Systémy elektronické kontroly vstupu a návrh rozšíření jejich funkčnosti

Electronic Access Control Systems and a Proposal to Extend Their Functionality

Bc. Lukáš Sucháček

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Bc. Lukáš SUCHÁČEK**
Osobní číslo:	**A10340**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Systémy elektronické kontroly vstupu a návrh rozšíření jejich funkčnosti**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na principy elektronické kontroly vstupů (EKV).**
2. **V rámci rešerše se zaměřte na současně využívané systémy pro EKV, uveďte jejich přednosti a nedostatky.**
3. **Uveďte a popište metody identifikace používané v oblasti EKV a uveďte jejich principy, výhody i možnosti zneužití.**
4. **Na základě průzkumu trhu analyzujte a v přehledné formě uveďte, které funkce typickým uživatelům systémů EKV chybějí a které naopak nevyužívají.**
5. **S využitím předchozích zjištění navrhněte vylepšení systémů EKV a to včetně návrhu implementace nových funkcí.**
6. **Vhodnost a funkčnost řešení v rámci teoretické roviny ověřte a popište, jakým směrem se dle Vás bude ubírat oblast dané problematiky v blízké budoucnosti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, S. a kol.: Příručka zabezpečovací techniky. 3 vydání Blatná; Cricetus, 2006. 313 s. ISBN 80-902938-4.**
2. **KINDL, J.: Projektování bezpečnostních systémů I. 1. vyd. UTB Zlín 2004.ISBN 80-7318-165-7.**
3. **VLČEK, J.: Bezpečnost elektrických zařízení. Praha: BEN, 2007. ISBN 978-80-7300-222-0.**
4. **UHLÁŘ, J.: Technická ochrana objektů. 1. vyd. Praha: 2001. 205 s. ISBN 8072510762.**
5. **MATYÁŠ, Václav. Principy a technické aspekty autentizace. Data Security Management, Praha, Tate International., 2007, vol. XI, no. 1. s. 10 -16, ISSN 1211 -8737.**

Vedoucí diplomové práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Konzultant: **Ing. Radek Pospíšil**

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce pojednává o dostupných systémech elektronické kontroly vstupu, a zabývá se návrhem rozšíření její funkčnosti. Teoretická část se skládá z rešeršní činnosti na dané téma, a používanými metodami identifikace osob. Praktická část práce se zabývá analýzou průzkumu trhu a návrhem konkrétního systému na základě informací získaných průzkumem.

Klíčová slova: EKV, přístupový systém, čtečka, identifikace, identifikační médium.

ABSTRACT

This thesis deals with the available access control systems, and discusses a proposal to extend its functionality. The theoretical part consists of literature search activity on a given topic, and methods used for identifying persons. The practical part deals with the analysis of market research and proposal a specific system based on information obtained survey.

Keywords: ACS, access system, card reader, identification, identification media.

Na tomto místě chci poděkovat vedoucímu mé diplomové práce doc. Mgr. Milanu Adámkovi, Ph.D. za odborné vedení při její tvorbě.

Současně děkuji Ing. Radku Pospíšilovi z firmy JIMI CZ, a.s. za konzultace, cenné rady, podněty, připomínky a vstřícný přístup během zpracování této práce.

V neposlední řadě děkuji mé rodině za morální i materiální podporu během celého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době jsou stále častěji kladeny zvyšující se nároky na ochranu soukromí a s tím spojenou ochranu osobních údajů a dat. Tento fakt se ve velké míře týká bezpečnostních aplikací a systémů, přicházejících do styku s těmito informacemi. Mezi tyto patří systémy pro elektronickou kontrolu vstupu (EKV), které sice majetek nechrání přímo, ale umožňuje omezení přístupu do zabezpečených prostor, kontrolu přístupu osob k němu a určování přístupových práv. Systémy EKV jsou v dnešní době vývojově na slušné úrovni, při projektování je tak důležité najít co efektivnější systém pro daný objekt, aby byla využívána alespoň většina funkcí systému. Cílem práce je navrhnout optimální systém EKV, u něhož bude směrodatným aspektem zvýšení uživatelského komfortu. Jako základ pro tento návrh poslouží informace získané průzkumem trhu, které budou sloužit jako vstupní data pro tvorbu návrhu. V první části této práce se budu zabývat principem funkčnosti a rozborem struktury v současné době používaných systémů EKV. V práci se budu taky mimo jiné věnovat metodám identifikace používaných v této oblasti. Kvalita každého systému EKV se určuje právě podle typu identifikačního mechanismu. Mechanismus ověřování identity uživatele je obecně založen na tom, co zná pouze uživatel (např. heslo), co uživatel vlastní (např. identifikační předmět), nebo na tom, co je pro uživatele charakteristické (např. otisk prstu). Druhá část práce se bude týkat nejprve analýzy průzkumu trhu, s cílem zjištění spokojenosti s používáním systémů EKV. Dalším přínosem, který od průzkumu očekávám je zjištění funkcí, které by vedly k usnadnění používání těchto systémů. Poté na základě výstupů průzkumu provedu samotný návrh systému. Závěrem práce se budu zabývat směrem, kterým by se mohla daná problematika ubírat.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ ROZDĚLENÍ OBJEKTOVÉ OCHRANY

Objektová bezpečnost je složitý proces, kterým se provádí technické a personální zajištění ostrahy objektu tak, aby narušení, napadení nebo zcizení, respektive zničení jakékoliv utajované a citlivé skutečnosti bylo eliminováno na minimum. Při provádění objektové ochrany je třeba znát předmět ochrany, tedy co se má chránit a cíl ochrany, to znamená, před čím budeme chránit.

Základní formy ochrany objektu jsou:

a) Fyzická ochrana,
b) Organizační a režimová opatření,
c) Mechanické a technické prostředky ochrany.

1.1 Fyzická ochrana

Jedná se o nejčastější formu ochrany osob a majetku. Bývá zpravidla prováděna živou silou (nejčastěji tedy vrátní, hlídači, strážní, hlídací služba, policisté). Její největší výhodou je, že lze v případě potřeby provést okamžitý zásah a odvrátit tak případné hrozící nebezpečí chráněnému zájmu. Z finančního hlediska se ovšem jedná o nejdražší způsob ochrany objektů, u mechanických a technických prostředků ochrany jsou sice vyšší pořizovací náklady, ale jejich provoz nebývá finančně náročný. [6]

1.2 Organizační a režimová opatření

Organizační a režimová opatření bývají obvykle popsána v provozním řádu objektu, který zavazuje všechny osoby oprávněné pro vstup do objektu. Vedle jiných náležitostí obsahují i seznamy osob oprávněných vstupovat do chráněných prostorů objektu, seznam dopravních prostředků oprávněných vjíždět do objektu, způsob kontroly prokazování oprávněnosti k vstupu nebo vjezdu do objektu, pokyny, nařízení a příkazy k určitému chování a jednání v chráněných objektech, často vydaných písemně, většinou formou tabulek, nápisů na budovách, či stěnách uvnitř objektu. [6]

1.3 Mechanické a technické prostředky ochrany

Tato forma objektové ochrany se dělí na :

a) Mechanické zábranné systémy
b) Technické prostředky ochrany

1.3.1 Mechanické zábranné systémy

Řadíme zde veškeré mechanické prvky, které zabraňují, nebo ztěžují násilné vniknutí nepovolané osoby do chráněné zóny nebo objektu především přes oplocení nebo cestou dveřních nebo okenních otvorů. Poskytují ochranu svou mechanickou pevností.

- mechanické zábranné systémy obvodové ochrany (klasické a bezpečnostní oplocení, vrcholové zábrany, podhrabové překážky, brány, branky, závory, atd.),
- mechanické zábranné systémy plášťové ochrany (okna, dveře, mříže, rolety, žaluzie, bezpečnostní skla, bezpečnostní dveře, přídavné zámky atd.),
- mechanické zábranné systémy předmětové ochrany (komorové trezory, úschovné objekty, ohnivzdorné skříně, příruční pokladničky atd.). [4]

1.3.2 Technické prostředky ochrany

Jedná se o ochranu prováděnou elektronickými prvky, jejíž použitím se zabraňuje, ztěžuje, nebo oznamuje narušení ochrany objektu nebo zabezpečené oblasti. Mezi technické prostředky ochrany patří zejména:

- poplachové, zabezpečovací a tísňové systémy (PZTS),
- elektrická požární signalizace (EPS),
- uzavřené televizní okruhy (CCTV),
- systémy kontroly vstupu (ACCESS),
- poplachové přijímací centrum (PPC),
- biometrické identifikační systémy,
- elektronická ochrana zboží,
- ochrana dat a informací,
- satelitní vyhledávání vozidel,
- zdravotní a nouzová signalizace.

2 OBECNÝ POPIS SYSTÉMŮ PRO ELEKTRONICKOU KONTROLU VSTUPU

Systémy pro elektronickou kontrolu vstupu (EKV) patří do kategorie technické prostředky ochrany objektu a řídí přístup pověřených osob v zájmových prostorách na základě přístupových práv, přidělených jednotlivým osobám. Jeho hlavním úkolem je nahradit standardní klíčový systém, a zabránit přístupu nepovolaným osobám do míst, kde nemají přístup povolen. Systém může být autonomní, to znamená, že pracuje nezávisle na PC a softwaru. Autonomní systémy jsou ideální pro kontrolu přístupu do archivů, počítačových sálů, trezorů nebo skladů, do nichž mají povolen přístup jen někteří zaměstnanci. Tyto systémy nejsou nákladné, jsou jednoduché a rychle se instaluji. Nebo je systém řízen počítačem. Přístupová oprávnění se definují podle časových, prostorových a personálních dispozic ve vztahu ke konkrétním osobám, které jsou vybaveny identifikačním médiem, pomocí kterého oprávněná osoba ovládá koncové akční prvky, např. elektromechanické zámky, elektromotorické zámky, turnikety, apod., které umožňují vstup do chráněného prostoru. Díky ovládání systému počítačem je možné měnit přístupová data v reálném čase, sledovat pohyb osob v zabezpečeném prostoru, ukládat informace o pohybu osob v objektu, a používat další aplikace. Pokud dojde ke ztrátě nebo odcizení identifikačního média, lze řídící panel jednoduše a rychle přeprogramovat. Systém může dále ukládat a poskytovat informace o používání identifikačních médií i kódů, nabídnout obsluze přehledy událostí v systému nebo generovat zprávy z databází. Systém EKV umožňuje uchovávat a spravovat informace o tisícovkách zaměstnanců a osob, a poskytovat informace o jejich docházce. Velkou výhodou je nahrazení mnoha klíčů jednou kartou nebo čipem, čím se zvyšuje uživatelský komfort. [1,6]

Obecně můžeme princip systémů EKV vysvětlit jako – **KDO** se dostane **KAM** a **KDY**.

Systémy EKV se instalují podle stupně důležitosti. Bezpečnostní oblasti strategických podniků, bank, trezorových místností, výpočetních center, apod., mají přístupové systémy důmyslnější, a mnohdy s vícenásobnou kontrolou a jištěním. U méně náročných aplikací jako je například střežení panelového domu, rodinného domu, provozoven apod., se instaluje systém méně náročný, ale přesto bezpečný pro daný druh ochrany. [1]

2.1 Hlavní funkce systému

V této podkapitole uvedu funkce, které by měl kvalitní přístupový systém ovládat. Samozřejmě ne všechny systémy obsahují všechny vyjmenované a popsané funkce, obvykle si zákazník vybírá systém tak aby splňoval jeho požadavky, tedy podle funkcí, které bude skutečně využívat. Uživatelem mám, namysli osobu žádající průchod místem přístupu.

- Řízení vstupů

  Jedná se o základní činnost, která zpracovává žádosti o povolení vstupu respektive průchodu. Uživatel zažádá buď to přiložením identifikačního média, nebo zadáním pinu o povolení průchodu příslušným prvkem (nejčastěji tedy dveřmi, turniketem, apod.). Podle přidělených oprávnění je pak reakcí buď odblokování dané zábrany, nebo odepření vstupu a případné vyhlášení příslušného poplachu. Aby případný výpadek řídících jednotek neznamenal kolaps celého systému, měl by být tento systém konstruován jako distribuovaný, to znamená, že by měl být schopen po určitou dobu fungovat bez součinnosti databázových a řídících jednotek. Zpravidla bývá toto zajišťováno nahráváním definic oprávnění přímo do řídících jednotek, které jsou pak po určitou omezenou dobu schopny fungovat autonomně.

- Definice časových oken a přístupových zón

  Další funkcí systému je volba časových úseků. V ovládacím software přístupového systému se dá nastavit, v jakém čase může do objektu či určité zóny daná osoba či skupina osob vstoupit. Nedílnou součástí je pak možnost definice přístupů do jednotlivých zón objektů, např. sklad, kancelář, vývojové centrum, atd. To znamená například: Zaměstnanec Pavel Dvořák má povolen přístup do kanceláře neomezeně pondělí – pátek, ale do skladu má nastavena omezení pondělí - středa v časech 6:00 – 11:30, 12:00 – 14:00. Ve čtvrtek a pátek pouze 6:00 – 11:30, v jiný čas se do skladu nedostane.

- Monitoring událostí a stavů systému

  Tato funkce zajišťuje obsluze možnost permanentního dohledu nad děním v objektech. Hlavní výhodou je možnost rychle reagovat na nestandardní a mimořádné situace. Ty musí být signalizovány poplachy, ať už opticky či

akusticky, s okamžitým zobrazením místa výskytu takové situace na monitorech v řídící místnosti. Ovládací software, zároveň musí přehlednou formou zobrazovat aktivity v jednotlivých kontrolovaných přístupových bodech (kdo, kde a kdy prošel). Dále pak je možno do systému nahrát k osobním údajům také fotografie, které by dále mohli sloužit také k vizuální kontrole uživatelů.

- Vzdálené ovládání

  Koncové ovládací prvky (čtečky, vstupy, výstupy) připojené do systému EKV mají svoji reprezentaci v řídících jednotkách. Ty musí umožnit pracovníkům monitorovacího střediska vzdáleně ovládat všechny tyto prvky a vysílat jim řídící povely. V kombinaci s monitoringem systému musí být možné z jediného místa realizovat velmi rychlý zásah v případě výskytu nestandardních nebo mimořádných událostí, to znamená například umožnit průchod dveřmi bez použití karty, zablokovat přístupové body, aktivovat nebo deaktivovat zařízení.

- Antipassback

  Jde o funkci, která brání opakovaným vstupům na jednu kartu. K tomu aby tato funkce mohla fungovat musí být nastavena část čteček pro vstup do objektu (vstupních), a část čteček pro opuštění objektu (výstupních). Zjednodušeně řečeno antipassback sleduje, zda při načtení karty na některé vstupní čtečce, bylo předcházející čtení provedeno na čtečce výstupní. Jinými slovy řečeno zda osoba před dalším vstupem objekt nejprve opustila. Pokud tato podmínka není splněna systém vyhodnotí identifikaci jako neplatnou a neumožní tak vstup do objektu. Tak může zabránit situaci, kdy si více osob před vstupem předává kartu pro získání přístupu. Funkce dále sleduje čas uběhlý od poslední čtení této karty. Pokud je kratší než přednastavený interval, vstup opět není umožněn. Jsou případy kdy se antipassback vůbec nevyužívá a naopak případy kde se bez něj nejde obejít.

  • Globální antipassback:

    Rozhodování zde provádí řídící počítač s datovým serverem. Ten shromažďuje data o průchodech čtečkami, na kterých je antipassback aktivován a rozhoduje, zda dotyčné kartě vstup umožní. V tomto případě se vyžaduje trvalé připojení a činnost komunikačního i datového serveru. [6]

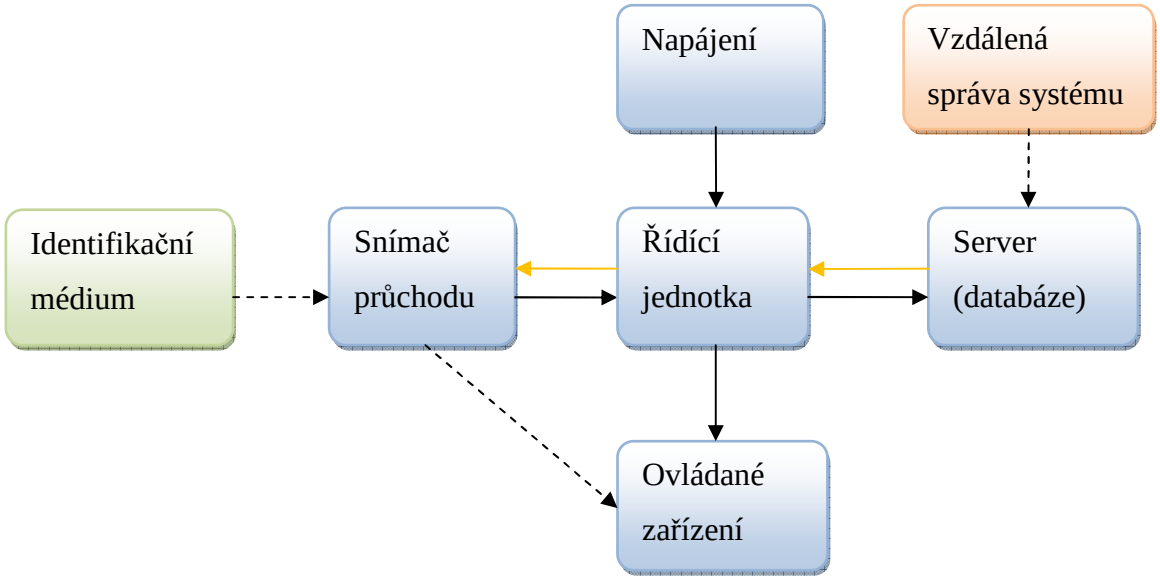
• Lokální antipassback:

Funguje pouze v rámci jedné řídící jednotky, kontroluje pouze více vstupů, na níž se aktivuje zapnutím příslušného systémového příznaku. Na výstupní čtečce může být platná karta čtena i vícekrát po sobě, a vždy dojde k sepnutí příslušného relé. Protože se ale pořadí vstup-odchod kontroluje pouze uvnitř jedné jednotky, nelze zabránit druhému vstupu do objektu na jiné jednotce. [6]

- Optická i akustická signalizace autentizace,
- Signalizace nezavřených dveří po průchodu,
- Signalizace násilného pokusu o otevření,
- Vyhodnocování stavu a doby otevření dveří,
- Signalizace poruch,
- Kontrola osoby v závěsu, tj. zda prošla opravdu jen jedna osoba,
- Evidence návštěv,
- Uvolnění přístupových cest v případě požáru,
- Záloha a obnovení systému,
- Možnost exportu a tisku dat.

2.2 Struktura systémů EKV

Celý systém pro elektronickou kontrolu vstupu se teoreticky skládá ze dvou částí a to sice z části hardwarové, do které spadá řídící jednotka, snímač průchodů (obvykle čtečka nebo klávesnice), ovládané zařízení, tedy přístupová místa jako dveře, turnikety, elektrické zámky apod., přenosová zařízení a server, nejčastěji tedy počítač obsahující databázi uživatelů a software pro ovládání systému. Druhou částí je část softwarová, která slouží pro správu systému. Správa systému může být prováděna i přes klasický internetový prohlížeč po přihlášení do systému, tím pádem prakticky odkudkoliv, což představuje obrovskou výhodu a uživatelský komfort. Nejjednodušší funkční topologie systému elektronické kontroly vstupu je znázorněna na následujícím obrázku.



Obrázek 1: Topologie EKV

- **Identifikační médium**

Jedná se z hlediska vstupu do objektu zabezpečeného systémem kontroly vstupu o nejdůležitější prvek, bez kterého se do objektu nedostaneme. Identifikační médium je čip, karta nebo přívěšek, který má přiřazen každý uživatel systému. Každé médium obsahuje kódovanou informaci, která při načtení do systému identifikuje svého majitele. Pro komfortnější aplikace jsou využívány bezkontaktní identifikační technologie, kdy systém pracuje s různými typy bezkontaktních karet. Jako ověření identity může sloužit taky PIN. Dalším typem je biometrická identifikace, která se stále více rozšiřuje, díky její nezaměnitelnosti. Prostředky identifikace osob rozeberu podrobněji v dalších kapitolách.

- **Snímač průchodu**

Patří zde především bezkontaktní a kontaktní čtečky, ale taky klávesnice. Čtečky opatřené klávesnicí mají své místo především v aplikacích pro vyšší stupeň zabezpečení, kdy je autentizace čipem nebo kartou doplněna ještě zadáním PIN kódu. V jednoduchých aplikacích bez větších nároků na bezpečnost lze nasadit také moduly pracující pouze s číselným kódem. Obecně čtečka pro bezkontaktní a kontaktní identifikaci je zařízení, které přijímá informace od identifikačního média a má za úkol tuto informaci bezpečně přečíst a dekódovat. Čtečky karet se liší mezi sebou množstvím faktorů od základních technických parametrů, jako jsou velikost, tvar, napájení, pracovní teplota, čtecí vzdálenost, apod. Dále je to schopnost odolávat externím vlivům, ať už vlivem počasí v prostředí ve kterém se

bude používat, nebo míře rizika, při nichž by hrozilo poškození vandalismem, případně sabotáží čtečky.

- **Řídící jednotka**

Řídicí jednotky jsou zařízení, která na základě informací ze snímače (nejčastěji čteček karet) rozhodují o poskytnutí nebo odmítnutí přístupu do zabezpečeného prostoru. Je to mikroprocesorem řízená jednotka obsahující komunikační rozhraní pro připojení k PC. Dále je uvnitř obsažena paměť pro uložení přístupových práv a jednotlivých naprogramovaných funkcí v autonomním režimu. Ta bývá zálohovaná vnitřní baterií, takže ani při výpadku napájení nejsou žádná data ztracena. Řídící jednotka musí být umístěna v instalačním krytu s kontaktem samoochrany (tamper).

- **Napájení**

Napájení bývá zálohováno akumulátorem, který slouží k pokrytí výpadků síťového napájení. Zdroje se používají převážně spínané, které se vyznačují nezanedbatelnou úsporou spotřebované energie. Baterie je 12ti voltová a kapacita se volí podle odběru dané aplikace. V případě větších odběrů lze též použít baterie dvě. Výpadek napájení řídící jednotky musí být systémově monitorován a signalizován jako porucha.

- **Ovládané zařízení**

Jedná se o koncové prvky vstupního systému, jsou to zařízení otevírající, případně uzavírající přístup do objektů. Patří zde různé elektrické zámky pro odblokování vstupu, turnikety, závory, brány atd.

- **Server**

Je to zařízení pro správu, monitorování a evidenci přístupových systémů.

