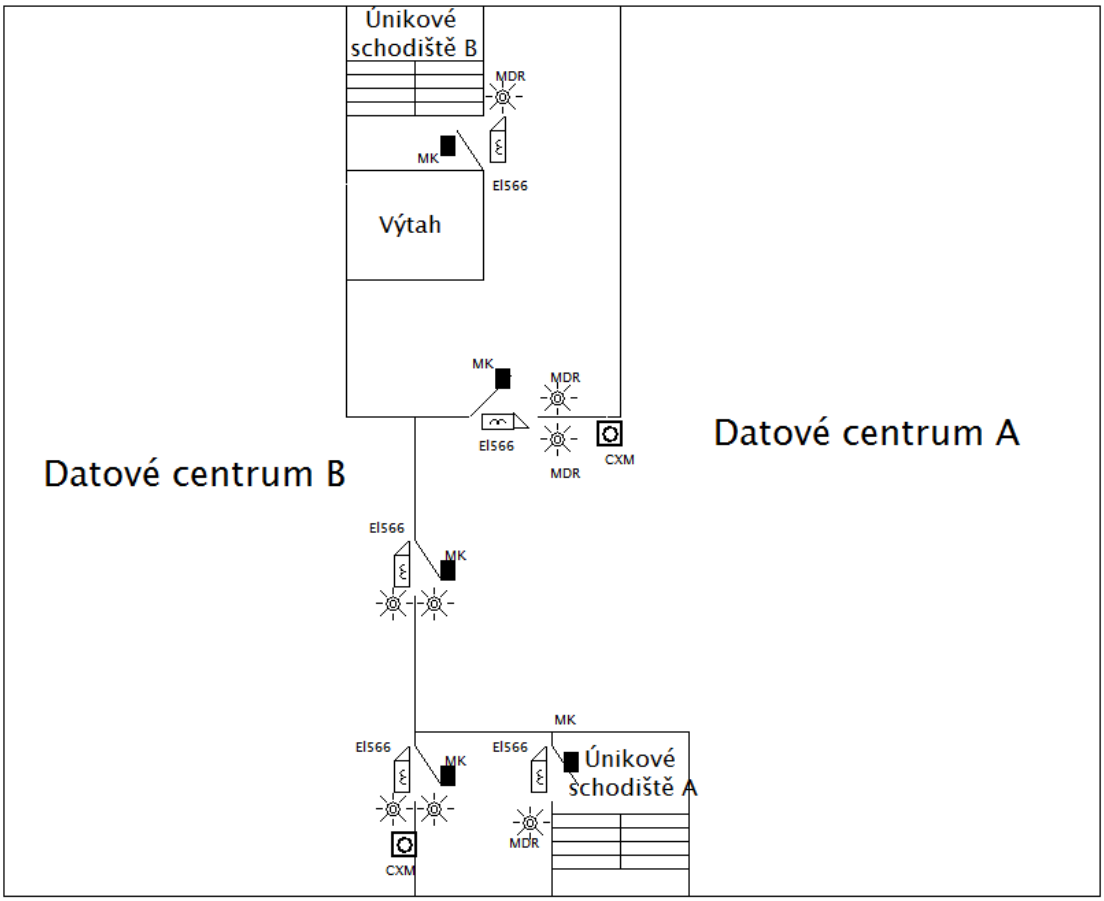
Obr. 17. Schéma rozmístění komponent ACS v 2.NP, zdroj: vlastní archiv autora



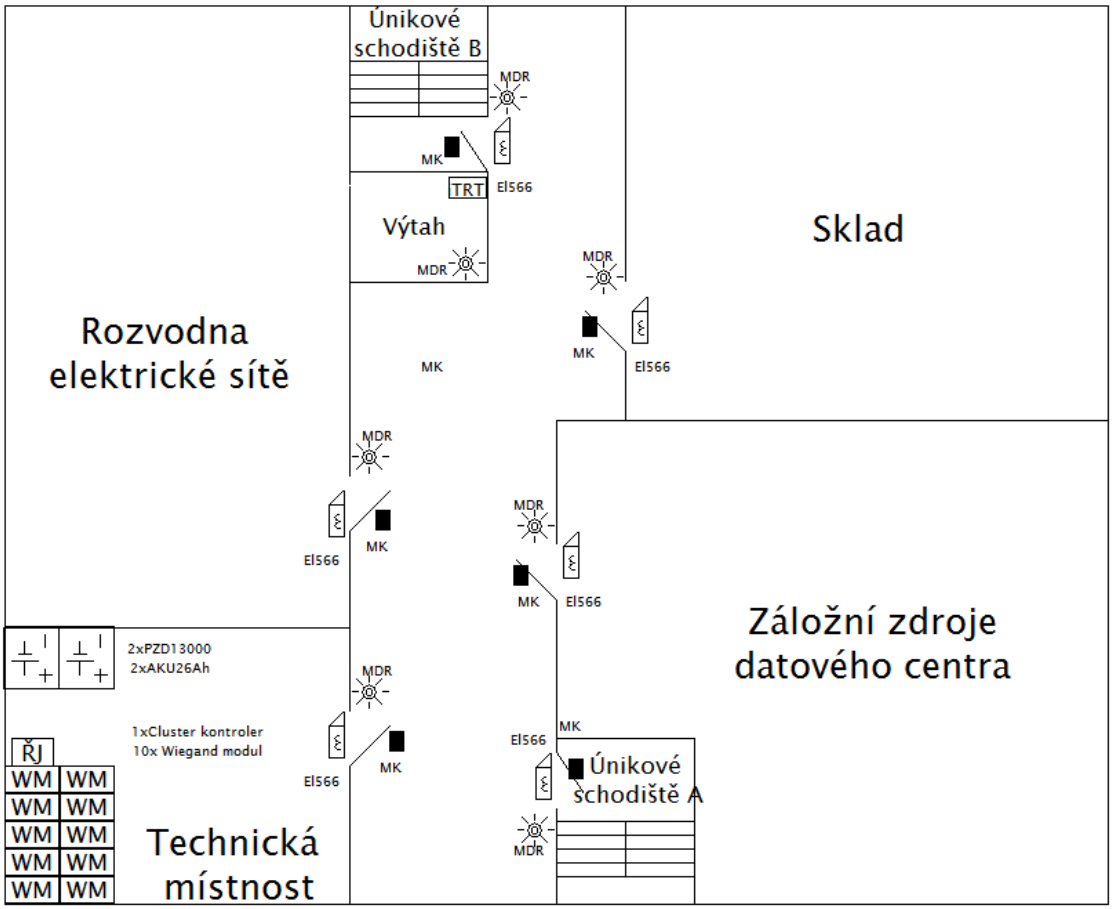
Obr. 18. Schéma rozmístění komponent ACS v 1.NP, zdroj: vlastní archiv autora



