Přístupové a docházkové systémy – úprava systému v laboratoři pokročilých bezpečnostních technologií na UTB ve Zlíně

Access and attendance systems - treatment system in the laboratory of advanced security technology TBU in Zlín

Lukáš Kolůch

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš KOLŮCH**
Osobní číslo:	**A08123**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Přístupové a docházkové systémy – úprava systému v laboratoři pokročilých bezpečnostních technologií na UTB ve Zlíně**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na přístupové a docházkové systémy.**
2. **V rámci rešerše se zaměřte na klasické a biometrické systémy.**
3. **Realizujte komunikaci mezi čtečkou a systémem WinPack.**
4. **Realizujte připojení Time Station terminálů k PC a jejich propojení s docházkovým systémem.**
5. **Vytvořte souhrnnou dokumentaci k vytvořenému pracovišti biometrických systémů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAIN, Anil K.; LI, Stan Z. . Encyclopedia of Biometrics. 1st edition: Springer, 2009. 1419 s. ISBN 978-0-387-73003-5.**
2. **RAK, Roman; MATYÁŠ, Vašek; ŘÍHA, Zdeněk. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Vyd. 1. Praha: Grada, 2008. 631 s. ISBN 978-80-247-2365-5.**
3. **L-1 Identity Solutions [online]. c2010 [cit. 2011-02-02].**
4. **NStar [online]. c2011 [cit. 2011-02-02]. Honeywell.**
5. **International Biometric Group [online]. c2011 [cit. 2011-02-02].**

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

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Předmětem bakalářské práce je rozbor nejpoužívanějších metod autentizace používaných u docházkových a přístupových systémů zaměřený především na biometrickou metodu autentizace pomocí otisku prstu. Praktická část se zabývá realizací propojení biometrické čtečky se systémem WinPack a popisem propojení terminálů TimeStation s programem Docházka Plus.

Klíčová slova: otisk prstu, přístupový systém, docházkový systém, TimeStation, Docházka Plus

ABSTRACT

Subject of this thesis is an analysis of the most commonly used authentication methods used for attendance and access control systems primarily focused on biometric authentication method using a fingerprint. The practical part deals with the realization of the connection biometric reader with system WinPack and description of the connection TimeStation terminals with the program Docházka Plus.

Keywords: fingerprint, access system, attendance system, TimeStation, Docházka Plus

Poděkování

Na tomto místě bych chtěl velmi poděkovat vedoucímu bakalářské práce panu doc. Mgr. Milanu Adámkovi, Ph.D. za odbornou pomoc a cenné rady, dále děkuji panu Ing. Petru Kováčovi za konzultace a cenné připomínky při řešení bakalářské práce a v neposlední řadě bych chtěl poděkovat své rodině za morální a finanční podporu při studiu.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Žijeme v době, kdy si firmy čím dál tím víc uvědomují potřebu chránit svůj majetek a snaží se co nejefektivněji využít svých finančních a lidských zdrojů, a proto zde existují přístupové a docházkové systémy, které nám poskytují dokonalý přehled o pohybu osob nebo vozidel v monitorovaném prostoru a poskytují nám i informace o pracovní morálce zaměstnanců, které slouží jako podklady pro zpracování mzdové agendy. Finanční prostředky, které firmy investují do docházkových a přístupových systémů se jim mnohonásobně vrátí snížením počtu odcizeného firemního majetku, zvýší se i pracovní morálka jejich zaměstnanců a omezí se i počet chyb, které vznikají při manuálním zpracování docházkových dat.

U docházkových a přístupových systémů existuje mnoho metod, kterými člověk prokazuje svou identitu. Autentizační metody jsou většinou založeny na těchto třech principech, že daný uživatel něco zná (heslo, PIN,…), že daný uživatel něco vlastní (karta, čip) a v neposlední řadě, že daný uživatel něčím je (charakteristické vlastnosti daného uživatele např. otisk prstu).

Tato práce je rozdělena do dvou částí. V první části teoretické budu rozebírat nejpoužívanější metody využívané u přístupových a docházkových systémů. Zaměřím se hlavně na biometrickou metodu autentizace pomocí otisku prstu, která se v poslední době stává čím dál tím více oblíbenou z důvodu snižující se ceny biometrických terminálů a jednoduchosti jejich používání. V druhé části praktické budu prakticky realizovat spojení biometrické čtečky Bioscrypt V-Pass se systémem WinPack, dále pak budu realizovat propojení dvou terminálů TimeStation s docházkovým softwarem Docházka Plus a na toto propojení vytvořím jednoduchou úlohu.

Cílem práce je ukázat a popsat nejvíce používané metody autentizace u docházkových a přístupových systémů. Dále pak provést a popsat zapojení přístupového (čtečka Bioscrypt V-Pass a WinPack) a docházkového systému (terminály TimeStation a Docházka Plus).

I. TEORETICKÁ ČÁST

1 IDENTIFIKACE, AUTENTIZACE A AUTORIZACE

V prostředí docházkových a přístupových systémů a nejen tam se setkáváme s výrazy identifikace, autentizace a autorizace. A proto si v této části vysvětlíme, co tyto výrazy znamenají.

- **Identifikace** je proces, při kterém se snaží systém přiřadit známé veličiny z databáze k neznámému subjektu, aby se z neznámého subjektu stal známý subjekt. Systém si klade prostou otázku: „Kdo jsi?“.
- **Autentizace** je proces, při kterém systém ověřuje, že subjekt je skutečně tím, za koho se vydává (ověření informací, získaných identifikací). Systém si klade prostou otázku: „Jsi opravdu ten subjekt za, který se vydáváš?“. V případě autentizace osob rozlišujeme následující způsoby autentizace:
  - Autentizace na základě biometrických vlastností (např. otisky prstů).
  - Autentizace na základě toho, že něco vlastní (např. čipová karta).
  - Autentizace na základě toho, že něco zná (např. heslo).

  Pokud použijeme kombinaci více způsobů autentizace, tak tomu říkáme více složková autentizace.
- **Autorizace** je proces, při kterém jsou subjektu poskytnuty přístupová práva na základě provedené identifikace a autentizace.

2 ZÁKLADNÍ AUTENTIZAČNÍ METODY

Autentizační metody jsou většinou založené na třech základních principech:

1. daný uživatel něco zná (heslo, PIN,…)
2. daný uživatel něco vlastní (karta)
3. daný uživatel něčím je (charakteristické vlastnosti daného uživatele např. otisk prstu)

Každá s těchto metod má svoje výhody a nevýhody.

Obr. 1. Typy identifikačních médií. [11]

2.1 Hesla

Jedná se o nejjednodušší a nejpoužívanější způsob autentizace v dnešní době. Je založen na tom, že daný uživatel něco zná, to znamená, že veškeré informace, které potřebuje k přístupu má ve své hlavě a nemusí si neustále sebou nosit nějakou fyzickou věc. Uživatel zadá do systému svoje ID a heslo a systém prohledá svoji databázi, a pokud se údaje v databázi shodují s údaji, které uživatel zadal, je mu umožněn přístup.

U většiny přístupových a docházkových systémů se ID a heslo pro jednodušší zadávání skládá jen s řetězce čísel. V systému může být i nastaven alarm, který se spustí po několika špatných zadáních a informuje nás o tom, že se systémem může manipulovat neoprávněná osoba.

Výhody:

- jednoduché ovládání
- jednoduchá údržba
- snadné přenášení (heslo máme v hlavě)

Nevýhody

- celkem snadná zjistitelnost hesla
- nebezpečí zapomenutí hesla
- i při použití správného hesla nejde zaručit, že se jedná o osobu, které bylo heslo uděleno

2.2 Autentizační tokeny

Tento způsob autentizace je založen na tom, že daný uživatel něco vlastní, tím je myšlen nějaký fyzický objekt často označovaný jako token. Tokeny jsou zařízení, které musí uživatelé stále nosit s sebou, aby se mohli autentizovat.

Tokeny mají specifické fyzické vlastnosti (tvar), elektrické vlastnosti (elektrický odpor, elektrickou kapacitu) nebo obsahují tajné informace (kvalitní heslo nebo kryptografický klíč) anebo jsou schopny provádět kryptografické výpočty.

Nejčastěji používané tokeny:

- karty (s čárovým kódem, magnetickým proužkem, čipové kontaktní/bezkontaktní)
- čipové tokeny (čip Dallas)

Výhodou tokenů je jejich obtížnější kopírování, jejich případná ztráta lze snadno zjistit a také jsou schopny uchovávat a zpracovávat náhodné informace s velkou entropií (míra informace).

Nevýhodou tokenů je vzájemná nekompatibilita různých typů. Další nevýhodou je možnost ztráty, protože náhrada je časově náročná a uživatel bez tokenu nemůže být rozpoznán a navíc se může token sám porouchat což je samo o sobě při pokusu o autentizaci těžko odhalitelné.

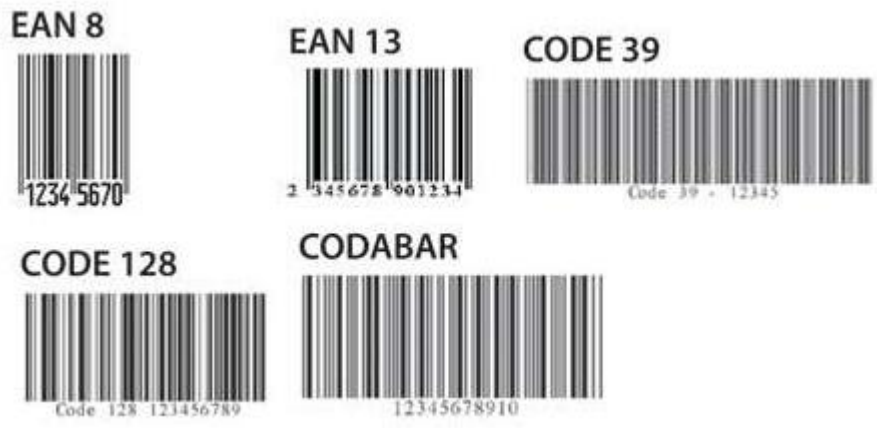
2.2.1 Karty s čárovým kódem

Karty opatřené jedinečným čárovým kódem (zakódovanou alfanumerickou informací) identifikují svého nositele a mají proto široké využití u jakýchkoliv identifikačních systémů (docházkové systémy, přístupové systémy, stravovací systémy, atd.)

Nejpoužívanější a nejrozšířenější jsou čárové kódy EAN 8 a EAN 13. Dalšími používanými kódy jsou CODE 39, CODE 128, ITF, UPC, CodaBar atd.

- **EAN 8** – pevná délka 7 čísel + 1 kontrolní číslo, minimální šířka čárového kódu je 20 mm.
- **EAN 13** – pevná délka 12 čísel + 1 kontrolní číslo, minimální šířka čárového kódu je 25 mm.
- **CODE 39** – proměnná délka podle počtu znaků, alfanumerické znaky, minimální šířka 3,75 mm na znak.
- **CODE 128** – proměnná délka podle počtu znaků, alfanumerické znaky, minimální šířka 3,75 mm na znak.
- **UPC – A a B** – pevná délka 12 čísel, minimální šířka čárového kódu je 25 mm.

Čárový kód může být zakryt speciální barvou, ale pak je čitelný pouze infračerveným paprskem, čímž se zvyšuje bezpečnost.