- **Komunikační rozhraní**

Komunikace mezi jednotlivými prvky systému EKV mohou probíhat pomocí několika rozhraní, proto se používají různé převodníky. Mezi používaná rozhraní patří:

RS232 – jedná se o jedno z nejstarších počítačových rozhraní. Jeho hlavní nevýhodou je krátká maximální délka vodičů (podle normy maximálně 15 metrů). Nízká odolnost proti rušení a nebezpečí vzniku zemních smyček (propojením dvou zařízení napájených z různých potenciálů může dojít k poškození nebo zničení zařízení).

RS485 – odolná komunikační sběrnice, má vysokou odolnost proti rušení. Maximální délka jedné větve RS485 je až 1200 metrů. Lze ji prodloužit pomocí opakovačů.

Wiegand – je standardní rozhraní, kterým komunikují čtečky bezkontaktních karet. Přesněji - komunikace je jednosměrná. Čtečka po sejmutí kódu vyšle v protokolu Wiegand kód a některé další údaje. Označení Wiegand je vždy doplněno ještě číslicí, která označuje typ protokolu. Mezi nejčastější patří protokoly Wiegand 26, 30, 32, 40 a 42.

USB – jde o univerzální sběrnici používanou na nejrůznějších elektronických zařízeních. V současné době jsou k dispozici tři různé verze rozhraní: 1.1, 2.0 a 3.0.

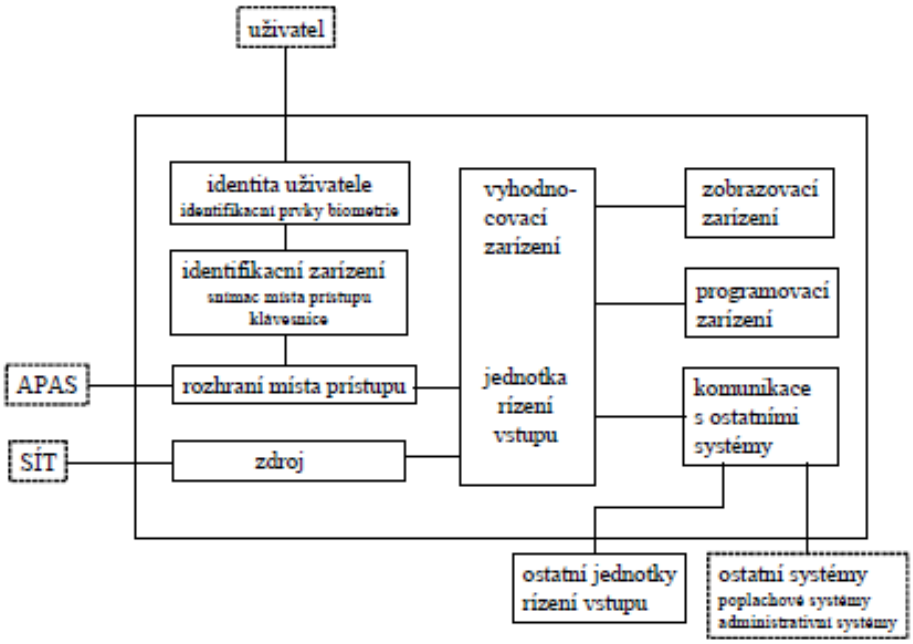
Ethernet – technologie používaná pro počítačové sítě LAN. Komunikace zde probíhá pomocí protokolu TCP/IP, jedná se o nejrozšířenější rodinu protokolů. Stále více nahrazuje ostatní komunikační rozhraní, zejména pro použití na delší vzdálenosti (v řádu kilometrů). Dovoluje použití prakticky neomezeného počtu systémových prvků. Velkou výhodou systémů postavených na IP technologiích je možnost využít systém napájení PoE (Power over Ethernet – napájení přes ethernet). Po jediném kabelu, navíc jednoduše a levně dostupném totiž lze přenášet jak komunikační data tak i napájení koncových prvků.

2.3 Systémové požadavky

Tyto požadavky řeší norma ČSN EN 50 133-1, celým názvem *Všeobecné požadavky na systémy kontroly vstupů pro použit v bezpečnostních aplikacích*. Pokud je některá část systému kontroly vstupu součástí zabezpečovacího poplachového systému, musí tato část splňovat současně i příslušné požadavky norem na zabezpečovací systémy. Norma ČSN EN 50 133 se skládá z 6 částí:

- Část 1. Systémové požadavky
- Část 2. Identifikační zařízení
- Část 3. Vyhodnocovací zařízení - Zobrazovací a programovací zařízení
- Část 4. Výstupní ovládací prvek přístupového místa
- Část 5. Komunikace
- Část 7. Pokyny pro aplikace

Na následujícím obrázku je zobrazeno funkční schéma systému kontroly vstupu převzaté z normy:



Obrázek 2: Blokové schéma systému EKV podle ČSN 50133-1

Podle ČSN EN 50133-1 jsou definovány následující pojmy:

Tabulka 1: Pojmy dle ČSN 50133-1 [7]

Systém kontroly vstupu	Systém obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro řízení vstupů.
Přístup	Akce vstupu dovnitř nebo výstupu ven ze zabezpečeného prostoru.
Jednotka řízení vstupů	Zařízení, které rozhoduje o uvolnění jednoho, nebo několika přístupových míst a řídí sled souvisejících ovládání
Filtr přístupu	Jeden, nebo několik zabezpečených prostorů přiřazených k přístupové úrovni.
Úroveň přístupu	Oprávnění uživatele z pohledu přístupu do stanoveného přístupového filtru a souvisejícího časového filtru
Místo přístupu	Místo, ve kterém může být přístup ovládán pomocí dveří, turniketem nebo jinou zabezpečovací závorou
Rozhraní místa přístupu	Zařízení, které ovládá uvolnění a zabezpečení místa přístupu poté, co byl přístup poskytnut
Snímač místa přístupu	Zařízení používané k získávání rozpoznávacích údajů z identifikačního zařízení nebo biometrie
Výstraha	Požadavek na lidský zásah po aktivaci indikátoru

Hlášení	Podávání informací pro správu systému nebo pro ostatní systémy
Apas	Ovládací prvky a senzory místa přístupu (elektronické zámky, turnikety a závory, příkladem senzorů jsou kontakty a spínače)
Událost	Změna objevující se uvnitř systému kontroly vstupů
Chybné povolení	Poskytnutí přístupu neoprávněnému uživateli
Chybné odmítnutí	Odepření přístupu oprávněnému uživateli
Časový filtr	Jedna, nebo více časových zón přiřazených k přístupové úrovni
Časová zóna	Jeden, či více časových intervalů kombinovaných s kalendářními informacemi
Časový interval	Časový interval mezi dvěma danými okamžiky indikujícími začátek a konec platné periody v rámci časové zóny
Identita uživatele	Informace, které jsou přenášeny přímo uživatelem do rozpoznávacího zařízení pomocí identifikačního prvku uživatele

2.3.1 Klasifikace identifikace

Podle ČSN EN 50 133-1 se rozdělují třídy identifikace:

- Třída identifikace 0 - žádná přímá identifikace,
- Třída identifikace 1 - informace uložené v paměti,
- Třída identifikace 2 - identifikační prvek nebo biometrie.
- Třída identifikace 3 - identifikační prvek nebo biometrie spolu s informací uloženou v paměti.

Třída identifikace 0 je založena na prostém požadavku o přístup bez identity uživatele, například stisknutí tlačítka pří odchodu ze zabezpečeného prostoru. Používá se jako doplněk k některé z dalších tříd identifikace 1 - 3. Tento typ lze použít pouze na vstupu do zabezpečené oblasti kategorie Důvěrné nebo Vyhrazené. Třída 1 využívá k identifikaci uživatele hesla, osobní identifikační čísla aj. Třída 2 je založena na používání identifikačních prvků, karet, přívěsků, fyzických klíčů, nebo biometrických charakteristik jako je otisk prstu, geometrie obličeje, aj. Nejvyšší třídou je identifikace založena na používání kombinace identifikačního prvku, nebo biometrie, a informace uložené v paměti. Při kontrole vstupu do objektu nebo zabezpečené oblasti kategorie Přísně tajné, se používají zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů.

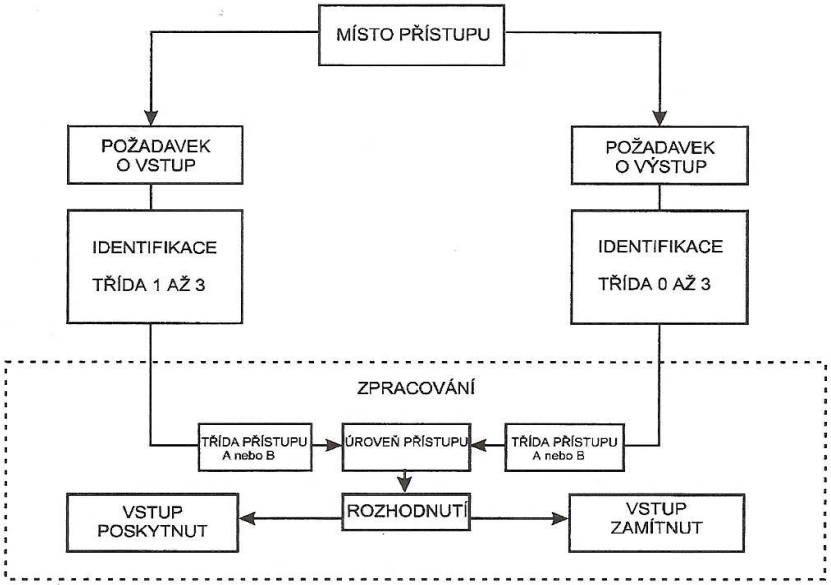
2.3.2 Klasifikace přístupů

- Třída přístupu A

platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr, ani ukládání přístupové transakce.

- Třída přístupu B

platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřídu, která se vztahuje na místo přístupu zahrnující časové filtry ale bez funkcí ukládání dat.(uvolnění přístupového místa poté, co byl rozpoznána identita uživatele)



Obrázek 3: Klasifikace přístupů

2.3.3 Třídy prostředí

- Třída I: Prostředí vnitřní

Vlivů prostředí, které se vyskytuje ve vytápěných místnostech.Předpokládají se změny teplot v rozmezí + 5 °C až + 40°C při střední relativní vlhkosti okolo 75 % bez kondenzace

- Třída II: Prostředí vnitřní všeobecné

Působení vlivů prostředí, které se vyskytuje všeobecně v objektech, kde není udržována stálá teplota. Předpokládají se změny teplot v rozmezí – 10 °C až + 40 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.

- Třída III: Prostředí venkovní chráněné

Vlivy prostředí, které se vyskytují všeobecně vně budov s tím, že komponenty EZS nejsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí – 25 °C až + 50 °C při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.

- Třída IV: Prostředí venkovní všeobecné

Prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty jsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí – 25 °C až + 60 °C při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.

2.4 Společné funkční požadavky

2.4.1 Napájení

Při připojení nebo odpojení napájení nesmí v žádném případě dojít k chybnému uvolnění vstupu. Nepožaduje se však, aby systém kontroly vstupu napájel apas. Vstupy a výstupy napájení každého komponentu systému kontroly vstupů musí být chráněny proti zkratu.

2.4.2 Vnitřní zabezpečení

Neoprávněná osoba nesmí mít možnost bez použití nástrojů si zajistit přístup, to platí pro třídy identifikace 1 až 3.

2.4.3 Ochrana programování

Musí být k dispozici zabezpečovací prostředky k zabránění neoprávněné změny předvolených postupů. Poměr počtu různých kombinací kódu k počtu oprávněných osob musí být nejméně 1000:1, minimální počet kombinací musí být 10 000, správce systému musí mít možnost změnit tento přístupový kód.

2.4.4 Ovládání míst přístupu

Systém kontroly vstupů musí být vybaven rozhraním pro spojení s apas. Toto rozhraní musí zahrnovat jeho ovládání a monitorování stavu zabezpečení. Skříňka, ve které je umístěna svorkovnice rozhraní místa přístupu musí být opatřena tamper kontaktem, aby

při otevření byla detekována sabotáž. Systém musí dále monitorovat stav apas, zda je nebo není uzavřen. Ovládací výstup rozhraní místa přístupu musí být sepnut, pokud je přístup povolen, a musí být zrušen, pokud uběhl předvolený časový úsek uvolnění apas a nebo monitoring signalizuje, že je apas otevřen.

2.4.5 Identifikace

Úroveň zabezpečení je ovlivněna řadou faktorů, z nichž nejdůležitější jsou počet kombinací a snadnost zhotovení duplikátu.

- Pro třídu identifikace 1 platí:

Poměr počtu různých kombinací kódů k počtu identifikovatelných uživatelů musí být nejméně 1000:1, a zároveň minimální počet kombinací v systému musí být 10 000

- Pro třídu identifikace 2 a vyšší platí:

Každému uživateli musí být v jednom systému přiřazena jednoznačná identita. Struktura kódování musí poskytovat nejméně milion kombinací a každá informace identifikace předaná do systému musí být s touto strukturou porovnána. Četnost chybných povolení nesmí být větší než 0,01 %. Míra chybných odmítnutí musí být menší než 1 %. Nesmí být použit identifikační prvek, u něž je předpoklad že by mohl být zhotoven jeho duplikát.

- Pro třídu identifikace 3 platí:

Informace uložené v paměti používané současně s identifikačním prvkem nebo biometrií musí mít minimálně 10 000 kombinací.

2.4.6 Požadavky na komponenty

- Otevření krytů

Otevření nebo oddálení komponentů z jejich montážní polohy nesmí být možné bez použití nástrojů (například šroubováku, klíčů).

- Nastavení

Nastavovací body (spínače, potenciometry) musejí být umístěny uvnitř krytu komponentu.

- Rozhraní místa přístupu

Musí být umístěno vnitř krytu, který je vybaven detekcí sabotáže, která je aktivována při otevření krytu normálními prostředky. Rozhraní místa přístupu musí být umístěno uvnitř

krytu, který je opatřen prostředky pro ukrytí kabelových průchodů nebo prostředky umožňujícími monitorování propojení.

- Kryty rozhraní místa přístupu

Musejí splňovat alespoň IP 3x podle EN 60529. V závislosti na třídě prostředí zařízení jsou požadavky následující:

- třída prostředí I, II…IP 30
- třída prostředí III…IP 32
- třída prostředí IV…IP 34

Pzn. IP = ochrana před dotykem živých částí, před vniknutím pevných cizích těles a vniknutím vody. Stupeň zabezpečení (IP) je normalizován dle ČSN EN 60529/DIN 40050. Za písmeny IP je dvojčíslí, případně přídavné a doplňkové písmeno např. IP 12 XX kde:

- První číslice popisuje stupeň ochrany osob před nebezpečným dotykem a stupeň ochrany zařízení před vniknutím cizích předmětů.
- Druhá číslice popisuje stupeň ochrany před vniknutím vody.
- Přídavné písmeno (nepovinné), může nabývat hodnot A, B, C nebo D.
- Doplňkové písmeno (nepovinné), se používá k doplňkovým informacím, používaná písmena jsou H, K, M, S, W.

- Identifikační zařízení

Pokud je možné poskytnutí přístupu jednoduchou manipulací (např. testovacím prvkem, servisním nástrojem, zkratem), musí být kryt identifikačního zařízení vybaven detekcí sabotáže, která je aktivována při otevření krytu normálními prostředky. Identifikační zařízení musí být opatřeno prostředky pro ukrytí kabelových průchodů nebo prostředky umožňujícími monitorování propojení. S výjimkou běžného otevírání s použitím identifikačního prvku nebo biometrického čtení musí kryt identifikačního zařízení splňovat alespoň IP 3X.

V závislosti na třídě prostředí zařízení jsou požadavky následující:

- třída prostředí I, II…IP 30, IK 04
- třída prostředí III…IP 32, IK 04
- třída prostředí IV…IP 34, IK 06

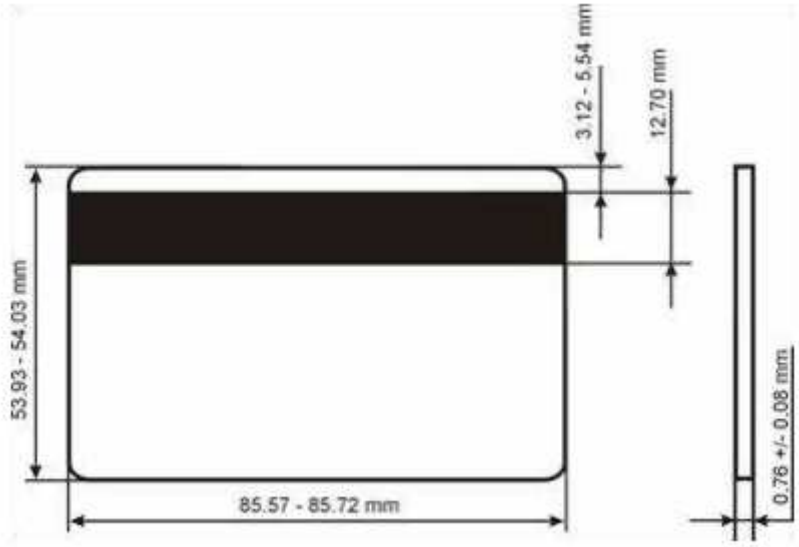
(IK = odolnost proti nárazům)

3 PROSTŘEDKY IDENTIFIKACE OSOB

3.1 Magnetický systém

Jako identifikační médium se zde používají karty velikosti standardních kreditních karet, jiné provedení zde prakticky není možné, protože při čtení dat musí být karta protažena čtecí hlavou. Karta je vybavena magnetických proužkem obsahující údaje o kartě a uživateli. Karty s magnetickým pruhem umožňují kontaktní přístup k informacím uložených na magnetické pásce, která zároveň slouží jako paměťová karta. Při průtahu karty čtečkou nejdříve dojde ke zmagnetizování, vytvoří se množství malých permanentních magnetů, a poté stav těchto magnetů tvoří jednoduché binární rozhodování:

- Zmagnetizování – logická 1
- Nezmagnetizování – logická 0



Obrázek 4: Magnetická karta

- Karty s magnetickým pruhem HiCo (High Coercivity)

Jedná se o typ, který umožňuje vysokou hustotu záznamu. Magnetické karty s pruhem HiCo jsou karty, které se používají jako věrnostní, slevové, protože se na tyto karty dá nahrát určitá informace, dále pak mohou sloužit jako identifikační médium pro systémy elektronické kontroly vstupu. Největší výhodou u těchto karet je především jejich nízká pořizovací cena a snadná identifikace. Ovšem jsou zde i záporné stránky těchto karet, a to je jejich snadná zničitelnost, možnost poškození magnetického pruhu, stačí, aby se karta nechala v blízkosti magnetu a tím by došlo k jejímu znehodnocení.

- Karty s magnetickým pruhem LoCo (Low Coercivity)

Mají nízkou hustota záznamu. Platí to samé co u karet s magnetickým pruhem HiCo. Kódováním magnetického pruhu můžeme na kartu nahrát informace, které se týkají uživatele karty. Kartu je možno nahrát podle přání uživatele.

Podle normy ISO 7811, existují 3 stopy magnetického záznamu:

1 stopa (IATA) - má 79 znaků, dají se na ní nahrát jen alfanumerické znaky.

2 stopa (ABA) - má 40 znaků, dají se na ní nahrát jen číslice 0-9 a rovnítko.

3 stopa (THRIFT) - má 107 znaků, využívá se k bankovním účelům pro uchování PIN, dají se nahrát jen číslice 0-9, rovnítko, dvojtečka.

Obrázek 5: Rozložení stop magnetické karty

Výhodou magnetických karet je, že data jsou dynamická, to znamená, že uložený záznam lze později kdykoli přepsat nebo aktualizovat. Životnost uložených dat a karty je vysoká, udává se 5 až 6 let. Další velkou výhodou použití magnetických karet je jejich ekonomická nenáročnost.

Mezi nevýhody patří možnost poškození dat při vystavení silnému magnetickému poli, nebo při poškrábání magnetické vrstvy, což se může stát velice snadno, poté se karta stane nečitelnou a je nutné ji vyměnit. Velkou nevýhodou magnetických karet je jejich bezpečnost. Bez velkých problém lze kartu přečíst a vyrobit duplikát.

Čtečky magnetických karet se rozlišují podle toho, ze které stopy je informace sejmuta, a to pro první, druhou, nebo třetí stopu. Podle toho, kolik stop pak současně je čtečka karet schopna současně dekódovat se dělí čtečky na jednostopé, dvoustopé a třístopé.

3.2 Optický systém

Jako identifikační prvek je zde použit běžný čárový kód, se kterým se setkal snad každý. Cena karty s čárovým kódem je prakticky zanedbatelná. Zato pro okopírování karty s čárovým kódem stačí obyčejná kopírka – zde tedy nelze hovořit o jakémkoliv zabezpečení. Mechanické opotřebení karty je velmi malé, cena snímače, jeho umístění a použití je v podstatě stejné jako u magnetického systému. Princip identifikace spočívá v tom, že v kódu je uložena číselná hodnota, podle které je pak nalezena v databázi. Čtení kódů probíhá nejčastěji pomocí laserového paprsku. Šířka v podélném směru představuje pro čtečku logickou informaci. Snímač vysílá světelný paprsek a sleduje, zda je odražen na bílém pozadí nebo pohlcen černým proužkem. První a poslední proužky slouží k synchronizaci. Pro snadné zkopírování nelze použít v bezpečnostních systémech, ale např. v knihovnách, supermarketech atd. Nejpoužívanějšími typy čárového kódu jsou EAN 8, EAN 13, CODE 39, CODE 128, CODABAR, atd. Čárový kód může být zamaskován speciální barvou. Čárový kód je pak čitelný pouze infračerveným paprskem.[6]

Obrázek 6: Příklad čárového kódu

V závislosti na principu snímání čárového kódu rozlišujeme snímače na laserové a digitální. Klasické laserové snímače pracují na výše popsaném principu. V posledních letech se ovšem začali používat snímače digitální. Ty fungují na podobném principu jako digitální fotoaparáty. Nejdříve dojde k vyfocení čárového kódu. Následně se jeho obsah dekóduje pomocí dekodéru, který je součástí snímače. Velkou výhodu u digitálních snímačů je, že umožňuje vícesměrné čtení jak 1D, tak i 2D symbolů.

3.3 Kontaktní systém

Jedná se o variantu kde je při provádění autentizace potřeba kontaktu identifikačního média a čtečky. Média mívají nejčastěji podobu kovového pouzdra nebo kreditní karty, které jsou opatřeny kontaktním polem. Při kontaktu dojde k zapojení čipu do obvodu, a poté může probíhat obousměrná komunikace. Jako identifikační médium se používá kontaktní čipová karta, nebo kontaktní čip.

