Trendy vývoje identifikačních prostředků osob

The trend analysis of a person identification equipment

Bc. Kamil Zobaník

Diplomová práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

*** nascannované zadání str. 1 ***

*** nascannované zadání str. 2 ***

ABSTRAKT

Diplomová práce je zaměřena na identifikační prostředky osob a možnosti jejich využití v oblasti naplnění bezpečnostní politiky organizace. V práci je provedeno hodnocení slabin a předností jednotlivých kategorií identifikačních prostředků. Vlastnosti současně využívaných identifikačních prostředků mají některé své zápory, které zajisté v budoucnosti odstraní nastupující řada identifikačních prostředků, které již budou lépe vyhovovat vysokým nárokům na bezpečnost jejich odběratelům. Práce se zabývá vývojovými trendy identifikačních prostředků aplikovaných do několika různých sfér využití s výhledem do budoucnosti a jejich použitím v oblasti naplnění bezpečnostní politiky organizace.

Klíčová slova: bezpečnostní politika organizace, čipové karty, tokeny, identifikační prostředky, biometrie

ABSTRACT

The main aim of this dissertation is to identify identification resources and their application in terms of sufficient implementation of occupation safety. Also, it focuses on evaluation of benefits and drawbacks of identification resources. It has been analysed before that current identification resources are distinguished by certain weaknesses, which are considered to be eliminated by impending identification resources. The main reason for innovative studies in this area is to comply with high expectances of customers. Finally, this dissertation deals with trends of possible development of identification resources from different points of view.

Keywords: security policy of organization, chip cards, tokens, identification resources, biometrics

Děkuji vedoucímu mé diplomové práce doc. Ing. Luďku LUKÁŠOVI, CSc. za odborné vedení, za materiálovou podporu a informace, a také za rady, návrhy a připomínky během zpracování diplomové práce.

Prohlašuji, že jsem na diplomové 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 …….

Podpis diplomanta

OBSAH

ÚVOD

S rostoucí kriminalitou a potřebou zabezpečit osoby, majetek a informace, vzrostly také nároky na způsob zabezpečení přístupů do objektů. Vzniká zde také poptávka v oblasti průmyslu po automatické identifikaci osob vstupujících do různých chráněných prostor. Osobám, které pracují nebo se pohybují v organizaci, jsou přidělena přístupová práva. Po jejich identifikaci při vstupu do objektu některým z identifikačních prostředků a jejich úspěšné autentizaci, se automaticky provede odblokování prostředků a prostor, nacházejících se uvnitř zařízení. Během pohybu osob v takto zabezpečené budově je také často využívána možnost informovat se o poloze a pohybu každé z přihlášených osob. Vzhledem ke skutečnostem, že se osoby pohybující v objektu neustále někde identifikují a některé identifikační prostředky potřebují pro jejich autentizaci biometrické údaje nebo jiná osobní data, tak bývá vytvořena databáze osob, ve které jsou tyto údaje shromážděny. Vzniká tak ovšem riziko spojené s únikem informací a tím i nutnost pracovat se zákonem o ochraně osobních údajů. Cílem této práce je zhodnotit soudobé i perspektivní identifikační prvky, jejich vlastnosti a parametry a vhodným výběrem identifikačních prostředků spolehlivě naplnit bezpečnostní politiku organizace.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Bezpečnostní politika organizace je základní písemný dokument organizace, definující hlavní bezpečnostní požadavky a nařízení s cílem zajistit ochranu a bezpečnost aktiv organizace. Jejím účelem je jasně vymezit co chce organizace chránit, proti čemu a jakým způsobem se bude ochrana realizovat. Stanovením bezpečnostní politiky organizace se rozumí organizační a řídící akty, normy, pravidla, pokyny, nařízení, technologické vybavení, jejichž cílem je maximálně ochránit danou organizaci proti ztrátám, rozkrádání, vloupání, krádežím, ale i jiným nekriminálním jevům ohrožujícím stabilní a bezproblémový chod organizace.

Základními narušiteli stability organizace jsou havárie, požáry, únik důležitých informací, výpadky provozu, selhání lidského faktoru a podobné situace. Z hlediska řízení organizace sem také patří informace o ohrožení subjektu organizace. Stanovují se bezpečnostní, provozní a obchodní rizika ohrožující chod organizace. Koncepce s návrhy k ochraně organizace v rámci technických, technologických, organizačních, personálních a informačních problémů. [1]

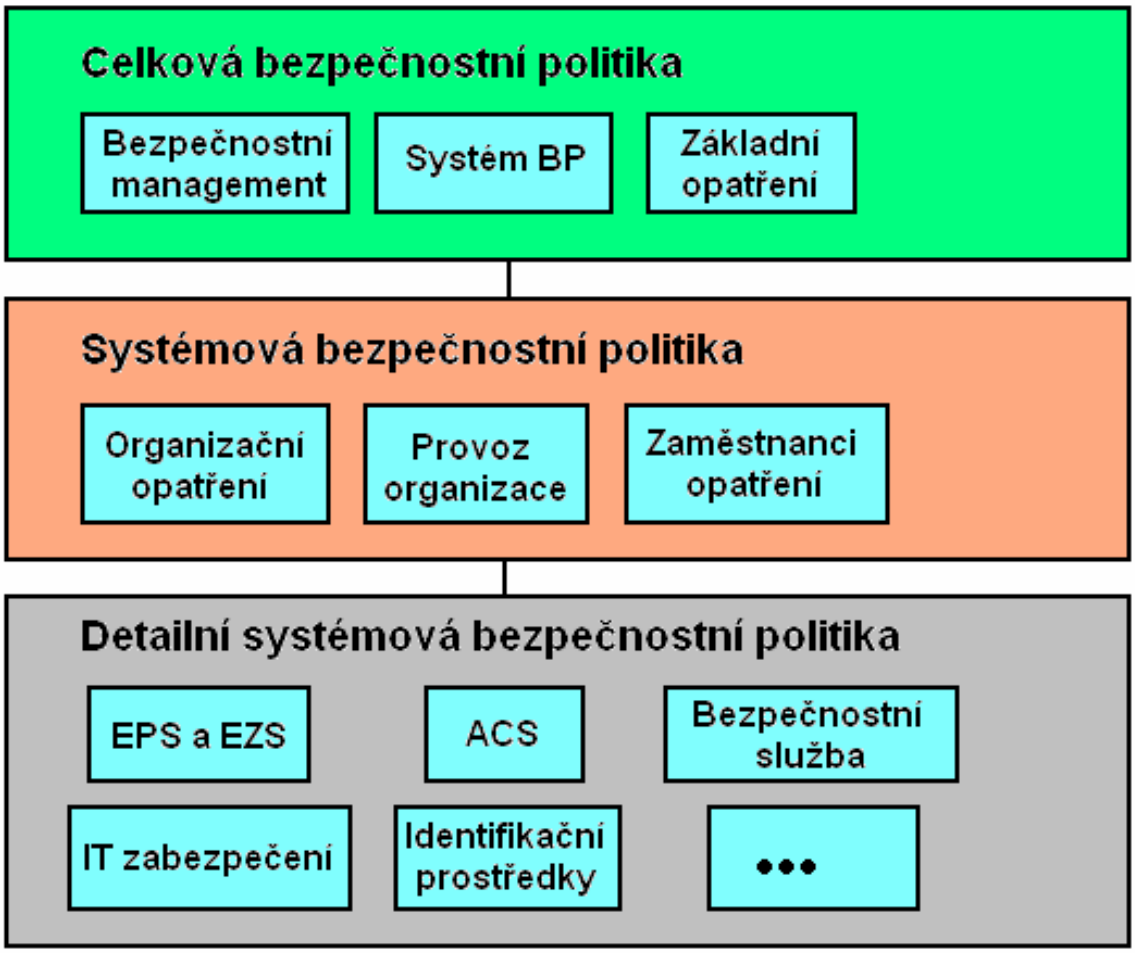
Bezpečnostní politika organizace odráží také přístup organizace k řešení jednotlivých oblastí bezpečnosti, kterými jsou bezpečnost osob, informací, majetku a ochrana životního prostředí. Definuje organizační a systémová opatření, kde mohou být zahrnuty také konkrétní nástroje a technologie, které jsou použity k realizaci bezpečnostních opatření v organizaci. Hlavním pilířem bezpečnosti a stability podniku je tedy stanovení koncepce bezpečnostní politiky organizace, což je jeden z nosných dokumentů podniku, který je součástí řídících dokumentů managementu. Některé organizace mající pod sebou další podřízené organizace zpracovávají tzv. doktrínu. Doktrína je písemný dokument obsahující bezpečnostní zásady, které slouží k realizaci a vymezení pravidel bezpečnostní politiky. Takto zpracovaná směrnice je pak závazná pro všechny podřízené právní subjekty. Směrnice je navíc závazná i pro některé dodavatele, subdodavatele a spolupracující subjekty. [1]

Bezpečnostní politika organizace má mít charakter povinných nařízení, které může měnit pouze velice úzká skupina lidí (zejména vedoucí organizace na návrh bezpečnostního manažera). Určitá bezpečnostní doporučení mohou mít také významní majitelé aktiv organizace. Každý podnik aniž by si to uvědomoval, má svoji bezpečnostní politiku, i když

to tak v mnoha případech nenazývá. Jestliže řídící pracovník podniku dá pokyn „každý den ve 22 hodin se bude uzamykat vstupní brána“, jde už o stavbu bezpečnostní politiky, nejde však o „koncepci bezpečnostní politiky“ jako takové. Kvalifikovaný a zkušený management podniku mezi prvními z činností řízení při vzniku podniku stanoví svoji bezpečnostní politiku. [1]

Pro vypracování dokumentu bezpečností politiky organizace existuje několik různých přístupů. Dokumenty pro specifikaci bezpečnostní politiky organizace a její úspěšnou implementaci do praxe je doporučeno zpracovávat podle následujícího schématu.

- Celková bezpečnostní politika
- Systémová bezpečnostní politika
- Detailní systémová bezpečnostní politika (technická bezpečnostní politika)



Obr. 1. Schéma pro zpracování bezpečnostní politiky

1.1 Přínosy zpracování bezpečnostní politiky

Dokumentace popisuje stav bezpečnosti organizace v jednotlivých oblastech. Definuje aktiva organizace, jejich důležitost pro organizaci a způsob nakládání s nimi. Navrhuje základní ochranná opatření, jejichž použití může přinést výrazný efekt zvýšení bezpečnosti. Velmi často patří do těchto opatření organizační změny a definování zodpovědnosti na jednotlivých pozicích v organizaci. Analýza bezpečnostní politiky slouží zároveň jako podklad pro definování, vypracování a vyhlášení bezpečnostní politiky organizace jako nosného dokumentu. Součástí je také návrh základních nápravných opatření. Samotný fakt, že organizace zpracovává studii bezpečnostní politiky, signalizuje vážný zájem organizace zabývat se její bezpečností. Komplexní přístup ke všem aspektům bezpečnosti ukazuje i na vazby uvnitř organizace a její fungování. Pokud chce být organizace při zpracování bezpečnostní politiky opravdu objektivní měla by analýzu bezpečnosti organizace z části přenechat na nezávislé organizaci. Pohled zvenčí často odhalí a pojmenuje chyby, o kterých se uvnitř organizace může vědět, ale nemluví se o nich. [2]

Jedním z možných způsobů, jak získat podklady k dokumentaci bezpečnostní politiky organizace je ten, že organizace vytvoří neformální pracovní skupinu, sestavenou z odpovědných pracovníků jednotlivých oblastí, jichž se bezpečnost dotýká a externího zpracovatele studie. Tato skupina postupně prochází a analyzuje, kde by měla být v organizaci zavedena nová bezpečnostní opatření. Je možné, že tato skupina může využívat komunikace s ostatními zaměstnanci organizace, aby se nalezlo vhodné řešení aktuálního problému a zavedlo se nové bezpečnostní opatření. Informace se získávají analýzou současného stavu bezpečnosti uvnitř organizace, která se může provádět formou pohovorů s jednotlivými pracovníky a také vhodně sestavenými dotazníky. [2]

1.2 Zpracování bezpečnostní politiky

1.2.1 Analýza aktiv

Analýza aktiv vymezuje, co chce organizace chránit tedy aktiva. Bývají to zdraví a život osob, data a informace, cennosti a majetek, znalosti, technologie a know how. Aktivem je vše, co má pro organizaci hodnotu. Správné řízení aktiv je pro úspěch organizace životně důležité a je hlavní odpovědností všech úrovní řízení. [2]

Aktiva organizace zahrnují:

- fyzická aktiva (majetek, vybavení organizace,…)
- informace (dokumenty, databáze,...)
- schopnost vytvářet určité produkty nebo poskytovat služby
- pracovní sílu, školení pracovníků, znalosti zaměstnanců, zapracování apod.
- nehmotné hodnoty (např. abstraktní hodnota firmy, software, image firmy, dobré vztahy s okolními organizacemi a místním prostředím atd..)

Většina nebo všechna z těchto aktiv mohou být považována za dostatečně cenná na to, aby si zasloužila určitý stupeň ochrany.

1.2.2 Analýza hrozeb

Analýza hrozeb vymezuje, proti jakým hrozbám chceme aktiva chránit. Mezi tyto hrozby patří útoky na majetek a zdraví osob a ostatní aktiva organizace. Další hrozbou je zneužití dat a informací k poškození organizace nebo jejich klientů, narušení chodu a stability podniku. Aktiva jsou předmětem mnoha typů hrozeb. Hrozba má schopnost způsobit nežádoucí jev, který může mít za následek poškození systému nebo organizace a jejích aktiv. Hrozby mohou mít přírodní nebo lidský původ a mohou být náhodné nebo úmyslné. Škoda způsobená vlivem uskutečněné hrozby může být dočasné povahy nebo může být trvalá, jako je tomu v případě zničení, nebo nevratného poškození aktiv. [2]

Velikost škody způsobené hrozbou se může při každém výskytu značně měnit. Havárie či přírodní katastrofa nebo selhání lidského faktoru může způsobit různě velkou škodu v závislosti na jejich intenzitě. Takové hrozby mají často přiřazen i stupeň síly, která je s nimi spojena. Hrozba může být destruktivní nebo nedestruktivní.

1.2.3 Analýza zranitelnosti

Zranitelnost chápeme jako slabá místa v systému, která mohou být hrozbou využita a mohou vést k nežádoucím následkům. Jsou to příležitosti, které mohou umožnit hrozbě, aby způsobila škodu. Například absence mechanizmu řízení přístupu a identifikačních prostředků zvýší zranitelnost na takovou úroveň, že by mohla umožnit naplnění hrozby nežádoucího proniknutí k množství aktiv a jejich ztrátu. Tomuto se snažíme zabránit použitím co nejkvalitnějších identifikačních prostředků. Analýza zranitelnosti se zabývá zkoumáním slabých míst, která mohou být využita identifikovanými hrozbami. Zranitelnost konkrétního systému nebo aktiva vůči určité hrozbě je vyjádřením o jednoduchosti, se kterou může být systém nebo aktivum poškozeno. [2]

1.2.4 Analýza dopadů

Dopad je důsledek naplnění nežádoucího jevu, způsobeného buď náhodně nebo úmyslně, který má vliv na aktiva. Následky mohou mít podobu zničení určitých aktiv, poškození organizace, ztráty důvěryhodnosti, dostupnosti, autenticity, individuální zodpovědnosti nebo spolehlivosti. Měření dopadů umožňuje vytvoření rovnováhy mezi výsledky nežádoucích incidentů a náklady na ochranná preventivní opatření s ohledem na četnost jejich výskytu.

Kvantitativní a kvalitativní měření dopadů se provádí:

- stanovením finančních nákladů
- přiřazením empirické stupnice síly

1.2.5 Analýza rizik

Analýza rizik vymezuje, jaká rizika hrozí sledovaným aktivům. Analyzuje se jak velká jsou tato rizika, proti kterým organizace aktiva chrání. Do analýzy nezbytně patří i kolik je ochotna organizace investovat do eliminace těchto rizik. Riziko je potenciální možnost, že daná hrozba využije zranitelnosti, aby způsobila ztrátu nebo poškození aktiv nebo skupiny aktiv, a tedy přímo nebo nepřímo organizace. Riziko je charakterizováno jako kombinace dvou faktorů, pravděpodobností výskytu nežádoucího incidentu a jeho dopadu. Analýza rizik tedy dále zpřesňuje odhad dopadů v závislosti na jejich četnosti s využitím statistik

výskytu nežádoucích incidentů a ukazuje na místa, kde je nutno aplikovat ochranná opatření a jaké investice na jejich implementaci jsou adekvátní. [2]

1.2.6 Stanovení omezení

Omezení stanovují obvykle řídící pracovníci organizace a jsou ovlivněna prostředím, ve kterých organizace vyvíjejí svoji činnost.

Některá omezení, která by měla být vzata v úvahu:

- organizační
- finanční
- personální
- právní
- technická

Tyto faktory musí být při výběru a implementaci ochranných opatření vzaty v úvahu. Časem, sociálním vývojem a kulturou organizace se mohou omezení měnit stejně tak, jako se mění potenciál hrozby, proto musí být prováděny periodicky stále nové revize.

Výsledkem těchto analýz je návrh protiopatření a vymezení rozpočtu organizace na jejich realizaci. Mezi protiopatření může patřit zavedení některé z následujících technologií. [2]

1.2.7 Protiopatření

Protiopatření jsou činnosti, nařízení a technické vybavení, které mají snížit riziko, že se hrozba naplní. V případě, kdy dojde k naplnění hrozby, závisí na protiopatřeních, aby se snížil její dopad na minimum, popřípadě aby následky vůbec nebyly znát. Protiopatření tedy chrání aktiva organizace a náklady na protiopatření nikdy nesmí překročit cenu aktiv, která chrání.

Příklady protiopatření:

Elektrická zabezpečovací signalizace (EZS) – slouží k zabezpečení objektu proti vloupání

Elektrická požární signalizace (EPS) – slouží k zabezpečení objektu proti požáru

Přístupové a docházkové systémy (ACCESS) – slouží k evidenci a identifikaci osob

Uzavřené střežící a dohlížecí televizní okruhy (CCTV) – doplňuje systémy EZS a ACCESS

Identifikační prostředky osob - jsou součástí systému ACCESS, využívají především identifikačních karet nebo RFID tokenů

Biometrické identifikační systémy – jsou součástí systému ACCESS využívají k rozpoznání osob nezaměnitelných biometrických vlastností

Elektronické označování aktiv – slouží k označování majetku organizace, nejčastěji se využívají čárové kódy a RFID tokeny

Ochrana dat a informací (PKI) – slouží k zabezpečení komunikace po datové síti a také k ochraně dat uvnitř počítače [1]

II. PRAKTICKÁ ČÁST

2 IDENTIFIKAČNÍ PROSTŘEDKY OSOB

Identifikační prostředky slouží k rozpoznání osob, zvířectva, přepravovaného zboží, prodejních artiklů a různých dalších předmětů. Jejich použitím získáme přehled nad některými informacemi o autorizovaných věcech, zvířatech nebo osobách. V historii lidstva se jako jedny z prvních identifikačních prostředků začaly používat hesla. Účelem jejich použití bylo rozpoznat nepřátele, protože ve větších armádách nebo společenstvech nebylo možné znát okolo sebe všechny osoby patřící do společenstva. Jako první z identifikačních předmětů se tedy používaly amulety a pečetě. Využívaly se nejčastěji k označování zpráv nebo zásilek. Pokud byla pečeť porušena, byla zpráva považována za nedůvěryhodnou. Pečetě a amulety dávaly adresátovi informaci o tom, kdo zprávu poslal. V současné době doplnily tyto identifikační prostředky novější technologie.