Obr. 2. Ukázka různých druhů čárových kódů.[16]

2.2.2 Karty s magnetickým proužkem

Magnetický proužek karet pracuje na obdobném principu jako pásek kazety – tj. slouží jako nosič jednoduchých datových informací, které pak čtecí zařízení čte nebo na proužek ukládá a provádí odpovídající operaci – tj. např. otevře dveře nebo závoru, zaznamená vstup, přičte nebo odečte body, provede finanční transakci atp.[16]

Páska na magnetických kartách obsahuje celkem tři stopy, z nichž každá má svůj specifický význam a umožňuje uložit určité množství specifické informace.[15]

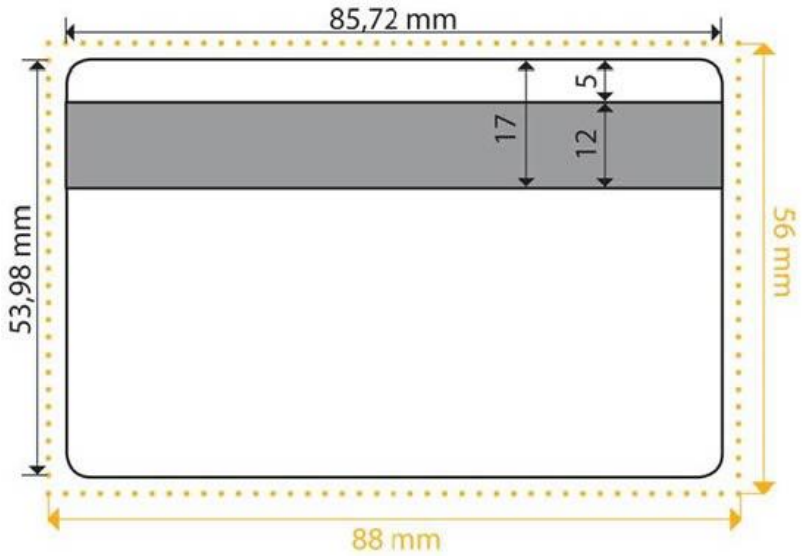
1. **stopa:** byla definována v roce 1969 Mezinárodní asociací leteckých dopravců IATA (International Air Transportation Association), proto aby usnadnila automatické odbavování cestujících. V roce 1970 ji přijali i americké banky. Je na ní možné uložit až 79 alfanumerických znaků. Hustota kódování je 210 bpi.
2. **stopa:** byla definována společností ABA (American Bankers Association) pro použití karty při on-line finančních transakcích. Je na ní možné uložit až 40 numerických znaků (pouze čísla 0-9 a rovnítko). Hustota kódování je 75 bpi.
3. **stopa:** byla definována bankami (THRIFT) pro finanční transakce. Používá se pro uložení informací, které umožňují ověřit PIN. Jako jediná je tato stopa definovaná pro čtení i zápis což znamená, že informace uložené v této stopě jde měnit. Je na ní možné uložit až 107 numerických znaků (pouze čísla 0-9, rovnítko a dvojtečku). Hustota kódování je 210 bpi.

Karty s magnetickým proužkem se dále dělí na dva typy podle hustoty zápisu. Hustota zápisu nemá vliv na počet nahraných stop nebo dat, ale má vliv na odolnost záznamu a možnost jeho ovlivnění vnějšími magnetickými vlivy.

- **LoCo (Low Coercivity):** nízká hustota záznamu. Nižší cena. Snadná zničitelnost.
- **HiCo (High Coercivity):** vysoká hustota záznamu. Vyšší odolnost proti vnějším vlivům než u LoCo.

Typ, umístění a rozměry magnetického proužku jsou dány normou ISO 7811.

Mezi největší nevýhody karet s magnetickým proužkem patří životnost a další z bezpečnostního hlediska závažnější nevýhodou je možnost snadného vytvoření duplikátu existující karty, z toho důvodu se dnes přechází na bezpečnější karty a to karty čipové.



Obr. 3. Rozměry karty a magnetického proužku.[16]

2.2.3 Čipové karty

Čipové karty jsou v současnosti hojně používány v mnoho aplikacích. Jako příklad lze uvést platební systémy, přístupové a docházkové systémy. V těchto případech je pomocí čipových karet ověřována identita uživatele. Většina dostupných karet je standardizována normami ISO, ale existují i vlastní řešení různých výrobců.

Čipová karta se skládá z karty, čipu a kontaktních plošek i vestavěné antény podle typu komunikačního rozhraní. Samotná karta je vyrobena z PVC a čip je zalisován uvnitř karty. Velikost karty je standardizována podle normy ISO 7810 a rozmístění plošek podle normy ISO 7816.

Čipové karty osazené procesorem jsou označovány názvem „smart card“. Nejčastěji se používají procesory skupiny Intel 8051 a jejich klony.

Další součástí čipu jsou paměti typu ROM, EEPROM a RAM.

Paměť ROM (Read Only Memory)

- umožňuje pouze čtení nelze do ní zapisovat, obsah v ní zůstává i po odpojení napájení a je určena jako paměť programu.

Paměť EEPROM (Electrically Erasable Programmable Read-Only Memory)

- umožňuje zápis i čtení, obsah v ní zůstává i po odpojení napájení a je určena jako bezpečné uložiště dat např. klíčů.

Paměť RAM (Random-Access Memory)

- umožňuje zápis i čtení, obsah v ní nezůstává po odpojení napájení a je určena jako operační paměť.

Čip může dále obsahovat různé koprocesory pro symetrickou a asymetrickou kryptografii, generátor náhodných čísel a blok pro výpočet kontrolního součtu.

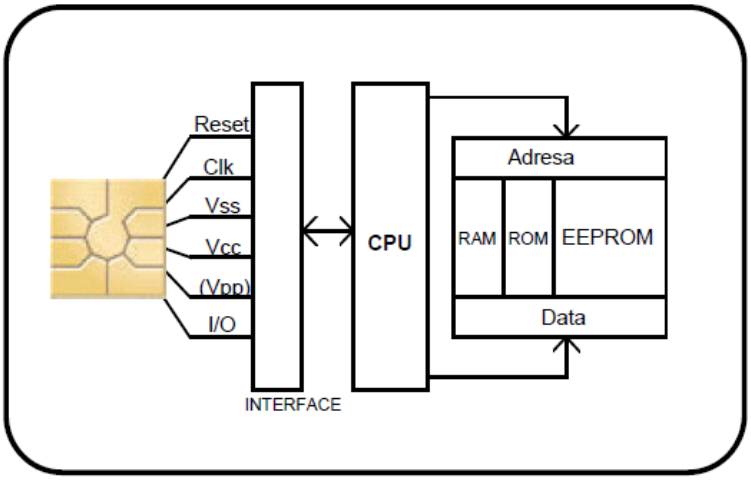
Pro čipové karty jsou vytvořeny speciální operační systémy, které se označují zkratkou SCOS (Smart Card Operating Systems) a jsou uloženy v paměti ROM.

Čipové karty se dělí na dva základní druhy:

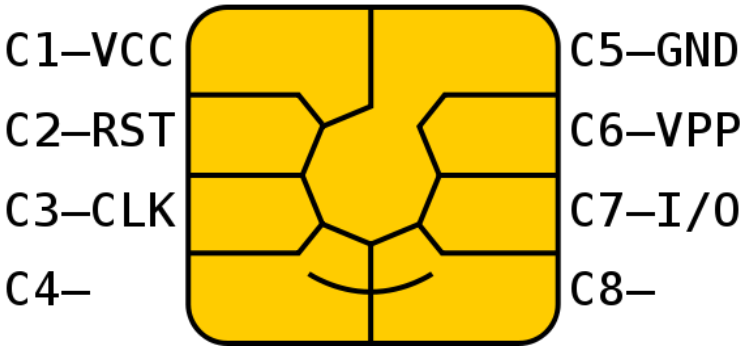
- kontaktní čipové karty
- bezkontaktní čipové karty

2.2.3.1 Kontaktní čipové karty

Kontaktní čipová karta je vybavena kontaktními ploškami s osmi kontakty, jejichž umístění a funkce se řídí normou ISO/IEC 7816-2. Jednotlivé kontakty se používají pro sériovou komunikaci, napájení čipu, přivedení externího taktovacího signálu a programovacího napětí. Rozšíření komunikačních možností čipové karty specifikuje standard ISO/IEC 7816-12 a díky němu jsou dnes vyráběna karty obsahující rozhraní USB přímo v čipu, označované USB-ICC.



Obr. 4. Struktura čipové kontaktní karty.[19]



Obr. 5. Kontaktní plošky kontaktní karty.[20]

VCC – Napájení čipu

RST – Reset

CLK – Hodinový signál

GND – Uzemnění

VPP – Vstup programovacího napětí

I/O – Sériový vstup a výstup

C4, C8 – AUX1, AUX2 kontakty pro USB rozhraní nebo jiné použití

2.2.3.2 Bezkontaktní čipové karty

Bezkontaktní čipová karta využívá k bezkontaktní radiové komunikaci na krátkou vzdálenost (do 10 cm) frekvenci 13,56MHz. Bezkontaktní komunikace je definována standardem ISO/IEC 14443. V minulosti byla hlavní překážka nasazení bezkontaktních karet vysoká energetická náročnost čipů při kryptografických operacích prostřednictvím radiového přenosu. V současnosti lze díky miniaturizaci a snižující se spotřebě provádět pohodlně i kryptografické operace založené na algoritmech RSA nebo ECC. S využitím radiového přenosu se, ale objevují nová bezpečnostní rizika, která je nutné řešit a to neoprávněné čtení, odposlouchávání a přesměrování.

Jako nedostatečně zabezpečené čipové karty se v roce 2008 ukázali karty Mifare Classic, kdy se objevili postupy na prolomení algoritmu Crypto1, který tyto karta používají. Toto prolomení umožňuje duplikování karty a s tím související bezpečnostní rizika.

2.3 Biometrika

Pojem biometrika pochází z řeckých slov „bios“ (život) a „metron“ (měřit měření), což by znamenalo v doslovném překladu „měření živého“. Biometrika se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních vlastností a proporcí.

Biometrické metody můžeme rozdělit na dvě rozdílné aplikace autentizaci a identifikaci.

- **Autentizace** je proces, kdy uživatel předkládá tvrzení o své identitě a na základě této udané identity systém porovná aktuální biometrické informace s informacemi v databázi. Systém odpovídá na otázku: „Je to opravdu ta osoba za, kterou se sama vydává?“
- **Identifikace** je proces, při kterém uživatel identitu sám nepředkládá a systém prochází veškeré záznamy v databázi, aby našel shodu a identitu sám rozpoznal. Systém odpovídá na otázku: „Kdo to je?“ Z toho jasně vyplívá, že identifikace je náročnější než autentizace, protože systém musí projít všechny záznamy v databázi a s rostoucí velikostí databáze se přesnost identifikace snižuje a klesá i rychlost.

Biometrických technologií existuje mnoho a jsou založeny na měření fyziologických vlastností člověka (otisk prstu) nebo na chování člověka (dynamika podpisu). Systémy postavené na fyziologických vlastnostech člověka jsou spolehlivější a přesnější než systémy založené na chování člověka, protože měření fyziologických vlastností je lépe opakovatelné a není ovlivněno v takové míře psychickými, fyziologickými stavy člověka (stres, nemoc).

Největším rozdílem mezi biometrickými a klasickými systémy je odpověď na autentizační požadavek. Biometrické systémy nedávají jednoznačnou odpověď typu ano/ne, tak jako u hesla, které buď zadáme dobře nebo špatně nebo u karty, která je platná nebo neplatná a to z důvodu, že při snímání biometrické informace nastane vždy určitá odchylka a proto systém nemůže určit identitu uživatele absolutně, ale jen s určitou pravděpodobností.

Technicky je možné vytvořit systém, který by vyžadoval 100% schodu biometrické informace, ale takový systém by byl nepoužitelný, protože výsledek snímání by byl vždy aspoň trochu odlišný a takový uživatel by byl téměř vždy odmítnut. Proto, aby byl systém použitelný, musíme nastavit určitou odchylku biometrické informace což, ale dává větší šanci podvodníkům s podobnými biometrickými vlastnostmi.

Nejčastější používané biometrické metody:

- otisk prstu – měří se struktura papilárních linií
- geometrie tváře – měří se vzdálenosti specifických částí obličeje (oči, nos a ústa)
- duhovka oka – porovnává se obrazový vzorec duhovky
- sítnice oka – porovnává se struktura žil na očním pozadí
- dynamika podpisu – měří se rychlost psaní a rozdíly v dynamice tlaku
- hlas – porovnává se tón a zbarvení hlasu
- geometrie ruky – měří se rozměry dlaně a prstů
- tvar ucha – měří se rozměry viditelné části ucha
- DNA – porovnává se řetězec deoxyribonukleové kyseliny

U přístupových a docházkových systémů je v současné době nejčastěji používanou identifikační metodou otisk prstu. Tato technologie je nejpoužívanější, protože je cenově dostupná, je dostatečně rychlá, spolehlivá a přesná.

2.3.1 Přesnost Biometrických systémů

Přesnost a efektivnost biometrických systémů lze měřit pomocí statických koeficientů, které nám umožní porovnání jednotlivých biometrických systémů. Koeficientů existuje řada a zde si popíšeme, co znamenají.