3.3.1 Čipové karty

Čipové karty (nebo taky smart card) se používají jako kontaktní médium od jednoduché paměťové karty pro autentizaci nebo předplacené telefonní karty až po multiaplikační kartu s mikroprocesorem a kryptoprocesorem pro náročné aplikace. Jde o velice bezpečné a spolehlivé médium pro uchování a přístup k informacím uloženým na čipu karty. Na karty, které jsou osazovány kontaktními čipy je možno uložit velké množství dat, na těchto čipech může probíhat více aplikací najednou. U systémů kontroly vstupu jsou méně používané, ovšem často se využívají v informačních technologiích (přihlašování k počítačové síti, k PC apod.). V dnešní době se zásadně využívají standardní karty splňující požadavky ISO 7816-1. Standart ISO/IEC 7810 definuje velikost karty na 85,60x53,98 mm a šířka 0,76 mm. Vyrábí se ve dvou provedeních, respektive rozměrech. Tím větším jsou běžné platební karty a malý rozměr mají SIM karty mobilních telefonů. Je možné vytvořit tzv. hybridní kartu, která umožňuje různě kombinovat datová média na kartě a tak využívat výhody každého z nich. Je možno vyrobit kartu např. s kontaktním a bezkontaktním čipem, kartu s kontaktním čipem a magnetickým proužkem atd.

Na světovém trhu existuje celá řada výrobců kontaktních čipů, které lze implementovat do plastové karty. Tyto čipy jsou vyráběny s různými parametry podle druhu a náročnosti aplikace.

Aplikace karet:

- Paměťové karty

identifikační karty, předplacené telefonní karty, elektronická peněženka, přístupové systémy, karty zdravotních pojišťoven, elektronické jízdné, členské a klubové karty

- Mikroprocesorové karty

bankovní karty, elektronické peněženky, GSM karty, zdravotnictví, předplacené TV a satelit, multifunkční karty

Výhody použití čipové karty - karty s kontaktním čipem

- velká rozšířenost systému a podpora řady výrobců
- vysoká bezpečnost
- možnost uložení značného množství dat
- možnost běhu více aplikací na jednom čipu

Nevýhody použití čipové karty - karty s kontaktním čipem

- kontaktní řešení
- možnost mechanického poškození čipu

Obrázek 7: Čtečka čipových karet

3.3.2 Kontaktní čip Dallas

Identifikační čipy Dallas jsou výrobkem firmy Dallas Semiconductor. Jedná se v podstatě o polovodičové paměti uzavřené do kovového pouzdra o průměru 16mm. Tyto paměti obsahují jedinečný 48-bitový kód, který umožňuje jednoznačnou identifikaci předmětu či osoby. Mimo základní provedení čipu s označením DS1990A jsou k dispozici i další typy, které mají navíc paměť typu EEPROM, do které lze nahrát libovolné údaje, a tyto údaje jsou pak při každé identifikaci přenášeny do čtecího zařízení. Čipy Dallas neobsahují žádný zdroj energie a informace, které jsou v nich obsažené jsou přenášeny do čtecího zařízení v okamžiku přímého kontaktu se čtecí plochou. Přenos dat probíhá po jednom vodiči a je velmi rychlý (20ms).

Výhodou čipů Dallas je jejich jednoduchost a příznivá cena. Mají malou velikost, a jsou praktické při použití na klíčích. Další velkou výhodou je nemožnost vytvoření falešného duplikátu, výrobce zaručuje, že nevytvoří nikdy čip se stejným kódem.

Oproti bezkontaktním čipům jsou více náchylné na znečištění, protože při čtení musí být zajištěn jejich kvalitní kontakt se čtecí plochou. U čteček může nastat tzv. „zatuhnutí" systému následkem výboje statické elektřiny mezi čipem a terminálem.

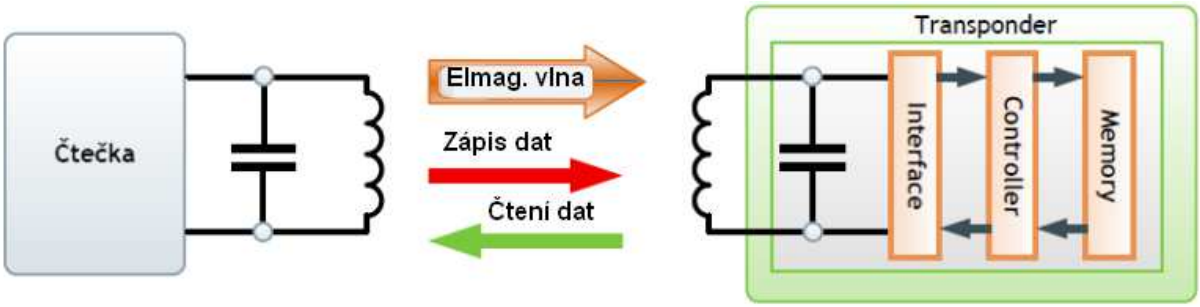
Obrázek 8: Čtečka a čip Dallas [18]

3.4 Bezkontaktní systém

Jedná se o v dnešní době nejpoužívanější metodu autentizace osob před vstupem do objektu, která je založena na radiovém přenosu dat mezi identifikačním médiem a čtečkou. Technologie, kterou se radiofrekvenční komunikace provádí se nazývá RFID (Radio Frequency Identification). Informace jsou ukládány v elektronické podobě do malých čipů neboli tagů či transpondérů, ze kterých následně může probíhat čtení pomocí radiových vln. Jde tedy o bezkontaktní paměťové prvky, které se vyznačují tím, že nepotřebují při identifikaci pevný kontakt se čtečkou, komunikace probíhá pouhým přiblížením. Standardní vzdálenost, která je potřebná k tomu aby došlo k přečtení informace z média je 5 – 10cm, lze dosáhnout i větší vzdálenosti. Čtečky jsou standardně napájeny 12 V, pro čtení na větší vzdálenost mohou vyžadovat i 24 V. V podstatě celý systém pracuje jako dvouanténní, jedna anténa je umístěna v transpondéru a druhá je připojena ke snímači. Transpondéry mohou být v různém provedení - většinou podle charakteru aplikace (např. karty velikosti kreditních karet, přívěsky, plastové disky, atd...).

Čtečka neustále vysílá na svém nosném kmitočtu elektromagnetickou vlnu, která je přijata anténou transpondéru za dodržení podmínky, že obě antény, čtečky i transpondéru, jsou naladěny na stejnou frekvenci. Indukované napětí vyvolá elektrický proud, který je

usměrněn a nabíjí kondenzátor v transpondéru, tato akce trvá cca 50 milisekund. Uložená energie je použita pro napájení logických a rádiových obvodů transpondéru. Když napětí na kondenzátoru dosáhne minimální potřebné úrovně, transpondér začne odesílat odpověď čtečce. Čtečka signál upraví na plně digitální elektrický signál a předá do systému k dalšímu zpracování, kde se rozhodne v našem případě o vpuštění osoby do objektu. Doba identifikace obvykle netrvá déle než 100 – 120 milisekund.[6]



Obrázek 9: Princip bezkontaktní autentizace

Jak jsem naznačil, transpondéry mohou být vyrobeny v několika provedeních lišících se jak tvarem, tak i funkcí. Co se týče funkce, existují typy určené pouze pro čtení uloženého kódu (R/O transpondéry), stejně jako typy s možností naprogramování kódu vlastního o délce 64 bitů do interní EEPROM (R/W transpondéry).

- R/O transpondéry jsou užívány jako jedinečné a nekopírovatelné. Obsahují unikátní kód, neexistují tedy dva stejné transpondéry. Tyto prvky jsou široce použitelné ve všech aplikacích zabývajících se velkými databázemi s nezáměnnými položkami.
- R/W transpondéry jsou určeny mimo jiné pro ukládání dat. Mohou být programovány, čteny a měněny prakticky neomezeně. Programování se provádí rovněž bezkontaktně. Uživatel si tak může sám tvořit kódy ke snadné integraci s jeho počítačovým systémem zpracování dat.

Problematiku RFID se zabývá řada standardů. Základní rozdělení, podle frekvenčního rozsahu požívaného při komunikaci je znázorněno v následující tabulce.

Tabulka 2: Standardy rfid komunikace

Pásmo	Rozsah	Použití	Standardy
LF	< 135 kHz	identifikace zvířat, přístupové systémy, kličky do zapalování	ISO/IEC 18000-2
HF	13,553-13,567 MHz	čipové karty, přístupové systémy, platební karty, občanské průkazy, pasy, jízdenky	ISO/IEC 18000-3, ISO/IEC 14443, ISO/IEC 15963, ISO/IEC 18092, ISO/IEC 21481
UHF	433 MHz	aktivní transpondéry pro nákladní dopravu a vojenskou logistiku v USA a zemích NATO	ISO/IEC 18000-7
	840-960 MHz	sledování zboží po jednotlivých kusech, ochrana proti krádežím, zavazadla v letectví, doprava	ISO/IEC 18000-6, ISO/IEC 29143
	2,45 GHz	správa položek	ISO/IEC 18000-4
		určování polohy v reálném čase	ISO/IEC 24730-2, ISO/IEC 24730-5

Pro systémy kontroly vstupu je využíváno kmitočtu 125 kHz a 13,56 MHz. Transpondéry pracující s kmitočtem 13,56 MHz mají rychlý cyklus čtení - zápis, cca 20 kB/sec (tj. cca 10 x rychlejší než u čipů s frekvencí 125 kHz), kratší reakční dobu a vysokou bezpečnost přenosu. Většina technologií funguje antikolizně, to znamená, že pokud se dostane více čteček do čtecího dosahu, vzájemně se neruší. Mezi nejznámější a nejdostupnější patří tyto technologie:

Tabulka 3: Produkty EM Microelectronic [13]

EM Microelectronic			
Produkt	**Frekvence**	**Paměť**	**ISO**
EM4102	125 kHz	8 byte (read only)	
EM4105	125 kHz	16 byte	11784/85
EM4305	125 kHz	64 byte	11784/85
EM4450	125 kHz	125 byte	
EM4469	125 kHz	16 byte	11784/85

Tabulka 4: Produkty Atmel (Temic) [13]

Atmel (Temic)			
Produkt	**Frekvence**	**Paměť**	**ISO**
Temic 5557	125 kHz	330 bit	11784/85
Temic 5567	125 kHz	330 bit	11784/85

Tabulka 5: Produkty LEGIC [13]

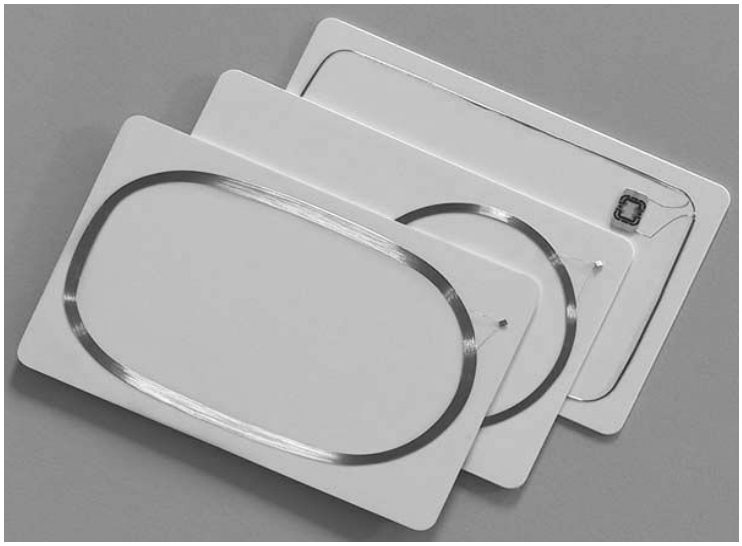
LEGIC®			
Produkt	**Frekvence**	**Paměť**	**ISO**
Advant ATC128-MV210	13.56 MHz	128 byte	15693
Advant ATC256-MV210	13.56 MHz	256 byte	15693
Advant ATC512-MP110	13.56 MHz	512 byte	14443A
Advant ATC1024-MV110	13.56 MHz	1024 byte	15693
Advant ATC2048-MP110	13.56 MHz	2048 byte	14443A
Prime MIM256	13.56 MHz	256 byte	
Prime MIM1024	13.56 MHz	1024 byte	

Tabulka 6: Produkty Philips [13]

Philips			
Produkt	**Frekvence**	**Paměť**	**ISO**
Mifare® Ultralight MF0 IC	13.56 MHz	64 byte	14443A
Mifare® MINI MF1 IC S20	13.56 MHz	320 byte	14443A
Mifare® Standard MF1 IC	13.56 MHz	1024 byte	14443A
Mifare® 4K MF1 IC S70	13.56 MHz	4096 byte	14443A
Mifare® DESFire MF3 IC	13.56 MHz	4096 byte	14443A
I-Code® 1 SL1 IC S30	13.56 MHz	64 byte	
I-Code® SL2 IC S20	13.56 MHz	128 byte	15693
HitagTM 1 HT1 IC S30	125 kHz	256 byte	
HitagTM 2 HT2 IC S20	125 kHz	32 byte	11784/85
HitagTM S HTS IC H32	125 kHz	4 byte (read only)	
HitagTM S HTS IC H56	125 kHz	32 byte	11784/85
HitagTM S HTS IC H48	125 kHz	256 byte	11784/85

Tabulka 7: Produkty HID

HID			
Produkt	**Frekvence**	**Paměť**	**ISO**
iCLASS 2000	13.56 MHz	256 byte	15693
iCLASS 2001	13.56 MHz	2048 byte	15693
iCLASS 2100	13.56 MHz	256 byte	15693
iCLASS 2010 PROX	13.56 MHz	256 byte	7816
iCLASS 2011 PROX	13.56 MHz	2048 byte	7816



Obrázek 10: Konstrukce klasické bezkontaktní karty

3.5 Biometrie

Slovo biometrie označuje měření určitých vlastností člověka, její podstatou je na základě unikátnosti získaných vlastností identifikovat uživatele. Vlastností, které mohou sloužit k identifikaci uživatele je celé řada, a dělí se do dvou základních skupin a to fyziologické a behaviorální. Do první skupiny patří mimo jiné i v systémech kontroly vstupu asi nejpoužívanější otisky prstů, či verifikace oční duhovky. Do druhé skupiny tedy behaviorální spadají například dynamika podpisu a verifikace hlasu. Na první pohled je biometrie u systémů kontroly vstupu díky své složitosti stále málo využívaná, a často bývá místo ní aplikován přístup pomocí karet, hesel, či tokenů. V poslední době se však hojně rozšiřuje, a to i díky velké konkurenci na trhu a klesající ceně. Velkou výhodu tohoto způsobu identifikace je jeho bezpečnost, to je způsobeno tím, že se ověřuje totožnost osoby, a ne pouze přítomnost správné karty nebo znalost hesla. Tím odpadá potřeba u sebe nosit kartu a pamatovat si heslo.

Mezi největší výhody biometrické identifikace patří především:

- vysoký stupeň spolehlivosti (osvědčené technologie lze jen obtížně oklamat),
- zanedbatelné provozní náklady,
- praktičnost (není co ztrácet ani přenášet),
- zřejmost (výsledek identifikace je jednoznačný a okamžitý),
- efektivnost (přímé datové propojení s databází a počítači).

3.5.1 Měření biometrických metod

Pro měření biometrie se používá míra pravděpodobnosti chybného odmítnutí FRR - False Rejection Rate. FRR je pravděpodobnost, že vyhodnocení dvou biometrických vzorků od stejné osoby dopadne odlišně a systém tak správnou (oprávněnou) osobu vyhodnotí chybně.

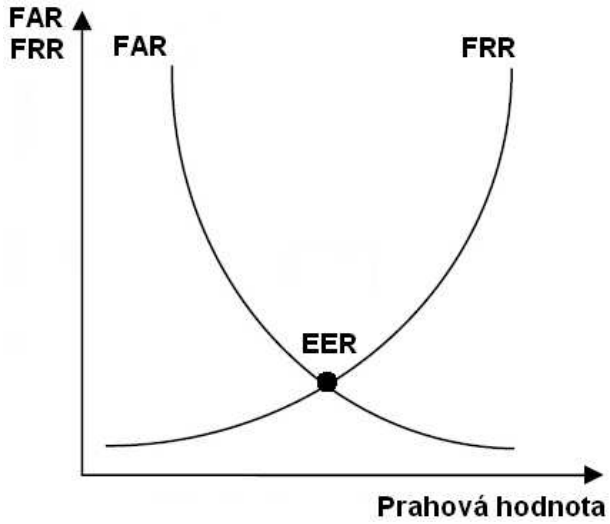
FRR = počet neshodných vzorků/celkový počet

Míra chybného přijetí FAR - False Acceptance Rate ukazuje pravděpodobnost přijetí odlišného vzorku jako správného. To znamená, že systém vyhodnotí dva odlišné vzorky jako totožné.

FAR = počet shodných porovnání rozdílných vzorků/celkový počet

Biometrické systémy mají různé citlivosti nastavení. Pokud citlivost nastavíme jedním směrem, zařízení bude náchylné k odmítání i oprávněných osob. Pokud je nastavíme druhým směrem, bude propouštět osoby oprávněné, ale i osoby nežádoucí. Podle praktického použití, prostředí a požadavků použijeme správné nastavení, abychom eliminovali výše uvedené negativní vlivy.

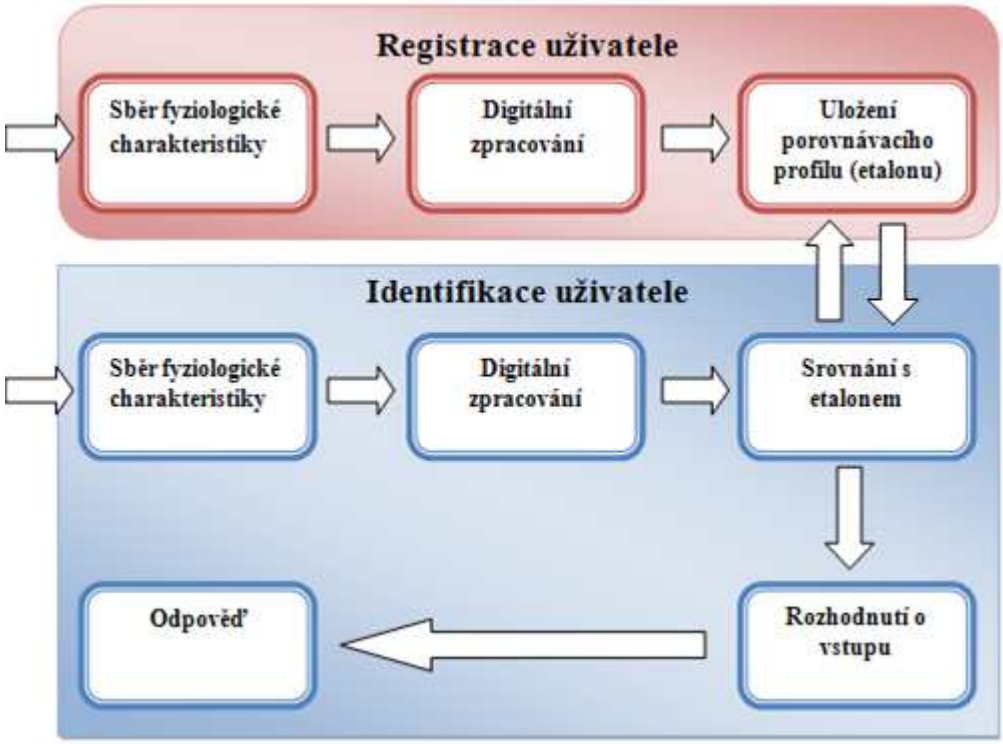
Míra, při které jsou si obě tyto hodnoty rovny se označuje jako ERR neboli míra rovné chyby. Podle této hodnoty lze alespoň přibližně určit bezpečnost biometrického systému. Nicméně první dva výše uvedené parametry mají daleko vyšší vypovídající hodnotu. [8,9]



Obrázek 11: Závislost FRR a FAR na prahové hodnotě

3.5.2 Princip biometrické identifikace

Předpokladem pro provedení je sejmutí a zápis fyziologické vlastnosti uživatele, která je dále uložena jako osobní porovnávací šablona (etalon). Snímání a zápis je potřeba provádět opatrně, jelikož kvalita pořízeného obrazu má zásadní vliv na proces ověřování. Z nasnímaných dat vybere biometrický systém nejvýraznější rysy specifické pro uživatele, a z nich pak vytvoří etalon, který se uloží do databáze a každé ověřování totožnosti pak probíhá jako porovnání nového měření s uloženým profilem. Celý proces je zobrazen na následujícím schématu.



Obrázek 12: Princip biometrické identifikace

Většina biometrických systémů pracuje následujícím způsobem:

-nejdříve dojde ke sběru fyziologické charakteristiky, ze které se pak vytvoří datový soubor (obraz, zvuk, atd.), který obsahuje biometrickou vlastnost, která z něj jde vyextrahovat použitím vhodného snímače.

-dále dojde k prověření kvality dat. Pokud jejich kvalita nevyhovuje, jsou okamžitě odmítnuta nebo je uživateli poskytnuta vhodná rada pro zvýšení kvality sejmuté biometrické vlastnosti (např. upozornění na směr snímání, polohu části těla atd.).

-vyextrahování požadované biometrické veličiny z datového souboru a vytvoření šablony vzorku.

-zápis dat, tedy uložení šablony jako porovnávacího profilu (etalonu) do archívu referenčních šablon systému či aplikace (dle definování místa ukládání).

-ověřování, které probíhá porovnáním aktuálního vzorku s uloženým etalonem užitím algoritmu pro určení shody a vygenerování hodnoty (skóre), která je rozhodná pro determinování stupně shody.

