Vývoj a současné trendy počítačově podporovaných technologií identifikace

The development and current trends in computer-assisted technologies of identification

Michal Šmiraus

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

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

Jméno a příjmení:	**Michal ŠMIRAUS**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Vývoj a současné trendy počítačově podporovaných technologií identifikace**

Zásady pro vypracování:

1. **Zmapujte vývoj a metody užívané k individuální identifikaci osoby.**
2. **Rozveďte možnosti moderních technologií při zpracování informací.**
3. **Vymezte pojmy indentifikace a verifikace.**
4. **Popište a srovnejte jednotlivé identifikační metody.**
5. **Seznamte se s přístrojovou technikou použitou při identifikaci.**
6. **Vlastní práci doplňte obrazovými podklady a grafy.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

1. Porada, Viktor a kol. Kriminalistika. Akademické nakladatelství CERM, s.r.o. Brno, 2001. ISBN 80-7204-194-0
2. Čandík, Marek. Objektová bezpečnost II. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-217-3
3. Rak, Roman. Biometrické docházkové systémy a měření jejich výkonnosti. In: Security Magazín, Roč. XII, vyd. 54, 2/2005. Family media, spol. s.r.o., Praha, 2005. ISSN 1210-8723.
4. International Biometric Group (IBG) http://www.ibgweb.com
5. Biometric Consortium http://biometrics.org (informace o vývoji, výzkumu a aplikaci identifikace a verifikace osob na biometrické bázi)
6. FindBiometrics http://findbiometrics.com
7. European Biometric Forum (EBF) http://eubiometricforum.com

Vedoucí bakalářské práce: JUDr. Vladislav Štefka
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: 22. února 2008

Termín odevzdání bakalářské práce: 3. června 2008

Ve Zlíně dne 22. února 2008

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ať chceme nebo ne, každý z nás se v dnešní době setkává s různými formami identifikačních systémů. V kterémkoli obchodě se zboží rozlišuje podle etiket s čárovým kódem, bankomat po nás chce kartu s magnetickým proužkem, telefonní automat nás spojí po vložení čipové karty s kontaktním polem atd. Vždy se však jedná o jistý způsob nakládání s informacemi, našimi (někdy vysoce důvěrnými) informacemi, které je třeba čím dál tím lépe střežit. S rostoucí cenou informací totiž navíc vzrůstá přímou měrou také riziko jejich možného zneužití a je stále důležitější, aby k našim informacím neměl přístup nikdo nepovolaný. Bezpečná a jednoznačná identifikace za využití prostředků moderní výpočetní techniky nám přitom může výrazně pomoci možným (nejen) informačním ztrátám zabránit.

Cílem mé bakalářské práce je zpracování zevrubného přehledu nejpoužívanějších identifikačních technologií v bezpečnostním i civilním sektoru.

Klíčová slova: identifikační systémy, biometrie, přístupové systémy, ezoterická identifikace

ABSTRACT

Whether we want it or not, each of us is today beset with various forms of identification systems. In any supermarket goods are discriminated by the barcode labels, teller wants a card with a magnetic stripe, telephone will connect us by inserting a smart card with contact field, etc. Always, however this is a sure way of dealing with information, our (sometimes highly confidential) information and that must be increasingly better guard. With the increasing price of information is in addition also increasing the risk of a direct contribution to their possible misuse, and it`s increasingly important that our information hasn`t had access from nobody unsignificant. Secure identification by the use of modern computer technologies can help us to avoid (not only) possible information losses.

The aim of my bachelor thesis is processing the comprehensive survey of identification technologies in the security and civilian sector.

Keywords: identification systems, biometrics, access system, esoteric identification

Na tomto místě bych rád poděkoval svým rodičům za morální a finanční podporu při studiu, dále pak panu Ing. Vladimíru Šiškovi z oddělení systémů automatické identifikace firmy Phobos spol. s r.o. za cenné podněty k doplnění informací o dané problematice získané v rámci odborné exkurze v podniku.

Poděkování patří také JUDr. Vladislavu Štefkovi za kvalitní odborné vedení, připomínky a poskytnuté konzultace při zpracování mé bakalářské práce.

„Technický vývoj směřuje vždy od primitivního přes komplikované k jednoduchému“

Antoine de Saint-Exupéry

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně dne 3.6. 2008

…….

Podpis diplomanta

OBSAH

ÚVOD

Z historického hlediska je problematika spolehlivé identifikace, tedy rozpoznávání osob, stará jako lidstvo samo. V dávných dobách byla tato identifikace založena především na osobní známosti a vzhledu rozpoznávaných lidí. Lidé tehdy žili v poměrně malých a uzavřených komunitách, proto jim nečinilo problém zapamatovat si tváře svých druhů, přičemž vlastně nevědomky používali základní a přirozenou vlastnost, kterou i dnes používá každý z nás – vizuální biometrickou identifikaci.

S postupným rozšiřováním a rozvojem lidské společnosti (např. rozvoj obchodů či zahraniční politiky) však tato jednoduchá metoda přestala postačovat a vznikla zde nová potřeba dobře rozpoznat také identitu osob nám neznámých. V té době se však tento problém týkal stále jen poměrně malého počtu osob.

Identifikační technologie založené na vědeckých základech byly vyvíjeny až specializovanými bezpečnostními službami (kriminalistickými ústavy, tajnými službami apod.) především pro své vlastní profesní potřeby. Při vývoji se často využívaly vědecko-technické poznatky ze zpracování zpravodajských a vojenských informací. Identifikace osoby hrála a hraje velmi důležitou roli také při vyšetřování trestného činu či při soudním dokazování. Tak jak narůstala kriminalita, tak se v praxi ujímaly nové identifikační metody s jejichž pomocí bylo úspěšně řešeno stále více případů a vzrůstaly také požadavky na možnou automatizaci takového identifikačního zkoumání.

Prvořadým zájmem byla pochopitelně identifikace člověka – pachatele. Později pak byla identifikace chápána mnohem obecněji, z daleko širšího záběru praktického využití. Potřeba spolehlivé identifikace osob nadále výrazně vzrostla v souvislosti s dalším rozvojem lidské civilizace (zejména se svobodným pohybem osob, zboží a rozvojem dopravy) a dnes, v době počítačů, se tento problém stává doslova problémem každého z nás.

V minulosti byly identifikační systémy v běžném praktickém životě občana založeny především na znalosti nebo vlastnictví určité věci, případně jejich kombinací. Svoji identitu osoby v úředním styku prokazovaly pasem, občanským, řidičským, služebním průkazem, rodným listem, ID kartou. V přístupu k různým automatům, založených na výpočetní technice, pak přístupovým heslem s využitím **PIN** ***(Personal Identification Numer)***.

Tyto prostředky však neposkytují dostatečnou jistotu, že prokazující se osoba je skutečně tou osobou, za kterou se vydává. Heslo může být prozrazeno, uhodnuto odposlechnuto nebo odpozorováno z klávesnice. Pasy, ID karty, průkazy mohou být odcizeny nebo zfalšovány. Důvody proč se lidé snaží předstírat jinou než vlastní identitu, jsou různé. Většina případů se však omezuje na vlastní prospěch, především finančního charakteru, snahu o získání citlivých informací případně skrytí vlastní identity.

Udává se, že jen v USA dosahují ztráty způsobené podvody realizované zneužitými bankovními kartami a počítačovými hackery až 200 miliard ročně.

Z těchto důvodů je dnes věnováno mnoho úsilí na vývoj nových identifikačních metod, které by byly schopny spolehlivě zajistit skutečně průkaznou, rychlou a jednoznačnou identifikaci osob. Jedním z nejperspektivnějších odvětví je v tomto směru biometrie a biometrické identifikační prostředky, které mají dnes stále větší uplatnění jak v kriminalistice a bezpečnostní činnosti obecně, tak i v běžném občanském životě.

I. TEORETICKÁ ČÁST

1 HISTORICKÝ VÝVOJ POČÍTAČOVĚ PODPOROVANÝCH TECHNOLOGIÍ IDENTIFIKACE

Přestože v době plošného rozvoje elektroniky v sedmdesátých a osmdesátých letech minulého století ještě výkonnost výpočetní techniky nebyla zdaleka dostatečná pro řešení složitých identifikačních úloh, velká pozornost byla věnována právě důslednému a podrobnému zkoumání všech možných vztahů, metod, markantů a charakteristik využitelných pro identifikaci. Cílem bylo maximálně zefektivnit, formalizovat a zjednodušit algoritmy spojené s identifikací osob tak, aby je bylo možné bez ztráty přesnosti využít pro zpracování na tehdy ne dostatečně výkonné výpočetní technice.

Dostatečně silný a účinný aparát přitom poskytly vědní obory, ležící mimo primárně zamýšlenou kriminalistickou oblast – matematika, logika, kybernetika, informatika, technické disciplíny (snímací a měřící technika) apod.

Kriminalistika se pro identifikaci snažila vyhledávat jevy pro člověka individuální, zvláštní a specifické, pomocí nichž by se pak prováděla identifikace individua osoby. Na této filosofii byla a je založena klasická teoretická kriminalistická identifikace, jejíž mohutný a silný teoretický základ byl v našich podmínkách rozvíjen zejména v padesátých a sedmdesátých letech sovětskou školou. [1]

Při dnešním systémovém pojetí identifikace, které je umožněno novými teoretickými poznatky z mnoha vědních oborů i výkonným zázemím již dostatečně výkonné moderní výpočetní techniky, lze dospět k závěrům, že i individuální lidské charakteristiky, jako jsou otisky prstů, lidský hlas, fyzický vzhled tváře, písemný i mluvený projev, je možné obecně analyzovat a modelovat za využití komplexního i systematického přístupu. Pro identifikaci osoby pomocí biometrických charakteristik pak lze využít také obecné metody, využívané pro identifikaci v řadě „civilních“ vědních oborech. Pochopitelně, že tyto metody mají ve vztahu k identifikaci člověka své specifičnosti, ale vycházejí ze základních metod užívaných pro obecné vědecké porovnání dvou objektů.

Přestože kriminalistika je úzce spjata s dalšími bezpečnostními vědami, nelze ji z pohledu dnešní světové globalizace trhů principiálně komercializovat. Státní kriminalistické ústavy a forenzní instituce nemají ve svém popisu práce primárně vyvíjet i technologie, využitelné v civilním, zejména pak obchodním sektoru. Řada především starších kriminalistických teoretiků navíc nepostihla a nepochopila možnosti, které

moderní věda a výkonná výpočetní technika nabízejí, takže mnoho kriminalistických škol si myslím svým způsobem „zaspalo dobu“ a žije svůj život mimo současný reálný svět.

Důsledek je logický. Dříve čistě kriminalistické metody a technologie jsou dnes vynášeny z uzavřených státních institucí, pracujících v bezpečnostním a obranném sektoru, do vnějšího prostředí civilních vědecko-výzkumných institucí a zde dále intenzivně rozvíjeny. Výsledné produkty jsou vzhledem k co nejširšímu využití (a tedy i zisku z nich) realizovány mnohem obecněji, s daleko širším aplikačním využitím. Jejich zpětné nasazení v kriminalistické praxi je pak jen jedna z mnoha možností jejich využití.

Již zmiňovaná globalizace světového trhu a bouřlivý rozvoj mikroelektroniky a komunikací (osobní počítače, Internet, mobilní telefony) v devadesátých letech, to vše se díky nevídanému množství uživatelů pozitivně odrazilo i v cenové hladině takovýchto produktů a služeb. Co si dříve mohly dovolit jen finančně silné státní instituce je během několika málo let najednou dostupné nepoměrně větší skupině různorodých zákazníků. Díky konkurenčnímu boji v oblasti počítačového průmyslu a telekomunikací, jehož cílem je zisk, se k uživatelům dostávají i dříve nepřístupné technologie za přijatelnou cenu, která neustále klesá, popř. za stejnou cenu jsou nabízeny stále technicky dokonalejší prostředky.

To, co bylo speciálně vyvíjeno pro vojenský a bezpečnostní komplex v uzavřených laboratořích a střediscích, to dnes vyvíjí komerčně orientované firmy pro civilní trh a své produkty, s případnými specifickými a nadstandardními modifikacemi, nabízejí i pro využití v oblasti vojenství a bezpečnosti. Pod státní kontrolou zůstávají špičkové strategické technologie jen několika světových velmocí, které si mohou dovolit vývoj drahých a náročných technologií ve strategických vojenských a zpravodajských oblastech, které vyžadují rozsáhlý výzkum a pochopitelně i vysoký stupeň utajení.

Rozvoj nových informačních technologií je determinován nejen lidskou touhou po poznání, ale i ekonomickou stránkou věci: na jedné straně ušetřit (náklady na výrobu a distribuci produktu) na straně druhé (v tržně orientovaných společnostech) zvýšit zisk. Stranou nezůstává ani lidské pohodlí, které je spojováno s komfortem i tzv. uživatelskou přítulností. Nemalou roli hraje i vlastnost člověku bytostní – lenost.

Požadavky na uživatelský komfort a pokud možno také úplná automatizace prováděných operací, to vše se promítá i do vlastního nasazení nových identifikačních technologií v praxi, jak následně budu ilustrovat v dalším textu.

Jako model možného vývoje použitých identifikačních metod, od starších jednoduchých až po moderní a vyspělé, uvedu příklad ostrahy objektu, do kterého mohou zaměstnanci vjíždět vozidly.

První kontroly v této praktické situaci byly v dávné minulosti prováděny pomocí strážných (vrátných), kteří kontrolovali identitu osoby a vozidla na základě předkládaných dokladů, umožňující vstup do objektu. S postupným rozvojem množství vozidel i parkovacích míst bylo neúnosné zaměstnávat stále větší a větší počet vrátných.

Nejprve se tak objevily identifikační karty s automatickým otevíráním závory a počítačovým vyhodnocováním času, stráveném v objektu. Později, aby řidiči nemuseli být obtěžování zdlouhavým stahováním okna vozu, což zejména v zimních měsících mohlo být značně nepříjemné, objevily se následně kamerové systémy schopné číst poznávací značku vozidla, tu digitalizovat a porovnat s počítačovou evidencí vozidel, kterým bylo uděleno oprávnění vjezdu do objektu.

Objevil se tu však problém, protože z hlediska regulace přístupu v režimových objektech není zpravidla ani tak rozhodující oprávnění pro vjezd vozidla, jako rozpoznání osoby ve vozidle. Pak by nebylo dokonce ani podstatné, v jakém automobilu osoba vjíždí do kontrolovaného objektu. S pomocí moderních kamerových systémů jsme dnes schopni řešit i tuto alternativu a přístupové systémy, umožňující vizuální identifikaci jsou dnes předmětem rozsáhlého vědeckého výzkumu a bádání.

Pochopitelně, že úrovni ochrany vstupu do objektu musí odpovídat i úroveň všech kontrolních mechanismů, vycházejících z bezpečnostní politiky ostrahy daného objektu, přičemž na použité způsoby zpracování charakteristických informací, které dále rozvedu v následujících kapitolách a dle kterých vlastní identifikaci provádíme, je třeba klást patřičný důraz, protože např. při budování komplexně zabezpečeného prostoru sehrává spolehlivá a pokud možno plně automatická identifikace oprávněnosti (autenticity) vstupujících osob velice významnou roli.

2 VÝZNAM INFORMACÍ V MODERNÍ DOBĚ

Jak již bylo zmíněno v předchozí kapitole, technický a hospodářský vývoj po 2. světové válce přinesl prudký rozvoj technologií rychlé komunikace, které pracují bez ohledu na hranice států. Rozmáhá se mezinárodní obchod, umožněný pružnými dopravními technikami, vzniká světový trh, konkurence a monopoly. S těmito průvodními jevy globalizace v dnešní době však stále roste a sílí význam informací a informační techniky. Vzniká globální elektronizovaný finanční trh včetně investic, jednotný trh nových technologií a technicky náročných výrobků.

Bohužel tento dynamický rozvoj společnosti, poznání, vědy a techniky se nevyužívá jen pro „sféru dobra“. Od nepaměti jsou lidské poznatky a technické prostředky využívány i ve „sféře zla“, která má nejrůznější podoby. Od lokálních a globálních válek přes různé hrubosti a násilnosti až po kriminalitu všeho druhu a rozsahu, která má u nás v současnosti stoupající trend. K potírání zločinnosti by měla kriminalistika využívat dokonalejší metody a prostředky než pachatelé trestných činů, což dnes není zdaleka skutečností. Proto by mělo být pro současnou dobu charakteristické zvýšené úsilí nejen v tom, zabezpečit nejmodernější techniku pro boj s kriminalitou, ale i rozvoj vlastních kriminalistických věd.

Jednou z důležitých metod při odhalování pachatelů je identifikace, jejímž cílem je ztotožňování objektů (osob zvířat, předmětů), které mají vztah k trestnému činu.

V souladu s teoretickými rozbory v oblasti identifikace se pak jedná o identifikaci objektovou, která, je-li aplikována na kriminalistiku, což jí dává určitá specifika, bývá označována jako identifikace kriminalistická. Základem každé úspěšné identifikace jsou v takovém případě informace o všem, co může hodnověrně potvrdit něčí identitu, na základě čehož pak je možno např. usvědčit pachatele trestného činu, umožnit vstup oprávněné osoby do objektu s režimovým opatřením, realizovat ověřeným způsobem finanční transakce apod.

Odkud informace získáváme a jakým způsobem jsme schopni různé druhy informací využít, zpracovat či dále analyzovat, o tom pojednávají následující kapitoly.

2.1 Základní přístupy k získávání informací

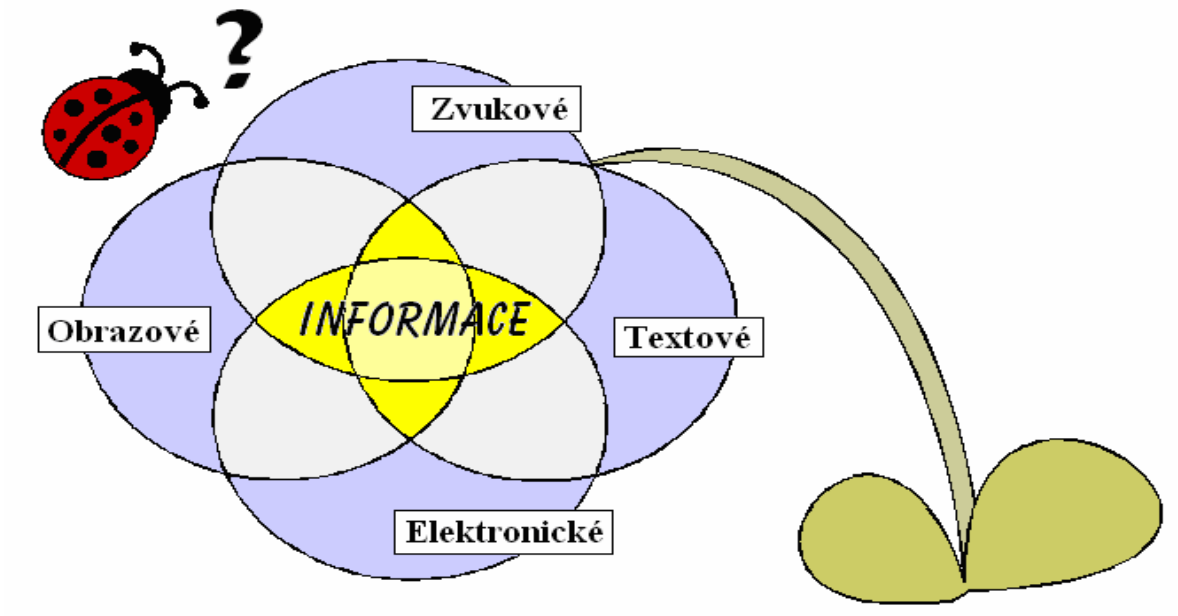
Při získávání, vytěžování a analýze informačních zdrojů rozlišujeme dva základní směry. První je **klasický agenturní přístup**, známý z prostředí zpravodajských služeb, který pro získávání informací využívá lidských schopností (agentů, informátorů, tajných spolupracovníků, operativních důstojníků, …). V odborné literatuře se s tímto druhem zpravodajství setkáváme pod zkratkou **HUMINT** ***(HUMan INTelligence)***. Ten jako jediný může postihnout plány a záměry sledovaných aktérů ještě před prvými kroky k jejich realizaci. Dodnes platí za nejúčinnější metodu vytěžování informací, avšak výsledky přicházejí pomalu – nasnadě jsou výhody a nevýhody lidského faktoru.

Druhým směrem je pak možnost **nasazení technických prostředků** (monitorovacích stanic, odposlechů, sledování, automatizované vyhodnocování komunikace, pohybu apod.)

Tyto dva základní přístupy jsou (byly a budou) využívány v různých zpravodajských službách v jinou dobu a protože jsou oba přístupy samy o sobě vyhraněné, budou také různě, periodicky preferovány, přičemž je velmi efektivní oba způsoby mezi sebou kombinovat a vzájemně doplňovat, neboť oba mají své přednosti i nedostatky.

2.2 Charakteristické členění informací

Identifikace byla donedávna doménou čistě bezpečnostního sektoru. Ještě v průběhu osmdesátých let 20. století to byly právě zpravodajské a policejní složky, které jako jediné ve velkém, intenzivně a systematicky shromažďovaly informace o osobách a nejrůznějších objektech. Velké množství informací vyžadovalo také nasazení výkonných automatizačních prostředků s cílem urychlit a celkově zkvalitnit proces vyhodnocování informací, přičemž všechny rozvinuté průmyslové státy do této oblasti investovaly nemalé prostředky. Špičková, výzkumná, vývojová i provozní pracoviště pracovala na nejvyšším stupni utajení. Pozornost byla věnována všem formám informací v klasické i počítačové podobě. Členění informací na následující čtyři základní druhy, tedy obrazové, textové, elektronické, akustické je však pouze formální, protože ve skutečnosti se informace obvykle různě prolínají (obr. 1), a to zejména při jejich zpracování počítačem. Ručně psaný text může být při zkoumání a analýze chápán jako obrazová informace; stejně tak zvuková, textová nebo obrazová informace může být transformovatelná do podoby elektronické. Jednotlivé charakteristické druhy informací v dalších kapitolách rozeberu podrobněji.



Obr. 1. *Charakteristické členění informací*

2.3 Obrazové informace

Na zpracování obrazových informací je kladen velký důraz, protože jsou názorné, lehce pochopitelné a především pro člověka mají výraznou vypovídací hodnotu. S novodobým rozvojem kosmické techniky a výškového leteckého snímkování byly analyzovány nejrůznější záběry zemského povrchu. Nešlo přitom jen o klasickou vizuální fotografii, ale i o kombinaci magnetických, tepelných a radarových obrazových záznamů.

Např. s přístroji pracujícími v infračervené oblasti, které jsou citlivé na teplo, dokázali analytici nejen „vidět dovnitř budovy“, ale byli schopni například říci i po několika hodinách, že na vzletové dráze startovalo letadlo. Počítače z obrazových snímků dokázaly analyzovat kouř vycházející z kouřovodu a pomocí spektrální analýzy určit, co se spaluje. Klasická fotografie byla často nahrazována stereo fotografií, která umožňovala plastické vidění. Letecké snímky pořízené z různých úhlů pak také dokázaly zobrazit například trávu slehnutou vlivem tlaku od pneumatik či chůze člověka. Počítačová korekce obrazu si musela umět rutinně poradit s nápravou zakřivení způsobeného senzory satelitů nebo atmosférickými jevy. Uskutečňovalo se zaostření mimoohniskových obrazů, sestavení jednolitého barevného obrazu z několika snímků pořízených v různých spektrálních pásmech, což mělo za cíl učinit určité předměty zřetelnější. Běžné byly změny kontrastu mezi zkoumanými objekty a jejich pozadím, zvýraznění určitých obrysů, vymazání stínů, potlačení odlesků a spousta dalších činností.

Poměrně progresivně se v dnešní době vyvíjí vědecko-technická oblast na pomezí umělé inteligence, souhrnně označovaná jako „počítačové vidění“, což je zjednodušeně řečeno napodobení schopnosti lidského vidění pomocí technických prostředků. Teoreticky i prakticky se zde řeší složité problémy spojené se snímáním obrazu v návaznosti na jeho digitalizací nebo dále různým prostorovými i formátovými transformacemi, filtracemi (včetně odstraňování šumu), detekcí hran a zaostřováním obrazu. Vidění člověka je téměř vždy podmíněno předchozími skutečnostmi z viděného světa. Aktuální snahou v tomto směru je efektivně porovnávat zobrazovaná data s nějakým předem naučeným modelem.

Samotnou kapitolou „vyšší školy“ zpracování obrazu je pak vyhledávání určitých objektů v obraze (letadla na letišti, lodě na moři, viry, bakterie), jejich určení (tedy vlastní identifikace) spojené případně ještě navíc s počítáním množství a klasifikace do určených tříd. Zejména díky možnosti analýzy pohybu a analýzy objektů v trojrozměrném obraze se počítačové vidění promítlo i do celé řady civilních činností.

Samotné získávání zpracování a analýza obrazů nebyla však ve zpravodajství a v práci s informacemi obecně postačující. Obrazy jsou totiž zpravidla až projevem určitých okolností, činů nebo jevů již dávno existujících mimo vědomí pozorovatele nebo zpracovatele informací.