False Acceptance Rate (FAR) [%]

Koeficient FAR (koeficient chybného přijetí) udává pravděpodobnost toho, že systém vyhodnotí neoprávněnou osobu jako oprávněnou a umožní ji přístup do systému, kde může způsobit škody. Jedná se o velmi důležitý parametr z bezpečnostního i marketingového hlediska.

$$FAR = \frac{N_{FA}}{N_{IIA}} \cdot 100 \ [\%]$$

N_{FA} - počet chybných přijeti

N_{IIA} - počet všech pokusů neoprávněných osob o identifikaci

False Rejection Rate (FRR) [%]

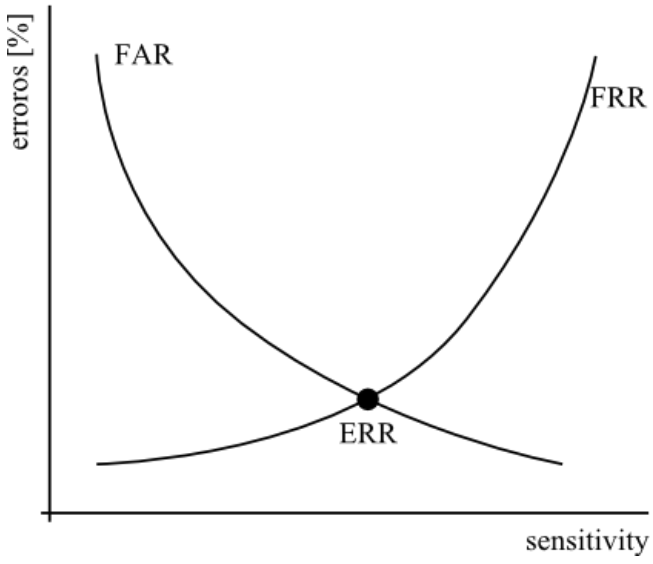
Koeficient FRR (koeficient chybného odmítnutí) udává pravděpodobnost toho, že systém vyhodnotí oprávněnou osobu jako neoprávněnou a neumožní ji přístup do systému. Jedná se o parametr, který nemá z bezpečnostního hlediska žádný význam, ale z uživatelského hlediska je tento parametr hodně důležitý, protože zlepšuje komfort používaného systému.

$$FRR = \frac{N_{FR}}{N_{EIA}} \cdot 100 \ [\%]$$

N_{FR} - počet chybných odmítnutí

N_{EIA} - po počet všech pokusů oprávněných osob o identifikaci

Chyby FAR a FFR jsou nejčastěji vyjádřeny v procentech, ale jde je vyjádřit i poměrem. Např. FAR 0,001% odpovídá poměru 1: 100 000, což v tomto případě znamená, že jeden ze 100 tisíc neoprávněných pokusů o přístup do systému může být propuštěn jak oprávněný.



Obr. 6. Vztah mezi FRR a FAR. [10]

Failure to Enroll Rate (FER) [-]

Koeficient FER udává poměr osob, u kterých selhal proces sejmutí biometrické vlastnosti. Tato veličina je pohyblivá a nemá vztah jenom k osobě, ale i ke konkrétní biometrické vlastnosti, kterou snímáme. Můžeme taky určit i osobní FER, které udává vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání.

Failure To Acquire (FTA) [%]

Koeficient FTA jedná se o tzv. koeficientu selhání přístupu. Jedná se o případ, kdy je uživateli správně načtena biometrická vlastnost, ale systém ji neustále odmítá i po mnoho pokusech.

False Identification Rate (FIR) [%]

Koeficient FIR udává pravděpodobnost toho, že při procesu identifikace je načtená biometrická vlastnost chybně přiřazena k některému referenčnímu vzorku.

False Match Rate (FMR) [-]

Koeficient FMR udává poměr neoprávněných osob, které jsou chybně rozpoznány jako oprávněné osoby během srovnávacího procesu. Koeficient FMR se liší od FAR v tom, že do FMR se nezapočítávají odmítnutí z důvodu špatné kvality snímku.

False Non-Match Rate (FNMR) [-]

Koeficient FNMR udává poměr oprávněných osob, které jsou chybně rozpoznány jako neoprávněné osoby během srovnávacího procesu. Koeficient FNMR se liší od FRR v tom, že do FNMR se nezapočítávají odmítnutí z důvodu špatné kvality snímku.

Tab. 1. Srovnání biometrických metod. [11]

	Oko - duhovka	**Oko - sítnice**	**Obličej**	**Otisk prstu**	**Geometrie ruky**	**Podpis**	**Hlas**
Přesnost porovnání	velmi vysoká	velmi vysoká	vysoká	vysoká	vysoká	vysoká	vysoká
Náročnost na použití	střední	nízká	střední	vysoká	vysoká	vysoká	vysoká
Odolnost proti útoku	velmi vysoká	velmi vysoká	střední	vysoká	vysoká	střední	střední
Akceptovatelnost	střední	střední	vysoká	střední	vysoká	velmi vysoká	vysoká
Dlouhodobá stabilita	vysoká	vysoká	střední	vysoká	střední	střední	střední

2.3.2 Otisk prstu

Identifikace na základě otisku prstu je jednou z nejstarších biometrických metod. Pro svou jedinečnost a stálost se otisk prstu používá k identifikaci už celé století. V dnešní době je tato identifikace už plně automatizovaná. Tato metoda je především oblíbená pro relativní jednoduchost získávání srovnávacího vzorku, je použitelná u většiny populace (identifikovat nelze jen jedince, kteří nemají obě ruce i nohy).

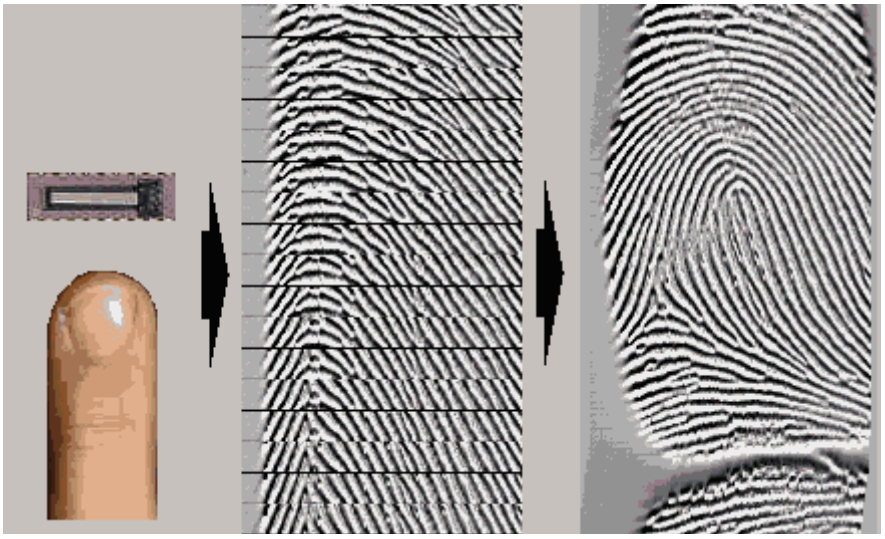
Metody zachycení otisku prstů:

Statické snímání

Jedná se o nejpoužívanější metodu snímání otisku prstu. Uživatel jen přitiskne svůj prst na senzor. Výhodou této metody je jednoduché ovládání, kdy stačí jen přiložit prst na senzor. Nevýhody jsou možné poškození snímače velkou silou tlačení prstu, nehygieničnost a na senzoru můžou zůstat latentní otisky.

Snímání šablonováním

U této metody uživatel přejíždí prstem po senzoru, který snímá obraz pomocí segmentů, které jsou následně spojeny v otisk pomocí speciálního algoritmu. Výhody jsou, že na senzoru nezůstávají latentní otisky, snímač je stále čistý a snímání je rychlé. Nevýhody jsou, že obsluha není úplně jednoduchá, uživatel se musí naučit, jak má přejíždět po senzoru.



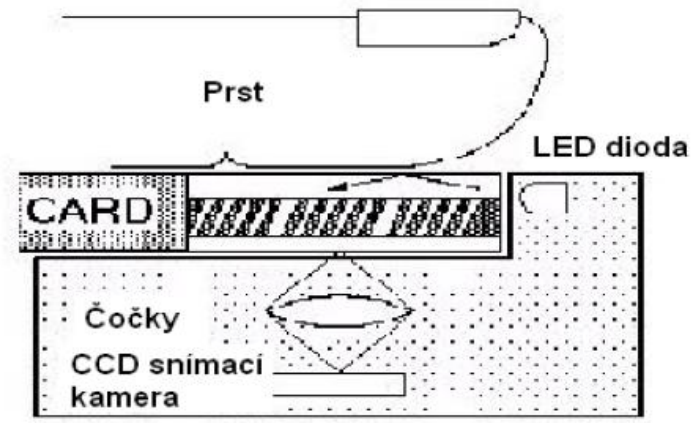
Obr. 7. Zachycení obrazu prsti šablonováním. [8]

2.3.2.1 Optické snímače otisku prstu

Optické snímače otisku prstu jsou založeny na několika metodách. Zde si tyto metody popíšeme.

Optické snímače založené na principu odrazu (reflexní)

Princip tohoto snímače spočívá v tom, že přidržíme prst nad podsvětlenou vrstvou, světlo se odrazí od prstu a putuje do CCD snímače, který zachytává obraz otisku. Nevýhody tohoto snímače jsou, že je náchylný k chybám z důvodu špinavého prstu nebo skenovací plošky což vede ke špatnému odrazu.



Obr. 8. Princip optické snímače založené na principu odrazu. [8]

Optické snímače založené na principu odrazu (reflexní) se skládáním obrazu

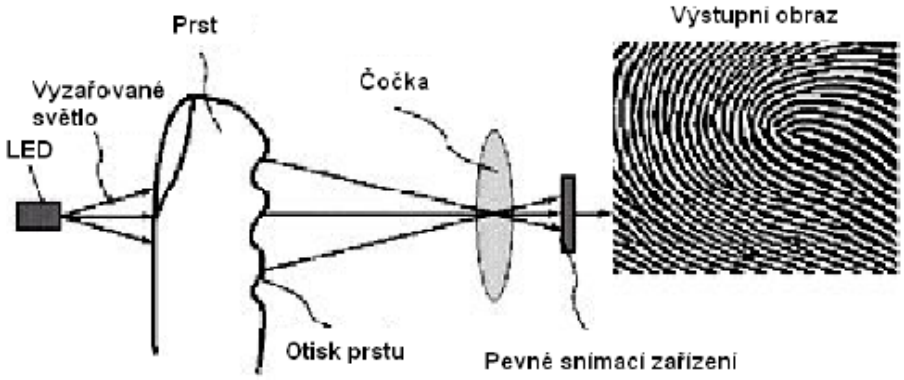
Princip snímání je stejný jako u předchozího snímače, jen výsledný obraz je snímán šablonováním a ne staticky.

Optické bezkontaktní snímače

Tato technologie nepotřebuje optický hranol pro přímé snímání otisku prstu. Světelný paprsek z LED diody se odráží pod různými úhly od papilárních linií prstu do optické čočky. Zpracování signálu provádí CMOS čip.

Transmisní optické snímače

Princip snímání je založen na snímání světelných paprsků procházejících prstem, který je z vrchní části od nehtu prosvětlován všesměrovým zdrojem světla. Zpracování obrazu je stejné jako u předchozích principů pomocí systému čoček a snímacího čipu. Dle výrobce se jedná buď o CCD, nebo o CMOS.



Obr. 9. Princip transmisního optického snímače otisku prstu. [8]

TFT optické snímače

U tohoto typu snímače je nahrazeno klasické snímací zařízení (CMOS nebo CCD) TFT displejem.

Elektro-optické snímače

Princip je založen na tom, že některé polymerní materiály emitují světelné záření. Pokud tento materiál přímo propojíme se snímacím zařízením, získáme otisk prstu tím, že polymerní materiál emituje světlo jen v místech, kde se ho prst dotýká a to je v našem případě jen ve styčných bodech papilárních linií.