2.1 Využití identifikačních prostředků v oblasti naplnění bezpečnostní politiky organizace

Jednoznačně velice důležitým a účinným prvkem v oblasti naplnění bezpečnostní politiky organizace jsou právě přístupové systémy (ACCESS), ve kterých se dnes využívá veliké množství identifikačních prostředků. Použitím identifikačních prostředků získáme silnou kontrolu nad děním v organizaci. Co však také získáme se zavedením přístupových systémů je levnější provoz, ušetření drahé pracovní síly, kterou by jsme jinak potřebovali na kontrolu osob, také získáme výhodu předejít selhání lidského faktoru v oblasti sebe obohacování na úkor firmy.

S použitím identifikačních prostředků zaručíme také přehled nad aktivy organizace, jako je její vybavení, hardware a jiná pro organizaci důležitá aktiva. Fyzická aktiva organizace jednoduše označíme identifikačními prostředky ideálně RFID tokeny, které při průchodu okolo terminálu signalizují co se právě pokouší vynést z místnosti či budovy, ale díky ochraně dveří a vynucené identifikaci osob k jejich otevření se dozvíme také kdo označenou věc přenáší.

3 DRUHY IDENTIFIKAČNÍCH PROSTŘEDKŮ

Identifikační prvky můžeme rozdělit na takové, kde potřebujeme mít nějaký identifikační předmět a na druhou skupinu, do které budou patřit identifikace heslem a identifikace založená na biometrii, která je uložena v databázi.

3.1 Historické identifikační prostředky

Hesla a znaky

Amulety a pečetě

3.2 Soudobé identifikační prostředky

Heslo nebo PIN

Čárové kódy 1D, 2D a 3D

Tokeny a čipové karty

Biometrické identifikační prostředky

Ve své diplomové práci uvádím pouze identifikační prostředky, které si lidé neuchovávají pouze ve své hlavě, ale mají je vždy sebou jako fyzický předmět nebo část těla. Analyzuji soudobé identifikační prostředky, ze kterých uvádím identifikační karty, tokeny a biometrické identifikační prostředky.

4 ČÁROVÉ KÓDY

Čárové kódy byly vyvinuty, aby zautomatizovaly proces označování a registrace předmětů a usnadnily jejich identifikaci. Až později se začalo využívat čárových kódů také v oblasti identifikace osob. Jejich vznik je datován na první polovinu 20. století a jejich masové rozšíření na druhou polovinu 20.století. Současně existují stovky druhů čárových kódů, ale pouze málo z nich se dočkalo masového nasazení a využití. Čárové kódy se současně využívají v případech, kdy má organizace zavedený fungující systém a nechce investovat do nového bezpečnějšího systému. Karty, které obsahují pouze čárový kód mají velice nízké pořizovací náklady. Takovéto jednoduché zabezpečení se využívá například ve vzdělávacích organizacích, kde se počítá s krátkou dobou jejich životního cyklu a velkým množstvím vydaných karet. Čárové kódy spadají do oblasti automatické identifikace neboli registrace dat bez použití kláves. Do této oblasti se také zařadily magnetické kódy používané na kreditních kartách, ale také standardizované strojově čitelné písmo s technologií OCR. Tato technologie se stala doplňkem pro identifikační karty, takže se s ní na identifikačních kartách můžeme setkat. Přidanou hodnotou, kterou nám použití doplňkových technologií na identifikačních kartách přináší je možnost dohledání majitele karty a nebo automatizace při výrobě a vydávání identifikačních karet. Navíc jak zde bylo uvedeno můžeme karty s čárovým kódem využívat jako jednoduchou a levnou možnost identifikace osob. [3]

4.1 Charakteristika a funkce čárových kódů

Většina kódů se skládá z tmavých čar a ze světlých mezer (1D a 2D kódy), které se čtou pomocí snímačů vyzařujících zpravidla červené světlo. Toto světlo je pohlcováno tmavými čarami a odráženo světlými mezerami. Snímané jsou tedy rozdíly v reflexi, které snímač přeměňuje v elektrické signály odpovídající šířce čar a mezer. Tyto signály jsou převedeny v číslice nebo písmena, jaká obsahuje příslušný čárový kód. To tedy znamená, že každá číslice či písmeno je zaznamenáno v čárovém kódu tak, že se předem přesně nadefinují šířky čar a mezer. Data obsažená v čárovém kódu mohou zahrnovat takřka cokoliv: číslo výrobce, číslo výrobku, místo uložení ve skladu, číslo série nebo také jméno osoby, které je třeba povolen vstup do standardně uzavřeného prostoru. [3]

Přesnost

Užití čárových kódů je jedna z nejpřesnějších a rychlých metod k registraci velkého objemu dat. Při ručním zadávání dat dochází k chybě průměrně při každém třístém zadání, při použití čárových kódů se počet chyb snižuje až na jednu milióntinu. Tyto chyby se dají navíc eliminovat, je-li do kódu zavedena kontrolní číslice, která ověřuje správnost čtení ostatních číslic. Spolehlivost proti záměně kódu se osvědčila v mnoha zemích vybavením transfuzních stanic čárovými kódy, aby byli stoprocentně rozlišeni rozdílní dárci a následně nemohla být použita pro pacienta nevhodná krev. [3]

Rychlost

Testováním bylo zjištěno, že v porovnání s ručním zadáváním kódu přes klávesnici je i ta nejlepší písařka nejméně třikrát pomalejší než jakýkoliv běžný snímač. [3]

Flexibilita

Čárové kódy je možné tisknout na materiály odolné vysokým teplotám nebo naopak extrémním mrazům, na materiály odolné kyselinám a odolné nadměrné vlhkosti. [3]

Produktivita a efektivita

Využíváním čárových kódů v supermarketech se produktivita při odbavování zákazníků u pokladny zvýší nejméně o 30 %. Kromě toho je možno v jakémkoliv okamžiku zjistit stav skladových zásob jednotlivého zboží. Studie zpracovaná pro americké Ministerstvo obrany ukázala, že v některých oblastech se při zavedení čárových kódů zvýší efektivita práce až o 400 %. [3]

4.2 Typy čárových kódů a jejich rozdělení

1D čárové kódy – snímá se šířka čar a šířka mezer mezi čarami

2D čárové kódy – snímá se šířka a délka čar a také šířka a délka mezer mezi čarami

3D čárové kódy – využívají opět dvou rozměrů, ale jiného principu snímání

4.2.1 1D čárové kódy

U těchto kódů je informace uložena na úsečce a výška kódu je z důvodu opravy možného mechanického poškození, nebo částečné chybě při tisku kódu. Je definováno několik mezinárodních standardů, které se využívají v různých výrobních a spotřebních odvětvích.

EAN

Čárový kód EAN je jedním z nejznámějších typů kódování u nás. V naší oblasti se konkrétně používá EAN 13 a jeho kratší varianta EAN 8, kterými se označuje zboží běžně obchodované v obchodních řetězcích (EAN = European Article Numbering = evropské číslování zboží). Čárový kód EAN dokáže kódovat číslice 0 až 9, přičemž každá číslice je kódována dvěma čárami a dvěma mezerami. Může obsahovat buďto 8 číslic (EAN-8) nebo třináct číslic (EAN-13). První dvě nebo tři číslice vždy určují stát původu (např. ČR má číslo 859), dalších několik číslic (většinou čtyři až šest) určují výrobce a zbývající číslice kromě poslední určují konkrétní zboží. Poslední číslice je kontrolní, která ověřuje správnost čtení při dekódování. Čísla jednotlivým státům přiděluje sdružení EAN International se sídlem v Bruselu. Nasazení standardizovaného kódu řídí registrační organizace každé země (u nás sdružení GS1 Czech Republic – donedávna EAN ČR). Tím, že přidělování kódů EAN řídí registrační autorita je dosaženo jedinečnosti označení zboží = žádný jiný druh zboží na světě nemůže být označen stejným čárovým kódem. [3]

Obr. 2. EAN-13

Obr. 3. EAN-8

Code 39

Velmi rozšířený kód používaný v nejrůznějších aplikacích s výjimkou maloobchodu. Je přizpůsoben jako norma v automobilovém průmyslu, ve zdravotnické službě, v obraně a v mnoha dalších odvětvích průmyslu a obchodu. Je schopen kódovat číslice 0 až 9, písmena A až Z a dalších sedm speciálních znaků, přičemž každý znak je reprezentován pěti čárami a čtyřmi mezerami. Analýza pravděpodobnosti chyby odhaduje, že při užití Code 39 může dojít k chybě dekódování až po přečtení cca 30 miliónů znaků. [3]

Obr. 4. Code 39

Interleaved 2 z 5

Tento kód dovoluje vysokou hustotu zápisu (až 8 znaků na 1 cm). Je často využíván v nejrůznějších odvětvích průmyslu pro interní aplikace. Jeho speciální standardizovaná verze ITF-14 patří rovněž do systému UCC/EAN, kde se používá pro označování obchodních jednotek. Dokáže kódovat číslice 0 až 9, přičemž každá číslice je reprezentována buď pěti linkami nebo pěti mezerami. Jednotlivé znaky se kódují v párech, tzn. že první znak daného páru se kóduje linkami a druhý znak mezerami mezi tyto linky umístěnými, takže kód ITF musí vždy obsahovat sudý počet znaků. [3]

Obr. 5. ITF-14

Obr. 6. Interleaved 2 z 5

Codabar

Tento kód je mezinárodně využíván pro označování krevních bank v transfuzních stanicích. Je prakticky jedním z nejstarších čárových kódů. Je schopen kódovat číslice 0 až 9 a šest speciálních znaků. Každý znak je reprezentován čtyřmi čarami a třemi mezerami a nabízí výběr čtyř znaků začátku a konce, které se mohou využít pro oddělení typů dat. [3]

Obr. 7. Codabar

4.2.2 2D čárové kódy

S narůstajícími nároky na objem dat, které je nutno do čárových kódů zakódovat, byly vyvinuty koncem 20. století 2D čárové kódy, které jsou oproti běžným 1D čárovým kódům složitěji konstruovány a složitěji čitelné. U těchto kódů je informace uložena v rámci matice. Dvojdimenzionální kódy nesou informaci jak v horizontálním tak i ve svislém směru. Původně byly dvojdimenzionální kódy vyvinuty pro průmyslové aplikace, kde byl požadavek uložit velké množství dat na malé ploše. První použití se nalezlo na obalech v lékařském a elektrotechnickém průmyslu, kde byla právě malá využitelná plocha hlavním omezením. Mnohem později se 2D kódy prosadily i v aplikacích, kde prostor nebyl omezením. V současnosti je k dispozici asi tak 20 různých 2D symbolik. Některé z těchto kódů sebou nesou všechny údaje a jsou tak nezávislé na vnějším systému. Mají v sobě také často integrovány samo-opravné kódy. Mezi tyto kódy patří PDF-417, Aztec a další. [3]

Rozdělení 2D čárových kódů podle způsobu uložení informace

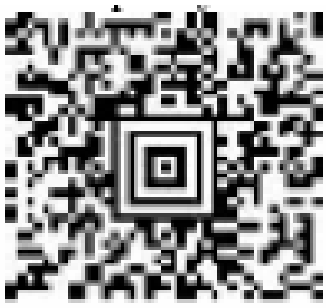
Skládané (stacked) a víceřádkové symboliky - vznikají složením jednodimenzionálních kódu skládajících se z čar a mezer proměnné šířky.

Maticový kód (Matrix code) - označuje 2D kódy, kde jsou data definována dvojrozměrnými souřadnicemi tmavých bodů v matici. Všechny body v matici mají pevný rozměr.

Ordinální čárový kód - je vertikálně redundantní, což znamená že ve svislém směru jsou uložena tatáž data. V podstatě se tedy jedná o jednorozměrný kód. Výška takovýchto sloupců může být zmenšena bez ztráty informace a má jen bezpečnostní funkci. Čím vyšší budou sloupce, tím vyšší je pravděpodobnost, že kód bude čitelný i při porušení. [3]

Aztec Code

Aztec Code byl vyvinut s důrazem na snadný tisk a jednoduché dekódování. Symboly jsou čtvercového tvaru ve čtvercové mřížce a s čtvercovým zaměřovačem (bullseye) uprostřed symbolu. Nejmenší rozměr Aztec Code tvoří čtverec o 15x15 modulech a největší o rozměrech 151x151 modulech. Nejmenší čárový kód Aztec Code kóduje 13 čísel nebo 12 písmen. Největší kód Aztec Code kóduje 3832 čísel, 3067 písmen nebo 1914 bajtů dat. Při tisku symbolu není třeba bílé ohraničení okolo symbolu. Je celkem definováno 32 rozměrů a jejich uživatel si může zvolit Reed-Solomonovo chybové kódování v rozsahu 5% - 95% datové oblasti. Doporučená úroveň je 23% datového prostoru plus 3 kódová slova. Kódovat lze všech 8-bitů. Hodnoty 0 - 127 jsou interpretovány jako znaky sady ASCII, zatímco hodnoty 128 - 255 jsou interpretovány jako ISO 8859-1, Latin Alphabet No. 1. Dále lze dekódovat dvě slova mimo datovou oblast. [3]



Obr. 8. Aztec Code

PDF-417

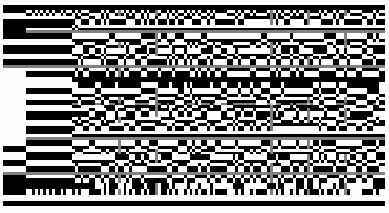
Verze 2D čárového kódu s velmi vysokou informační kapacitou a schopností detekce a oprav chyb (při porušení kódu). PDF 417 je patentem firmy SYMBOL. Označení PDF 417 (Portable Data File) vychází ze struktury kódu. Každé kódové slovo se skládá ze 4 čar a 4 mezer o šířce minimálně jednoho a maximálně šesti modulů. Celkem je však modulů ve slově vždy přesně 17. Na rozdíl od tradičních čárových kódů, které obvykle slouží jako klíč k vyhledání údajů v nějaké databázi externího systému, si PDF 417 nese všechny údaje s sebou a stává se tak nezávislým kódem na vnějším systému. Kódem PDF 417 lze zakódovat běžný text, grafiku a navíc speciální programové instrukce. Velikost datového souboru může přitom být až 1,1 kB. Příkladem použití mohou být nejrůznější identifikační karty, řidičské průkazy (v některých státech USA), PDF 417 se využívá i pro kódování diagnózy pacientů. [3]

Výhody: Lze je tisknout a přenášet na levném médiu tedy papíru. Korekce chyb na tak vysoké úrovni, že můžeme bezchybně dekódovat kód, který je až z 50 % fyzicky poškozen.

Obr. 9. PDF-417

Datastrip Code

Datastrip Code byl vytvořen v Softstrip Systems. Jedná se o nestarší symboliku z dvourozměrných symbolik. Jedná se o patentovaný kódovací a snímací systém umožňující tisk dat, grafiky a digitalizovaného zvuku na papír ve velmi komprimovaném formátu a následné jej bezchybně číst počítačem. Kódování Datastrip Code obsahuje paritu pro každé kódové slovo, zajišťuje vysokou spolehlivost a odolnost proti chybám. [3]



Obr. 10. Datastrip Code

Super Code

Super Code byl vytvořen Y. Wangem v roce 1994. Symbolika používá rámcovou strukturu (paket) rozdílnou od struktury víceřadé symboliky. Jsou zde předepsány přesnosti v horizontálním umístění symbolu v paketu, ale je zde mnohem větší volnost v umístění paketu horizontálně a vertikálně než u víceřadých symbolik. Maximální počet znaků na symbol při nejnižší úrovni chybové korekce je 4083 alfanumerických znaků, 5102 číslic nebo 2546 bytů. Symboly čárového kódu Super Code obsahují kódová slova pro opravu kódu založena na Reed-Solomonovu algoritmu opravy chyb, který slouží nejen k nalezení chyb, ale také k opravě chybně dekódovaných nebo vynechaných kódových slov. Uživatel si může vybrat jednu ze 32 úrovní opravy chyb. [3]

Obr. 11. Super Code

Code 49

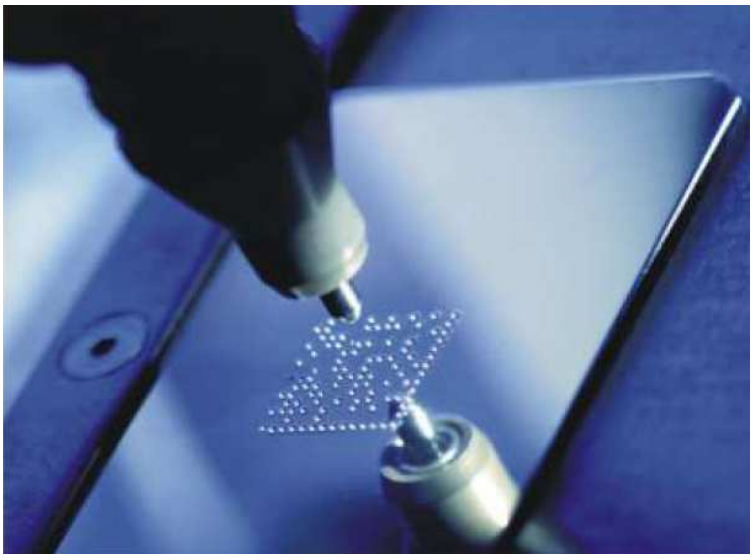
Code 49 vytvořil David Allaisem v roce 1987 v Intermec Corporation. Code 49 splnil vývojový požadavek firmy na uložení velkého množství dat na poměrně malou plochu pomocí složení několika symbolů čárových kódů nad sebou. Každý symbol může být složen ze 2 až 8 řad. Každá řada je složena z úvodní prázdné oblasti, start oblasti, 4 datových slov kódujících 8 znaků s posledním znakem ve funkci kontrolního znaku řady, stop oblasti a konečné prázdné oblasti. Každá řada kóduje data do 18 čar a 17 mezer a každá řada je oddělena proužkem o šíři jednoho modulu. Kód je spojitá symbolika proměnné délky, která umí kódovat kompletní 128 znakovou ASCII tabulku. Kód lze skenovat pomocí ručního laserového snímače nebo CCD snímačem. [3]

Obr. 12. Code 49

4.2.3 3D čárové kódy

Jde o běžný čárový kód, který se liší technologií tisku a jeho snímáním. Využívá se zde hloubky záznamu, tedy je Embosovaný (vytlačen jako kód na platební kartě do bankomatu). Snímání se pak provádí na změně výškových rozdílů (nejde vůbec o jasové snímání kontrastu, takže barva značení není důležitá). Tyto kódy se využívají v mechanicky namáhaných aplikacích. Běžně se nazývají jako hloubkové čárové kódy.