-na závěr je docíleno výsledku ověřování. Pokud skóre shody překročí předdefinovanou hranici, tak je přístup umožněn, v opačném případě je žádost odmítnuta. [8]

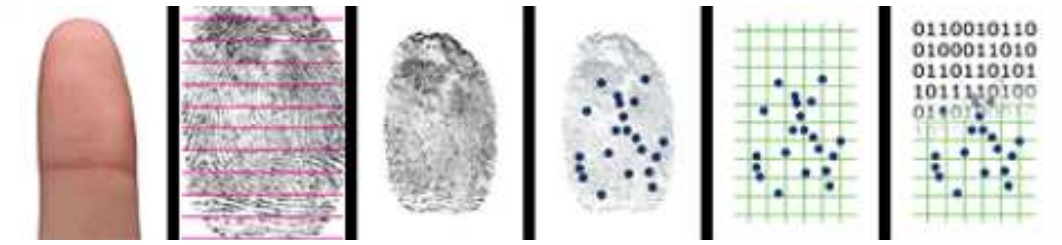
3.5.3 Možnosti ukládání etalonů:

a) uložení etalonu v biometrickém čtecím zařízení – výhodou této možnosti je rychlejší reakce při identifikaci, z důvodu nezávislosti na datovém spojení s databází etalonů. Nevýhodou ovšem je, že v případě závady je nezbytné znovu nainstalovat databázi etalonů nebo opětovně projít etapou zápisu
b) uložení etalonu ve vzdálené centrální databázi - tato možnost se zcela přirozeně nabízí pro IT systémy. Hlavní nevýhodou tohoto řešení je, že jakmile je síť mimo provoz, tak biometrický systém je vyřazen z činnosti.
c) uložení etalonu v přenosných tokenech – tento způsob nevyžaduje žádné lokální nebo centrální ukládání etalonů. Uživatel si nosí svůj etalon s sebou na tokenu, čipové kartě nebo jiném nosiči, a může jej použít všude tam, kam má povolen přístup. Nevýhodou tohoto řešení je vyšší finanční nákladnost a složitost biometrického systému z důvodu kombinace tokenového a biometrického čtecího zařízení na všech identifikačních místech.
d) kombinace předcházejících způsobů.[9]

3.5.4 Biometrická identifikace na základě otisku prstu

Jedná se o nejznámější, nejpropracovanější a nejpoužívanější biometrickou metodu, používanou pro přístupové systémy. Identifikace otisku prstu je s oblibou používaná především pro relativní jednoduchost získání srovnávacího vzorku, pro vysoké procento použitelné populace (nelze identifikovat pouze jedince, kteří přišli o obě ruce), dále pro četnost zdrojů ze kterých lze získat vzorek, tedy 10 prstů, a především pro vysokou míru spolehlivosti. Pro porovnání otisků prstů se používají identifikační body tzv. markanty. Tyto body se nacházejí v rýhách vzoru. Při porovnání otisků se sleduje jak přítomnost markantů, tak i jejich umístění v daném otisku. Otisk prstu obsahuje v průměru 75 – 175

identifikačních bodů. V praxi není stanoven přesný počet bodů nutný k rozlišení mezi dvěma otisky. Zásadou pro zabezpečovací techniku je, že se otisky uchovávají ve srovnávacím archivu pouze v digitální formě.[6,9]



Obrázek 13: Postup získání digitálního kódu z otisku prstu [9]

Z obrázku naskenovaného článku prstu jsou expedovány speciální znaky a archivovány jako biometrický klíč. Žádné otisky prstů nejsou ukládány, nýbrž pouze přeměněny na binární kód, který nelze znovu proměnit na otisk prstu. Nejdůležitějším prvkem této metody jsou tedy snímače otisků prstů.

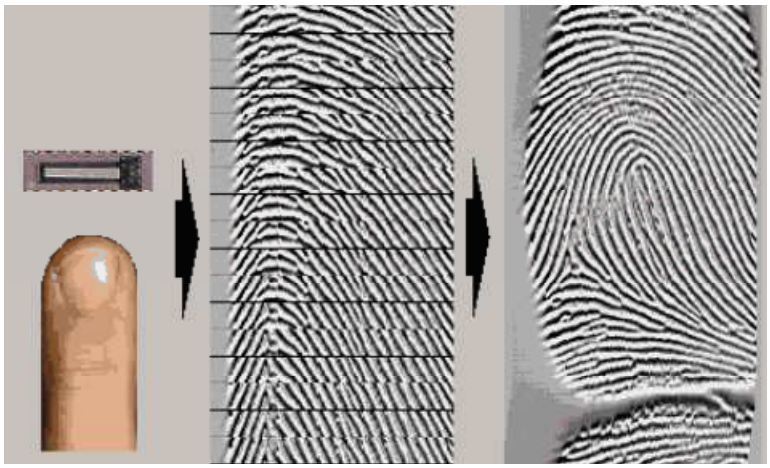
3.5.5 Metody získání otisku prstu

- Statické snímání

Jedná se o nejběžnější a nejvíce rozšířenou metodu snímání otisku prstu. Při snímání uživatel přitiskne daný prst na senzor, tak aby s ním nijak nepohyboval, a dojde k jeho přečtení. Výhodou této metody je jednoduché ovládání (stačí pouze přiložit prst). Na druhou stranu je zde řada nevýhod: přehnanou silou tlačení prstu může uživatel rozlomit snímací čočku (obzvlášť je-li doba snímání delší, uživatel znervózní a přitlačí více), přiložení prstu a jeho současné pootočení vede k deformaci pokožky a celého otisku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky.[8]

- Snímání šablonováním

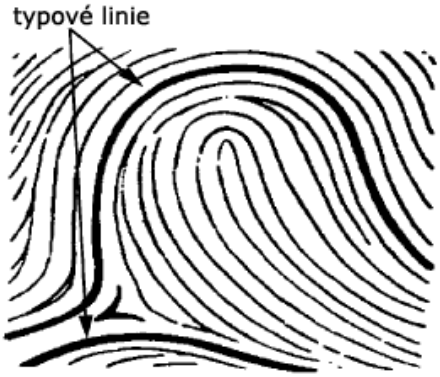
Při šablonování uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů. Snímač mívá často tvar úzkého pruhu. Mezi výhody šablonovaného snímání patří: snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor; na snímači nezůstávají skryté (latentní) staré otisky; uživatel nemá pocit, zanechaného otisku prstu a snímání je rychlé. Nevýhodou je, že obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup.[8]



Obrázek 14: Šablonování otisku prstu [10]

3.5.6 Klasifikace vzorů otisků

Bříško každého prstu obsahuje drobné prolákliny a vyvýšeniny. Na hranici pokožky a škáry se jsou tzv. škárové papily, které slouží k vyživování pokožky, ty jsou silné a zvlněné. Právě nepříliš velké variace papilárních linií umožňují jejich klasifikaci. Vzorovou oblast otisku tvoří linie, obklopeny typovými liniemi, které definujeme následovně. Jsou to dvě nejvnitřnější linie utvořené tak aby obemknuly centrální část otisku.[10]



Obrázek 15: Typove linie otisku prstu [10]

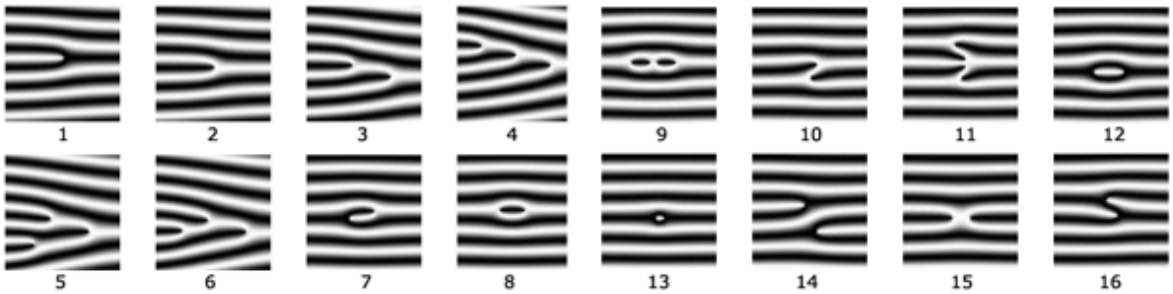
Papilární linie rozbíhající se do tří směrů se nazývá delta. Prvním kdo popsal jednotlivé typy charakteristických vzorů papilárních linií, byl Jan Evangelista Purkyně. Ten je klasifikoval do devíti základních vzorů. Z tohoto rozdělní vznikla novodobá klasifikace, jež rozeznává tři nejzákladnější vzory. [10]

1. Smyčka – v tomto případě papilární linie tvoří smyčku, mezi deltou a středem centrální oblasti musí být alespoň jedna probíhající linie. Smyčky tvoří téměř 2/3 vzorů všech otisků prstů.

2. Vír – Vír, neboli taky spirála obsahuje nejméně dvě delty s alespoň jednou samostatně probíhající linií, která může vytvářet kruhové, oválné či spirálovité obrazce, jejíž středem je jádro. Vír tvoří 1/3 všech otisků prstů.

3. Oblouk - Tento typ tvoří pouhých 5 - 10 % všech otisků. Papilární linie zde vytvářejí jednoduché oblouky. Typ neobsahuje žádné delty a dá se rozdělit do podkategorií oblouk plochý / klenutý.

Vzory, které papilární linie vytvářejí, se nazývají markanty. Jan Evangelista Purkyně publikoval v jeho seznamu devět charakteristických vzorů, v dnešní době jich je známo asi 16. Pro elektronickou identifikace se obvykle využívají pouze dva markanty a to rozdvojení a ukončení. Celkový výčet těchto vzorů vidíme na následujícím obrázku. [10]



Obrázek 16: Vzory papilárních linií [10]

Tabulka 8: Názvy vzorů papilárních linií

1	začínající / končící	5	trojitá vidlice typu2	9	dvojitý vír	13	bod
2	jednoduchá vidlice	6	trojitá vidlice typu3	10	most	14	přerušená linie
3	dvojitá vidlice	7	hák	11	dvojitý most	15	kříž
4	trojitá vidlice typu1	8	jednoduchý vír	12	interval	16	boční kontakt

3.5.7 Algoritmy rozpoznávání otisků prstů

Jelikož doposud nebyly stanoveny žádné standardy, které by definovaly typy algoritmů, až na několik sjednocených výrobců, si každý výrobce může určit, jakým způsobem budou algoritmy rozpoznávání řešeny. Přesto se zpravidla používají dva následující principy.

- Zkoumání podle globálního vzoru

Velkou výhodou tohoto typu jsou jeho nároky na rozlišení snímků, kdy nám standardně postačí 250 dpi a při snímání otisku tímto způsobem nevadí ani drobné poranění prstů. V sejmutém otisku, který je roztříděn do určité skupiny klasifikace, se postupně dále vyhledávají základní vzor, oblast vzoru, delty a počítají se i papilární linie. Cílem této metody je posouzení, zda míra závislosti dvou jevů je natolik vysoká, abychom mohli dojít k závěru, že porovnávané otisky jsou shodné. [10]

- Zkoumání podle podrobností

Tato metoda je oproti zkoumání podle globálního vzoru o něco náročnější na kvalitu snímku otisku, je zapotřebí alespoň dvojnásobné rozlišení. V tomto zkoumání se využívá markantů, jejich typu, pozice a orientace v otisku. Během binarizace neboli první fáze se z nasnímaného otisku vytvoří černobílý obraz a vzory jednotlivých papilárních linií se postupně ztenčují. Ve chvíli kdy mají vzory velikost jednoho pixelu, přistoupíme k samotnému vyhledávání a extrakci identifikačních bodů. Pak může proběhnout vlastní porovnávání otisků, přičemž se porovnávají vlastnosti nalezených markantů. Během těchto postupů se bere v úvahu i elasticita kůže a jiné zavádějící okolnosti. [10]

3.5.8 Snímače otisků prstů

Nejdůležitějším prvkem sytému jsou snímače otisků prstů. V současné době se na trhu vyskytuje několik typů snímačů, jako jsou například optoelektronické, kapacitní, teplotní, elektroluminiscenční, radiofrekvenční, tlakové, ultrazvukové, snímače na bázi fotonových krystalů atd. Všechny tyto technologie poskytují poměrně širokou škálu možností, přičemž každý má své výhody a nevýhody, které je třeba zvážit. Mezi nejpoužívanější patří:

- Optoelektrické snímače

Tato technologie je nejstarší a zároveň také nejrozšířenější. I do budoucna se zdá být nejvhodnější metodou pro toto odvětví. Jsou ideální především pro rozpoznání založené na

marketech. Umožňují jednoduché sejmutí otisku CCD detektorem, využívající osvětlení celé plochy prstu. Odrážené světlo pak prochází luminoforní vrstvou k CCD detektoru, kde se vytvoří obraz otisku. Mezi výhody patří vysoká kvalita čtení, statická odolnost a rezistence vůči vlivům okolního prostředí. Na druhou stranu je třeba si dát pozor na některé nevýhody. Například znečištění nebo poškození prstu může způsobit jeho nekorektní vykreslení na otisku. Stejně tak otisk zůstávající na detektoru může zkreslit další pořizované otisky. [6]

- Kapacitní snímače

U těchto snímačů, které se skládají ze dvou desek je využíváno rozdílu kapacity mezi deskou snímače a povrchem prstu tzn., že snímač rozeznává vyvýšeniny nebo prohlubně. Při snímání otisku je potřeba přiložit prst na citlivou plochu osazenou velkým množstvím elektrod, které pak převedou kapacitně otisk prstu na digitální obraz, ten se dál zpracovává. Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor. Mezi hlavní výhody patří malý rozměr, jednoduchý princip funkčnosti, vysoká kvalita a nízká pořizovací cena. Nevýhodou těchto snímačů je určitě jejich krátká doba životnosti z důvodu zničení snímače vlivem statické elektřiny, proto je nutné je měnit. Výměna se provádí ve většině případů v rozmezí tří let.

- Teplotní snímače

Jádrem teplotních snímačů je malý citlivý pyrodetektor, který snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostoru mezi nimi. Obraz otisku prstu se získává přejížděním prstem po citlivé ploše snímače. Výsledný obraz otisku je ve formě digitálních pásů. Následně se digitální obrazy skládají do výsledného obrazu otisku. U této metody existuje nebezpečí, že při několikanásobném přejíždění prstem přes snímač bude sejmuta vždy jiná část prstu, což výrazně limituje možnost vytvoření databáze otisků. Navíc tyto snímače neposkytují dostatečně vysokou kvalitu obrazu otisku, a proto nejsou pro použití v přístupových systémech vhodné.

3.5.9 Další používané biometrické metody:

- Geometrie ruky,
- Geometrie tváře,
- Duhovka oka,
- Sítnice oka,

- DNA,
- Tvar krevního řečiště ruky,
- Absorpční spektrum lidské kůže,
- Povrchová topografie rohovky,
- Struktura žil na zápěstí,
- Tvar článku prstu a pěsti,
- Vrásnění článků prstů,
- Tvar ucha,
- Ušní boltec,
- Tvar a lůžko nehtu,
- Planktogram – otisk bosé nohy,
- odraz zvuku v ušním kanálu,
- a další.

3.5.10 Behaviometrika

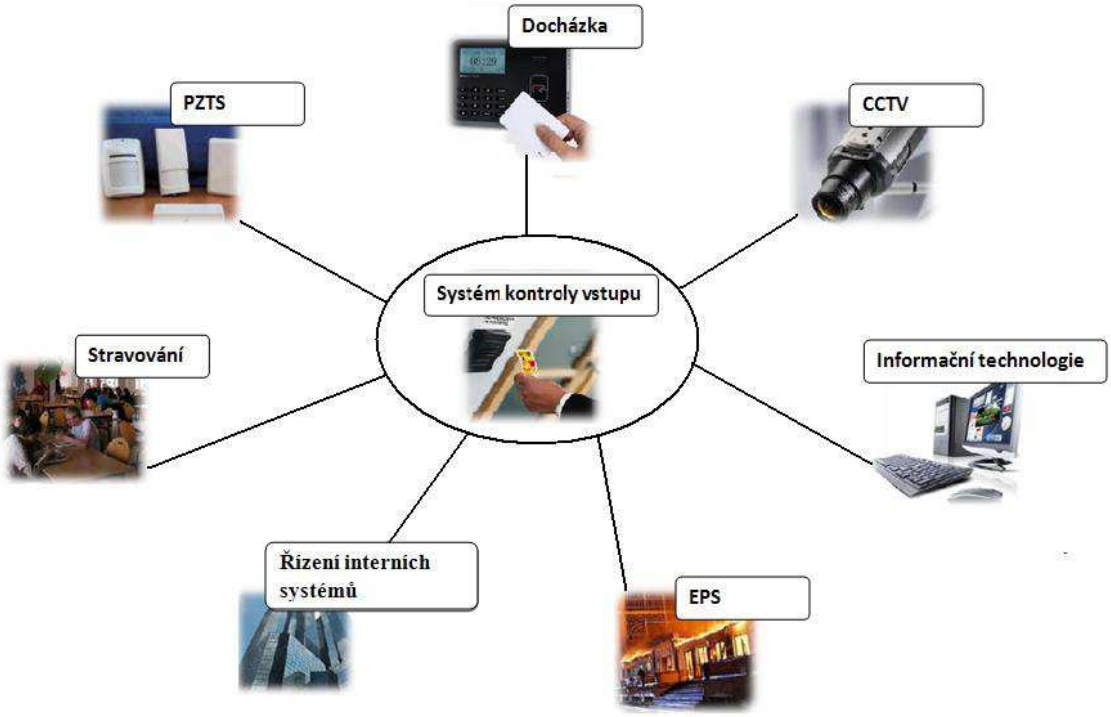
Jedná se o speciální podkapitolu biometriky, při níž nedochází ke sledování fyzických parametrů ale vlastností člověka, které jsou pro každého člověka jedinečné. Rozhodně jsou to zajímavé systémy, protože umožňují průběžnou kontrolu – nestačí, že oprávněný uživatel provedl autentizaci, neboť systém následně pozná, kdy v průběhu práce usedá ke klávesnici jiná osoba. V podstatě zde neexistuje možnost napodobení, protože nuance jsou tak drobné, že se je člověk nemůže naučit. [8]

Do oboru behaviometriky patří například:

- Psaní na klávesnici,
- dynamika podpisu,
- dynamika chůze,
- akustická charakteristika hlasu,
- tvar a pohyb rtů,
- identifikace podle způsobu pohybu očí,
- dynamika úsměvu,
- identifikace podle dynamiky pohybu myší,
- a další.

4 INTEGRACE S JINÝMI SYSTÉMY

Systémy kontroly vstupu mohou být i v kombinaci s dalším poplachovým systémem, potom tvoří společně jednu bezpečnostní aplikaci. Tyto systémy mohou být různě kombinovány s uzavřeným kamerovým systémem, docházkovým systémem, stravovacím systémem, apod. V neposlední řadě pak integrace do informačních technologií a řízení interních systémů. Integrace pochopitelně zvyšuje efektivitu systémů kontroly vstupu, a v mnoha případech se používá. V současné době se většinou používají tyto kombinace systémů kontroly vstupu:



Obrázek 17: Integrace s jinými systémy

- Integrace systému EKV s PZTS

Jedná se o velmi často používanou součinnost mezi systémem kontroly vstupu a poplachovým zabezpečovacím systémem. Po úspěšném provedení identifikace a následném umožnění vstupu uživateli se na trase, nebo v místnostech kam má uživatel povolen přístup odalarmuje systém PZS, tak aby nedošlo k vyvolání nežádoucího poplachu. Používá se všude tam, kde nestačí pouze elektronická kontrola vstupu, ale je nutno ještě zajistit objekt, nebo jeho část poplachovou zabezpečovací signalizací.[2,6]

- Integrace systému EKV s EPS

Asi nejčastější a nejjednodušší integrace se provádí právě se systémem elektrické požární signalizace. Používá se k zajištění automatického otevření únikových tras v případě detekce požáru systémem EPS. Z důvodu rychlosti reakce, spolehlivosti a univerzálnosti je integrace prováděna zapojením napájení elektrických zámků přes kontakt signalizačního relé systému EPS. Z bezpečnostního hlediska se jedná o velmi důležitou funkci. Důležité je aby se v případě vyhlášení požáru vědělo kolik osob se v objektu zabezpečeném systémem EKV nachází. V dnešní době tuto možnost většina systémů podporuje. Je ale důležité aby se při vstupu do objektu identifikovaly opravdu všechny osoby. U systémů, které nejsou současně využívány i jako docházkové totiž ve vyšší míře hrozí že se identifikuje jedna osoba a poté projde více osob než se zase dveře zaklapnou. To zda uživatelé tuto povinnost dodržují, bývá zpravidla řešeno režimovým opatřením. [2]

- Integrace systému EKV se CCTV

Používá se tam, kde je nutno kontrolovat nejen pohyb osob po objektu, ale i sledovat celkovou činnost osoby nebo osob v objektu a mít permanentní kontrolu veškerého pohybu v objektu s možností včasné reakce na nežádoucí situaci, která může vzniknout např. ve věženích, vojenských skladech., letištích, jaderných elektrárnách, chemických provozech apod. Kamerový systém může být z důvodu úspory energie vypnutý a zapne se až po identifikaci osoby přístupovým systémem. Kamery se umisťují taky často, aby měli v záběru identifikační zařízení (terminál, čtečku atd.), a to nejčastěji z důvodu vandalismu či jiného poškození. [2]

- Integrace systému EKV s docházkovým systémem

Nejviditelnější komponentou docházkového systému je docházkový terminál nahrazující někdejší píchací hodiny, docházkové sešity a knihy docházky elektronickým zařízením. Docházkový terminál ale určitě není rozhodující částí systému. Těžiště kvalitního docházkového systému spočívá především v softwarovém řešení. Moderní docházkové systémy musí být schopné zpracovávat pevnou i pružnou pracovní dobu s rovnoměrným i nerovnoměrným rozdělením, různé typy směn, přerušení pracovní doby, dovolené, evidovat noční a přesčasovou práci, pohotovost a pracovní cesty a současně hlídat splnění všech zákonných požadavků a limitů. Důležitá je vazba na personální agendu, neboť docházka se eviduje pro osoby v pracovněprávním vztahu k zaměstnavateli. Neméně důležitá je vazba na zpracování platů a mezd, které závisí na evidenci

odpracované doby. Většina současných systémů získává vstupní data prostřednictvím docházkových terminálů. Existuje řada typů terminálů, od nejjednodušších, pouze s pevně přiřazenými tlačítky, přes specializované terminály s textovým nebo grafickým displejem až po průmyslové tablety s dotykovou obrazovkou a plnohodnotným operačním systémem. [11]

- Integrace systému EKV se systémem pro výdej stravy

Systém stravování se nejčastěji používá pro podnikové jídelny, školy a internátní zařízení, domovy pro seniory a další podobné instituce. Systém nahrazuje a automatizuje standardní stravenkový systém. Správa probíhá buď to přes terminál, nebo přes internet., kde si obvykle uživatelé navolí dopředu jídla, která se potom vydávají automaticky na výdejních místech přiložením karty nebo čipu k výdejnímu snímači.

- Integrace systému EKV s řízením interních systémů

Tato integrace se používá především v moderních inteligentních budovách a nabízí další nadstandardní funkce, jako například řízení a zabezpečení výtahů. Pro náročnější uživatele se dá nastavit automatické řízení klimatizace a topení, zapnutí či vypnutí osvětlení, odtažení či zatažení rolet po úspěšné identifikaci a následném vstupu uživatele do objektu a určitě i další funkce.

- Integrace systému EKV s informačními technologiemi

Jedná se o přihlašování k PC, do sítí a různých software, aplikací, atd.. Vzhledem k omezeným možnostem zapamatovat si kódy a hesla se stále více využívá identifikačních karet a biometrické identifikace, která se v dnešní době často implementuje do elektronických zařízení (počítače, notebooky, mobily, tablety, atd.).