Obr. 19 . Schéma rozmístění komponent ACS v 1.PP, zdroj: vlastní archiv autora



Obr. 20 . Schéma rozmístění komponent ACS v 2.PP, zdroj: vlastní archiv autora



Obr. 21. Schéma rozmístění komponent ACS v 3.PP, zdroj: vlastní archiv autora

5.2 Návrh MZS

Nedílnou součástí ACS jsou prvky MZS, které právě zajištují fyzickou bezpečnost hlídaných vstupů. Na rozdíl od systému PZTS, systém ACS aktivně chrání před vstupem neoprávněné osoby, což je zajištěno prvky MZS v kombinaci s elektronickými zámky ovládanými ze systému ACS.

Vzhledem k faktu, že nejvíce chráněný prostor se nalézá v 2.PP, je především nutné zamezit vstupu právě do těchto prostor včetně kritických částí datového centra. Za kritické částí můžeme považovat prostor elektrické rozvodny, místnost se záložními zdroji a klimatizační jednotku.

Pro plášťové vstupy volíme úměrně bezpečné dveře. Plášťové vstupy do objektu jsou celkem 4. Jedná se o:

- Hlavní vstup v 1.NP
- Zadní únikový východ v 1.NP
- Vstup na únikové schodiště A v 1.PP
- Vstup k výtahu a únikovému schodišti B v 1.PP

Ačkoliv jsou vstupy na únikové schodiště A a B v prostorách garáže chráněny garážovými vraty, považujeme i tyto vstupy za plášťové, kvůli nízké bezpečnosti garážových vrat a potenciálně vysokému riziku vstupu narušitelů přes tyto vstupy.

Vstupy budou vybaveny plnými dveřními křídly s minimální bezpečnostní třídou RC 4 dle ČSN EN 1627. Do těchto dveří budou instalované samozamykací bezpečnostní zámky Abloy EL566 s vícebodovým jištěním Multi-point. Tyto zámky jsou vybaveny bezpečnostním certifikátem pro RC 4, ale díky svému vybavení jako jsou monitorovací kontakty a možnost přenastavení zámku, budou zámky EL 566 využity pro veškeré vstupy. Se zámky bude rovněž instalované bezpečnostní kování Ikon SX03 typu klika-klika rovněž s certifikátem RC 4. Únikový východ v zadní části objektu v 1.NP bude sloužit pouze pro účely únikové cesty, jinak nebude využíván. Vzhledem k vyššímu riziku vstupu narušitele přes tento zadní vstup, jsou dveře doplněny jištěním elektromagnetem M62 s přídržnou silou 545 kg.

Po obvodu budovy jsou v nadzemní části okna, kterými je možné vniknout do prostoru. Na tyto okna budou nalepeny bezpečnostní fólie s certifikací P2A dle ČSN EN 356.

Vstupy do vysoce chráněných prostor budou vybaveny dveřmi s plnou výplní s certifikací RC4 a bezpečnostními zámky EL566 včetně kování SX03.

Jedná se o vstupy do:

- Rozvodny elektrické energie v 3.PP
- Místnosti se záložními zdroji v 3.PP
- Datového centra A v 2.PP
- Datového centra B v 2.PP
- Místnosti s klimatizační jednotkou v 3.NP

Vjezd vozidel bude zabezpečen automatickými sekčními vraty.

Vnitřní stavební otvory budou osazeny pouze standardními dveřmi s RC2 ovšem se zachováním technologie zámků a kování.

Důležitou součástí prvků MZS je rovněž i perimetrická ochrana ve formě plotu. Plot včetně vstupní brány a branky zajišťuje prvotní ochranu proti nežádoucímu vstupu osob. Pro zachování vyšší bezpečnosti této bariéry bude na vrchní části plotu instalován žiletkový drát. Vstupní branka bude vybavena jednoduchým elektrickým otvíračem určeným do venkovních prostor. Automatická posuvná samonosná brána bude zajišťovat bezpečnost vjezdu vozidel. Pro zajištění uzavřené brány bude sloužit doplňkový elektronický vratový zámek GL1M.

