Acta Informatica Pragensia, 2019, 8(1), 4–17
DOI: 10.18267/j.aip.122
Original Article

Případová studie využití technologie RFID pro zabezpečení výpočetní techniky proti odcizení a tendence uživatelů obcházet zabezpečení

A Case Study of RFID Technology Application for Protection of Computing Technology Against Theft and Users' Tendency to Bypass the Protection

Dušan Brodani [1]

Abstrakt

Studie se zabývá testováním zabezpečení výpočetní techniky a příslušných periférií v korporátní organizaci na bázi technologie identifikace na rádiové frekvenci (RFID). Potenciál RFID technologie je dále využit i k získání statistických dat z provozu v reálném čase. Na základě porovnání RFID technologie postavené na krátkých a ultra krátkých vlnách (vysoké a velmi vysoké frekvenční pásmo) byla vybrána vhodná varianta pro provoz, vybraná zařízení byla označena RFID tagy a v testovacím i ostrém provozu byla monitorována úspěšnost jejich detekce. Po třech měsících provozu proběhlo vyhodnocení nákladů na zavedení zabezpečení a přínosů v podobě snížení počtu pokusů o odcizení zabezpečených zařízení. Dalším výstupem je stanovení hranice celkové hodnoty zabezpečené výpočetní techniky oproti ztrátám způsobeným odcizením, aby se společnosti vyplatilo investovat do zabezpečení pomocí RFID. Potvrdilo se, že nasazení tohoto typu zabezpečení se organizaci jen na zamezení přímých ztrát vrátí za čtyři roky. Tendence uživatelů obcházet zabezpečení byly minimální. Na vyhodnocení výsledků pak navazuje další možné využití potenciálu RFID do budoucna i nad rámec samotného zabezpečení, například pro optimalizaci skladových zásob a sledování pohybu jednotlivých položek mezi uživateli. Jedná se zejména o zefektivnění využití pracovního času u pracovníků IT oddělení, zamezení nedostupnosti položek výpočetní techniky a zvýšení úrovně IT služeb poskytovaných uživatelům.

Klíčová slova: RFID, zabezpečení, výpočetní technika, krátké vlny, ultra krátké vlny.

Abstract

The study focuses on testing the protection of computing technology and peripheral devices based on radio-frequency identification (RFID) technology in a selected corporate organization. The potential of RFID technology is also employed to obtain statistical data about real-time use of the devices. Based on the comparison of high and ultra-high frequency of RFID technology, the appropriate variant was selected for operation, selected devices were tagged with RFID tags, and the success of their detection was monitored both in the test period and in real operation. After three months' operation, the cost connected with protection implementation and its benefits was assessed. The main benefit is reducing the number of stolen devices. Users' tendency to bypass the protection was minimal. A further result of this study is determining the overall value of computing technology and peripheral devices to be

[1] Department of Information and Knowledge Engineering, Faculty of Informatics and Statistics, University of Economics, Prague, W. Churchill Sq. 4, 130 67 Prague 3, Czech Republic
✉ dusan.brodani@vse.cz

protected against loss caused by theft that would make the investment in RFID technology pay off for the corporation. It was confirmed that deploying this type of protection pays off for the organization in four years thanks to the prevention of direct losses. After the assessment of the results, a possible future use of RFID potential beyond the protection itself is considered, that would optimize a corporation's inventory and track the movement of individual devices among users. These considerations include, in particular, the efficiency of use of IT staff working time, the prevention of unavailability of devices and the increase of the level of IT service provided to users.

Keywords: RFID, Protection, Computing technology, High frequency, Ultra high frequency.

1 Úvod

Technologie RFID (Radio-Frequency IDentification) se pro účely zabezpečení používá zejména v oblasti obchodu a skladové logistiky. Oproti jiným zabezpečovacím technologiím nabízí RFID mnohem větší potenciál než jen pro účel samotného zabezpečení a tato technologie, bývá nasazena i tam, kde je potřeba monitorovat označené položky v logistickém řetězci, automatizovat evidenci nebo umožnit uživatelům samoobslužnou manipulaci. To přináší řadu dalších možností, pokud by se v budoucnu uvažovalo rozšířit zabezpečení i o další funkcionality, které můžou být jen nástavbou na již zavedený základní systém.

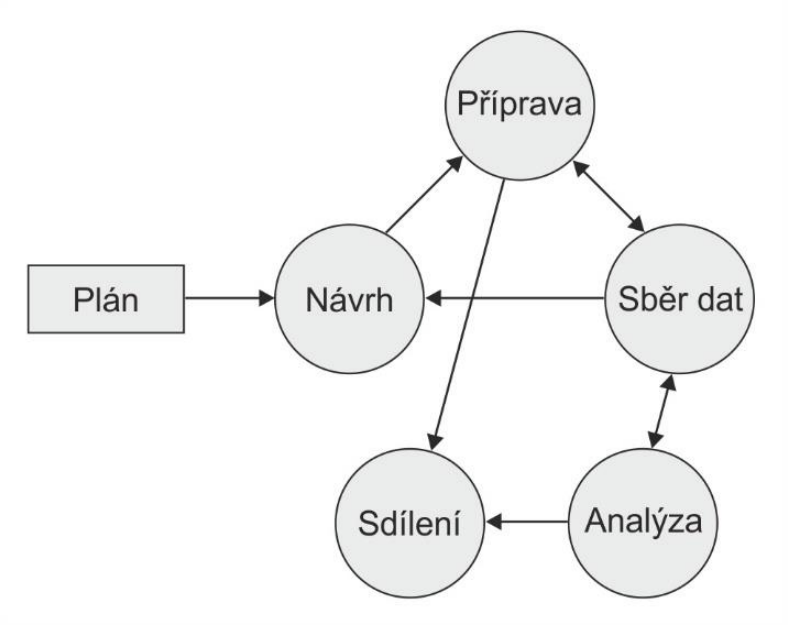
Mnoho řešení ve světě využívá obecně dostupné komponenty RFID technologie pro vytvoření proprietárních jedno nebo víceúčelových systémů, k dispozici jsou ale i modulární systémy, které respektují standardy a lze tak kombinovat nebo v budoucnu rozšiřovat systém s použitím komponentů od různých výrobců. Stejně tak je možné za dodržení standardů vyvíjet a sestavit vlastní řešení pro některou součást v systému, co může přinést úsporu nákladů, pokud jsou požadovány jen specifické funkce komponent nebo optimalizace jejich vlastností (Bunker & Elsherbeni, 2017). Zabezpečení skladových položek na bázi RFID přináší zejména otázky, které se týkají míry úspěšnosti detekce a tím pádem i spolehlivosti celého systému. I když v rámci testování jsme výraznější problém nezaznamenali, snažili jsme se dodržet doporučené postupy pro zařízení místnosti a eliminovat potenciální zdroje rušení. Pro optimalizaci detekce v interiéru se vyvíjí i vylepšení lokalizačního algoritmu (Yong et al., 2018), faktem ale je, že v případě nálezu významného zdroje rušení, jako je například vedení napěťových kabelů pod podlahou v paralelním směru se snímači, je nutné plánované umístění snímačů přehodnotit nebo i zvážit, zda vůbec v problematické části interiéru zařízení instalovat (Zhang et al., 2017a). Protože používání označení RFID etiket je poměrně rozšířeno pro různé oblasti, je velice pravděpodobné, že systém může zaznamenávat a vyhodnocovat i neznáme etikety, které vyvolají falešné poplachy. V praxi se používá filtrování, které má za úkol detekovat etikety nesplňující příslušnost k systému a vyřadit je tak z načítání (Zhang et al., 2018). Detekce neznámých etiket sice není stoprocentní, často se stává, že některé pole v etiketě nese relevantní informaci i pro jiné systémy, ale v případě vysokého počtu neznámých etiket ovlivňujících systém by stálo za úvahu toto filtrování implementovat.