2.3.2.2 Rádiové snímače otisku prstu

Princip činnosti je založen na měření síly rádiového signálu, který je vysílán do prstu a je snímán maticí miniaturních antén, které tvoří styčnou plochu s prstem. Síla signálu se mění v závislosti na odporu, tedy na vzdálenosti mezi kůží a soustavou antén, to znamená, že radiový signál je jiný v místě, kde se prst přímo dotýká senzoru a v místě, kde se ne nedotýká (prohlubně papilárních linií).

2.3.2.3 Tlakové snímače otisku prstu

Jedna z nejstarších myšlenek pro získání otisku prstu, ale až v poslední době se technologie piezoelektrických materiálů dostala na takovou úroveň, že je tato metoda použitelná k identifikaci pomocí otisku prstu. Princip této metody je takový, že snímač je složen ze tří vrstev vodivé, nevodivé (gel) a vodivé. Při přiložení prstu dojde ke stlačení první vodivé vrstvy v místech vrcholů papilárních linií, která projde nevodivým gelem a dotkne se druhé vodivé vrstvy.

2.3.2.4 Teplotní snímače otisku prstu

Princip činnosti je založen na tom, že snímač obsahuje citlivý pyroelement, který snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostoru mezi nimi.

Nevýhody: nízká kvalita snímače, špatná kvalita výstupního obrazu otisku

2.3.2.5 Ultrazvukové snímače otisku prstu

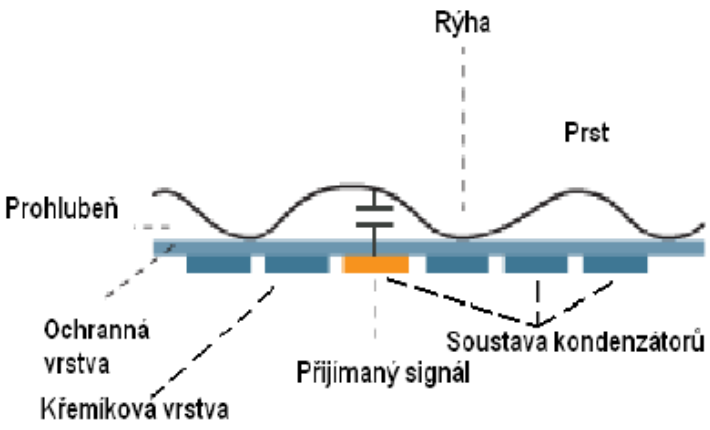
Princip činnosti je založen na měření odražené zvukové vlny, což je podobný princip jako u sonaru. Výhodou této metody je, že ultrazvuk snadno pronikne nečistotami, které by jinak znehodnotily obraz zachycený pomocí optického snímače.

2.3.2.6 Kapacitní snímače otisku prstu

Princip činnosti je založen na rozdílu kapacity mezi deskou snímače a povrchem prstu. Snímač představuje jednu desku kapacitoru a druhou desku představují jednotlivá místa na prstu. Otisk se tak z pixelů získá v digitální formě. Pro získání obrazu položíme prst na citlivou plochu osazenou velkým množstvím elektrod, které převedou otisk prstu na digitální obraz, který se dále zpracovává. Papilární linie jsou k citlivé ploše více přitisklé než mezery mezi nimi, takže mají vyšší kapacitní odpor.

Výhody: malé rozměry, jednoduchý princip funkce, vysoká kvalita a poměrně nízká cena.

Nevýhody: nízká životnost (zničení snímače statickou elektřinou), špatná funkce ve vlhkém prostředí, nutnost měnit snímač v rozmezí 3let



Obr. 10. Princip kapacitního snímače otisku prstu. [8]

3 KOMUNIKAČNÍ ROZHRANÍ

Přístupové a docházkové systémy využívají různých komunikačních rozhraní. Zda si popíšeme nejčastěji používaná rozhraní RS232, RS485, Wiegand a Ethernet, které je poslední dobou velmi časté.

3.1 RS232

RS232 je sériové rozhraní, které bylo původně vytvořeno pro obousměrnou komunikaci bezi dvěma zařízeními. Obsahuje celkem 9 signálů. Většina zařízení si ale vystačí jen se třemi: RxD, TxD a GND (dva směry dat a zem napájení). Pracuje na fyzické vrstvě. Přenos informace je asynchronní s pevně nastavenou přenosovou rychlostí.

Nevýhody rozhraní RS232:

- maximální délka vodičů - dle normy pouze 15 metrů (lze prodloužit)
- nízká odolnost proti rušení
- nebezpečí vzniku zemních smyček (propojením dvou zařízení napájených z různých potenciálů může dojít k poškození nebo zničení zařízení). 100% ochrana galvanické oddělení.

3.2 RS485

RS485 je sériové, asynchronní rozhraní. Používá se hlavně u průmyslových zařízení a v prostředích s požadavky na vysokou odolnost proti rušení.

Dvouvodičová verze RS485 využívá pouze dva vodiče. Linka je polo-duplexní, to znamená, že v jednu chvíli může vysílat pouze jedna strana (tzv. systém dotaz - odpověď).

Čtyřvodičová verze RS485 využívá čtyři vodiče. Linka je plně-duplexní, to znamená, že v jednu chvíli mohou vysílat obě strany.

Maximální délka jedné větve RS485 je až 1200 metrů. Můžeme ji prodloužit pomocí opakovačů. Na jedné větvi může být dle normy maximálně 32 zařízení.

3.3 Wiegand

Wiegand je standardní rozhraní, používané jako výstup ze čteček bezkontaktních karet. Kounikace je pouze jednosměrná - ze čtečky do připojeného zařízení (například Wie232). Fyzickou vrstvou Wiegandu jsou tři vodiče - GND, DATA0 a DATA1. Přenášená data se mírně liší v závislosti na typu protokolu Wiegand. Nejčastěji je možné se setkat s protokoly Wiegand 26 a Wiegand 30. Protokol je zabezpečen paritou. Výhodou rozhraní Wiegand je hlavně možnost připojení čtečky na poměrně velkou vzdálenost.[9]

3.4 Ethernet

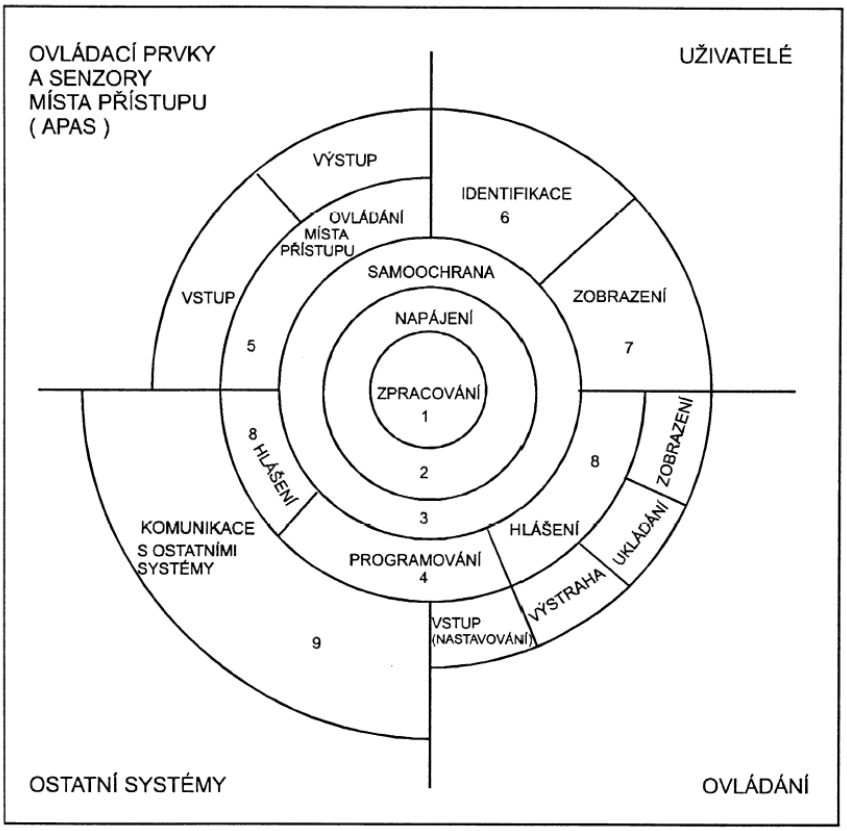
Ethernet je standartní síťové rozhraní využívající pro komunikaci protokol TCP/IP. K propojení jednotlivých zařízení se používá kroucené dvojlinky se čtyřmi kroucenými páry, z nichž jsou většinou využity pouze dva, protože přístupové a docházkové systémy jsou většinou omezeny rychlostí 100Mbit/s, která využívá právě jen dva páry. Doporučená maximální délka mezi dvěma zařízeními je 100 metrů. Nejpoužívanějším konektorem je RJ-45. Pro svoji jednoduchost, nízkou cenu a je tímto rozhraním vybaveno čím dál tím více přístupových a docházkových terminálů.

4 PŘÍSTUPOVÉ SYSTÉMY

Přístupové systémy mají za úkol zabezpečit ochranu majetku a informací tím, že omezují pohyb osob a vozidel po objektu na základě přidělených přístupových práv. Přístupový systém jednoznačně identifikuje osobu pomocí přístupové karty, čipu, otisku prstu a podle práv, které má daná osoba nastavena pro danou část objektu umožní nebo zamítne průchod dveřmi, turniketem, bránou, závorou, atd. Jednotlivé průchody osob jsou zaznamenány a umožňují zpětně dohledat pohyb konkrétní osoby přes průchody.

Základní architektura přístupových systémů:

- **čtecí a snímací zařízení**
- **vyhodnocovací jednotka**
- **výstupní prvek** (zámek, indikátor obsluhy)
- **napájecí zdroje**
- **dohledové a správní pracoviště**



Obr. 11. Základní funkce přístupového systému. [11]

4.1 Úkoly přístupového systému

Především ve spolupráci s ostatními mechanickými a elektronickými systémy plní

základní dva úkoly:

1. Řídí pohyb osob v objektu v denním režimu, to jest v době kdy je systém PZS zpravidla odblokován, nebo jeho část je odblokována a nestřeží.
2. Poskytují informace o pohybu osob v objektu, trvale tyto informace zaznamenávají a sledují a zaznamenávají místo pohybu a čas. Tím přispívají k ochraně objektu i režimovým opatřením. Plněním těchto funkcí pak je jasná komplexní funkce elektronické kontroly vstupu z hlediska logiky nasazení.

Další úkoly přístupového systému:

- omezení přístupu nepovolaných osob do určitých prostor objektu (sklady, výpočetní centra, velíny, kanceláře, nebezpečné prostory, utajované prostory, ochrana know-how)
- omezení přístupu mimo určité časové úseky (zaměstnanci, návštěvníci, noční, denní, úklid, zásobování)
- registrace délky pobytu, doby pobytu, místa a účelu
- sledování a dokumentování pohybu, místa a času osob a zařízení, monitorování stavu v objektu, měření návštěvnosti, vytíženosti pracovníků, objektu, využívání zdrojů, materiálu (kopírky, výtahy), vytížení dalších kapacit, zvýšení bezpečnosti technologických objektů a provozů, dohled, zamezení zbytečného a nepovoleného pohybu po objektu

4.2 Zpracování informací u přístupových systémů

Přístupové systémy můžeme dělit podle toho, kde je umístěna databáze uživatelů a přístupových práv a to na systém s distribuovanou databází a systém s centrální databází.

4.2.1 Systém s distribuovanou databází

U systémů s distribuovanou databází je ve všech řídících jednotkách, které slouží k otvírání dveří uložena kopie informace o ID uživatele a jeho přístupových právech. Každá změna

ID a přístupových práv musí být automaticky nebo ručně distribuována do každé z těchto jednotek. Tento proces je náročnější na komunikaci v rozsáhlých systémech a také řídící jednotky musí být vybaveny větší pamětí, což vede k vyšší ceně systému. Výhodou tohoto systému je vysoká spolehlivost, díky tomu, že řídící jednotky jsou schopny pracovat bez přerušení nezávisle na ostatních jednotkách. Tohoto systému distribuce se využívá u rozsáhlých systémů, kde jsou vzdálené řídící jednotky a velký počet uživatelů

4.2.2 Systém s centrální databází

U systémů s centrální databází jsou u dveří umístěna pouze čtecí a snímací zařízení s výstupními prvky, po identifikaci uživatele čtečkou se ID uživatele odesílá do centrální řídící jednotky, ve které dochází k provedení rozhodnutí o povolení či zamítnutí přístupu a výsledný povel se odesílá zpět k příslušným dveřím.[21]

4.3 Norma ČSN EN 50133

Skupina norem ČSN EN 50133 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích obsahuje informace o systémových požadavcích na sytém, informace o všeobecných požadavcích na komponenty až po informace o pokynech pro aplikace.