Pro představu:

Mnohdy není až tak důležité mít k dispozici první snímek posledního utajovaného letounu nepřítele jako spíše informace o rozhodnutí jej postavit, navíc ještě společně s celým teoretickým, vývojovým a výrobním know-how. Letoun je jen jeden z mnoha produktů, určité technologické úrovně, která byla výrobcem již úspěšně zvládnuta, a tedy ve velkosériové produkci dokáže vyrobit další podobné objekty se stejnými vlastnostmi, jako právě nalezený jedinečný objekt. Ze strategického vojenského hlediska přiměřené obrany je zjištění už vyrobených nových zbraňových systémů informací pozdní.

Je proto nutné mít k dispozici i „signály“, které předpovídají vznik (nebo cílený, plánovaný záměr) určitých objektů, činností nebo událostí.

2.4 Textové informace

Pro vyhledávání a analýzu textových informací jsou dnes běžně užívány především tzv. ***fulltextové technologie***, které se z původně zpravodajského prostředí promítly také do oblasti Internetu nebo činnosti speciálních firem v komerčním sektoru, zabývajících se monitoringem tisku a informačním servisem. Fulltextové technologie pracují s tiskem v elektronické podobě, u něhož jednotlivá písmena mají jasnou předepsanou hodnotu dle známého standardu **ASCII** ***(American Standard Code for Information Interchange)***.

Fulltextové technologie slouží k vyhledávání zájmových (klíčových) slov, které v daném informačním zdroji tvoří cíleně hledaný výraz. Díky rychlému indexování takovýchto klíčových slov pak lze dosáhnout vysoké efektivnosti vyhledávání důležitých nebo zajímavých informačních zdrojů pro potřeby knihoven, redakcí, autorů apod.

Poněkud složitější je automatické vyhledání informací z ručně psaného textu. Zde se nejprve musí písmo rozpoznat, následně potom převést do elektronické podoby a až potom porovnávat. Tyto transformace – rozpoznání ručně psaného písma se realizují pomocí metod, blízkých zpracování obrazu, tj. vyhledávání a rozpoznávání jednotlivých znaků v textovém dokumentu.

Z informačního hlediska je v ručně psaném projevu mnohem více informací než v textu psaném strojově. Obojí texty sice mají stejný slovní obsah, stejně formalizované vyjadřování a používané charakteristické lingvistické rysy – způsoby vyjadřování, slovní zásobu, slang, gramatiku apod. U ručně psaného textu však přibývá navíc ještě charakteristický rukopis. Ten je informačně také velmi důležitý z grafologického hlediska nejen pro psychology, ale např. i pro kriminalisty, protože ručně psané písmo obsahuje osobní, charakteristické rysy, které lze využít pro jednoznačnou identifikaci osoby i její další případnou psychologickou analýzu.

Díky tomu, že již existuje rozličný software pro přenos obsahu ručně psaného textu do elektronické podoby, lze v budoucnosti očekávat vznik samostatných automatických expertních systémů, vyhodnocujících osobnost pisatele právě podle jeho rukopisu.

2.5 Akustické informace

V oblasti zpracování zvukových dat byla od samého počátku věnována pozornost nejen zvukové analýze strojních zařízení vojenského charakteru, např. motorů blížících se letadel nebo lodních šroubů plavidel, ale i lidského hlasu. Automatické zpracování mluveného slova vyžaduje rozpoznání určitého hlasu, jeho analýzu a převedení obsahu tak, aby bylo možno takto získané informace dále účinně a rychle vyhodnocovat. Mnoho technologií zpracování zvuku je založeno na poznatcích ze zpracování obrazu, protože zvuk je možné graficky převádět na nejrůznější grafy, histogramy, obrazové informace a ty porovnávat ze známými vzorky, které jsou rovněž graficky znázornitelné.

Nabízí se i kombinace automatizované analýzy (rozpoznávání lidského hlasu) a fulltextových technologií. Rozhovory je možné realizovat v reálném čase, případně je zaznamenávat na archivační média a ty později dle potřeby zpětně vyhodnocovat. V rozhovorech lze vyhledávat zájmová témata (podobně jako při fulltextové práci s tištěnými informacemi), např. pozornost věnovat telefonátům, kde se hovoří o *atentátu* a *prezidentovi*; identifikovat osobu na základě jejího hlasu, její telefon, popř. graficky na digitální mapě znázornit její pohyb. Předpokladem je strojové „porozumění“ mluveného slova a jeho automatizovaný převod do elektronického textu. Pak už je možné využít dnes běžné metody zpracování, vyhledávání a analýzy textových informací, tak jak bylo popsáno v předchozí kapitole.

Telekomunikační technologie jdou však mnohem dál. Prostřednictvím služby **WAP *(Wireless Aplication Protocol)*** dochází k propojování mobilních telefonů s internetem. Lze tak zajistit okamžitý operativní bezdrátový přístup k obrovskému množství informací (Internet, E-mail, ale i speciální počítačové zájmové evidence bezpečnostních služeb apod.)

Spojení mobilních telefonů s digitální mapou je v zahraničí již běžně využíváno – slouží k operativnímu monitorování pohybu např. vozidel taxislužby, spedičních firem apod. s cílem optimalizace činností i účinné kontroly a ochrany osob, vozidel nebo zboží.

Z bezpečnostního hlediska je využití těchto možností více než zřejmé – operativní sledování zájmových osob s možností odposlechu, monitorování pohybu i času, kde se osoba zdržovala, jak tam byla dlouho s kým byla v kontaktu apod.

2.6 Elektronické informace

Elektronické informace v jakékoliv podobě doplňují předchozí druhy informací, které jsem uvedl. Získávání, vyhodnocování a využití elektronických informací je v odborné literatuře označováno jako signální zpravodajství **SIGINT** ***(SIGnals INTelligence)***. Je to zpravodajství získané monitorováním elektromagnetických vln nebo signálů z kteréhokoliv zdroje, včetně cizích radiových vysílačů, radarů, satelitů a kosmických lodí. Do této oblasti se v poslední době řadí i monitorování mobilních telekomunikačních prostředků. Podstatná část elektronických zdrojů je chráněna šifrováním.

Poznámky:

1. Profesionálně využívané technologie zpravodajských služeb jsou na mnohem vyšší úrovni než technologie dostupné běžné veřejnosti. Patří sem technologie OCR, technologie pro rozpoznávání hlasu a technologie pro vyhodnocování informačního obsahu, které jsou orientované především na práci v reálném čase. Tomu odpovídá i výkonnost nasazených zpravodajských prostředků.
2. Hlavním problémem všech odposlechových služeb je nenechat se zahltit informacemi. K rozpoznání informací se používají speciální výkonné čipy. Je jich celá řada a dokážou předzpracovávat obrazové faxové nebo hlasové „záchyty“. Pro vlastní vyhodnocování těchto dat jsou pak používány i další čipy, protože informace musí být zpracovány s minimálním zpožděním. Tyto čipy filtrují zdrojová data přes desítky tisíc složitých zájmových profilů. Základními stavebními prvky takovýchto profilů mohou být: jednotlivá slova, z nich složené fráze a slovní spojení, jména, telefonní čísla, čísla bankovních kont, různé názvy, řeč (jazyk – např. arabština), lokalita, čas, typ komunikačního spoje ale i hlasová identifikace jednotlivé osoby. Složité profily mohou být vytvářeny různými logickými výrazy s těmito prvky (operátory *a*, *nebo*, blízkost výskytu některých slov ve větě apod.). V souvislosti se zpracováním a analýzou elektronických zdrojů byly také zejména pro zpravodajské služby vyvinuty speciální systémy třídění a získávání informací, které jsou zcela odlišné od běžných fulltextových technologií, které pracují na bázi – tzv. N-gramová analýzy. [1]

Pro rozsáhlost a komplexnost této problematiky se jí však zde v této práci nebudu blíže zabývat, neboť mým primárním cílem je zpracovat možnosti a metody moderních identifikačních technologií obecně, a to s důrazem na věcnost a názornost výkladu.

3 ELEKTRONICKÉ SYSTÉMY AUTOMATICKÉ IDENTIFIKACE

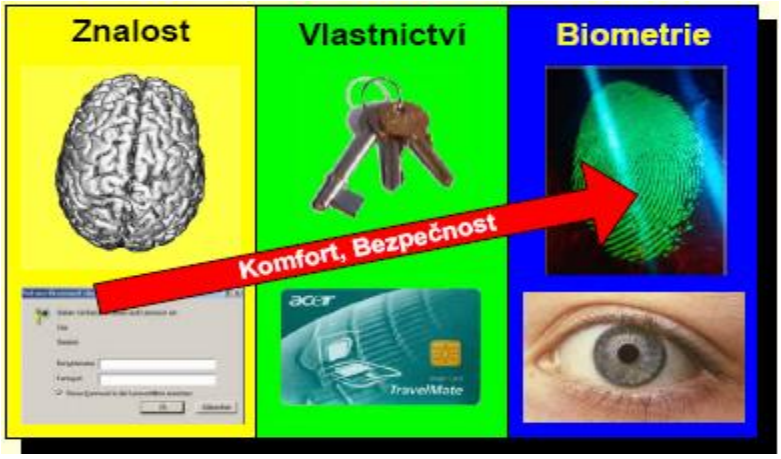
Bezpečnostní sbory, stejně jako věda a technika neustále hledají účinné identifikační metody, které lze automatizovat, a tím urychlit a zároveň snížit provozní náklady na straně jedné a zvýšit přesnost, celkovou spolehlivost a komfort použití na straně druhé (obr. 2)

Pojem samotné identifikace je tedy v praxi vždy neodmyslitelně spjat s požadavkem na efektivní, bezpečné a rychlé potvrzení identity (fyzické či elektronické), přičemž vlastní identita je založena na:

>>> **Něčem co víme** („we know“)

>>> **Něčem co máme** („we have“)

>>> **Něčem co jsme** („we are“)



Obr. 2. *Vzájemný vztah komfortu a bezpečnosti v rámci použitého systému ověřování identity*

Autentizace, tedy vlastní ověření identity, jejíž cílem je potvrzení probíhající identifikace, se pak na základě těchto vyslovených principů v praxi realizuje heslem (PIN), předmětem (ID karta) nebo vlastním tělem (biometricky), přičemž pro dosažení odpovídající úrovně zabezpečení je možné tyto jednotlivé způsoby navzájem kombinovat.

Ochrana hmotného i nehmotného majetku firmy, kontrola přístupu k informacím, přehled o pohybu pracovníků v areálu vzhledem k jejich povinnostem a oprávněním, to vše jsou nové a stále významnější faktory, které považujeme za hlavní priority v rámci svých rozvojových cílů. Jedním z nástrojů, který může pomoci řešit tuto oblast jsou níže popsané metody identifikačních systémů, které představují více či méně spolehlivé řešení s řadou přidaných hodnot ve formě standardních i nadstandardních služeb.

3.1 Optické rozpoznávání znaků – OCR

OCR ***(Optical Charakter Recognizing)***, je softwarovou technologií převodu textu uloženého v bitmapovém formátu do formátu textového. OCR je speciálním případem vektorizace, tedy rozpoznávání písma. Text uložený v bitmapě není chápán jako text, ale jen jako sada tmavých a světlých bodů v obrázku.

OCR program tedy musí identifikovat v bitmapě různé tvary a porovnat je s předlohou a rozhodnout jaké písmenko, ten který shluk představuje. Situace je navíc zkomplikována tím, že texty bývají napsány v různých fontech a dokumenty bývají často nekvalitní. Zvláště xeroxované dokumenty bývají „zašpiněné“, tzn. obsahují rozmazaná písmenka a šmouhy. Program se tedy musí snažit i určit zda tečka poblíž identifikovaného písmenka „c“ je háček a nebo jen nějaké smítko. Novější trasovací programy pracují tak, že dokument procházejí několikrát za sebou a při posledních průchodech už spolupracují s tzv. spell-checkerem (kontrola pravopisu). Mnohé programy pro převod písma do elektronické podoby se umí i „učit“. Když například chci převést do textového formátu sadu dokumentů psaných na jednom psacím stroji, mohu OCR program naučit, že dotyčnému stroji ustřelovalo písmenko „z“ a „k“ bylo trochu rozmazané.

Vektorizace

Vektorizací rozumíme převod dat z rastrového formátu do formátu vektorového. Jedná se o úlohu obtížnou, neboť informací uložených v rastrovém formátu je méně, než informací uložených ve formátu vektorovém, a tak je potřeba nové informace automaticky generovat, nebo je ručně do dat doplnit. Na základě toho pak existuje vektorizace:

- **ruční**, tedy obsluhovaná uživatelem. Na zobrazovacím zařízení (monitoru) se zobrazí rastrový obrázek a podle něj uživatel zadává pomocí vstupního digitalizačního zařízení (tablet nebo myš) jednotlivé vektorové entity. Ruční vektorizace je nejpřesnější, ale velmi zdlouhavá a náročná. Zvláštním příkladem ruční vektorizace může být přímá digitalizace papírové předlohy digitizérem bez použití mezistupně rastrového obrázku.
- **automatická**, obsluhovaná programem. Program musí být schopen na základě informací o barvě jednotlivých bodů určit základní entity,ze kterých se obraz skládá.

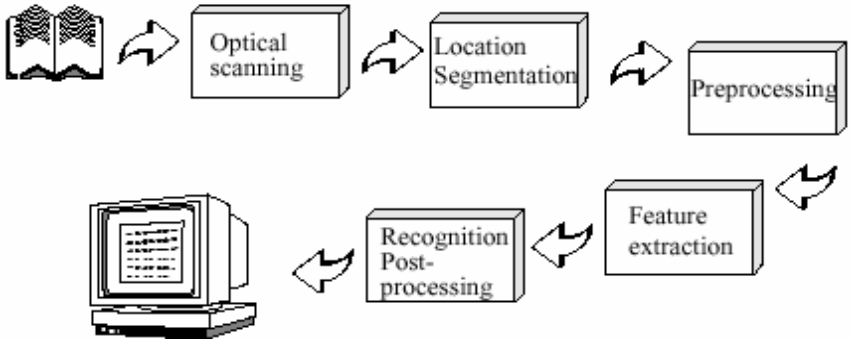
V mnoha případech se pro takový postup používají metody příbuzné umělé inteligenci. Automatickou vektorizaci lze v současné době použít jen u jednoduchých a zřetelných předloh.

- **poloautomatická** vektorizace je dnes nejčastější. Samotnou vektorizaci provádí program, který je v případě sporných situací korigován a opravován uživatelem. Kvalita vektorizace a její rychlost závisí na stupni automatizace.

Princip identifikačního systému OCR

Typické OCR systémy využívají optického skenování (digitalizace), segmentace a lokace snímaného textu, preprocessing (eliminace šumu), extrakce vzhledu a vlastní rozpoznání spojené ještě často s postprocessingem (oprava chyb).

Identita každého znaku je nalezena porovnáním extrahovaných znaků s popisem každého symbolu získaného v učící fázi. Nakonec jsou získané informace využity pro rekonstrukci slov a čísel do originálního textu.

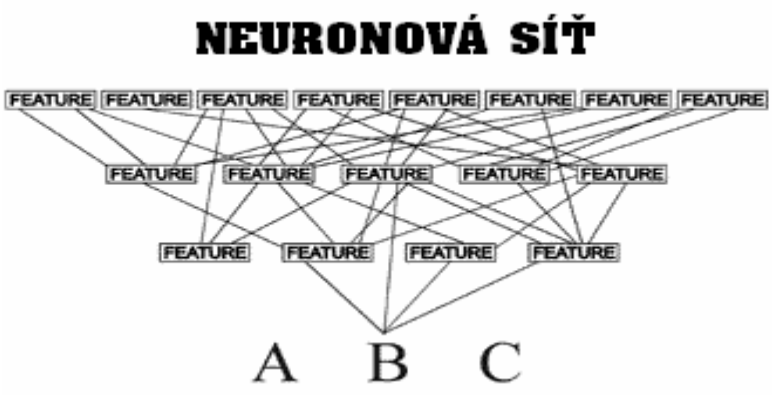


***Obr. 3.** Schématický princip činnosti systému OCR*

OCR algoritmy

Nejčastěji používané techniky OCR jsou dnes založeny na tzv. Markovových modelech neuronových sítích, které zaznamenaly velký úspěch i v rozpoznávání řeči. Jsou to vlastně stavové stroje, které využívají kontextové informace. Počítače obecně nemají problémy s rozpoznáváním dobře napsaných znaků, které se moc neliší od daných vzorů, ale psané znaky jsou mnohdy nejednoznačné a nečitelné i pro člověka. Lidé jsou však schopni v některých případech číst i slova s nečitelnými znaky, a tak by to mělo být i u počítačů. Algoritmy založené na principu rozpoznávání znak po znaku by na takovém slově neuspěly, ukazuje se, že kontextová významová informace je nejen užitečná, ale často i nutná. [10]

Neuronové sítě nezadávají explicitně instrukce počítači, respektive metody na řešení problému, avšak bombardují síť tréninkovými vstupními daty, přičemž pokaždé je počítána chyba (odchylka) hodnot neuronů ve výstupní vrstvě. Základní myšlenkou celého tohoto algoritmu je zpětné šíření vypočtených odchylek do předcházejících vrstev. Čím více dat, tím větší a hlubší poznatky nabude systém a zvětší se tak šance na odstranění chybných vzorů. Neuronové sítě jsou tedy lépe připraveny na vstupy nízké kvality na rozdíl od klasických modelů. Vytrénované sítě jsou schopny vyvodit pravděpodobný odhad, který se pak při vytvoření patřičného výstupu stává důležitou složkou v řešení daného problému.



Obr. 4. *Model umělé neuronové sítě pro systém OCR*

3.2 Optické čárové kódy

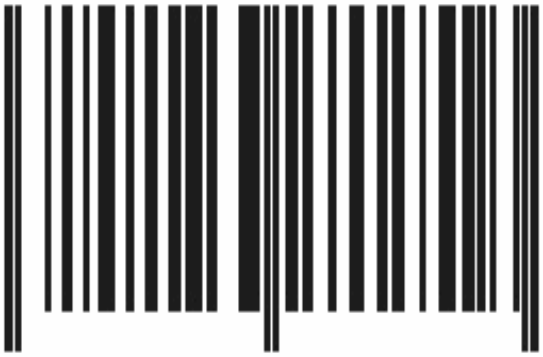
Právě tak jako například písmo (strojově čitelné systémem OCR) jsou optické kódy vlastně jednoduché optické digitální paměti. Klasické a převážně pouze pro čtení určené čárové kódy patří do rodiny optických kódovacích postupů.

Každý čárový kód je tvořen sekvencí čar a mezer s definovanou šířkou. Ty jsou při čtení transformovány podle své sytosti na posloupnost elektrických impulsů různé šířky a porovnávány s tabulkou přípustných kombinací. Pokud je posloupnost v tabulce nalezena, je prohlášena za odpovídající znakový řetězec. Nositelem informace je nejenom tištěná čára, ale i mezera mezi jednotlivými dílčími čarami. Krajní skupiny čar mají specifický význam - slouží jako synchronizační pro čtecí zařízení, které podle nich generuje signál Start/Stop. Technická specifikace pak vyžaduje ochranné světlé pásmo bez potisku před a za synchronizačními čarami.

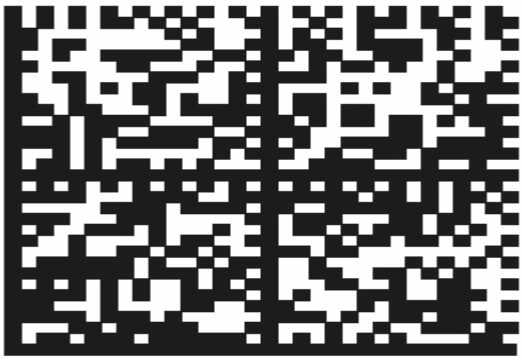
Patent na čárový kód byl poprvé udělen v roce 1949. Podle způsobu, jakým se konkrétní znak kóduje do skupiny pruhů, se kódy dělí do skupin. V současné době je definováno přibližně 200 různých standardů čárových kódů.

Nejpoužívanější standardy čárových kódů

Nejběžnější je jednorozměrný lineární kód (1D), novější jsou dvourozměrné (2D) kódy v různých modifikacích, například sloupcové nebo maticové. U nejnovějších trojrozměrných (3D) kódů je třetím rozměrem barva. Optické postupy kódují data pomocí barevných oblastí různé šířky nebo kontrastem či barvou odlišitelných ploch. Pro čtení musí být všechny kódy přímo viditelné snímačem (lze číst až na vzdálenost 10 m).



Obr. 5. *Princip jednorozměrného (1 D) optického kódu: sled čar různé šířky*



Obr. 6. *Princip dvourozměrného (2 D) maticového optického kódu:obdélníčky*

Optické kódovací postupy byly již standardizovány pro různé druhy použití a obory z hlediska zobrazení kódu a s tím spojených datových struktur.

Příkladem je kód **EAN** ***(European Article Numbering)***, známý ze spotřebitelského zboží, který umožňuje užitím většího množství tzv. zaznamenávačů dat nebo klíčů umístit na poměrně malou etiketu čárového kódu velké množství dat.

Upravená podoba tohoto kódu například umí uchovávat ISBN kódy knížek nebo ISSN kódy časopisů a jiných periodik. Z kódu EAN lze zjistit také zemi původu nebo způsob užití daného zboží, a to na základě prvních tří znaků kódu.

(např. 859 - Česká republika; 858 - Slovensko; 980 - vratné účtenky; …)

V případě nejpoužívanější varianty tohoto čárového kódu v našich zemích EAN-13, jsou jednotlivé symboly kódovány do 13 čísel, rozdělených do čtyř částí:

- ***Systémová číslice**, obsahující první dvě nebo tři číslice, které jak jsem zmiňoval obvykle identifikují zemi, kde je zaregistrovaný výrobce*
- ***Kód výrobce**, skládající se ze čtyř nebo pěti číslic v závislosti na systémovém kódu*
- ***Kód výrobku**, skládající se z pěti číslic, které mohou být použity k označení zboží*
- ***Kontrolní číslice**, tzv. samodetekční kód ověřující správnost zadaných dat*

Méně jsou používány kódy EAN-8, které fungují na stejném principu, ale jsou vyhrazeny a používány pro menší položky, na které je v praxi problém umístit 13místný kód, jako třeba cukrovinky, drobné předměty v úzkých obalech apod.

Plošný kód (2D) se užívá například u poštovních známek nebo ke značení desek plošných spojů, kde je pro obvyklé čárové kódy málo místa. Zpravidla je tištěn na papírových etiketách, snášející teploty pájení. Nověji se vypaluje laserem přímo na desky, a dokonce se tak značí i potiskovací šablony.

Mezi přednosti optických kódovacích postupů patří laciné etikety, standardizované techniky a velké rozšíření. Nevýhodné je oproti tomu poměrně malé množství zaznamenaných dat, zpravidla jen čtecí přístup k datům, nutnost přímé viditelnosti mezi etiketou a čtečkou a malá odolnost proti nepříznivým vlivům okolí.

3.3 Kontaktní magnetické a čipové systémy

Magnetické systémy v praxi existují již od počátku sedmdesátých let, kdy byl systém identifikace pomocí magnetického proužku používán na papírových a na filmu založených ID kartách, stejně jako na kreditních kartách. Modernější čipové systémy vznikly zejména na základě požadavků zajištění větší bezpečnosti a odstranění neduhů občasné nespolehlivosti, kterými se vyznačovaly starší magnetické systémy.

Obě tyto technologie se dnes mohou v zásadě kombinovat, přičemž do budoucna se počítá spíše s převahou modernějšího čipového systému.

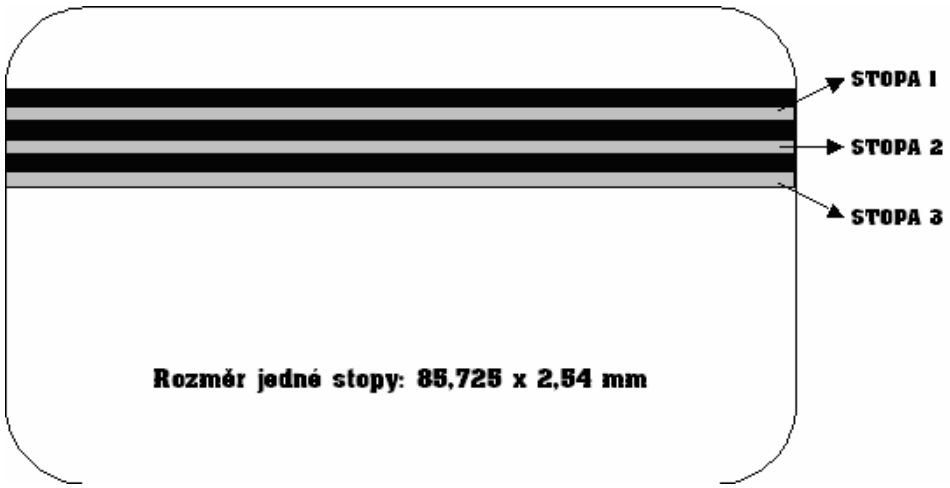
Kontaktní magnetický identifikační systém

Používá se prakticky pouze ve spojení s identifikátory velikosti kreditních karet, použití jiného provedení je prakticky nemožné. Karty jsou velmi levné, zato se však dají relativně snadno padělat a podléhají míře opotřebení, která je ovlivněna:

- *vlastním protahováním karty snímačem – dochází k mechanickému poškození*
- *přítomností magnetických polí, které je může i trvale znehodnotit*

Vlastní technologie je založena na zaznamenávání (kódování) dat do magnetického pásku, na němž se po jeho zmagnetování ve vodorovných stopách vytvoří spousta malých permanentních magnetů. Pokud chceme na kartu nějaká data zaznamenat, potřebujeme k tomu dosti silnou magnetickou indukci působící na jeden z permanentních magnetů. Je přitom důležité působit přesně jen na jedno místo, jinak by se samotný proces záznamu ovlivňoval a tím znehodnocoval data, která přepsat nechceme, či která jsme právě přepsali.