Cílem případové studie zavedení RFID zabezpečení bylo snížení počtu odcizených položek a vyhodnotit, od jaké hodnoty zabezpečených položek bude nasazení zabezpečení pro společnost rentabilní. Vedení společnosti pozitivně vnímá zvyšování úrovně bezpečnosti a rozpočet počítá s náklady na projekty v této oblasti. Otázkou bylo, zda přinesou vynaložené náklady na zabezpečení skutečně radikální pokles přímých i nepřímých ztrát a umožní efektivnější sledování využití majetku, jeho evidenci a optimalizaci plánování skladových zásob. Popřípadě

zda budou mít uživatelé tendenci zabezpečení obcházet, nebo je úplně odradí od pokusů některé z položek odcizit.

2 Metodika provedení případové studie

Studie byla provedena podle doporučené metodiky pro přímé pozorování situace a shromáždění dostatečného množství kvantitativních i kvalitativních dat pro analýzu (Yin, 2014). Případovou studii je možné zařadit mezi testovací případové studie, kde byl ověřován předpoklad, že zvýšené náklady na zabezpečení budou mít synergický efekt pro ochranu majetku, optimalizaci jeho využití v provozu i zefektivnění využití pracovního času. Hlavní otázkou, na kterou měla tato případová studie přinést odpověď je, zda náklady vynaložené na zabezpečení skutečně přinesou radikální pokles přímých i nepřímých ztrát, a navíc umožní efektivnější sledování využití majetku, jeho evidenci a optimalizaci plánování skladových zásob. Zdrojem dat bylo testování limitů detekce u vybrané technologie, komparace případů odcizení před a po nasazení zabezpečení a statistika vypůjčení jednotlivých položek v průběhu dne. Sběr dat v ostrém provozu probíhal po dobu 3 měsíců a v této době nebylo do sledování zasahováno, ani se neprováděli změny technologického nebo jiného charakteru.



Obr. 1. *Postup provedení případové studie. Zdroj: (Yin, 2014).*

Plán na zavedení zabezpečení pomocí technologie RFID vznikl na základě vyhodnocení ztrát (kapitola 3.1). Na začátku byl autorem představen postup, který do budoucna umožňoval postupné rozšíření zabezpečení o další lokality v budově i zapojení dalších funkcí pro optimalizaci skladových zásob. Tento postup počítal s testovací fází, která má při minimálních nákladech prověřit funkčnost technologie a demonstrovat její rentabilitu (Obr. 1). Ve fázi návrhu proběhlo porovnání dostupných technologií a výběr nejvhodnější varianty s ohledem na možné rozšíření v budoucnu (kapitola 4.1). Příprava implementace se zaměřila na konkrétní modelovou místnost, v které bylo možné provést studii při minimálních nákladech na dodatečné úpravy (kapitola 4.6). Sběr dat pak probíhal v rámci testování i ostrého provozu, kdy byl do případové studie zapojen zaškolený obslužný personál a zatím chybějící automatizace sběru některých informací pro statistické účely byla prováděna ručně (kapitola 5). Po 3 měsíčním sběru dat z ostrého provozu byla provedena jejich analýza, vyhodnocení úspěšnosti nasazení zabezpečení a celkové porovnání návratnosti investice (kapitola 6). Výsledkem je stanovení

hranice, jakou hodnotu by měl mít majetek, který má být zabezpečen proti odcizení, aby vůbec mělo smysl uvažovat o nasazení RFID technologie. Po zavedení zabezpečení a prozkoumání pokusů o odcizení některých položek bylo diskutováno, zda by stejného efektu nebylo možné dosáhnout při menší investici (kapitola 7).

3 Představení organizace a implementačního kontextu

Společnost, ve které proběhla studie, patří mezi korporace a v mateřské společnosti pracuje více než 150 zaměstnanců, pro které IT oddělení spravuje počítačovou síť a různou výpočetní techniku od sestav počítačů, přes telefony až po audio-video vybavení. Zatímco v evidenci majetku jsou některé položky, jako je počítač nebo telefon, evidovány přímo na jednotlivé uživatele, kteří jsou za ně odpovědni, jiné jsou uživatelům k dispozici ve sdíleném režimu. Toto sdílené vybavení mají možnost využívat i externí osoby, které nejsou zaměstnanci, ale účastní se meetingů nebo školení v prostorách společnosti. Často se na vyžádání zapůjčují různé napájecí adaptéry, video redukce pro promítání z jejich počítačů nebo i celé počítačové sestavy. Většina položek je však volně k zapůjčení v rámci vybavení zasedacích místností, aby byly v případě potřeby ihned k dispozici. Zejména u menších komponentů často dochází k jejich odnášení z prostor společnosti a jen výjimečně se tyto položky povede vrátit zpátky. Ne vždy jde o vědomé odcizení, zejména když se jedná např. o malý vysílač v USB portu pro bezdrátovou myš a klávesnici, ale bezdrátový komponent je bez konkrétního spárovaného vysílače nepoužitelný. U nevrácených napájecích adaptérů nebo speciálních video redukcí pro konkrétní typ počítače pak nastává i problém s nutností zakoupit nové položky na sklad, ale po dobu, než je objednávka vyřízená a doručena je snížena úroveň poskytovaných IT služeb.

3.1 Ztráty společnosti a potřeba zvýšení zabezpečení výpočetní techniky

Protože jednotlivé případy nevrácení zapůjčeného vybavení představují často ztrátu od několika stokorun až po tisíce korun, byla zpracována statistika všech evidovaných případů za poslední dva roky. Celková ztráta pro společnost představovala 45220 Kč jen na pořizovací hodnotě 67 položek bez započítání času pracovníků IT, kteří museli každý případ vyhodnotit a zpracovat (Tab. 1).