5.3 Návrh ACS

Pro účely návrhu maximálně bezpečného systému ACS lze ze současné nabídky výrobců dlouze vybírat, avšak vzhledem k vysoké modernizaci a konkurenci se systémy ACS zásadně neliší. Prakticky nejmarkantnější rozdíly dnes vznikají především v ekonomické položce a dlouhodobé spolehlivosti. Existují i výrobci, kteří jsou zaměření na výrobu ekonomických řešení, které samozřejmě nenabízí tolik možností jako déle etablovaní výrobci. Pro zabezpečení modelového domu využijeme systém Access Portal Pro (dále jen „AP Pro“) od jihoafrického výrobce Impro Technologies (Pty) Ltd. Systémy Impro se vyznačují především velmi dlouhodobou spolehlivostí se zachováním vysoké míry bezpečnosti. Řada přístupových systémů Access Portal je v současnosti nejnovějším produktem tohoto výrobce.

AP Pro je přístupový systém založený na SQL Express databázovém systému. Jeho hlavní předností je správa systému pomocí WEB serveru, který je vytvářen v rámci spuštěné servisní služby na serverové stanici přístupového systému. Výhodou tohoto uspořádání je možný přístup z klientských stanic bez nutnosti instalace jakéhokoliv dalšího softwaru. WEB server je založen na podpoře jazyka HTML5. Díky tomu lze do správy systému přistupovat téměř z jakéhokoliv moderního IT zařízení jako je počítač, tablet, či chytrý telefon. Tímto vysokým uživatelským komfortem se ovládání přístupového systému stává velice jednoduché a především velice rychlé tzn. efektivní. V případě ztráty RFID tagu je otázkou doslova několika vteřin zamezení přístupu daného tagu. To je samozřejmě možné pouze za předpokladu propojení systému ACS do Internetu.

I přes různé metody zabezpečení vzdálené komunikace zůstává připojení jakékoliv poplachové aplikace do Internetu bezpečnostním rizikem. Vzhledem k faktu, že v modelovém objektu bude k dispozici fyzická ostraha, jejíchž jedním z úkolů bude správa RFID tagů a ovládání systému ACS, nebude systém ACS zapojen do veřejné datové sítě. Přístupová oprávnění v rámci softwaru jsou přidělována na základě jednotlivých kompetencí uživatelů, tzn., že pro každého uživatele může být vytvořen jedinečný přístup do ovládání systému. Softwarová přístupová oprávnění budou vytvářena dle zásad normy ČSN EN 50133.

5.3.1 RFID média

Pro aplikaci bezpečného systému ACS je především nutné zvolit vhodnou bezpečnou technologii, ke které bude přizpůsoben technologický celek systému, především pak čtečky a zpracování dat v řídícím kontroleru a databázi.

Z předchozího textu v teoretické části této práce je patrné, že současně bezpečnou nepřekonanou a široce dostupnou technologií pro přístupové systémy je MiFare DESFire EV1. Existují samozřejmě i bezpečnější řešení v podobě technologie SmartMX2, avšak to je vzhledem k poměrně krátké existenci na světovém trhu zatím méně dostupné. Vzhledem k faktu, že bez využití PKI SmartMX2 nabízí v identifikační oblasti totožný postup jako u technologie MiFare DESFire EV1, je pro účely bezpečného přístupového systému vhodné využít již etablovanou technologii MiFare DESFire EV1. Z ekonomického hlediska je rovněž vhodné volit spíše technologii MiFare DESFire EV1.

RFID tagy budou realizovány ve standardní kartě formátu ID-1 dle ISO/IEC 7810. Karta bude potištěna doplňkovými informacemi pro možnost provedení fyzické kontroly, popřípadě k rychlé identifikaci ztracené karty. Na kartě bude vytištěno jméno a příjmení držitele karty, jeho fotografie, logo společnosti a zaměstnanecké ID číslo.

Pro splnění podmínek zákona č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů musí být zaměstnanci udělen souhlas provozovateli se zpracováním osobních dat.

Důležitým aspektem týkajícím se RFID karet je rovněž vytvoření organizačních pravidel, ze kterých bude jednoznačně jasné, že v případě ztráty, nebo zcizení karty je povinnost

neprodleně informovat ostrahu objektu, která dle nastavených režimových opatření musí okamžitě zrušit přístupové oprávnění konkrétní karty.

5.3.2 Čtečky

Čtečky volíme primárně s ohledem na zvolenou technologii RFID tagů. MiFare DESFire EV1 pracuje na frekvenci 13,56MHz a je plně kompatibilní s ISO/IEC 14443-A. Z tohoto hlediska musí i čtečka splňovat kritéria dané touto normou. Odpovídající model čtečky je například MDR901 od totožného výrobce Impro.

Obr. 22. čtečka MDR 901,
zdroj: http://www.impro.net

MDR901 je RFID čtečka moderního vzhledu s krytem z kombinace ABS (Akrylonitril-Butadien-Styren) plastu a nerezové oceli. Čtečka využívá tzv. multi-disciplinární technologii, která spočívá v současném využití dvou pracovních frekvencí 125 kHz a 13,56 MHz, čímž je zaručena kompatibilita se spoustou typů RFID. Pro účely této modelové situace, bude však čtečka nastavena pouze na pracovní frekvenci 13,56MHz. Datový výstup z čtečky bude nastaven do tzv. RAW módu aby došlo k přenesení veškerých dat. MDR využívá Wiegand komunikačního rozhraní, které je při zapojení do dveřního terminálu iTRT šifrováno pomocí 128-bitového AES s Diffie-Hellmanovou výměnou

klíčů. Tím je zabezpečena komunikace čtečky a terminálu proti překonání metodou zachycení a opětovného přenesení dat.