5 AUTENTIZAČNÍ METODY

Kvalita jakéhokoliv automatizovaného systému kontroly vstupu je závislá téměř výhradně na kvalitě identifikačního mechanismu, a tvoří pevné základy pro ochranu informací. Je-li identita uživatele ověřena v rozsahu povolené odchylky, je systémem zprostředkován přístup do prostředí s řízeným přístupem, v opačném případě je přístup zamítnut. Identifikační metody obecně mohou být založeny buď na něčem co daný uživatel zná, něčem co daný uživatel má, nebo něčem čím daný uživatel je. Typickým příkladem metod spadajících do první z těchto kategorií je heslo, PIN (osobní identifikační číslo), nebo určitá přístupová fráze. Druhá kategorie je založena na vlastnictví identifikačního předmětu, nejčastěji tedy karet, přívěsků apod. A konečně, do kategorie třetí pak spadají různé charakteristiky daného jedince, jejichž typickým příkladem je otisk prstu. Všechny tyto metody ale mají svá pro a proti.[6]

5.1 Autentizace heslem

Jedná se o v současné době nejjednodušší způsob identifikace, a přesto, nebo právě proto je používána ve velkém množství aplikací. S používáním hesel má své zkušenosti každý uživatel počítače. Zadání správného hesla po něm požaduje zpravidla již startující operační systém. Výhoda identifikace založené výhradně na hesle je, že může být po technické i programové stránce realizována velice jednoduše, a tím i levně. Přesto tato metoda velice často selže z mnoha důvodů. Mezi nejčastější důvody selhání patří už jen to, že je uživateli dovoleno, aby si heslo vytvořil sám, a tím pádem má tendenci zvolit si takové, které se mu lehce pamatuje, a pak může být lehce uhodnutelné. Dalším problémem může být heslo vygenerované z náhodné kombinace znaků, v tomto případě často hrozí, že si ho uživatel z důvodu obtížného zapamatování někam poznamená.

Zjednodušenou formou hesla je PIN, poskytující jinou možnost posílení bezpečnosti. V tomto případě je zpravidla omezen počet pokusů, které jsou k dispozici pro uhádnutí PINu. Pokud uživatel v daném počtu pokusů nezadá správné heslo, nastává obvykle zablokování PINu a je nutné ho poté složitějším mechanizmem odblokovat, tím se vynuluje počet chybných pokusů, nebo uživatel dostane identifikační číslo nové. Toto se ovšem u systémů kontroly vstupu dá aplikovat pouze při vícefaktorové identifikaci, kdy se uživatel nejdříve prokáže předmětem a poté je vyzván k zadání PINu. Obvyklý PIN je složen pouze z číslic a jeho délka bývá nejčastěji 4 znaky, pro větší bezpečnost lze ovšem použít i 5-8 znaků. Je důležité, aby PIN znali pouze oprávnění uživatelé, nejlépe nazpaměť.

Charakteristikou správného používání PINu je, že je distribuováno zabezpečeným způsobem, není nikde poznamenáno, je často obměňován a to alespoň každé dva měsíce. Při zadávání PINu je důležité soukromí, to znamená nepřipustit jakékoli vměšování cizích osob do průběhu jeho zadávání. Taktéž je zpravidla doporučeno při zadávání PIN zakrývat klávesnici rukou, či tělem, a zabránit tak jakémukoli odpozorování cizími osobami.[6,12]

5.2 Autentizace předmětem

Obecné označení pro identifikační předmět, který potvrzuje identitu svého vlastníka, je token. Pod tímto pojmem si můžeme představit čipovou kartu, USB token, ale i bezkontaktní čip různého tvaru. Token musí být jedinečný a obtížně padělatelný. Tokeny používané v automatizovaných identifikačních systémech jsou vybaveny informací, která je používána při provádění identifikačního protokolu. Vzhledem k tomu, že informace uložená na tokenu je jedinečná, musí být zabezpečena proti duplikaci nebo krádeži. Největší hrozba pro bezpečnost takovéhoto typu systému spočívá v tom, že token může být ukraden. Tato hrozba může být zmírněna tím, že identifikační systém používá vícefaktorovou identifikaci (např. token v kombinaci s PIN). Bez znalosti PINu je pak ukradený nebo padělaný token systémem kontroly vstupu odmítnut.

Používané identifikační předměty jsou:

- Tokeny pouze s pamětí - jsou obdobou mechanických klíčů, paměť obsahuje jednoznačný identifikační řetězec. Patří zde především magnetické, elektronické nebo optické karty.

- Tokeny udržující hesla - vydají určený kvalitní klíč po zadání jednoduchého uživatelského hesla,

- Tokeny s logikou - umějí zpracovávat jednoduché podněty typu: vydej následující klíč, vydej cyklickou sekvenci klíčů,

- Inteligentní tokeny (smart cards) - mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu, mohou šifrovat, generovat náhodná čísla apod.

I přes nesporné výhody, které používání identifikačních předmětů s sebou přináší, je stejně jako u hesel hlavní nevýhodou jejich přenositelnost. Tato vlastnost má u obou identifikačních metod za následek, že pouhá znalost hesla či vlastnictví identifikačního předmětu umožňuje komukoli vydávat se za někoho jiného, než ve skutečnosti je. [6,12]

5.3 Biometrická identifikace

Je založena na automatizovaném zjišťování a porovnávání jedinečných biologických charakteristik uživatelů přístupového systému. Biometrické charakteristiky (biometriky) jsou měřitelné fyziologické nebo chování se týkající vlastnosti, které mohou být využitelné pro ověření identity jednotlivce.

Biometrické techniky můžeme použít na dvě rozdílné aplikace: na autentizaci neboli verifikaci identity a na identifikaci. Autentizace je proces, při kterém subjekt předkládá tvrzení o své identitě (např. vložením karty) a na základě takto udané identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami. Odpovídáme na otázku: "Je to opravdu ta osoba, za kterou se sama vydává?" Při identifikaci naopak člověk identitu sám nepředkládá, systém prochází všechny záznamy v databázi, aby našel patřičnou shodu a identitu uživatele sám rozpoznal. Systém odpovídá na otázku: "Kdo to je?" Je zřejmé, že identifikace je podstatně náročnější proces než autentizace. Se zvyšujícím se rozsahem databáze se přesnost identifikace snižuje a rychlost klesá.

Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je odpověď systému na autentizační požadavek. Biometrické systémy nedávají jednoduché odpovědi typu ano/ne. Podpis člověka však není vždycky naprosto stejný, stejně tak pozice prstu při snímání otisku se může trochu lišit. Biometrický systém proto nemůže určit identitu člověka absolutně, ale místo toho řekne, že s určitou pravděpodobností se jedná o daného jedince.[12]

5.4 Vícefaktorová autentizace

Jak jsem již naznačil, používání vícefaktorové autentizace se zpravidla využívá u vyššího stupně zabezpečení kontroly vstupu. Nejčastěji se tedy jedná o dvoufaktorovou autentizaci, která zahrnuje kombinaci identifikačního tokenu a PINu. Systém bývá nejčastěji nakonfigurován tak, že se uživatel nejdříve prokáže tokenem a pokud je systémem přijat, je vyzván k zadání PINu, může tomu být však i obráceně. Další cestou, která se zde nabízí, je využití biometrických údajů. Ty mohou být kombinovány jak s tokenem, tak s PINem. Při použití biometrických metod se tak dostáváme ke tří- a vícefaktorové autentizaci.

5.5 Porovnání metod

Hesla lze použít pouze pro nejnižší stupeň zabezpečení. Největší jejich nevýhodou je, že se jich dá relativně snadno zmocnit a že jsou přenositelná. Tokeny lze použít pro vyšší stupeň zabezpečení. Lze se jich však také relativně snadno zmocnit a jsou přenositelné.

Kombinace tokenu a hesla (PIN) lze použít pro poměrně vysoký stupeň zabezpečení. Tato kombinace je značně odolná při odcizení nebo ztrátě tokenu, avšak není odolná vůči zapůjčení tokenu a vyzrazení hesla - jsou přenositelné.

Biometriky lze použít pro nejvyšší stupeň automatizovaného zjišťování a porovnávání zabezpečení. Nelze je ztratit ani jednoduše přenášet a představují jedinečný identifikátor uživatele - jsou nepřenositelné.

Souhrnně však hesla, identifikační tokeny i biometriky mohou být podrobeny útokům. Heslo může být uhodnuto, token může být ukraden a biometrika může být sofistikovaně napodobena. Tyto hrozby mohou být výrazně zmenšeny použitím jednotlivých identifikačních metod ve vzájemné kombinaci.

Vzhledem k tomu, že biometrická zařízení je obtížné oklamat, je ověření identity uživatele pomocí biometrik mnohem spolehlivější než při pouhém používání hesel nebo autentizačních předmětů. Vhodná příležitost pro integraci biometrik do identifikačních procesů se naskytne tehdy, podaří-li se zautomatizovat autentizační proces tak že uživatele příliš neobtěžuje. Biometriky v žádném případě nepředstavují všelék pro všechny možné problémy spojené s identifikací jednotlivce. Svými možnostmi však představují prostředek, který je v identifikačních nástrojích nezastupitelný a bez něhož nelze v současné době realizovat zabezpečovací projekt nejvyšší úrovně. [6,9]

II. PRAKTICKÁ ČÁST

6 METODA DOSAŽENÍ CÍLU PRÁCE

V praktické části práce jsem na základě průzkumu trhu zmapoval analýzu spokojenosti uživatelů s používáním systémů EKV, s cílem zjištění funkcí, které typickým uživatelům systémů EKV chybějí a které naopak nevyužívají. Další provedený průzkum se týká spokojenosti a komfortu se správou systémů, a je tedy určen právě správcům těchto systémů. Jako nástroj pro získávání informací jsem zvolil metodu online dotazníku.

6.1 Dotazníkový průzkum

Jak jsem již naznačil, použitou technikou sběru informací bylo dotazování pomocí online dotazníku. Obecně je dotazník vlastně způsob psaného řízeného rozhovoru. Na dotazy, které jsou na rozdíl od rozhovoru psané, se vyžadují písemné odpovědi, ať už formou výběru z odpovědí nebo zapsáním vlastního názoru. Tuto metodu jsem zvolil z důvodu menší časové náročnosti. Dotazníky jsem vytvořil po registraci na internetových stránkách www.vyplnto.cz, distribuce probíhala e-mailem, případně za použití jiných komunikačních programů a sociální sítě. Respondenti, kteří odpovídali na otázky, jsou běžnými uživateli systémů EKV. V dotaznících se vyskytují dva typy otázek.

- Uzavřené otázky – tyto otázky nabízejí tázanému volbu mezi dvěma či více možnými odpověďmi, např. ano - ne - nevím. Tento typ otázek se používá nejčastěji pro kvantitativní průzkumy. Nesmí se stát, že někdo nebude umět na uzavřenou otázku zodpovědět. Proto je třeba věnovat velkou pozornost struktuře odpovědí.
- Otevřené otázky - resp. otázky s otevřeným zakončením dávají odpovědím tázaného širší vztahový rámec. Otázky tohoto typu jsou pružné, mají možnost prohlubování. Dotazovaní někdy uvedou nečekané odpovědi, které mohou často napomoci k řešení dané problematiky, kvůli které je průzkum prováděn.

6.2 Průzkum uživatelského komfortu

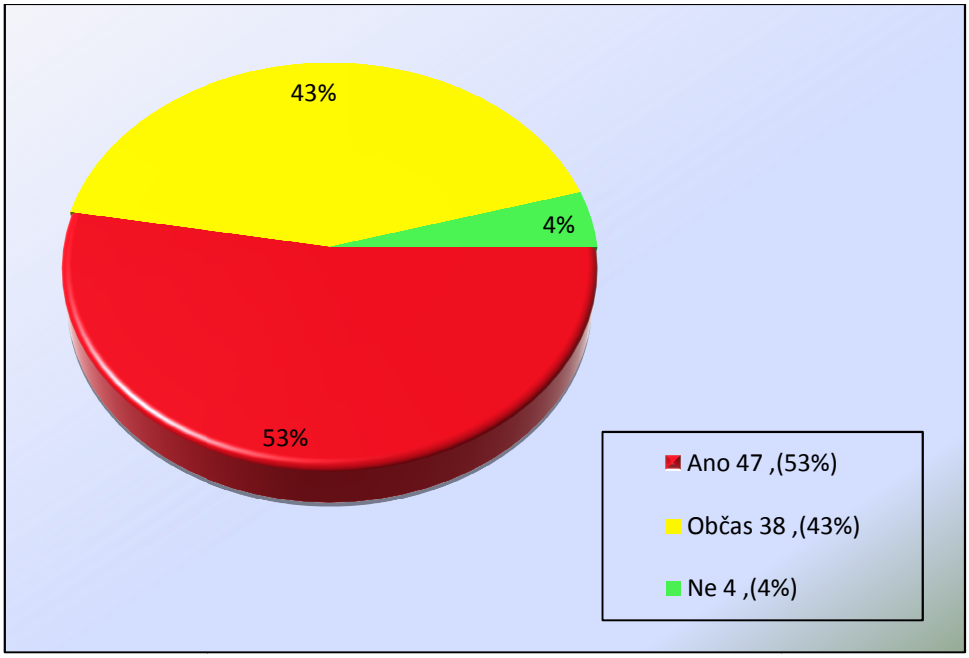
Cílem tohoto průzkumu bylo zjištění míry spokojenosti koncových uživatelů s používáním systémů EKV. Samotná struktura dotazníku byla tvořena:

- Úvodní část – obsahovala popis problematiky, smysl a účel dotazníku,
- Vlastní soubor otázek,
- Poděkování za strávený čas a vyplnění dotazníku.

Samotný online dotazník obsahoval 12 otázek, při jeho vyplňování museli respondenti odpovědět na všechny uvedené otázky, byly tedy povinné. Způsob zobrazení dotazníku spočíval v zobrazení všech otázek na jednou. Z celkového počtu byly 4 otázky zcela uzavřené, tj. odpovídající musel vybrat jednu z uvedených odpovědí. Zbylých 8 bylo polo-uzavřené otázky, kde byla přidána možnost „jiná odpověď“ pro dopsání vlastního názoru. Dotazník vyplnilo celkem 89 respondentů (zpravidla se běžně neuvažuje vyplnění všech rozeslaných dotazníků).

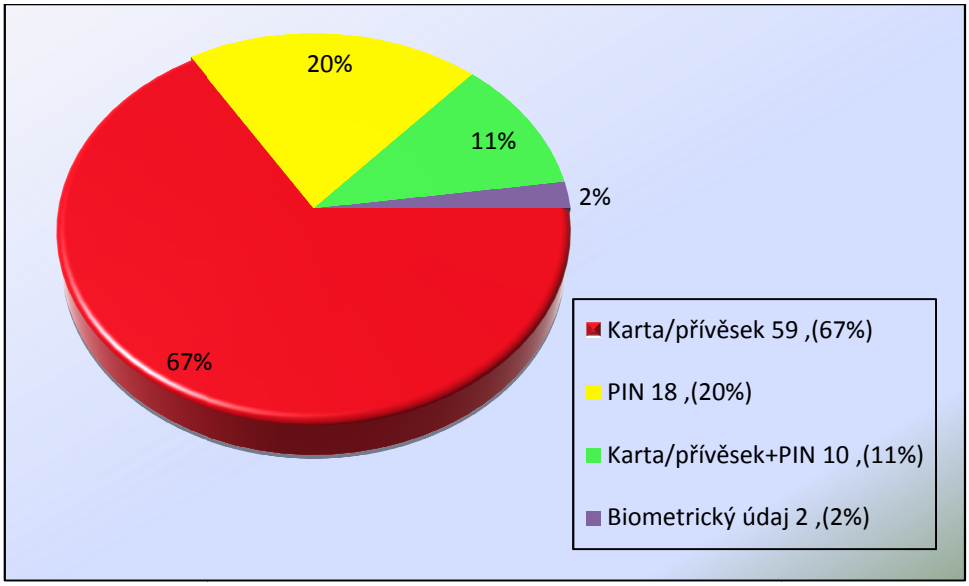
6.2.1 Interpretace výsledků dotazníkového průzkumu uživatelské spokojenosti

Graf 1: Používáte systémy elektronické kontroly vstupu pravidelně?



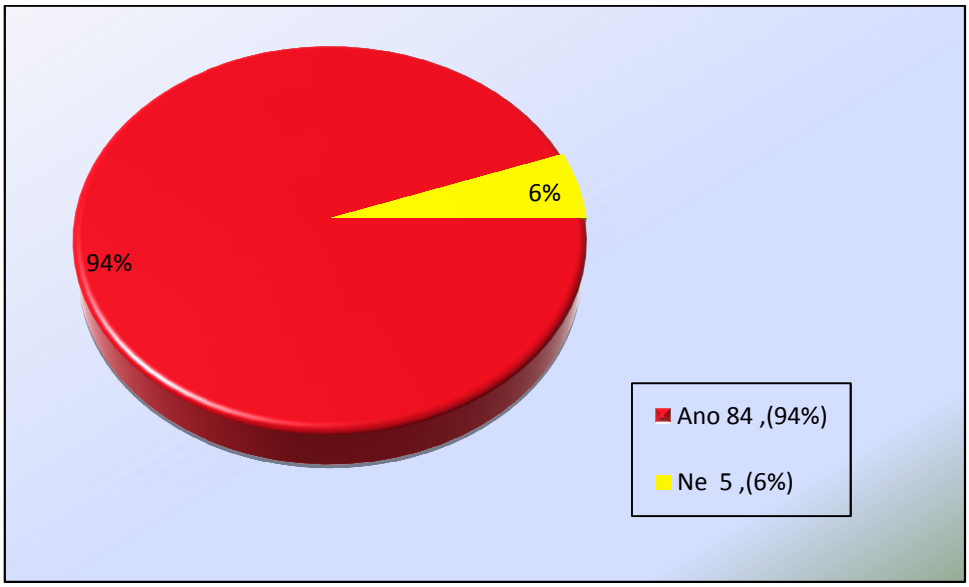
První otázka dotazníku sloužila spíše k ověření, zda odpovídající používá systémy EKV pravidelně, občas nebo jen příležitostně. Z uvedených odpovědí je vidět že většina respondentů přichází do styku s těmito systémy pravidelně, a jejich odpovědi mají určitě vyšší vypovídající hodnotu.

Graf 2: Jak se prokazujete při identifikaci?



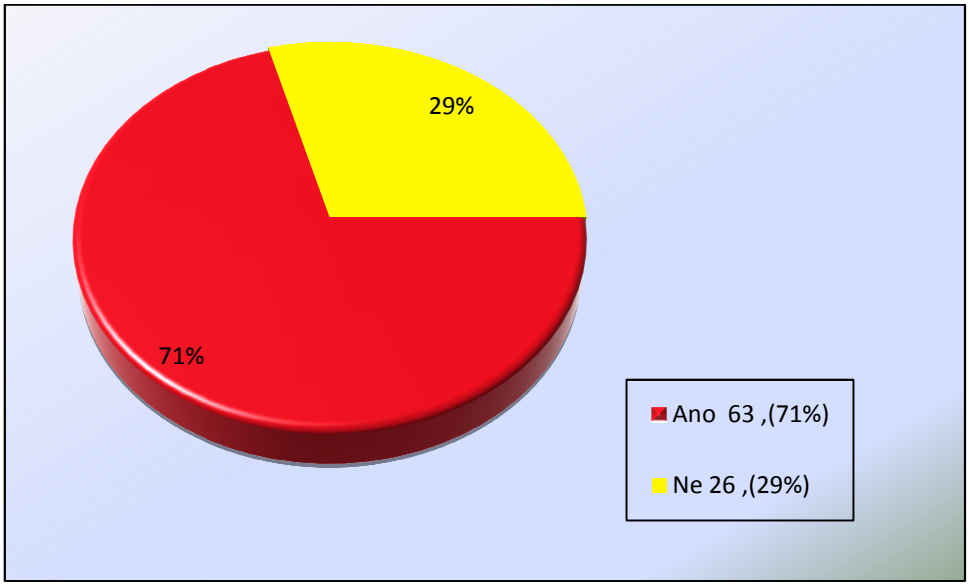
Odpovědi týkající se způsobu identifikace resp. autentizace, nejsou nijak překvapivé. Potvrzují jenom to, že jako nejčastější forma autentizace se v současné době používají bezkontaktní karty, které jsou rozumným kompromisem mezi kvalitní nákladnější biometrikou a ochranou heslem. Za zmínku určitě stojí 11% uživatelů používajících vyšší stupeň zabezpečení vstupu, a to dvoufaktorovou autentizaci v podobě kombinace karty, či přívěsku a PINu.

Graf 3: Je podle Vás ovládání elektronické kontroly vstupu intuitivní a pohodlné?



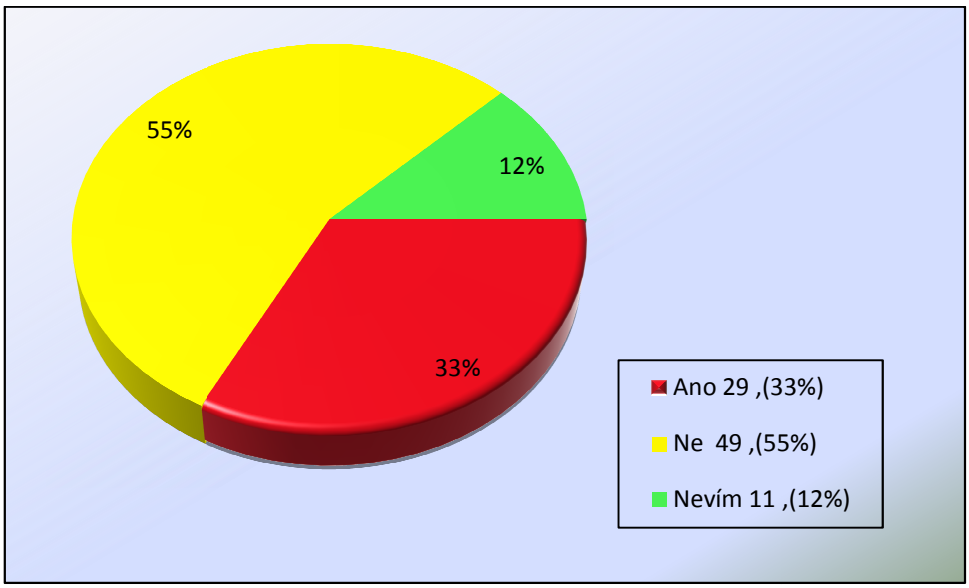
Průzkumem bylo dále zjištěno, že pro naprostou většinu (94%) je ovládání systémů EKV intuitivní a pohodlné

Graf 4: Používáte identifikační kartu/předmět pro ovládání jiných zařízení?



Z celkového počtu 63 uživatelů (71%), kteří uvedli, že identifikátorem ovládají i jiná zařízení než jenom vstupní prvky, využilo 15% možnosti uvedení jakého zařízení. Mezi tyto patřil stravovací systém, ovládání výtahu a kopírky.

Graf 5: Slouží systém který používáte, také k evidenci docházky?



U téměř třetiny oslovených respondentů funguje systém EKV také jako docházkový. V 55% slouží systém pouze jako přístupový. Zbylých 12% respondentů konstatovalo, že neví.