Tab. 1. *Seznam odcizených položek a jejich hodnota. Zdroj: (Autor).*

Popis	Počet	Cena	Celková cena
Dálkové ovládače pro prezentace nebo jejich USB vysílače	13 ks	550 Kč/ks	7150 Kč
Bezdrátové myši a klávesnice nebo jejich USB vysílače	16 ks	420 Kč/ks	6270 Kč
Video redukce Apple	9 ks	820 Kč/ks	7380 Kč
Video redukce digitální (HDMI, DP)	5 ks	310 Kč/ks	1550 Kč
Video konvertory analog-digital (VGA-HDMI)	4 ks	785 Kč/ks	3140 Kč
Napájecí adaptéry Apple	6 ks	1900 Kč/ks	11400 Kč
Napájecí adaptéry (HP, Lenovo, Dell, Asus)	7 ks	680 Kč/ks	4760 Kč
USB kabel Apple Lightning	7 ks	510 Kč/ks	3570 Kč

Po vyhodnocení celkových ztrát bylo doporučeno zavést větší stupeň ochrany pro zapůjčené položky a hledal se způsob, který nebude vnímán příliš negativně zejména častými externími návštěvníky z vysokého managementu. Pokud není vyžádána podpora meetingu ze strany IT oddělení, probíhá vypůjčení a zapojení doplňkového vybavení zasedacích místností samoobslužně, na tuto možnost jsou externí uživatelé upozorněni asistentkami před zahájením meetingu nebo školení. Bylo potřebné najít řešení, kdy bude možné označit položky různých rozměrů a tvarů, a které umožní jejich detekci při průchodu kontrolním místem.

3.2 Náklady na zvýšení zabezpečení majetku pomocí technologie RFID

Pro technologii RFID bylo rozhodnuto z důvodu, že někteří zaměstnanci IT oddělení měli zkušenosti s jejím nasazením v jiných provozech a usnadnili tak její implementaci. Protože RFID poskytuje mnohem širší využití, než je jen funkce pro zabezpečení, již od začátku bylo plánováno využít tento potenciál i pro evidenci dalších položek IT majetku, zejména pro optimalizaci inventarizací a sledování stavu a pohybu skladových položek. Dlouhodobě je požadován výrazně přesnější přehled o aktuálním stavu IT vybavení, které je ve společnosti k dispozici, zejména z důvodu častých zápůjček náhradního vybavení pro zaměstnance a naplnění potřeby nárazově zabezpečovat IT vybavením různé interní i externí akce společnosti.

Důležitým faktorem pro rozhodování je cena. Již použitá RFID průchodová brána byla pořízena za 50000 Kč bez DPH. Cena nové průchodové brány je kolem 130000 Kč bez DPH a vyplatí se proto až při vysoké frekvenci výpůjček. Cena jedné etikety se pohybuje kolem 5,5 Kč bez DPH při zakoupení balení 1000 etiket. Stolní snímač pro načtení a označení jednotlivých položek stojí 24500 Kč bez DPH. Celá investice do hardware pro zabezpečení pomocí RFID tak vychází při zakoupení použité brány na 80000 Kč bez DPH, co při úspěšném zamezení ztrát představuje v modelovém případě návratnost za cca 4 roky.

Celková hodnota chráněných položek v testovacím provozu je přibližně 200000 Kč bez započítání hodnoty velkých zařízení, jako jsou notebooky nebo projektory. Pro další rozšíření systému na další místnosti by se vzhledem k prostorovému uspořádání v budově muselo počítat s další průchodovou bránou.

Při uvažování nad zabezpečením je tedy potřebné vyhodnotit, jakou hodnotu mají zabezpečené položky, jaká je frekvence jejich pohybu a zda se uvažuje i nad využitím dalších funkcí, které RFID umožňuje. Do systému lze zapojit další komponenty, jako jsou ruční snímače pro inventarizace, chytré regály ve skladech, bezobslužní vracení položek z výpůjčky nebo sledování pohybu položek v reálném čase (Pane et al., 2018). Po vyhodnocení pak lze stanovit hranici, při které by bylo nasazení RFID rentabilní z hlediska chráněných hodnot nebo optimalizace pracovních procesů.

4 Návrh pro instalaci zabezpečovacích prvků

4.1 Výběr technologie zabezpečení: analýza a komparace dostupných systémů

Pro účel zabezpečení majetku a detekci položek při průchodu určeným místem se v praxi používají EM (elektromagnetické systémy) nebo RFID. Zabezpečení výpočetní techniky sebou nese i specifikum v elektromagnetickém vyzařování u elektricky aktivních položek, od kterého je potřeba zabezpečovací prvek odstínit, co je u EM pásků více problematické. RFID technologie byla prakticky od začátku upřednostněna z důvodu jejího využití i pro účely evidence a inventarizace majetku. Další výhodou byla možnost označit položky RFID etiketami s logem společnosti, čím se odlišily od bezejmenného příslušenství ve vlastnictví uživatelů.

Protože se zvažovalo rozšíření RFID technologie i pro evidenci jiných položek výpočetní techniky, staly se výpůjčky HW v zasedacích místnostech testovacím provozem, u kterého se simulovaly i další možnosti technologie než jen funkce zabezpečení. Pro nasazení tak byl porovnáván hlavně dosah při čtení etiket v detekčních bránách a při načtení položek ručním snímačem, který se používá pro inventarizaci majetku. Předmětem komparace RFID systémů se tak stala HF (high frequency) a UHF (ultra high frequency) technologie a standardy, které umožní kompatibilitu a rozvoj systému do budoucna.

4.2 Princip a fungování RFID technologie

Technologie RFID se skládá ze dvou základních prvků: čtecí zařízení, paměťové médium, které komunikuje se čtecím zařízením. Čtecí zařízení je zabudováno v pracovních stanicích, bezpečnostních branách, zařízeních pro samoobslužní výpůjčky nebo v ručním snímači pro inventarizaci položek.

Paměťové médium je malý čip s pamětí a anténou, zpravidla umístěn na papírové etiketě. Etiketa nemá zapotřebí žádný zdroj napájení, protože elektromagnetické pole generuje anténa připojena k RFID snímači. Když se v tomto poli ocitne RFID etiketa s transpondérem, v její anténě se generuje proud, který nabije kondenzátor a ten pak aktivuje čip. Důležité je, že etiketa samotná nevytváří vlastní elektromagnetické pole, ale jen mění pole vyvolané čtecím zařízením. To ve svém poli detekuje změny a převádí je na digitální data. Na to, aby bylo možné využít všechny možnosti RFID technologie, je potřebné k uvedeným dvěma prvkům přidat také komunikaci RFID s evidenčním systémem.