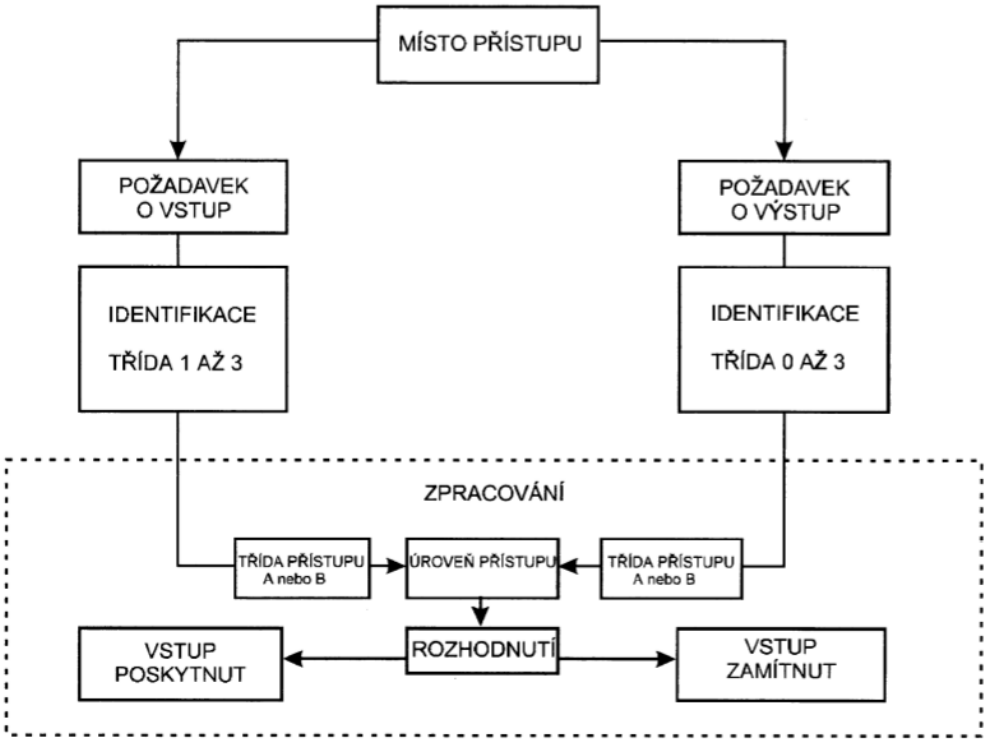
Tato norma, taky řeší stupně zabezpečení a to podle identifikace a přístupu.

Třídy identifikace jsou podle normy rozděleny do čtyř tříd:

- **Třída identifikace 0 –** bez přímé identifikace: Pouze požadavek na vstup bez identifikace uživatele (tlačítko, čidlo pohybu,…).
- **Třída identifikace 1 –** informace uložená v paměti: Požadavek na heslo, identifikační číslo, atd.
- **Třída identifikace 2 –** identifikační nebo biometrický prvek: Požadavek na použití identifikačních prvků (karta, klíče,…) nebo biometrie (otisk prstu, atd.).
- **Třída identifikace 3** - kombinace identifikační nebo biometrický prvek společně s informací uloženou v paměti. Požadavek na použití kombinace identifikačního prvku nebo biometrie a informace uložené v paměti

Třídy klasifikace přístupů jsou podle normy rozděleny do dvou tříd:

- **Třída přístupu A –** stupeň zabezpečení nevyžaduje časové filtry ani ukládání přístupové transakce
- **Třída přístupu B –** pro přístup, který zahrnuje jak časové filtry, tak funkci ukládání. Zahrnuje taky podtřídu vztahující se na místo přístupu s časovými filtry, ale bez funkce ukládání.



Obr. 12. Tradiční postup povolení přístupu.[11]

5 DOCHÁZKOVÉ SYSTÉMY

Docházkové systémy slouží jako náhrada tzv. píchacích hodin, docházkových sešitů a knih docházky. Umožňují automatickou evidenci příchodů, odchodů a přerušení pracovní doby zaměstnanců. Moderní docházkové systémy jsou schopny zpracovat 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. Nasazením docházkového systému se omezí možné chyby, které mohou vzniknout při manuálním zpracování docházkových dat a vedení firmy a zaměstnanci mají aktuální přehled o odpracovaných hodinách v daném měsíci. Docházkové systémy využívají stejné čtečky jako přístupové systémy.

5.1 Zákoník práce

Evidence docházky není žádným způsobem regulována (není ze zákona povinná) a není většinou totožná s evidencí pracovní dobry, protože pouze označuje čas po, který je zaměstnanec přítomen na pracovišti, ale neoznačuje čas po, který pracuje. Proto platí, že si evidenci docházky může zaměstnavatel upravit podle svých potřeb. V praxi je obvyklé, že evidence docházky slouží zároveň jako podklad pro vedení evidence pracovní doby. V tomto případě, ale může docházet ke zkreslení evidence pracovní doby z důvodu, že zařízení pro evidenci docházky je příliš daleko od pracoviště zaměstnance.

Evidence pracovní doby je ze zákona povinná a musí ji vést každý zaměstnavatel. Nedodržení této zákonné povinnosti je možné kvalifikovat jako správní delikt dle zákona o inspekci práce (zákona č. 251/2005 Sb., ve znění pozdějších předpisů). Za tento správní delikt lze uložit zaměstnavateli pokutu až do výše 400.000,- Kč.

Právní úprava evidence pracovní doby je zakotvena v § 96 odst. 1 a 2) zákoníku práce (zákona č. 262/2006, ve znění pozdějších předpisů). Zaměstnavateli je tímto ustanovením uložena povinnost vést u jednotlivých zaměstnanců evidenci:

a) odpracované

1. pracovní doby [§ 78 odst. 1 písm. a)]
2. práce přesčas [§ 78 odst. 1 písm. i) a § 93]

3. další dohodnuté práce přesčas [§ 93a]

4. noční práce [§ 94]

5. doby v době pracovní pohotovosti [§ 95 odst. 2]

b) pracovní pohotovosti, kterou zaměstnanec držel [§ 78 odst. 1 písm. h) a § 95].

Na žádost zaměstnance je zaměstnavatel povinen umožnit zaměstnanci nahlédnout do jeho účtu pracovní doby nebo evidence pracovní doby a do jeho účtu mzdy a pořizovat si z nich výpisy, popřípadě stejnopisy na náklady zaměstnavatele.[5]

5.2 Členění z hlediska způsobu připojení

- **On-line** – stálé propojení docházkového terminálu s řídícím počítačem. Data jsou terminálem průběžně zasílána ke zpracování řídícím počítačem.
- **Off-line** – dočasné propojení docházkového terminálu s řídícím počítačem. Data z terminálu se stahují manuálně. Off-line systémy nevyžadují stálé připojení PC.

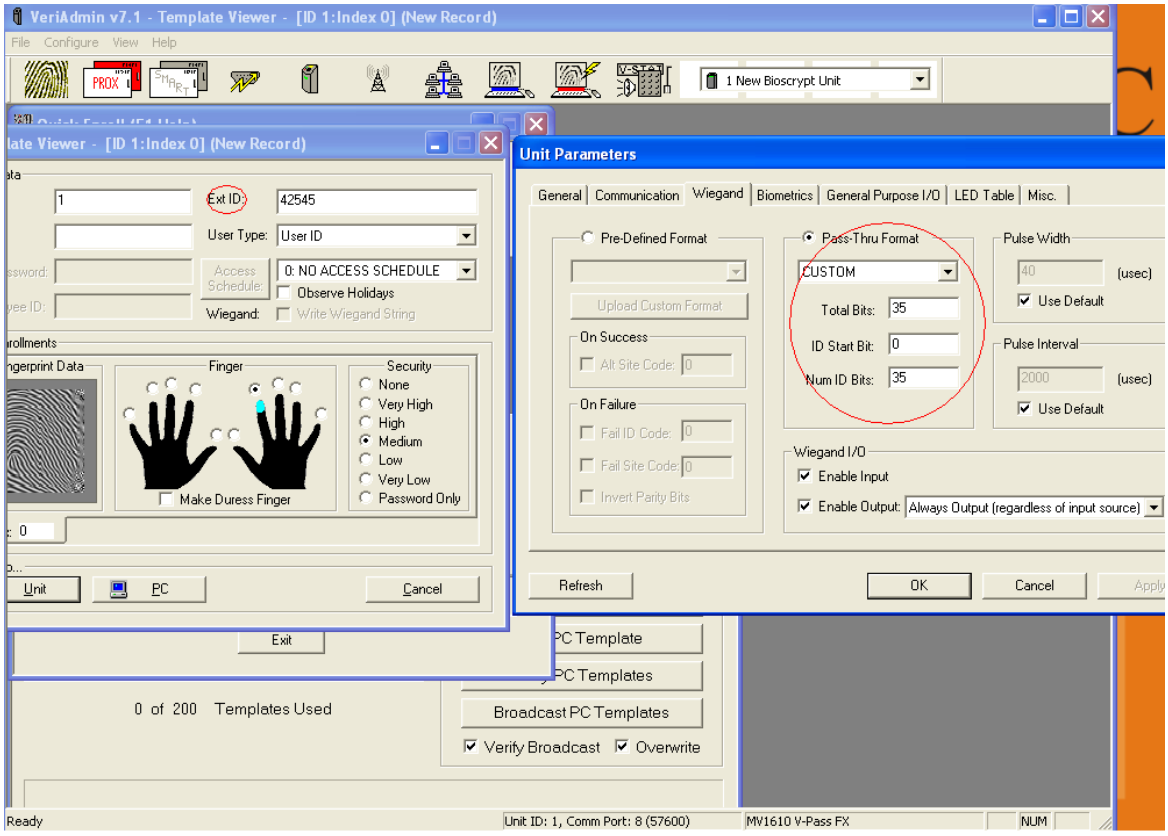
II. PRAKTICKÁ ČÁST

6 REALIZACE KOMUNIKACE MEZI ČTEČKOU A SYSTÉMEM WINPACK

Cílem tohoto bodu bylo propojení biometrické tyčky Bioscrypt V-Pass se systémem WinPack, které se bohužel nezdařilo z důvodu porušení systému WinPack, který nebylo možné oživit a z toho důvodu nemohlo být dokončeno propojení tohoto systému se čtečkou Bioscrypt V-Pass.

6.1 Bioscrypt V-Pass povolení Extended ID

K tomu aby mohla čtečka Bioscrypt V-Pass pracovat se systémem WinPack je nutné pomocí programu VeriAdmin povolit u registrovaného uživatele použití Extended ID, a to tak, že v nastavení parametrů Wiegand přepneme do Pass-Thru Format a Num ID Bits nastavíme větší než 32, tímto dosáhneme aktivace Extended ID v možnostech nastavení uživatele.