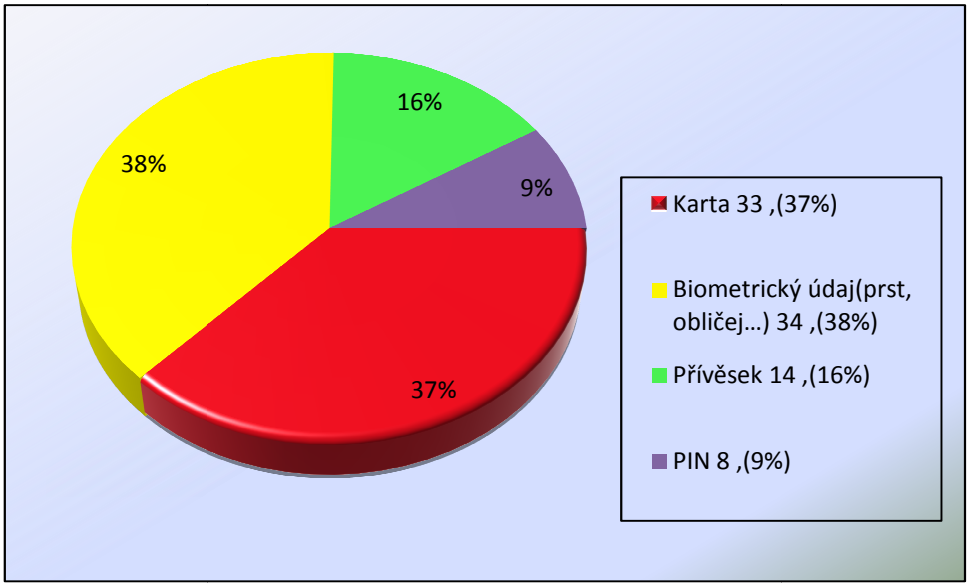
Grafy dalších dvou otázek záměrně vynechám, protože se jedná opět o odpovědi typu Ano – Ne. Jedná se o otázky:

- *„Stalo se, že se Vám identifikační karta/předmět ztratil nebo byl odcizen?“*

  Výsledkem tohoto dotazu bylo, že 85% uživatelů nikdy nemělo problém se ztrátou nebo odcizením identifikačního předmětu (identity). Zbylých 15% muselo tuto nepříjemnost řešit. S ohledem na statistiku se jedná o každého cca 6 uživatele. Bohužel spočívá příčina tohoto problému především v neopatrnosti uživatelů při přenášení a uchovávání identifikátoru. Bez včasného zablokování přístupu ztracené identity by mohlo dojít v zabezpečeném objektu ke značným škodám.
- *„Stalo se, že se Vám identifikační karta/předmět zničil?“*

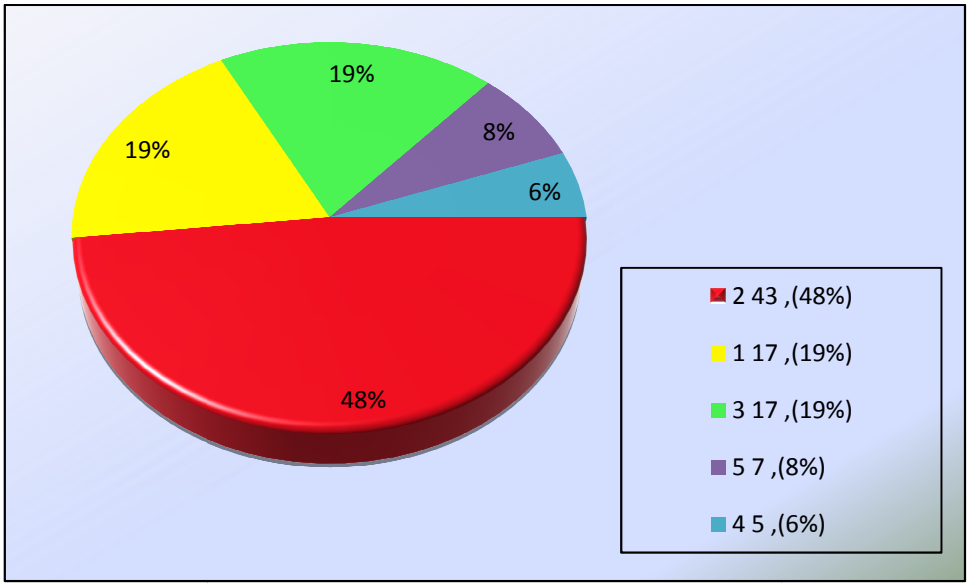
  Tento problém řešilo z celkového počtu respondentů 28%. Mezi příčiny nefunkčnosti byly uvedeny rozlomení či nalomení karty, poškození čipu a poškrábání magnetického pásku. Poškození identifikačního předmětu se nejčastěji děje jeho opotřebováním, nesprávnou manipulací a nekvalitnosti materiálu, z něhož byl předmět vyroben.

Graf 6: Používání jakého identifikátoru je podle Vás nejkomfortnější a nejpohodlnější?



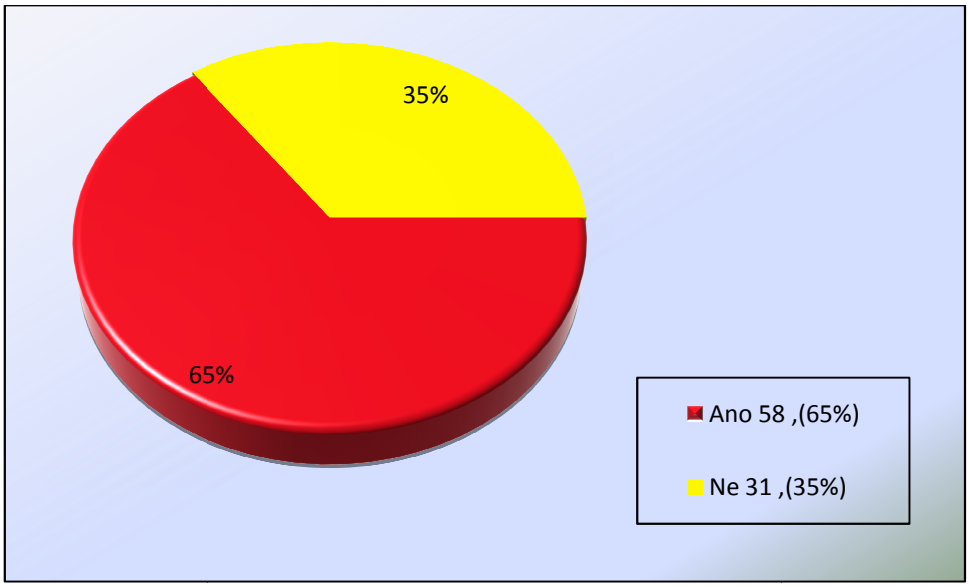
Čistě názorová otázka na komfort a pohodlnost při provádění identifikace do systému EKV ukazuje překvapivě vyšší procento uživatelů (38%), kteří přikládají sympatie biometrickým systémům. Druhým nejoblíbenějším autentizačním prostředkem je v dnešní době nejrozšířenější bezkontaktní karta (37%). Poměrně nízké procento respondentů (16%) vidí jako nejpohodlnější používání identifikačního přívěsku. Nejmenší oblibu sklidila podle očekávání autentizace heslem (9%).

Graf 7: Kolik různých identifikátorů využíváte (např. v práci, doma, na bazénu, v obchodě, na parkovišti, přihlášení k PC, apod.)?



Jak je vidět z výše uvedeného grafu vyplívá, že naprostá většina respondentů (81%) využívá více než jeden identifikátor. Téměř polovina (48%) běžně používá na různých místech identifikátory dva. Tři identifikační předměty potřebuje k přístupu do zájmových prostor 19% odpovídajících. Mezi odpověďmi se dále vyskytlo použití 4 (6%), a dokonce 5 (8%) identifikátorů.

Graf 8: Myslíte si, že by bylo vhodné jeden identifikátor používat na více různých místech?



Důvodem zařazení této otázky do průzkumu je myšlenka sjednocení více identifikátorů pod jeden. Jak je vidět většina odpovídajících (65%) by uvítala, kdyby měli jeden identifikátor a ten fungoval všude, kde potřebují. Vzhledem k tomu, že početná část uživatelů (viz. Graf č. 7) používá více, než jeden identifikátor se tato myšlenka jeví velmi zajímavě.

Předposlední otázka se týkala problémů při používání systému. Naprostá většina (80%) se nesetkala při používání s žádnými problémy. Ve zbylých 20% zazněly problémy jako zamrznutí systému či nepřijetí oprávněného čipu čtecím zařízením.

Na závěr byla položena otevřená otázka, tj. odpovídající musel napsat vlastní odpověď:

"Napadá Vás nějaká funkce, která by usnadnila používání systému?"

Kromě záporných odpovědí by osloveným uživatelům usnadnilo používání, případně by viděli přínos ve:

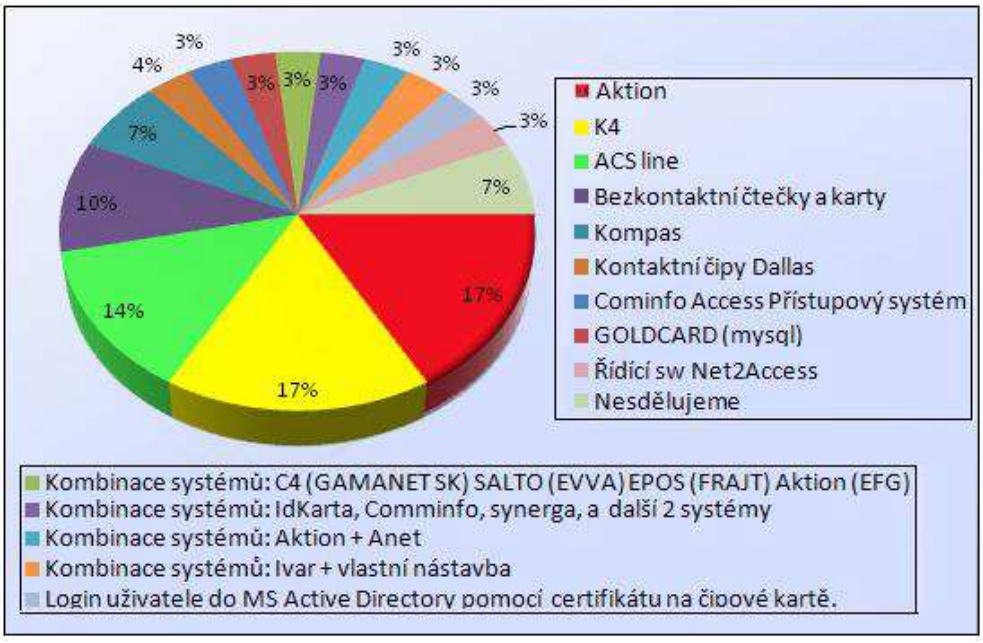
- Zvýšení čtecí vzdálenosti mezi snímacím zařízením a identifikačním médiem,
- Sloučení více identifikátorů,
- Identifikace přes mobilní telefon,
- Integrace do celkového systému.

6.3 Průzkum komfortu správy systémů

Cílem tohoto průzkumu je analýza spokojenosti správců systémů EKV s jeho správou, nastavováním a údržbou. Dotazník byl tvořen z 8 povinných otevřených otázek, na které správci systémů, IT technici či jiné osoby mající správu na starosti odpovídali. Průměrná délka vyplňování jednoho dotazníku byla 10 minut. Dotazník byl rozeslán do cca 140 firem či jiných institucí, kde byl předpoklad používání systému EKV. Celkový počet vyhodnocených vzorků je 31, osobně jsem čekal více, nicméně tento počet pro náš průzkum určitě postačil. Návratnost dotazníku činila 20%, nejedná se ovšem o poměr rozeslaných dotazníků ku vyplněným, ale o poměr vyplněných ku zobrazeným (to znamená, že zbylých 80% respondentů dotazník pouze otevřela ale nevyplnila, případně neodeslala data). Je to dáno ať už bezpečnostní politikou daného subjektu nesdělovat informace o zabezpečení objektu, nebo neochotou k vyplnění dotazníku.

6.3.1 Interpretace výsledků dotazníkového průzkumu komfortu správy

Graf 9: Jaký typ systému používáte?



První otázka dotazníku určeného pro správce systémů EKV se týkala typu používaného systému. Pro informaci uvedu stručnou charakteristiku nejvíce používaných.

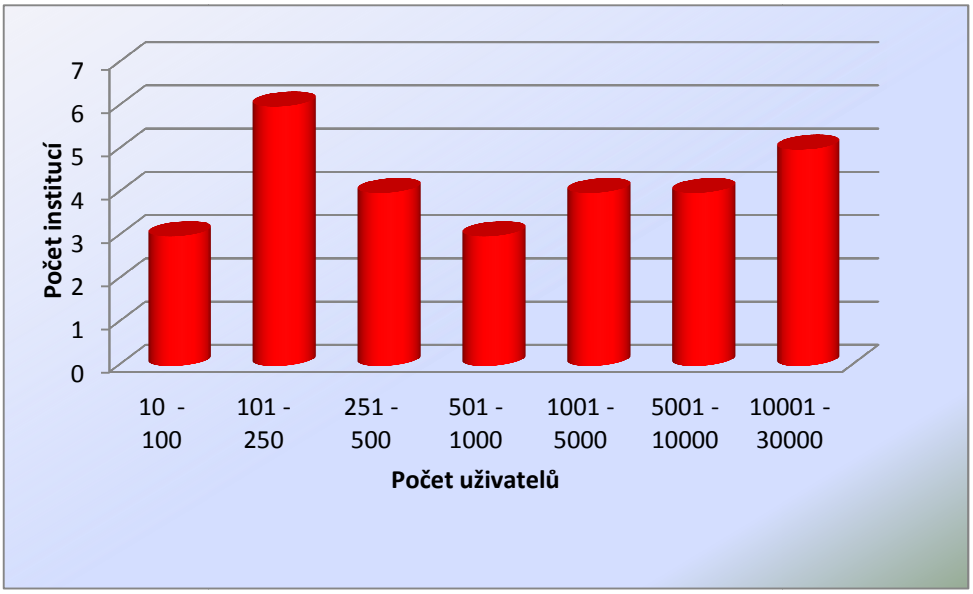
Nejčastěji se vyskytujícím systémem, ať už samostatně nebo v kombinaci s dalšími systémy je Aktion. Jedná se o produkt firmy EFG CZ spol. s.r.o. zahrnující kompletní sortiment prvků pro přístupové, docházkové a evidenční aplikace. Systém Aktion umožňuje realizovat rozsáhlá systémová řešení v oblasti identifikace a bezpečnosti od kontroly přístupů, evidence docházky, stravovacího systému, přístup k IT technologiím, až po ovládání externích zařízení.

Dalším typem je systém kontroly vstupu K4 od výrobce IMA s.r.o. Jedná se o sofistikovaný přístupový systém, jehož charakteristikou je vzdálená správa formou outsourcingu. Konkrétně to znamená, že systém spravuje pro zákazníka na dálku výrobce a v budovách je pouze příslušný HW. Výhodou je, že zákazníkovi zcela odpadá starost se správou systému a jeho servisem. Nevýhodou je pak nutnost komunikace s poskytovatelem služeb (IMA) při potřebě změn (zavedení nové karty, změny vlastností systému).

Třetí nejpoužívanější je systém ACS line od výrobce Estelar s.r.o. Nabízí ucelené řešení v oblastech evidence docházky, kontrola přístupu, objednávka a výdej stravy, evidence výroby, a další.

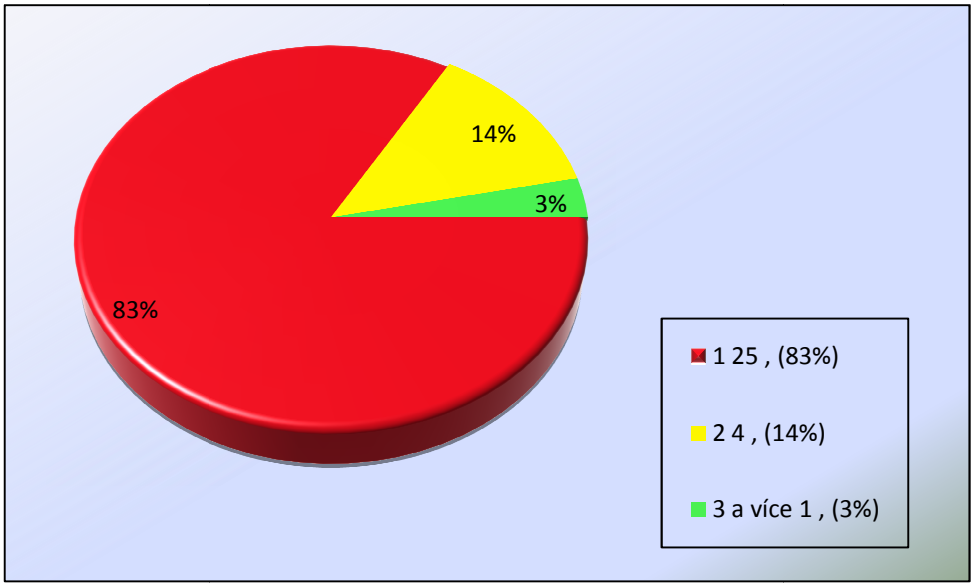
Systém Kompas firmy PC Help a.s., je řešení, které se uceleně zaměřuje na správu a řízení lidských zdrojů. Součástí systému jsou základní moduly, mezi které patří Personalistika, Vzdělávání a Mzdy, ale také ucelený systém docházky.

Graf 10: Kolik osob systém elektronické kontroly vstupu využívá?



Mezi respondenty tohoto průzkumu byli správci subjektů, mající na starosti správu od 30 uživatelů až po obrovské databáze spravující přístup pro 30000 uživatelů.

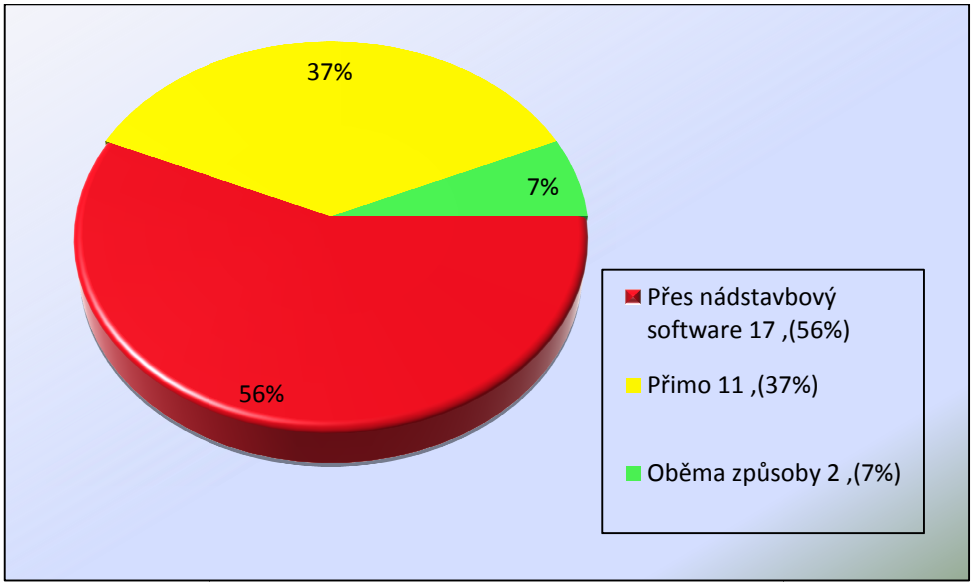
Graf 11: Kolik různých identifikátorů v rámci jednoho systému kontroly vstupu používáte?



Typ	Počet
Mifare	11
EM4102	3
HID	2
Neuveden typ	17

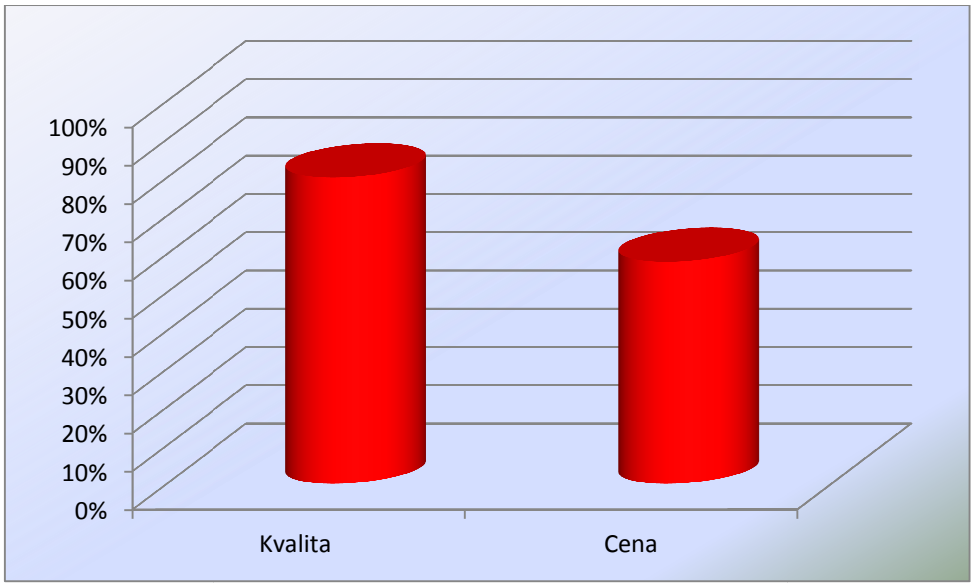
Tímto dotazem jsem měl na mysli, kolik různých typů karet, technologií a podobně zaměstnanci v dané firmě využívají. Téměř polovina respondentů uvedla pouze počet používaných identifikátorů, bez uvedení jeho typu. Ti, kteří typ uvedli, nejčastěji využívají čipu Mifare (11), naopak v dnešní době u nás nejpoužívanější EM4102 se používá pouze ve třech. Je škoda, že více než polovina oslovených neuvedla typ používané karty či identifikátoru. Na druhou stranu je třeba chápat určitou opatrnost správců při sdělování informací týkajících se zabezpečení vstupu do objektu. V některých firmách používají více typů identifikátorů proto se celkový počet v tabulce nerovná počtu vyhodnocených dotazníků.

Graf 12: Spravujete systém přímo nebo přes nadstavbový software?