Samotné čtečky MDR jsou chráněny proti demontáži optickým tamperem. Po sejmutí vrchní části dojde ihned k přenosu poplachové informace v rámci systému ACS a k zobrazení poplachu na obslužném monitoru.

Pro vícenásobný proces autentizace doplníme hlavní vstupy biometrickou čtečkou otisků prstů. Systém AP Pro bude nastaven na těchto citlivých vstupech s požadavkem na potvrzení identifikace RFID karty právě pomocí biometrického otisku prstu daného uživatele. Vzhledem k předpokladu maximálního počtu 50 zaměstnanců datového centra můžeme využít například čtečku Fingkey Access s maximálním počtem 1000 otisků prstů uložených v paměti. Čtečka je propojena do AP Pro pomocí TCP/IP protokolu a biometrického serveru, který pracuje jako další servisní služba na serverové stanici. Čtečka Fingkey Access je vybavena 500 dpi optickým skenerem a je rovněž vybavena detekcí živého prstu.

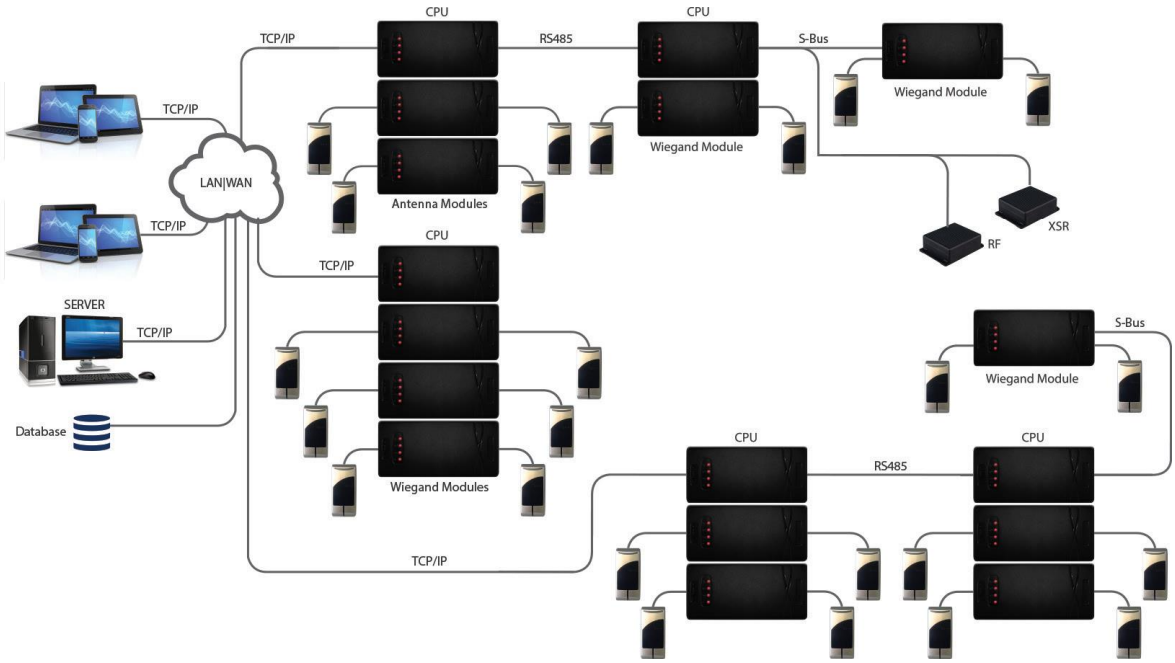
Obr. 23. Biometrická čtečka otisku prstů Fingkey Access, zdroj: http://www.nitgen.com

5.3.3 Struktura – terminály, kontroler

Hierarchie systému je patrná z následujícího obrázku. Koncové zařízení jako jsou zámek, čtečka a dveřní senzor jsou zapojeny do dveřních terminálů nebo Wiegand modulů. Jak již bylo zmíněno komunikace mezi čtečkami a Wiegand moduly je šifrována. Zámky jsou napěťové ovládány 12 V DC. Veškerá kabeláž je vždy vedena skrytě, popřípadě v zabezpečeném prostoru. Wiegand moduly jsou zapojeny v tzv. clusterech – hnízdech, kde jsou pomocí spojovacího konektoru zapojeny přímo do řídícího Cluster kontroleru. Do kontroleru může být zapojeno maximálně 8 Wiegand modulů a dalších 32 dveřních terminálů lze připojit přes sběrnici RS 485 nebo S-BUS. Komunikace přes RS 485 probíhá pomocí Impro Secure protokolu a S-BUS je opět zabezpečen pomocí 128-bitového AES

šifrování. Vzhledem k poměrně malým rozměrům celé budovy je možné provést instalaci veškeré technologie ve dvou místech. Pouze je nutné vhodně dimenzovat kabeláž.

Jeden Cluster kontroler je vybaven pamětí až pro 10 000 držitelů karet a 100 000 transakcí. Z pohledu řízení celého technologického celku je systém typu OFF-LINE, neb veškeré řízení systému obstarává Cluster kontroler. Pro aktuální přehled pohybu osob po budově je však nutné data okamžitě přenášet do serverové aplikace AP Pro, ke které jsou dále připojeni klienti přes WEB server.