Čtečka identifikačních magnetických karet načítá informaci z magnetického záznamu na kartě, převede ji na elektrický signál a předá k dalšímu zpracování [7]. Samotná čtečka nevyhodnocuje oprávnění vstupu ani nezaznamenává průchod. To je práce případného připojeného terminálu, přístupové jednotky, vyhodnocujícího počítače apod.



Obr. 7. *Magnetický proužek ID karty s vyznačením datových stop*

Pásek na magnetických kartách obsahuje celkem tři stopy, z nichž každá má svůj specifický význam a umožňuje uložit určité množství specifické informace.

1.stopa - Tato stopa byla definována Mezinárodní asociací leteckých dopravců **IATA** ***(International Air Transportation Association)***, aby usnadnila automatické odbavení cestujících, již v roce 1969. Následně tuto normu přijaly v roce 1970 i americké banky. Tato první stopa je schopna pojmout až 79 alfanumerických znaků.

2.stopa - **ABA** ***(American Bankers Association)*** vytvořila standart pro tuto stopu, aby tím umožnila použití karet při on-line finančních transakcích, kde se používá nejvíce. Do této stopy je možné uložit 40 numerických znaků 0-9 a rovnítko.

3.stopa - I tato třetí stopa byla vytvořena bankami (THRIFT) pro finanční transakce. Tato stopa se nejčastěji používá pro uložení informací, které umožňují ověřit PIN při bankovních operacích. Na rozdíl od zbývajících dvou vrstev je tato vrstva definována jako read/write, což znamená, že je možné informace uložené v této stopě přehrávat, například při odečítání kreditů, apd. Do této stopy je možné uložit až 107 numerických znaků 0-9, rovnítko a dvojtečku.

Jednotlivé datové struktury upravuje norma ISO 3554 / ISO 7811, standardní rozměry jsou 85,6 x 54 x 0,76 mm – klasický vizitkový formát, ze kterého dále vychází všechny dnes běžně používané bankovní karty i většina karet identifikačních.

Technologie kódování použitých magnetických proužků je významně spojena s jedním zásadním pojmem v této oblasti, a tím je:

Koercivita – technický termín určující intenzitu magnetického pole, která způsobí změnu dat v magnetické stopě. Udává se v Oerstedech (Oe) a zjednodušeně řečeno určuje, jak náročné je zakódovat potřebné informace do magnetické stopy (proužku), které tak v praxi mohou být dvojího provedení:

LoCo ***(Low Coercivity)*** **–** 300 Oe – jsou spíše hnědé barvy, mají nízkou hustotou záznamu a také menší odolnost vůči negativnímu magnetickému rušení.

HiCo ***(High Coercivity)*** – 4000 Oe – většinou černé barvy mají hustotu záznamu podstatně větší a jsou také více odolné vůči silnému magnetickému poli. Kódovat karty s touto magnetickou stopou je mnohem náročnější než karty s magnetickou stopou LoCo, neboť kódování vyžaduje větší výkon. Karty HiCo jsou proto nepatrně nákladnější.

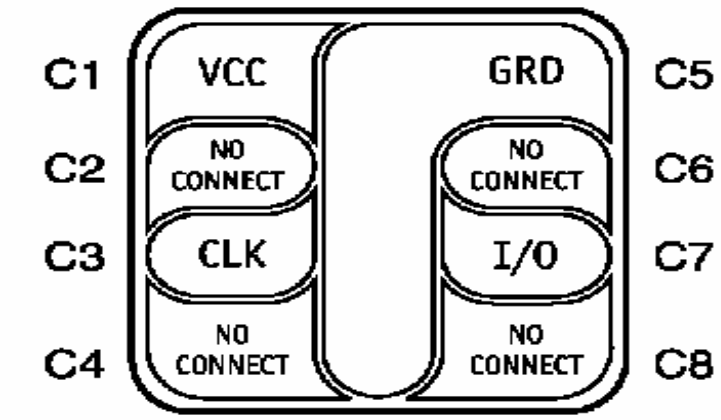
Velkou nevýhodou je nutnost umístění snímače tak, aby byl dobře a volně přístupný pro vložení karty a tedy je i volně přístupný také vandalům. Rovněž samotný fakt, že při každém průchodu či příjezdu musíme vytahovat kartu a protahovat ji snímačem, není příjemný. Automatická identifikace (např. sklady, automatické parkoviště, automatická identifikace osob) je v tomto systému značně ztížená a i samotná spolehlivost čtení bývá velmi často nízká - například v hotelích vybavených pokojovými zámky na principu magnetických karet je běžné, že pokoj otevíráme třeba i na deset pokusů.

Z důvodu postupného přechodu ze systému magnetických karet na systém modernějších kontaktních či bezkontaktních karet čipových je dnes možné využít i tzv. karet hybridních, které představují čipové karty v kombinaci s magnetickým pruhem (LoCo nebo HiCo). Tyto druhy karet jsou již v současné době standardizovány.

Kontaktní čipový identifikační systém

Čipové identifikační systémy ať již ve své kontaktní či (jak bude podrobně uvedeno v následující kapitole) bezkontaktní podobě, platí za dnes prakticky nejpoužívanější standard pro ověřovaní autenticity osob, dat a transakcí.

Aplikace čipových karet zahrnuje jejich nejčastější použití jako úvěrové nebo **ATM** (***Automated Teller Machine)*** bankovní karty, **SIM** ***(Subscriber Identity Module)*** karty pro mobilní telefony, autorizační moduly pro placenou televizi či média pro ověření elektronického podpisu. Díky použitým kryptografickým algoritmům dnes zajišťují čipové identifikační systémy vysokou míru bezpečnosti a je prakticky nemožné je padělat.



Obr. 8. *Struktura čipu v kontaktní identifikační kartě*

Kontaktní čipová karta má kontaktní plošku s osmi kontakty, jejichž funkce a umístění na čipové kartě je standardizováno normou ISO/IEC 7816-2. Jednotlivé kontakty slouží pro napájení čipu, sériovou komunikaci, přivedení externího taktovacího signálu a programovacího napětí. Důležité rozšíření komunikačních možností čipové karty specifikuje relativně nový standard ISO/IEC 7816-12, na jehož základě jsou již dnes vyráběny karty integrující USB rozhraní přímo na čipu, označované USB-ICC. Jejich hlavní výhodou je možnost eliminace čtečky čipových karet, která je nahrazena standardním USB rozhraním počítače, ke kterému je připojen kontaktní adaptér obsahující čipovou kartu v SIM formátu.

Ochrana dat před neoprávněným přístupem je řešitelná pomocí různých opatření, mezi nejsilnější patří správně implementovaná kryptografická ochrana. Potřebné hlavní klíče jsou generovány a uloženy v bezpečném systému pro správu klíčů a následně importovány na čipovou kartu pro rutinní použití. Čipová karta a programové vybavení umožňují bezpečně šifrovat a dešifrovat pracovní šifrovací klíče, které jsou následně využity k vlastnímu šifrování nebo dešifrování dat. Při poruše nebo ztrátě karty je možné hlavní klíče importovat na náhradní kartu.

Důležitou kryptografickou operací je také vytvoření zaručeného elektronického podpisu, který umožňuje autentizovat např. dokumenty a transakce, ověřit jejich integritu a zaručit nepopiratelnost podepisující osoby. Na rozdíl od operací identifikace nebo autentizace osoby, které mají víceméně jednorázový charakter, je platnost elektronického podpisu permanentní. Tím naléhavější je potřeba využití bezpečného zařízení pro vytvoření (ale i ověření) elektronického podpisu. Čipová karta s podporou asymetrické kryptografie umožňuje vygenerovat potřebné kryptografické klíče přímo na čipu a využít privátní klíč pro vytvoření elektronického podpisu, samozřejmě pouze po úspěšné verifikaci podepisující osoby. Podepisující osoba má jistotu, že bez jejího vědomí (tedy bez držení karty a současně znalosti kódu PIN) není možné např. na daný dokument elektronický podpis vytvořit.

Zkušenosti z praktického nasazení ukazují, že optimální volbou pro bezpečnost systémů i pohodlí uživatelů je kombinované využití čipové karty pro více podnikových systémů a aplikací. Čipová karta může být běžně osazena jedním nebo dvěma čipy se dvěma, nebo dokonce i třemi rozhraními (kontaktní ISO sériové, USB, bezkontaktní RF). Tato kombinace umožňuje použít jednu kartu pro fyzický i logický přístup, elektronický podpis i šifrování. Karta se tak stává „generálním klíčem“, který doslova i obrazně otevírá přístup k prostředkům a informacím podniku, úřadu i jiné organizace. [11]

3.4 Bezkontaktní čipové rádiové systémy – RFID

RFID ***(Radio Frequency IDentification)*** – je moderní technologie identifikace objektů pomocí radiofrekvenčních vln. Tento systém lze úspěšně nasadit v mnoha odvětvích a oblastech, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos těchto načtených dat k následnému zpracování.

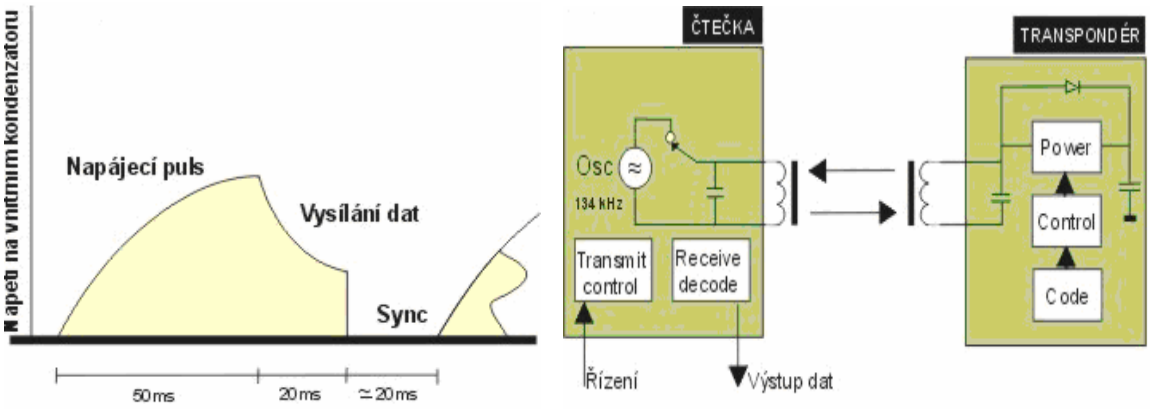
Informace jsou v elektronické podobě ukládány do malých čipů-tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln. Toto zpracování se však neděje po jednotlivých čteních jako např. u čárových kódů, ale hromadně. Současná čtecí zařízení dokážou najednou načíst až několik set tagů za minutu.

S myšlenkou na vznik bezdrátové technologie zpracování informací přišla před lety největší maloobchodní firma WalMart, která rovněž před několika desetiletími stála u zrodu čárového kódu. Základem byla myšlenka vyvinout takovou technologii, která dokáže objekt identifikovat na větší vzdálenost, bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více objektů současně. V současné době se technologie RFID velice rozvíjí a dochází k nasazení v mnoha dalších oblastech trhu, největší uplatnění nachází v logistice, výrobě, sledování objektů - logistických jednotek (zboží, palet, kontejnerů), sledování majetku, sledování zavazadel na letištích a evidence osob.

Princip RFID identifikace

Rádiové systémy automatické identifikace jsou založeny na principu přenosu dat elektromagnetickými vlnami mezi nosičem snímačem (čtečkou) a pohyblivým objektem (ID karta, automobil, palety ve skladu atd.). Objekt musí být vybaven takzvaným transpondérem (RFID tag), což je elektronický obvod, který obsahuje přijímací/vysílací anténu, nabíjecí kondenzátor, paměť a nepotřebuje napájení z baterie.

V zásadě celý systém pracuje jako dvouanténní, kdy jedna je v transpondéru a druhá je připojena ke snímači. Transpondéry mohou být v různého provedení - většinou podle charakteru aplikace (např. klasické karty, skleněné tyčinky, plastové disky, válce atd...) [2]



Obr. 9. *Princip činnosti rádiového identifikačního systému*

Čtečka vysílá výkonový impuls o délce asi 50ms. Jakmile se v dosahu antény objeví transpondér, vysílací impuls čtečky je přijat anténou transpondéru, která je naladěna na stejnou frekvenci jako čtečka. Přijatá energie vysílacího pulsu je v transpondéru usměrněna a vzniklým napětím se nabije interní kondenzátor. K napájení transpondéru během jeho zpětného vysílání slouží právě toto napětí indukované na vnitřním kondenzátoru.

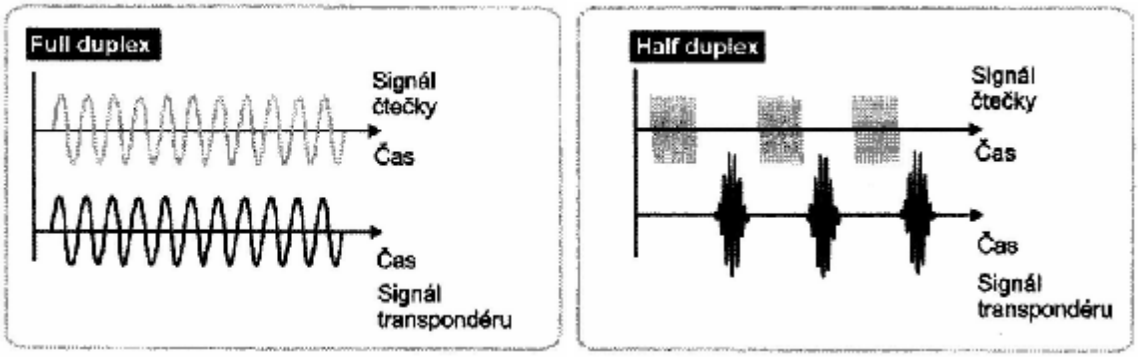
Po ukončení vysílacího pulsu čtečky se přes anténu transpondéru okamžitě vyšlou data z paměti čipu zpět k přijímací části čtecího zařízení. Délka přenášených dat je 128 bitů včetně zabezpečovacího kódu a přenos trvá 20 ms. Tato data jsou následně zachycena anténou čtečky a dekódována. Poté je nabíjecí kondenzátor transpondéru vybit a očekává se další nabití a čtení. Perioda mezi dvěma cykly (znovunačtení tagů) je mezi 20 ms až 50 ms a je závislá na nastavení snímače.

Velkou výhodou při použití této technologie je možnost plně automatické identifikace – transpondéry mohou být na snímaném objektu umístěny prakticky kdekoliv, snímač je dovede identifikovat (podle provedení) i na několik metrů.

Přenos dat

Přenos dat z transpondéru se provádí těmito způsoby:

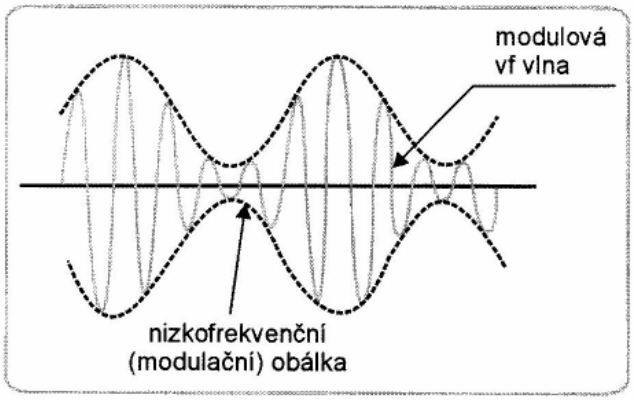
- **FDX (full duplex)** – data i energie se přenáší současně
- **HFX (half duplex)** – střídá se přenos dat s přenosem energie



Obr. 10. *Možné způsoby přenosu dat u RFID systémů*

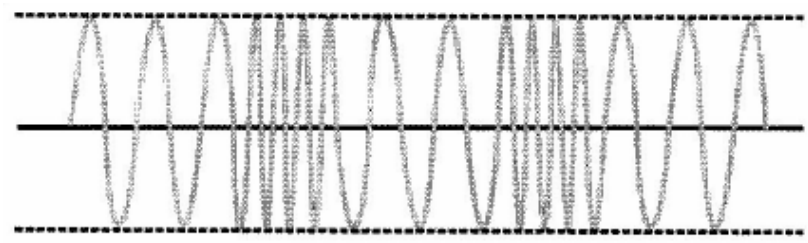
Přenos dat může probíhat rovněž dvěma způsoby **modulace**, a to amplitudovou **ASK** ***(Amplitude Shift Keying)*** nebo frekvenční **FSK** ***(Frequency Shift Keying)***.

Rozšířenější modulace je amplitudová z důvodu jednoduššího principu modulace, kdy základní vlně, tzv. nosné, měníme amplitudu signálu v rytmu přenášené informace.



Obr. 11. *Amplitudová modulace RFID signálu*

Frekvenční modulace přenáší informaci změnou frekvence nosné vlny. Změnu kmitočtu provádí tzv. rezonanční obvod, který je součástí elektroniky transpondéru. Tento přenos informací je náročnější, ale podstatně odolnější vůči rušivým vlivům.



Obr. 12. *Frekvenční modulace RFID signálu*

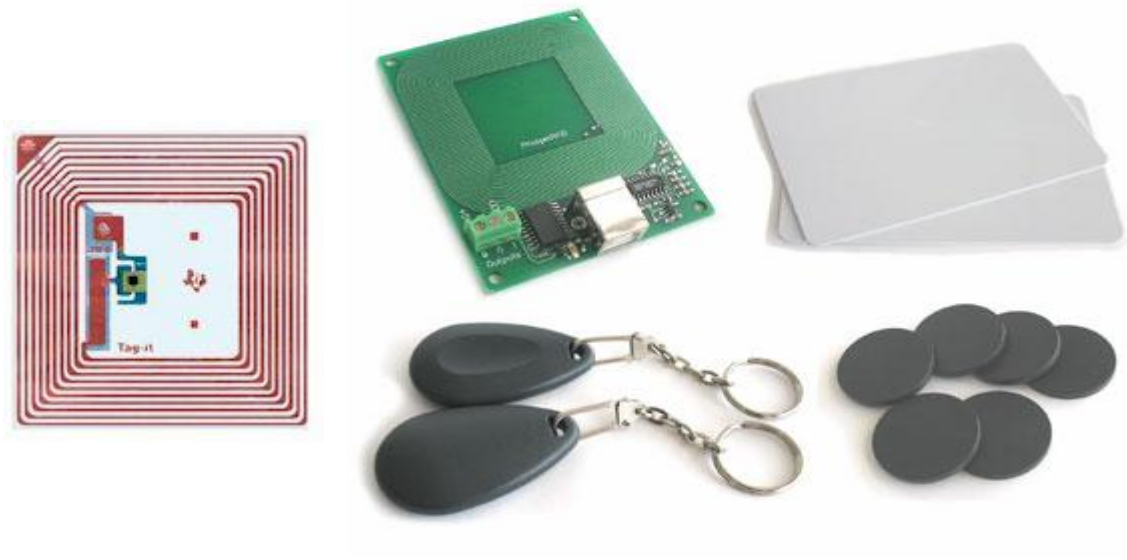
Používané standardy

Celosvětově nejrozšířenější RFID technologie je nízkofrekvenční (LF), označována jako **RFID 125 (134,2) kHz**, která nabízí čtecí vzdálenost okolo 15cm (a velmi často ji najdeme v použití pro přístupové a docházkové systémy). Zajímavé u této varianty je i to, že 134,2 kHz frekvence je vyhrazena pro identifikaci zvířat.

RFID 13,56MHz vysokofrekvenční systémy jsou určeny také pro kontrolu vstupu, logistiku, balíkovou přepravu apod. Navíc nabízí vyšší přenosovou rychlost informací a vyšší bezpečnost, ale bohužel také kratší čtecí vzdálenost (a vyžadují dražší vybavení). Nejčastěji toto provedení najdeme u elektronických peněženek, jízdenek a vstupenek. Používá se i pro identifikaci předmětů. Právě toto provedení (označované jako ISO 15693) by mělo být nejrozšířenějším typem v budoucnosti. V aktivním provedení umožňuje i metrové čtecí vzdálenosti a díky antikoliznímu vybavení umožňuje „hromadné“ čtení.

RFID 5,8GHz (ale i 2.4Ghz) je zajímavá technologie hlavně ve spojení s **aktivními** transpondéry, které mají vlastní zdroj energie, díky čemuž se čtecí vzdálenost zvyšuje až na deset metrů (a některá provedení zvládají i desetinásobek). A tomu odpovídá i využití – identifikace vozidel, kontejnerů a pohybujících se předmětů.

Čím vyšší frekvence, tím pochopitelně vyšší rychlost přenosu informace a nižší vzdálenost ve které je schopná čtečka číst identifikátor, což je problém odstranitelný jedině s použitím aktivních identifikátorů, tedy těch s vlastním napájením.



Obr. 13. *Nejčastější provedení pasivních RFID identifikátorů – tagů*

Vlastní předmět – identifikátor (transpondér) v případě RFID systémů zpravidla slouží pouze jako zdroj poskytující identifikační kód **EPC** (**E**lectronic **P**rodukt **C**ode)**,** s pomocí kterého dojde k vazbě informací v počítači s informacemi na transpondéru.

Co se týče funkce, existují typy určené pouze pro čtení uloženého kódu (R/O transpondéry), stejně jako typy s možností naprogramování kódu vlastního o délce 64 bitů do interní EEPROM (R/W transpondéry).

R/O transpondéry jsou užívány jako jedinečné a nekopírovatelné. Každý takovýto transpondér obsahuje unikátní kód, neexistují tedy dva stejné transpondéry. Tyto prvky jsou široce použitelné ve všech aplikacích zabývajících se velkými databázemi s nezáměnnými položkami. Jsou však určeny pouze ke čtení a data na nich uložená dále není možné měnit.

R/W transpondéry jsou určeny mimo jiné pro ukládání dat, nebo pro uživatelsky definovatelné identifikační kódování. Mohou být programovány, čteny a tisíckrát měněny. Programování se děje rovněž bezkontaktně, pouze elektromagnetickým polem vytvářeným snímačem. Uživatel si tak může sám tvořit kódy ke snadné integraci s jeho počítačovým systémem zpracování dat. Nebo například při aplikacích ve výrobním procesu lze do R/W transpondérů zapisovat výsledky operací během zpracování výrobku

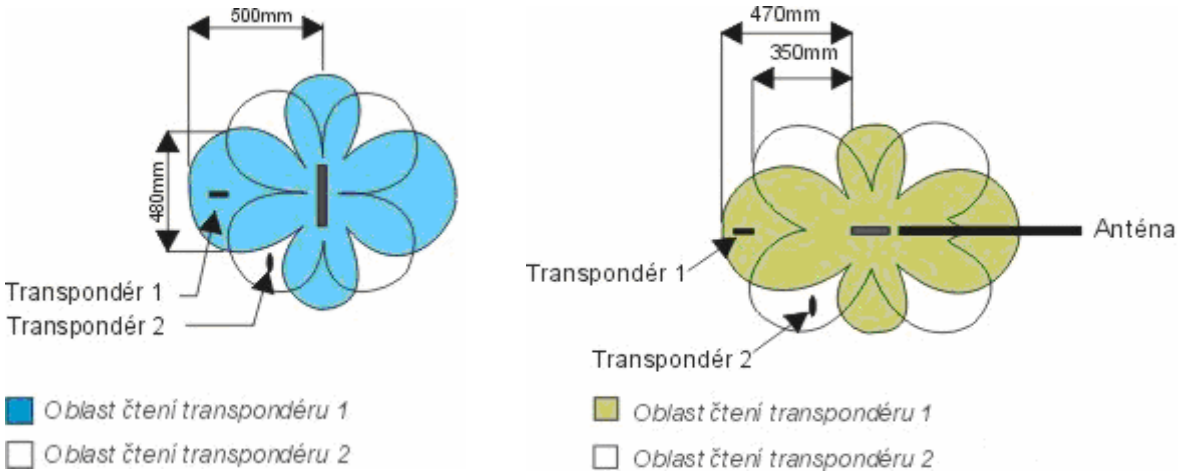
Čtecí vzdálenost

Velká čtecí vzdálenost při zachování vysoké spolehlivosti čtení je jednou z velkých výhod RFID identifikačních systémů. Čtecí vzdálenost je závislá na mnoha kritériích: typu transpondéru, elektromagnetickém rušení, orientaci transpondéru a typu antény. Obecně, standardní skleněný transpondér s výkonnou čtečkou a velkou anténou lze číst do vzdálenosti asi 1m – viz obr. 3 a 4.

Větší transpondéry lze číst asi do dvou metrů. Malá čtečka (handheld) dovede číst na vzdálenosti kratší, typicky asi 0.2m pro skleněný transpondér.

Orientace transpondéru

Orientace transpondéru vzhledem k anténě je také velmi významná. Nevhodná orientace nepatřičným natočením způsobí zkrácení čtecí vzdálenosti – viz (obr. 14.).