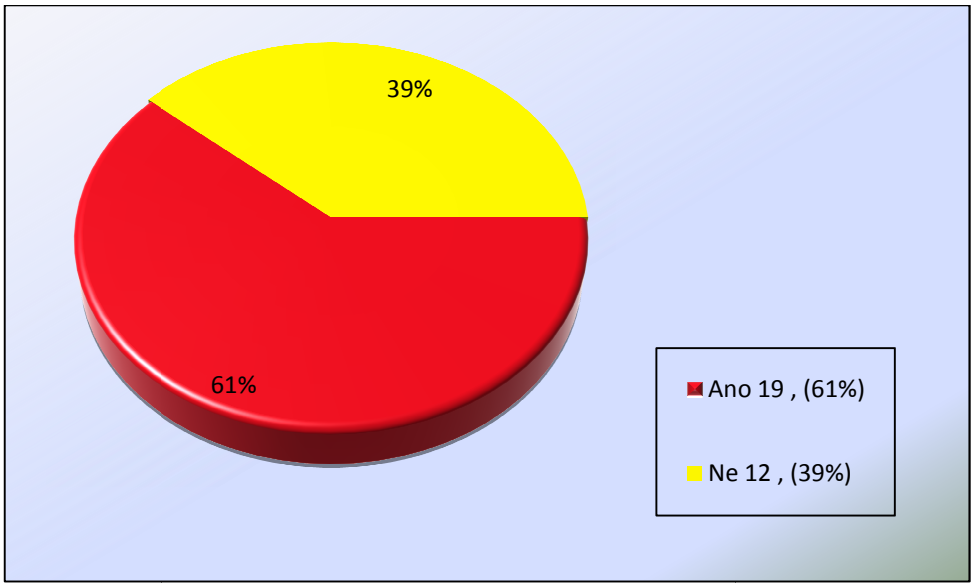
Průzkum dále ukázal, že z celkového počtu 31 odpovědí, spravuje systém EKV přes nadstavbový software 56%. Přímo spravuje systém 37% správců. U zbylých 7% je správa systému prováděna oběma způsoby, tedy jak přímo, tak přes nadstavbový software.

Graf 13: Jste spokojeni s kvalitou a cenou systému?



Dotazem týkajícím se spokojenosti s kvalitou a cenou systému se ukázalo, že 80% správců je s kvalitou spokojeno. S cenou je spokojena půlka, což je poměrně málo.

Graf 14: Víte o funkcích systému, které jste nikdy nevyužili?



V rámci průzkumu byla položena také otázka, zda existují funkce systému, které daný subjekt nevyužívá. Odpověď je překvapivá, 61% správců uvedlo, že jsou funkce, které nevyužívají. Zbylých 39% plně využívají systém EKV. Se zjištěním z předchozího dotazu (viz. Graf 13.) spokojenosti s cenou systému, se kterou je spokojena polovina dotazovaných, do jisté míry vyplívá proč tomu tak je. Dle mého názoru jsou tyto systémy pro daný subjekt neefektivní. To znamená, že obsahují funkce, které nejsou využívány a pochopitelně, systémy s větším rozsahem funkcí jsou také dražší. Nicméně, naprostá většina správců je spokojena s možnostmi systému EKV.

Poslední položená otázka zněla: *„O které funkcionality byste systém rádi rozšířili?“*

Z celkového počtu 31 správců, kteří se průzkumu zúčastnili, 19 nemá potřebu rozšíření, nebo neví, o jaké funkce by systém rozšířili. Ve zbylých případech by usnadnilo používání, a správci by rádi rozšířili systém EKV o následující funkce:

- Rozšíření dle potřeb a změn Zákoníku práce,
- Identifikace pohyb osob,
- Úprava kontrolních reportů pro kontrolu mzdové nadstavby,
- Speciální funkcionality související se specifickými požadavky na zaokrouhlování dat a způsobem výpočtu nároků jednotlivých uživatelů na stravenky,
- Mobilní zařízení pro rozpoznávání osob - zejména v souvislosti s BOZP,

- Přístup do jednotlivých provozů firmy,
- Uživatelská tlačítka pro otevírání jednotlivých vstupů,
- Tisk směnovnic,
- Převod dat do mzdového systému,
- Zjednodušený výpis příchodů a odchodů vybrané skupiny pracovníků (tiskové sestavy).

7 NÁVRHY OPTIMÁLNÍHO SYSTÉMU KONTROLY VSTUPU

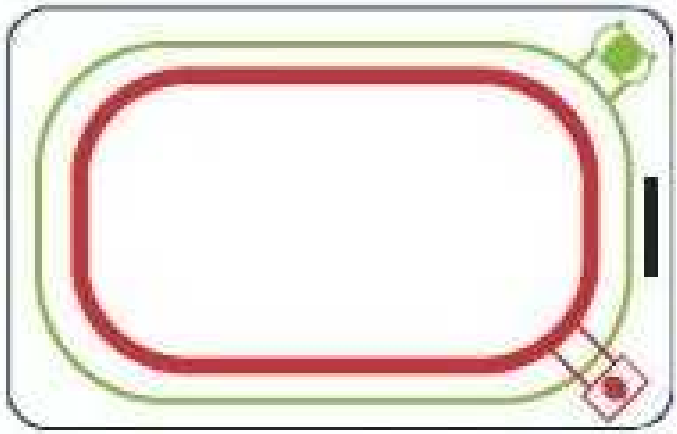
Na základě průzkumu byly zjištěny funkcionality a vylepšení, které by běžní uživatelé a správci systémů elektronické kontroly vstupu uvítali. Tyto informace poslouží jako vstupní data pro návrh systému EKV. Cílem navrhnutého systému je zajištění bezpečného, průkazného, spolehlivého a uživatelsky pohodlného vstupu a pohybu osob v prostorách zabezpečeného objektu. Systém bude využívat k autentizaci uživatelů bezkontaktní karty a čtečky karet, instalované u vstupů do objektů, případně jiných dveří, u kterých je vyžadována kontrola pohybu osob. Výstupy systému budou směřovány na centrální administrátorské stanoviště. Odtud bude prováděn monitoring systému EKV, správa a diagnostika systému.

Technické řešení a použité komponenty:

7.1 Bezkontaktní karty

Identifikace osob pohybujících se po objektu je realizována prostřednictvím přidělených bezkontaktních karet. Každé kartě je možné přidělit přístupová oprávnění, tzn. definovat prostory a časová okna, kdy je uživateli umožněn vstup. Zařazením karty do příslušné přístupové skupiny dojde k aplikaci skupinových nastavení na konkrétní kartu. Nejdůležitějšími aspekty při volbě karty je její životnost a kvalita. Průzkumem bylo zjištěno, že většina uživatelů používá běžně dva a více identifikačních předmětů. Dále by pak většina uvítala sjednocení pod jednu kartu. Na základě získaných informací, s cílem zvýšení uživatelského komfortu volím bezkontaktní kartu kombinující dvě technologie.

Vybral jsem produkt *HID iCLASS 2020 Prox*. Jedná se o bezkontaktní duální kartu o velikosti paměti 2Kb s 2 aplikačními oblastmi, podporující normu ISO 15693. Karta iCLASS Prox kombinuje iCLASS (13,56 MHz) a HID 125 kHz Prox technologii v jedné kartě standardní tloušťky. Tato technologie zajišťuje vysokou bezpečnost s vzájemnou autentizací mezi kartou a čtečkou, šifrovaný přenos dat, a 64bit generované klíče pro čtení a zápis. Karta je tenká, pružná, vyrobena z polyvinyl chloridu (PVC). Cena takovéto karty se pohybuje kolem cca 260 Kč za kus, při nákupu 100 kusů. Na následujícím obrázku je vidět řešení karty, červenou barvou je znázorněn transpondér 125 kHz, zelenou pak 13,56 MHz.[16]



Obrázek 18: Bezkontaktní duální karta *HID iCLASS 2020 Prox*

7.2 Čtečka bezkontaktních karet

Hlavním úkolem čtečky je správně, kvalitně a co nejrychleji dekódovat data přijaté, v našem případě z duální bezkontaktní karty *HID iCLASS 2020*. Uživatelským průzkumem bylo zjištěno, že největším přínosem pro používání systému EKV je zvýšení čtecí vzdálenosti. Požadavek na vyšší čtecí vzdálenost je tedy směrodatný pro výběr čtečky. Bezkontaktních čteček pro systémy EKV s dosahem nad 15 cm není v dnešní době na trhu mnoho. Pochopitelně taková čtečka má vyšší pořizovací náklady, nicméně jedná se o systém, který si klade za cíl zvýšení uživatelského komfortu. Tudíž finanční stránka není na prvním místě.

Pro můj návrh jsem zvolil produkt výrobce *HID, typ iCLASS R90*. Jedná se o čtečku bezkontaktních karet s dlouhým dosahem. Má robustní, atraktivní provedení a instalace této čtečky je poměrně snadná. Čtečka pracuje na frekvenci 13.56 MHz, a podporuje identifikační karty a čipy iCLASS (ISO 15693). Dosah pro typ navržené karty je cca. půl metru, přičemž přenos dat mezi kartou a čtečkou je šifrovaný. Čtečka dále poskytuje vyšší stupeň zabezpečení díky posílenému kódování, které obstarávají vysoce bezpečné 64bitové diverzifikované klíče pro vzájemné ověřování. Tato čtečka je vhodná pro použití jak v interiéru, tak v exteriéru. Cena čtečky se v dnešní době pohybuje kolem 18000 Kč.

Další technické parametry:

Tabulka 9: Technické parametry čtečky *HID iCLASS R90*

Rozměry:	30.5 x 30.5 x 3 cm
Hmotnost:	283,5 g
Čtecí vzdálenost:	45 cm
Spotřeba:	420 mA, max. 1300 mA při 12 V DC
	210 mA, max. 700 mA při 24 V DC
Provozní teplota:	-30 až +65°C
Provozní vlhkost:	5 až 95% bez kondenzace
Rozhraní:	Wiegand
LED dioda:	3stavová (volitelně)
Barva krytu:	černá
Technologie:	iCLASS, DESFIRE, MIFARE

Obrázek 19: Čtečka HID iCLASS R90

7.3 Dveřní jednotka

Dveřní jednotky jsou zařízení ovládající elektromechanické a elektrické dveřní zámky a otvírače přístupových míst. Přijímají data z bezkontaktních čteček, které dále předávají do řídící jednotky, která se rozhodne o přístupu. Zpravidla se přístupové jednotky montují v co nejkratší vzdálenosti od čtečky, aby byla transakce povolení vstupu vyřízena co nejrychleji. Zvolil jsem dveřní jednotku *e-DATA TLC 200 DU*. Jednotka obsahuje určité

kontakty pro její ovládání, mezi tyto patří kontakt pro dveřní tlačítko, dveřní rám, otvírače dveří nebo pohybové čidlo, sabotážní spínač, stavové LED diody a kontakt pro zaseknuté dveře. Cena této přístupové jednotky je 8400 Kč.

Použitá dveřní jednotka podporuje všechny standardní typy čteček karet:

- HID bezkontaktní,
- HID iCLASS,
- Legic,
- Mifare,
- EM,
- ISO 15693 / 14433.

Ke dveřní jednotce je možno připojit dvě čtečky, to znamená ovládání dvou jednostranných vstupů nebo jednoho oboustranného vstupu. Komunikace mezi čtečkou a danou dveřní jednotkou probíhá přes rozhraní wiegand (max. 150 m).

Další specifické vlastnosti:

Tabulka 10: Vlastnosti dveřní jednotky *TLC 200 DU* [14]

Rozhraní:	Data čtečky:	1 x RS485 (max. 1400m)
		2 x RS232 (max. 25m)
		2 x Wiegand (max. 150m)
	Řízení:	RS485
	Vstupy/Výstupy:	5 x výstupů, 2 x relé, 2 x rozhraní snímačů
Napájení:	10 až 28V DC / 120mA	
Hmotnost:	cca. 300 g	
Provozní teplota:	-10°C až 60°C	
Relativní vlhkost:	0 až 95% , nekondenzující	
Rozměry:	120 x 120 x 40 mm	

7.4 Řídící jednotka

Řídící jednotka tvoří jádro celého systému EKV. Rozhoduje o povolení či zamítnutí vstupu do zabezpečeného objektu. Použil jsem řídící jednotku *TLC 200.24 MU*. Obsahuje zabudovanou aplikaci pro kontrolu vstupu, správu systému, uživatelské nastavení a hlášení událostí. Ovládání je přístupné přes 10/100 Mbps síť Ethernet prostřednictvím libovolného standardního webového prohlížeče. K modulu řídící jednotky *TLC 200.24 MU* je možno připojit až 12 dveřních jednotek *TLC 200 DU*, z nichž každá umožňuje připojení 2 čteček, což je celkem až 24 bezkontaktních čteček Řídící jednotky je možno spojit do skupin a určit jednu hlavní řídící jednotku a tak centrálně řídit stovky čteček (dveří). Je to mikroprocesorem řízená jednotka, která uvnitř obsazena pamětí pro uložení přístupových práv a jednotlivých naprogramovaných funkcí v autonomním režimu. Tato jednotka obsahuje paměť typu CompactFlash o velikosti 2 GB. Procesor je taktován na frekvenci 600 MHz, paměť RAM je velikosti 128 MB. [15]

Komunikace mezi dveřními jednotkami a řídící jednotkou probíhá přes rozhraní RS 485. Napájení, rozměry a provozní podmínky jsou totožné jako u použité dveřní jednotky (jedná se o produkty jednoho výrobce). Cena jednotky se pohybuje kolem 14 000 Kč.

Vlastnosti řídící jednotky:

- Modulární provedení (1 až 24 čteček),
- Připojení přes 10/100 Mbps Ethernet,
- Vestavěný web server,
- Funkční ihned po připojení (UPnP),
- Vestavěná aplikace pro kontrolu vstupu,
- GSM Modem / GPRS Class 10 / Dual band Class 1 & 2 SMS
- Analogový Modem RJ11 Port
- Rozhraní USB
- Programovatelný SOAP (SOAP = protokol pro posílání zpráv XML a je základem webových služeb),
- 2 kanálový RS485
- 3x vstup (sabotáž, slabé baterie, chyba AC napájení), 1x výstup (poplach)
- Administrace přes standardní web prohlížeč,
- Kapacita 5000 uživatelů / 15000 událostí.

Obrázek 20: Dveřní jednotka *TLC 200 DU* a řídící jednotka *TLC 200.24 MU* [15]

7.5 Napájení a záložní zdroje

Systém EKV je v normálním provozním režimu napájen ze síťového rozvodu 230V/50 Hz. K zajištění napájení zařízení jsou využity vlastní zdroje. V závislosti na počtu instalovaných přístupových jednotek a čteček se pak připojí určitý počet zdrojů. Pro napájení navrhují kompletní lineární zálohované napájecí zdroje napětí 13,8V, *typu KPN-18-30LAW*. V případě výpadku sítě je pak každý zdroj vybaven vlastním záložním zdrojem 12V DC (olověný bezúdržbový akumulátor s kapacitou 18 Ah). Přechod napájení na záložní napájení z akumulátoru je zajištěn automaticky, bez rušivého vlivu na funkci zařízení.

Technické parametry zálohovaného zdroje:

Tabulka 11: Parametry zdroje

Jmenovité vstupní napětí:	230V AC / 50 Hz
Výstupní napětí:	13.8V DC
Max. výstupní proud:	3A
Proudové omezení:	3A
Pojistka výstupního napětí:	4A/T
Síťová pojistka:	400mA/T
Opětovné dobití akumulátoru:	za 24hod (pro aku 18Ah)
Rozsah provozní teploty:	-20 až +30° C
Rozměry (š x v x h) :	125 x 260 x 400 mm

7.6 Zapisovací čtečka

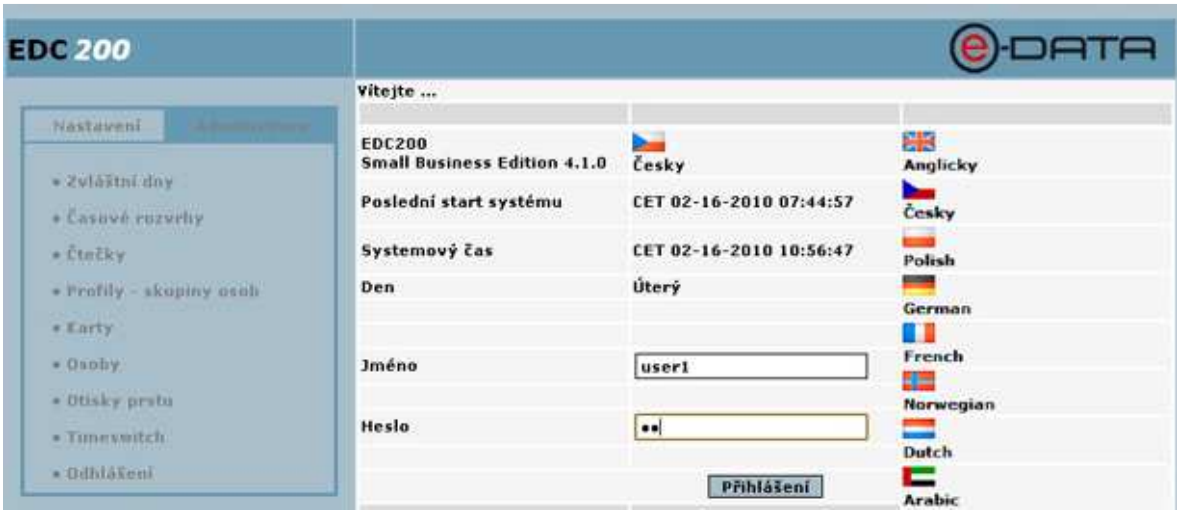
Jde o čtečku, pomocí které se upravují karty pro osoby mající pověření ke vstupu do objektu. Pro můj návrh jsem zvolil *AIR ID iCLASS*. Jedná se o čtecí a zapisovací zařízení nejpoužívanějších typů karet, tedy i pro čipy výrobce HID. Čtečka umožňuje připojení k PC přes USB. Pracuje na frekvenci 13,56 kHz, čtení a zápis provádí do vzdálenosti 20mm.

7.7 Komunikace a kabelové provedení

Komunikace mezi řídící jednotkou a dveřními jednotkami probíhá pomocí komunikačního rozhraní RS 485 (kabel *Belden 8723*). Mezi bezkontaktními čtečkami a dveřními jednotkami přes komunikační rozhraní Wiegand (kabel *FI-HX08/02*). Dále pak komunikuje řídící jednotka s PC, ze kterého se provádí správa pomocí protokolu TCP/IP (kabel *UTP cat. 5e*). Pro rozvody napájení 12V DC od zdrojů bude použit flexibilní kabel *HO5VV-F 2x2,5*. Takto navrhnutý systém EKV neobsahuje žádné externí převodníky, je tedy využito komunikačních vstupů a výstupů zahrnutých v jednotlivých prvcích.

7.8 Správa systému

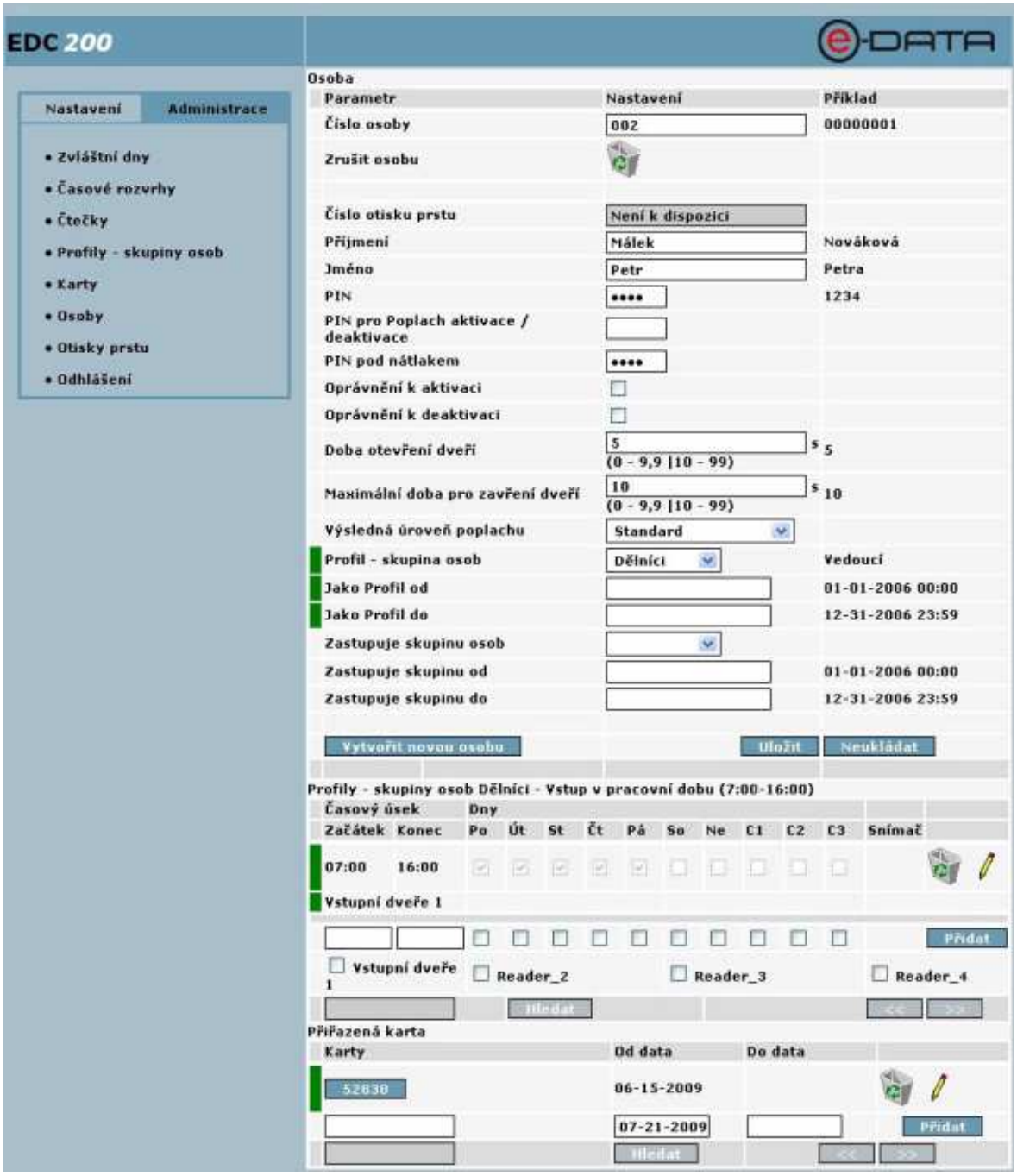
Takto navržený systém EKV obsahuje zabudovanou aplikaci pro kontrolu, správu, uživatelské nastavení a hlášení událostí. Tato aplikace pracuje na platformě JAVA a je přístupná přes jakýkoliv webový prohlížeč po napsání příslušné IP adresy řídící jednotky do adresného řádku prohlížeče a následném přihlášení k aplikaci. Případně je možné přihlášení přes průzkumník Windows, kde je potřeba v menu síťová připojení vybrat příslušnou řídící jednotku. Velkou výhodou je snadné připojení ze vzdáleného místa pomocí internetu a spravovat tak systém prakticky odkudkoliv. V aplikaci se nastaví časy a místa, kam mají jednotlivé osoby, nebo skupiny osob přístup. Záznamy o všech vstupech a výstupech z objektů jsou ukládány do databáze. Poté je možno kdykoliv zobrazit přehled o tom, která osoba kdy v kolik hodin a kam vstoupila. Dále je možno zobrazit pokusy o nepovolené vstupy do objektu, počet osob v objektu a další události. Pro další použití uložených vstupních dat, je umožněn jejich tisk či převod k dalšímu zpracování. Prostředí správy systému je zobrazeno následujícími obrázky.