RFID etiketa spojuje identifikační i bezpečnostní funkci. Na čipu je uložen jednoznačný identifikátor položky a další údaje, jako např. označení společnosti a země. Zaznamenává se zde informace, zda je položka vypůjčena nebo zastřežena. Tento údaj je uložen v tzv. AFI byte a poskytuje více informací než jen dva základní stavy. Je v něm uložena i informace o odvětví, ze kterého konkrétní etiketa pochází. Na základě toho konkrétní bezpečnostní brána reaguje jen na relevantní etikety, ale k jinému zboží, které je zabezpečeno kompatibilním systémem RFID a prochází bránou, bude netečná.

Systémy na bázi RFID se skládají z 3 základních součástí: nosiče informací, antény a ovladače. Jednotlivé součásti tohoto systému mají různou podobu, výkon i velikost. V praxi se používá velké množství velikostí a podob RFID čipů, od miniaturních o rozměrech 0,4 x 0,4 mm až po čipy určené k průmyslovému využití s velikostí 100 x 100 mm. Pro čtení a zápis dat slouží také různé typy antén a ovladačů. Některé systémy využívají oddělené antény a ovladače, u jiných jsou antény a ovladače integrované do jednoho zařízení. Antény mají různé tvary a velikost, ovladače potom zajišťují komunikaci mezi anténou a řídícím počítačem. Nosič informací, který se označuje také jako „tag“ (tag – štítek), obsahuje cívku, paměťový polovodičový čip a u aktivních systémů i baterii. Pasivní nosiče informací čerpají energii prostřednictvím antény a vzhledem ke svým zanedbatelným požadavkům na údržbu mají téměř neomezenou životnost. Nosiče informací jsou vyráběny v mnoha velikostech, s různými kapacitami, s různým dosahem a také v provedeních pro různé rozsahy provozních teplot. Většina těchto nosičů je odolná proti fyzickému poškození, vlhkosti, chemikáliím a povětrnostním vlivům. Smart tags neboli chytré štítky jsou velice tenké RFID čipy, které vysílají informace o produktu, na němž jsou umístěny. V každé etiketě tedy může být zapsána informace o vlastnostech dané položky a identifikační kód. RFID etikety je možné kromě zakoupení u dodavatele i vyrábět na míru ve vlastní režii, kdy se používá tisk etiket na inkoustové tiskárně, která umožňuje tisk vodivým stříbrným inkoustem. Jedná se ale o řešení speciálních potřeb, které je v současnosti nákladnější než nákup standardních etiket pro běžné účely, které jsou běžně k dispozici na trhu (Koski et al., 2012).

Ve své nejjednodušší podobě je čtecí zařízení pouze širokým vchodem – portálem, který má po obvodu umístěn jeden nebo více RFID snímačů. Jsou určeny především pro čtení pasivních etiket, které dostávají napájení od snímače. Komplikujícím faktorem je to, že v automatizovaném procesu snímání etiket není pevně stanoveno, protože položky mají různé rozměry a etikety na nich různé umístění a orientace každé z nich se liší. Hlavním určujícím faktorem přesnosti je proto umístění antén – snímačů na portálu tak, aby se maximalizovala pravděpodobnost načtení etikety. Čitelnost pasivní značky je přímo závislá na množství energie, kterou přijímá, co v praxi znamená konkrétní vzdálenost mezi etiketou a snímačem a jejich orientacemi vůči sobě navzájem. Cílem optimálního umístění antény snímače je tedy maximalizovat oblast v rámci portálu, kde etikety získají alespoň minimální výkon potřebný pro jejich čtení v jejich všech možných orientacích (Wang et al., 2017).

4.3 Standardy a pravidla pro RFID

RFID systémy vyrábí mnoho různých firem po celém světě a ve světě jsou proto nasazované různé systémy. Od počátku se proto jevilo jako klíčové, aby výrobky různých firem byly navzájem kompatibilní a dokázali spolu komunikovat. Výrobci proto dodržují standardy ve formě norem. Pro koncového zákazníka to má výhodu v tom, že může kombinovat zařízení od více výrobců, které splňují danou normu. Standardy a pravidla určují:

- **technické parametry RFID řešení** – jako je vymezení frekvence bezdrátového přenosu, fyzikální vlastnosti etiket, přenos signálu, přenosový protokol – jsou důležité právě proto, aby zařízení od dvou různých výrobců byla navzájem kompatibilní,
- **rozsah a způsob uložení informací na paměťovém médiu** – toto je důležité, aby jakýkoliv systém uloženým datům „rozuměl“ a věděl, kde najít potřebný údaj,
- **komunikaci s evidenčním systémem** – tj. způsob, jakým bude systém získávat informace uložené v paměťovém médiu, a jak bude informace poskytovat nějakému zařízení RFID.

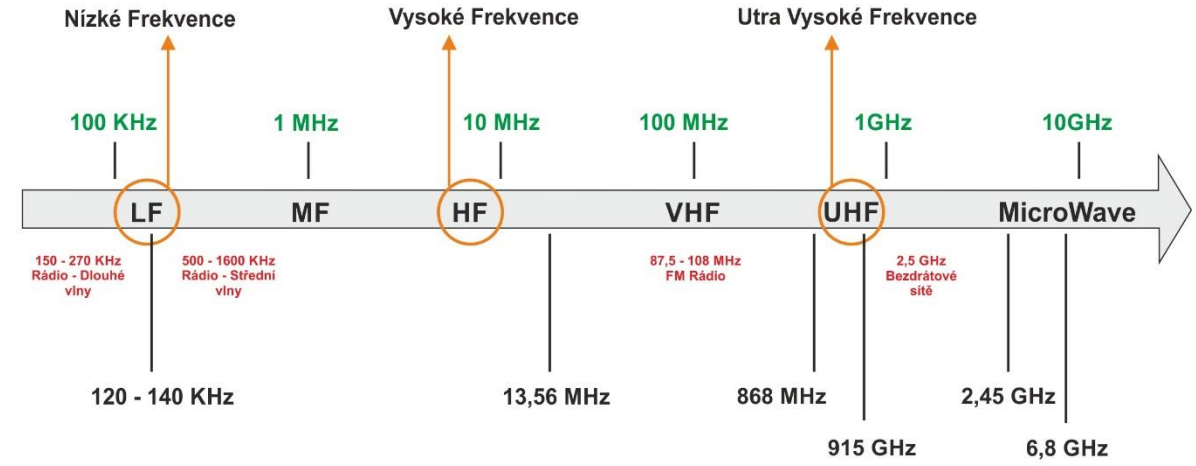
4.4 Komunikace RFID – SIP2

Původně proprietární přenosový protokol SIP (Standard Interchange Protocol) společnosti 3M doznal značného rozšíření, a především jeho druhá aktualizovaná verze (SIP2) se stala standardem u většiny zařízení RFID, která komunikují s informačním systémem. Jeho funkcí je především předávání informací o jednotlivých položkách a osobách. Často se však stává, že výrobci zařízení implementují ve svých zařízeních pouze podmnožinu tohoto protokolu, je tedy dobré před nasazením prověřit, zda jsou všechny potřebné funkce skutečně k dispozici (Zajíček & Rýzek, 2013).