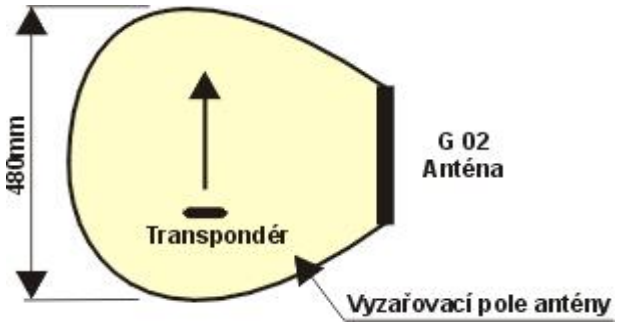
Obr. 14. *Čtecí oblasti transpondéru v závislosti na jeho orientaci*

Nejpoužívanějším prvkem v oblasti zabezpečení přenosu dat je 16 bitový CRC algoritmus (CRC-CCITT), který zajišťuje, že budou přenášena jen platná data. V případech, kdy intenzita elektromagnetického pole není dost silná ke spolehlivému přenesení dat, čtečka automaticky odpovídá řídicímu počítači příznaky NO READ nebo INVALID.

Rychlost pohybu transpondéru

Mnoho dnešních aplikací v praxi vyžaduje, aby byl transpondér přečten za pohybu. Jelikož čtecí cyklus při standardním nastavení je asi 120ms, musí se transpondér nacházet ve čtecím poli antény alespoň po tuto dobu. Jelikož tvar čtecího pole antény je proměnlivý, nelze obecně stanovit, jak rychle se může transpondér pohybovat.

Typicky lze říci, že 32 mm skleněný transpondér se může pohybovat rychlostí asi 3m/s je-li dostatečně blízko antény – viz obr. 15.



Obr. 15. *Efektivita čtení transpondéru za pohybu*

Je několik způsobů, jak přizpůsobit standardní konfiguraci vyšším rychlostem pohybu transpondéru. Jedním z nich je zkrácení nabíjecího času transpondéru, jiný předpokládá rozdělení jedné antény do dvou, vysílací a přijímací. Z praxe lze říci, že při velké anténě bylo dosaženo rychlosti pohybu transpondéru asi 65 m/s - tj. 240 km/h.

Jako ve většině systémů založených na FM modulaci, bude čten transpondér se silnějším signálem. Tak, jak se budou transpondéry pohybovat, bude se měnit jejich priorita.

Například: budou-li se dva transpondéry vzdálené od sebe 10 cm pohybovat ve čtecím poli antény, bude čten napřed první transpondér a poté druhý, jakmile se přiblíží více k anténě než prvý. Budou-li dva transpondéry ve stejné vzdálenosti vůči anténě a budou-li stejně orientovány, nebude načten žádný. Tak jak se bude rozdíl mezi nimi zvětšovat, tak bude růst i schopnost systému správně rozlišit jeden z nich. Typický případ - standardní 32 mm transpondér bude správně čten, bude-li jeho vzdálenost od druhého asi 50 mm.

Umístění snímače

Může být libovolné, třeba i za stěnou nebo v ní. Může být umístěn dokonce i zcela mimo identifikační místo, kde bude namontována pouze anténa. Takto lze snímač bezpečně ochránit před vandaly. Při průchodu osob pak při vhodně umístěné anténě a transpondéru není třeba vůbec kartu vytahovat a přesto k identifikaci dojde – tzv. FREEHAND systém. Velkou výhodou je tedy možnost plně automatické identifikace – transpondéry mohou být na snímaném objektu umístěny skoro kdekoliv, snímač je dovede identifikovat (podle provedení) i na několik metrů.

3.5 Srovnání nejpoužívanějších systémů s příklady praktické aplikace

Ze všech v současné době používaných systémů automatické identifikace se z hlediska efektivity, tedy v praxi jednoduchosti, spolehlivosti a rychlosti nejvíce využívají systémy optického čtení čárových kódů a rádiových identifikačních systémů.

Od kdysi velmi propagovaného systému magnetických karet, se již v dnešní době pomalu upouští, OCR je zase pro potřeby efektivní identifikace technologie pomalá a drahá proto jsem pro další analýzu zvolil pouze systémy čárového kódu a RFID. [8]

Optická vs. rádiová identifikace

Před několika desetiletími si evidenci zboží pomocí čárových kódu nedokázal nikdo ani představit a přesto je to dnes již naprosto běžná technologie, která se využívá i v mnoha dalších oblastech než kam byla původně určena.

RFID tagy mají oproti štítkům s čárovým kódem několik zásadních výhod. Štítek s čárovým kódem musí být umístěn na viditelném místě pro čtecí zařízení a tím je zároveň vystaven vlivům poškození – odtržení, zašpinění, teplotní a povětrností vlivy atd. RFID tag však lze umístit do značeného objektu tak, aby nebyl těmto vlivům vystaven přímo, čímž může být několikanásobně odolnější než štítek s čárovým kódem. Mnoho výrobců v současné době již umísťuje RFID tagy do svých výrobků, palet či kontejnerů již přímo ve výrobě a mnoho dalších firem se na toto připravuje.

Největší výhody RFID tagů jsou však tyto dvě. Za prvé je to možnost pomocí čtecího zařízení načíst najednou velké množství tagů na větší vzdálenost (např. průjezd paletového vozíku čtecím portálem v reálném čase). V případě štítků s čárovým kódem se musí načíst postupně čárové kódy ze všech výrobků na paletovém vozíku. Za druhé je to možnost zápisu či změny informací přímo do RFID tagu.

Čárový kód je i přesto v současnosti nejrozšířenějším a nejvíce standardizovaným způsobem průmyslové identifikace, u kterých jde o malé objemy dat (např. číslo zboží) na levných etiketách při poměrně rychlém čtení levnými skenery (oproti kamerám pro OCR).

Technika RFID není zatím ani tak rozšířená (i když se roční přírůstky pohybují kolem 20 %) ani celosvětově standardizovaná jako čárový kód. Princip RFID však má však nebývalý inovační potenciál, neboť umožňuje zcela nové přístupy k zaznamenávání a přenosu dat. Významným kritériem pro volbu metody identifikace je také vliv okolí. Kovy nacházející se v oblasti elektromagnetického pole systému RFID mají zpravidla utlumující účinek, a tedy záporný vliv na stávající elektromagnetické pole (indukce vířivých proudů). Na druhé straně však mohou být kovy použity jako reflektory pole, a mají tak kladný vliv. Jinak však není provoz systémů RFID téměř vůbec ovlivňován vnějšími podmínkami, jako jsou špína, vlhkost, teplota, nárazy nebo poškrábání povrchu.

Oproti etiketám s čárovými kódy mají transpondéry dlouhou životnost – u aktivních transpondérů až deset let nebo až jeden milion čtecích a zaznamenávacích cyklů.

Cena RFID transpondéru je však oproti nosičům optických kódů mnohem vyšší, což je možná také jeden z důvodů, proč ještě nedošlo k tak masovému rozšíření. Zlevnění se dá očekávat vlivem dalšího technologického vývoje a zavedením velkosériové výroby. Cílem je, aby pasivní transpondér stál v přepočtu asi 6 Kč. Cena čtečky (případně kombinované se zaznamenávacím zařízením) závisí na použitých anténách, potřebném výkonu, přenosových kmitočtech a použité inteligenci přístroje. Jednoduché příruční přístroje mají cenu srovnatelnou s dnešními čtečkami čárového kódu.

Technologie RFID je v současné době považována za přímého nástupce čárových kódů, z hlediska budoucího vývoje se však nepředpokládá úplné nahrazení čárových kódů, zato sílí nárůst praktických aplikací využívajících nejčastěji právě technologie rádiové identifikace. S některými druhy identifikačních systémů, které dnes v praxi běžně fungují, vás nyní v dalších podkapitolách seznámím.

3.5.1 Elektronické zámkové systémy

Jak již je z názvu zřejmé, jedná se o systémy ochrany vstupu zamezující přístupu do střeženého objektu. V praxi se proto často setkáváme také s označením – **přístupový systém**. Protože se jedná o bezpečnostní aplikaci, je problematika praktického použití takového přístupového systému přesně definovaná normou ČSN EN 50 133 Poplachové systémy – Systémy kontroly vstupů, na základě čehož pak každý takový systém musí obsahovat prvky místa přístupu, vyhodnocovací a řídící jednotky, programovací zařízení, ovládací prvky a zdroj napájení. [5]

Tato norma také řeší různé stupně zabezpečení systému, a to na základě:

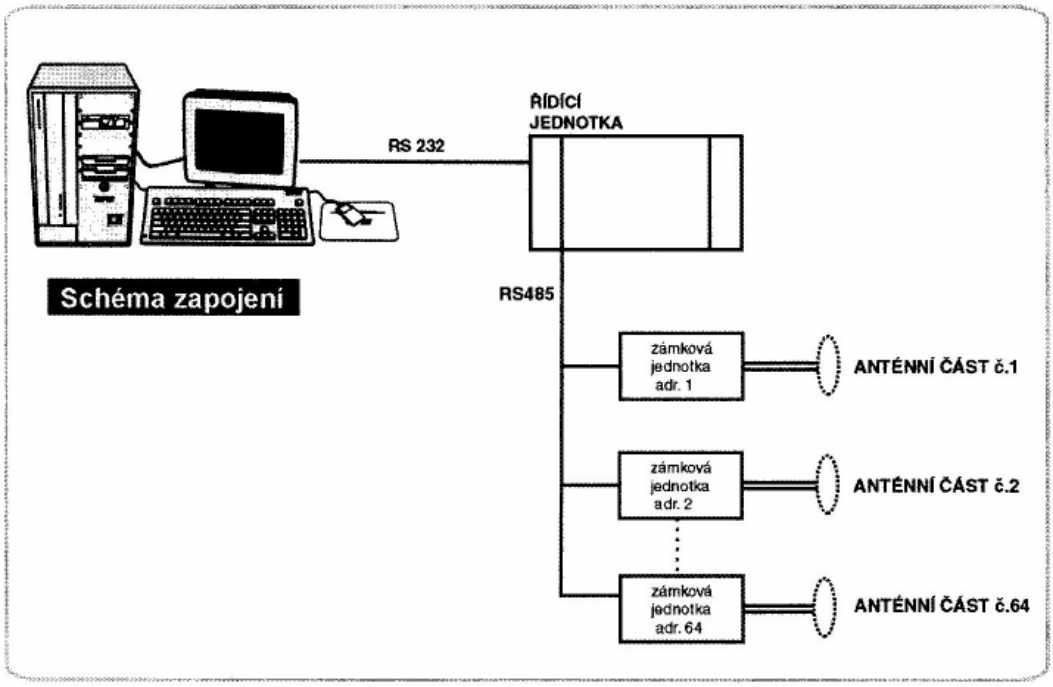
- **identifikace**, která stanovuje její kvalitu podle 4 tříd:
  - **třída 0** – bez přímé identifikace (tlačítko)
  - **třída 1** – identifikace je uložena v paměti (heslo)
  - **třída 2** – podle identifikačního prvku (karta, otisk prstu)
  - **třída 3** – kombinace identifikačního prvku a informace v paměti
- **přístupu**, který je rozdělen do dvou tříd:
  - **třída přístupu A** – nevyžaduje časový filtr ani ukládání dat
  - **třída přístupu B** – vyžaduje časový filtr a ukládání dat

Elektronické dveřní zámky jsou dnes v praxi nejpoužívanějším zajištěním proti neoprávněnému přístupu. Jsou to samostatné jednotky řízené mikropočítačem, které jsou zavěšeny přímo na dveřích a díky vlastnímu napájení nepotřebují žádné propojení s okolím.

Zámky jsou osazeny snímači čipových či magnetických karet někdy i v kombinaci s biometrickými čtečkami, které společně nahrazují klasické mechanické zámky. Odemykají se buď protažením karty snímačem dveřního zámku, využitím biometrického identifikátoru nebo bezkontaktně pomocí RFID čipu. Mikropočítač zámku čte údaje z použitého identifikačního prostředku a vyhodnocuje, zda se jedná o platný identifikátor nebo nikoli. V případě, že z přečtených dat porovnáním se svojí databází rozkóduje, že se jedná o platnou kartu, vydá pokyn k odblokování mechanického zámku dveří a vstupující má možnost stiskem kliky pokoj otevřít.

V paměti zámku se uchovávají informace o přístupových operacích, které s ním byly prováděny. Oprávněný pracovník může tedy kdykoli zjistit kdo a kdy zámek otevřel, nebo se o to pokoušel a sice s minutovou přesností. Standardně jsou v nabídce dveřních zámků mechanické zadlabací zámky s funkcí ANTIPANIC, která umožňuje zevnitř dveře kdykoli otevřít pouhým stiskem kliky, tedy i v případě, kdy je zámek uzamčen závorou. Uživatel tedy není ani v případě paniky vystaven stresu z odemykání zámku. Funkce AUTOMATIC DEADBOLT představuje revoluci v bezpečnosti, neboť zajistí, že zavřené dveře pokoje jsou vždy zároveň i uzamčeny. Kdykoli se dveře zavřou, dojde automaticky k vysunutí spodní závory zámku do zárubně dveří. Běžné systémy tohoto typu lze totiž uzamknout na závoru pouze uzamčením zevnitř pokoje. Pokud např. host opouští pokoj a zavře za sebou dveře, spodní závora se nevysouvá a dveře zůstávají lidově "zabouchnuté". [18]

V praxi může přístupový systém vyšší kategorie např. rozvětvené organizace vypadat takto: všichni uživatelé jsou vybaveni identifikačním prvkem (kartou) a rozděleni do skupin. Ty jsou předem definované a určují povolení přístupu na jednotlivá místa. Lze definovat přístup neomezený, zakázaný nebo ohraničený určitým časovým pásmem.Veškeré průchody osob sledovanými místy jsou evidovány, ukládány a připraveny pro následnou analýzu. Veškeré údaje o uživatelích jsou uloženy v centrální databázi a přístup k nim má pouze oprávněná osoba. Celý systém sledování přístupu osob pak může být dále doplněn i dalšími nadstavbovými moduly jako je evidence návštěv, výdej klíčů apod.



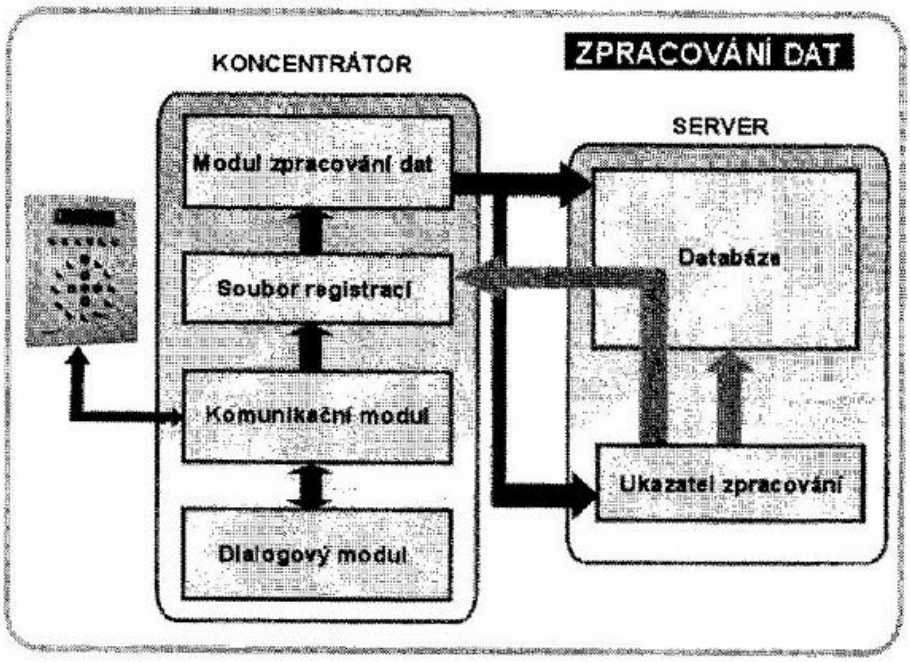
Obr. 16. *Blokové schéma přístupového systému s automatickými zámky*

3.5.2 Docházkové a evidenční systémy

Cílem těchto systémů je evidence docházky, sledování pohybu zaměstnanců během pracovní doby a vytváření podkladů pro další zpracování (např. výpočet mezd apod.).

Efekt těchto identifikací spočívá ve zvýšení komfortu uživatelů jak při registraci tak i při prohlížení vlastních údajů, úspoře administrativních sil a bezproblémové archivaci dat pro vlastní i kontrolní účely. Základní údaje (příchod, odchod) jsou snímány pomocí docházkových terminálů a každému zaměstnanci je přiděleno identifikační médium (karta, přívěsek apod.), pomocí kterého provádí registraci v zaměstnání při příchodu či odchodu.

Při zavádění docházkového systému je nutné definovat strukturu organizace od nejnižšího článku – zaměstnance až k managementu, podle čehož pak jednotlivé zaměstnance rozdělíme do skupin, kterým nastavíme patřičná oprávnění, která v závislosti na dané organizační struktuře určí, zda je možné např. zobrazit data všech zaměstnanců nebo jen vybrané skupiny (mistr může zasahovat jen do dat pracovníků své dílny, k ostatním nemá přístup). Model pracovní doby se může konkretizovat podle typu (volný, pružný nebo pevný), cyklu (pravidelný, nepravidelný, náhodný) a denního úvazku. V další konfiguraci je možné zvolit např. zaokrouhlování odpracované doby, započítávání přestávky, tolerance pozdního příchodu, interval doby přesunu na pracoviště, přesčasy apod.



Obr. 17. *Blokové schéma docházkového systému*

Všechna data, která byla vložena do docházkového systému automaticky (na terminálu) nebo manuálně (oprávněným pracovníkem), se zpracovávají a mohou se zobrazit u zaměstnance jako docházkový list. Ten obsahuje za daný měsíc součtové řádky jednotlivých dní s udáním všech sledovaných parametrů. Takto nashromážděná data lze samozřejmě převést do tiskové podoby, která v konečné fázi může posloužit jako podklad pro mzdový program organizace, kde následně dojde k přepočtu odpracovaných hodin a ostatních dat do finální podoby v korunách.

Pro účely docházkových a přístupových systémů se nejčastěji využívají bezkontaktní čipové karty pro svoji neomezenou životnost (uváděná jako parametr). Z hlediska použitého čipu se však jedná pouze o kartu paměťovou, eventuálně s jednoduchou paměťovou ochranou (pro tyto účely postačující).

3.5.3 UHF / mikrovlnné identifikační systémy

Samostatnou a početně mnohem méně zastoupenou kategorií bezkontaktních identifikačních řešení jsou systémy pracující na **UHF** ***(Ultra High Frequecy)*** nebo systémy mikrovlnné s frekvencemi řádově stovek MHz až jednotek GHz. Využití v praxi nacházejí především u identifikace vozidel, kde je čtecí vzdálenost jedním z nejdůležitějších kriterií.

S těmito prostředky dnes není problém dosahovat s vysokou spolehlivostí čtecích vzdáleností i několik desítek metrů. Zde je ale nutné si uvědomit, že čtecí vzdálenost nemusí vždy nutně znamenat jen přínos. V úvahu je třeba brát také např. možnost nechtěného načtení transpondéru na vozidle, které třeba jen projíždí v blízkosti snímacího zařízení, ale nepožaduje provedení své identifikace nebo naopak faktické nenačtení transpondéru např. v případě v praxi často používaných mýtných bran, kdy druhé vozidlo jedoucí těsně za kamionem nemusí být čtecím zařízením správně vyhodnoceno.

Aplikace takovýchto systémů by proto měly vyžadovat uživatelsky nastavitelnou maximální čtecí vzdálenost podle podmínek konkrétní instalace, anebo transpondéry aktivované uživatelem (např. tlačítkem) při požadavku na identifikaci.

V této oblasti se lze také mnohem častěji než u dříve zmiňovaných technologií setkat s tzv. aktivními transpondéry, tedy identifikátory používajícími pro svůj vlastní provoz vnitřní napájecí baterie. Právě to umožňuje dosáhnout mnohem větší čtecí vzdálenosti než s transpondéry pasivními, na druhou stranu mají baterie použité v aktivních identifikátorech omezenou životnost, a je tak třeba se zamýšlet i nad otázkou jejich periodické výměny a nákladů s tím spojených.

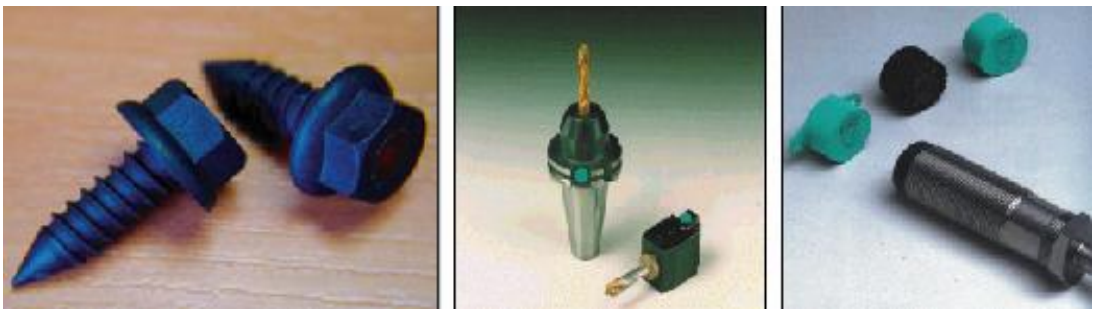
Další důležitou záležitostí u těchto systémů je vhodnost, v některých případech až dokonce nutnost, aby použitá technologie nabízela i tzv. antikolizní mechanismy při detekci většího počtu transpondérů přítomných najednou ve čtecím poli snímače, protože tento stav může v praxi velmi snadno nastat. Nicméně většina v současné době nabízených technologií v této oblasti, obdobně jako je tomu u řady čteček pracujících dle norem ISO 14443 a ISO 15693, už tyto vlastnosti má. [3]

3.5.4 Sledování výrobních procesů

Prudký rozvoj automatizace v průmyslové výrobě je následován neméně prudkým rozvojem automatizace v dopravě a logistice. Zde vyvstává zásadní problém jednoznačně a spolehlivě identifikovat dopravovaný a sledovaný materiál. Výhody automatické identifikace jsou dobře patrné např. při manipulaci se zbožím v obchodě. V současné době si už asi nikdo nedovede představit supermarket bez pokladen se snímači čárového kódu, které stále platí za nejpoužívanější možnost evidence a sledování pohybu zboží.

Na identifikační systém použitý v průmyslovém prostředí jsou ovšem kladeny vyšší nároky. Systém nesmí být ovlivněn znečištěním, nosič kódu musí být odolný proti poškození, identifikace musí být možná i při vzájemném pohybu nosiče kódu a snímacího zařízení. Těmto požadavkům v praktickém průmyslovém nasazení opět nejlépe vyhovují vlastnosti RFID rádiové identifikace.

Elektromagnetický princip má totiž v tomto případě oproti ostatním podstatnou výhodu. Dovoluje přenos informace oběma směry – od nosiče kódu ke čtecímu zařízení i naopak. Lze tedy nosič kódu změnit v nosič dat a libovolně měnit jeho obsah. Jednoznačná identifikace je zabezpečena i při zcela volném pohybu výrobku a použité transpondéry rovněž mohou mít pro účely průmyslového nasazení nejrůznější tvary (šrouby, pečeti, zátky) případně mohou být integrovány přímo v některém s výrobních nástrojů, kde jednoznačná identifikace umožňuje přiřadit každému nástroji položku databáze, ve které jsou uchovány potřebné informace, např. datum zavedení nástroje, provozních hodiny, údržba, ostření atd.



Obr. 18. *Možné provedení průmyslových transpondérů*

Typickou aplikací je také sledování výrobku na montážní lince. Veškeré operace s výrobkem jsou automaticky dokumentovány, což má význam v systémech řízení jakosti výroby. Aplikace, využívající elektromagnetický identifikační systém IDENT-M, bývají také instalovány např. na linkách finální montáže automobilů. V nosiči dat jsou uloženy údaje, které tvoří doprovodnou dokumentaci automobilu. Automatická identifikace umožňuje okamžité nastavení stanoviště linky pro plánované výrobní operace.

Identifikační systémy mohou mít v průmyslu ještě mnoho dalších uplatnění. Zajímavé jsou např. aplikace při dopravě tekutin, kde identifikace nasazení správné hadice (nosič kódu je v přírubě) zajišťuje, že tekutina skutečně poteče tam, kam má.

3.5.5 Parkovací systémy

Parkovací systém je speciálním případem přístupového systému, u něhož se při vlastní realizaci vyskytují dva v praxi největší problémy. Rychlost a spolehlivost.

Většina současných parkovacích systémů je pomalá a nespolehlivá. Řidiči musí nejprve někdy složitě manévrovat před čtečkou karet aby se dostali co nejblíže, pak musí zastavit, otevřít okno a vložit někam nebo alespoň přiložit ke snímači svou přístupovou kartu. A co bývá horší, spousta řidičů svou kartu nemůže ihned najít a tak se tvoří řady čekajících nespokojených zákazníků. Vynásobíme-li tento problém u větších parkovišť stokrát, vznikají dopravní zácpy a komunikační problémy.