Obr. 24. Obecné schéma struktury systému Access Portal Pro, zdroj: http://www.impro.net

5.3.4 Napájecí zdroje

Ačkoliv je návrh napájecích zdrojů často až sekundární záležitostí je funkčnost a spolehlivost systému ACS založena právě na vhodně dimenzovaných zálohovaných napájecích zdrojích. Při poruše napájecího zdroje dojde k vypnutí části, nebo celého systému. Z tohoto důvodu volíme ověřené profesionální zdroje, které jsou především dimenzované pro dlouhodobý spolehlivý provoz. Takový zdroj se vyznačuje dobře odvětrávaným prostorným krytem, nejlépe plechovým, který dobře předává vnitřní tepelnou energii vznikající ve zdroji svému okolí.

Při návrhu napájecích zdrojů je nutné spočítat celkový proudový odběr všech připojených komponent. Celkový odebíraný proud počítáme včetně všech možných aktivací zámků a akčních členů, neb v ovládacím rozhraní je možné v jeden moment spustit otevření všech dveřních vstupů. V našem případě, budou zámky EL566 nastaveny v reverzním režimu, aby došlo k naplnění smyslu normy ČSN 730804 Požární bezpečnost staveb – Výrobní objekty. Tzn., že musíme počítat s trvalým proudovým odběrem těchto zámků. Pokud požadujeme dlouhodobě spolehlivý provoz napájecích zdrojů je vhodné je předimenzovat, aby nebyly po celou dobu provozu na své maximální úrovni zátěže.

V systému ACS bude instalováno:

- 29 ks elektromechanických zámků EL 566 (maximální proudový odběr jednoho kusu zámku 550 mA/)
- 1 ks elektromagnetu M 62 (proudový odběr 250 mA)
- 38 ks čteček MDR (proudový odběr jedné čtečky 100 mA)
- 19 ks Wiegand modulů (proudový odběr jednoho modulu 97 mA)
- 2 ks Cluster kontroleru (maximální proudový odběr 640 mA)
- 3 ks terminálů O 16 (maximální proudový odběr 500 mA)

Veškeré hodnoty proudového odběru jsou platné za předpokladu napájení komponent 12 V DC (Direct Current – stejnosměrné napájení). Sečtením všech hodnot získáme hodnotu proudového odběru 25,3 A. Na základě výsledné hodnoty volíme 4 ks zálohovaného napájecího zdroje PZD13000 (výrobce Elso s.r.o., Česká Republika) s výstupními parametry 10 A / 12 V DC.

Profesionální napájecí zdroje jsou rovněž zálohovány pomocí gelových akumulátorů. Dobu zálohování volíme především s ohledem na zajištění bezpečného stavu objektu i při výpadku elektrické sítě. Vzhledem k faktu, že modelový objekt je datové centrum, je zajištěno celkové napájení kritických datových částí i po dobu výpadku napětí. Z tohoto pohledu můžeme hovořit o dvojitém zálohování a není tedy nutné dimenzovat celou dobu zálohování systému pouze ve zdrojích pro ACS. Zálohování napájení datového centra je zajištěno záložními zdroji, které slouží pouze po přechodovou dobu než dojde ke spuštění záložního motorového generátoru elektrického proudu, který zajistí bezpečné napájení i po

delší dobu výpadku v řádech hodin. Pokud dojde k dlouhodobému výpadku pak lze kritické systémy datového centra udržet v provozu i po dobu několika dní, avšak je otázkou jestli při tak dlouhém výpadku je předmětné udržení datové struktury v provozu.

5.3.5 Integrace s PZTS

Systém ACS lze integrovat s ostatními poplachovými i nepoplachovými aplikacemi. Pro účely zabezpečení prostor a detekce jejich narušení bude v objektu instalován systém PZTS s návazností ovládání z ACS. Jednotlivé prostory rozdělíme na tzv. bloky, jejichž aktivace bude závislá na stavu obsazení zón, které definujeme v ACS. Integrace musí být realizována dle podmínek stanovených normou ČSN CLC/TS 50398 Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky.

V případě vstupu do zóny ACS dojde k deaktivaci zabezpečení daného bloku a naopak. Tím je na maximální možnou úroveň zajištěna bezpečnost hlídaného prostoru. Operátoři systému tedy ostraha objektu má neustálý přehled na stavem zabezpečovaných zón, včetně konkrétních informací o vstupu osob do těchto prostor.

Objekt bude rozdělen do následujících přístupových zón (bloků PZTS):

- Únikové schodiště A
- Únikové schodiště B
- Kompletní 3.PP
- Datové centrum A
- Datové centrum B
- Garáže
- Administrativní část 1.1
- Administrativní část 1.2
- Administrativní část 2
- Klimatizační jednotka

- Technická místnost v 3.NP

Některé zóny budou ovládány manuálně prostřednictvím klávesnice systému PZTS, jiné budou ovládány automaticky dle stavu obsazení zón.

Pro automatické ovládání zabezpečení je nutné instalovat obousměrnou kontrolu vstupu. Tím je zaručena registrace příchozích a odchozích osob, na jejímž základě může být ovládán stav bloku PZTS. Automatické ovládání bude použito především v kritických místech s častým přístupem:

- Datové centrum A
- Datové centrum B
- Klimatizační jednotka
- Únikové schodiště A
- Únikové schodiště B
- Administrativní části

Propojení obou systémů může být realizováno například prostřednictvím sběrnice RS485, kde je nutné pro integraci vytvořit komunikační protokol mezi oběma systémy. Jednodušší variantou je propojení pomocí PGM (Programmable) výstupů ze systémů ACS a aktivačních vstupů systému PZTS. Takovýto přenos lze považovat za simplexní, neb přenesení informace je pouze jednosměrné. V případě vyhlášení poplachu systémem PZTS nedochází k žádné interakci s ACS, avšak dochází k naplnění režimových opatření, které jsou v objektu nastaveny pro fyzickou ostrahu.