Obr. 13. VeriAdmin – nastavení Wiegand a ukázka povoleného Extended ID

7 PROPOJENÍ TERMINÁLU TIMESTATION S DOCHÁZKOVÝM SYSTÉMEM DOCHÁZKA PLUS

Tato kapitola se zabývá propojením terminálů TimeStation s programem Docházka Plus. Původně bylo mým plánem propojit terminály TimeStation takovým způsobem, že by byly oba dva zároveň propojeny s počítačem a přes Docházku Plus by se z každého samostatně stahovala data. Při testování takového zapojení jsem, ale zjistil, že program Docházka Plus, ale i program TimeBook po připojení obou terminálů k počítači vidí pouze ten, který byl připojen jako první, proto původně plánované propojení nepřicházelo v úvahu. Z toho důvodu jsem vymyslel propojení, kdy bude každý terminál autonomní a bude obsahovat stejné zaměstnance. Jeden bude například umístěn u vstupu, do firmy, kde si lidé budou evidovat odchody a příchody na pracoviště a druhý bude například u jídelny, kde si lidé budou evidovat příchod na oběd a odchod z obědu a až na konci měsíce se každý terminál obejde s notebookem s nainstalovaným programem Docházka Plus, do kterého se stáhnou veškeré údaje s obou terminálů, které se v Docházce Plus automaticky spojí a vznikne nám přehledná sestava o odpracované době našich zaměstnanců

7.1 TimeStation

TimeStation je moderní biometrický docházkový terminál. K jeho provozu nejsou potřeba žádné karty, stačí vám jen váš prst. TimeStation nevyužívá skutečný obraz prstu, čímž bezpečně chrání soukromí zaměstnance. Jeho výhody jsou:

- **Přenositelnost** – TimeStation pracuje i na baterie po velmi dlouhou dobu. Proto může být umístěn i tam, kde není síťová zásuvka.
- **Jednoduchá správa** – TimeStation umožňuje administrátorovy přímý přístup k funkcím editace, mazání a výpisu záznamu o uživatelích, uživatelé mohou nahlížet na svou vlastní docházku a odpracované hodiny.
- **Snadná manipulace s daty pomocí PC přes USB port –** TimeStation umožňuje flexibilní propojení s PC pomocí softwaru Docházka Plus, který poskytuje plnou kontrolu a přístup ke TimeStationu a jeho databázi, snadný výpočet mzdy.[22]

Obr. 14. TimeStation terminály.

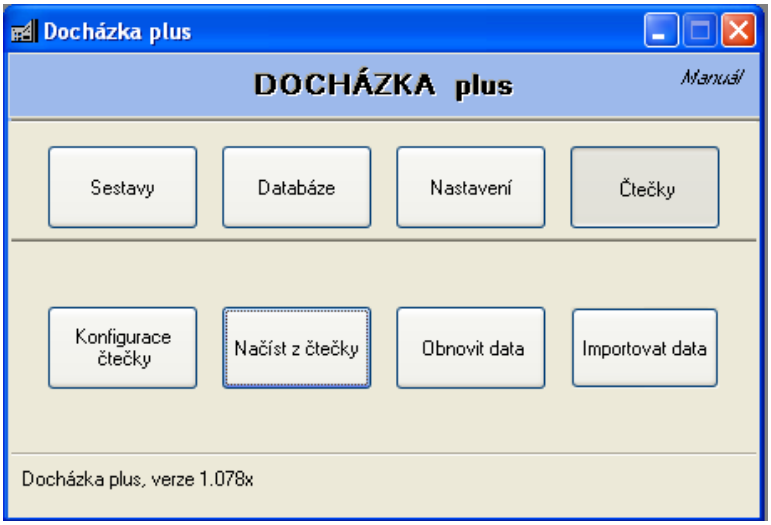
Tab. 2. Specifikace TimeStation.

Položka	**Specifikace**
Maximum otisků prstů	3 administrátoři, 1000 uživatelů
Metody verifikace	Otisk prstu / ID / heslo
Displej	4 řádky Zobrazuje datum, čas, ID a zprávy
Napájení	DC 5V 2A, 4 1.5V AA baterie, USB
Rozměry	190mm x 138mm x 45mm
PC konektor	USB 1.1
Další	Podsvícení displeje Funkce minimálního odběru z baterií

7.2 Docházka Plus

Jedná se o doplněný program "Docházka" pro použití se systémy Intagral, InTagral Plus/Biometrix, TimeStation, ACTAtek, DSE-100 a DSE-200. Umožňuje evidenci docházky v pracovní dny i víkendy, poskytuje několik tiskových sestav, možnost ruční

úpravy dat se zachováním informace o změně, neomezený počet příchodů a odchodů denně, nastavení přerušení a výjimek z pracovní doby, možnost práce ve vícesměnném provozu, použití více čteček, zaokrouhlování, aj.[23]



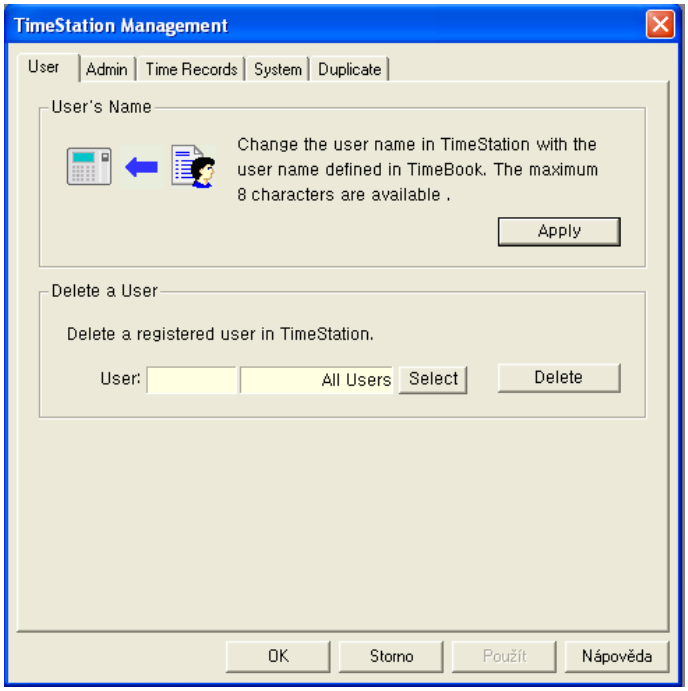
Obr. 15. Hlavní menu programu Docházka Plus.

7.3 Nastavení TimeStation

Zde se budu zabývat nastavením TimeStation a to vymazáním, registrací administrátora, registrací uživatelů a přenesením dat z jednoho terminálu na druhý.

7.3.1 Vymazání terminálu TimeStation

Pokud terminály TimeStation před námi někdo používal, tak nejdříve provedeme vymazání všech údajů. Toto provedeme tak, že nejdříve připojíme jeden terminál k počítači a pomocí programu TimeBook, a to tak, že klikneme na tlačítko *SETUP* a na první záložce „User“ provedeme vymazání všech uživatelů (Delete a User -> Select -> Select All -> Delete), na druhé záložce „Admin“ provedeme vymazání všech administrátorů (Delete Admin -> Delete All) a na třetí záložce „Time records“ provedeme vymazání všech časových záznamů (Delete All Time Records -> Delete All). Poté terminál odpojíme a to stejné provedeme s druhým terminálem.



Obr. 16. TimeBook – okno pro správu terminálu.

7.3.2 Registrace administrátora

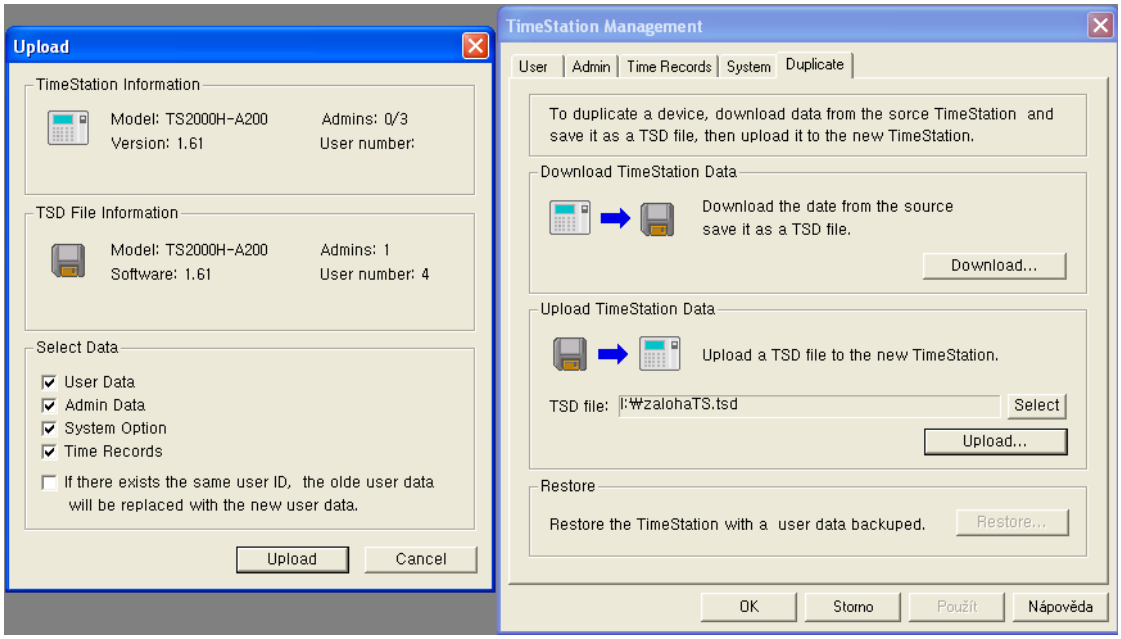
Po vymazání všech údajů z TimeStation je nutné nastavit administrátora, a to tak, že stiskneme *MENU -> ENT* zde vybereme, zda se má administrátor prokazovat otiskem nebo heslem, my vybereme *ZADAT OTISK ADMIN* a zadáme ID administrátoru (až devítimístné číslo, které nesmí začínat 0). Po tomto kroku nás terminál vyzve k přiložení prstu na snímač 2krát až 9krát podle toho jak vyhodnotí otisk. Pak nás terminál informuje o úspěšné registraci. Můžete registrovat až 3 administrátory a každý administrátor si musí pamatovat svoje jedinečné ID.

7.3.3 Registrace uživatelů

Registrace uživatelů probíhá tak, že se nejdříve přihlásíme do terminálu jako administrátor. Vybereme možnost *ZADAT/ZRUSIT UZIV*, zadáme ID uživatele (až devítimístné číslo, které nesmí začínat 0) nejlépe takové aby končilo 0, protože poslední číslo ID se nezadává do Docházky Plus, poté nás terminál vyzve k přiložení prstu na snímač 2krát až 9krát podle toho jak vyhodnotí otisk. Pak nás terminál informuje o úspěšné registraci. Můžete registrovat až 1000 uživatelů a každému uživateli až 10 prstů.

7.3.4 Přenesení uživatelů na druhý TimeStation

Abychom nemuseli provádět registraci uživatelů na obou terminálech, tak ji provedeme jen na jednom a na druhý terminál je přeneseme pomocí programu TimeBook, a to tak, že klikneme na tlačítko *SETUP* a na páté záložce „Duplicate“ provedeme stažení dat z terminálu (Download -> zatrhneme věci, které chceme stáhnout -> Download -> vybereme umístění zálohy), poté co jsme provedli stažení dat z jednoho terminálu, tak ho odpojíme připojíme druhý terminál a provedeme nahrání zálohy (Select -> vybereme umístění zálohy -> Upload -> zatrhneme věci, které chceme nahrát -> Upload). Tímto postupem si ulehčíme hodně práci, protože není nutné provádět zdlouhavou registraci uživatelů vícekrát.



Obr. 17. TimeBook – okno pro nahrání dat do TimeStation.

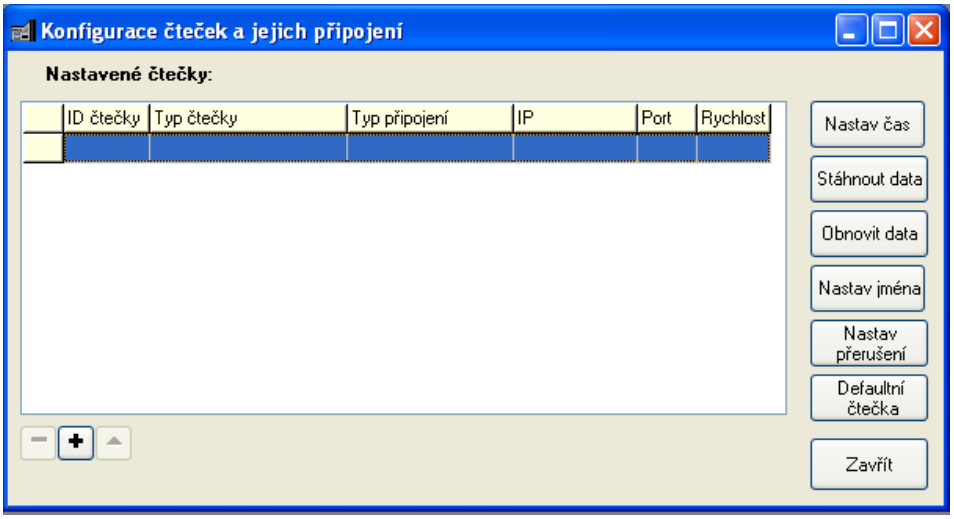
7.4 Nastavení programu Docházka Plus

Zde se budu zabývat nastavením programu Docházka Plus a to propojením s TimeStation, nastavením směn, středisek, správou zaměstnanců atd.