Také servis u těchto systémů nebývá levný ani jednoduchý, zato však bývá častý. Například u systémů založených na kontaktních kartách (nebo paměťových kontaktních systémech), magnetických snímačích nebo optických čtečkách je třeba časté čištění čteček, a to tím častěji, v čím špinavějším prostředí pracují.

Použití RFID technologií se logicky nabízí jako jedno z možných řešení eliminace těchto problémů. V tomto případě je tedy každý automobil, který má na parkoviště přístup, vybaven transpondérem ve tvaru disku, který se připevní přísavkou zevnitř na okno. Jakmile se automobil přiblíží k parkovacímu automatu (čtečce RFID), je signál z transpondéru zachycen, vyhodnocen a jeho jedinečný identifikační kód je poslán počítači, kde se vyhodnotí a na základě výsledku se otevře závora pro vjezd na parkoviště. Ve stejném okamžiku se provede registrace vjezdu nebo výjezdu spolu s časem pro výpočet parkovného. Tento proces trvá několik milisekund a řidič nemusí otevírat okno, ba dokonce ani zastavit. Čtecí vzdálenost pro tento diskový transpondér bez napájení je okolo 1,5 m, což je asi třikrát více než bývá pracovní dosah takzvaných "proximitních systémů". [19]

Proximitní systémy se vyznačují podobnou funkcí co se týče bezkontaktní "handfree" činnosti, ale dosah bývá jen asi 30 cm. To znamená, že v těchto případech musí řidič stejně zastavit, otevřít okno a proximitní kartu přiblížit do pracovního dosahu čtečky. Kromě toho, že RFID systém má velkou čtecí vzdálenost, je jeho další výhoda, že anténa i čtečka nemá žádné štěrbiny a mohou být umístěny tak, že zabraňují svému poškození jak vandaly tak i povětrnostními podmínkami či kontaminacemi z okolí.

4 VYUŽITÍ BIOMETRICKÝCH IDENTIFIKAČNÍCH METOD

Moderní biometrické technologie nabízejí automatizovaný způsob zjištění nebo ověření identity žijící nebo zemřelé osoby na základě měřitelných a nezaměnitelných biometrických charakteristik. Tyto charakteristiky jsou prokazatelné, přesné a jedinečné pro každého člověka a nemohou být kopírovány ani zaměněny.

Přestože se v poslední době o biometrii hovoří převážně v souvislosti s počítačovou bezpečností, její počátky sahají hluboko do minulosti. Z literatury je například známo, že první poznatky o biometrii a používání tohoto termínu jsou odbornou veřejností. registrovány již v první polovině 19. století, avšak její jasné definování jako pojmu je spojeno až s rozvojem statistiky a biologie koncem 19. století.

Z hlediska vnitřní bezpečnosti, ochrany majetku, zdraví a života osob, představuje dnes biometrie skutečně významný fenomén v životě téměř každé země. V boji proti terorismu může sehrát jako jedno z opatření dosti podstatnou roli.

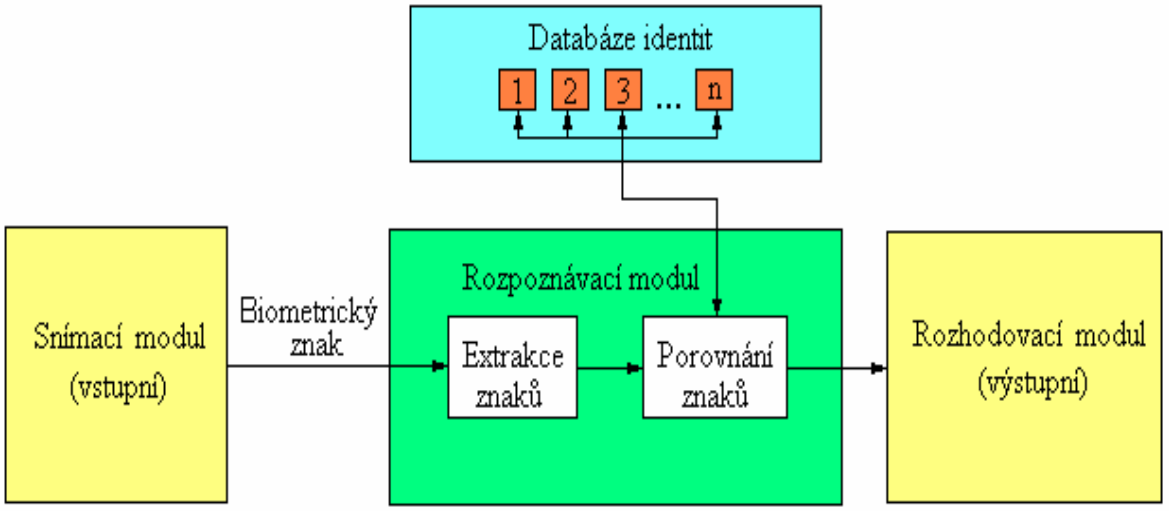
Přitom je však třeba respektovat skutečnost, že i když se pojmy biometrika, biometrie nebo biometrické systémy v kriminalistice v podstatě nevyskytují, hraje měření znaků osob i dnes v kriminalistice a především v kriminalistické identifikaci rozhodující poslání. Pokud se v souvislosti se zajištěním uvedených hodnot a svobod občanů rozhodne o zavedení a „měření“ nějakého nového biometrického znaku, nelze tak učinit bez odpovídajícího zajištění technické a metodologické vybavenosti těch policejních pracovišť, která budou takováto měření v rámci důkazní kriminalistické identifikace provádět.

4.1 Obecný princip biometrických identifikačních systémů

Jak je z předchozích odstavců zřejmé, jednotlivé biometrické identifikační metody používají rozdílná technická zařízení a pracují na odlišných principech. Přesto je možné po určitém formálním zjednodušení jejich funkcí zevšeobecnit a vytvořit obecný popis jejich identifikační podstaty a následného technologického (počítačového) zpracování.

Realizace biometrických identifikačních metod vyžaduje jednak hardware (čtecí zařízení, kamery, mikrofony, optická čidla atd.), který snímá biometrické charakteristiky a převádí je do elektronické podoby, a jednak software, který sejmutá data převádí do žádané podoby a následně provede vyhodnocení.

Předtím než bude možné ověřovat identitu na základě biometrických charakteristik, musíme nejprve sejmout šablonu zvolené charakteristiky. Tato šablona (v zahraniční literatuře často označovaná jako ***Template***) je uložena a slouží jako referenční údaj pro účely následného porovnání se vzorkem sejmutým v okamžiku identifikace. Procesu ukládání šablon se v odborné anglické literatuře říká ***Enrollment***. Šablona je potom přiřazena k identifikátoru dotyčného jedince – je-li ovšem znám. Bývá to zpravidla rodné číslo, jméno a příjmení, datum narození, počítačové přihlašovací jméno (login), PIN, číslo zdravotní nebo sociální pojistky (používané v zahraničí častěji než u nás rodné číslo).



Obr. 19. *Obecné schéma biometrického identifikačního systému*

Tento proces sejmutí a ukládání šablon je klíčovým faktorem v celém procesu a má zásadní vliv na úspěšnost aplikace biometrických metod. Slabá kvalita šablony může vést k nezdaru při budoucích pokusech o identifikaci a k nutnosti celý proces ukládání šablon opakovat. Důležitou otázkou je, kde jsou šablony ukládány. V zásadě existují tři možnosti:

- uložení šablon v samotném čtecím zařízení
- uložení šablon v centrálním archivu (např. počítačové databance)
- uložení v přenosném prvku, jako je např. čipová karta či dokonce jako paměť telefonu

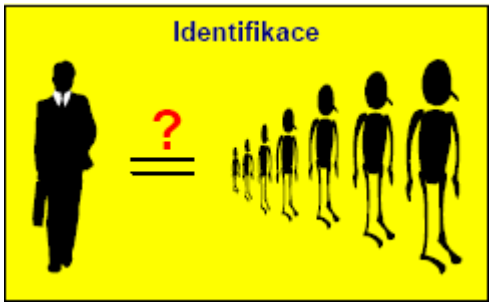
Všechny tři varianty mají své výhody a nevýhody a vhodnost jejich použití závisí na konkrétním identifikačním systému a jeho implementaci.

4.2 Vymezení pojmů verifikace a identifikace

Protože proces ověření identity může probíhat v zásadě dvojím způsobem, rozlišuje se **verifikace** a **identifikace**. V následujícím textu se pokusím objasnit čím se tyto dva (v souvislosti s identifikací poměrně zásadní pojmy) vyznačují.

Obr. 20. *Verifikace – porovnání 1:1*

Verifikace předpokládá, že **objekt (jedinec) udá svou identitu a úkolem biometrického identifikačního systému je tuto identitu potvrdit**. Objekt sám nebo obsluha biometrického snímacího zařízení zadá identifikátor dotyčného verifikovaného jedince a poté se sejme vzorek požadované biometrické charakteristiky. Systém vyhledá v archivu šablonu pro dotyčného jedince a porovná ji s aktuálně sejmutým vzorem. Při vzájemné shodnosti obou údajů je proces ověření identity (verifikace) ukončen. Tímto způsobem dnes pracuje většina technických, přístupových zařízení.



Obr. 21. *Identifikace – Porovnání 1:N*

Identifikace se od verifikace liší tím, že **identita jedince není známá a je nutné ji zjistit**. Biometrická charakteristika objektu (jedince) se sejme vhodným způsobem jako v předchozím případě, ale protože není zadán identifikátor jedince, musí se postupně prohledávat archiv šablon a porovnávat je s aktuálním sejmutým vzorem do té chvíle, než dojde ke shodě údajů obou objektů. Je zřejmé, že identifikace je mnohonásobně náročnější na výkon identifikačního systému než verifikace.

4.3 Lidské tělo vs. soukromí

Identifikační technologie podporované výpočetní technikou, se velice rychle rozvíjejí a v praxi se stále ve větší míře setkáváme s jejich aplikačním nasazením, které však často nebývá nikterak jednoduché ani přímočaré. Vznikají totiž pochopitelně obavy z možného nepochopení nebo zneužití těchto technologií, zejména z pohledu ztráty osobní svobody a soukromí, z vyzrazení či dokonce zneužití intimních (osobních) údajů atd.

V poslední době se projevuje dokonce i strach z určité potenciální diskriminace (např. genetické), pocházející z velkého množství těch nejosobnějších údajů a sahajících až do podstaty naší biologické existence. Setkáváme se s nedůvěrou či dokonce odporem ochránců lidských práv, ale také s problémy politického, společenského nebo náboženského charakteru. Podstatou nepochopení je ale zpravidla neznalost samotné věcné podstaty jednotlivých identifikačních postupů i základů daných informačních technologií, nebo jejich smysl při ochraně našich práv a svobod před pachateli závažných trestných činů, které s navíc s rozvojem vědy a techniky stále zdokonalují a je čím dál těžší je objasnit. Proto je potřeba rychle a včas odhalit (identifikovat) pachatele, dřív než stihne spáchat řadu dalších společensky závažných a nebezpečných trestných činů.

Tak např. pro identifikaci pachatele pomocí struktury deoxyribonukleové kyseliny (DNA) stačí teoreticky jediná buňka jeho těla. Pro identifikaci s využitím genetického profilu se využívá jen nepatrná část řetězce DNA, která neobsahuje žádné informace ve smyslu vlastností osoby (podoba, povaha, zdravotní stav atd.). Policejní složky v zahraničí ve svých ***komparačních metodách*** *využívají jen nezbytně nutné sekvence DNA pro samotnou identifikaci, které jsou navíc registrované pouze jako číselné či písmenné kódy jednotlivých položek a jsou tak mimo komparační databázi nepoužitelné a tedy nezneužitelné. Do komparační databáze jsou zanášeny pouze informace identifikující odsouzené zločince nebo charakterizující biologické stopy z míst neobjasněných trestných činů s cílem jejich pozdějšího využití pro objasňování nově spáchaných trestných činů.*

Ke zcela odlišnému účelu než bezprostředně orientované komparační databáze slouží tzv. ***databáze evidenční*** *(mající biologický nebo evidenční charakter), ve kterých jsou uloženy zdravotní záznamy, obsahující často důvěrné osobní údaje, někdy i včetně výsledků specializovaných genetických vyšetření. Je celkem logické, že se vyskytují obavy z možného zneužití takové evidenční databáze prozrazením registrovaných dat.* [14]

Myslím si, že v případě takto pojatých evidenčních databází (a patří mezi ně i např. personální agenda) lze s oprávněností těchto obav souhlasit. Informační obsah jednotlivých položek dává totiž smysl i mimo databázi, a jako takový je tedy zneužitelný.

Evidenční databáze DNA jsou přitom charakteristické pro zdravotnická zařízení. V policejní identifikační praxi se využívají pouze databáze komparační, s podstatně omezeným množstvím informací. Komparační databázi lze proto chápat obdobně jako např. počítačový ***systém AFIS*** *(**A**utomatic **F**ingerprint **I**nformation **S**ystem). Sekvence DNA je totiž stejnou „genetickou" paralelou jako otisk prstu, ovšem s mnohem vyšší přesností a objemem informací.* [21]

S pouhého daktyloskopického otisku palce, stejně tak jako zkrácené sekvence DNA v komparační databázi, nelze kromě jednoznačné identifikace osoby zjistit žádné další fyzické, zdravotní nebo osobnostní charakteristiky či jinak vypovídající údaje.

4.4 Praktické požadavky na biometrické identifikační metody

Stejně jako u jiných metod, tak i u biometrie je třeba před vlastním nasazením do praxe zvážit některá specifická hlediska, neboť biometrické identifikační metody se ve své podstatě od sebe odlišují jak ve funkci tak v použitém principu.

V úvahu bychom měli brát především následující parametry:

Přesnost: Dokonale přesná biometrická metoda neexistuje. U verifikačních technologií, regulující přístup k technologickým zařízením se proto zavádějí tzv. míry chybovosti:

- **FAR** ***(False Accept Rate)***, která udává pravděpodobnost, s jakou bude neoprávněný jedinec verifikován a autorizován k určitým činnostem.
- **FRR** ***(False Reject Rate)***, jež udává zase pravděpodobnost, s jakou nebude oprávněný jedinec (který by normálně měl mít přístup) verifikován a autorizován.

Obě míry mohou být ve většině metod nastaveny na požadovanou hodnotu pravděpodobnosti. Mezi uvedenými mírami neexistuje inertní vztah – jestliže jednu hodnotu snížíme, zvýší se zároveň ta druhá a naopak. V praxi pak např. čtečka otisku prstů bude buď málo citlivá a vpustí do objektu i nepovolanou osobu nebo naopak bude citlivá přespříliš a snadno může dojít k tomu, že se přes ni nedostane osoba ověřená, která např. vlivem pracovních podmínek má znečištěné nebo příliš vlhké prsty.

Rychlost: Jednotlivé biometrické metody se od sebe liší v rychlosti, s jakou mohou být načtené vzorky porovnány se šablonou umístěnou v archivu. Rychlost je nepřímo úměrná požadované přesnosti a tím složitosti šablony. Šablony pro komerční účely např. umožňují verifikaci osoby při vstupu do informačního systému, se kterým pracuje jen několik desítek lidí a ostatní mají přístup vyloučen jinými opatřeními (technickými, organizačními, administrativními – např. zamítnutí přístupu do režimového objektu s chráněnými informacemi, technologiemi apod.), mohou být mnohem jednodušší než šablony biometrických metod používané pro soudní identifikaci. Složitost šablony je dána i množstvím a vlastnostmi porovnávaných kriterií mezi vzorkem a šablonou.

Velikost šablony: Velmi důležité je, kde mají být šablony uloženy a jakou mají velikost. Bude rozdíl, jestliže máme k dispozici rozsáhlý datový sklad, nebo jestli ukládáme šablonu na čipovou kartu s poměrně nízkou kapacitou.

Cena: Je zpravidla závislá na hodnotách, které má biometrická metoda chránit, dále záleží na přesnosti a garantované spolehlivosti zařízení.

Velikost snímacích zařízení: Identifikační zařízení, a tím i provedení včetně rozměrů snímacího prvku, musí vyhovovat požadavkům a možnostem konkrétní implementace.

Dotěrnost: Různé biometrické metody identifikace požadují od identifikovaných osob různý stupeň spolupráce. Tyto osoby musí být ochotny například vložit prst nebo ruku na čtecí zařízení pro získání otisku prstů nebo geometrie dlaně, případně nechat si svítit do oka pro získání vzorku očního pozadí. V bezpečnostní praxi může být osoba donucena podrobovat se na základě různých organizačních nebo administrativních opatření identifikačnímu zkoumání, které vyplývá např.ze stupně utajovaných informací režimového pracoviště apod. Dotěrnost pak z tohoto pohledu nemusí být vždy rozhodující, protože důraz je kladen obecně na bezpečnost, která požaduje např. vysokou přesnost a spolehlivost identifikace v rámci použité technologické metody.

Režim činnosti: Důležitým hlediskem je, zda biometrické identifikační zařízení bude muset zjistit identitu jedince v archivu mnoha šablon (identifikace, též nazývaná jako porovnání *One-to-Many*) nebo jestli pouze porovná vzorek se šablonou (verifikace, též nazývaná jako porovnání *One-to-One*). Některé biometrické metody jsou vhodné pro režim verifikace, ale ne pro režim identifikace.

Provozní podmínky: Biometrické metody jsou ovlivňovány prostředím, ve kterém pracují. Vysoká vzdušná vlhkost například znemožňuje získávání kvalitního otisku prstu. Vysoká úroveň okolního hluku zase omezuje možnosti rozpoznávání hlasu, který je zahlušen a zkreslen šumem, podstatně ovlivňujícím snímanou akustickou charakteristiku.

Kulturní a náboženská omezení: Pro některé země a národy jsou některé biometrické metody nepřijatelné nebo nerealizovatelné.

Tak např. v jedné africké zemi bylo rozhodnuto vydávat humanitární podporu po živelné katastrofě. Vznikl opodstatněný požadavek jednoznačně identifikovat osobu, které již byla podpora poskytnuta, a tím zabránit vícenásobnému vydání podpory jedné a téže osobě. Vzhledem k vysoké negramotnosti nebylo možné příjem stvrzovat podpisem. Navíc neexistovala žádná evidence osob. Jako možné řešení se jevilo stvrzení převzetí státní podpory otiskem prstu a jeho následným zanesením do informačního systému (typu AFIS). Nízká kultura a vysoká korupce však způsobily, že státní úředníci umožnili otiskovat useknuté články prstů i podezřelým osobám, které je opakovaně přinášely od různých poškozených osob. Biometrickou daktyloskopickou evidenci poskytnuté humanitární podpory nebylo možné dále využívat.

Prokázání životnosti identifikovaného objektu: Především komerční využití biometrických identifikačních metod tak s sebou přináší další problém. Zejména z hlediska ochrany před násilným zneužitím biometrických metod (useknuté ruce, prsty, atd.) je třeba jasně prokázat, že identifikovaný objekt, jeho část nebo určitý charakteristický projev, na němž je biometrická identifikace založena, je opravdu v době vlastní identifikace „živý“.

Při identifikaci osob založené na daktyloskopických poznatcích se navíc může zkoumat a prokazovat např. pohyb krve v kapilárách pokožky. Komerčně využitelnou vizuální biometrickou identifikaci na základě podoby tváře, lze poměrně snadno oklamat, a tak při identifikaci je osoba navíc požádána, aby např. mrkla, udělala grimasu apod. Obecně lze konstatovat, že je nutné další doplňkové prověřování a vyhodnocování. Teprve pak je reálný závěr, že osoba byla nejen správně identifikována, ale že je i živá.

4.5 Rozbor dostupných prostředků biometrické identifikace

Mezi biometrické prostředky řadíme takové, které zjišťují totožnost uživatele na základě jeho unikátních fyzických vlastností (otisk prstu, sken oční duhovky, a podobně), případně jeho chování (dynamika podpisu). Trendem je v současné době využití různých biometrických prostředků v kombinaci s jinými druhy autentizace (PIN, RFID karta …)

Obecné použití biometrických identifikačních prostředků je však zatím vždy o hledání kompromisu mezi pohodlím lidí a striktními požadavky na autentizaci, zvláště tam, kde je zapotřebí např. odbavit velké množství zaměstnanců nebo třeba při hraničních kontrolách.

Protože možných způsobů biometrické identifikace dnes existuje celá řada, v následujících kapitolách uvedu jen ty opravdu nejpoužívanější metody vyhodnocování biometrických charakteristik v civilním a bezpečnostním sektoru.

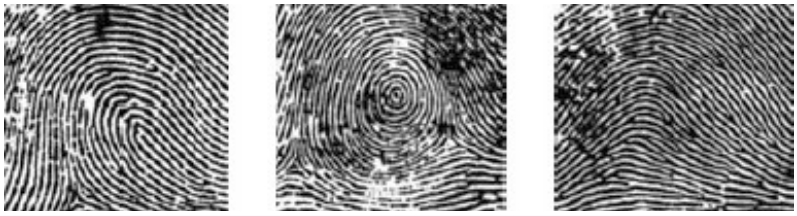
4.5.1 Snímání otisků prstů

Vyhodnocování otisků prstů patří k nejstarší, nejznámější a nejrozšířenější biometrické metodě. Otisky prstů jsou nejvyužívanější způsob identifikace nejen v kriminalistice, ale i v běžném životě, a to zejména v různých bezpečnostních systémech, bankách, bezpečnostních službách apod. Tyto biometrické systémy poměrně rychle „identifikují“ oprávněnou osobu na základě předem vytvořeného referenčního vzorku v databázi a umožňují jí vstup do objektu, přístup do určitých systémů, přístup k určitým službám apod. Tato biometrická identifikace se řadí do skupiny daktyloskopických identifikací. Daktyloskopie představuje nauku o obrazech papilárních linií na vnitřních stranách článků prstů a dlaní člověka. Tvary papilárních linií, jejich průběh a směr jsou u jednotlivých osob odlišné, a to dokonce i u jednovaječných dvojčat.

Daktyloskopie využívá tzv. tři daktyloskopické zákony, které lze zjednodušeně definovat takto:

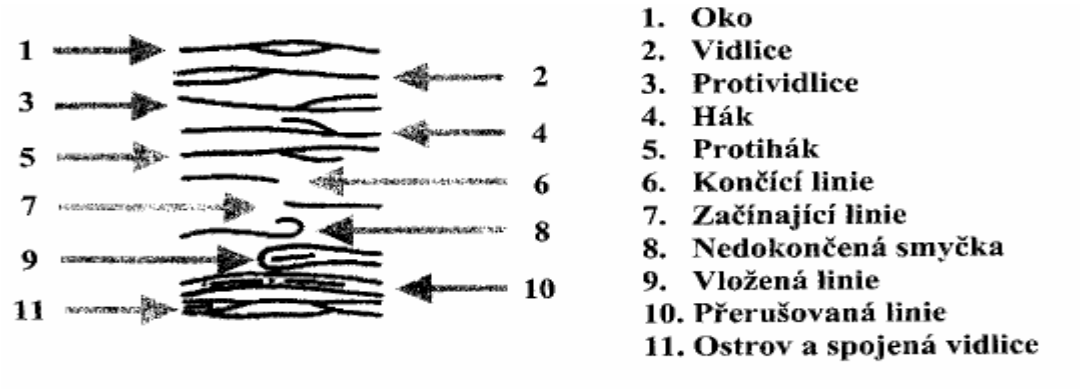
- na světě neexistují dva jedinci, kteří mají shodné obrazce papilárních linií
- obrazce papilárních linií jsou po celý život relativně neměnné
- obrazce papilárních linií jsou trvale neodstranitelné, pokud není odstraněna zárodečná vrstva pokožky

Vnitřní povrch prstů obsahuje vyvýšené drobné brázdovité útvary, které vytvářejí různé vzory. Tyto vzory se dělí do tří hlavních kategorií, a to **smyčky**, **přesleny** a **oblouky** (obr. 22). Důležité je to, s jakou frekvencí se vyskytují. Například smyčky obsahuje 65% všech otisků, přesleny něco kolem 30% a oblouky jen asi 5% všech otisků.



Obr. 22. *Základní klasifikační vzory - smyčka, přeslen a oblouk*

Kromě určení vzoru daktyloskopického otisku prstu je třeba ještě určit shodnost individuálních znaků, resp. zvláštnosti papilárních linií – markantů. Tyto body se nacházejí v rýhách vzoru. Za individuální znaky se považují zejména:



Obr. 23. *Individuální znaky papilárních linií*

Pokud chceme srovnávat otisky prstů **podle předem sejmutého vzoru**, který může být uložen v samotném čtecím zařízení i mimo něj, rozložíme si nejprve vytvořený obraz po sejmutí snímačem na jednotlivé oblasti a poté porovnáváme jednotlivé linie sejmutého otisku se vzorovým. Metoda je použitelná i při drobných poraněních, stačí na ni čtečka s rozlišením 250 dpi. Pokud používáme **rozbor podle podrobnosti**, pak studujeme otisk mnohem důkladněji. Zajímá nás typ znaků na otisku, jejich pozice v otisku i celková orientace. Po naskenování prstu je předloha nejprve upravena tak, že se jednotlivé linie ztenčí na šířku jednoho pixelu - tím se v podstatě vytvoří zjednodušený model obrazu a až pak dochází ke srovnávání. Metoda je výrazně přesnější, ale i malé poranění zásadním způsobem mění výsledek. Vyžadována je čtečka vyšší citlivosti, nejméně 500 dpi.