5.3.6 Integrace s EPS

Po celém objektu bude instalován systém EPS (Elektrická požární signalizace) a SHZ (Stabilní hasicí zařízení). Přímo v místnosti datového centra pak bude systém SHZ s hašením požárů pomocí inertních plynů. V případě vyhlášení požárního poplachu v místnostech datového centra nebude umožněn vstup do těchto místností po dobu plnění prostoru plynem. Totožný systém SHZ bude instalován v 3.PP budovy v rozvodně elektrické energie a v místnosti se záložními zdroji.

ACS bude propojen s EPS za účelem ovládání konkrétních vstupů při vyhlášení požárního poplachu. Především se jedná o uvolnění požárních únikových cest tedy o kompletní vstupy v únikových schodištích A a B a o únikové východy z objektu.

5.3.7 Integrace s CCTV

Vnitřní prostory včetně přilehlého pozemku budou monitorovány kamerovým systémem. Integrace mezi ACS a CCTV (Closed Circuit Television – uzavřený televizní okruh) bude spočívat ve spojení zaznamenaných videosekvencí a jednotlivých transakcí. Pro potřeby dohledání historie průchodů pak bude jednoduše identifikovatelná osoba na základě vytvořené transakce RFID karty a kamerového záznamu. Vybrané prostory pak budou monitorovány nezávisle na přístupovém systému.

5.4 Fyzická ostraha

V objektu bude neustále přítomna fyzická ostraha. Recepce objektu bude zároveň sloužit jako bezpečnostní stanoviště, kde budou signalizovány důležité stavy poplachových systémů. Pro ovládání a monitorování systému ACS bude v recepci vyhrazen klientský počítač s permanentním připojením do WEB serveru systému.

Hlavní vstup do budovy bude realizován kolem recepce, kde zároveň bude docházet k další doplňkové autentizaci vstupujících osob. Doplňková autentizace zaměstnanců bude spočívat v porovnání obličeje procházející osoby s uloženou fotografií v databázi karet, která bude automaticky generována systémem na monitoru ostrahy.

V případě návštěvy bude ostraha vydávat návštěvnické karty, které budou mít minimální přístupové oprávnění pouze do prostor účelu návštěvy. Tyto karty budou pomocí sběrného boxu odebrány při průchodu vnitřními odchozími dveřmi. Úplný odchod z budovy bude umožňovat právě ostraha v recepci.

5.5 Cenový předpoklad

Cenový předpoklad je vytvořen v závislosti na výše popsaném návrhu a vychází z aktuálně platných ceníků dodavatelů pro Českou Republiku.

Tab. 2. Cenový předpoklad navrhovaného zabezpečené objektu systémem ACS, zdroj: vlastní archiv autora

AKCE : Zabezpečení datového centra
ČÁST : ACS

č.pol.	položka	m.j.	poč. m. j.	cena za m.j. materiál	cena za m.j. montáž	cena celkem materiál	cena celkem montáž
001	HCW910 - Cluster kontroler s 1 Wiegand modulem, S-BUS/RS485/LAN	ks	2	11 739 Kč	800 Kč	23 478 Kč	1 600 Kč
002	HMW900 - Wiegand modul pro 2 Wiegand čtečky, S-BUS, RS-485	ks	17	6 027 Kč	400 Kč	102 459 Kč	6 800 Kč
003	APP900 - licence pro provozování systému Access Portal Pro	ks	1	32 573 Kč	600 Kč	32 573 Kč	600 Kč
004	MDE900 - registrační USB čtečka s multi-disciplinární technologií	ks	1	9 471 Kč	400 Kč	9 471 Kč	400 Kč
005	MDR901 - elegantní čtečka MDR s multi-disciplinární technologií (125kHz a 13,56MHzú	ks	38	3 318 Kč	400 Kč	126 084 Kč	15 200 Kč
006	XRT920 - inteligentní dveřní terminál iTRT pro 2 Wiegand čtečky, RS-485, LAN	ks	1	9 261 Kč	800 Kč	9 261 Kč	800 Kč
007	XDBv902 - sběrný box na karty, v nerezovém stojanu, se čtečkou MDR	ks	1	71 925 Kč	1 500 Kč	71 925 Kč	1 500 Kč
008	XOT900 - terminál O16 s 16 ti výstupní relé	ks	3	16 233 Kč	1 500 Kč	48 699 Kč	4 500 Kč
009	TMD400 - bezkontaktní RFID karta s technologií MiFare DESFire EV 1, 13,56MHz	ks	100	118 Kč	10 Kč	11 800 Kč	1 000 Kč
010	KKSZ100 - plechový uzamykatelný kryt	ks	4	879 Kč	300 Kč	3 516 Kč	1 200 Kč
011	KDT-P - plastový kryt pro dveřní terminál	ks	1	386 Kč	300 Kč	386 Kč	300 Kč
012	PZD13000 - profesionální zálohovaný napájecí zdroj 10A/12 V DC	ks	4	5 890 Kč	800 Kč	23 560 Kč	3 200 Kč
013	AKU26 - záložní akumulátor 26Ah/12 V DC	ks	4	2 140 Kč	- Kč	8 560 Kč	- Kč
014	NIT910 - biometrická čtečka otisku prstu Fingkey Access	ks	4	14 827 Kč	600 Kč	59 308 Kč	2 400 Kč
015	EL566 - elektromechnický vícebodový zámek Abloy	ks	29	20 000 Kč	600 Kč	580 000 Kč	17 400 Kč
016	EA218 - kabel s konektore pro zámky Abloy	ks	29	770 Kč	200 Kč	22 330 Kč	5 800 Kč
017	EA324 - Protiplech univerzální	ks	29	430 Kč	200 Kč	12 470 Kč	5 800 Kč
018	EA281 - kabelová průchodka zadlabací	ks	29	950 Kč	- Kč	27 550 Kč	- Kč
019	SX03 - bezpečnostní kování Ikon, klika-klika	ks	29	4 670 Kč	200 Kč	135 430 Kč	5 800 Kč
020	M62 - elektromagnet Securitron s přídržnou silou 545 kg	ks	1	8 500 Kč	1 500 Kč	8 500 Kč	1 500 Kč
021	ZA-62 - nastavitelná Z-konzole	ks	1	3 400 Kč	1 500 Kč	3 400 Kč	1 500 Kč
022	Kabeláž (FTP 5E LSOH, ohebná chránička)	kpl	1	27 000 Kč	45 000 Kč	27 000 Kč	45 000 Kč
023	Zapojení, oživení a naprogramování systému	kpl	1		10 000 Kč	- Kč	10 000 Kč
024	Revize připojení do elektrické sítě	kpl	1		6 000 Kč	- Kč	6 000 Kč
025	Výkresová dokumentace skutečného provedené	kpl	1		12 000 Kč	- Kč	12 000 Kč
026	Drobný instalační materiál	kpl	1	5 000 Kč		5 000 Kč	- Kč
027	Doprava	kpl	1		5 000 Kč	- Kč	5 000 Kč
	Celkem bez DPH (Materiál - Práce)					**1 352 760,00 Kč**	**155 300,00 Kč**
	Celkem bez DPH - součet						**1 508 060,00 Kč**
	DPH	**21**	**%**				**316 692,60 Kč**
	Konečná cena s DPH						**1 824 753,00 Kč**