4.5 HF versus UHF technologie

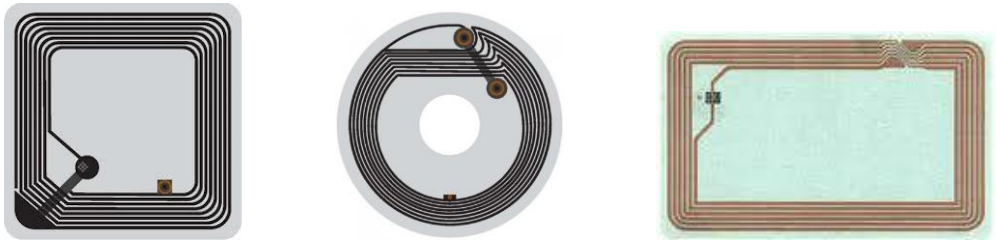
V porovnání HF a UHF technologie má za sebou HF podstatně více zkušeností. Je komerčně dostupná již od devadesátých let, od roku 1999 existují globální standardy a desítky výrobců poskytují čipy, etikety, antény, čtečky a software. Frekvence 13,56 MHz patří do mezinárodní výzkumné a medicínské skupiny, která je dostupná celosvětově (Afrooz & Ygal, 2017). Bohužel toto není případ UHF. Organizace pro standardy jako je *EPC Global Inc.* se snaží v spolupráci s vládami jednotlivých států o harmonizaci UHF frekvencí. Dnes se ale šířka pásma v jednotlivých regionech pohybuje od 860–960 MHz. Spojené státy používají pro RFID aplikace frekvenci 915 MHz, zatím co Evropská Unie 868 MHz (Obr. 2). Minimálně v jedné zemi je UHF pásmo vyhrazené pro vojenské účely. Tato nejednotnost vyhrazených frekvencí

způsobuje, že výrobci produkují specifické čipy a čtečky pro každý region, a to způsobuje problémy pro společnosti, které se snaží vyvíjet své produkty pro globální trh.

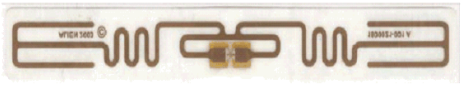


Obr. 2. *Rozdělení RFID podle frekvencí. Zdroj: (Autor).*

Výhodou UHF technologie jsou ale výrazně nižší náklady na RFID etikety, jejich větší dosah i provedení v menších rozměrech (Obr. 3, 4). Při nasazení v uzavřeném systému, nemusí být absence globálních standardů problémem. Přibližně od roku 2010 se ve světě objevují řešení, která vsadila právě na UHF, zejména v USA a Evropě. Podle případových studií prakticky všechny nasadili proprietární řešení od jednoho výrobce, i když určitým rizikem může být, že v budoucnu nemusí být jejich řešení zcela kompatibilní s globálně přijatými standardy. Existuje i řešení, které v sobě spojuje HF a UHF technologii pro etikety i snímače, ale pro běžné využití je nákladnější a využívá se spíše pro postupný přechod od již nasazené HF technologie k UHF (Bilgic & Yeğin, 2016). Větší přínos může znamenat použití duálních snímačů, které detekují HF i UHF etikety použité pro různé typy zařízení, kde UHF přináší lepší výsledky u označení elektricky aktivních prvků, které generují rušivé elektromagnetické záření (Ching & Tai, 2009).



Obr. 3. *HF RFID etiketa. Zdroj: (RFID4u, 2018).*



Obr. 4. *UHF RFID etiketa. Zdroj: (RFID4u, 2018).*

4.6 Zabezpečení výpočetní techniky na bázi RFID

Nasazení RFID pro zabezpečení majetku má výhodu zejména v tom, že lze pomocí průchodových bran nastavit, které oblasti jsou pro přesun položek povolené, a které nikoliv. V praxi se jedná např. o položky, které mají zůstat v jedné místnosti, typicky technika, která je zapůjčená externím osobám při prezentacích nebo vybavení zasedacích místností. Další

položky je povolené přesunovat v rámci určitých lokalit nebo celých budov a u některých se jedná jen o evidování, zda se nacházejí v určitém prostoru – např. kolik uživatelských notebooků má právě možnost připojit se k lokální síti a nakolik tedy bude úspěšné aplikování nové síťové politiky.

RFID etikety lze celkem spolehlivě přilepit na zařízení a v některých případech je i ukrýt dovnitř zařízení. V každém případě je před konečnou aplikací nutné provést důkladnější testování u konkrétního typu zařízení, protože elektronické přístroje často negativně ovlivňují šíření signálu mezi etiketou a čtecím zařízením.

Tab. 2. *Různé RFID frekvence a jejich obvyklé aplikace. Zdroj: (RFID4u, 2018).*

Skupina	Frekvence	Dosah	Aplikace
LF	100–500 kHz	do 50 cm	Kontrola přístupu, ID zvířat, bezklíčový přístup
HF	13,56 MHz	do 1 m	Kontrola přístupu, smart cards, knihovny, označení proti odcizení
UHF	866–956 MHz	5 m a více	Logistický řetězec, třídění batožin, výběr mýta
Microwave	2,45 GHz	1–3 m	Sledování zásilek, výběr mýta