Nejčastěji se využívá technologie značení mikroúderem a značení laserem. Značení je mechanicky velmi odolné, viditelné i pod vrstvou barvy, s velmi vysokou rychlostí značení. Tyto vlastnosti předurčují tuto mikroúderovou technologii k aplikacím pro označování mechanicky namáhaných materiálů a výrobků. Jde o kontaktní značení, kdy hrot vysokou frekvencí kmitání a tlakem vytváří písmo, nebo grafiku v podstatě do jakéhokoliv povrchu. Pro svou odolnost je 3D značení velmi často využíváno v automobilovém průmyslu, kde se prosazuje schopnost značit 2D kód do hloubky, který pojme mnohem více informací na malou velikost plochy v porovnání s 1D čárovým kódem. Značící zařízení je navrženo speciálně pro kontaktní značení na plastové, kovové, dřevěné a skleněné povrchy. Mikroúderové značící zařízení nabízí nesmazatelné, kyselinám a olejům odolné, opticky velmi dobře viditelné značení. Tisk 3D kódů má výhodu, že není potřeba žádné médium, protože se kód vytlačuje přímo do označované věci. Využívají se 2D kódy s vysokou hustotou záznamu dat na malé ploše. [3]



Obr. 13. Ukázka tisku 3D kódu na kovovou plochu

Výhody použití čárových kódů

- Levný způsob pro identifikaci osob a majetku organizace
- Levný a nenáročný tisk 1D a 2D kódů u 3D jsou pouze vyšší pořizovací náklady
- Tisk 3D kódů probíhá přímo na označovanou věc není potřeba dalšího média odolný proti poškození

Nevýhody použití čárových kódů

- Čárové kódy jsou jednoduše duplikovatelné a tisk 1D i 2D kódů zvládne i běžná tiskárna

Pro identifikaci osob se používají čárové kódy vytištěné nebo mikroúderové značení nanesené na identifikační plastovou kartu. Z čárových kódů je nejlepší využít 2D čárové kódy. Hodně používaným kódem je PDF-417, který se běžně používá např. na řidičských průkazech a identifikačních průkazech v USA. Kódy na identifikační karty si můžete zvolit podle vlastního uvážení, kromě těch, které podléhají registrační organizaci např. kódy EAN, které se používají v celé Evropské unii k číselnému označování zboží.

5 IDENTIFIKAČNÍ KARTY

Identifikační karty existují a vyvíjejí se déle jak čtvrt století. Identifikační karty se během této doby vyvinuly od jednoduchého předmětu k uchování informací na identifikaci osoby až po složitý kryptografický prostředek, který je klíčem k bezpečnému přístupu k informačním a komunikačním technologiím. S identifikačními kartami se setkáváme v běžném životě ve městech velice často. Mnoho lidí má již při sobě množství identifikačních karet, kde každá z nich má svůj specifický účel a zřejmě ještě dlouho nebude možné všechny tyto karty nahradit pouze jedinou. Nebylo by to z hlediska bezpečnosti a také z hlediska ručení organizace za zneužití komplexní karty využívané ve více organizacích najednou realizovatelné. Za univerzální kartu by se zřejmě nechtěl nikdo zaručit. Nejjednodušší případ identifikace, se kterým se asi každý mohl setkat je předplacená telefonní karta s pamětí a pevnou logikou. Řada uživatelů platebních karet přechází z karet s magnetickým proužkem na čipové karty a každý majitel mobilního telefonu používá SIM kartu. Společným faktorem těchto karet je relativně vysoká bezpečnost specializované čipové technologie a použití standardní kontaktní plošky pro komunikaci mezi kartou a terminálem. Stále častěji je možné se setkat i s použitím bezkontaktních čipových karet s rádiovým přenosem, zejména v případě přístupových systémů budov, docházkových systémů a aplikací v hromadné dopravě.

5.1 Dělení identifikačních karet

- Karty s magnetickým proužkem
- Karty čipové (s procesorem) kontaktní
- Karty čipové (s procesorem) bezkontaktní

5.2 Identifikační karty s magnetickým proužkem

Identifikační karty s magnetickým proužkem existují již od počátku 70. let. Tato technologie je vzhledem k její jednoduchosti a možnostem jejího použití v oblasti naplnění bezpečnostní politiky organizace pomalu na ústupu. Karty s magnetickým proužkem se řídí standardem EMV. Umístění a rozměry magnetického proužku jsou dány normou ISO7811. Magnetický proužek může obsahovat až tři stopy na různých pozicích. Existují dva typy

karet s magnetickými proužky a to LoCo a HiCo, které se volí podle použitého systému. [4]

5.2.1 LoCo

Jednodušší na kódování a nepatrně levnější než karty s magnetickou stopou HiCo. (Světle hnědý proužek)

5.2.2 HiCo

Nejvyšší úroveň odolnosti magnetické stopy před poškozením rozptýleným magnetickým polem. Kódování vyžaduje větší výkon. (Tmavý proužek)

Obr. 14. Identifikační karty s magnetickým proužkem

Identifikačních karty s magnetickým proužkem slouží pouze jako paměťové médium, na které se zaznamenává stopa s informacemi, které na kartě její provozovatel vyžaduje. Technologie magnetického proužku není svázána s žádnou elektronikou uvnitř karty. Jde pouze o magnetickou vrstvu nanesenou na identifikační kartu ještě před laminací.

Oblasti použití identifikačních karet s magnetickými proužky jsou v současné době ještě jako bankovní karty, které rychle banky vyměňují za bezpečnou technologii identifikačních čipových karet s PKI. Karty s magnetickým proužkem se využívají tam, kde hodnota aktiv není tak vysoká, aby se někdo zaměřil na duplikování karet s magnetickými proužky. Mezi oblasti využití těchto identifikačních karet budou i nadále patřit věrnostní programy a také díky nízkým pořizovacím nákladům sem patří identifikační karty osob na konferencích.

Elektromagnetická interference mezi magnetickým proužkem a integrovanými obvody v čipové kartě je testována. Identifikační karta mající magnetický proužek nesmí nijak způsobit poškození čipové karty nebo nesmí být zhoršeny či změněny funkce při čtení,

zápisu nebo mazání magnetických stop. Naopak záznam nebo čtení integrovaných obvodů na čipové kartě nesmí způsobit chybnou funkci magnetických stop nebo zařízení pro zápis, čtení nebo manipulaci. [4]

Srovnání způsobu platby kartou s magnetickým proužkem s čipovou kartou

U identifikačních platebních karet s magnetickým proužkem musel její držitel podepisovat prodejní doklad. U identifikační čipové platební karty budete vyzváni k zadání PIN prostřednictvím výzvy na displeji a zadáte jej prostřednictvím klávesnice. Pokud budete platit čipovou kartou v zahraničí u obchodníka, který akceptuje čip, můžete být přesto vyzváni k ověření podpisem. Přestože se jedná o transakci za použití identifikace čipovou kartou, tak platební terminál nemusí umožňovat ověření prostřednictvím PIN. Tyto typy platebních terminálů jsou ve Francii a Belgii. [4]

Vliv magnetického pole na identifikační kartu s magnetickým proužkem

Vystavení identifikační karty s magnetickým proužkem statickému magnetickému poli o intenzitě 79500 A/m (1000 Oe) vymaže obsah magnetických stop identifikační karty s magnetickým proužkem. Stejné magnetické pole nesmí způsobit poškození nebo chybnou funkci integrovaných obvodů uvnitř identifikační čipové karty. [5]

Výhody použití karty s magnetickým proužkem

- Snadná identifikace
- Levné a dostupné řešení
- Možnost uchování a přenosu dat

Nevýhody použití karty s magnetickým proužkem

- Malá odolnost proti poškození záznamu (mechanicky, magneticky)
- Nízká bezpečnost a poměrně snadná duplikovatelnost
- Kapacita záznamu je menší než u čipových karet

5.3 Čipové karty

Srdcem všech čipových karet je polovodičový čip (integrovaný obvod) vyvinutý speciálně pro konstrukci čipové karty nebo podobného zařízení. Zajímavostí jsou mezi identifikačními kartami chytré smart karty, které obsahují podobné komponenty jako osobní počítač - procesor, specializované kryptografické koprocesory, různé typy pamětí a vstupně/výstupní kanály integrované na jediném čipu. Moderní čipy mají implementovánu řadu bezpečnostních mechanismů, které ztěžují různé typy útoků na bezpečnost a jsou odolné proti invazivním útokům (například použití chemikálií a mikrosond) i neinvazivním útokům (například použití diferenciální analýzy spotřeby DPA). Neméně důležitou částí čipové karty je software - operační systém, který je umístěn v paměti ROM v rámci výrobních fází čipu. Právě kombinace čipu a operačního systému je podstatou konkrétní čipové karty. To co zbývá je úkon připevnění čipu na kontaktní plošky, ochrana čipu pomocí vhodného materiálu a zalisování vzniklého modulu do plastového nosiče čipové karty. [6]

Základní rozdělení čipových karet

- Kontaktní paměťové karty
- Karty čipové (s procesorem) kontaktní
- Karty čipové (s procesorem) bezkontaktní

Kryptografické čipové karty používané v systémech PKI umožňují generování a uložení kryptografických klíčů v bezpečné paměti a provádění kryptografických operací přímo na kartě. Běžně jsou implementovány *šifrovací* algoritmy DES, TDES, RSA, SHA1, AES a ECC.Kryptografické čipové karty jsou bezpečné prostředky pro širokou škálu aplikací (IAS, SSO atd.) na různých HW platformách a operačních systémech. Kryptografické čipové karty jsou počítače s vlastním operačním systémem, aplikací a komunikačním rozhraním.Pro neautorizované osoby nesmí být čipová karta jednoduše čitelná ani snadno padělatelná.

Typické využití čipových karet:

- Identifikace osob
- Elektronické platby
- Přístupy do objektů
- Cestovní průkazy
- Bankovnictví
- Systémová bezpečnost přístupu k PC
- Placená TV
- Telefonování z budky
- Mobilní telefonování

Informace uchovávané na čipové kartě

Na čipové kartě mohou být uloženy elektronické identity, příslušné RSA klíče a jejich certifikáty ve standardu X.509 vydané různými certifikačními autoritami. Čipová karta může být potištěna či kombinována s dalšími bezpečnostními prvky (čárový kód, fotografie nebo magnetický proužek).

5.3.1 Kontaktní čipové karty

Čipové karty jsou evropským vynálezem a Evropa má velkou instalovanou základnu kontaktních čipových karet, rozvinutý průmysl a náskok před ostatním světem v této oblasti. 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 jsou dva kontakty rezervované pro budoucí využití, které se již v současnosti používají u některých karet pro alternativní USB rozhraní. Systém identifikace s použitím čipových karet je možné využívat v operačních systémech firmy Microsoft, ale také v dalších operačních systémech a lze tak snadno vybudovat systém PKI. Díky bezpečné identifikaci osob lze vybudovat bezpečné informační systémy. Čipové karty lze stále využít i v systémech, které ještě nepodporují PKI. [6]

Čipová karta je stále v dosahu svého držitele, který ji může použít kdekoliv ji potřebuje. Identifikační karta může být kombinována s bezkontaktním rozhraním pro přístupové systémy. Dále může být karta potištěna a použita jako identifikační průkaz zaměstnance.

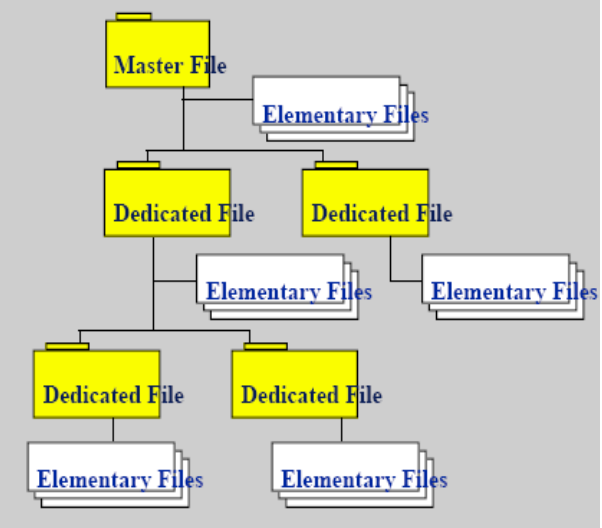
Typy pamětí, které bývají v čipových kartách použity jsou RAM (Random Access Memory), ROM (Read Only Memory) a EEPROM (Electrically Erasable Programmable ROM). Karty používají buď jednodušší výpočty nebo velmi náročné kryptografické operace. [7]

Přínosy čipových karet

- Zvýšení bezpečnosti
- Vyšší paměťová kapacita (chráněná)
- Šifrování (kryptografické operace)
- Možnost off-line provozu (bez sdílené databáze)

Vnitřní adresářová struktura na čipové kartě (kontaktní i bezkontaktní)

- Na čipových kartách je použita stromová adresářová struktura stejně jako u jakéhokoliv jiného operačního systému
- Kořenový adresář MF (Master File)
- Podadresář DF (Dedicated File)
- Datový soubor EF (Elementary File)



Přístupová práva adresářů

- ALW (vždy)
- NEV (nikdy)
- PRO (chráněný, je potřeba správný klíč)
- ENC (šifrovaný, rozšíření PRO)

Obr. 15. Adresářová struktura

Standardy pro čipové karty

- CEN (Com'te Europeen de Normalization) – vytváří standardy pro platební čipové karty
- ANSI – podvýbor pro identifikační karty, který vytváří americkou část ISO/IEC/JTC1/SC17 WG4
- ECBS (European Committee for Nankiny Standards) – bankovní standardy pro Evropu
- ETSI (European Telecommunications Standard Institute) – vytváří evropské standardy pro karty a mobilní telefony
- Bank Cards – skupina ICC Specification Working Group vytvořila specifikaci EMV pro čipové karty, provádějící finanční transakce [6]

Základní standardy pro čipové karty

- ISO / IEC Point Technical Committee 1 / Subcommittee 1

  Identifikační karty a související zařízení
- Working Group 4 - kontaktní karty
- Working Group 8 - bezkontaktní karty
- Technical Committee 68 / Subcommittee 6

  Bankovní karty a karty provádějící finanční transakce
- SC6 / Working Group 5

  Standardizace komunikace mezi kartami a terminály
- SC6 / Working Group 7

  Bezpečnostní architektura systémů s kartami [7]

ISO Standardy pro čipové karty

Výrobou nebo programováním čipových karet se ve světě zabývá mnoho výrobců. Aby nebyl konečný zákazník omezen na výrobky jednoho výrobce a také byla možná spolupráce více firem, byly specifikovány charakteristické rysy identifikačních karet normami ISO (International Organization for Standardization). Obsah norem ISO určuje výrobci základní vlastnosti pro výrobu konkrétní čipové karty. Čipové karty se tedy mohou vyrábět tak, aby splňovaly několik norem najednou a vyhovovaly několika standardům, čímž výrobci dosáhnou kompatibility s několika existujícími zaběhnutými systémy najednou. Používání norem ISO otevřelo výrobcům místo na světovém trhu.

ISO 7816 (popis normy)

- 7816 - 1: Charakteristické fyzikální rysy
- 7816 - 2: Karty s kontakty - Rozměry a umístění kontaktů
- 7816 - 3: Charakteristické elektrotechnické rysy a třída identifikace pro integrované obvody karet pracujících s napětím 5V, 3V a 1.8V
- 7816 - 4: Organizace, bezpečnost a příkazy pro výměnu
- 7816 - 5: Registrace dodavatelských aplikací
- 7816 - 6: Vnitřní uspořádání datových prvků pro výměnu

ČSN ISO 10202 (popis normy)

- 10202-1: Životní cyklus karty
- 10202-2: Proces transakce
- 10202-3: Vztahy mezi kryptografickými klíči
- 10202-4: Zabezpečené aplikační jednotky
- 10202-5: Použití algoritmů
- 10202-6: Ověření držitele karty
- 10202-7: Správa klíčů
- 10202-8: Všeobecný pohled a principy

Možnosti spojené s použitím čipových identifikačních karet

Čipové karty mohou používat správce úložiště, který zajistí automatické zaregistrování certifikátů z karty do operačního systému hned po jejím zasunutí do čtečky karet. Výrobci identifikačních karet dodávají ke svým technologiím také ovládací software pro různé operační systémy, který zajišťuje jejich správnou funkci. K dalšímu vybavení komplexního řešení identifikačního systému může také patřit správce karty. Správce karty je prostředí, ve kterém je zobrazen obsah karty. Dále je možné přidat nebo odebrat klíče a certifikáty, odblokovat kartu, změnit PIN a změnit PUK. Správce karty je aplikace, která by měla jejího uživatele navést na řešení potíží s kartou. Na kartě můžeme uchovávat i další důvěrné informace jako přihlašovací jména a hesla k nejrůznějším účtům, které autorizaci pomocí aplikací tzv. Single Sign-on vyžadují. Nemusíte je nosit ve své hlavě stačí jen zasunout kartu do čtečky karet a získáte automaticky přístup ke všem svým účtům jejich přihlašovací údaje jsou na kartě uloženy.

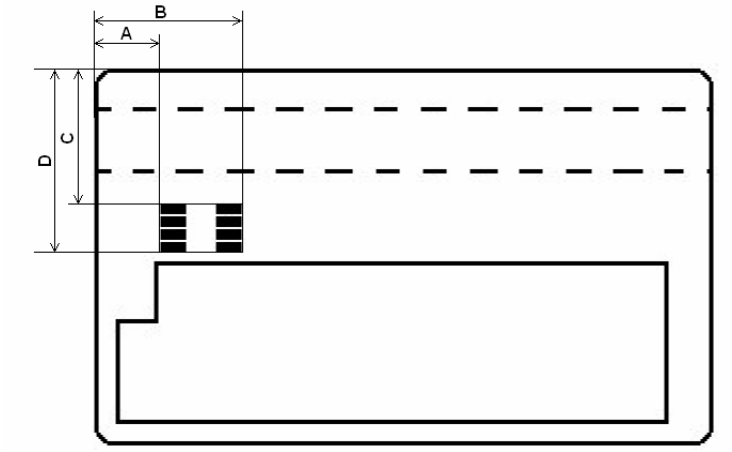
Čipové karty prokazatelně zvyšují bezpečnost informačních technologií, bezpečnost bezhotovostních finančních transakcí. Zvyšují také stupeň integrace několika bezpečnostních aplikací v organizacích do používání jednoho identifikačního prvku, kterým je právě čipová karta. Proto, aby mohly být čipové karty použitelné i v přístupových systémech a zároveň i při identifikaci při finančních transakcích jsou kontaktní a bezkontaktní technologie integrovány v jedné čipové kartě. Podle způsobu integrace dvou technologií do jedné karty nazýváme karty jako hybridní čipové karty nebo duální čipové karty.