7.4.1 Propojení TimeStation s Docházka Plus

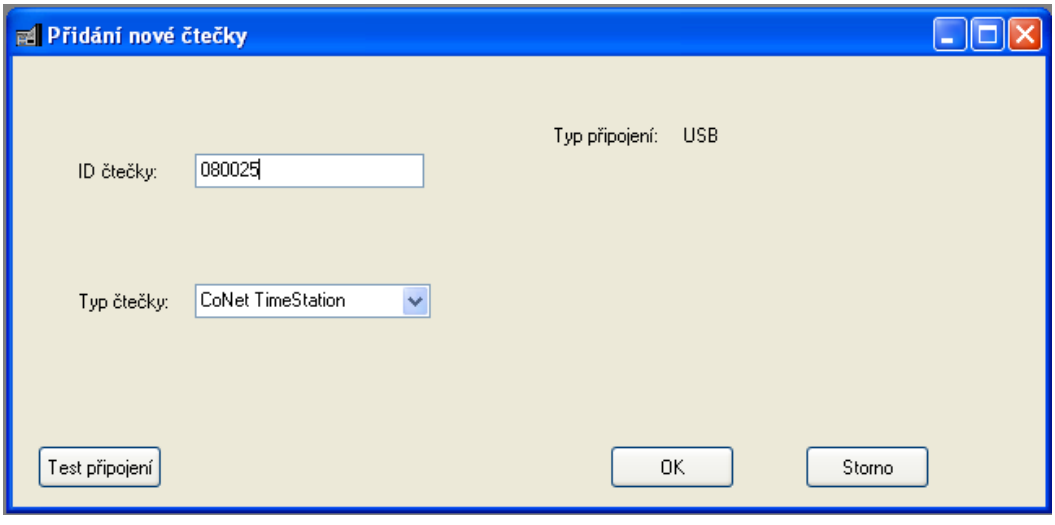
Propojení provedeme v menu Čtečky -> Konfigurace čtečky. Pomocí tlačítka plus se dostaneme do rozhraní pro přidání nové čtečky, zde vybereme náš typ čtečky CoNet

TimeStation a ID čtečky (ID můžete zadat jakékoliv, protože ho Docházka Plus při propojení s terminálem nijak nevyužívá).



Obr. 18. Docházka Plus - menu pro konfiguraci čteček.

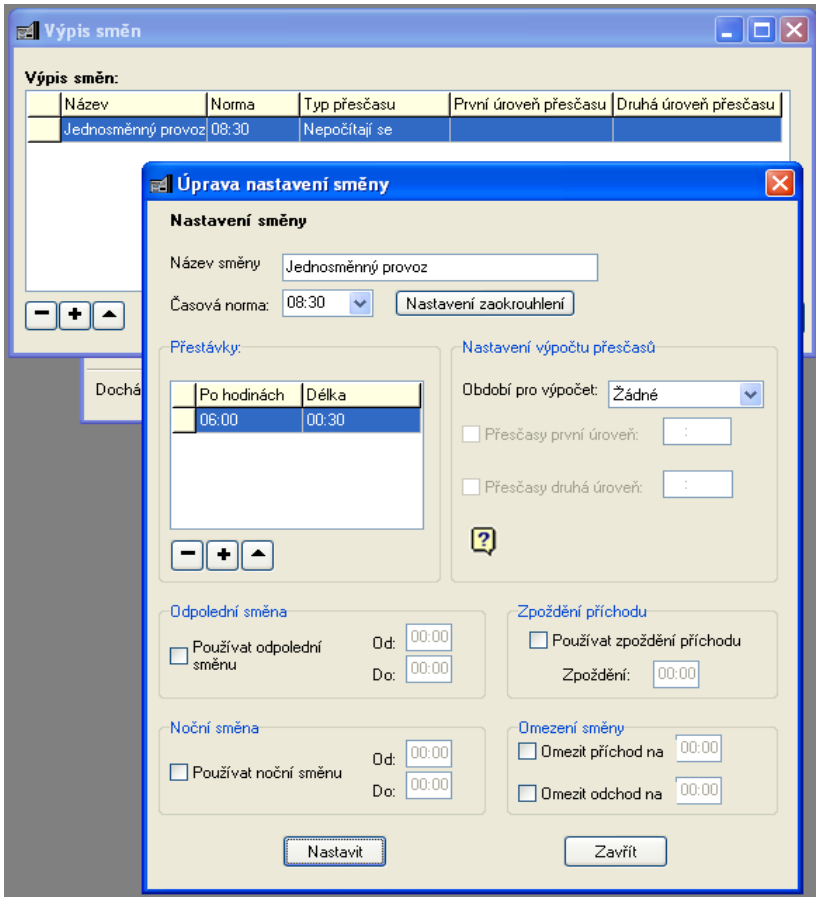
- **Nastav čas** – nastaví terminálu TimeStation stejný čas jako je v počítači
- **Stáhnout data** - stáhne docházková data z terminálu
- **Obnovit data** – načte docházková data od zadaného data
- **Nastav jména** – terminál bude zobrazovat u zaměstnanců taková jména, jaká jsou nastavena v Docházce Plus u jejich ID
- **Nastav přerušení** – funkce není dostupná pro TimeStation
- **Defaultní čtečka** - funkce není dostupná pro TimeStation



Obr. 19. Docházka Plus - okno pro přidání čtečky.

7.4.2 Nastavení směny

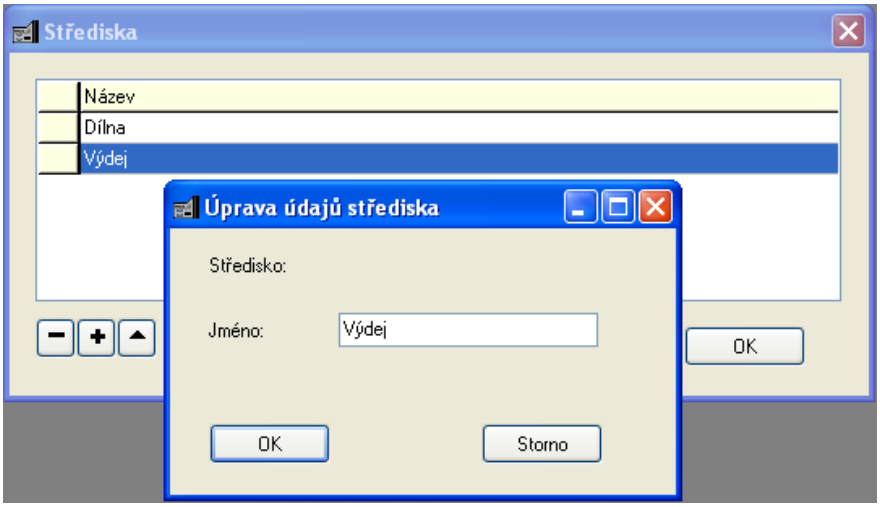
Pomocí tlačítek *Nastavení - > Nastavení směny* se dostanete do rozhraní pro nastavování směn a zde můžete přidávat směny a nastavovat délku směny, po jaké době může být přestávka, kdy začíná ranní směna a kdy odpolední, jakým způsobem chcete počítat přesčasy atd.



Obr. 20. Docházka Plus – nastavení směn.

7.4.3 Přidání středisek

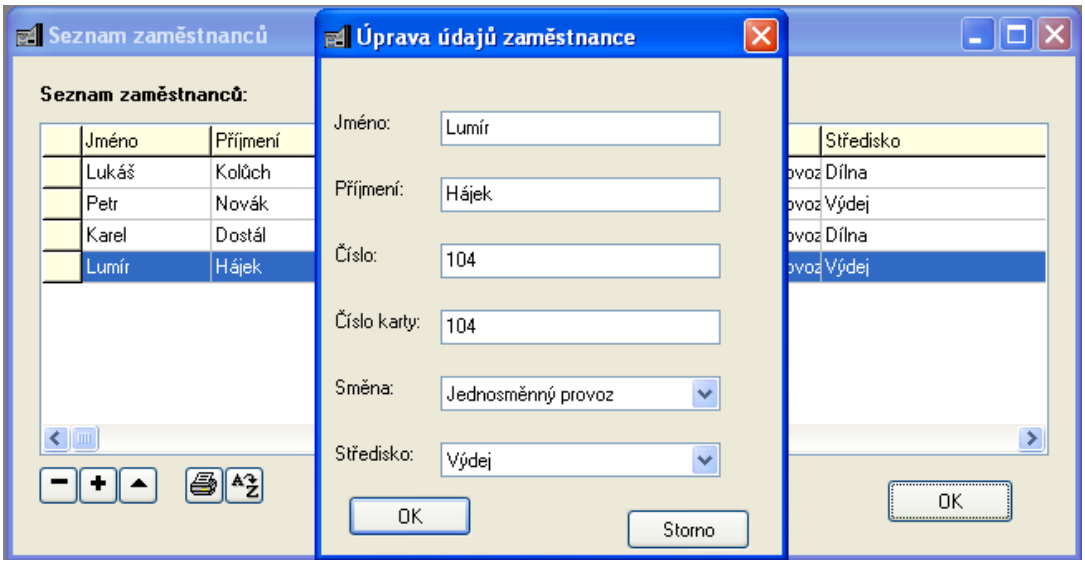
Pomocí tlačítek *Databáze -> Střediska* se dostanete do výpisu středisek a zde můžete přidávat nová střediska, editovat existující střediska a mazat střediska



Obr. 21. Docházka Plus – úprava názvu střediska.

7.4.4 Správa zaměstnanců

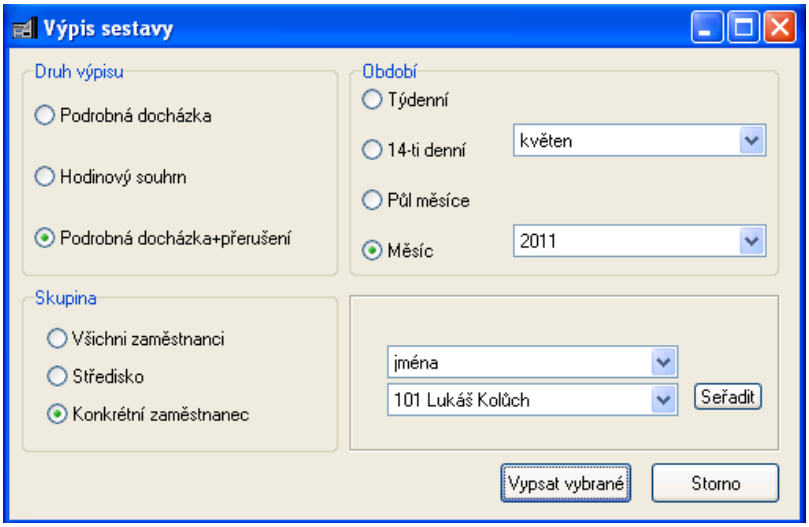
Pomocí tlačítek *Databáze -> Zaměstnanci* můžete přidávat, editovat a mazat zaměstnance. Důležité je si zapamatovat, že číslem karty se rozumí ID otisku v TimeStation bez posledního čísla (např. pokud má zaměstnanec v TimeStation ID 1010, tak do Docházky Plus zadáme číslo karty 101).



Obr. 22. Docházka Plus – úprava údajů zaměstnance

7.4.5 Sestavy

Zde můžete provádět úpravy docházkových dat, např. pokud si například zaměstnanec zapomněl zaevidovat příchod, tak mu ho můžete zaevidovat manuálně. Dále zde můžete generovat a tisknout různé sestavy podle vámi zadaných parametrů (jméno, středisku, přerušení).



Obr. 23. Docházka Plus – generování sestavy.

8 NÁVRH ÚLOHY – DOCHÁZKOVÝ SYSTÉM

Zde jsem provedl návrh úlohy pro docházkový systém, tvořený dvěma TimeStation terminály a programem Docházka Plus.