Obrázek 21: Přihlášení do systému pro správu [17]

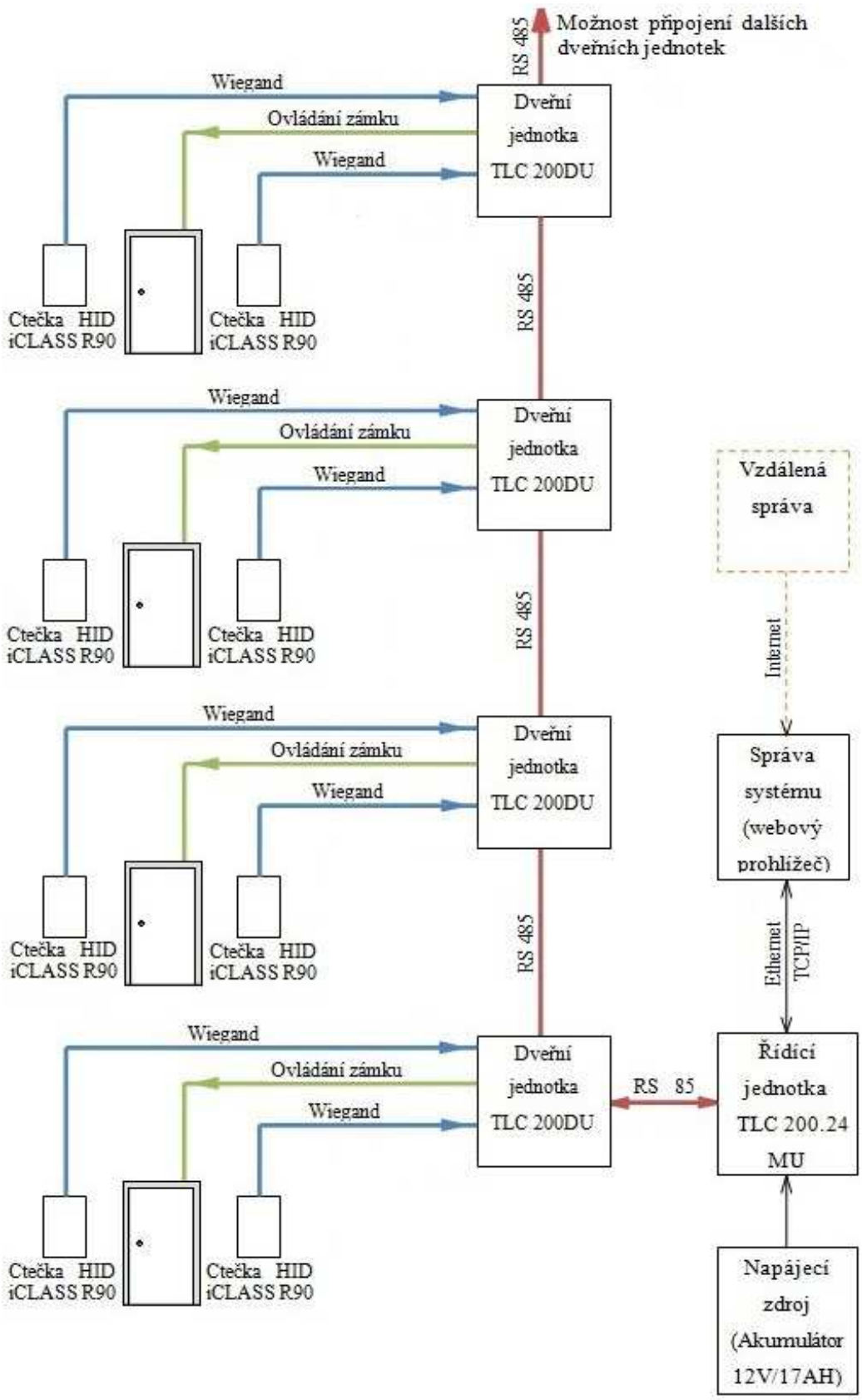
Obrázek 22: Nastavování skupin uživatelů [17]

Obrázek 23: Aktivace/Deaktivace karet [17]



Obrázek 24: Nastavené oprávnění vstupu jednotlivých osob [17]

7.9 Schéma a konfigurace systému



Obrázek 25: Schéma navrhovaného systému

Bezkontaktní čtečky *HID iCLASS R90* jsou osazeny jak u vstupu, tak u výstupu. Je to z důvodu sledování úplného pohybu osob po objektu tj. příchody i odchody. Dalším přínosem tohoto řešení je zavedení funkce antipassback, která brání opakovaným vstupům na jednu kartu. To že zabezpečení do objektu je podmíněno použitím přístupového prvku, zařazuje tento systém EKV do třídy identifikace 2, třída přístupu je potom typu B. Dalším přínosem systému je přístup do všech zpřístupněných místností či objektů pomocí jedné karty. Každá osoba s oprávněním ke vstupu do objektu obdrží duální bezkontaktní kartu *HID iCLASS 2020.* Autentizace probíhá technologií iCLASS (13,56 MHz), uživatel má možnost využívat kartu i v jiných oblastech. K tomu slouží možnost nahrání dalšího kódu na čip 13,56 MHz pomocí kompatibilní USB zapisovací čtečky *AIR ID iCLASS* , případně využívat kód čipu 125 kHz, který slouží pouze ke čtení. Další výhodou použití této karty je možnost aplikace jiných typů kompatibilních bezkontaktních čteček, v případě rozšiřování o další místnosti či objekty. Jako ovládaná zařízení pro tento systém kontroly vstupu poslouží jakékoliv elektrické a elektromechanické zámky nebo otvírače či turnikety. Všechny navržené komponenty v rámci daného systému EKV vyhovují zákonu 22/97 Sb. (Zákon o technických požadavcích na výrobky) a prováděcím předpisům (nařízením vlády).

Při vstupu do objektu přiblíží uživatel kartu do blízkosti čtečky, nejdále ovšem půl metru od ní. Systém vyhodnotí přístupová práva, otevře dveře a zaeviduje datum a čas vstupu. V případě, že přístupová práva nesouhlasí, osoba se snaží vstoupit např. mimo pracovní dobu, nebo do míst kam nemá přístup, tak systém zaeviduje datum a čas přiložení karty, ale dveře neotevře. Systém dále monitoruje stav dveří. Jejich případné nezavření do určité doby, nebo násilné otevření vyvolá v nastaveném intervalu poplach. Tím že řídící jednotka zahrnuje aplikaci pro správu systému EKV, odpadá investice do dalšího SW.

Navržený systém EKV doporučuji pro zabezpečení menšího, případně středního objektu. Co se týká rozšíření, tak největší přínos bych viděl v umístění kamer nad čtečky umístěné v klíčových místech objektu. Hlavním důvodem tohoto řešení potom bude při neoprávněném pokusu o vstup, zjištění kdo takovou činnost provádí, případně zaznamenání činnosti osoby spojené s pokusem o vyřazení systému z provozu, nebo jiné narušení systému EKV.

8 BUDOUCNOST SYSTÉMŮ EKV

Směr, kterým se bude tato problematika v blízké budoucnosti ubírat, není lehké předpovídat. Nicméně kromě neustálého růstu ve vývoji novějších technologií v oboru informatiky, hardware, software a počítačového odvětví vůbec bych viděl budoucnost v expanzi biometrických systémů. Nesprávná osoba na nesprávném místě může v dnešní době elektronicky ovládaného světa způsobit mnoho škod. Biometrické systémy nabízejí nejkvalitnější způsob identifikace osob. A právě tato oblast identifikace podléhá v dnešní době vyšší míře vědecké činnosti při zkoumání ať už nových technologií identifikace, nebo neustálému vylepšování již stávajících a používaných metod. Biometrie zaznamenala v posledních letech velký nárůst možností. Ačkoliv neprožívá asi tak velký boom, jak se předpokládalo, je třeba vzít v úvahu, že toho má biometrie ještě hodně před sebou. Její největší výhodou bezesporu zůstane nepřenositelnost identifikačního prvku, kterým je v tomto případě sám člověk. Předpokládá se, že technologie otisků prstů si nadále udrží největší podíl na trhu z důvodů aktuálně nejlepšího poměru mezi náklady, spolehlivostí a optimálností pro uživatele. Využití ostatních typů biometrie určitě poroste s klesajícími pořizovacími náklady, zlepšováním technologií a z toho vyplývajícím nárůstem poptávky. Účelem biometrie v budoucnu nebude jenom chránit náš majetek a bezpečnost, ale také urychlit a usnadnit ověřování osobní identity tam kde je to velmi často zapotřebí. Pomineme-li v některých případech vyšší pořizovací náklady je biometrická identifikace bezpečnostní technologií naší blízké budoucnosti, respektive také již současností, neboť výzkum a vývoj v tomto odvětví jde velmi rychle kupředu. Za zmínku určitě stojí rozpoznání na základě rekognice, tedy znovupoznání. Při identifikaci se pak uživateli žádajícímu o přístup zobrazí např. osobní fotografie, kterou předtím na server uložil, mezi množstvím jiných (náhodných) fotografií, přičemž uživatel musí zvolit tu správnou. Stejně tak se ale najdou útočníci, kteří se budou snažit biometrii různými způsoby obelstít. Proto je potřeba neustále tyto technologie modernizovat a vylepšovat. Stále nejefektivnější ale určitě bude vícefaktorová identifikace, kombinující více biometrických metod.

Integrace do celkového systému zabezpečení objektu již není žádná novinka. Nic méně i zde bych viděl možnost určitého dalšího vývoje. Potenciál bych viděl hlavně ve vývoji a zdokonalování software, který by sbíral a poskytoval informace o celkovém stavu objektu, a byla tak možnost řídit rizika z jediného počítače.

Dalším možným způsobem, který může ovlivnit budoucnost elektronické kontroly vstupu je technologie NFC (Near Field Communication). Jedná se o technologii určenou pro bezdrátový přenos dat na krátké vzdálenosti. Ta by neměla dle standardu ISO 13157 přesáhnout vzdálenost 20 cm. Přenos dat probíhá na frekvenci 13,56 MHz pomocí elektromagnetické indukce. Jelikož je NFC odvozena od standardu určené například pro platební karty, předpokládá se její využití především v mobilních zařízeních všeho druhu. Již dnes je možné otevírat mobilním telefonem vstupní dveře. V České republice je tento systém zatím v testování. Předpokládá se kromě využití v přístupových systémech taky placení účtů v obchodech, jídelnách, apod. Nutno dodat že smart phonů, které tuto technologii ovládá ještě moc není, nicméně se neustále připravuje stále více modelů.

Oblast komunikace je další oblastí, která se s přibývajícím časem rozvíjí. Mezi přístupovými systémy se často začíná využívat IP technologie, která umožňuje prakticky neomezené použití systémových prvků. V tomto případě se jedná hlavně o čtečky a kontroléry. Počet připojených prvků, by pak mohl být omezen dostupným volným počtem IP adres v síti. To už ale v dnešní době vyřeší IP protokol verze 6. Velkou výhodou tohoto řešení je použití stávajících ethernetových sítí a možnost napájení prvků přes síť (PoE). Pro systémy EKV spravující několik rozsáhlých objektů, dejme tomu i na úrovni několika měst, by určitě byl přínos nasazení optických kabelů. Aplikováním optických kabelů lze značně prodloužit kabeláž, prakticky bez omezení rychlosti přenosu dat.

Na závěr je třeba ještě vzpomenout problém odcizení identity, který postihuje stále více osob užívajících přístup do určitých prostor či systémů. Nepovolaná osoba, jak již sem naznačil, totiž může napáchat v zabezpečeném objektu značné škody. Proto je potřeba v objektech uchovávajících aktiva vyšší hodnoty či jiné cennosti, jejíž ztráta by způsobila určitou újmu, používat vyšší stupeň zabezpečení v podobě vícefaktorové identifikace.

ZÁVĚR

Systémy elektronické kontroly vstupu, kolem kterých se celá tato práce točí, jsou velmi perspektivní záležitostí. S těmito systémy se většina z nás setkává v běžném životě velmi často. Kontrola vstupu do objektu a ven z něj, by měla byt jedním ze základních kamenů bezpečnostní politiky každého podniku. Schopnosti dnešních systémů EKV dávno přerostly ty, kterými disponovaly jedny z prvních systémů. V dnešní době, kdy je na trhu vysoká konkurence přístupových a identifikačních systémů založených na různých principech, je zapotřebí vybrat ten nejvhodnější pro daný objekt, jak za účelem kontroly vstupů, tak kontroly docházky uživatele. Moderní počítačem řízená kontrola vstupu a monitorovací systém umožňuje realizovat kontrolu pohybu a monitoring v širokém rozsahu. Požadavky na tyto systémy určuje norma ČSN EN 50 133 - *Všeobecné požadavky na systémy kontroly vstupů pro použití v bezpečnostních aplikacích*. Stále častěji se pak využívá integrace systémů EKV do celkového systému objektů.

V teoretické části této práce jsem se zabýval principem funkčnosti, strukturou a požadavky kladenými na systémy EKV. Dále jsou rozebrány způsoby identifikace osob, mezi které v oblasti řešené problematiky spadá magnetický, optický, kontaktní a bezkontaktní systém. Speciální disciplínou identifikace je biometrika, kterou se až na identifikaci podle otisků prstů v práci zabývám jen obecně. Poslední oblastí rozebranou v teoretické části jsou autentizační metody pro přístup do objektů zabezpečených systémem EKV.

V praktické části je provedena analýza průzkumu trhnu, pro niž jsem zvolil dotazníkovou metodu. Průzkumy byly provedeny jak mezi běžnými uživateli, tak správci systémů EKV. Vyhodnocením výsledků průzkumů byly získány vstupní data pro tvorbu návrhu systému EKV, který by zvýšil komfort používání. Velkým přínosem navrženého systému EKV je použití duální bezkontaktní karty, kombinující technologii 13,56 MHz (přepisovatelná) a technologii 125 kHz (pouze pro čtení). Danou kartu je tak možno použít pro velké množství aplikací a čteček. Vzhledem k požadavku na vyšší čtecí vzdálenost, a následným zařazením takového zařízení do návrhu, bych viděl tento aspekt z hlediska uživatelského komfortu jako klíčový. Navržený systém bych doporučil pro menší až střední objekty. Závěr práce je věnován blízké budoucnosti systémů EKV.

ZÁVĚR V ANGLIČTINĚ

Access control systems, around which revolve all this work are very promising business. With these systems, most of us encounter in everyday life very often. Access control to the building and out of it, should be one of the cornerstones of the security policies of each company. ACS systems capabilities of today's long outgrown those which possess one of the first systems. Nowadays, when the high competition in the market access and identification systems based on different principles, it is necessary to choose the most appropriate for the object, how to control inputs and user attendance. Modern computer-controlled access control and monitoring system allows you to implement motion control and monitoring in a wide range. The requirements for these systems determines the standard EN 50133 - General requirements for access control systems for use in security applications. Increasingly, the ACS uses a systems integration into the overall system objects.

In the theoretical part of this work, I dealt with the principle of functionality, structure and the demand for ACS systems. Are also discussed ways of identifying the persons to have solved the problem of falling magnetic, optical, contact and contactless systems. Special discipline identification is biometrics, which is to identify the fingerprints of the work deal only in general. The last area discussed in theoretical part of the authentication methods for access to secure objects ACS system.

In the practical part is an analysis of survey jerks, which I chose for the questionnaire method. Surveys were conducted among regular users and administrators EKV. By evaluating the survey results were obtained input data for the creation of ACS system design, which would increase the comfort of use. A major benefit of the proposed system is to use the ACCESS dual contactless cards, combining technology, 13.56 MHz (rewritable) and 125 kHz technology (read only). So the card can be used for many applications and readers. Due to the demand for higher read range, and the subsequent inclusion of such equipment in the draft, I saw this aspect in terms of user-friendliness as a key. The proposed system would recommend for small to medium objects. The conclusion is devoted to the near future of ACS.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK, Stanislav.a Kol. *Příručka zabezpečovací techniky*. Cricetus, 2006, 313 s. ISBN 80-902938-4.

[2] LAUCKÝ, JUDR., Vladimír. *Technologie komerční bezpečnosti II*. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.

[3] LAUCKÝ, JUDR., Vladimír. *Technologie komerční bezpečnosti I*. Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-119-3.

[4] KINDL, Jiří. *Projektování bezpečnostních systémů I*. UTB Zlín, 2004. ISBN 80-7318-165-7.

[5] ČERNÝ, JUDR., Josef, IVANKA, ING., Ján a A KOL. *Systemizace bezpečnostního průmyslu I*. Univerzita Tomáše Bati ve Zlíně, 2006, 135 s. ISBN 80-7318-402-8.

[6] SUCHÁČEK, Lukáš. *Systémy kontroly vstupu pro komerční objekty*. Zlín, 2010. Bakalářská práce. UTB Zlín.

[7] ČSN EN 50133-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky*. Březen 2001, s. 28.

[8] ŠČUREK.MGR. ING., Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*: *Studijní text*[online]. VŠB TU Ostrava, 2008, 58 s. [cit. 2012-04-04]. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf

[9] *Security magazín č.92*.(listopad/prosinec 2009) Praha 1 : Family media. 12 s.

ISSN 1210-8723.

[10] SKOUMAL, Miroslav. *Identifikace člověka pomocí biometrických údajů*. Univerzita Jana Evangelisty Purkyně v Ústí nad Labem, 2007. Bakalářská práce.

[11] ROSOL, Ivo. Moderní docházkové systémy. [online]. IT SYSTEMS 12/2011[cit. 2012-03-15]. Dostupné z: http://www.systemonline.cz/hrm-personalistika/moderni-dochazkove-systemy.htm.

[12] KRHOVJÁK, Jan, MATYÁŠ Václav. *Autentizace a identifikace uživatelů*. Zpravodaj ÚVT MU. ISSN 1212-0901. 2007, roč. XVIII, č. 1, s. 1-5.

[13] Identifikační systémy ID-karta. [online]. [cit. 2012-04-20]. Dostupné z: http://www.id-karta.cz/identifikace-3/cipy-20/

[14] *Timelink* [online]. 2012 [cit. 2012-05-03]. *TLC 200 DU - Dveřní jednotka pro 2 čtečky*. Dostupné z WWW: <http://www.timelink.cz/products/tlc-200-du-dverni-jednotka/>.

[15] *Timelink* [online]. 2012 [cit. 2012-05-03]. *TLC 200.24 MU - Řídíci jednotka pro 1 až 24 dveří.* Dostupné z WWW: <http://www.timelink.cz/products/tlc-400-mu-ridici-jednotka-timelink/>.

[16] *Sovte* [online]. 2012 [cit. 2012-05-03]. *2020 ICLASS PROX CONTACLESS SMARTCARD.* Dostupné z WWW: < http://www.sovte.cz/cipove-karty.php/>.

[17] *Timelink* [online]. 2012 [cit. 2012-05-03]. *Elektronická kontrola vstupu.* Dostupné z WWW: <*http://www.timelink.cz/pristupove-systemy*/>.

[18] *ADIGlobal*[online]. 2012 [cit. 2012-04-06]. *Kontaktní Dallas čip.* Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/w/45289ADE9D8B5BB3C125735900628A82?OpenDocument />.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKV	Elektronická kontrola vstupu
LAN	Místní síť
Wifi	Bezdrátová síť
CCTV	Systém, uzavřený kamerový televizní okruh (Closed Circuit Television)
PZS	Poplachové zabezpečovací systémy
RS 232	Standard definující komunikační rozhraní
RS 485	Standard definující komunikační rozhraní
TCP/IP	Protokoly pro komunikaci v síti
PC	Počítač
PIN	Osobní identifikační číslo
RFID	Rádio frekvenční identifikace
USB	Univerzální sériový port
LED	Luminiscenční dioda
UTP	Nestíněná kroucená dvojlinka
PoE	Napájení přes Ethernet
CCD	Charge-Coupled Device
HID	Název společnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA I: DOTAZNÍK UŽIVATELSKÉ SPOKOJENOSTI

1. **Používáte systémy elektronické kontroly vstupu pravidelně?**
   - Ano
   - Ne
   - Občas

2. **Jak se prokazujete při identifikaci?**
   - Karta/přívěsek
   - PIN
   - Karta/přívěsek+PIN
   - Biometrický údaj (otisk prstu, snímání obličeje…)
   - Jinak – jak? ……

3. **Je podle Vás ovládání elektronické kontroly vstupu intuitivní a pohodlné?**
   - Ano
   - Ne (můžete uvést, co se Vám nelíbí do pole Jiná odpověď)

4. **Používáte identifikační kartu/předmět pro ovládání jiných zařízení (kopírka, výtah, stravování…)?**
   - Ano (můžete uvést jaké do pole Jiná odpověď)
   - Ne

5. **Slouží systém který používáte, také k evidenci docházky?**
   - Ano
   - Ne
   - Nevím

6. **Stalo se, že se Vám identifikační karta/předmět ztratil nebo byl odcizen?**
   - Ano
   - Ne

7. **Stalo se, že se Vám identifikační karta/předmět zničil?**
    - Ano (můžete uvést jak do pole Jiná odpověď)
    - Ne

8. **Používání jakého identifikátoru je podle Vás nejkomfortnější a nejpohodlnější?**
    - Karta
    - Biometrický údaj (prst, obličej …)
    - Přívěsek
    - PIN

9. **Kolik různých identifikátorů využíváte (např. v práci, doma, na bazénu, v obchodě,na parkovišti, přihlášení v PC...)?**
    - 1, 2, 3, 4, 5

10. **Myslíte si, že by bylo vhodné jeden identifikátor používat na více různých místech (například v práci i doma apod.)?**
    - Ano (můžete rozvést svoji myšlenku do pole Jiná odpověď)
    - Ne

11. **Měli jste nějaké problémy při používání systému?**
    - Ano (můžete uvést jaké do pole Jiná odpověď)
    - Ne

12. **Napadá Vás nějaká funkce, která by usnadnila používání systému?**
    - Ne
    - Jiná odpověď ……

PŘÍLOHA II: DOTAZNÍK SPOKOJENOSTI SE SPRÁVOU SYSTÉMU

Na otázky respondenti odpovídali vlastními slovy.

1. **Jaký typ systému používáte?**

2. **Kolik osob systém elektronické kontroly vstupu využívá?**

3. **Kolik různých identifikátorů v rámci jednoho systému kontroly vstupu používáte (Mám na mysli různé typy karet, technologií apod (HID, Mifare, 125kHz, 13.56Mhz, iCLASS, DESFire...))?**

4. **Spravujete systém přímo nebo přes nadstavbový software?**

5. **Jste spokojeni s možnostmi systému (definování přístupových práv, časová okna, antipassback, evidence docházky…)?**

6. **Jste spokojeni s kvalitou a cenou systému?**

7. **Víte o funkcích systému, které jste nikdy nevyužili?**

8. **O které funkcionality byste systém rádi rozšířili?**