ZÁVĚR

Využití identifikačních systémů a technologií bude stále více záležitostí běžného života. Již v současnosti jsme obklopeni spoustou personálních identifikátorů ať už se jedná o občanský průkaz, zaměstnanecký RFID tag, nebo bezkontaktní platební kartu. Technologie RFID je celosvětově využívána pro jakékoliv aplikace. Současně bezpečné RFID technologie MiFare DESFire EV1 a SmartMX2 nemusí být však bezpečné navždy. Je jen otázkou času, kdy dojde k objevení metody překonání pokročilých metod šifrování. Ale je také nutné připomenout, že s vývojem bezpečnostních aplikací samozřejmě budou přicházet nové bezpečnostní mechanismy, které mohou zaručit dočasnou, či snad trvalou bezpečnost identifikační technologie.

Vzhledem k modernímu trendu maximálního zjednodušení lidského života, je možné, že budeme v budoucnu nositeli RFID čipu pevně umístěného v lidském těle. Ovšem je důležité se především zamyslet, zdali je vážně potřebné a žádoucí nechat se takto permanentně označit. Ačkoliv tato eventualita zní jako sci-fi myšlenka, realita není vůbec vzdálená a již dnes je určitě technologicky možné nechat si implementovat RFID tzv. pod kůži.

Dle mého názoru velice kvalitním identifikátorem je samotné lidské tělo. Samozřejmě principy biometrického čtení musí být nejprve opřeny o výzkum v oblasti unikátních znaků jedince, avšak již samotný francouzský kriminalista Alphonse Bertillon koncem 19. století položil základy biometrického čtení svou metodou antropometrického měření. Důležitým aspektem biometrické identifikace je přesnost a spolehlivost biometrických čteček a pokud má být takovýto identifikační systém masově využíván, je potřeba brát i ohled na ekonomické náklady. Avšak po nalezení takovéto vhodné technologie možná již nebudeme muset používat různé karty, čipy, ale bude stačit pouze naskenovat část lidského těla.

ZÁVĚR V ANGLIČTINĚ

Using identification systems and technologies will increasingly be a matter of everyday life. Already now we are surrounded by lots of personal identifiers whether a national identity card, employment RFID tag or a contactless payment card. RFID technology is used globally for any application. At the same time secured RFID technology MIFARE DESFire EV1 and SmartMX2 but may not be safe forever. It is only a matter of time before the discovery of methods for overcoming the advanced encryption methods. But it must also be noted that with the development of security applications, of course, will come new security mechanisms that can guarantee a temporary or perhaps permanent security identification technology.

Due to the modern trend of maximum simplification of human life, it is possible that in the future we will carry RFID chip firmly placed in the human body. However, it is important to consider in particular whether it is really necessary or desirable to let the thus permanently mark. Although this possibility sounds like sci-fi idea, the reality is not far, and already is certainly technologically possible to have implemented RFID under the skin.

In my opinion very quality identifier is the human body itself. Of course, reading biometric principles must first be laid at the research on the unique character of the individual, but already French criminologist Bertillon in the late 19th century laid the foundation for biometric reading his method of anthropometric measurements. An important aspect of biometric identification is the accuracy and reliability of biometric readers and if such an identification system to be used en masse, it is also necessary to take into account the economic costs. However, after such a finding suitable technology may no longer have to use different cards, chips, but will only need to scan a human body part.

SEZNAM POUŽITÉ LITERATURY

[1] 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.

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

[3] PARET, Dominique. *RFID at ultra and super high frequencies: theory and application*. Chichester: John Wiley, 2009, xx, 527 s. ISBN 978-0-470-03414-9.

[4] SHEPARD, Steven. *RFID: radio frequency identification*. New York: McGraw-Hill, 2005, xvi, 256 p. ISBN 00-714-4299-5.