Druhů snímačů dle použitého principu při snímání existuje na trhu celá řada, ale v zásadě se v praxi nejvíce uplatňují ***dva druhy snímačů – optické a kapacitní:***

Optické si můžeme zjednodušeně představit jako fotoaparát s bleskem. Právě blesk prst při skenování osvítí, čímž se jeho linie zvýrazní (vystouplé části linií odrazí světlo, rýhy pohltí) - obraz je pak zachycený CCD prvkem a odtud je převedený do světa nul a jedniček.

Kapacitní snímače jsou také někdy označované jako silikonové. Prst je v jejich případě přikládaný na elektronický prvek tvořený soustavou miniaturních polovodičů. Křemíkový plátek pak funguje jako jedna deska kondenzátoru, prst coby druhá. Kde jsou papilární linie přiložené k plátku, je jiný odpor než v místech, kde nejsou. Tím vlastně vzniká elektronický obraz. Tyto snímače mají oproti těm optickým menší rozměr a i jejich cena je příznivější. Ale vadí jim suché nebo naopak vlhké prsty, protože právě (ne)přítomnost vlhkosti mění odpor a v konečném důsledku vytváří zkreslený obraz - což přináší problémy s rostoucí chybovostí.

Oba dva systémy přitom mají i společné problémy: především jde o přesné umístění prstu na zařízení, protože i odchylka o několik málo stupňů může srovnávací software zmást, takže je nutné ji kompenzovat. Druhým problémem je rychlost: dnešní prvky jsou dobré pro verifikaci, ale při identifikaci jejich rychlost dramaticky klesá (hodí se tak maximálně pro databáze se stovkami šablon).

V poslední době se začalo experimentovat i s dalším snímačem, který provádí skenování bezkontaktně pomocí ultrazvukových vln. Tato technologie je ale zatím v plenkách, snímače jsou mimo jiné příliš rozměrné. Velkou výhodou této metody ovšem je, že její přesnost neovlivňuje vlhkost nebo špinavé ruce, tak jako tomu může být u klasických optických a kapacitních snímačů, které se s těmito neduhy v praxi často potýkají.

4.5.2 Rozpoznávání řeči a hlasu

V dnešní informační společnosti se předávání informací odehrává zpravidla mluveným slovem. Je to efektivní, přirozený a pohodlný způsob komunikace.

Hlasový vstup je při rozpoznání (analýze) řeči nebo hlasu ovlivněn mnoha faktory přičemž nejvýznamnějším je řečová složitost vstupu. Na aplikace pro zadávání příkazů a ovládání (command and control) jsou kladeny nejmenší nároky. Jedná se o přístup, kdy člověk ovládá zařízení pouze jednoduchými (jedno či více slovnými) příkazy. Tyto příkazy

se rozpoznají ze slovníkové databáze čítající několik desítek slov, na jejich základě se pak provedou případné povely a pokud to bylo vyžádáno, tak se v posloupnosti slov či v jednoduchých větách podá uživateli zpráva o výsledku příkazu.

Vyšší nároky jsou kladeny na aplikace pro diktát. Tyto aplikace se musejí vyrovnat s plynulou řečí a nezávislosti na mluvčím. Nejvyšší nároky na rozpoznání představují aplikace pro diktát s integrovaným porozuměním mluvenému jazyku. Další specifickým hlediskem je prostředí použití. Nejjednodušší je použití v tichém prostředí a pro jednoho mluvčího. Obtížnost stoupá s použitím plynulé řeči v závislosti na prostředí a na mluvčím.

Jednou z řešených úloh je i syntéza řeči z textu **TTS** (***Text-To-Speech Synthesis)***, někdy nazývaná jako konverze textu na řeč. Je to nejen nejobecnější, ale také nejnáročnější způsob syntézy. Část posluchačů se mylně domnívá, že to, co slyší často z počítače, je skutečně syntetická řeč vzniklá převodem z textu. Ve většině případů se však jedná o tzv. „resyntézu“ neboli reprodukci původní promluvy. Skutečný TTS systém je však schopen generovat promluvu z libovolného textu. Cílem výzkumu v této oblasti je vytvořit systém, který převede automaticky libovolný text (korespondence, e-maily, SMS-zprávy, novinové a časopisecké články, knihy apod.) na mluvenou řeč. Tato syntetická řeč však nesmí, ani po delší době, posluchače unavovat, ani od něj vyžadovat přílišnou pozornost, musí být tedy co nejvíce přirozená. Přirozenosti řeči napomáhá dobrá prozódie (výslovnost).

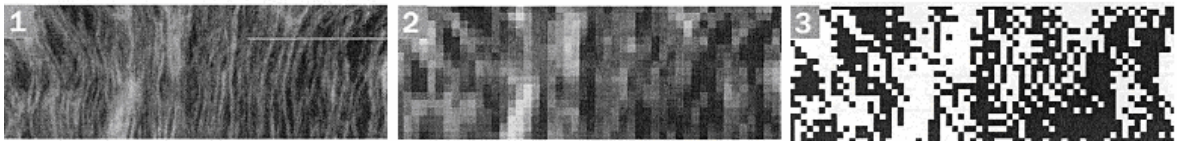
4.5.3 Sken oční duhovky a sítnice

O něco více exotičtěji působí biometrické technologie spojené s očima, jmenovitě tedy snímání oční duhovky a sítnice. Obě tyto techniky mají jednu společnou a velice příjemnou vlastnost, a to přesnost. Identifikace snímáním duhovky i sítnice patří mezi nejpřesnější biometrické možnosti, ruku v ruce s tím nejsou pro většinu uživatelů ani většinou přespříliš obtěžující nebo náročné na naučení.

Proces rozpoznávání oční duhovky

Detailním zkoumáním lidského oka lze v duhovce zaregistrovat několik jasně viditelných vnějších znaků (kruhy, skvrny, rýhy, koróny atd.), které jsou stabilizovány během prvního roku po narození a zůstávají neměnné celý život. Při snímání dochází k digitalizaci těchto rysů, přičemž je pořizován černobílý snímek uživatelova oka ve vysokém rozlišení (obr.24).

V prvním kroku tohoto identifikačního postupu tedy nejde o nic jiného než o digitální vyfotografování očí. Následně systém vyhodnotí komplexní vzor duhovky, snímek rozloží na malá políčka, jejichž obsah se matematickými operacemi převede na číselné hodnoty, reprezentované stupněmi šedi. Políčka světlejší než průměr se poté změní na bílá, zbylá obdrží černou barvu. Bílá a černá pak představují jedničky a nuly ve vzorové šabloně, 512 bajtů velkém datovém bloku, který reprezentuje skenovanou duhovku.



Obr. 24. *Proces rozpoznávání oční duhovky*

Dnes neexistuje žádná jiná biometrická charakteristika člověka, která by poskytovala více rozlišovacích možností než právě oční duhovka. Nalezení dvou identických duhovek náhodným výběrem je mnohonásobně méně pravděpodobné než nalezení dvou identických otisků prstů. Dokonce i obě duhovky jednoho člověka jsou rozdílné a jedinečné. Ani dvě identická dvojčata nemají duhovky stejné.

K rozpoznávání se obvykle používá spodní půlkruh duhovky – kruhový segment se přitom transformuje na pravoúhlý proužek. Jelikož je struktura duhovky u osob s tmavou barvou očí v normálním světle těžko rozeznatelná, osvětlují se oči při fotografování neviditelným infračerveným světlem, které lépe proniká očním barvivem, melaninem.

Výhodou této metody je, že není vyžadován žádný fyzický kontakt mezi duhovkou a snímající kamerou, tím je používání rychlé, pohodlné a vysoce přesné. Dokonce ani fotografie oka nebo skleněné oko nemohou přelstít takovýto systém.

Skenování oční duhovky dnes ve velkém používají Spojené arabské emiráty, a to ke kontrole osob vykázaných ze země. Dříve se často stávalo, že po vyhoštění si dotyčné osoby změnily jméno, nechaly si vystavit nový pas a vrátily se. Nyní jsou všichni příchozí na letištích a dalších hraničních přechodech kontrolováni, což denně představuje čtvrt až půl miliónu osob. Dodnes bylo odhaleno přes deset tisíc osob, které se chtěly nelegálně vrátit, ačkoliv byly v minulosti ze země trvale vykázány. Systém je natolik kvalitní, že zatím nebyla zaznamenána žádná chyba, kdy by si někdo oprávněně stěžoval, že nebyl vpuštěn neprávem (zda byl naopak někdo vpuštěn, ač být neměl, se dozvíme těžko). Spolehlivost systému je udávaná jako jedna ku osmdesáti miliardám.

Proces rozpoznávání oční sítnice

Oční sítnice, stejně jako duhovka obsahuje velké množství specifických anatomických znaků, které zajišťují její vysokou identifikační přesnost. Protože sítnice není viditelný lidský orgán, používají se pro její transformaci do viditelné podoby koherentní infračervené světelné zdroje. Důvodem je, že cévy sítnice rychleji absorbují infračervenou energii než ostatní tkáně, což způsobuje, že tyto cévy jsou na snímaném obraze tmavší.

Pomocí infračerveného paprsku se v tomto případě skenuje okolí tzv. slepé skvrny, jejíž struktura je vlastně jakýmsi unikátním "otiskem prstu". Metoda je však v praxi drahá, náročná a neoblíbená (přeci jen infračervený paprsek do oka je pro mnoho osob méně přijatelný než pouhé vyfotografování). Další problémy jsou technického rázu. Zařízení se musí umístit na stěnu, přičemž osoby menšího i většího vzrůstu mají problémy správně ke čtečce (nastavené na průměrnou výšku) přistoupit. Skenování navíc musí probíhat bez brýlí (u duhovky brýle nejsou problém) či bez kontaktních čoček, trvá 10 až 15 sekund - duhovka pod pět sekund. Navíc vědci se dodnes neshodli na tom, zda se struktura sítnice v okolí slepé skvrny s věkem nemění. Vše nasvědčuje tomu, že ano, což by metodu rozpoznávání oční sítnice z biometriky bez pardonu diskvalifikovalo.

4.5.4 Geometrie tvaru a otisku dlaně

Tvar ruky se u člověka s věkem nemění: jedná se např. o poměry délky a šířky prstů. Tato metoda ale umožňuje vzhledem k vysoké chybovosti pracovat jen s omezeným množstvím vzorků - hodí se k verifikaci, ale nikoliv pro vyhledávání konkrétních osob. Její výhodou ale je - na rozdíl třeba od otisků prstů, kterých za sebou každý z nás zanechává denně stovky - že siluetu nikde neotiskujeme a pro potenciálního útočníka je obtížné ji získat. Každopádně se jedná o stabilní technologii, která se ve velkém používá už přes třicet let. Nepodléhá módním vlnám nebo technologickým výkyvům, i dnes se lze tedy setkat se spolehlivě fungujícími přístroji patnáct let starými.

Podobně jako otisky prstů lze použít i otisk dlaně. Vyžaduje to ale nasazení rozměrné čtečky, ale na druhou stranu se díky mnohem většímu počtu srovnávacích bodů dosahuje vyšší přesnosti. Pro představu: čtečka dlaně stojí 2 000 až 4 000 dolarů, snímač otisku prstu začíná někde u 20 dolarů. Rozdíl je tedy více než znatelný.

4.5.5 Rozpoznávání obličeje

Rozpoznávání druhých osob podle obličeje provádíme s pomocí vlastního mozku dnes a denně. A to jak v oblasti verifikace, tak identifikace. Ideálem výzkumníků je pochopit, na základě jakých principů pracuje lidský mozek, jaké parametry vyhodnocuje, jak je srovnává - to by vedlo k vytvoření dokonalých kamerových systémů se stoprocentní schopností identifikace.

Pro biometrické určování totožnosti podle celého obličeje existuje mnoho metod, avšak než se nám podaří přesně rozluštit (podaří-li se to vůbec) tajemství fungování lidského mozku, musíme se spokojit s ryze technickým přístupem. Postupujeme tedy v zásadě stejným způsobem jako třeba policie: studujeme jednotlivé charakteristiky, z nichž se obličej skládá. Určujeme pozici jednotlivých částí obličeje, vzdálenosti mezi nimi, rozdíly mezi pravou a levou stranou. V praxi někoho poznáme, i když se šklebí, dělá opičky, používá mimiku. Stejně tak počítač nemá problém s tím, když někdo přibere, nechá si narůst plnovous, zestárne. Mnohem větší problém je, že si nedokáže poradit s pootočeným obličejem. Prostě při analýze snímku z boku nepozná, že dotyčnou osobu zná zepředu. [9]

4.5.6 Identifikace podle DNA

Kyselina deoxyribonukleová se jako identifikační prvek používá v policejní praxi od druhé poloviny osmdesátých let. Vzorky DNA získané na místech činu ještě dnes v mnoha případech ovlivňují přešetření kriminálních případů starých desítky let.

Struktura DNA je odlišná u všech lidí s výjimkou jednovaječných dvojčat a s věkem se nemění. Přesnost zkoumání DNA je důvodem pro stále širší využití této technologie i přesto, že získávání otisků DNA představuje poměrně náročnou a zdlouhavou proceduru. Tato metoda se zrodila jako vedlejší produkt výzkumu, zaměřeného na celkem jinou problematiku, a to na studium struktury lidského genetického materiálu, s využitím při diagnostice genetických onemocnění.

V současné době umožňují metody analýzy DNA určit původ biologických stop s takovým stupněm jistoty, jaký poskytuje daktyloskopie a navíc je tato metoda identifikace jedním z nejrychleji se rozvíjejících oborů kriminalistické biologie, kde je pro tento druh zkoumání zaveden název "*molekulárně genetická expertiza a analýza DNA*". [12]

4.5.7 Ezoterická a behaviometrická identifikace

Pod označením „ezoterická identifikace“ je uvedena poslední a tak trochu nevšední skupina biometrických identifikačních metod. Patří sem metody, které v praxi nejsou zatím běžně známé, či rozšířené a dostatečně prověřené na rozsáhlém souboru testovaných případů. Prozatím se nepoužívají jen pro bezpečnostně-komerční aplikace, ale v určitých případech jsou v zahraničí využívány i pro policejně-soudní potřeby. Nicméně jsou to metody, kterým je do budoucna věnována mimořádná pozornost a časem se mohou stát rovnocennými partnery pro soudní nebo bezpečnostně-komerční identifikaci.

Mezi ezoterické identifikační metody se řadí topografie žilního řečiště ruky, termovizní obrazy tváře, tvar vnějšího ucha a otisk ušního boltce, dynamika podpisu, otisky rtů a pórů, pleťová spektroskopie, pach lidského těla, analýza produktů metabolismu, obsah solí v lidském těle a v poslední době zejména identifikace na základě podélného rýhování nehtů ruky, které lze vyhodnocovat podobně jako čárové kódy. Tato metoda je zatím ve stadiu testování, ale představuje možnost levné a velmi rychlé biometrické identifikace. Nevýhodou však zřejmě bude nízká odolnost proti podvrhům.

Speciální podkapitolou biometriky je také „behaviometrika“, při níž dochází ke sledování vlastností (nikoliv fyzických parametrů) člověka. Typickým příkladem může být třeba styl psaní na klávesnici - četnost úderů, jejich rytmika - toto je pro každého člověka jedinečné. Na stejném principu pracuje také ověřování pomocí monitorování pohybu počítačových myší. Rozhodně jsou to zajímavé systémy, protože umožňují průběžnou kontrolu - nestačí, že oprávněný uživatel provedl autorizaci, neboť systém následně pozná, kdy v průběhu práce usedá ke klávesnici jiná osoba. V podstatě zde neexistuje možnost napodobení, protože nuance jsou tak drobné, že se je člověk nemůže naučit.

Do behaviometrických identifikačních metod řadíme také studium lokomoce – stylu chůze, gest, mimiky a jiných typických znaků. Můžeme tak identifikovat osobu i na velkou vzdálenost, což nám dává velkou možnost usvědčit např. pachatele trestné činnosti (krádeží, loupeží), teroristy a extremisty, kteří při své činnosti používají kuklu, převlek či jiné maskování a nezanechají na místě činu žádnou biologickou ani materiální stopu. (do budoucna se uvažuje i o nasazení tohoto druhu identifikace s pomocí družic na oběžné dráze). Obecným problémem u některých z těchto faktorů je skutečnost, že se v čase mění.

4.6 Současné možnosti použití biometrie

Oblasti, kde je žádoucí spolehlivá identifikace osob, je celá řada, a proto i biometrické identifikační systémy mohou najít široké uplatnění v nejrůznějších oblastech.

Stávající biometrické systémy „identifikují“ přímo člověka, nikoli předměty, kódy či hesla. Používají se všude tam, kde je třeba zajistit vysokou spolehlivost, transparentnost, bezpečnost a zároveň jednoduchost a komfort. Biometrický průmysl se proto stále více zaměřuje na počítačově snazší a poměrně rychlou verifikaci oprávněných osob. Magnetické nebo čipové karty, identifikační karty i klasické domovní klíče mohou být ztraceny, odcizeny nebo zkopírovány. Hesla nebo PIN kódy mohou být zapomenuty, odpozorovány nebo sdíleny více uživateli. Zato u všech biometrických systémů je nutné, aby procesu identifikace nebo ověření identity byla daná osoba vždy fyzicky přítomna. V případě, že je vyžadována vysoká úroveň zabezpečení systému, lze biometrii s výhodou použít i v kombinaci s jinými metodami autentizace, jako je heslo/PIN nebo čipová karta.

Spektrum použití biometrických systémů je značně široké a uplatnění nacházejí v nejrůznějších oblastech. Nejběžnější jsou systémy pro fyzické přístupy do budov (například jako náhrada za klasické klíče a sloužit tak k otevření dveří domů, bytů či kanceláří) nebo k informacím (tj. autorizaci přístupu do počítačových sítí, pracovních stanic nebo pro zpřístupnění klientského účtu v bankomatech), dále jako kontrola totožnosti nebo ochrana dat. Biometrii lze využít i v souvislosti s elektronickým podpisem, kde může sloužit k omezení přístupu k soukromému klíči uživatele.

Ve státní správě nachází biometrie uplatnění v soudnictví a soudním vyšetřování při identifikaci pachatelů, při zabezpečení věznic nebo na letištních terminálech.

O postupném zavádění biometrických technologií se uvažuje i na hraničních přechodech v Evropě. Německá hraniční policie na hraničním přechodu Rozvadov–Waidhaus mezi Českou republikou a Spolkovou republikou Německo v nedávné době skenovala fotografie z cestovních pasů a porovnávala tyto obrazy v počítačovém systému s autentickými snímky majitelů cestovních pasů.

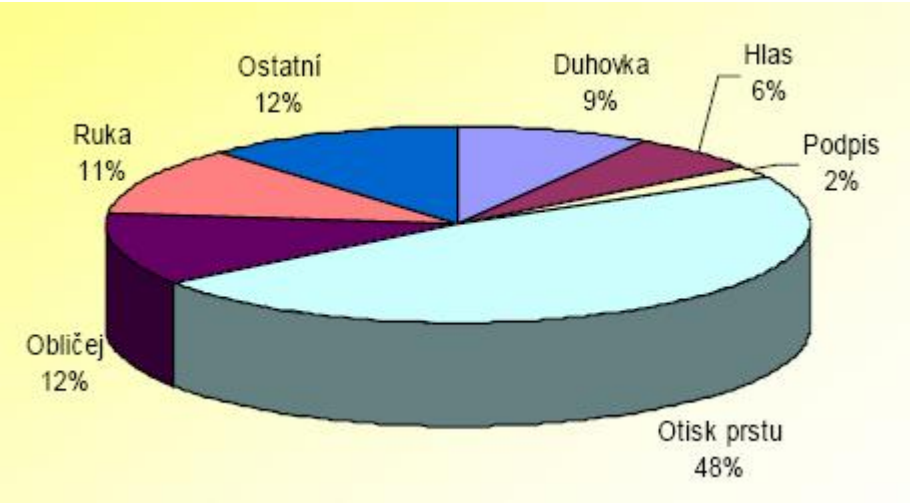
V kriminalistice se v Evropské unii nahrazuje zařízení pro tlakový otisk palce stanicí značky LiveScan, která papilární linie na prstech a dlani digitálně zpracuje na skeneru a údaje o nich vede v elektronické evidenci.

Přednost skenu oční sítnice dává např. Mezinárodní úřad pro civilní letectví **CAO** ***(International Civil Aviation Organisation).*** Pro mezinárodní sjednocení průkazů totožnosti a cestovních dokladů je i příslušný úřad OSN.

Již v současnosti je to především realizace elektronického čipového pasu, spojená s digitálním a biometrickým znakem. Tento znak je na kartě uložen a zašifrován. Autentizace probíhá bez porovnání s databází, tzn. výlučně prostřednictvím porovnání znaku na průkaze s odpovídajícím znakem osoby, která průkaz předkládá. Zatím neexistuje shoda ve stanovení doby platnosti průkazu. Uvažuje se o době platnosti v délce deseti let.

V aplikacích biometrie na rozhraních výpočetních systémů ve službách, spotřební elektronice a průmyslu nacházejí uplatnění především již zmíněné moderní metody založené na elektronickém snímání otisků prstů, především v kombinaci s optikou. Jde o ověřenou metodu, s jejíž pomocí lze při přijatelných nákladech dosahovat velmi velké přesnosti. V současnosti nejde však jen o konstrukci snímačů a jejich cenu. Na trhu pro tuto důležitou oblast zatím stále ještě chybí nabídka úplného a snadno použitelného řešení zahrnujícího dostatečnou ochranu na všech úrovních, počínaje přístupem k aplikačním programům až po přístup k základnímu systému vstupů a výstupů počítače (BIOS).

V grafu je uveden přehled používaných biometrických technologií v soudobé praxi



Obr. 25. *Biometrické identifikační systémy a jejich podíl na trhu*

II. PRAKTICKÁ ČÁST

5 PROBLEMATIKA BEZPEČNOSTI ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

Ve velmi dávné historii, na počátku samotného obchodování, kdy ještě nebyly vynalezeny peníze, se obchodovalo ve své nejprimitivnější formě tzv. barteru, což je přímá výměna zboží a služeb za jiné zboží a služby. Postupem času však toto obchodování bylo více a více komplikovanější, a tak byl barter nahrazen různými formami peněz.

Důvěryhodnost peněžního systému byla garantována místní, národní či mezinárodní bankou, která kontrolovala tisk nových bankovek a ražbu nových mincí. Platba v hotovosti pomocí mincí a bankovek se stala a stále je nejpoužívanější formou směny peněz.

V posledních letech však pozorujeme trend, kdy lidé placení v hotovosti stále více omezují, což je způsobeno především díky tomu, že lidé již nechtějí shromažďovat u sebe větší sumy peněz, ale mají je raději na svých peněžních kontech, kde se úročí a dále pak díky větší bezpečnosti svých finančních prostředků (když mi někdo ukradne platební kartu na PIN, ještě to neznamená, že přicházím o peníze, protože zloděj PIN nezná, ale když mi někdo ukradne peněženku s penězi, tak už se s nimi nesetkám).

Postupem doby tak vznikly různé šeky, platební poukázky - "plastikové" peníze a ty "opravdové" peníze se začaly přesouvaly hlavně mezi bankami po bezpečných finančních sítích. V poslední době se rozvíjí také obchodování přes telefon a internet, kdy se nakupující ani prodávající navzájem nevidí, a tak může být velmi problematické hodnověrně ověřit, zda se nakupující či prodávající nepokouší o podvod.

Implementace elektronických plateb je odbornou veřejností uznávána jako jedna z nejvíce rostoucích oblastí v elektronické komerci, což si uvědomují hlavně obchodníci a snaží se tak co nejvíce vyvíjet své vlastní platební systémy. Tato skutečnost má za následek to, že již dnes je na trhu několik možných řešení elektronických platebních systémů a jejich počet neustále narůstá. Očekává se, že dokud se trh nestabilizuje, bude tento trend pokračovat. Cílem praktické části této práce je zmapovat a popsat vlastnosti, případně možná rizika zneužití v praxi dnes běžně dostupných elektronických platebních systémů.

5.1 Obecné požadavky na bezpečnost peněžních transakcí

Konkrétní bezpečnostní požadavky na elektronické platební systémy (dále jen EPS) se liší v závislosti na rysech jednotlivých systémů, obecně však mezi základní vlastnosti [16], těchto systémů patří: důvěrnost, integrita, utajenost, autorizace, interoperabilita, dostupnost a spolehlivost přenášených dat. Stejně jako ve světě klasických peněz, i ve světě elektronických plateb stále budou existovat rizika porušení důvěryhodnosti a bezpečnosti. Jde jen o to, aby použité kryptografické mechanismy a protokoly tato rizika minimalizovaly.

Uplatňované bezpečnostní politiky šifrováním zpráv brání porušování důvěrnosti a elektronickými podpisy brání nepoctivým zákazníkům, aby se podvodně vydávali se za jiné osoby, nepoctivým obchodníkům, aby falšovali elektronické platební příkazy zákazníků a konečně chrání i integritu přenášených dat. Používání důvěryhodného software brání krádežím v počítačových systémech pomocí různých trojských koňů.

Možností jak ochránit elektronické transakce je mnoho, avšak mezi základní požadavky, které systém elektronických plateb musí splňovat, patří zde v úvodu uvedené vlastnosti, které nyní blíže rozvedu v následujících odstavcích.