Zásady při výrobě identifikačních karet

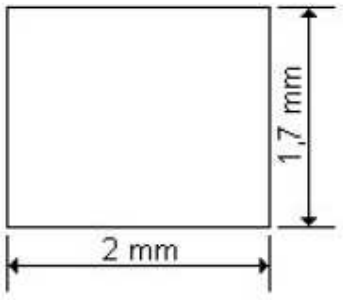
Tepelná ztráta integrovaného obvodu karty nesmí být větší než 2,5 W. V libovolném prostředí nesmí teplota na povrchu karty překročit 50 ° C. Integrovaný obvod karty nesmí být při normálním použití poškozen osobou nabitou statickou elektřinou. Funkce karty nesmí být ovlivněna výbojem kapacity 100 pF o napětí 1 500 V přes odpor 1 500 Ω mezi kterýmkoli kontaktem a zemí. Karta musí být odolná proti poškození povrchu a všech součástí a musí zůstat neporušena během normálního použití, skladování a manipulace. Povrch všech kontaktů a kontaktní oblast (celý vodivý povrch) nesmí být poškozen tlakem, ekvivalentním působení tlaku 1,5 N ocelovou kuličkou o průměru 1 mm. [5]

Umístění kontaktů na kontaktní čipové kartě

Část normy ISO 7816 definuje osm kontaktů. Kontakty mohou být umístěny buď na přední nebo na zadní straně karty, ale v obou případech jsou rozměry vztaženy k levému a hornímu okraji odpovídajícího povrchu karty Obr.16. Minimální rozměr každého kontaktu na kontaktní ploše je uveden na Obr. 17. [5]



Obr. 16. Umístění kontaktní plochy



Obr. 17. Rozměry kontaktů

Tabulka 1.: Rozměry pro umístění kontaktní plochy na kartě

Rozměry [mm]	A	B	C	D
C1	10,25	12,25	19,23	20,93
C2	10,25	12,25	21,77	23,47
C3	10,25	12,25	24,31	26,01
C4	10,25	12,25	26,85	28,55
C5	17,87	19,87	19,23	20,93
C6	17,87	19,87	21,77	23,47
C7	17,87	19,87	24,31	26,01
C8	17,87	19,87	26,85	28,55

Tabulka 1. doplňuje rozměry k Obr.16., kde uvádím umístění kontaktní plochy na identifikační kontaktní čipové kartě.

Výhody použití kontaktních čipových karet

- bezpečné úložiště osobních údajů
- ověřování probíhá přímo uvnitř karty
- možnost využití karty na Single Sign-On aplikace
- při ztrátě karty je možné její použití zablokovat

Nevýhody použití kontaktních čipových karet

- zatím nejsou podporovány všemi terminály
- slabinou je lidský faktor (osoba, která neopatrně zachází s PIN kódem)

5.3.2 Předplatní čipové karty (telefonní karty)

Používají rozdílnou technologii, která nezaručuje takovou bezpečnost, jako čipové karty, které používají šifrování (kryptografické karty). Kryptografické čipové platební karty se dají označit za naprosto bezpečné a zřejmě jedinou hrozbou pro možné zneužití kryptografických čipových karet bude sám jejich uživatel (napíše PIN na kartu).

Rozdělení oblastí předplatní karty

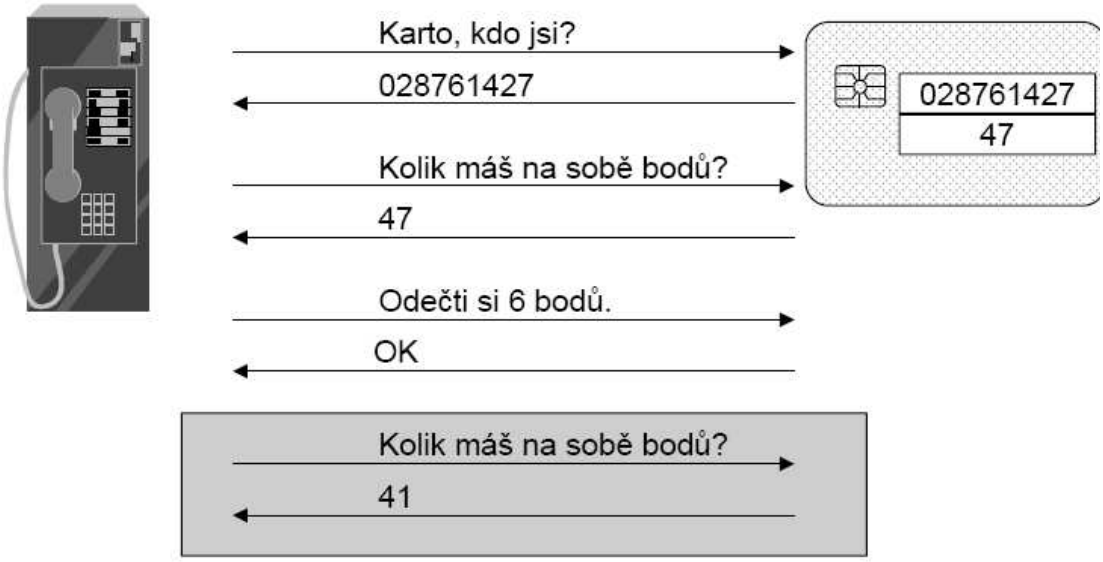
- Systémová oblast - je naprogramovaná od výrobce a má vlastnost paměti ROM
- identifikace systému, kontrolní součty, sériové číslo, parametry karty (sériová EPROM)
- Oblast jednotek - jednotce odpovídá jeden bit

  počáteční nastavení bitů na “0“

  po zaplacení se jednotka nastaví na “1”
- Oblast se super-jednotkami (u některých karet) - používá se pro dobíjení karty

bit super-jednotky se nastaví na “1“ a tím se bity v oblasti jednotek nastaví na “0”

Předplatní čipová karta není obvykle zabezpečená šifrováním.



Obr. 18. Algoritmus funkce telefonní karty

Zhodnocení systému telefonních karet

Slabá místa

- systém neprovádí kryptografickou autentizaci a zabezpečení zpráv
- lze vyrobit emulátor, který simuluje chování rozhraní telefonu
- lze blokovat či modifikovat některé příkazy

Protiopatření

- detekce chování karty na nestandardní podněty
- použití čipu v ISO pouzdru
- použití kryptografické čipové karty (šifrování)

5.3.3 Bezkontaktní čipové karty

Bezkontaktní čipové karty se začaly používat ve velkém množství v docházkových a přístupových systémech. Důvodem pro jejich nasazení bylo nejenom pohodlí, ale hlavně nutnost neustále prokazovat svou identitu při průchodu chráněnými dveřmi. Použití kontaktní čipové karty je principově pomalejší, protože se karta musí do čtecího terminálu zasunout a poté ji musíme zase vyjmout. Z tohoto hlediska nasazení bezkontaktních čipových karet zvyšuje rychlost identifikace a také její komfort.

Bezkontaktní komunikace s čipovou kartou je standardizována na úrovni normy ISO/IEC 14443. Určitou komplikací jsou dvě nekompatibilní specifikace A a B, které (naneštěstí) odrážejí vliv zástupců silných komerčních firem ve standardizačních výborech. Důsledkem je ztížená interoperabilita a nutnost použití bezkontaktních čteček, které podporují obě specifikace. V současné době také probíhá standardizace vyšších přenosových rychlostí až na hodnotu 848 kbitů/sekundu, což usnadní zápis a čtení větších objemů dat, zejména v oblasti biometrie.

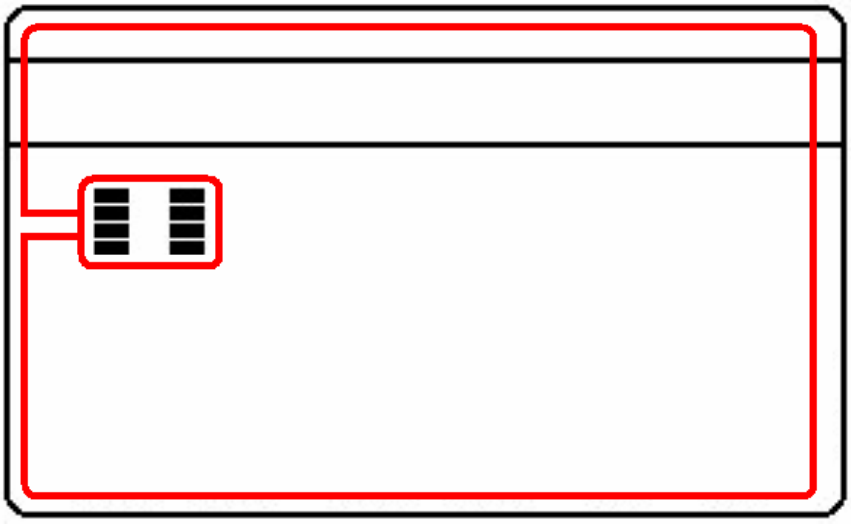
Ještě nedávno byla hlavní překážkou využití sofistikovaných kryptografických možností čipových karet prostřednictvím radiového přenosu příliš vysoká energetická náročnost čipů. V současné době díky pokračující miniaturizaci (rozměry čipu jsou okolo 12 mm^2) a snižující se spotřebě lze realizovat i komplexní transakce založené na RSA s využitím bezkontaktního radiového přenosu.

Princip činnosti bezkontaktní čipové karty

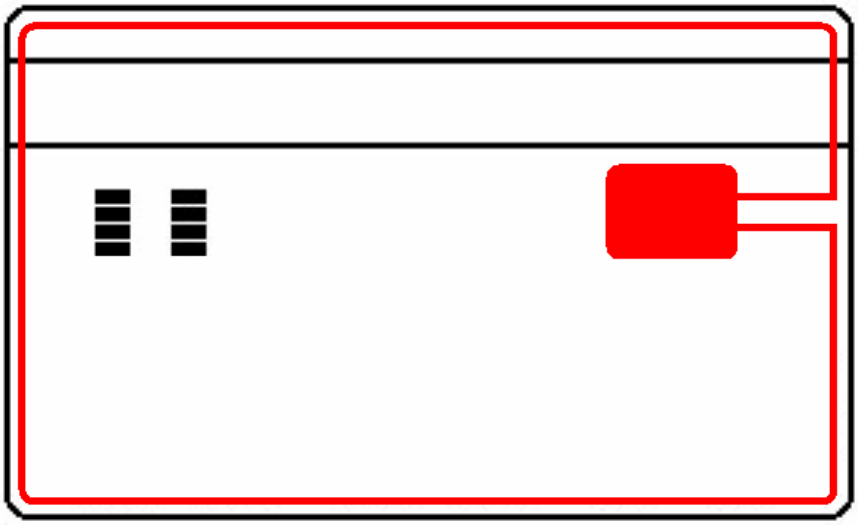
Čipová karta nemá vlastní zdroj elektrické energie, proto je zcela závislá na dodávce energie ze čtečky. V případě bezkontaktní karty se energie přenáší ve formě indukce elektromagnetického pole ze čtečky do antény čipové karty. Nosná frekvence je nejčastěji 13,56 MHz a vzdálenost mezi kartou a čtečkou je závislá na použitém typu karty i čtecího zařízení. Energie indukovaná v anténě karty slouží k napájení čipu. Zajímavým problémem je zpětný přenos informace od karty ke čtečce. Bezkontaktní čipová karta používá princip zátěžové modulace, kdy odebírá určité množství energie z elektromagnetického pole čtečky a poté co dojde k přenosu energie na kartu, tak karta zpětně vyšle informaci, kterou čtečka vyhodnotí. [5]

5.3.4 Duální a hybridní čipové identifikační karty

Tyto identifikační karty v sobě obsahují jak kontaktní technologii, tak i bezkontaktní technologii. Duální čipová karta má společnou elektroniku pro její kontaktní i bezkontaktní část. Obě dvě technologie jsou tedy vzájemně propojeny. Jiným typem je hybridní čipová karta, která má oddělenou kontaktní a bezkontaktní část, kde každá z těchto částí má svůj vlastní řídící čip, který je na druhou technologii na společné kartě naprosto nezávislí. Oba dva typy čipových karet mají po obvodu karty zalisovanou anténu.



Obr. 19. Duální čipová identifikační karta



Obr. 20. Hybridní čipová identifikační karta

Výhody použití bezkontaktních čipových karet

- není potřeba přikládat identifikační kartu na čtečku
- identifikace proběhne bez potřeby narušit činnost ověřované osoby
- možnost využití karet v přístupových systémech a dopravních systémech
- není nutné zadávat ručně kód

Nevýhody použití bezkontaktních čipových karet

- zatím nejsou tyto karty na takové úrovni zabezpečení jako kontaktní čipové karty
- informace lze zachytávat při rádiovém přenosu, slabinou je tedy právě bezkontaktní komunikace
- osoba držící kartu má přístupová práva stejná jako její pravý majitel

6 RFID TAGS (RÁDIO-FREKVENČNÍ IDENTIFIKAČNÍ ZNAČKY)

Největší výrobce RFID značek je firma Sokymat. Uvádím zde tedy její technologie, které mohou být zapouzdřeny do rozmanitých obalů. Typy pouzder mají specifikaci podle účelu, ke kterému mají být používány. Tyto identifikační značky jsou v současnosti používány k označování zvířat podkožními značkami, v zemědělství byly masově využity v celosvětovém měřítku pro označení dobytka, ale i ostatních hospodářských zvířat. Identifikace osob využívána v současných docházkových a jídelních systémech probíhá RFID značkami zapouzdřených do tzv. klíčenek nebo RFID identifikačních karet.

6.1 RFID tokeny firmy Sokymat

6.1.1 Unique

Čip 125kHz RFID IO pouze pro čtení 64 bitů

Charakteristické vlastnosti

- Operační paměť: 64 bitů ROM (*EM* 4102)
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba
- Několik voleb přenosové rychlosti dat a typů kódování *(výběr pouze během výroby zařízení)*
- Rychlost přenosu dat : 2, 4 nebo 8kbd
- Typ modulace : Manchester, Biphase nebo PSK
- Standardně výrobce nastavuje : Manchester, 2kbd
- Záruka jedinečnosti a jednoznačnosti kódů
- Zvláštní identifikační kódy na přání zákazníka [8]

6.1.2 Q5

Čip 125kHz RFID IO pro čtení i zápis 330 bitů

Charakteristické vlastnosti

- Operační paměť: 264 bitů EEPROM, (224 *bitů uživatelské paměti* + 8x1 *bit* OTP funkce,
- 32 *bitová konfigurace*), 64 bitové sériové číslo (*přístup jen na čtení pouze se specifickým příkazem*) + 2x1bit uzamčený
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba
- Několik voleb přenosové rychlosti dat a typů kódování (*výběr podle požadavků uživatele*)
- Rychlost přenosu dat : od 1 do 62kbd
- Typ modulace : FSK, Manchester, Biphase, PSK nebo NRZ
- Standardně výrobce nastavuje : Manchester, 2kbd
- Záruka jedinečnosti a jednoznačnosti kódů

Pracovní režimy

- Maximální definice bloků : definování počtu čtecích bloků
- Heslový mód : dovoluje přečíst jedno slovo po zadání hesla
- Přímý přístupový mód : dovoluje přečíst jedno slovo bez zadání hesla
- Odpověď na požádání : modulace transpondéru aktivovaná pouze na požádání
- Zastavení modulace : příkaz zastavit modulaci transpondéru
- Obrácený výstup dat : inverzní datový tok
- Rychlá zapisovací metoda : dovoluje rozdělení programování na 2 etapy
- Ochrana proti zápisu : příkaz uzamknout slova nezávisle jedno na druhém
- Sekvenční terminátor : speciální funkce [8]

6.1.3 HTS 256

Čip 125 kHz RFID IO pro čtení i zápis 256 bitů, antikolize a šifrování

Charakteristické vlastnosti

- 256 bitová EEPROM paměť organizovaná v 8 stránkách po 32 bitech (192 bitů *uživatelské paměti v prostém módu nebo* 128 *bitů uživatelské paměti v šifrovacím módu*)
- 32 bitová permanentní paměť
- Uzamykací bity po 2 stránkách
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba
- Několik voleb přenosové rychlosti dat a typů kódování (*výběr podle požadavků uživatele*)
- Rychlost přenosu dat : 2,4 nebo 8kbd
- Typ modulace : Manchester nebo Biphase
- Standardně výrobce nastavuje : Manchester, 2kbd
- Shoda s ISO 1784/785, 14223- 1 pro německé a holandské závodní holuby a
- Německé odpadové hospodářství standardní BDE

Pracovní režimy

- Zákazník si může zvolit ze dvou pracovních režimů
- TTF (*transpondér vysílá nejprve signál*) : Stránky 4, 5, 6, 7 se přenesou po nabití
- RTF (*antikolize*) : čtečka navazuje komunikaci se značkou jako první po přiblížení
- Založeno na Unique identifikačních číslech
- Identifikační rychlost 20 značek/sec
- Šifrování : Vzájemná legalizace založená na 48 bitových tajných klíčích
- (*identifikace trvá do* 48*ms*) [8]

6.1.4 HTS 2048

Čip 125 kHz RFID IO pro čtení i zápis 2048 bitů, antikolize a šifrování

Charakteristické vlastnosti

- 2048 bitová EEPROM paměť organizovaná v 64 stránkách po 32 bitech (1984 bitů *uživatelské paměti v prostém módu nebo* 1920 *bitů uživatelské paměti v šifrovacím módu*)
- 32 bitová permanentní paměť
- Uzamykací bity po 2 stránkách, 2 nebo 4 blocích
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba
- Několik voleb přenosové rychlosti dat a typů kódování (*výběr podle požadavků uživatele*)
- Rychlost přenosu dat : 2,4 nebo 8kbd
- Typ modulace : Manchester nebo Biphase
- Standardně výrobce nastavuje : Manchester, 2kbd
- Shoda s ISO 1784/785, 14223- 1 pro německé a holandské závodní holuby a
- Německé odpadové hospodářství standardní BDE