Úloha - propojení dvou terminálů TimeStation s programem Docházka Plus:

1. Poveďte vymazání terminálů TimeStation.

Vymazání (administrátorů, uživatelů a časových záznamů) provedete pomocí program TimeBook. Nezapomeňte, že PC může pracovat jen s terminálem, který byl připojen jako první, proto pro provádění akcí s druhým terminálem musíte nejdříve první odpojit!

2. Zaregistrujte administrátora.

Registrace se provádí pomocí tlačítek na terminálu. Zapamatujte si ID, které jste použily!

3. Zaregistrujte několik uživatelů.

Každý uživatel musí mít jedinečné ID, které nezačíná 0 (pro pozdější přidávání uživatelů do Docházky Plus doporučuji, aby ID končilo 0).

4. Přeneste uživatele na druhý TimeStation.

Použijte program TimeBook.

5. Propojte TimeStation s Docházkou Plus

V nastavení čtečky v Docházce Plus vyberte CoNet TimeStation a ID zadejte libovolné.

6. V Programu Docházka Plus si nastavte střediska a směny.

7. Vytvořte v Docházce Plus zaměstnance.

Číslo karty se musí shodovat s ID, které jste zadali v TimeStation, ale nesmí obsahovat poslední číslici)

8. Odešlete do terminálu jména, která jsou použitá a příslušných ID zaměstnanců v Docházce Plus.

Toto provedete v okně pro konfiguraci čteček pomocí tlačítka „Nastav jména“.

9. Vyzkoušejte si na terminálech několikrát příchod, odchod a oběd aby terminály obsahovaly nějaké docházkové záznamy.

10. Stáhněte tyto záznamy z terminálů do programu Docházka Plus.

Stažení provedete v menu „Čtečky“ pomocí tlačítka „Načíst z čtečky“.

11. Zkuste si úpravu docházkových záznamů v programu Docházka Plus.

Úprava se provádí v menu „Sestavy -> Úprava dat“, kde si vyberete zaměstnance, u kterého chcete měnit docházková data a den, který chcete měnit. (Můžete měnit, přidávat a mazat časy jeho příchodů, odchodů atd..)

12. Zkuste si vygenerovat sestavy podle vámi zadaných parametrů (vyzkoušejte různé parametry).

Generování se provádí v menu „Sestavy -> Tisk sestavy“, kde si vybíráte parametry generované sestavy.

ZÁVĚR

Stále častěji se v běžném životě setkáváme s přístupovými a docházkovými systémy. Zejména v posledních letech dochází k velkému rozšíření těchto systémů především u velkých a středních firem, ale zájem začínají mít i menší a malé firmy. Důvodem je především stále nižší cena, ale i nesporné výhody, které tyto systémy mají a firmy si to velice dobře uvědomují. Rozšiřování těchto systémů pomáhá i lepší dostupnost biometrických systémů, které jsou čím dál tím více oblíbené pro jejich příznivou cenu, rychlost ověření a snadné použití.

V bakalářské práci jsem se zaměřil na nejpoužívanější metody autentizace pomocí hesla, tokenu a především na biometrickou metodu autentizace pomocí otisku prstu, kde jsem popsal metody, jakými se určuje přesnost a principy nejpoužívanějších biometrických snímačů otisku prstu. V praktické části bohužel nastal problém se systémem WinPack, který nebylo možné oživit a tedy ani propojit s biometrickou čtečkou Bioscrypt V-Pass a tak u tohoto bodu bylo splněno jen povolení Extended ID, které je nutné, proto aby systém WinPack mohl pracovat s biometrickou čtečkou. Dále jsem řešil propojení dvou terminálů TimeStation s programem Docházka Plus, kde jsem popsal postup propojení a možnosti nastavení a práci s docházkovými daty. Jako poslední jsem navrhl jednoduchou úlohu na, které si studenti můžou vyzkoušet práci s docházkovým systémem tvořeným terminály TimeStation a programem Docházka Plus.

ZÁVĚR V ANGLIČTINĚ

More and more often we meet in daily life with access and attendance systems. Especially in recent years have seen a great expansion of these systems, especially in large and medium-sized companies, but interest is beginning to have smaller and small companies. The reason for this is primarily a still lower price, but also the undisputed advantages that these systems are and the company's very well aware of this. The expansion of these systems also helps better availability of biometric systems, which are increasingly popular for their low price, speed validation and ease of use.

In the Bachelor's work I was focused on the most widely used authentication method using a password, token, and in particular on the biometrickou authentication method using fingerprint, where I described the method, which specifies the accuracy and the most commonly used principles of biometric fingerprint sensors. In the practical part, unfortunately, there is a problem with the system of WinPack, that could not be revived and, therefore, the link to the biometrickou reader, Bioscrypt V-Pass, and so at this point has been met only permit Extended ID, which is necessary, therefore, that the system could work with WinPack biometrickou reader. Furthermore, I solved the interconnection of two terminals TimeStation with Docházka Plus, where I described the process of linking and the possibility of setting up and working with attendance records. As the last, I´m proposed a simple task to which the students can try to work with attendance system formed by TimeStation terminals and program Docházka Plus.

SEZNAM POUŽITÉ LITERATURY

[1] *FMiB experienced* [online]. c2009 [cit. 2011-03-15]. Přístupové a docházkové systémy. Dostupné z WWW: <http://www.fmib.cz/pristupove-a-dochazkove-systemy.php>.

[2] *SystemOnLine* [online]. c2011 [cit. 2011-05-03]. Dostupné z WWW: <http://www.systemonline.cz>.

[3] *TETRONIK* [online]. c2011 [cit. 2011-03-15]. Dostupné z WWW: <http://www.tetronik.cz/>.

[4] *Z-WARE* [online]. c2008 [cit. 2011-03-15]. Dostupné z WWW: <http://www.z-ware.cz/>.

[5] *Business.center.cz* [online]. c2011 [cit. 2011-04-19]. Zákon č. 262/2006 Sb., zákoník práce. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/zakonik-prace/>.

[6] ŠKUBAL, Jaroslav; LIŠKUTÍN, Tomáš. *Epravo.cz* [online]. 3.12.2010 [cit. 2011-04-19]. Evidence pracovní doby. Dostupné z WWW: <http://www.epravo.cz/top/clanky/evidence-pracovni-doby-68481.html>.

[7] Osobní doklady x identifikace, autentizace, autorizace. *Crypto-World : Informační sešit GCUCMP* [online]. 15.1.2007, roč. 9, 1/2007, [cit. 2011-04-19]. Dostupný z WWW: <http://crypto-world.info/casop9/crypto01_07.pdf>. ISSN 1801-2140.

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

[9] *Papouch* [online]. c2011 [cit. 2011-04-22]. Dostupné z WWW: <http://www.papouch.com>.

[10] BENEŠ, Radek. *Access server* [online]. 2010-11-18 [cit. 2011-04-22]. Autentizační metody založené na biometrických informacích. Dostupné z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>.

[11] ČSN EN 50133-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 1: Systémové požadavky*. Praha : Český normalizační institut, 2001. 36 s.

[12] TEPLÝ, Tomáš. *Přístupové systémy*. [s.l.], 2010. 36 s. Přednáška. České vysoké učení technické. Dostupné z WWW: <http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/Prednaska%20ACS.pdf

[13] *Comfis.cz* [online]. c2008 [cit. 2011-05-01]. Technologie BIOMETRIKY. Dostupné z WWW: <http://comfis.cz/biometrie>.

[14] KOVÁČ, Petr. *Návrh biometrického identifikačního systému pro malou organizaci*. [s.l.], 2009. 85 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[15] *SOOM.cz* [online]. 2007 [cit. 2011-05-03]. Bezpečnost magnetických karet. Dostupné z WWW: <http://www.soom.cz/index.php?name=articles/show&aid=427>.

[16] *Bestaprint s.r.o.* [online]. c2011 [cit. 2011-05-03]. Plastové karty. Dostupné z WWW: <http://www.bestaprint.cz/karty>.

[17] *Oksystem* [online]. c2011 [cit. 2011-05-03]. Dostupné z WWW: <http://www.oksystem.cz>.

[18] PUST, Radim. Kontaktní a bezkontaktní čipové karty. *Sdělovací technika*. 2010, č. 3, s. 27-29. Dostupný také z WWW: <http://www.stech.cz/index.php?id_document=401157826&at=1>. ISSN 0036-9942.

[19] HANÁČEK, Petr; MATYÁŠ, Vašek. Čipové karty v informačních systémech. *Sborník konference Datakon 2003*. 2003, s. 15-22. ISSN 80-210-3215-4.

[20] *Wikipedia, the free encyclopedia* [online]. 2011 [cit. 2011-05-03]. Smart card. Dostupné z WWW: <http://en.wikipedia.org/wiki/Smart_card>.

[21] LAUCKÝ, Vladimír. *Technologie komerční bezpečnostiu II*. druhé. Zlín : [s.n.], 2007. 123 s. ISBN 978-80-7318-631-9.

[22] *TimeStation Uživatelská příručka*. [s.l.] : [s.n.], 25.06.2008. 24 s.

[23] *Elpo* [online]. c2011 [cit. 2011-05-12]. Dostupné z WWW: <http://www.elpok.cz>.

[24] *SOFTWARE DOCHÁZKA PLUS : příručka uživatele*. [s.l.] : [s.n.], c2011. 13 s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PIN	Personal Identification Number
ID	IDentification
IATA	International Air Transportation Association
ABA	American Bankers Association
bpi	Bits Per Inch
LoCo	Low Coercivity
HiCo	High Coercivity
ISO	lnternational Organization for Standardization
PVC	Polyvinylchlorid
ROM	Read Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
RAM	Random-Access Memory
SCOS	Smart Card Operating Systems
USB	Universal Serial Bus
MHz	Mega Hertz
RSA	Rivest -Shamir -Adleman
ECC	Error Checking and Correcting
DNA	Deoxyribonukleová kyselina
FAR	False Acceptance Rate
FRR	False Rejection Rate
FER	Failure to Enroll Rate
FTA	Failure To Acquire
FIR	False Identification Rate
FMR	False Match Rate

FNMR	False Non-Match Rate
CCD	Charged Coupled Device
LED	Light Emitting Diode
CMOS	Complementary Metal–Oxide–Semiconductor
TFT	Thin Film Transistor
RxD	Receive Data
TxD	Transmit Data
GND	GrouND
TCP/IP	Transmission Control Protocol / Internet Protocol
PZS	Poplachový zabezpečovací systém
ČSN	Česká technická norma
PC	Personal Computer

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: UKÁZKA SESTAVY Z PROGRAMU DOCHÁZKA PLUS

PODROBNÝ PŘEHLED O DOCHÁZCE

OD: 1.5.2011 DO: 31.5.2011 Datum přehledu: 13.5.2011

Lukáš Kolůch

Číslo zaměstnace: 101 Karta číslo: 101

Den	Přích.	Odch.	Přích.	Odch.	Výjimky		Odprac. hod.					
					Druh	Čas	Celkem	S přeruš.	Bez přest.	Norm.	Přesčas1	Přesčas2
1-Ne												
2-Po	06:30	15:03					08:33	08:03	07:33			
3-Út	06:28	15:00					08:32	08:04	07:34			
4-St	06:35	15:10					08:35	08:05	07:35			
5-Čt	06:29	15:15					08:46	08:19	07:49			
6-Pá	06:26	15:02					08:36	08:07	07:37			
7-So												
8-Ne												
9-Po	06:27	15:00					08:33	08:05	07:35			
10-Út	06:28	14:59					08:31	08:03	07:33			
11-St	06:26	15:00					08:34	08:01	07:31			
12-Čt	06:32	15:15					08:43	08:11	07:41			
13-Pá	06:26	15:02					08:36	08:08	07:38			
14-So												
15-Ne												
16-Po												
17-Út												
18-St												
19-Čt												
20-Pá												
21-So												
22-Ne												
23-Po												
24-Út												
25-St												
26-Čt												
27-Pá												
28-So												
29-Ne												
30-Po												
31-Út												
Dnů: 10	CELKEM ODPR.					00:00	85:59	81:06	76:06	187:00	-110:54	00:00
	CELKEM SOBOT						00:00		00:00			
	CELKEM NEDĚL						00:00		00:00			
	CELKEM ODPOLEDNÍ						00:00		00:00			
	CELKEM NOČNÍ						00:00		00:00			
	CELKEM SVÁTKŮ						00:00		00:00			