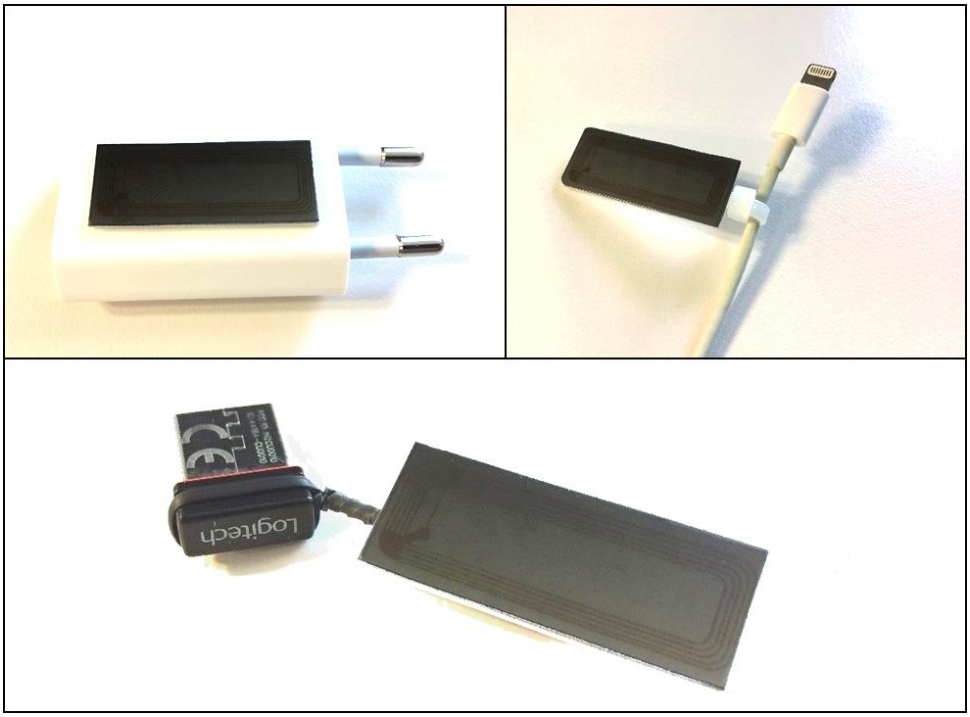
Pro označení položek byl zvolen RFID HF standard 13.56 MHz, který má širokou podporu hardwaru i aplikací, a jednotná velikost pasivních etiket 15x38 mm na 1,5mm plastovém podkladu, který zabezpečil odstup od kovových povrchů (Benamara et al., 2016). Čip na etiketách je typu NXP I-Code SLIX, HF 13.56 MHz, ISO: 15693, 18000-3, co je důležité z hlediska kompatibility s jinými systémy (Rajaraman, 2017). V první fázi byla umístěna RFID průchodová brána v místě u vstupu k 4 velkým zasedacím místnostem tak, aby její dosah garantoval, že bude při průchodu osob detekovat všechny etikety v místě průchodu (Tab. 2). Umístění doplňujícího vybavení zasedacích místností k zapůjčení bylo z jednotlivých místností sjednoceno do jednoho ve společném prostoru mezi průchodovou bránu a vstupy do místností. IT oddělení označilo pomocí RFID stolního snímače 120 položek RFID etiketami, kde se kromě nastavení zabezpečení zapsaly i další doplňující informace k jednotlivým položkám. Příliš malé položky, jako jsou USB vysílače k bezdrátovému příslušenství, se označili etiketou, která je k nim pevně přilepena na delším plastovém pásku.

5 Provedení případové studie

V rámci testování se testovalo spuštění alarmu v průchodové bráně při různém umístění položek v obalech, možné rušení nalepené etikety na vypnutém i zapnutém notebooku nebo průchod více položek najednou. Úspěšnost detekce dosáhla 96 % z 500 pokusů, odstínění etikety se povedlo náhodně při umístění etikety mezi dva notebooky těsně u sebe nebo pak experimentálně umístěním do různých kovových obalů.

Testovala se i rychlá inventarizace položek pomocí zapůjčeného ručního snímače, kdy se rychle načetly všechny položky v dosahu, a porovnáním se seznamem byl vyhodnocen rozdíl k dohledání. Za tímto účelem byla do každého RFID tagu vložena informace podle ISO 28560-2 do pole Primary Object ID (Ayre, 2012), aby bylo možné po načtení identifikovat každý typ zařízení. U tohoto testu byla zaznamenána nižší schopnost detekce, pokud se etiketa nacházela v blízkosti větších kovových předmětů, nicméně po vícenásobném skenování vyhrazeného

prostoru pro položky z menší vzdálenosti (cca 0,5 m) se povedlo načíst všechny. Kontrola úplnosti vybavení je tak velice rychlá a je možné provádět jí podle potřeby i několikrát denně. Při pokusech o odstranění nalepených etiket bylo konstatováno, že lepidlo drží velmi pevně a často dojde spíše k poškození povrchu zařízení, na kterém je etiketa nalepena. Výjimkou jsou malé položky, jako jsou USB vysílače nebo mini video redukce, kde je etiketa s RFID čipem umístěna na plastovém pásku, který je k předmětu připevněn sice pevně, ale menší plochou (Obr. 5). Snadnější cesta, jak odstranit etiketu, která je nalepená celou plochou, resp. znehodnotit její zabezpečovací funkci, je tenkým ostrým nožem etiketu na předmětu zboku nařízнout a pokusit se oddělit anténu od podkladové vrstvy nebo poškodit samotnou anténu v etiketě. Funkčnost a detekci RFID čipu je možné ovlivnit i jinými způsoby, které ale již vyžadují použití více invazivních postupů, jako je například vstříknutí vodivého gelu k samotné anténě nebo přerušení antény na konkrétním místě (Hutter et al., 2010). U malých položek je pak snadnější odlepit plastový pásek s etiketou díky lepší páce nebo přeříznout samotný pásek. V každém případě by se ale již jednalo o záměr obejít zabezpečení a manipulace s etiketou by vyžadovala čas a prostor.



Obr. 5. *Řešení označení malých položek. Etikety ještě nemají nalepený štítek s logem společnosti. Zdroj: (Autor).*

Do pilotního provozu již byly nasazeny položky označené RFID čipy, které na sobě měly i výrazný potisk loga společnosti. Asistentky prošly zaškolením, aby před meetingem informovaly interní i externí uživatele o novém umístění doplňkového vybavení zasedacích místností k zapůjčení a při zaznamenání akustického alarmu upozornili uživatele, zda nezapomněl ve svém počítači USB vysílač k bezdrátovému zařízení. V čase pilotního provozu byl ruční snímač jen zapůjčený, ale využíval se pro rychlou kontrolu aktuálního stavu položek na konci dne.

Důležitý parametr, který jsme v rámci studie sledovali, byla frekvence výpůjček jednotlivých položek uživateli a počet stavů, kdy došlo k vyčerpání dostupných položek a omezení uživatelů. Ideální by bylo mít na místě snímač, který by detekoval aktuální počet vypůjčených a vrácených položek v místnosti (za předpokladu, že na začátku jsou všechny položky umístěné v dosahu snímače). Pro tento účel by šlo použít tzv. chytrý regál, který má snímač zabudován v polici.

Monitorování umístění položek v reálném čase by výrazně zlepšila přesnost a efektivitu správy (Zhang et al., 2017b). Zkušenost z jiné studie poukazuje na to, že pro provoz je mnohem efektivnější mít informaci o stavu položek, které jsou k dispozici přímo uživatelům než o stavu položek, které leží ve skladu (Goyal et al., 2016). V období 1 měsíce byl kontrolován i stav vypůjčených položek vícekrát v průběhu dne, aby se získala statistická data, které položky jsou ve stavu vypůjčení nejčastěji, s tím, že při nejbližší optimalizaci bude doporučeno systém doplnit právě o snímač dostupných položek přímo v místnosti.