Pracovní režimy

- Zákazník si může zvolit ze dvou pracovních režimů
- TTF (*transpondér vysílá nejprve signál*) : Stránky 4, 5, 6, 7 se přenesou po nabití
- RTF (*antikolize*) : čtečka navazuje komunikaci se značkou jako první po přiblížení
- Založeno na Unique identifikačních číslech
- Identifikační rychlost 20 značek/sec
- Šifrování : Vzájemná legalizace založená na 48 bitových tajných klíčích
- (*identifikace trvá do* 48*ms*) [8]

6.1.5 Titan

Čip 125 kHz RFID IO pro čtení i zápis 1k bit

Charakteristické vlastnosti

- 1k bitová EEPROM (EM 4x50)
- Paměť je organizována ve 32 slovech z 32 bitových *(928 bitů uživatelské paměti)*
- 64 bitová Laser ROM je zárukou jedinečnosti zařízení
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba (*čtení* I=3μA, *zápis* I=40μA)
- Několik voleb přenosové rychlosti dat a typů kódování (*výběr podle požadavků uživatele*)
- Rychlost přenosu dat : 2,4 nebo 8kbd
- Typ modulace : Manchester
- Standardně výrobce nastavuje : Manchester, 2kbd

Bezpečnostní charakteristika

- Heslo složené z 32 bitů
- Uživatelsky definovaná oblast čtení paměti po zapnutí
- Uživatelsky definované blokování zápisu do oblasti paměti
- Uživatelsky definovaná ochrana proti čtením z paměťové oblasti [8]

Organizace paměti

Word	Bit 0 ----------31
0	Password
1	Protection word
2	Control word
3 : 31	928 bits of user EEPROM
32	Device serial number
33	Device identification

Password : Write Only, NO Read access
Protection Word :
0-7 First word read protected
8-15 Last word read protected
16-23 First Word Write Inhibited
24-31 Last word Write Inhibited
Control Word :
0-7 First word read
8-16 Last word read
16 Password check On/Off
17 Read after write On/Off
18-31 User available
User Memory : 928 bits available
Device serial number : Laser ROM (unicity)
Device Identification : Laser ROM

Obr. 21. Organizace paměti systému Titan

6.1.6 HITAG 1

Čip 125kHz RFID IO pro čtení i zápis 2k bity

Charakteristické vlastnosti

- 2k bitová EEPROM paměť, 16 bloků na každé 4 stránky, 1 stránka obsáhne 32 bitů
- 32 bitové továrně naprogramované sériové číslo
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba (*čtení* I=9μA, *zápis* I=25μA)
- Typ modulace : Manchester
- Rychlost přenosu dat : 4kbd
- Oblast paměti je chráněna před zápisem
- Antikolizní protokol
- Vzájemná legalizace
- Zašifrovaný dálkový přenos [8]

6.1.7 HITAG 2

Čip 125kHz RFID IO pro čtení i zápis 256 bitů

Charakteristické vlastnosti

- 256 bitová EEPROM paměť organizovaná v 8 stránkách po 32 bitech
- 32 bitové továrně naprogramované sériové číslo
- Pracovní kmitočet : 125kHz
- Bezdotykové napájení, velmi nízká spotřeba (*čtení* I=7μA, *zápis* I=20μA)
- Několik voleb přenosové rychlosti dat a typů kódování (*výběr podle požadavků uživatele*)
- Rychlost přenosu dat : 2,4 nebo 8kbd
- Typ modulace : Manchester nebo Biphase
- Standardně výrobce nastavuje : Manchester, 2kbd

Pracovní režimy

- Kryptovací mód : zašifrovaná datová komunikace
- Heslový mód : heslo zadané před zápisem nebo čtením dat
- Veřejný režim A : pracuje pouze se 64 bitovými Manchester, 4kBd čtecími zařízeními
- Veřejný režim B : ISO kompatibilní podle normy 11784/785
- Veřejný režim C : pracuje s Philips rodinou PIT PCF7930/31 [8]

6.1.8 I-Code

Čip 13,56 MHz RFID IO pro čtení i zápis 512 bitů

Charakteristické vlastnosti

- 512 bitová EEPROM paměť organizovaná v 16 blocích po 4 bajtech (384 *bitová uživatelská paměť*)
- 64 bitové jedinečné sériové číslo
- Pracovní kmitočet : 13,56 MHz
- Rychlost přenosu dat : 26,5kbd
- Typ modulace : 423,75 kHz náhradní provoz Manchester kódování
- EAS (*elektronický článkový dozor*) 256 bitová kombinace
- Antikolize: čtečka navazuje komunikaci se značkou jako první po přiblížení
- Posuzuje se 64 bitové jedinečné sériové číslo
- Identifikační rychlost 20 značek/sec
- Ochrana před zápisem pro každé slovo [8]

6.1.9 I-Code SL2

Čip 13,56 MHz ISO15693 RFID IO pro čtení i zápis 1024 bitů

Charakteristické vlastnosti

- 1024 bitová EEPROM paměť organizovaná v 32 blocích po 4 bajtech (896 *bitová uživatelská paměť*)
- 64 bitové jedinečné sériové číslo
- Pracovní kmitočet : 13,56 MHz
- Shoduje se s ISO 15693
- EAS (Electronic Article Surveillance)

Organizace paměti

1024 bitová EEPROM paměť je rozdělena do 32 bloků. Blok je nejmenší přístupová jednotka. Každý blok se skládá ze 4 bajtů (1 blok = 32 bitů). Bit 0 v každém bajtu představuje nejnižší platný bit (LSB) a bit 7 nejvyšší platný bit (MSB), v tomto pořadí. [8]

	Byte 0	Byte 1	Byte 2	Byte 3	
Block -4	UID0	UID1	UID2	UID3	Unique Identifier (lower bytes)
Block -3	UID4	UID5	UID6	UID7	Unique Identifier (higher bytes)
Block -2	Internally used	EAS	AFI	DSFID	EAS, AFI, DSFID
Block -1	00	00	00	00	Write Access Conditions
Block 0	x	x	x	x	User Data
Block 1	x	x	x	x	
Block 2	x	x	x	x	
Block 3	x	x	x	x	
Block 4	x	x	x	x	
Block 5	x	x	x	x	
Block 6	x	x	x	x	
Block 7	x	x	x	x	
...	...				
...	...				
...	...				
Block 27	x	x	x	x	User Data

Obr. 22. Organizace paměti systému I-Code SL2

Hodnoty (v hexadecimálním zápisu) ukázané v tabulce nahoře jsou uložené v EEPROM.

Obsah bloků označených x ' v tabulce je po doručení nenadefinovaný.

Pro čtení a zápis mohou být adresované jen bloky 0 až 27.

Sedna LRi64

Čip 13,56 MHz ISO15693/1800-3 RFID IO 120 bitů

Charakteristické vlastnosti

- 120 bitová EEPROM paměť organizovaná v 32 blocích po 8 bitech
- 64 bitová jedinečné uživatelská identifikace
- 56 bitová WORM (*jednou pro zápis – mnohonásobné čtení*)
- AFI seznam (*aplikační rodinný identifikátor*)
- DSFID seznam (*ukládání dat do paměti s identifikátorem formátu*)
- Pracovní kmitočet : 13,56 MHz
- Shoduje se s ISO 15693
- 10% ASK modulace používání L impulzního kódu (26*kbit/s*)
- Manchester kódování s 423kHz pomocnou nosnou frekvencí a (26*kbit/s*) datovým tokem [8]

Pouzdra RFID značek

Obr. 23. Pouzdra RFID značek firmy Sokymat

Obr. 24. Příklad využití RFID tokenů na identifikační karty a klíčenky

Výhody použití RFID Tokenů

- Rychle se zjistí jejich ztráta
- Nejsou jednoduše kopírovatelné
- Tokeny samy o sobě mohou být schopny zpracovávat nebo přenášet další informace (jméno osoby nebo název zboží, cena, datum, hesla, poznámky atd.)

Nevýhody použití RFID Tokenů

- Při použití RFID tokenů na označování zboží je zapotřebí ke kontrole a odstraňování ochranných značek speciální čtecí zařízení, které značku zároveň sundá a speciálně vycvičená osoba pro tuto činnost
- Token musí být dostatečně složitý aby se zvýšila obtížnost jeho zkopírování
- Může se polámat přestat fungovat což by mělo být jednoduše detekovatelné uživatelem

RFID tokeny se při identifikaci osob používají jako různé přívěsky na klíče, ale vyrábí se také ve formě identifikačních karet. Jako novou možnost identifikace osob předpokládám použití RFID tokenů implantovaných pod kůži člověka. Když se označují zvířata lidé by nemuseli být výjimkou. Je to snad otázka času, kdy etické či morální zásady umožní učinit tento významný zásah do soukromí lidí.

6.2 USB Tokeny

USB tokeny slouží hlavně pro uložení autentizačních údajů a certifikátů pro administrátora registrační autority. Každý USB token by měl splňovat podmínky neodmítnutelnosti a autenticity při využívání různými systémy PKI.

Funkce USB tokenu

Jádrem každého tokenu je inteligentní kryptografický čip, většinou s vlastním operačním systémem. Operační systém zajišťuje komunikaci s nadřazeným systémem, autentizaci a volání jednotlivých kryptografických operací. Mezi základní funkce kryptografického čipu patří generování asymetrického páru klíčů, import asymetrického páru klíčů, úložiště osobních certifikátů úložiště kořenových certifikátů CA a elektronický podpis s daným privátním klíčem. Generováním privátního klíče přímo na tokenu je zajištěno, že nebude existovat žádná další kopie klíče. Tímto pak token přináší faktickou a vynutitelnou podmínku neodmítnutelnosti použití privátního klíče. Navíc každé použití klíče vyžaduje autentizaci uživatele PINem. Tímto je osobní vlastnictví (privátní klíče) chráněno dvou-faktorovou autentizací, vlastnictvím USB tokenu a znalostí PIN.

Rozhraní USB Tokenu

Součástí každého typu USB tokenu jsou i příslušné ovladače a sada knihoven pro vytváření příslušného rozhraní pro aplikace. Souhrnně se všechny vrstvy pracující mezi tokenem a aplikací nazývají middleware. Bez ohledu z jakých vrstev je middleware složen.

(PKCS#15, PKCS#1) na nejvyšší úrovni se nejčastěji používají tato rozhraní pro aplikace:

PKCS#11: Nejpoužívanější rozhraní nezávislé na systému. Využívají především nativní utility karty, aplikace z rodiny Mozilla, Entrust a další. Toto rozhraní je také používáno v prostředí Linuxu.

MS CAPI: Microsoft crypto API. Token je registrován jako další CSP (crypto service provider). Zpřístupňuje operace tokenu v nativních Windows aplikacích IExplorer, MS Outlook, MS Office a OpenVPN.

Java API: Zpřístupňuje operace tokenu přímo pro JAVA prostředí. Většinou je JRE schopno použít volání systému a zprostředkovat přístup k certifikátům prostřednictvím MS CAPI.

Pro každý typ tokenu výrobce dodává příslušné knihovny. Přímo v knihovnách je dané rozložení jednotlivých datových struktur na tokenu (adresářová struktura). Proto je nutné použít pro daný typ tokenu příslušnou knihovnu. [9]

Srovnání výhod a slabin ID prostředků využívaných v informačních technologiích

Jedna z otázek při rozhodování o implementaci čipové technologie zní "Máme použít čipovou kartu nebo USB token?". Na první pohled se může zdát USB token výhodnější. Jeho základní přednost spočívá v odbourání potřeby čtecího zařízení a ve využití USB rozhraní a konektoru, který je dnes standardní součástí PC a notebooků. Při hlubším prozkoumání obou technologií zjistíme, že důvodů pro použití čipové karty je více.

- Čtečky čipových karet jsou již levné a dostupné periférie, jejich cena je srovnatelná s cenou samotné čipové karty. Výrobci notebooků nabízejí stále více modelů, které mají standardně zabudovanou čtečku čipových karet, k ostatním lze snadno připojit PCMCIA nebo USB čtečku.
- V současné době již přední výrobci čipových karet dodávají karty, které mají integrováno standardní sériové rozhraní podle ISO/IEC 7816-3 a současně USB rozhraní přímo na čipu.
- USB rozhraní čipové karty je součástí připravovaného standardu ISO/IEC 7816-12, který se brzy se brzy dostane do praxe. Velmi pravděpodobně lze očekávat, že po uvedení tohoto standardu do praxe dojde k rozšíření a běžnému používání USB rozhraní čipových karet.
- Čipová karta může být na rozdíl od USB tokenu vizuálně personalizována a může být opatřena bezpečnostními prvky, které brání duplikování karet. Mezi prvky s vysokou bezpečností patří aplikace pozitivního reliéfu, prvky CLI/MLI a celá řada tiskových technik, jako je mikrotext, duhové zbarvení, infračervené a ultrafialové inkousty. Neméně důležitá je bezpečnost personalizace (vytištění identifikačních údajů, fotografie a dalších informací), kde je možné například využít moderní technologie laserového gravírování a laserové perforace.
- Zadání kódu PIN, které je nutné pro určité operace (například při použití šifrovacích klíčů na kartě), se běžně provádí na klávesnici PC. [9]

7 BIOMETRICKÉ IDENTIFIKAČNÍ PROSTŘEDKY

Lidské tělo můžeme brát jako množinu počítačově zpracovatelných informací (biometrických znaků). Tyto informace lze uchovávat v databázi, ukládat na paměťová média a přenášet z místa na místo. Pokud tedy matematické obrazy charakteristik lidských morfologických znaků a biochemických parametrů budou uchovávány v databázích, mohou z nich být následně extrahovány a porovnávány navzájem i s jinými soubory relevantních dat. Zde se ale budeme potýkat s rizikem zneužití těchto datových souborů. Použitím biometrických identifikačních prostředků budeme mít permanentní kontrolu nad sledovanými osobami, aniž by si to uvědomovali. Některé z identifikačních metod mohou probíhat bez vědomí identifikované osoby jen stěží, například sejmout otisk prstu vyžaduje spolupráci identifikovaného. Existují však zařízení, která mohou člověka identifikovat, aniž se na tom sám úmyslně podílí. Některým zařízením stačí, jestliže sledovaná osoba projde identifikačním prostorem (detektorem, o němž ani neví), a lze takto získat potřebné biometrické informace dostačující k identifikaci.

Současná zařízení identifikují osoby tím, že dokážou přečíst a vyhodnotit četné specifické identifikační biometrické parametry sledované osoby, zejména pak individuální naprosto specifické obrazce oční duhovky a sítnice, jedinečnost tvaru ušních boltců i další charakteristické identifikační parametry (chůzi, pach těla, dynamiku krevního toku, charakteristické morfo-kinetické rysy podepisování, akustické spektrální charakteristiky hlasu, morfémové identifikanty tváře a další znaky. Přestože biometrická analýza není úplně nejnovější metodou ověření totožnosti, do popředí veřejného zájmu se dostala v důsledku opatření, která zavedly na letištích a hraničních přechodech Spojené státy americké po teroristických útocích z 11. září 2001.

Použití biometrických údajů pro porovnání je z hlediska ochrany soukromí určitě přijatelnější než jejich použití pro identifikaci. Porovnáváním se pouze ověřuje zda ten, kdo se prokazuje dokladem totožnosti je opravdu jeho oprávněným vlastníkem. V těchto případech ale také existuje riziko zneužití. Biometrické informace lze vyhodnocovat také off-line, tedy bez použití společné databáze, ve které jsou osobní údaje uchovávány. Taková databáze totiž vzbuzuje veliký zájem počítačových hackerů a je vystavována obrovskému množství útoků.

Proto se využívá srovnávání určitých přirozených biometrických znaků osoby, která je identifikována s biometrickými údaji, které jsou uloženy na paměťovém nosiči nejčastěji na nových čipových kartách. Pro verifikaci pak není zapotřebí vytvářet velké databáze. Je ovšem nutné použít technologie, které umožní, aby identifikační obrazy tzv. ikonické šablony byly umístěny na takovém paměťovém nosiči, který má osoba stále u sebe, tedy aby nebyly archivovány ve vzdálených databázích. Ikonickou šablonu je nutné nosit na vhodném přenosovém médiu papírovém dokladu či identifikační kartě. Příkladem využití verifikace v praxi by měl být evropský cestovní doklad. [10]

Vyjádření spolehlivosti biometrických systémů

U biometrických systémů se hodnota nepřesnosti udává pomocí dvou statistik: *míry chybného přijetí* (*FAR*) a *míry chybného odmítnutí* (*FRR*). Obě se vyjadřují v procentech a první z nich udává, jaké je riziko toho, že systém podvodníka chybně přijme jako oprávněného uživatele. Naopak FRR vypovídá o výši rizika toho, že systém chybně odmítne autorizovaného uživatele. Vztah mezi oběma mírami je takový, že čím nižší je FAR, tím vyšší je FRR, a naopak. [11]

7.1 Biometrická identifikace otiskem prstu

Tato biometrická identifikační metoda využívá rozdílnosti vnitřního povrchu otisků prstů, kde se pozorují drobné, vyvýšené, brázdovité útvary, které vytvářejí různé vzory na bříškách prstů. Tyto vzory se rozdělují do tří hlavních kategorií. Jsou to smyčky, přesleny a oblouky. Důležité u těchto různých typů vzorů je to, s jakou četností (frekvencí) se na prstu vyskytují. Například smyčky obsahuje 65% ze všech otisků, přesleny něco kolem 30% a oblouky jen asi 5% všech otisků. [11]

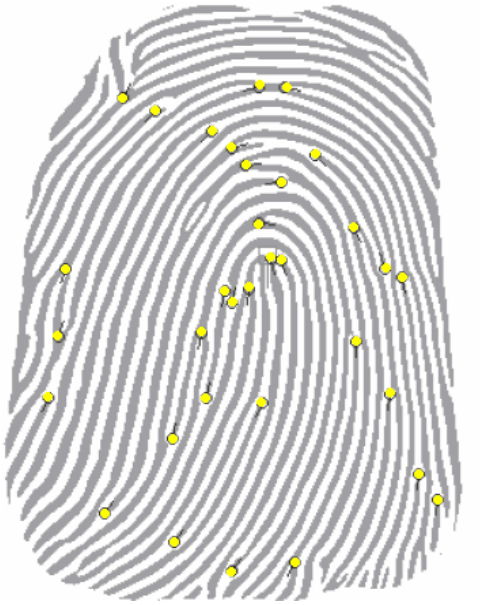
Obr. 25. Základní rozdělení typů otisků prstů

Pokud mají snímače otisků střežit cennější statky (například podniková data, automobily atd.) bývají ještě opatřovány tepelným snímačem. Má zabránit tomu, aby vetřelec nepoužil samotný prst, který od oprávněné osoby oddělil proti její vůli. Není ale třeba mnoho zvrácené fantazie, aby se našlo řešení. Konstruktéři proto vyvíjejí jiné metody nebo čtečky alespoň kombinují s vyhodnocováním dalších biometrických znaků. Lepší metodou jak využít rozdílnost jedinečných biometrických vlastností prstů je skenování průběhu cév uvnitř prstu zcela neinvazivní metodou. V Japonsku se tímto způsobem v současnosti zajišťují bankomaty, vstupy do místností či jednotlivé počítače. [11]

Klasifikace otisku

Při klasifikaci se používají vzory otisku a posloupnosti, ve kterých se vyskytují, k přípravě vzorce pro rozdělení vzoru do podskupin. Toto je základem klasifikace získaných otisků.