5.1.1 Důvěrnost, integrita, autorizace

Důvěrnost musí zabezpečit, že neautorizované osoby nemohou odposlechem komunikací v síti nebo vniknutím do zúčastněných počítačů zjistit takové informace, jakými jsou příkazy, platby a účty zákazníka. Taková vlastnost se zajišťuje pomocí kryptografie.

Aby se omezil výskyt krádeží a snížila se tudíž celková cena zpracování plateb, prověřuje se identita zúčastněných stran autentizací. Obchodník si musí být jistý, že zákazník je legitimní uživatel čísla účtu platné platební karty. Zákazník musí mít možnost identifikovat obchodníka, se kterým může bezpečně elektronicky obchodovat a musí si být jistý, že tento obchodník spolupracuje s finanční organizací, která akceptuje jeho platební kartu. Autentizace se implementuje digitálními podpisy a certifikáty. Zákazník zprávami reprezentujícími platební transakce sděluje co objednává, svoje personální data a platební instrukce Obsah zpráv se během přenosu nesmí změnit. Vlastnost integrity se obvykle implementuje digitálními podpisy.

Celistvý platební systém také nedovoluje, aby se převáděly peníze od uživatele, který tuto akci neautorizoval. Umožňuje také odmítnutí přijetí platby bez souhlasu, aby zabránil

podobným věcem jako je např. uplácení. Autorizace tvoří u neanonymních EPS nejdůležitější složku v platebních systémech a může být prováděna třemi způsoby:

- ***autorizace třetí stranou***

Ověřující stranou je typicky banka, která buď zamítne nebo potvrdí transakci použitím bezpečného venkovního kanálu (např. pošta, telefon). Typické použití je u objednávek po telefonu či mailu. Typické použití je u plateb typu **CNP** ***(Cardholder Not Present)***, dříve zvané **MO/TO** ***(Mail Order/Telephone Order).*** Kdokoliv, kdo zná data z kreditní karty může vyvolat transakci a odpovědný uživatel pak musí toto potvrdit nebo naopak říci, že jde o nepovolenou transakci. Obvykle pokud uživatel nepodá podnět proti dané transakci do 90 dní, je automaticky schválena.

- ***heslem***

Transakce chráněná heslem požaduje, aby každá zpráva od autorizované strany zahrnovala šifrovanou část pro kontrolu. Tato část je vypočítána pomocí tajného klíče, který je znám pouze autorizující a ověřující straně.

- ***digitálním podpisem***

V tomto typu autorizace požaduje ověřující strana digitální podpis autorizované strany. Digitální podpis zajišťuje nepopíratelnost původní zprávy, protože pouze majitel tajného podpisového klíče se mohl podepsat pod tuto zprávu (resp. podepsat se může každý, ale odpovídající digitální podpis majitele X může vytvořit pouze majitel X, protože ten je jediný kdo zná tajný klíč).

5.1.2 Interoperabilita a utajenost

V praxi je nutné, aby se na platebním systému současně podílely různé hardwarové a softwarové platformy. Každý obchodník může používat jiný počítačový systém, odlišné počítačové systémy mohou používat také jednotliví zákazníci, i banka obchodníka si může volit svoji vlastní počítačovou platformu. Potřebná interoperabilita se dosahuje aplikací standardizovaného platebního protokolu. Takovým protokolem je např. protokol SET, který k záruce za interoperabilitu přirozeně přidává i záruky za udržování výše zmíněných vlastností. U neanonymních EPS mohou některé zúčastněné strany požadovat tzv. utajenost transakce, čímž se myslí to, že některé informace o dané transakci (např. jméno plátce, příjemce, celková suma, atd.) zůstanou utajeny vůči třetím osobám.

5.1.3 Dostupnost a spolehlivost

Jednou z dalších důležitých vlastností EPS, je možnost provádět platby kdykoliv je to potřeba. Platební transakce musí být atomické - tj. provede se buď celá nebo žádná část transakce a nesmí se stát, že by systém zůstal v neznámem či nekonzistentním stavu. Žádný plátce by neakceptoval ztrátu peněz kvůli hardwarovým či softwarovým potížím. Dostupnost a spolehlivost tedy předpokládá především bezchybný chod všech počítačových komponent. A pokud už k nějakému problému dojde, je nezbytné mít vypracovaný plán návratu do původního konzistentního stavu. Chybové stavy zde nejsou dále probírány, protože většina vývojářů EPS je běžně ani s logických důvodů neuveřejňuje.

5.2 Nejpoužívanější technologie elektronických plateb

Sféra elektronických plateb je velice široká, existuje několik různých systémů, které mezi sebou soutěží o pozici suverénního lídra a snaží se přetáhnout obchodníky na svou stranu. Každá kategorie má své vítěze i poražené, nicméně je jisté, že dokud nebude jasně definované jedno řešení dominovat celému trhu, budou tyto platební modely jako jsou šeky, kreditní karty, virtuální peníze, dál existovat paralelně vedle sebe.

5.2.1 Elektronické karty

V současné době se používají platební karty několika druhů:

(*řazeno podle vývojového hlediska*):

Embosované karty: Typ a umístění embosovaného textu je specifikován standardem ISO 7811. Norma definuje embosování ve dvou oblastech - první je určena pro číslo karty (až 19 znaků), které identifikuje jak vydavatele, tak i držitele, a druhá oblast je vyhrazena na další údaje o držiteli, jako je jméno a adresa (4 řádky po 27 znacích).

Karty s magnetickým pruhem: Tento typ karet nese magnetický proužek, na kterém jsou uloženy údaje (250 B) o vlastníkovi, číslo karty atd. Kdokoliv s odpovídajícím čtecím zařízením na tyto karty si může přečíst uložené informace.

Čipové pamětové karty: Používají se pro jednoduché aplikace jako jsou předplacené telefonní karty, které mají chip s 60 nebo 120 pamětovými buňkami. Tyto buňky jsou použitelné jenom jednou, to znamená, že jakmile se paměťová jednotka použije, karta se dále stává bezcenná a může se vyhodit.

Čipové procesorové karty: Jak již název napovídá, karty obsahují mikroprocesor, který kontroluje přístup k informacím na kartě. Tyto karty zvyšují ochranu proti podvodům a používají se v těch nejdůležitějších (z hlediska bezpečnosti) aplikacích.

Optické karty: Zatím se vyrábějí bez procesoru, ale v budoucnu na tomto druhu karet jistě nebude chybět. Umožňují ukládání mnoha megabytů dat, nicméně údaje mohou být zatím zapsána jen jednou a nelze je smazat. Nacházejí využití například ve zdravotnictví, neboť jejich kapacita umožňuje uložení rentgenových snímků.

Kromě toho se platební karty dělí podle typu zúčtování na:

Debetní - jedná se o kartu, kterou lze platit nebo vybírat z bankomatu, pokud je na účtu, ke kterému byla karta vydána, dostatek peněz. K zúčtování dochází většinou chvíli po provedené transakci.

Kreditní - kartou se může nakupovat zboží nebo služby na úvěr. K zúčtování dochází až po určité bankou stanovené době. Úvěr se čerpá prostřednictvím revolvingového (opakujícího se) úvěrového limitu, který se obnovuje automaticky po splacení dlužné částky. Banky stanovují minimální výši splátky úvěru (obvykle 5 - 10 % z dlužné částky) a úvěrový limit (podle bonity klienta).

Charge - zde kartou nenakupujete na úvěr. Při zúčtování, které je také stanovené k určitému datu (obvykle 14 - 30 dní), musíte splatit celou dlužnou sumu. Charge kartou neboli kartou s odloženou splatností čerpáte samostatný úvěrový produkt, tak zvaný karetní úvěrový rámec účtu, poskytnutý k vašemu účtu.

5.2.2 Mobilní telefony

Zájem o mobilní telefony, jako autentizační zařízení pro platby, se neustále zvětšuje. Částečně za to může i nedostatek čtecích zařízeních pro smart karty u osobních počítačů. Předpokládalo se totiž, že tyto čtečky se stanou běžnou výbavou PC, což se nestalo a mobilní telefony tak můžeme použít pro různé druhy vzdálených i lokálních plateb. Můžeme s nimi platit za stahování dat do PC, telefonu, za nákup CD disků, knih, šatů po internetu, ale stejně tak v normálním kamenném obchodě, můžeme s nimi hradit parkovné, mýtné, různé zboží z prodejních automatů a nespočet dalších věcí.

Všechno to začalo s uvedením SMS zpráv s přidanou hodnotou, jejímž přijetím či posláním jsme si mohli stáhnout např. novou vyzváněcí melodii. Tento trh se rozrostl do velikosti přesahující 1 miliardu EUR pro samotnou Evropu [17] a stále roste díky neustálému uvádění nových digitálních služeb. Je tu tedy stále ještě velký potenciál, čehož si uvědomovali hlavně mobilní operátoři a tak postupně vznikalo nespočet skupin a projektů, které v této oblasti mají své zájmy a postupně vyvíjejí nové standardy a nové projekty. Mezi ty největší patří Mobile Payment Forum, PayCircle, The Mobey Forum a posledně ustanovená Mobile Payment Services Association tvořená největšími evropskými mobilními operátory (Vodafone, Orange, T-Mobile, Telefónica).

Nedlouho po té co přišel na svět **WAP** ***(Wireless Application Protocol)*** bylo potřeba vyřešit z hlediska bezpečnosti, jak dopravovat bezpečně data mezi klientem a WAP bránou. SSL protokol, známý z počítačového prostředí, nebylo možné použít, a tak vznikl nový protokol **WTLS** ***(Wireless Transport Layer Protocol)***. Zprávy používané v WTLS jsou funkčně identické k těm v SSL, avšak díky horší propustnosti linek se musely provést menší změny. Certifikáty použité ve WAPu jsou více kompaktní a dialogy jsou strukturovány tak, aby se posílaly jenom ty certifikáty, které jsou absolutně nezbytné. Cesta mezi WAPovou bránou a serverem je pak již dále zabezpečena protokolem SSL.

Všechny mobilní telefony si udržují detaily o identitě svého majitele v smart kartě, která se označuje jako **SIM** ***(Subscriber Identity Module)*** karta. WTLS toto napodobilo a z tohoto konceptu specifikovalo **WIM** ***(Wireless Identity Module)***, jež vykonává bezpečnostní funkce v aplikační úrovni WAPu, především ukládá a zpracovává informace potřebné k identifikace a autentizaci. Celé je to založeno na tom, že citlivá data (klíče) jsou uložena ve WIM a všechny operace s klíči se provádí taktéž v tomto modulu. WIM jako samostatný modul může být integrován na stejné SIM kartě (označováno jako SWIM), tvořen jinou samostatnou smart kartou a nebo může být implementován softwarově (Java).

Klíčovým faktorem pro platební operace prováděné mobilním zařízením resp. pro jejich masové rozšíření je jejich použitelnost, jednoduchost a bezpečnost. Tyto operace musí být rychlé, nesmí zákazníka zdržovat zadáváním desítek čísel a znaků. Nové technologie umožňující uživatelsky intuitivnější grafické prostředí, komunikaci typu RFID a Bluetooth. Nové verze mobilních prohlížečů a aplikační prostředí (Symbian, MIDP Java) vytvářejí pro mobilní komerci dobré základy, což se jistě v budoucnu projeví. Vznikají pilotní projekty jako např. mobilní peněženka, která podporuje nejrůznější typy plateb.

Mobilní telefon je na nejlepší cestě stát se ekonomicky zajímavým, bezpečným a dostupným platebním nástrojem. Proto je zájem mobilních operátoru v celém projektu pochopitelný. Taktéž banky, které vložily spoustu peněz do různých projektů elektronických peněženek a jejichž přínos byl mizivý, mají zájem se spojit s mobilními operátory a vytvořit nový efektivní platební model. Každá platba provedená mobilním telefonem bude znamenat pro mobilní operátory další vítaný zdroj příjmů. Více bezhotovostních plateb ve větším množství obchodů přinese bankám nové příjmy a obchodníkům potenciálně o něco větší tržby.

Výhodou placení zboží a služeb prostřednictvím mobilních telefonů je v jejich snadné dostupnosti a masovém použití. Mobilní telefony v rukách zákazníků představují již vybudovaný základ nové platební infrastruktury, do které nebude nutné znovu investovat. Mobilní operátoři mají uzavřeny roamingové dohody ve většině zemí světa, mohou tedy zajistit placení téměř kdekoli na zemi. Jejich nevýhodou však je, že nemají mezinárodní clearingový a zúčtovací systém, který mají banky a jejich platební asociace. Mobilní operátoři také nemají mezinárodně známou obchodní značku, jako je VISA nebo MasterCard. Překonat tyto nedostatky by stálo desítky miliard dolarů a řadu let - nebo uzavřít strategická partnerství s bankami jako se stalo např. ve Španělsku a zdá se, že bude následováno i v dalších, zejména evropských, zemích.

V současné době probíhá několik projektů [24], které jsou podpořeny velkými společnostmi. Ve Španělsku je to ambiciózní projekt Mobipay do jehož příprav bylo investováno přes 120 miliónů EUR. Kromě projektu Mobipay se v Evropě testují také další řešení. V Německu, Rakousku, Švédsku a Španělsku se testuje systém Paybox. V Dánsku ověřuje bankovní kartové centrum PBS a mobilní operátor Orange. Klient musí mít Orange SIM kartu a platební kartu vydanou společností PBS (VISA, MasterCard nebo Danmont) a musí si službu zaregistrovat. Poté si sám zvolí PIN, který se uloží na SIM kartu. Jeho mobilní telefon je pak používán jako osobní platební terminál.

Česká republika nestojí stranou tohoto vývoje. České banky před 10 lety zavedly jeden z nejmodernějších systémů platebních karet v Evropě (MUZO), Expandia Banka (dnes eBanka) a Paegas (nyní T-Mobile) zavedly v roce 1998 jako první na světě GSM banking. V dobíjení předplacených služeb mobilních telefonů pomocí bankomatů nebo nyní i SMS zpráv se české banky opět zařadily mezi nejrychlejší inovátory.

5.2.3 Mikroplatby

Z běžných platebních nástrojů jako jsou platba v hotovosti, šeky, platební karty je pro placení malých částek nejvhodnější platba v hotovosti (cash). Cash je však zdola limitován hodnotou nejmenší mince (např. jeden eurocent). Existuje však takové zboží, či spíše služby, kterým toto může činit problém. Například internetový magazín by chtěl za každý přečtený článek od čtenáře inkasovat malou částku nebo podobně internetová encyklopedie by si nechala platit za každé nalezené slovo ve své databázi atd. Tradičně se tento problém řeší pomocí předplacení služeb za fixní částku na určité období. Zatímco platby předem zaručují, že bude poskytovateli za provedené služby zaplaceno, omezuje to spoustu zákazníků, kteří chtějí používat služby jen příležitostně. Také je omezena možnost danou službu pouze vyzkoušet.

Proto před několika lety vzniklo nespočet nových platebních schémat (mikroplateb), které jsou zaměřeny na tyto časté a nízkohodnotové platby na internetu, z nichž však jenom pár zůstalo a v současné době se ještě používají. Aby byly mikroplatby úspěšné a svým provozovatelům se vyplatily, je třeba, aby je používala obrovská masa lidí, resp. aby počet samotných plateb byl obrovský a to především proto, že cena mikroplatby a tím pádem i zisk z ní nesmí být pro obchodníka příliš veliký. Dá se říct, že existující finanční komunita pro tento nový druh plateb nenašla příliš velké pochopení, a tak se začali objevovat mikroplatební modely od převážně softwarových firem Millicent, PayWord, MicroMint, DirectPay, I Like Q, Monetka atd.

Tyto platební systémy efektivně přenáší velmi malé částky a samotný komunikační provoz, jenž stojí peníze, je v těchto systémech udržován na nejmenším možném minimu. Díky tomu, že zisk z každé platby je velice malý, musí mikroplatební systém být schopen ověřit každou platbu velice levně, zároveň však musí redukovat počet výpočetně náročných operací. Mikroplatby mohou také představovat kreditní schéma, kdy vzniká virtuální kredit (měna), pomocí níž jednotlivé uživatele můžeme odměňovat a tím i motivovat k požadovaným úkonům (návštěva webových stránek atd.).

Dnes s odstupem pár let již můžeme říci, že celkové uživatelské přijetí mikroplatebních systémů bylo velmi pomalé, možná také díky nedostatku hodnotného obsahu, který není volně přístupný v nějaké formě jinde na internetu. Podobně obchodníci se zdráhali investovat do kvalitního obsahu, dokud neexistovala dostatečně velká základna uživatelů ochotných platit tyto malé částky. Drtivá většina uživatelů chápe internet jako bezplatný

zdroj informací, tudíž není ani v nejmenším ochotna za informace platit, a raději věnuje mnohem více úsilí a nákladů, aby získala danou informaci nebo službu "zadarmo". Běžné (makro) platby nejsou pro zákazníky zas až tolik novou věcí. Na placení prostřednictvím nějaké služby jsme zvyklí z každodenního života a i přesto dnes hodně uživatelů internetu elektronickým platbám příliš nevěří. Naopak mikroplatby jsou pro všechny zcela novým pojmem a tím přirozeně jeho začlenění do podvědomí trvá mnohem déle.

Tyto a jiné příčiny způsobily, že naprostá většina největších mikroplatebních projektů z let 1995 až 1999 již neexistuje. Nedá se říci, že by už dnes žádné čistě mikroplatební systémy neexistovaly. Stále jich několik je a s rozpínajícím se internetem přibývají. Třeba jako nedávno u nás uvedený společný projekt ČSOB a Poštovní spořitelny - Pay Sec. Nicméně se již nejedná o žádné vizionářské projekty. Jejich úloha je spíše komorní. [22]

5.2.4 Elektronické peníze

Jak už jsem se zmínil v úvodu praktické části této práce, peníze (pokud budeme brát jejich fyzickou podstatu) se postupem času vyvinuly z cenných platidel (vzácné kovy - zlato, stříbro) až k systémům založeným na kreditní bázi. Se vznikem elektronické komerce se začalo uvažovat také o elektronické formě peněz. Elektronické peníze (e-peníze) lze považovat [23] za náhradu mincí a bankovek, které se ukládají na elektronickém médiu, jako jsou čipová karta nebo paměť počítače, a které jsou obecně určeny pro uskutečňování elektronických plateb v omezené výši.

Elektronické peníze lze dělit podle několika hledisek. Jedno dělení elektronických peněz může být podle jejich povahy na "token-based" nebo "balance-based":

- **Token-based** el. peníze jsou opravdovou virtuální kopií skutečných mincí. Existují v předem definovaných hodnotách, které je pro rozměnění třeba poslat do vydávající banky. Každé minci je přitom přidělena určitá jedinečná číselná (registrační) hodnota, jejíž existence má zabránit problému dvojího utrácení. Z toho také vyplývá, že každá "mince" je použitelná pouze jednou. Typickým příkladem byl Ecash od firmy DigiCash.
- **Balance-based** el. peníze jsou častější a mají podobu pouhého kladného nebo záporného zůstatku na elektronickém účtu. Do této kategorie jsme mohli zařadit např. český internetový platební systém I LIKE Q.

Dalším kritériem, podle kterého můžeme el. peníze dělit je jejich samotná implementace.

- **Card-based** el. peníze, jak už název napovídá, jsou takové elektronické peníze, které jsou uloženy na nějakém přenosném médiu, typicky karta s integrovaným obvodem obsahující mikročip (smart karta). Tato "elektronická peněženka" zajišťuje různé kryptografické funkce a hlavně s ní můžeme platit i v reálném světě. Jako příklad můžeme uvést předplacené karty MasterCard, VISA.
- **Software-based** el. peníze jsou takové, jenž se spravují přes software nainstalovaný na PC, PDA, běžící pod standardním operačním systémem. Typické použití je pouze přes počítačové sítě jako je internet.

Podle povahy emitenta členíme elektronické peníze na **bankovní** a **nebankovní**. Zatímco nebankovní elektronické peníze jsou takové, jejichž (zjednodušeně řečeno) emitentem není banka, bankovní elektronické peníze jsou takové peníze, které vydává právnická osoba disponující bankovní licencí v souladu s ustanovením §6 zákona o bankách.

Elektronické peníze je třeba striktně vymezit vůči různým internetovým věrnostním systémům, které jsou jen pouhou obdobou běžných věrnostních programů, jaké dnes nabízí každý větší supermarket. Za typický příklad lze uvést tzv. „fazole“ společnosti Eastbiz Net Inc. nebo „dukáty“ od firmy Mafra a.s. Zásadní odlišnost spočívá v jejich omezené konvertibilitě v některou z existujících měn a z poměrně omezených možností využití. Internetové věrnostní body jsou tedy jen marketingovým nástrojem pro získání nových zákazníků a nikoliv platební nástroj typu elektronických peněz.

Jsou pro nás však ePeníze nezbytné? Abychom správně pochopili současnou situaci těchto elektronických platebních systémů, musíme se vrátit zpět do devadesátých let, kdy se začali objevovat první pilotní projekty jako DigiCash, CyberCash, CAFE nebo český MONET. Klíčovou myšlenkou bylo to, že ePeníze byly určitým způsobem "předplaceny" a nebyly spjaty s žádným účtem (anonymita). Navíc do toku peněz nebyla zapojena žádná třetí strana. Byla to doba, kdy "internetová bublina" rostla neuvěřitelným tempem a investoři se nebáli dávat peníze do těchto projektů, i když to nebyly banky, ale noví hráči (nebankovní), kteří stáli za těmito projekty a vstupovali tak do bankovní sféry.

Bublina však časem splaskla a ani velkým bankovním hráčům na tomto světě se moc nelíbilo, že by různé nebankovní společnosti mohli vydávat e-peníze mimo jejich trh a navíc tu byla pořád šance, že tyto společnosti budou prosperovat a v budoucnu jim ukrajovat z jejich chutného peněžního koláče. Takže zjednodušeně můžeme říci, že následovalo několik bankrotů a vznik několika nových direktiv, které se podepsali na tom, že v současné době jsou ePeníze většinou produktem vydávaným pouze bankami, software-based ePeníze v podstatě neexistují, všechny systémy používají nějaký typ účtu, pouze u pár systémů se dá říci, že jsou plně anonymní.

Suma sumárum, současné ePeníze stále nemůžeme považovat za elektronický ekvivalent fyzických peněz - cash. Rozdíl mezi elektronickými peněženkami (např. předplacené karty) a jinými karetními platebními systémy se stále více zmenšuje a dle mého názoru všechny elektronické platební systémy směřují k tomu, aby se globalizovali v jedno univerzální platební médium.

5.3 Zajištění jednoznačné identifikace u platebních karet

Spotřebitelé stále nemají příliš velkou důvěru v posílání detailů o své platební kartě po internetu, ale ve skutečnosti jejich strach vychází ze špatného důvodu. Většina lidí se obává toho, že tato data budou zachycena na cestě k obchodníkovi, což je dnes již prakticky nemožné z důvodu toho, že na všech hlavních komerčních stránkách je použit protokol SSL, který šifruje všechny důležité detaily o platební kartě.

Ten podstatný problém, který si většina lidí neuvědomí, je to, že neexistuje cesta, jak autentizovat zákazníka při on-line platební transakci za použití platební karty. Tím je míněno to, že nemáme rozšířený mechanismus k potvrzení identity nakupujícího v době nákupu (tím se myslí použití platební karty na internetu a ne v normálním kamenném obchodě, kde si prodavač vždy ověřuje, zda souhlasí váš podpis s podpisem na kartě).

Jestliže chce on-line nakupující v dnešní době platit kartou na internetu, musí vždy zadat údaje o této kartě do formuláře na serveru obchodníka. Takto však může vzniknout situace, kdy kdokoliv cizí může do formuláře napsat údaje o cizí platební kartě a obchodník nemá šanci jak zjistit zda tyto údaje jsou pravé. Bez efektivní autentizace tak vznikají problémy jako např. nedostatek důvěry zákazníků vyšší cena samotných služeb apod.

V důsledku toho se otevírají možnosti pro alternativní platební metody bez použití platebních karet. Existuje několik řešení, které jsou zahrnuty v platebních systémech jako např. Card Security Code a Address Verification Service či bezpečnější a komplexnější řešení, např. MasterCard SecureCode, Verified by Visa či protokol SET.

5.3.1 SET

Vraťme se nyní na počátek samé e-komerce, kdy začátkem 90-tých let došlo k utvoření dvou největších konkurenčních konsorcií, vedených dominantními společnostmi poskytující kreditní karty. MasterCard spolu s Netscape Corporation, IBM a ostatními vytvořily v roce 1995 specifický systém **SEPP** ***(Secure Electronic Payment Protocol)***. Nedlouho na to druhé konsorcium vedené Visou a Microsoftem představilo odlišný a nekompatibilní systém nazvaný **STT** ***(Secure Transaction Technology)***. Pokud by tato situace setrvala, vedlo by to ke skutečnosti, kdy by každá transakce musela odpovídat specifickým podmínkám podle použité specifikace.

Začátkem roku 1996 konečně zvítězil zdravý rozum a společnosti MasterCard a Visa oznámily vzájemnou dohodu o vývoji jednotného systému, pojmenovaného **SET** ***(Secure Electronic Transaction)***.

Nutnou podmínkou k bezpečnému použití SETu je to, aby každý subjekt zúčastněný při platební transakci byl certifikován, tj. musí vlastnit digitální certifikát vydaný certifikační autoritou, která ověřila totožnost daného subjektu.

Vlastník karty zahájí platbu s obchodníkem používajícím SET. Obchodník poté použije SET k autorizaci platby. Platební brána může být ovládána poskytovatelem nebo sdružením poskytovatelů nebo přímo asociací poskytující kreditní karty. Tato platební brána je předřazená finanční síti a skrz ní poskytovatel karty může být kontaktován pro jednoznačné autorizace jednotlivých transakcí.

5.3.2 3-D SET

Protože se SET na trhu příliš neujal, rozhodlo se několik prodejců a vývojářů zainteresovaných v tomto projektu vyvinout jinou implementaci SETu tzv. server-based. Server-based SET model redukoval technologii, která musela být použita u obchodníka a zákazníka na "malé" moduly (obchodník) a "tenké" digitální peněženky (zákazník).

Server-based SET neukládá digitální certifikáty na zákazníkovo zařízení, což otevírá možnost použití PDA, mobilních telefonů a dalších zařízení při uskutečňování SET transakcí. Díky tomu, že tato mobilní zařízení nemají uložen žádný digitální certifikát, je nezbytné použít bezpečnostní mechanismy jako je SSL či WTSL při spojení těchto zařízení se serverem, aby byla zabezpečena dostatečná ochrana přenášených dat..

Server-based SET je, jako jakýkoliv jiný systém, založený na certifikaci, avšak má určitá omezení, např. že používá certifikáty vydané pouze jednou certifikační autoritou. Hlavním nedostatkem však u server-based SETu je neschopnost spolupráce s SSL weby, které jsou v dnešní době odpovědné za většinu platebních transakcí.

5.3.3 Card Security Code, Address Verification Service

S rostoucím tempem e-komerce rostl také počet podvodů při platbách. Tyto podvodné nákupy si díky médiím získaly velkou popularitu. Odhaduje se [26], že v současnosti počet online plateb pomocí platebních karet dosahuje 2-4% z celkového počtu transakcí pomocí platebních karet, což je relativně málo. Nicméně možný výskyt podvodné transakce je v on-line světě 12x vyšší než ve fyzickém. Proto vznikly další podpůrné bezpečnostní mechanismy, které se těmto podvodům snaží předcházet.

Jedním z nich je i tzv. **CSC** ***(Card Security Code)*** spolu s **AVS** ***(Address Verification Service)***. CSC je vytištěn na každé platební kartě na zadní straně. Pomocí tohoto zadaného kódu, který zašleme on-line vydavateli této karty na ověření, si můžeme ověřit totožnost držitele karty. Tento kód nebývá nikde ukládán ani tištěn, je pouze na samotné kartě. Jak už název napovídá, AVS ověřuje zda-li souhlasí zadaná adresa majitele karty s adresou uloženou v databázi vydavatele karty.

Je však ale na první pohled patrné, že ani tyto kontroly nedokáží úplně zabránit podvodné platbě, neboť pokud někdo zcizí majiteli jeho kartu a zná i jeho plnou adresu, může se za něj podvodně vydávat.

V roce 2001, pět let po představení SETu, začali hlavní karetní společnosti znovu vyvíjet nové autentizační standardy pro on-line platby. Tentokrát však ale ne společně, nýbrž každý zvlášť. Visa vyvinula systém nazvaný 3-D Secure a MasterCard uvedl svůj vlastní systém, který nazval Secure Paymnet Application.

5.3.4 Visa 3-D Secure ("Verified by Visa")

Toto řešení nevyžaduje, aby držitel platební karty musel používat dodatečný software na svém počítači, na druhou stranu je třeba, aby byl uživatel registrován u vydavatele své platební karty, či aby použil nějaký jiný autentizující mechanismus (např. čipová karta). V momentě, kdy zákazník zmáčkne tlačítko "koupit" na obchodníkově webu, je aktivován plug-in (na straně obchodníka), který se dotáže VISA serveru, jestli je držitel karty zapsán v databázi VISA. Jestliže ano, pak je plug-inu předána webová adresa tzv. "Issuer Access Control Serveru", kde dochází k autentizaci zákazníka. Tomu vyskočí nové okno, kde vidí detaily o transakci a zároveň tam provádí svoji identifikaci a potvrzení objednávky. Tyto údaje následně zkontroluje vydavatel platební karty a digitálně se podepíše pod objednávku, kterou vrátí obchodníkovi. Obchodník údaje zkontroluje a pošle žádost k převodu peněz. Když vše dobře dopadne, může obchodník na druhé straně po 10-15 sekundách expedovat zboží.

5.3.5 MasterCard Secure Payment Application (SPA)

V květnu 2001 MasterCard představil své vlastní řešení **SPA** ***(Secure Payment Application)***. SPA je založena na spolupráci s **UCAF** ***(Universal Cardholder Authentication Field)*** a byla navržena tak, aby minimalizovala náklady na zapojení u obchodníka. UCAF je víceúčelový mechanismus pro přenos dat implementovaný obchodníky a jejich bankami za účelem sbírání autentizujících informací generovaných zákazníky. Jakmile jsou tyto informace získány, jsou přenášeny k vydavatelům platebních karet za účelem autentizace zákazníka a autorizace platby. UCAF podporuje spoustu bezpečnostních a autentizujících přístupů, mimo SPA také např. čipové karty a další. [25]

Podobně jako u "Verified by Visa" se musí zákazník autentizovat do SPA pomocí svého hesla či čipové karty. Vydavatel platební karty musí implementovat na své straně SPA server a zajistit distribuci SPA apletů ke svým zákazníkům. SPA server je odpovědný za generování specifických bezpečnostních tokenů (unikátní pro každou transakci), které jsou posílány obchodníkům, jejich bankám a zpět vydavatelům platebních karet pro kontrolu celé transakce.Uživatelé musí používat software na straně klienta (zmíněný SPA applet), jenž komunikuje s SPA systémem. Tyto malé klientské aplety nepřenáší žádné certifikáty jako SET peněženky. SPA applet je navržen tak, aby se "probudil" až když uživatel vstoupí na SPA kompatibilní platební stránku a chce realizovat platbu.

5.4 Rizika, způsoby a nejčastější místa zneužití bankovních karet

5.4.1 Podvod ztracenou nebo zcizenou kartou

Podvody ztracenou nebo zcizenou kartou jsou podvody provedené originální platební kartou, která se dostala mimo fyzickou kontrolu oprávněného držitele.

Podvodník se snaží použít nalezenou nebo ukradenou kartu jako oprávněný držitel karty, někdy se ani nesnaží věrohodně napodobit podpis, jindy využívá i ukradených a pozměněných nebo přímo padělaných osobních dokladů. Pro případ ztráty karty je výhodné mít k dispozici fotokopii přední i zadní strany karty, která může pomoci při vyšetřování podvodu.Občas dochází k podvodnému zadržení platební karty, a to buď cíleným nevrácením karty obchodníkem (který ji může dále postoupit do řetězce podvodníků) nebo umístěním zařízení před či přímo do čtečky bankomatu, které kartu zadrží (tzv. libanonská smyčka). Většina podvodů v této kategorii se uskuteční u obchodníků dříve, než je držitelem nahlášena ztráta karty. Zneužití ztracené či zcizené karty patří v České republice mezi nejčastější kartové podvody.

Jak předcházet tomuto podvodu? Chovejte se tak, abyste minimalizovali riziko ztráty či krádeže karty: ke kartě se chovejte jako k penězům, buďte na ni opatrní; kartu nespouštějte nikdy z dohledu a v žádném případě ji nenechávejte v odložené tašce nebo oděvu na veřejných místech; uchovávejte kartu pokud možno odděleně od osobních dokladů (pro cenné věci je nejvhodnější pás na peníze nebo bezpečná vnitřní kapsa v oblečení); nosíte-li kartu v tašce, držte tašku vždy zavíráním k sobě nebo ji mějte na klíně a v žádném případě ji v restauraci nebo na jiných veřejných místech neodkládejte volně na podlahu. V případě, že ke krádeži či ztrátě karty přesto dojde, kontaktujte okamžitě vydavatele karty, aby karta mohla být zablokována. V případě krádeže karty oznamte událost také policii a požádejte o kopii protokolu.

5.4.2 Podvod padělanou kartou

Padělaná karta je karta, která byla vyrobena a personalizována bez souhlasu vydavatele nebo taková, která byla právoplatně vydána, ale později byla vizuálně upravena nebo byla pozměněna její elektronická data.

Jedním ze způsobů padělání karet je tzv. skimming, což je postup, při kterém jsou originální údaje z magnetického proužku karty elektronicky zkopírovány na jinou kartu bez vědomí právoplatného držitele karty. V prvním kroku se data zkopírují a ve druhém se nahrají na novou, padělanou kartu. [15]

Zkopírování se nejčastěji děje:

- **u obchodníků**, kde nepoctivý pracovník obchodní společnosti zkopíruje obsah magnetického proužku před vrácením karty zákazníkovi, a poté získaná data využije nebo předá dále k výrobě padělané karty
- **u bankomatu**, kde podvodníci umístí speciální kopírovací zařízení, které zkopíruje všechna data z magnetického proužku karty

Jak předcházet tomuto podvodu ? Chovejte se tak, abyste riziko podvodu minimalizovali:

Během provádění transakcí kartu pokud možno neztrácejte z dohledu, i když je platební terminál někdy z provozních důvodů umístěn mimo obslužný prostor; vždy porovnávejte výpisy transakcí s uschovanými prodejními a výplatními doklady a kontrolujte, zda nedošlo k nějakým neoprávněným transakcím; při zadávání PINu u bankomatu nebo platebního terminálu braňte jeho odpozorování a zadávejte jej diskrétně; při ukládání karet do úschovy (např. do hotelového trezoru nebo na recepci) zajistěte, aby karta nebyla volně přístupná nebo abyste poznali, zda s kartou nebylo neoprávněně manipulováno (doporučujeme kartu ukládat v zamčeném pouzdře nebo v obálce s podpisem či parafou v místě zalepení obálky).

Tento druh podvodu se v posledních letech objevuje na území České republiky stále častěji. Z dosavadních zkušeností vyplývá, že ke zkopírování údajů z magnetického proužku karty dochází nejčastěji u bankomatů, v barech, u čerpacích stanic a někdy i v hotelech. Při odhalení neoprávněné transakce kontrolou výpisu či na základě upozornění vydavatelem může být oprávněný držitel karty vyzván k jejímu odevzdání za účelem dalšího vyšetřování.

Také banky mají k dispozici řadu možností, jak čelit podvodům padělanou kartou:

- **zavedení čipových karet**, kdy po jejich úplném zavedení lze očekávat pokles výskytu podvodů s padělanou kartou, protože použitý čip zamezí kopírování údajů
- **inteligentní počítačové programy**, které mohou sledovat chování platební karty a rozpoznat neobvyklé typy transakcí.

5.4.3 Podvod bez přítomnosti karty

Podvody bez přítomnosti karty jsou takové, při kterých buď platební karta nebo držitel karty nejsou fyzicky přítomni na místě uskutečňovaného prodeje. Podvodníci využívají podvodně získaná data o platební kartě k provedení nákupu prostřednictvím písemné, telefonní, faxové nebo internetové objednávky.

Vzhledem k tomu, že obchodník nemá možnost fyzicky zkontrolovat kartu ani identitu držitele karty, je míra rizika zneužití vyšší než u běžných transakcí. U transakcí bez fyzické přítomnosti karty proto dochází ke zvýšenému výskytu neoprávněných transakcí.

Podvodníci obvykle data o kartě získávají ze zahozených nebo zkopírovaných potvrzení o transakcích, jejich podvodným vyžádáním např. e-mailem (phishing), z fiktivních internetových obchodů, vykrádáním databází s údaji o provedených transakcích (database hacking), apod. Obdobně jako u podvodu padělanou kartou se právoplatný držitel karty o podvodu nedozví, dokud neobdrží výpis s rozpisem transakcí.

Jak předcházet tomuto podvodu? Nedávejte možnost podvodníkům získat informace o vaší kartě:

Všechny doklady obsahující vaše osobní údaje nebo údaje o kartě či účtu pečlivě uschovejte. Pokud se je rozhodnete vyhodit, nejdříve je roztrhejte nebo rozdrťte. Nikdy nenechávejte svou kartu nebo doklady s jejími údaji na volně přístupných místech. Nikomu nedovolte používat vaši kartu. Používání karty neoprávněným držitelem je trestný čin.

Pro platbu kartou u obchodníka si vybírejte jen důvěryhodné obchodní společnosti. Máte-li pochybnosti, zaplaťte raději hotově. Bezprostředně po obdržení zkontrolujte bankovní nebo kartové výpisy transakcí vůči uschovaným prodejním a výplatním dokladům. Takto včas zjistíte, zda vám nejsou účtovány nerealizované transakce. Pokud na výpisu naleznete podezřelou transakci, kontaktujte ihned vydavatele karty.

Také banky dnes mají k dispozici řadu možností, jak čelit podvodům bez fyzické přítomnosti karty:

- **úplný zákaz transakcí** bez přítomnosti karty
- **omezení maximální výše transakcí** bez přítomnosti karty
- **umožnění platby bez přítomnosti karty jen na vyžádání** (dočasné odblokování na základě žádosti držitele karty a následné zablokování)
- **vydání virtuální karty se sníženými limity**, která je určena pouze pro platby bez přítomnosti karty

5.4.4 Podvod kartou ztracenou v poště

Podvod kartou ztracenou v poště je založen na zcizení karty během přepravy od vydavatele karty před tím, než ji mohl převzít právoplatný držitel karty, a jejím následném zneužití neoprávněným držitelem. Držitel karty nemá možnost zabránit vzniku této situace, ale může pomoci jejímu včasnému odhalení. V případě, že očekává zásilku platební karty (při prvním vydání karty či její obnově), která se neuskuteční v předpokládaném čase, měl by kontaktovat vydavatele karty. Ke ztracení zásilky s platební kartou dochází pouze ojediněle. Banky využívají řadu opatření, která snižují riziko zneužití takto zcizené karty: základním opatřením proti případnému zneužití zasílané karty, je odesílání platební karty v neaktivním stavu (tj. není povolena autorizace plateb). Držitel karty po jejím obdržení musí provést aktivaci dle pokynů vydavatele karty a důležitým opatřením ze strany vydavatele je také časově oddělené zaslání platební karty a PINu ve dvou samostatných zásilkách. Vydavatelé zavádějí takový způsob zasílání karet a jejich následného monitoringu, aby umožnili včasné odhalení nedoručené zásilky či případného zneužití karty. [20]

5.4.5 Podvod se zcizenou identitou

K podvodu se zcizenou identitou dochází použitím podvodně získaných osobních údajů. K využití zcizené identity může dojít dvěma způsoby:

- **podvodná žádost o kartu** – podvodník může s pomocí zcizených nebo padělaných osobních dokladů požádat o otevření účtu a vydání karty;
- **převzetí účtu** – podvodník předstírá, že je skutečným držitelem karty a pokouší se podvést banku nebo kartovou společnost. Může také požádat banku o změnu parametrů karty nebo účtu (např. adresy) a následně o vydání nové karty.

V praxi je třeba v tomto případě dávat pozor hlavně na to, jakým způsobem se zbavujete dokumentů, které obsahují osobní údaje a údaje o naší kartě či účtu.

Potvrzení o výběru z bankomatu, výpisy, informace o zůstatku na účtu a prodejní doklady uchovávejte alespoň po dobu 2 měsíců pro možnost reklamace. Před vyhozením všechny dokumenty vždy roztrhejte nebo rozdrťte, apod.

Četnost zcizování identity v poslední době narůstá. V České republice se zatím tento druh podvodu zatím prakticky nevyskytuje, přesto je však na místě zachovávání opatrnosti.

ZÁVĚR

Z výčtu uvedených identifikačních postupů a metod je zřejmé, že potřeba efektivní, jednoznačné a hlavně spolehlivé identifikace je stěžejním požadavkem moderní doby.

Jednotlivé systémy, realizované za pomoci výkonné výpočetní techniky, jsou dnes dále rozvíjeny a upravovány pro možnosti jejich cílového využití v nejrůznějších oblastech lidské činnosti. Nové identifikační technologie se miniaturizují a dostávají se i do zařízení, ve kterých bychom je ještě před několika lety ani nehledali.

Setkat se tak v praxi můžeme například s technologiemi, usnadňující automatizaci a sledování výrobních procesů, rádiové identifikace vozidel, autonomní elektronické zámkové systémy, které v rámci systémů přístupových, brání vstupu nežádoucích osob aj.

Tyto a další vzájemně provázané technologie postupně přispívají ke zvýšení komfortu a bezpečnosti při minimální provozní náročnosti, přičemž aktuálně je velká pozornost soustředěna zejména na vysoce perspektivní odvětví identifikace, a tím je – biometrie.

Největší předností biometrie oproti jiným metodám je její jednoznačnost. Charakteristické rysy každého člověka jsou unikátní a žádní dva lidé nemají například shodné otisky prstů, a to ani v případě, že se jedná o jednovaječná dvojčata. Mimo to jde také především o rychlost identifikace a určitý stupeň spolehlivosti daný nezaměnitelností vlastností toho kterého jedince a v neposlední řadě také o možnost zdokonalování samotných systémů založených na jedné vlastnosti nebo na kombinaci několika z nich.

Zvláště pak v dnešní době je zavádění těchto systémů aktuální, protože teroristé, extrémisté a zloději dovedou obcházet např. přístupové systémy. Padělání klasických přístupových systému je totiž až na výjimky poměrně jednoduché. Proto se v souvislosti s bezpečností moderních identifikačních systémů zavádějí právě biometrické systémy. Padělání biometrických systémů je totiž mnohem složitější, ale z praxe jsou již dostatečně známé příklady, které nasvědčují tomu, že ani biometrie není neomylná. A proto se zpětně v rámci biometrie začaly dále zkoumat také latentní (skryté) identifikační znaky, neboť tyto je nejobtížnější padělat či napodobit. Vědecké bádání v oblasti esoterické identifikace je tak další možnou výzvou při hledání odpovědí na otázku jednoznačného potvrzování identity.

ZÁVĚR V ANGLIČTINĚ

The enumeration of those identification procedures and methods is palpable that the lack of effective, clear and reliable identification is especially one of the most important requirement of modern times.

The system implemented with the help of powerful computer technology are now further developed and adapted to their target for use in various fields of human activity. New identification technologies are being miniaturized and get into the facility aplication in which we aren`t seek them still a few years ago.

Come across in practice we can meet, for example, with technology of facility automatization and monitoring production processes, radio frequency identification vehicles, shutting autonomous electronic systems, which in the context of access, prevents the entry of undesirable persons, etc.

These and other interrelated technologies are gradually contribute to increasing the comfort and safety at the minimum operational performance, which is currently much attention focused particularly on the highly promising sector of identification technologies, and that is - biometrics.

The biggest advantage over other biometrics methods are uniqueness. Characteristics of each person is unique, for example, noone has identical fingerprints, even in the event of twins. In addition, it`s mainly about speed and a certain degree of reliability bz the inoccupation characteristics of each subject, but also the possibility of continuing improvement in systems based on single properties or a combination of several methods.

In particular, it`s now implementing these systems up to date because terrorists, extremists and thieves can bypass the traditional access systems. Counterfeiting classic access system is an exception relatively simple. Therefore, in relation with the safety, modern identification technologies are introduced biometric systems. Counterfeiting biometric system is much more complicated, but the practice is already sufficiently well-known examples, which suggests that even biometrics is inerrable. Therefore, within the biometrics began to explore the latent (hidden) identification, because they find it hardest to imitate or faked. Scientific research in the field of esoteric identification is another possible challenge in finding an answer to the question of explicit confirmation of identity.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] Porada, Viktor a kol. *Kriminalistika*. Akademické nakladatelství CERM, s. r. o. Brno, 2001, str. 166-176. ISBN 80-7204-194-0.

[2] Šrubař, Ivo. *Identifikační systémy*. Phobos spol. s.r.o., Horní 199 - Frenštát p.R. : [s.n.], 2007. <interní materiál>. s. 2-6.

[3] Nosek, Martin. *Základní požadavky na přístupové systémy*. In: Security Magazín, Roč. XIV., vyd. 78, 4/2007. Family media, Praha, 2007,. ISSN 1210-8723.

[4] Rak, Roman. *Biometrická identifikace a verifikace*. In: Security Magazín, Roč. X., vyd. 53, 3/2003. Family media, Praha, 2003,. ISSN 1210-8723.

[5] Čandík, Marek. *Objektová bezpečnost II*. Univerzita Tomáše Bati ve Zlíně 2004, ISBN 80-7318-217-3.

[6] O'Mahony, D., Peirce, M. a Tewari, H., *Electronic Payment Systems for E-Commerce*, Second Edition, Artech House 2002, ISBN 1-58053-268-3

Internetové zdroje:

[7] Zezula, Radek. *Přístupové systémy k identifikaci osob* [online]. 2002 [cit.2008-04-05]. Dostupný zWWW:<http://www.elektrorevue.cz/clanky/02054/index.html>.

[8] Hájek, Jan. Optické kódy a RFID. *Automatizace*. 2005, roč. 48, č. 7-8 [cit.2008-03-23], Dostupný z WWW: <http://www.automatizace.cz/article.php?a=777>.

[9] Přibyl, Tomáš. *Výhody a nevýhody biometrických systémů* [online]. 2005 [cit. 2008-05-29]. Dostupný z WWW: <http://www.scienceworld.cz/sw.nsf/ID/1A9F>.

[10] Kukačka, Marek. *Využití neuronových sítí při rozpoznávání znaků* [online]. 2006 [cit. 2008-05-14]. Dostupný z WWW: <http://www.scinet.cz/neuronove-site>.

[11] Hradil, Dušan - *Od magnetu k čipu*, publikováno říjen 2006 [online]. Dostupný z WWW: <http://www.penize.cz/info/zpravy/zprava.asp?NewsID=1314>

[12] Wikipedia, otevřená encyklopedie. DNA [online]. [cit. 2007-5-24].

Dostupný z WWW: <http://cs.wikipedia.org/wiki/DNA>

[13] Rosol, Ivo. *Čipové karty* [online]. 2001 [cit. 2008-05-12]. Dostupný z WWW: <http://www.systemonline.cz/it-security/cipove-karty.htm>.

[14] Škopek, Pavel. *Poznáme tě podle očí, chůze a tvaru ucha (Co to je biometrie?):* [online]. [cit. 2004-04-11]. Dostupný z WWW<http://technet.idnes.cz/A041103>

[15] Fialová, Běla. *Nebezpečné jsou bankomaty na odlehlých místech* [online]. 1998 [cit. 2008-04-17]. Dostupný z WWW: <http://fincentrum.idnes.cz/nebezpecne-jsou-bankomaty-na-odlehlych-mistech-frj /bank.asp?c=A071024_173022_fib>.

[16] Staudek J., Hanáček P., *Bezpečné elektronické platby a SET I*, LANcom, 3, 1998, 19-25, <http://www.fi.muni.cz/usr/staudek/readings/vyuka/security/set1.ps>

[17] *MeT White Paper on Mobile Transactions*, Mobile Electronic Transaction, Ltd., Leden 2003. Dostupný z WWW: <http://www.mobiletransaction.org>

[18] *Elektronické zámkové systémy* [online]. 2004 [cit. 2008-05-18]. Dostupný z WWW: <http://www.tencom.cz/my_mobile.php>.

[19] *Základní informace o technologii RFID* [online]. 2005 [cit. 2008-03-28]. Dostupný z WWW: <http://www.rfidportal.cz/index.php?page=rfid_obecne>.

[20] *Podvody s platebními kartami* [online].2003 [cit.2008-04-27]. Dostupný z WWW: <http://www.bankovnikarty.cz/web_sbk/bezpecnost/druhy_podvodu_cz.htm>.

[21] *Lidské tělo a soukromí* [online]. 2006 [cit. 2008-05-08]. Dostupný z WWW: <http://www.bigbrotherawards.cz/node/15>.

[22] *PaySec aneb PayPal po česku* [online]. 1998 [cit. 2008-05-22]. Dostupný z WWW: <http://www.lupa.cz/clanky/paysec-aneb-paypal-po-cesku/>.

[23] *Evropský parlament, Směrnice evropského parlamentu a rady 2000/46/ES*, září 2000

[24] *Mobipay Espana - impuls pro rozvoj m-commerce*, říjen 2002 . Dostupný z WWW: <http://www.penize.cz/info/zpravy/zprava.asp?NewsID=1297>

[25] *MasterCard Secure Payment Application*, Dostupný z WWW: <http://www.mastercardintl.com/newtechnology/ecommercesecurity/spa/>

[26] *GPayments*, Dostupný z WWW: <http://www.gpayments.com/>

SEZNAM POUŽITÝCH ZKRATEK

HUMINT HUMan INTelligence

SIGINT SIGnals INTelligence

AFIS Automatic Fingerprint Information System

RFID Radio Frequency Identification

OCR Optical Charakter Recognizing

EAN European Article Numbering

ASK Amplitude Shift Keying

FSK Frequency Shift Keying

EPC Electronic Produkt Code

UHF Ultra High Frequecy

FAR False Accept Rate

FRR False Reject Rate

TTS Text-To-Speech Synthesis

DNA Deoxyribonucleic Acid

PIN Personal Identification Number

CNP Cardholder Not Present

WAP Wireless Application Protocol

SSL Secure Sockets Layer

SIM Subscribe Identity Module

WIM Wireless Identity Module

SET Secure Electronic Transaction

CSC Card Security Code

AVS Address Verification Service

SEZNAM OBRÁZKŮ