[5] RANKL, Wolfgang. *Smart card applications: design models for using and programming smart cards*. Chichester: John Wiley, 2007, xviii, 217 s. ISBN 978-0-470-05882-4.

[6] BIENERT, Gerhard H. Schalk; Renke. *RFID: MIFARE and contactless smartcards in application*. Susteren: Elektor International Media BV, 2013. ISBN 978-190-7920-141.

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

[8] *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

[9] *Pij bezpečně: Na co si dát pozor při nákupu lahví alkoholu* [online]. [cit. 2015-05-23]. Dostupné z: http://www.pijbezpecne.cz/na-co-si-dat-pozor/

[10] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Všeobecné oprávnění č. VO - R/10/05.2014 - 3 k využívání rádiových kmitočtů a k provoz ování zařízení krátkého dosahu*. Dostupné také z: https://www.ctu.cz/cs/download/oop/rok_2014/vo-r_10-05_2014-03.pdf

[11] Sbírka zákonů: Zákon o ochraně osobních údajů a ozměně některých zákonů. *101/2000*. Tiskárna Ministerstva vnitra, p.o, 2000. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/

[12] JAŠEK, Ph.D., doc. Mgr. Roman a Ing. David MALANÍK Ph.D. *Bezpečnost informačních systémů*. Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.

[13] GARCIA, F. D., ROSSUM, P., VERDULT, R., SCHREUR, R. *Wirelessly pickpocketing a MIFARE Classic card* [online]. 2009 [cit. 2015-05-03]. Dostupný z http://blog.mmn-o.se/wp-content/uploads/2011/01/Pickpocketing.Mifare.pdf

[14] EM MICROELECTRONIC - MARIN SA. *EM4200: 128 bit Read Only Low Frequency Contactless Identification Device*. Version 3.2. Dostupné také z: http://www.emmicroelectronic.com

[15] NXP SEMICONDUCTORS. *HT2x: HITAG 2 transponder IC*. 2014. Rev.3.1. Dostupné také z: www.nxp.com

[16] NXP SEMICONDUCTORS. *MF1S70yyX/V1: Mifare Classic EV1 4K - Mainstream contactless smart card IC for fast and easy solution development*. Rev.3.1, 279331. Dostupné také z: http:// www.nxp.com

[17] NXP SEMICONDUCTORS. *MF3ICDx21_41_81: Mifare DESFire EV1 contactless multi-application IC*. Rev.3.1, 145631. Dostupné také z: http://www.nxp.com

[18] NXP SEMICONDUCTORS. *Frequently Asked Questions: On the security of Mifare DESFire MF3ICD40*. Dostupné také z: http://www.nxp.com

[19] NXP SEMICONDUCTORS. *SmartMX2 family: P60D080 and P60D144 - Secure high-performance dual interface smart card controller*. Rev.1., 197210. Dostupné také z: http://www.nxp.com

[20] COURTOIS, N. T. *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime* [online]. 17. 4. 2015 Dostupný z http://eprint.iacr.org/2009/137

[21] GARCIA, F. D., ROSSUM, P., VERDULT, R., SCHREUR, R. *Wirelessly pickpocketing a MIFARE Classic card* [online]. 2009 [cit. 2015-05-12]. Dostupný z http://blog.mmn-o.se/wp-content/uploads/2011/01/Pickpocketing.Mifare.pdf>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RFID	Radio Frequency Identification
ACS	Access Control System
IFF	Identification Friend or Foe
RADAR	Radio Detection And Ranging
EPC	Electronic Product Code
QR	Quick Response
ASK	Amplitude Shift Keying
PLL	Phase Locked Loop
EMC	Electromagnetic Compatibility
UHF	Ultra High Frequency
ČTÚ	Český telekomunikační úřad
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ICC	Integrated Circuit Card
UV	Ultra Violet
SIM	Subscriber Identity Module
ID	Identification
PCD	Proximity Card Reader
PICC	Proximity Integrated Circuit Card
ČSN	Česká státní norma
ETSI	European Telecommunications Standard Institute
EN	Evropská norma
SRD	Short Range Device

ROM	Read Only Memory
EEPROM	Electrically Erasable Programmable Read Only Memory
DES	Data Encryption Standard
AES	Advanced Encryption Standard
NIST	National Institute of Standards and Technology
PKE	Public Key Encryption
RSA	Rivest, Shamir, Adleman
ECC	Elliptic Curve Cryptography
CMOS	Complementary Metal Oxide Semiconductor
UID	Unique Identification
PZTS	Poplachový zabezpečovací a tísňový systém
OOK	On-Off Keying
NUID	Non-Unique Identification
CRC	Cyclic Redundancy Check
EAL	Evaluation Assurance Level
CC	Common Criteria
CPU	Central Processing Unit
UART	Universal Asynchronous Receiver/Transmitter
CIU	Contactless Interface Unit
MZS	Mechanické zábranné systémy
PIN	Personal Identification Number
DT	Domácí telefon
UPS	Uninterruptible Power Supply
PP	Podzemní podlaží
NP	Nadzemní podlaží

IT	Information Technology
TCP/IP	Transmission Control Protocol/Internet Protocol
SQL	Structured Query Language
HTML	HyperText Markup Language
ABS	Akrylonitril Butadien Styren
PGM	Programmable
EPS	Elektrická požární signalizace
SHZ	Stabilní hasicí zařízení
CCTV	Closed Circuit Television

SEZNAM OBRÁZKŮ

SEZNAM TABULEK