Ovšem klasifikace otisku a identifikace otisku jsou dva odlišné pojmy. Klasifikace se týká především evidovaných vzorů s otisky. Identifikace otisku je současné porovnávání jednoho otisku s druhým pomocí identifikačních bodů.

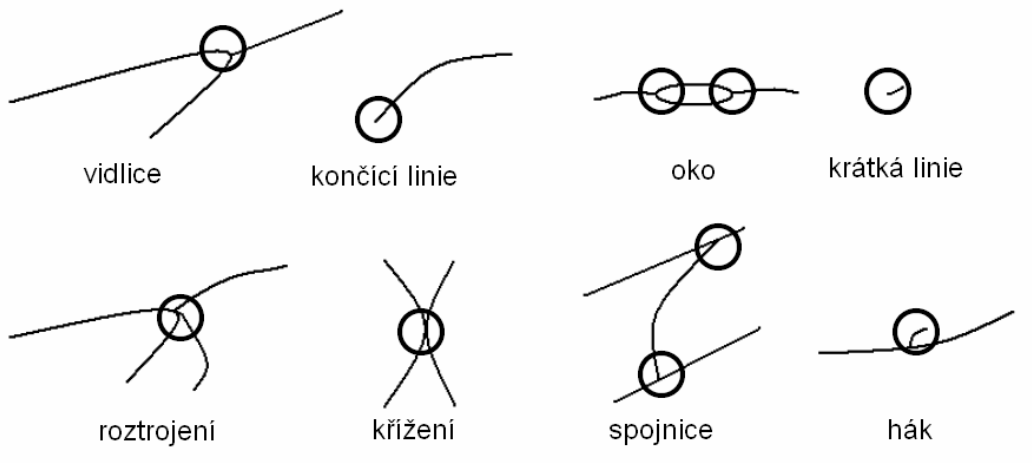


Obr. 26. Identifikační body na otisku prstu

Jednotlivé identifikační body

Systém, který chce navzájem porovnávat dva otisky, musí používat identifikační body. Tyto body se nacházejí v drážkách vzorů na bříškách prstů. Tyto body se nachází na některých z níže uvedených objektů.

- rozvětvení – konce dvou linií se spojují ve vidlici
- oko – uzavřená drážka s dvěmi navazujícími liniemi
- roztrojení – místo, kde se linie rozděluje na tři navazující linie
- křížení – místo, kde dochází k překřížení linií
- spojnice – přemostění mezi liniemi
- končící linie
- krátká linie
- body



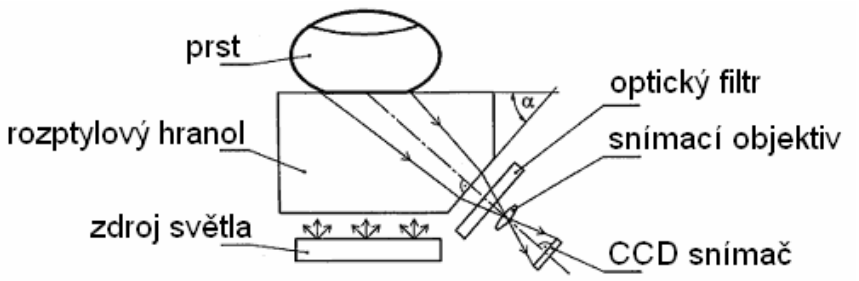
Obr. 27. Typologie identifikačních bodů na otisku prstu

Všechny z těchto objektů mají různou četnost jejich výskytů na otiscích prstů. Například krátké linie, rozdvojení a ukončovací linie jsou daleko frekventovanější než roztrojení, samostatné body a oko. Bezpečnostní systém musí být schopen rozpoznat tyto detaily a určit frekvenci, s jakou se vyskytují. Při porovnávání jednoho otisku s druhým, musí být na porovnávaném i vzorovém otisku přítomny stejné identifikační body. Tyto body musí mít zachovanou polohu a nacházet se na stejném místě. Musí mít stejný počet linií (drážek) ležících mezi identifikačními body, aby je bylo možné porovnat. Žádné body nesmí být odlišné, aniž by to bylo možné vysvětlit například tím, že nějaká nečistota nebo prach mohly zabránit pokračování linie na prvním otisku až do konce nebo vytvoření rozvětvení na druhém otisku. Každý otisk prstu obsahuje v průměru 75-175 identifikačních bodů. Neexistuje množina nebo požadovaný počet bodu nutný k pozitivní identifikaci mezi dvěma otisky. Posuzuje se kvalita otisku, jednoznačnost vzoru a identifikační body. [11]

Biometrická identifikační metoda porovnávání otisku prstu je nejrozšířenější a uživatelsky nejoblíbenější ověřovací metoda. Snímání otisků prstů má mnohaletou bohatou historii, takže se pro uživatele nejedná o nic cizího. Vlastní snímání je navíc poměrně rychlé a pohodlné. Existuje několik typů snímačů otisků prstů, z nichž mezi ty nejznámější patří optické, kapacitní a ultrazvukové. [11]

7.1.1 Optické snímače

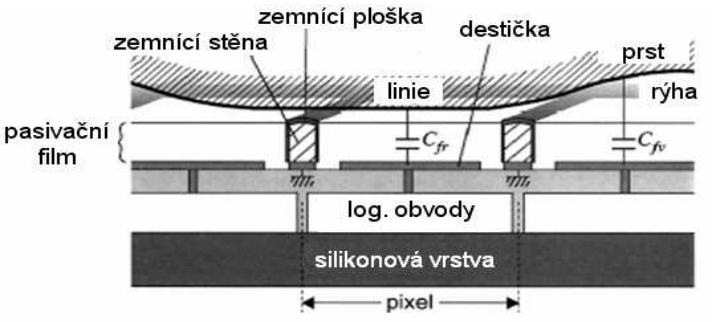
Optické snímače používají k osvětlování přiloženého prstu laserového světla. Následně dochází ke zkoumání rozptylu nebo odrazu světla v místech, kde se papilární linie přiloženého prstu stýkají se snímací plochou. Světlo, které dopadne na papilární linii, je odraženo zpět, naopak světlo dopadající do rýhy prstu se neodráží. [11]



Obr. 28. Optický snímač otisku prstu

7.1.2 Kapacitní snímače

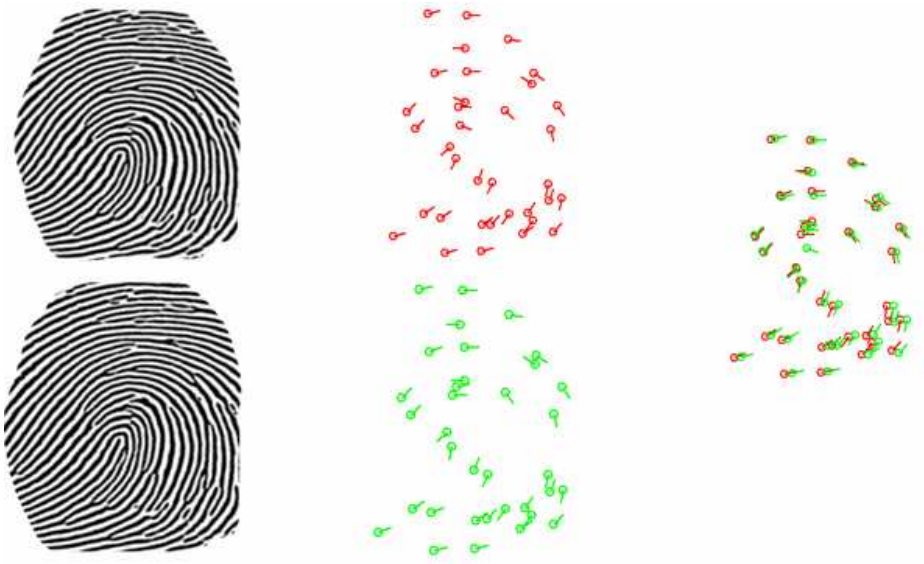
Kapacitní snímače se nazývají také silikonové. Měří kapacitní odpor v ploše dotyku prstu se snímací podložkou, kdy přiložený prst funguje jako jedna deska kondenzátoru a snímací podložka zastává druhou. Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor. Rozdíly těchto hodnot se zachytí a podle nich se vytvoří obraz otisku prstu. [11]



Obr. 29. Kapacitní snímač otisku prstu

7.1.3 Ultrazvukové snímače

Ultrazvukové snímače používají patentovanou technologii, jejímž vlastníkem je společnost Ultrascan. Čtecí zařízení při snímání vysílá zvukové vlny a díky následnému měření odporu kůže získá vzor papilárních linií na snímaném prstu. Technika ultrazvukového snímání se vyznačuje vysokou přesností i při znečištění prstu, čtecí zařízení však nabývá poněkud větších rozměrů. Algoritmy rozpoznávající otisk prstu mohou pracovat na základě zkoumání buď globálního vzoru, nebo podrobností otisku prstu. [11]



Obr. 30. Porovnávání identifikovaného otisku prstu

Obr. 31. Jeden ze způsobů duplikování otisku prstu

Úspěšnost kopie otisku prstu vyrobené podle postupu na Obr.32 se udává 70%. Z tohoto hlediska nemohu doporučit použití této technologie identifikace jako soběstačné. Pokud někdo chce používat otisky prstů k identifikaci doporučuji tuto technologii zkombinovat s nějakou další. [11]

Výhody použití biometrie otisku prstu

- nezaměnitelnost otisku prstu s jiným otiskem prstu
- pokud je otisk trochu poškozen, dojde přesto k rozpoznání osoby
- snadné použití v praxi
- nízké pořizovací náklady

Nevýhody použití biometrie otisku prstu

- otisk prstu lze s úspěchem duplikovat
- pro malou bezpečnost je nutné tuto technologii zkombinovat s některou další

7.2 Biometrická identifikace hlasem

Tvar a rezonance vokálního traktu (hlasivek, ústní dutiny, jazyka a zubů) je dostatečně odlišný u různých osob, takže metoda měření lidského hlasu muže být použita pro jejich identifikaci. Rozpoznávání hlasu a ověřování hlasu jsou dvě biometrická měření, která se používají zejména k řízení přístupu do informačních systému prostřednictvím telefonu.

Při rozpoznávání hlasu mluvčí vysloví slovo a systém určí které slovo v databázi odpovídá této výslovnosti. Toto určení systém provede na základe porovnání vyřčené výslovnosti s množinou výslovností uloženou v databázi a výběrem té, která vzhledem k ostatním slovům v této množině vyhovuje vyřčenému nejlépe. Na druhé straně, při ověřování hlasu je výslovnost mluvčího porovnána s dříve pořízeným záznamem a systém musí určit, do jaké míry se s ním shoduje. Tato shoda musí být absolutní, nikoliv relativní. Celkem, rozpoznávání vybírá největší shodu, s přihlédnutím k tomu, jak velká je shoda, zatímco ověřování je založeno na úplné shodě.

Porovnávání hlasu je nejlevnější metoda vzhledem k tomu, že je používán běžný mikrofon. Hlasové srovnání je ovšem poměrně nespolehlivé. Stačí si nachladit hrdlo zmrzlinou nebo vypít pár studených nápojů a verifikace hlasu nebude úspěšná. Pak můžete čekat u identifikačního zařízení než se vám vrátí správná intonace hlasu. [11]

Výhody použití biometrické identifikace hlasem

- snadné použití v praxi
- nízké pořizovací náklady

Nevýhody použití biometrické identifikace hlasem

- každá změna hlasu vede k neúspěchu při identifikaci
- technologii oklame nahrávka hlasu, jejíž pořízení je snadné
- není vhodné použít tuto technologii samostatně

7.3 Biometrická identifikace podpisu

Tato biometrická metoda identifikuje osobu na základě jejího podpisu s využitím velice spolehlivého biometrického zařízení použitého k jeho snímání. Osoba, která se identifikuje bude požádána o podpis. Podpis nebo iniciály se píší na speciální podložku s perem k ní určeným. Systém ověřuje podpis osoby na základe srovnání s uloženým podpisovým vzorem, který popisuje jak byl popis napsán. Není tedy důležitá jen podoba podpisu a tvar písmen, i když o to jde samozřejmě také. Tato metoda srovnává dynamiku podpisu, provedení tahu, sílu, se kterou tlačíme při psaní na podložku a rychlost psaní. Tyto vlastnosti podepisování nám dohromady dávají jednoznačnou charakteristiku podpisu osob.

- tlak pera
- styl písma
- rychlost

Každý podpis vyžaduje pouze 500 bajtů, takže jich na jediném serveru může být uloženo až několik stovek tisíc, nebo data podpisu lze uložit na magnetickou kartu a nejlépe na čipovou. Pro tuto biometrickou metodu se používá podložka citlivá na tlak, LCD, VGA displej který snímá pozici v ose X a Y a tlak elektronického pera. [11]

Výhody použití biometrie podpisu

- jedinečnost dynamiky podpisu nelze okopírovat (tlak pera a rychlost psaní)
- technologie je bezpečná a spolehlivá
- přirozenost (podepisování je běžná rutina)
- snadné použití v praxi

Nevýhody použití biometrie podpisu

- podpisový vzor lze kopírovat

7.4 Biometrická identifikace oční duhovky

Biometrická identifikace duhovky je založena na snímání lidské duhovky. Stejně jako například otisky prstu, i duhovku oka má každý člověk jedinečnou. Proto se tohoto faktu využívá pro identifikaci osob, zvláště v případě oprávnění k přístupu do informačního systému. Je tu vzhledem k otiskům prstu významný rozdíl. Nalezení dvou identických duhovek náhodným výběrem je přibližně 10^{54}krát menší než nalezení dvou identických otisků prstů. Také duhovky dvou identických dvojčat jsou samozřejmě zcela rozdílné a jedinečné. Ve skutečnosti jsou obě duhovky jednoho člověka rozdílné a jedinečné. Z tohoto pohledu neexistuje jiná externí biometrická charakteristika člověka, která by byla více rozlišovací než právě duhovka. Co se týče automatické identifikace, tak ta se považuje za velice důvěryhodný základ pokročilého identifikačního systému. [11]

Princip metody verifikace oční duhovky

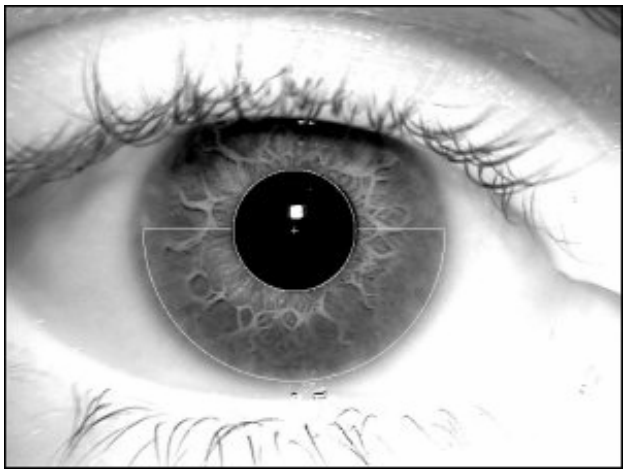
Metoda je založena na individuálnosti rozmístění a tvaru skvrn na duhovce lidského oka. Duhovka je externě viditelná a její snímání biometrických dat k verifikaci se provádí standardní video kamerou. Osoba se dívá do polopropustného zrcadla, kde z druhé strany je

umístěna kamera. Po sejmutí snímku oka osoby se ze získaného obrázku zjistí charakteristické znaky oční duhovky, které se kódují, uloží do paměti. Metoda je velmi spolehlivá, avšak patentově chráněná. Charakteristické rysy duhovky se stabilizují brzy po narození a zůstávají beze změny po celý život člověka. Jako příklad spolehlivosti je uváděn obraz 12-ti leté afgánské dívky a obraz téže dívky identifikované po 18-ti letech. Duhovka se tedy časově nemění. Je zde možnost onemocnění oka nebo poškození oční rohovky při nehodě. Při deformaci duhovky také nedojde ke správné identifikaci osoby a její autorizace se zamítne. [11]

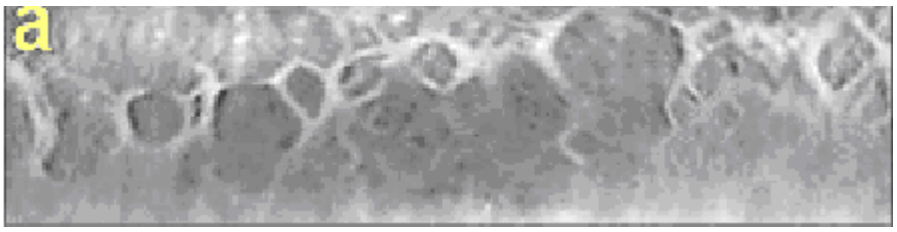
Obr. 32. Afgánská dívka identifikovaná po 18-ti letech

Popis metody snímání duhovky

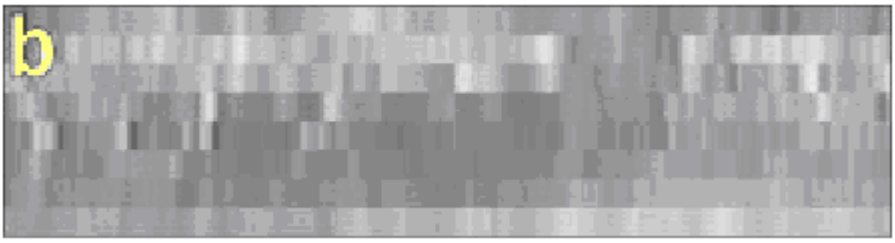
Nejprve se oční duhovka zachytí CCD snímačem a převede se do digitální podoby. Poté se oční duhovka převede do polárních souřadnic, provede se agregace obrazu do formátu 8×256 bodů a následně se transformuje Waveletovou transformací do 2d kódu (2D Gabor). Oční duhovka se porovnává se záznamem uloženým v databázi. [11]