6 Výsledky případové studie

Od nasazení zabezpečení pomocí RFID byla v období 3 měsíců odcizena jen jedna položka – USB kabel Apple Lightning, z kterého byla nalezena odtržená etiketa v zasedací místnosti. U jednoho adaptéru k notebooku byla zaznamenána poškozená etiketa při pokusu o odlepení. V pěti případech uživatelé vrátili zapomenutý adaptér, když je na to upozornil akustický alarm při odchodu ze zasedací místnosti. Ani jednou nebyl zaznamenán alarm při zapomenutém USB vysílači, zejména i z důvodu, že jsou výrazně označené plastovým páskem s logem společnosti, který nelze přehlédnout. Potvrdilo se tedy, že nasazení zabezpečení skutečně vedlo ke snížení přímých ztrát způsobených odcizením položek určených pro zápůjčky.

Analýza nákladů a přínosů má odpovědět na otázku, za jaký čas může společnost počítat s návratností investice. Kdy se tedy společnostem vyplatí uvažovat nad zabezpečením výpočetní techniky z pohledu nákladů na zavedení a efektivnost v provozu? Náklady na zavedení technologie představují především cenu za větší hardwarové komponenty, cena samotných RFID tagů je pak již poměrně nízká. Ve zkoumaném testovacím provozu jsme se dostali na cenu základního vybavení za přibližně 80000 Kč bez DPH, ale v ceně není započtena cena práce, kterou do testování vložilo interní IT oddělení. Při zakoupení vybavení za plnou cenu je potřeba počítat s částkou kolem 200000 Kč bez DPH. Proto by této investici měla odpovídat i cena a množství položek, které budou zabezpečeny a zejména frekvence jejich pohybu, kterou je potřebné sledovat a zaznamenávat.

Po přepočtu z testovacího prostředí by se tedy mělo jednat o položky v celkové hodnotě od 500000 Kč, u kterých je zvýšené riziko odcizení nebo u kterých je potřeba monitorovat jejich umístění nebo pohyb. Návratnost investice je odhadována do 5 let, co také umožňuje plánovat další optimalizaci nebo rozšíření systému. Nezanedbatelným přínosem, který je nutné pro každou společnost vyčíslit individuálně, je pak kromě zvýšení zabezpečení majetku i úspora pracovního času zaměstnanců, který může být zejména u odborných zaměstnanců využitý efektivněji.

Jedna z možností, jak povýšit zabezpečení položek, kdy systém vyhodnocuje, zda se položka nachází ve vymezeném prostoru nebo ne, je rozšíření systému o sledování pohybu položek (Li et al., 2018). Při nižších nákladech na počet RFID snímačů tak lze určit vzdálenost položek od samotného snímače nebo zda dochází k manipulaci s položkami. Pro náš účel sledování využití jednotlivých položek uživateli v čase by to znamenalo rozšíření funkce systému bez nutnosti navyšovat náklady na počet snímačů a získání relevantních dat pro optimalizaci počtu položek, které mají být k dispozici. S touto funkcionalitou jsme se zatím nesetkali v nabídce od dodavatelů, ale lze předpokládat, že v budoucnu se stane součástí nabízených komplexních nebo modulárních řešení.

7 Diskuze

7.1 Tendence uživatelů obcházet zabezpečení

Po nasazení zabezpečení do provozu byl počet odcizených položek snížen na minimum a tento stav přetrvává, co bylo i hlavním cílem studie. Dle mého názoru je výsledek ovlivněn zejména tím, že zabezpečení zařízení je viditelné a poměrně těžko odstranitelné, co výrazně eliminovalo snahu o odcizení. Označení pak i snižuje možnost zapomenutí odpojení malých součástí ze soukromých počítačů, jako jsou USB vysílače bezdrátových zařízení. Samotná detekce RFID etiket v průchodové bráně a spuštění alarmu se děje jen u malého procenta zapůjčených zařízení. To mě přivádí k myšlence, zda by pro samotné zabezpečení majetku bez možnosti implementace dalších funkcí, které RFID nabízí, nestačilo použít jen atrapy zabezpečovacích prvků za zlomek pořizovací ceny. Ve zkoumaném případě ale je zvažováno využít potenciál RFID i nad rámec zabezpečení majetku pro optimalizaci evidence a sledování oběhu zařízení mezi uživateli.

7.2 Optimalizace úrovně poskytovaných služeb pro uživatele

Vyhodnocení statistiky zapůjčených položek ukázalo, že nejvíc se za sledované období 1 měsíce zapůjčili video redukce Apple a HDMI k promítání (48x), bezdrátové ovládače pro prezentace (33x) a pak nabíjecí adaptéry k notebookům (25x). Pro specifické video redukce tak bylo doporučeno vytvořit větší skladovou zásobu, aby mohly být okamžitě doplněny v případě jejich nedostupnosti nebo nefunkčnosti a nedošlo ke snížení poskytovaného uživatelského servisu.

Z pohledu společnosti je otázka zákaznického servisu velmi důležitá a v některých diskusích s vedením společnosti byla dávána do popředí před samotné zabezpečení položek. Nedostatek požadovaných položek vždy přímo ovlivní kvalitu poskytovaných služeb a je jedno zda k výpadku došlo z důvodu odcizení položky nebo její nedostatečnou skladovou zásobou. Z tohoto důvodu je důležité, že implementovaná technologie v sobě již v základu kombinuje zabezpečení i sledování stavu jednotlivých položek a mělo to přímý vliv na pozitivní odezvu od vedení společnosti při představení návrhu. Při zvažování dalších funkcí, kterými by měl disponovat systém pro zabezpečení, byla prozkoumána i možnost pro ochranu před neoprávněným klonováním RFID čipů (Kamaludin et al., 2018), která sice zatím nebyla uplatněna v našem řešení, ale vyvolala otázku, zda by neměla být součástí jiných důležitých systémů, které společnost používá. Pro oprávnění osob ke vstupu a pohybu po budově společnosti se standardně využívají bezkontaktní HID (Hughes Identification Device) karty na bázi RFID. Na základě otázky, kterou jsem řešil u našeho projektu, byla ověřována a následně implementována ochrana pro odhalení naklonované HID karty v systému.

7.3 Potenciál technologie RFID na další rozšíření

Ve společnosti bylo již od začátku u systému uvažováno kromě úlohy zabezpečení i otestování jeho potenciálu nad rámec zabezpečení majetku pro další vylepšení skladové evidence a sledování položek výpočetní techniky, proto při návratnosti investice nebylo počítané jen se zamezením ztrát. Dalším důvodem jsou časté výpůjčky výpočetní techniky pro interní a externí zaměstnance, kteří zařízení používají mimo budovu společnosti. Systém proto může vyhodnocovat, jak často a jak dlouho jsou konkrétní položky ve stavu výpůjčky a zda se právě nacházejí v budově, mimo ni nebo ve skladu. To umožní optimalizovat počty a typy zařízení, které mají být k dispozici tak, aby nedocházelo k omezování uživatelů ani přebytkům na skladu.

Pro potřeby označování malých položek budou testovány vzorky mikro RFID tagů, zda lze v praxi dosáhnout dostatečných parametrů jejich dosahu a spolehlivosti čtení. Pro různé zařízení lze aplikovat různé typy tagů, zejména podle způsobu jejich pevného uchycení a následně dostatečného odstínění od kovových ploch a rušení ze samotného zařízení, aby byla zaručena spolehlivost detekce.

Obr. 6. *Různé typy RFID tagů. Zdroj: (Coresonant, 2018).*

Pro získání vzorků lze oslovit výrobce v Číně, kteří se specializují na výrobu mikro RFID tagů a souvisejících zařízení, nemusí se tak zakoupit pro účely testování celé balení v minimálním počtu 1000 ks. Z výsledků testování pak bude možné stanovit vhodné typy mikro tagů pro konkrétní zařízení a podle toho vybrat portfolio několika typů, které se budou dále aplikovat (Obr. 6).

Rozšíření systému RFID pak v další fázi předpokládá označit přibližně 2000 ks základních položek výpočetní techniky, zejména součásti počítačových sestav a zakoupení minimálně jedné průchodové brány a ručního snímače pro inventarizace. Důležitou součástí je i evidenční software, který musí být napojen přímo na RFID zařízení, a tak sledovat pohyb položek v reálném čase. Je zvažováno také zapojení modulů do stávající evidence, které budou dodávat data z průchodových bran a ručních snímačů, co by byla levnější alternativa k novému samostatnému systému evidence, který již s RFID přímo počítá. V každém případě by však mělo být dosaženo optimalizace pracovního času a počtu zařízení, která bude vyčíslena v úspoře dalších nákladů.

Seznam použité literatury

Afrooz, M., & Ygal, B. (2017). Improving logistics processes of surgical instruments: case of RFID technology. *Business Process Management Journal*, 23(2), 448-466. doi: 10.1108/BPMJ-06-2016-0127

Ayre, L. B. (2012). RFID Standards. *Library Technology Reports*, 48(5), 20-26.

Benamara, M., Grzeskowiak, M., Salhi, M., Lissorgues, G., Diet, A., & Le Bihan, Y. (2016). Improvement of HF RFID Detection for Small and Misaligned Tag. In *Proceedings of the 22nd International conference on applied electromagnetics and communications*. New York: IEEE. doi: 10.1109/ICECom.2016.7843885

Bilgic, M. & Yeğin, K. (2016). An HF/UHF dual mode RFID transponder antenna and HF range extension using UHF wireless power transmission. *Turkish Journal of Electrical Engineering & Computer Sciences*, 24, 3949-3960. doi: 10.3906/elk-1412-169

Bunker, R., & Elsherbeni, A. (2017). A modular integrated RFID system for inventory control applications. *Electronics*, 6(1), no. 2. doi: 10.3390/electronics6010009

Ching, S. H., & Tai, A. (2009). HF RFID versus UHF RFID - Technology for Library Service Transformation at City University of Hong Kong. *Journal of Academic Librarianship*, 35(4), 347-359.

Coresonant. (2018). RFID Tags. Retrieved December 10, 2018, from http://coresonant.appspot.com/html/Tags.html

Goyal, S., Hardgrave, B. C., Aloysius, J. A., & DeHoratius, N. (2016). The effectiveness of RFID in backroom and sales floor inventory management. *International Journal of Logistics Management*, 27(3), 795-815. doi: 10.1108/IJLM-03-2015-0051

Hutter, M., Plos, T., & Feldhofer, M. (2010). On the security of RFID devices against implementation attacks. *International Journal of Security and Networks*, 5(2-3), 106-118.

Kamaludin, H., Mahdin, H., & Abawajy, J. H. (2018). Clone tag detection in distributed RFID systems. *PLoS One*, 13(3), e0193951. doi: 10.1371/journal.pone.0193951

Koski, K., Koski, E., Virtanen, J., Björninen, T., Sydänheimo, L., Ukkonen, L., & Elsherbeni, A. Z. (2012). Inkjet-printed passive UHF RFID tags: review and performance evaluation. *International Journal of Advanced Manufacturing Technology*, 62(1-4), 167-182. doi: 10.1007/s00170-011-3782-8

Li, L., Guo, C., Liu, Y., Zhang, L., Qi, X., Ren, Y., Liu, B., & Chen, F. (2018). Accurate Device-Free Tracking Using Inexpensive RFIDs. *Sensors*, 18(9), no. 2816. doi: 10.3390/s18092816

Pane, S. F., Awangga, R. M., & Azhari, B. R. (2018). Qualitative evaluation of RFID implementation on warehouse management system. *Telkomnika*, 16(3), 1303-1308. doi: 10.12928/TELKOMNIKA.v16i3.8400

Rajaraman, V. (2017). Radio Frequency Identification. *Resonance*. 22(6), 549-575.

RFID4u. (2018). HF and NFC Tags. Retrieved December 10, 2018, from https://rfid4ustore.com/rfid-tags-labels/rfid-hf-nfc-tags/

Yin, K., R. (2014). *Case Study Research Design and Methods.* Thousand Oaks, CA: Sage.

Yong, W., Qing, L., Lei, W., & Hao, S. (2018). Improvement of RFID locating algorithm in warehouse security system. In Proceedings of *IEEE 13th International Conference on Electronic Measurement and Instruments* (pp. 190-195). New York: IEEE. doi: 10.1109/ICEMI.2017.8265762

Wang, L., Norman, B. A., & Rajgopal, J. (2017). Maximizing read accuracy by optimally locating RFID interrogators. In *RFID Handbook: Applications, Technology, Security, and Privacy* (pp. 181-198). Boca Raton: CRC Press. doi: 10.1201/9781420055009

Zajíček P., & Rýzek J. (2013). Standardy a pravidla pro technologii RFID. *Informačné technológie a knižnice*, 2013(2). Retrieved December 10, 2018, from http://itlib.cvtisr.sk/archiv/2013/2/standardy-a-pravidla-pro-technologii-rfid.html?page_id=2461

Zhang, Y., Chen, S., Zhou, Y., & Odegbile, O. (2018). Missing-tag detection with presence of unknown tags. In *Proceedings of the 15th Annual IEEE International Conference on Sensing, Communication, and Networking*. New York: IEEE. doi: 10.1109/SAHCN.2018.8397133

Zhang, L., Alharbe, N., & Atkins, A. S. (2017a). An IoT Application for Inventory Management with a Self-Adaptive Decision Model. In *Proceedings of the IEEE International Conference on Internet of Things* (pp. 317-322). New York: IEEE. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.77

Zhang, H., Feng, X., & Wen, J. (2017b). Research on storage location technology based on RFID. In: *Advanced Graphic Communications and Media Technologies* (pp. 673-681). Singapore: Springer. doi: 10.1007/978-981-10-3530-2_84

The article has been reviewed. | **Received:** 6 December 2018 | **Accepted:** 17 May 2019

Academic Editor: Stanislava Mildeova