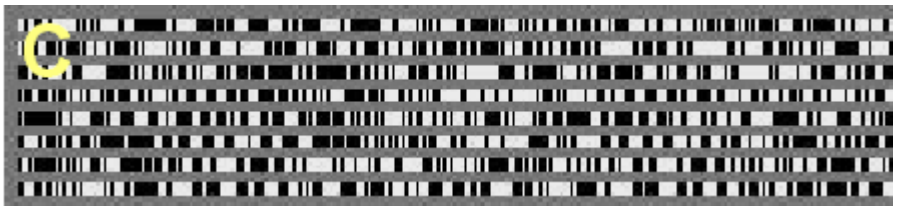
Obr. 33. Lidské oko s vyznačenou oční duhovkou



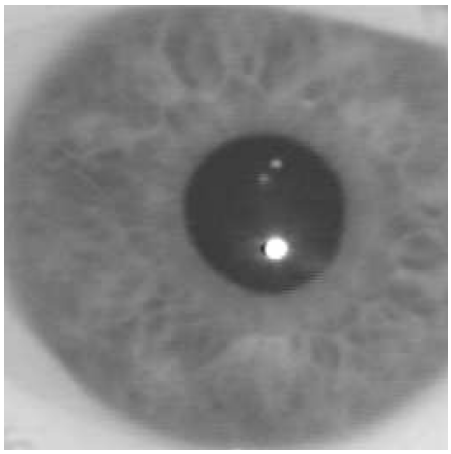
Obr. 34. Oční duhovka v polárních souřadnicích



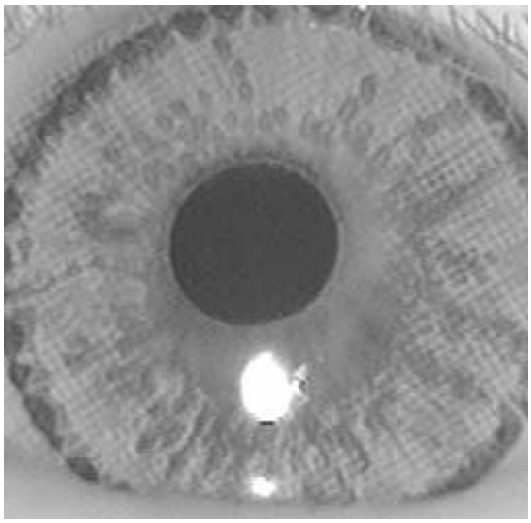
Obr. 35. Agregace obrazu oční duhovky do formátu 8x256 bodů



Obr. 36. Waveletova transformace snímku oční duhovky (2D Gabor)



Obr. 37 Oční duhovka člověka



Obr. 38 Nedokonalá kopie duhovky na kontaktní čočce

Výhody použití biometrie oční duhovky

- vysoká bezpečnost a spolehlivost
- duhovka se od jednoho roku života časově nemění (časová stálost)
- snadné použití v praxi

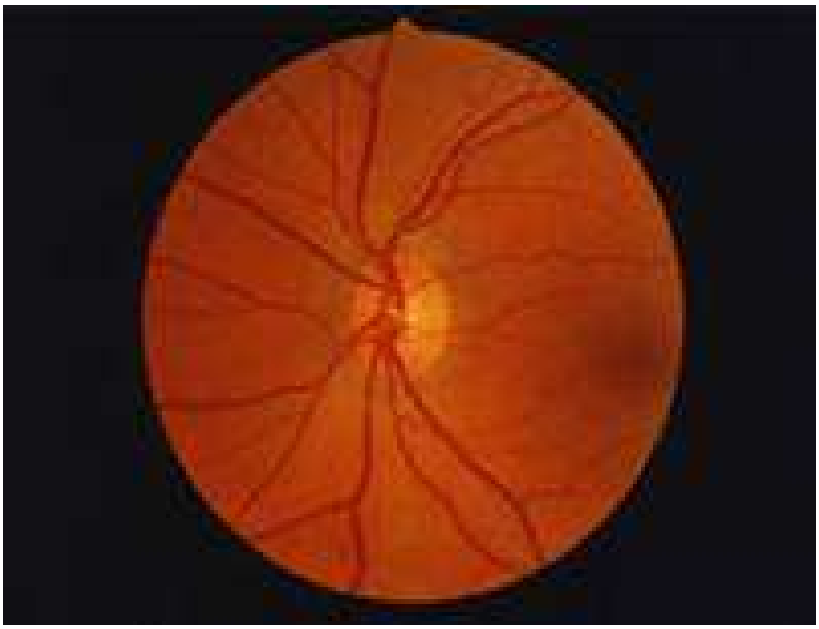
Nevýhody použití biometrie oční duhovky

- Vysoké pořizovací náklady
- Technologie chráněná patentem
- Pokud dojde k poškození rohovky osoba nebude rozpoznána

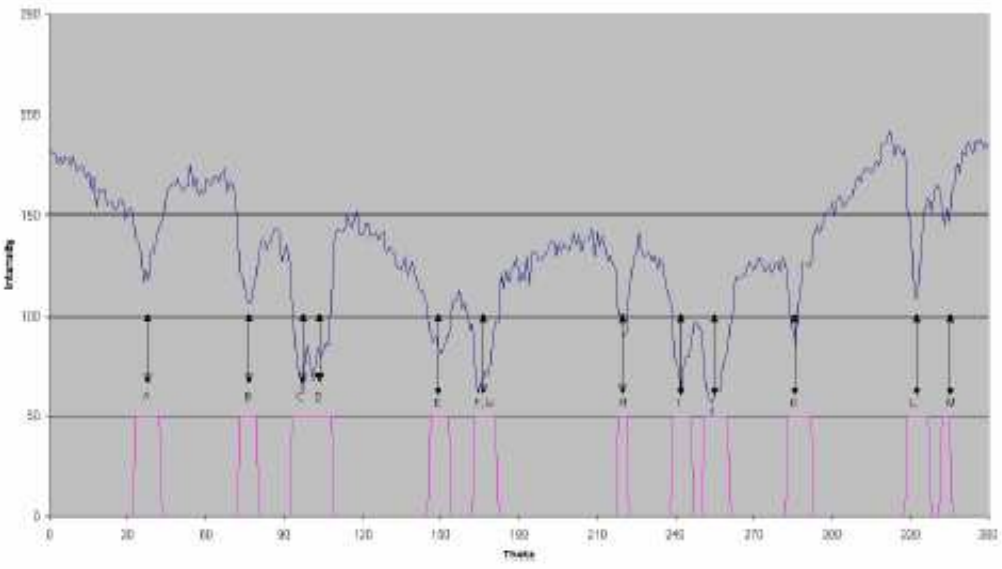
7.5 Biometrická identifikace oční sítnice

Sítnice je na světlo citlivý povrch zadní strany oka. Skládá se z obrovského počtu specializovaných nervových buněk, které se nazývají tyčinky a čípky. Tyto buňky převádějí světelné paprsky na nervové signály. Čípky poskytují barevné vidění. Díky své husté koncentraci umožňují čípky nejostřejší vidění. Tyčinky jsou mnohem citlivější na světlo než čípky, ale poskytují pouze černobílé vidění. Každá tyčinka a čípek je spojen s nervy, jejichž signály vystupují z oka pomocí očního nervu. Oční nerv, společně s artérií sítnice, vystupují z oka v bodě, kde nejsou žádné čípky ani tyčinky, jedná se o tzv. slepou skvrnu

na sítnici. Sítnice lidského oka je jedinečná a může být proto použita k identifikaci osob. Snímače sítnice lidského oka se jeví jako nejbezpečnější biometrická identifikační metoda. Neexistují chybná přijetí a chyba se také jeví být nemožnou. Bohužel stupeň chybných odmítnutí je vysoký, proto tato metoda nemůže být obecně přijatelná při identifikaci osob v masovém měřítku. Tato biometrická metoda identifikace našla uplatnění ve velmi redukovaných oblastech, jen pro velmi bezpečné kontrolní systémy, jako jsou jaderné reaktory nebo vojenská zařízení. [11]



Obr. 39 Oční sítnice



Obr. 40 Cévy znázorněné v polárních souřadnicích

Výhody použití biometrie oční sítnice

- vytvořit identický duplikát oka je nemožné
- technologie je na nejvyšší bezpečnosti (nepřekonatelná)
- bezpečné nasazení na ochranu cenných aktiv

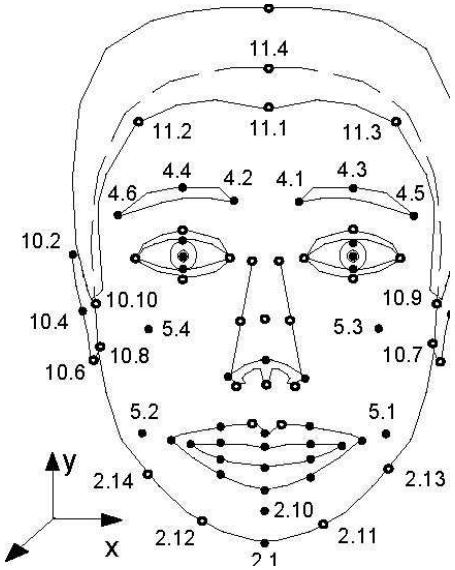
Nevýhody použití biometrie oční sítnice

- vysoké procento chybných zamítnutí (FRR)
- technologie není vhodná pro hromadnou identifikaci osob
- lidé neradi podstupují skenování očí (strach, že je něco píchne do oka)

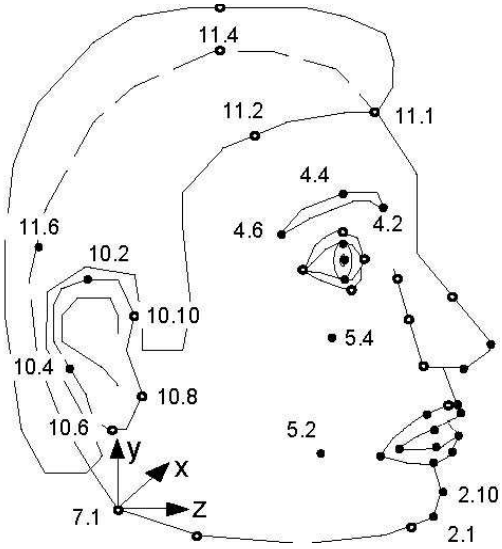
7.6 Biometrická identifikace geometrie obličeje

Rozpoznávání obličeje je založeno na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v paměti počítače. Ke snímání biometrických charakteristik obličeje se používá běžná kamera s dostatečným rozlišením. Autentizovaná osoba se nechá vyfotografovat a získaný portrét se digitálně zpracuje, aby mohl být využívaný k matematickému srovnání s identifikovaným obličejem. Pro vyhodnocení osob s použitím biometrie obličeje se používají metody obličejové metriky a metoda charakteristických obličejů. Autentizace podle obličeje je poměrně nespolehlivá a nepřesná metoda. Některá identifikační zařízení využívající k identifikaci porovnání biometrických vlastností obličeje jdou oklamat fotografií. U biometrického srovnání obličeje se vyhledávají základní body tváře (oči, nos, brada, ústa, uši apod.) a měří se vzdálenosti mezi těmito body. Základní idea spočívá v převedení obrazové funkce do číselného vektoru, který bude jednoznačný pro všechny vstupní údaje. K vytvoření daného vektoru se použijí takové prvky obličeje, které jsou snadno rozlišitelné a jejich závislost na osvětlení je malá, nejsou závislé na malých změnách velikosti a tvaru. Prvky obličeje musí mít co největší vypovídací schopnost. Tato metoda identifikace je výhodná i proto, že je účinná i v případech, kdy je vstupní obraz mírně rotován (až o 15 stupňů). Naměřené vzdálenosti slouží ke srovnání osoby identifikované terminálem s uloženými údaji. U charakteristických obličejů se zjišťuje míra shody portrétu s charakteristickými obličeji. U charakteristických obličejů,

kde se zjistí porovnáním největší shoda, se tyto míry shody ukládají a slouží k autentizaci osoby. [11]



Obr. 41 Geometrie obličeje zepředu



Obr. 42 Geometrie obličeje z profilu

Výhody použití biometrie obličeje

- snadné použití technologie (běžná kamera)
- identifikace může proběhnout bez vědomí sledované osoby

Nevýhody použití biometrie obličeje

- systém identifikace lze oklamat fotografií nebo maskou
- nevhodná technologie pro zabezpečení cenných aktiv

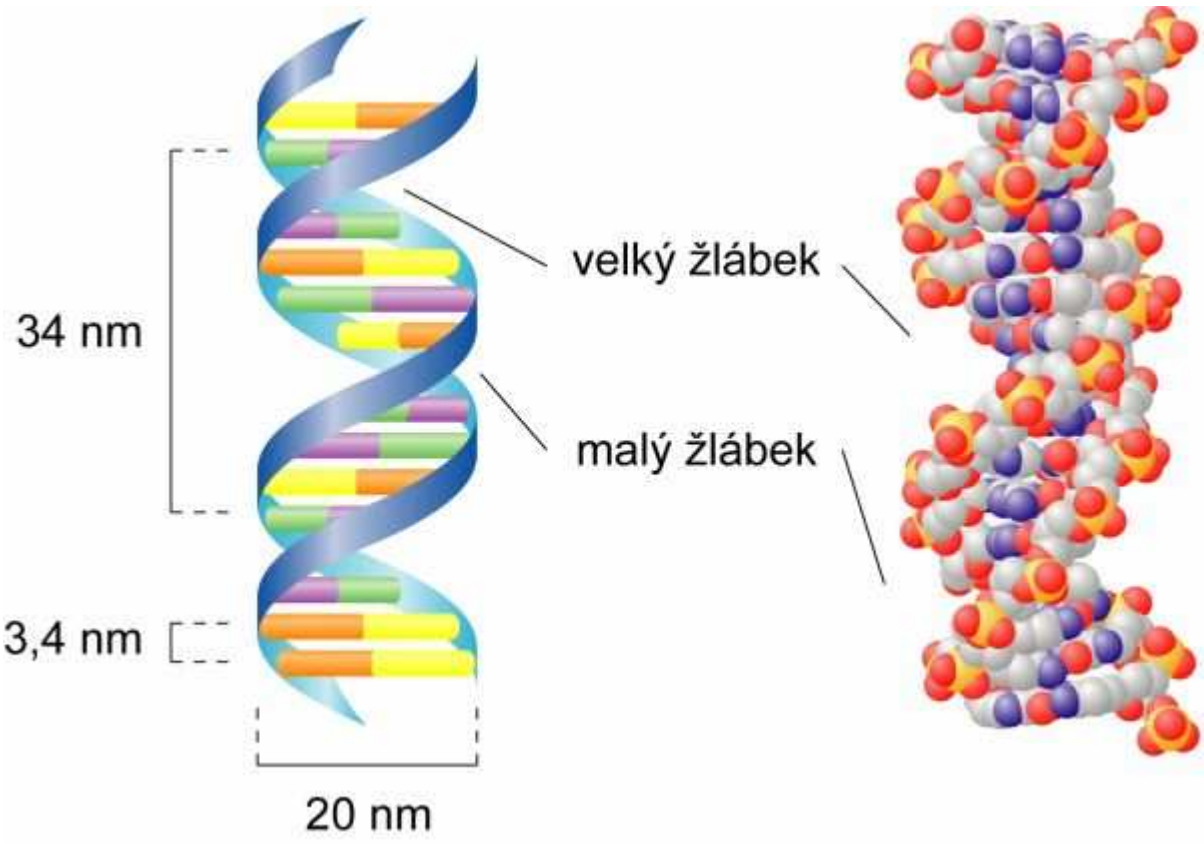
7.7 Biometrická identifikace založená na porovnávání DNA

Biometrická identifikace se opírá o jedinečnou strukturu DNA každého jedince. Na rozdíl od ostatních biometrických identifikačních znaků, které mohou být chirurgicky upraveny je struktura DNA stálá a je stejná pro každou buňku, tkáň i orgán člověka. DNA nelze doposud žádným způsobem změnit. [11]

Struktura DNA

Geny se dědí z generace na generaci, takže potomek získá řadu charakteristických rysů od svých rodičů. Kompletní genetický reprograf organismu je obsažen v každé jeho buňce. Kódový systém, který je podkladem pro reprograf, je založen na kódu v molekule DNA.

DNA je dlouhá molekula složena ze dvou vláken zkroucených do spirály zvané helix. Každé vlákno helixu je sestaveno z řetězce nukleotidových částí. Každá nukleotidová část obsahuje 3 složky: cukr, fosfát a jednu ze čtyř různých základních stavebních složek A, C, G, T (Adenin, Cytosin, Guanin, Thymin). Dva spletené řetězce helixu jsou svázány vazbami mezi nukleotidovými bázemi na protějších vláknech. To znamená, že posloupnost na jednom vlákně také určuje posloupnost na vlákně protějším. Také uvnitř vlákna je informace obsažená v dané části DNA určena přesným pořadím nukleotidových bází.

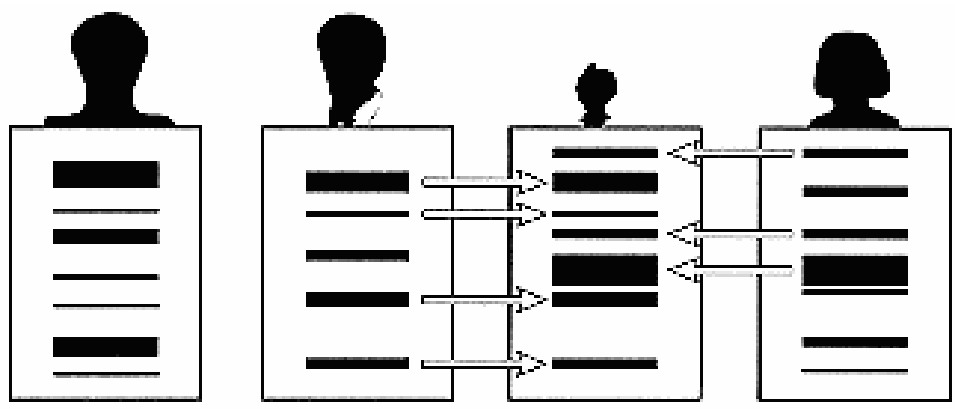


Obr. 43 Struktura šroubovice DNA

Princip identifikace se vzorkem DNA

DNA musí být získána z buněk nebo tkání těla, jako je krev, vlasy nebo kůže. Na rozbor DNA se používají restrikční enzymy, které štěpí DNA na určitých místech. Kousky DNA jsou setříděny podle velikosti prosévací technikou zvanou elektroforéza. Kousky DNA se

nechají projít gelem vyrobeným z agarosy (želatina vyrobená z jednoho druhu mořské řasy). Tato technika je biotechnologicky ekvivalentní prosévání písku přes postupně se zjemňující síta, čímž se určí velikost částice. Části DNA se umístí na plochou desku gelu. Gelem prochází elektrický proud. Protože DNA je nabitá záporně, pohybuje se směrem ke kladné elektrodě. Čím menší fragment DNA, tím rychleji se pohybuje. Oddělené fragmenty DNA se přenesou z gelu na nylonovou membránu umístěnou na jeho vrcholu. V tomto procesu se vlákna každého segmentu DNA chemicky rozštěpí. Následuje sondování, kde se přidáním radioaktivních nebo obarvených genových sond do nylonové membrány přenese vzorek, jehož rentgenový snímek se nazývá DNA-otisk. Každá sonda typicky ulpí jen na jednom nebo dvou specifických místech na nylonové membráně. Konečný DNA-otisk se vystaví působení několika sond (5-10 nebo více) současně. Výsledný obraz se podobá čárovým kódům. [11]



Obr. 44 Ukázka jedinečnosti DNA-otisku

Současné využití DNA-otisků

USA v současnosti využívá DNA-otisky v laboratořích FBI a také u policie ke zjištění vazeb podezřelých na biologickou evidenci. Porovnávají DNA získanou z krvavých stop, tkání a vlasů nalezených na místě činu. Od roku 1987 byla s použitím DNA-otisku vyřešena řada případů. DNA-otisky našli využití také k identifikaci otce dítěte v soudním systému, kdy je třeba stanovit otcovství v případech opatrovnictví a sporech o podpoře dítěte. Každý buňka jedince obsahuje stejný DNA-otisk, proto armáda Spojených států začala sbírat DNA-otisky všech osob pro pozdější použití v případě, kdy potřebují identifikovat oběti nebo osoby ztracené v akci. Metoda DNA-otisku začala být nadřazena metodám, které se používají dnes, jako jsou zubní karty nebo krevní skupiny. [11]

Výhody identifikace využitím DNA-otisku

- stačí pouze malý vzorek DNA, ke srovnání
- člověk za sebou neustále nechává stopy DNA
- neomylná identifikace

Nevýhody

- vzorek DNA lze získat bez vědomí nositele
- vyhodnocování DNA je drahé
- k ověření DNA je nutné odebrat vzorek (byť jen nepatrný)

8 SPECIFIKACE VÝVOJOVÝCH TRENDŮ

Vývojové trendy v oblasti identifikačních prostředků se nedají jednotně zhodnotit. Každá řada identifikačních prvků neslouží pro využití pouze v jedné aplikaci, ale je použita v několika možných odvětvích, kde je zrovna konkrétní technologie zapotřebí. Zaměřím se zde tedy na skupiny identifikačních prostředků podle technologie, kam by se mohl ubírat vývoj těchto identifikačních prostředků, které zde nadále setrvají a také ty, které dříve či později z důvodu jejich slabých míst zaniknou nebo se jejich použití posune do odvětví průmyslu, kde nebude potřeba takových nároků na spolehlivost.

Jakákoli dlouhodobá prognóza v tak dynamickém odvětví, jakým jsou identifikační prostředky osob je rozporuplná. Omezím se proto na odhad použitých vylepšení hlavních budoucích trendů, bez specifikace předpokládané doby realizace.

8.1 Budoucnost čárových kódů

Protože vývoj se nedá zastavit, tak ani vymizení používání čárových kódů jako identifikačního prostředku osob vzhledem k jejich jednoduchosti a tedy slabinám nelze odvrátit. Současně se můžeme ojediněle setkat s identifikací osob čárovými kódy někde na seminářích, kde nám pořadatelé semináře přidělí identifikační kartu. Ovšem i na těchto akcích je již využíváno jiných technologií mnohem profesionálnějších, kterými jsou karty s magnetickým proužkem. Dá se tedy říci že čárové kódy nemají v identifikaci osob žádnou budoucnost, ale mají stále budoucnost v oblasti označování zboží, přičemž cenné zboží, které to bude umožňovat bude označováno 3D čárovými kódy. 3D čárové kódy umožní při nákupu dopravního prostředku ověřit, že vozidlo a některé jeho díly jsou opravdu totožné s majitelem vozu.

8.2 Jak se bude vyvíjet kontaktní čipová karta

V oblasti hardware již nyní nastupují 32 bitové procesory, které umožní posunout mnohem dále možnosti současných čipových karet. Zejména platforma Java Card, která dominuje v mnoha oblastech, bude povýšena na vyšší generaci, umožňující využívat čipovou kartu jako komponent začleněný do počítačové sítě.

V oblasti software je očekávána implementace Java Standard Edition na čipové kartě, což mimo jiné umožní programátorům využívat všechny standardní datové typy, organizaci

paměti, RMI a protokol TCP/IP. Jedním z přínosů nové generace čipových karet založených na plné implementaci prostředí Java bude zvýšení přenositelnosti aplikací na čipové karty a snazší vývoj kódu pro běžné programátory. V souvislosti s implementací TCP/IP na čipové kartě lze očekávat i odklon od standardizovaných protokolů založených ISO/IEC 7816-4, které jsou současně 15 let staré a využití komunikačních a aplikačních protokolů založených na TCP/IP.

8.3 Bezkontaktní čipové karty s výhledem do budoucnosti

U bezkontaktních čipových karet je budoucnost zaručena. Ovšem v budoucích letech se bude pracovat na tom, aby bezkontaktní komunikace mezi čtečkou a kartou zaručila takovou bezpečnost jako je to u zatím nepřekonané technologie kontaktních čipových karet. Zřejmě ještě pár let potrvá než se stane používání bezkontaktních čipových karet každodenní součástí obyvatel naší země. Do budoucna bude implementace bezkontaktních čipových karet směřována do sektoru cestovních pasů a později také jako občanské průkazy. Přičemž takovým hlavním cílem bude sjednotit cestovní pas a občanský průkaz do jednoho dokladu. Dále se nám nabízí možnost bezkontaktního ověřování řidičského oprávnění, což je velmi blízká budoucnost.

8.4 RFID Tokeny s výhledem do budoucnosti

Rádio-frekvenční identifikační značky nebo-li tokeny jsou v současnosti také velice rozšířeny a je jen otázkou morálních zásad a přesvědčení lidí, zda se nám tato technologie doslova nedostane pod kůži. Je běžná věc, že se touto technologií označují zvířata. Tato identifikační značka v budoucnosti implementovaná pod kůži člověka může vyvolat strach a také jej u mnoha lidí nesporně vzbudí. Otázka proč mám mít identifikátor pod kůží, když se po té stanu cílem teroristů já sám. Když se nad tímto zamyslíte co bude tedy následovat jako řešení, abychom tuto nedůvěru zmírnili? Nabízí se nám na to řešení použít snímání životních funkcí a zajistit inteligentní funkci čipu. Pokud bude čip vyjmut z těla bude nefunkční a pokud bude například odebrána končetina, ve které je čip implementován bude opět funkce čipu zrušena. Těmito otázkami se budeme zabývat možná dříve jak za 20 let.

8.5 Biometrické identifikační prostředky s výhledem do budoucnosti

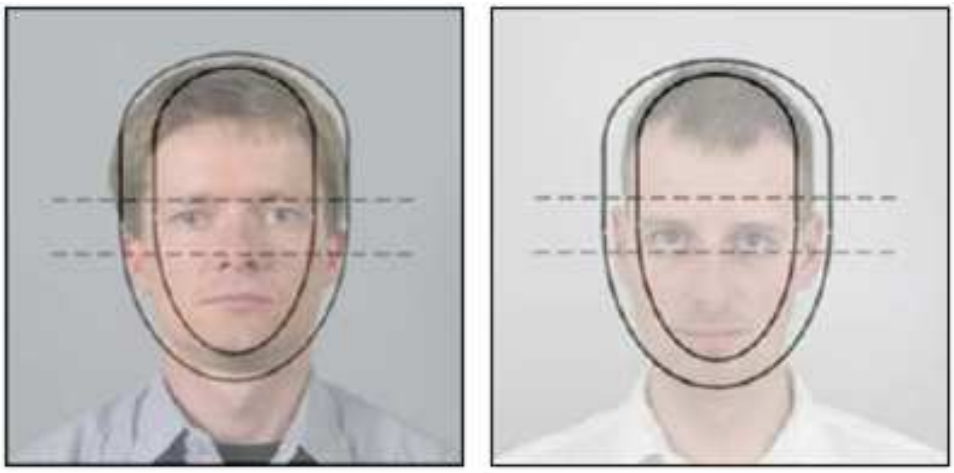
V budoucnu budou biometrické identifikační prostředky stále více využívány. Neustále se budou posouvat etické hranice pro jejich masové nasazení. Současně se biometrických identifikačních prvků využívá k ochraně letišť a leteckého provozu. Biometrické identifikační prostředky se však dostali i do oblasti komerčních přístupových systémů. Spouštěcím mechanismem pro jejich větší nasazení byly teroristické útoky z 11. září 2001. Bude nutné, aby bylo ověřování bezpečné integrovat biometrické informace o identifikované osobě přímo do identifikační čipové karty nebo do předchozí uváděné technologie tedy RFID tokenů. Databáze tedy nebudou nikdy tak bezpečné, aby se někdo nepokusil informace, které databáze shromažďuje získat. Proto je nutné přejít na metodu přímé verifikace biometrických údajů osoby s údaji, které bude mít vždy sebou na nějakém paměťovém nosiči.

Bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech

Zavedení biometrických prvků do cestovních dokladů naše vláda schválila roce 2005. Podle nařízení rady Evropské Unie mají členské státy EU cestovní doklady, které budou obsahovat bezkontaktní čip. Uvnitř čipu se pak budou nacházet biometrické prvky, konkrétně to má být biometrické zobrazení obličeje a digitálně zpracované otisky prstů. Protože stále častěji dochází k teroristickým útokům, bylo také nutné zvýšit bezpečnostní standardy pro cestovní doklady vydávané členskými státy EU. Zavedení si také vyžádali i Spojené státy americké, aby se v případě České republiky mohl zavést bezvízový styk. Povinnost zavést digitálně zpracovanou fotografii do pasu byla pro členské státy EU stanovena do data 28.8.2006. Otisky prstů by měli být zavedeny do poloviny roku 2008. Žádost o cestovní pas bude možné podat pouze na obecním úřadě obce s rozšířenou působností příslušného podle místa trvalého bydliště a v zahraničí na zastupitelských úřadech.

Protože se zde pracuje s osobními údaji, jsou také zavedena příslušná pravidla. Digitální fotografie a otisky prstů se mají pořizovat přímo na úřadech, na kterých budou podávány žádosti o cestovní doklad. Otisky prstů nebudou vedeny v žádné databázi. Po vyrobení cestovního dokladu a uplynutí reklamační lhůty (60 dní) budou záznamy o otiscích prstů zničeny. Po úplném zapojení České republiky do schengenské spolupráce se zavedli kontroly biometrických prvků na letištích obsluhující mimo schengenské lety.

Zde je možné předpokládat, že v blízké budoucnosti nebude docházet k padělání cestovních dokladů tak, jako v současném měřítku. Ani v budoucnosti nebude výjimkou, že kdo má vysoké finanční prostředky, má také větší možnosti obcházet zákony. S výhledem do budoucna je možné, že identifikace osob se zautomatizuje do takové míry, aby se mohlo vyloučit selhání lidského faktoru. Aktuálně platí, že biometrické údaje v pasech smějí být používány pouze pro ověřování pravosti dokumentu a totožnosti jeho držitele, a to za použití přímo dostupných porovnatelných prvků, kdykoli právní úprava vyžaduje předložení cestovního pasu. [12]



Obr. 45 Vzor focení obličeje do cestovního dokladu

ZÁVĚR

Cílem této práce bylo zhodnotit trendy vývoje identifikačních prostředků v oblasti naplnění bezpečnostní politiky organizace. Postupnou analýzou každého z uvedených identifikačních prostředků, jsem vyhodnotil jejich přednosti a slabá místa, se kterými by se měli nastupující technologie postupně vypořádat.

Organizace, které se zamýšlejí nad použitím identifikačních prostředků, aby tak zvýšily komfort a bezpečnost uvnitř organizace by měly zvážit jejich výběr podle účelu použití. Zavedení přístupového systému přinese do organizace kontrolu nad pohybem zaměstnanců a dále tu výhodu, že můžeme spořit energie, které organizace spotřebovává. Úspora energií je možná v inteligentních budovách, kde jsou systémy vytápění, klimatizace, osvětlení a rozvodů elektrické energie napojené na přístupový systém, který je speciálně naprogramován. Přístupový systém po úspěšné autentizaci osoby může zapnou v její kanceláři vytápění, automaticky zapnout zásuvku, ve které je kávovar nebo počítač. Takto se ušetří velké množství energie.

Výběr identifikačních prostředků je závislí na tom, co chceme chránit, jak spolehlivou technologii potřebujeme, na jakém místě ji chceme používat a na ceně technologie. Pokud potřebujeme opravdu rychle odbavovat klienty musí být identifikační zařízení rychlé a míra spolehlivosti chybného odmítnutí musí být co možná nejmenší. Na takové terminály se dají používat karty s čárovým kódem, karty s magnetickým proužkem, bezkontaktní čipové karty, RFID tokeny nebo biometrické identifikační prostředky s vyšší mírou chybného přijetí (FAR). Všechny tyto technologie slouží pro rychlou a jednoduchou identifikaci, avšak nezaručují takovou bezpečnost, aby se dali samostatně využít pro ochranu velice cenných aktiv. Pro ochranu vysokých hodnot doporučuji v organizaci využívat prostředky, jako jsou biometrie oční duhovky nebo biometrie sítnice, kde je ovšem vyšší míra chybného odmítnutí (FRR). Takové systémy nepropustí nesprávnou osobu k aktivům, ovšem osoba mající pověření se může identifikovat několikrát, než ji systém identifikuje jako oprávněnou osobu.

Ve své práci tedy uvádím přednosti a slabá místa jednotlivých technologii, ale konkrétní řešení v oblasti naplnění bezpečnostní politiky organizace se bude případ od případu lišit. Je tedy nemožné navrhnout univerzální řešení, které by se dalo ve všech organizacích beze změn použít.

CONCLUSION

The main aim of this dissertation was to assess trends of identification equipments in terms of fulfillment of organization's safety standards. Each presented analyses of identification equipment indicated their main advantages and drawbacks. It should be mentioned that innovative technology of contemporary identification equipments is believed to eliminate those drawbacks step by step.

When considering establishing the use of identification equipments within the organization to gain comfort and better security the main criteria for the selection should be the purpose of the use. For instance access system brings the opportunity to control the operation of staff and moreover it can save energy. The coveted economy use of energy is reached through the saving of power in terms of air conditioning, lights or electrical power network that is all operated by integrated access system which has been specifically programmed. Such access system after authentication of authorized person can switch the central heating on or activated the plug that provides power for the kettle or computer. It has been proved that these systems can safe significant amount of energy.

The process of choice within the available identification equipments is dependant on the needs of the organization. It has to consider what facilities should be protect and to what extend and also the price of investment. In case of quantitative intensity character of the identification equipments in use the false acceptance rate that is desirable to be as small as possible and the speed should meet the requirements. Then, identification card with magnetic stream, identification chip card contact less, RFID tags or biometric identification equipment can by used.

All the listed technologies provide fast and uncomplicated identification however the level of security is not good enough to protect valuable assets. To secure highly valuable assets it is recommended to employ such identification equipment as iris biometry, retina biometry, there is false rejection rate. Those identification equipments guarantee authorize usage but it may require longer time to make the identification.

The purpose of this study was to determine advantage and disadvantage of particular identification equipments. The findings revealed that the best solution for each organization must vary in terms of specific needs and premises. Therefore it is not possible to design universal solution for all organizations.

SEZNAM POUŽITÉ LITERATURY

[1] Judr.Laucký, V.: Technologie komerční bezpečnosti II., UTB Zlín, 2004

[2] Přínosy zpracování bezpečnostní politiky [online].[cit 2007-04-05], Grape Services a.s., Praha. Dostupný z WWW: http://www.grapeservices.cz/

[3] Čárové kódy [online].[cit 2007-04-10], Stanislav Duben, ČVUT Praha. Dostupný z WWW: http://www.duben.org/skola/fel/5.rocnik/NM/Index.htm

[4] Karty s magnetickým proužkem [online].[cit 2007-04-15], CardCode, Písek. Stránky firmy s ID prostředky. Dostupný z WWW: http://www.cardcode.cz/

[5] Technická norma. [online].[cit 2007-04-20], Stránky zabývající se elektronikou. Dostupný z WWW: http://www.id2.cz/normy/7816_part1_CZ.pdf

[6] Identifikační karty [online].[cit 2007-04-25], OKsystem s.r.o., Praha. Dostupný z WWW: http://portal.oksystem.cz/

[7] Čipové karty [online].[cit 2007-04-05], P.Hanáček, V.Matyáš, Brno. Dostupný z WWW: http://www.datakon.cz/datakon03/d03_tut_hanacek.pdf

[8] RFID Sokymat [online].[cit 2007-05-05], CYNTAG, Inc., USA. Dostupný z WWW: http://www.cyntag.com/

[9] USB Tokeny [online].[cit 2007-05-10], Cesnet, Praha. Dostupný z WWW: http://www.cesnet.cz/doc/techzpravy/2005/usbtokeny/

[10] Vize budoucnosti [online].[cit 2007-05-15], Ing.B.Nohelová, Praha. Dostupný z WWW: http://www.vesmir.cz/clanek.php3?CID=5914

[11] Zabezpečovací systémy [online].[cit 2007-05-20], Doc. Ing. Karel Burda, CSc. FEKT VUT, Brno. Dostupný z WWW: http://147.229.144.38/mzys/

[12] Elektronické pasy [online].[cit 2007-05-25], Ministerstvo vnitra, Praha. Dostupný z WWW: http://www.mvcr.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Přístupové systémy (ACCESS)
BP	Bezpečnostní politika
CCTV	Kamerové systémy a televizní okruhy
EAN	Evropské číslování zboží (European Article Number)
EEPROM	Electronically Erasable Programmable Read-Only Memory
EPROM	Erasable Programmable Read-Only Memory
EPS	Elektrická požární signalizace
EZS	Elektrická zabezpečovací signalizace
FAR	Míra chybného přijetí (False Acceptance Rate)
FRR	Míra chybného odmítnutí (False Rejection Rate)
HiCo	High Coercivity
ISO	Mezinárodní organizace pro normalizaci (International Organization for Standardization)
JRE	Java Runtime Environment
LoCo	Low Coercivity
OCR	Optické rozpoznávání znaků (Optical Character Recognition)
PIN	Osobní identifikační číslo (Personal Identification Number)
PKI	Prostředí, které umožňuje ochranu informačních systémů, elektronických transakcí a komunikace (Public Key Infrastructure)
RAM	Random-Access Memory
RFID	Identifikace na radiové frekvenci (Radio Frequency Identification)
ROM	Read-Only Memory
TCP/IP	Transmission Control Protocol (TCP), Internet Protocol (IP)
USB	Univerzální sériová sběrnice (Universal Serial Bus)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK