VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ AUTENTIZACE PŘEDMĚTEM A ZNALOSTÍ

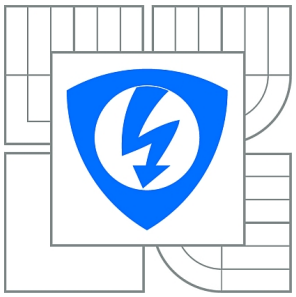
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE MICHAL ŠEVČÍK
AUTHOR

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ AUTENTIZACE PŘEDMĚTEM A ZNALOSTÍ

MODERN TOKEN-BASED AND KNOWLEDGE-BASED AUTHENTICATION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

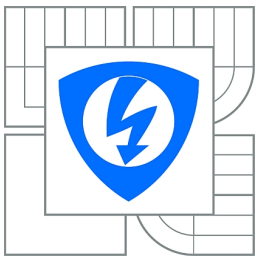
AUTOR PRÁCE — MICHAL ŠEVČÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. LUKÁŠ MALINA

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Michal Ševčík	***ID:***	119625
Ročník:	3	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Moderní autentizace předmětem a znalostí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se základními metodami autentizace. Vyhledejte a analyzujte používané autentizační předměty, jako jsou tokeny pouze s pamětí, inteligentní tokeny (smart cards), tokeny s logikou atd. Srovnejte jejich vlastnosti a parametry. Zhodnoťte jejich výpočetní a paměťové schopnosti. Navrhněte vhodný koncept autentizačního systému využívající autentizaci předmětem a znalostí. Návrh prakticky implementujte na přenosný programovatelný autentizační předmět (smart card). Výslednou funkční implementaci otestujte a proveďte výkonnostní a bezpečnostní analýzu.

DOPORUČENÁ LITERATURA:

[1] FINKENZELLER, Klaus. RFID handbook :fundamentals and application in contactless smart cards and identification /Chichester :Wiley & Sons,2003. 2nd ed. 427 s. : il. ISBN 0-470-84402-7.
[2] MAYES, Keith. Mayes. Smart Cards, Tokens, Security and Applications, 2009. 432 s. ISBN 1441944265.
[3] STALLINGS, William. Cryptography and Network Security. 4th edition. [s.l.] : [s.n.], 2006. 592 s. ISBN 0131873164.

Termín zadání:	7.2.2011	***Termín odevzdání:***	2.6.2011

Vedoucí práce: Ing. Lukáš Malina

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato bakalářská práce se zabývá moderní autentizací předmětem a znalostí. Převážně je zaměřena na autentizaci pomocí USB tokenů, Smart Java karet, Smart .NET karet a technologii NFC a jejich následné využití při autentizaci v místní síti.

KLÍČOVÁ SLOVA

Autentizace, Asymetrická kryptografie, USB tokeny, Čipové karty, Java karty, .NET karty, NFC

ABSTRACT

This bacherol thesis deals with a modern authentization using an object and knowledge. It mostly focuses on authentization by means of USB token, Smart Java Cards, Smart .NET Cards and NFC technology and their subsequent use in the authentization in a local network.

KEYWORDS

Authentization, Asymmetric cryptography, USB Tokens, Smart cards, Java cards, .NET cards, NFC

ŠEVČÍK, Michal *Moderní autentizace předmětem a znalostí*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 48 s. Vedoucí práce byl Ing. Lukáš Malina

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Moderní autentizace předmětem a znalostí“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

Poděkování

Tímto bych chtěl poděkovat vedoucímu své bakalářské práce Ing. Lukáši Malinovi za odborné vedení, cenné rady a čas strávený při konzultacích této práce a MUDr Radanu Havlíkovi, PhD. za podporu při psaní práce.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době plné informačních systémů se potřeba kvalitní a bezpečné autentizace stává přímo nutnou, abychom zajistili bezpečné užívání a kontrolu nad svým počítačem, elektronickou poštou, bankovním účtem a jinými dnes běžně používanými systémy.

Na úplném začátku své práce je probrána základní teorie k autentizaci. Je zde podrobně probráno, co je autentizace, čím se zabývá, jaké jsou její výhody a mnoho dalšího. Následně se kapitola člení do třech dalších podkapitol, ve kterých se zabývám autentizací předmětem, znalostí a žadatelem.

Na tuto kapitolu navazuje další, která má za úkol rozebrat základy kryptografie, především pak principy a typy asymetrické kryptografie. Je zde zároveň i zmínka o symetrické kryptografii a hashovacích funkcí.

Třetí kapitola je už zaměřená na problematiku autentizace čipovými kartami (Smart kartami) a USB tokeny. Je zde rozebrán princip jejich funkce, jejich využití v praxi a malé srovnání několika používaných typů.

Ve čtvrté kapitole se zaměřuji na technické porovnání technologií Javacard a .NET card. Jaké jsou jejich výhody a nevýhody, kdy je vhodné použít danou technologii pro programování karty.

Pátá kapitola se zabývá technologií NFC, zkoumá její parametry, bezpečnost a možnosti využití v autentizačním systému.

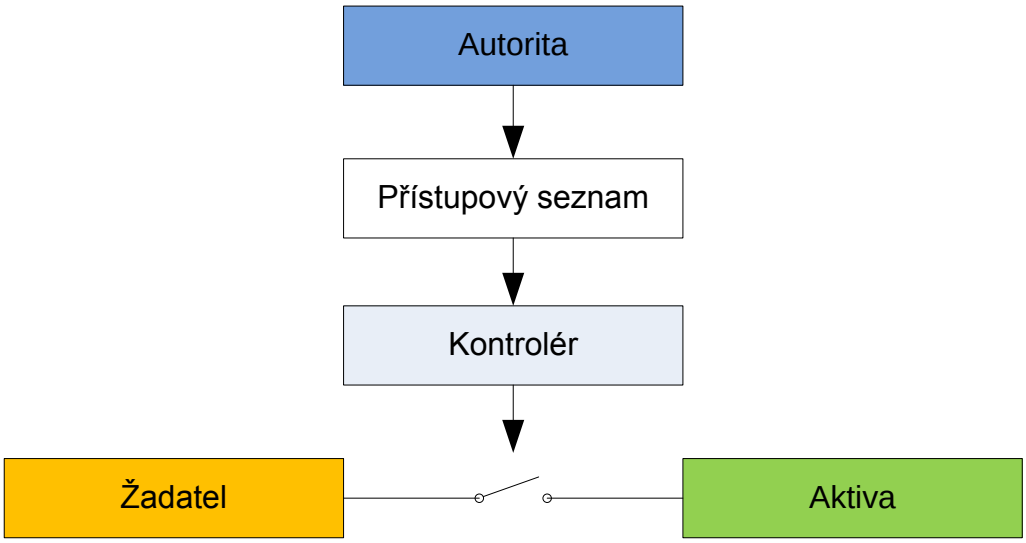
V poslední kapitola se zabývá návrhem využití autentizačních technologií v malé instituci. Součástí návrhu je přístupový, docházkový a stravovací systém. Navíc se v návrhu nachází lokální počítačová síť, do které se zaměstnanci přihlašují kombinací autentizace předmětu a znalosti. Všechny tyto systémy pak komunikují se servery, které jim zajišťují podporu v podobě aplikací, informací uložených v databázi ad. Všechny toto systémy jsou chráněny dvě hardwarovými firewally viz. obr. 6.1.

1 AUTENTIZACE

Autentizace pochází z německého slova die Authentisierung. Obecně autentizace slouží k ověření žadatelem předložených identifikačních údajů, tzn. ověření jeho proklamované identity a následnému řízení přístupu k některé z jeho poskytovaných služeb, nebo dat (aktiv). Z toho vyplývá, že hlavním úkolem autentizace je zamezení přístupu nepověřených osob, popř. útočníků, k chráněným službám a datům, nebo povolení přístupu osobám k tomu oprávněným.

Schéma řízeného přístupu je vidět na obr. 1.1, viz [3]

- **Žadatel** - je to osoba nebo zařízení, žádající o přístup k aktivům,
- **Autorita** - je to osoba nebo orgán, který rozhoduje kdo a v jakém rozsahu smí k aktivům přistupovat,
- **Přístupový seznam** - zde jsou uvedeny identifikační údaje uživatelů spolu s právy, která jim náleží,
- **Kontrolér** - osoba nebo zařízení povolující přístup k aktivům,
- **Aktiva** - cokoliv, co je organizací považováno za cenné (informace, zařízení, budovy, pověst organizace...).



Obr. 1.1: Schéma řízeného přístupu [3]

Princip řízeného přístupu je následující: Žadatel žádá o přístup k aktivům, při té příležitosti předá kontroléru svoje identifikační údaje. Ten ověří, zda tyto údaje náleží danému uživateli. Pokud souhlasí, tak si kontrolér v přístupovém seznamu najde daného žadatele, zjistí jeho přístupová práva a na jejich základě povolí žadateli přístup k aktivům. Pokud identifikační údaje nesouhlasí, je žadateli přístup k aktivům zamítnut.

1.1 Typy autentizace

Autentizaci dělíme na fyzickou, kdy jsou identifikační údaje žadatele o aktiva kontrolovány nějakou fyzickou osobou a na základě jejího rozhodnutí je žadateli povolen přístup k aktivům, nebo na automatizovanou, kde největším problémem je ověření, zda se žadatel nevydává za někoho jiného.

Autentizaci [3] dělíme na tří základní části:

- **Autentizace znalostí:** žadatel svoji identitu dokazuje znalostí (např. PIN, heslo),
- **Autentizace předmětem:** žadatel svoji identitu dokazuje předmětem (např. ID karta, Token, platební kartou, čipem...),
- **Autentizace žadatelem:** žadatel svoji identitu dokazuje svými charakteristickými vlastnostmi (např. otisky prstů, hlasem...).

Všechny třídy mají své výhody či nevýhody, proto se v praxi setkáváme nejčastěji s jejich různými kombinacemi.

1.1.1 Autentizace znalostí

V této oblasti autentizace je žadatel před povolením přístupu k aktivům dotazován na znalost určité přístupové informace, na jejímž základě je žadateli povolen přístup. Tuto informaci by měl znát pouze autorizovaný uživatel a před případnými útočníky by měla zůstat utajena. Uživatelé tuto informaci smějí mít uloženou pouze ve své paměti, proto musí být daná přístupová informace snadno zapamatovatelná. Což je v dnešní době plné informačních systémů velmi obtížné, protože uživatel většinou disponuje hned několika hesly (řetězec alfanumerických znaků) nebo autentizačních kódů (řetězce numerických znaků) od různých systémů (např. emailové schránky, ICQ, různých sociálních sítí, pinu od platební karty...). Proto se nelze divit, že si je uživatelé buďto někam zapisují, nebo používají stejná, většinou velmi jednoduchá hesla. Vezmeme-li v potaz další požadavky, které jsou v dnešní době kladeny na hesla:

- dlouhé aspoň 8 znaků,
- kombinace malých, velkých písmen, číslic i ostatních textových znaků,
- pro každý kontrolér jiné heslo,
- heslo nesmí mít nějaký význam,
- pravidelná obměna hesla,

zjistíme, že tento způsob autentizace představuje velké bezpečnostní riziko, proto se začal používat převážně v kombinaci i s jinou další třídou autentizace.

Druhou a silněji chráněnou metodou u autentizace znalostí obr. 1.2 je typ výzva-odpověď. Principem této metody je, že žadatel potvrdí vhodnou odpovědí kontro-

léru znalost reakce na jeho výzvu. Bezpečnost této metody je založena na tom, že kontrolér posílá výzvu pouze jednou a nikdy ne stejnou. Třetí a dnes posledním

Obr. 1.2: Autentizace pomocí znalosti

známým typem je autentizace nulové znalosti (v ang. Zero-Knowledge). Žadatel v této metodě prokazuje pouze svoji znalost hesla, ale nevyzrazuje žádnou jeho část kontroléru, ten na rozdíl od výše zmíněných metod heslo žadatele nezná. Metoda zachovává anonymitu uživatele. Podrobněji jsou tyto metody probrány v [3], [5], [6] a [25].

1.1.2 Autentizace předmětem

Jak je zřejmé z názvu této třídy, bude žadatel o přístup k aktivům prokazovat svoji identitu pomocí předmětu (tzv. Tokenu). Jelikož je přístupová informace uložena na paměťovém zařízení v Tokenu (např. čipová karta) nebo na jeho povrchu (např. průkaz totožnosti), je nutné, aby autorita zabezpečila daný předmět vhodnou technologií proti padělání a zároveň jej uživatel chránil před krádeží či ztrátou. Bezesporu největší výhodou tohoto typu autentizace je, že si uživatel nemusí pamatovat přístupovou informaci, která tím, že je uložena v Tokenu, může být delší a odolnější vůči slovníkovému útoku.

Podle [3], lze typy autentizačních předmětů dělit:

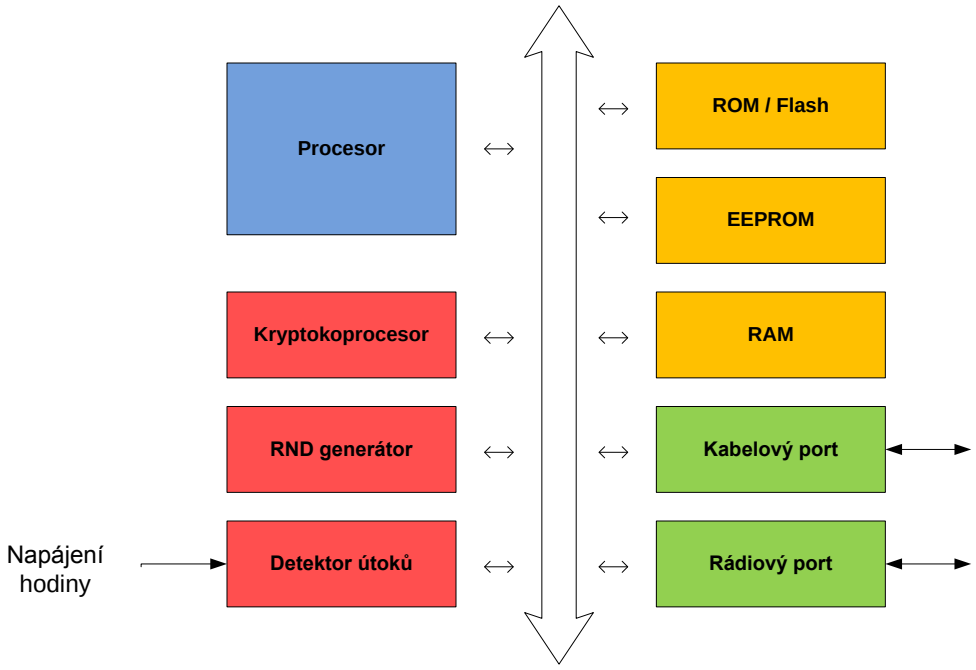
1. Úložiště,
    - s nechráněnými daty,
    - s chráněnými daty,

– s přístupovou ochranou,
– s kryptografickou ochranou,

2. Autentizátory.

Jako úložiště označujeme předměty, kde je autentizační informace pouze uložena, ale samotná autentizace se provádí na jiném zařízení. Úložiště se dělí na dvě třídy s nechráněnými a chráněnými daty. Z úložiště s nechráněnými daty lze autentizační informaci vyčíst bez jakéhokoliv omezení, použitím vhodného čtecího zařízení. Naopak u úložiště s chráněnými daty se už setkáváme s vyšším stupněm ochrany, kdy jsou autentizační informace chráněny jednoduchou kryptografickou šifrou (nutná znalost dešifrovacího klíče) nebo je k jejich vyčtení z paměti potřeba znalost hesla popř. klíče.

Autentizátory poskytují v sobě uloženým informacím nejvyšší možnou ochranu, protože se autentizační proces provádí přímo v nich a uložené autentizační informace se tak nemají jak dostat z autentizačního předmětu. Autentizátory (obr. 1.3) jsou jednočipové počítače, které pro vykonávání své činnosti musí obsahovat procesor (8, 16 nebo 32 bitový), paměť (ROM/Flash, EEPROM, RAM), komunikační rozhraní a občas i kryptografický koprocesor, který slouží k provádění složitějších kryptografických výpočtů. Jedná se např. o Smartkarty nebo USB tokeny obr. 1.4.



Obr. 1.3: Architektura autentizátoru [3]

Dle [5], se dělí typy autentizačních předmětů podle:

1. tvaru,
    - karty,
    - přívěsky,
    - náramky,
2. typu paměťového úložiště pro autentizační informaci,
    - magnetická páska / Wiegandův drát,
    - paměťový čip,
    - mikroprocesor,
3. komunikačního rozhraní,
    - snímač magnetického záznamu,
    - galvanické (kontaktní) rozhraní: ISO 7816, USB, I-Button,
    - rádiové (bezkontaktní) rozhraní: ISO 14443.

Obr. 1.4: Autentizační předměty

1.1.3 Autentizace žadatelem

Třetí možností je autentizace žadatelem. U toho způsobu autentizace dochází k porovnávání aktuálních charakteristik žadatele s uloženými záznamy, které se v terminálu nacházejí uloženy v kontejnerech nebo ve formě certifikátů autorizovaných příslušnou autoritou. Základními parametry pro to, aby se dal použit charakteristický rys žadatele k autentizaci, je jedinečnost a neměnnost dané charakteristiky. Kvůli požadavku na jedinečnost charakteristického rysu se používá tento typ autentizace pouze u osob. Autentizace založená na těchto údajích se nazývá Biometrická autentizace.

V současné době existují dvě třídy tohoto typu autentizace:

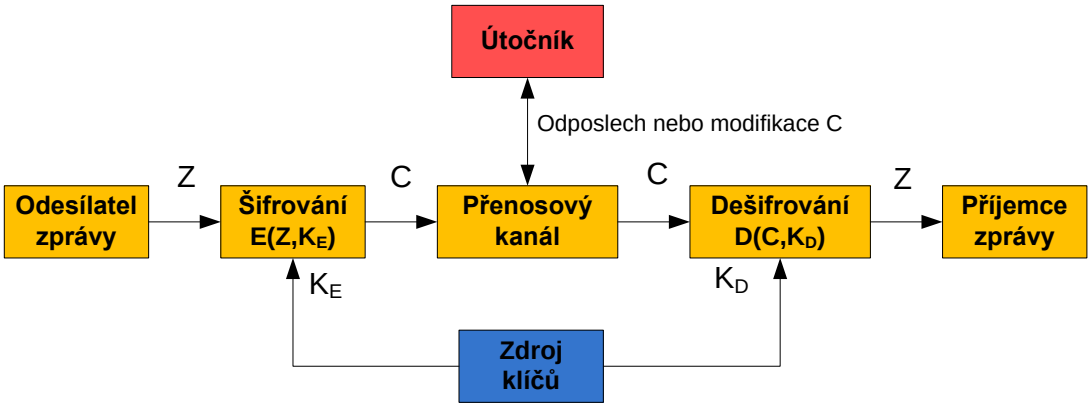
1. fyziologické metody,
2. behaviorální metody.

Fyziologické metody jsou metody, které se zaměřují na jedinečné a neměnné fyziologické charakteristiky člověka (např. otisky prstů, tvar obličeje...), zatímco

behaviorální metody jsou založeny na individuálnosti lidského chování (např. způsob psaní na klávesnici nebo způsob psaného podpisu). Mezi dnes nejpoužívanější biometriky patří ty založené na charakteristikách: otisky prstů, tvaru obličeje, oční duhovky, geometrie ruky, oční sítnice, hlasu, způsobu psaného podpisu, způsobu psaní na klávesnici. Více informací v [2].

2 KRYPTOGRAFIE

Je to věda, která má kromě jiného na starosti zajišťovat bezpečnost informačních systémů. Charakteristické pro ochranu kryptografického typu je, že přístup k aktivům je povolen po vyřešení určitého matematického problému. Matematické problémy jsou voleny tak, aby je případný útočník nemohl vyřešit v reálném čase. Žadatel o přístup k aktivům vlastní však nějakou tajnou informaci (znalost), s jejíž pomocí je schopen problém vyřešit a získat k nim přístup. Problematikou kryptografických ochran se zabývají dvě vědecké skupiny, jsou jimi kryptografie, která se zabývá konstrukcí kryptografických ochran, a kryptoanalýza, jež má na starosti jejich překonání. Kryptografické ochrany jsou nejrozšířenější používanou ochranou v informačních systémech, což je dáno jejich velmi snadnou implementací do systému. Dalšími jejich výhodami jsou jejich široké aplikační možnosti a vysoká odolnost vůči útokům. V praxi se používají na zaručení důvěrnosti a autentičnosti, nikoli k zajištění dostupnosti.



Obr. 2.1: Kryptografický systém [3]

Pojmy podle [3]:
Zpráva (Z) - informace, které jsou zakódovány všeobecně známým kódem,
Kryptogram (C) - jedná se o zašifrovaný text,
Šifrování (E) - je to proces transformace otevřené zprávy na zašifrovanou zprávu,
Dešifrování (D) - proces opačný k procesu šifrování,
Šifrovací klíč (K_E) - klíč používající se k šifrování odchozí zprávy,
Dešifrovací klíč (K_D) - klíč sloužící k dešifrování příchozí zašifrované zprávy.

Klíče sloužící k šifrování (K_E) a dešifrování (K_D) mohou být stejné ($K_\mathrm{E} = K_\mathrm{D}$), nebo různé ($K_\mathrm{E} \neq K_\mathrm{D}$).

Odesílatel v levé části kryptografického systému vysílá zprávu Z v nějakém známém jazyce. Tato zpráva je následně za pomoci šifrovacího klíče K_E ze zdroje klíčů

zašifrována do podoby kryptogramu C. Ten je následně přenášen přes přenosový kanál nebo uložen na záznamové médium. Na opačné straně kryptografického systému probíhá pomocí dešifrovacího klíče K_{D} dešifrování příchozího kryptogramu C do podoby zprávy Z. Dešifrovaná zpráva je pak předána příjemci zprávy. Největší nebezpečí ze strany útočníka hrozí přenášenému kryptogramu při jeho přenosu přes přenosový kanál nebo uložením na záznamové médium, kdy se útočník snaží získat nebo pozměnit obsah přenášeného kryptogramu C. Mezi šifrovacím a dešifrovacím klíčem platí [3], že $K_{\mathrm{D}} = \mathrm{f}(K_{\mathrm{E}})$, respektive $K_{\mathrm{E}} = f^{-1}(K_{\mathrm{D}})$. Na základě vlastností této závislosti dělíme kryptografické systémy do dvou základních skupin:

- Symetrické kryptosystémy - kryptografické systémy s tajným klíčem,
- Asymetrické kryptosystémy - kryptografické systémy s veřejným klíčem.

2.1 Asymetrické kryptosystémy

U kryptografických systémů s veřejným klíčem platí, že šifrovací klíče K_{E} a dešifrovací klíče K_{D} jsou navzájem od sebe různé a funkce $K_{\mathrm{D}} = \mathrm{f}(K_{\mathrm{E}})$, respektive funkce $K_{\mathrm{E}} = \mathrm{f}^{-1}(K_{\mathrm{D}})$ jsou výpočetně téměř nerealizovatelné. Minimální v dnešní době požadovaná délka klíčů je např. u RSA 1024 b, optimálně to je 2048 b, avšak chceme-li klíče využívat pro dlouhodobější účely, je vhodné použít klíče o délce 3072 b [13]. V asymetrickém kryptosystému je vždy jeden z dvojice klíčů zvolen jako tzv. tajný klíč a druhý jako tzv. veřejný klíč. To, který z klíčů je zvolen jako tajný nebo veřejný, nám určuje, zda systém bude zajišťovat důvěrnost či autentičnost. [3] Pokud je veřejným klíčem K_{E} a tajným klíčem K_{D}, tak zašifrovat přenášený kryptogram může kdokoliv, ale dekódovat jej může pouze příjemce vlastnící tajný klíč K_D. Tím je zajištěna důvěrnost a integrita přenášené zprávy. V opačném případě, je-li tajným klíčem K_{E} a veřejným klíčem K_{D}, může zprávu zašifrovat pouze odesílatel (majitel klíče K_{E}). Takový zašifrovaný kryptogram může pak dešifrovat kdokoliv se znalostí veřejného klíče K_{D}. Tak je zaručena autentičnost zprávy (princip digitálního podpisu).

Při návrhu asymetrického kryptosystému se využívá tzv. jednocestná funkce $y = \mathrm{f}(x)$, pro kterou je výpočet hodnoty y z argumentu x relativně jednoduchý, ale opačně výpočet hodnoty argumentu x ze znalosti hodnoty y je téměř nemožný. Podle typu použité jednocestné funkce se v praxi nejčastěji uplatňuje využití kryptosystémů založených na problému [3]:

- faktorizace čísla,
- diskrétního logaritmu,
- eliptických křivek.

Výhoda použití asymetrického kryptosystému spočívá v jednodušší distribuci

klíčů. Nevýhodou je pomalé šifrování a dešifrování. Z těchto důvodů se asymetrické systémy v praxi používají např. při přenosu klíčů pro symetrické systémy, výměně klíčů, šifrování krátkých zpráv, podepisování zpráv a autentizaci entit (data nebo osoba).

2.1.1 Kryptosystémy založené na problému faktorizace čísla

Tyto systémy jsou založeny na problému faktorizace čísla neboli problému rozkladu čísla na součin mocnin prvočísel. Nejpoužívanějším a nejznámějším kryptosystémem tohoto typu je kryptosystém označovaný zkratkou RSA. Byl vůbec prvním asymetrickým kryptosystémem vhodným pro podepisování a šifrování zpráv. RSA vznikl v roce 1977 a jméno dostal podle iniciál jeho autorů (Rivers, Shamir, Adlerman).

RSA se v praxi používá pro podepisování zpráv, čímž zaručuje autentičnost entit (data, zpráva, osoba), nebo při šifrování krátkých zpráv přenášejících klíče pro symetrické kryptosystémy či pro přenos hesel při autentizaci uživatelů. Konstrukce kryptosystému RSA [3]:

1. Nalezneme dvě velká prvočísla p a q.
2. Vypočítáme čísla: $n = (p \times q)$, $r = (p-1) \times (q-1)$.
3. Zvolíme veřejný šifrovací klíč e. Toto číslo musí být nesoudělné s číslem r.
4. Vypočítáme tajný šifrovací klíč $d = e - 1 \bmod r$.
5. Parametry e a n zveřejníme, ostatní parametry zůstanou tajné.

Postup při šifrování [3]:

1. Zprávu Z rozdělíme na bloky o stejné délce. Každý i-tý blok zprávy se chápe jako číslo z_i, kde musí platit, že $z_\mathrm{i} < n$.
2. Každý blok zprávy z_i zašifrujeme $c_\mathrm{i} = z_\mathrm{i}^\mathrm{e} \bmod n$.
3. Z bloků c_i poskládáme kryptogram C a odešleme jej adresátovi.

Postup při dešifrování [3]:

1. Kryptogram C rozdělíme na původní bloky c_i.
2. Každý blok kryptogramu dešifrujeme: $z_\mathrm{i} = z_\mathrm{i}^\mathrm{d} \bmod n$.
3. Z bloků z_i poskládáme zprávu Z.

Bezpečnost systému RSA je v dnešní době založena na nereálnosti rychlé faktorizace velkých čísel $n = 2^{1024}$ až 2^{2048}.

2.1.2 Kryptosystémy založené na problému diskrétního logaritmu

Logaritmické veřejné kryptosystémy [19], jsou to systémy založené na problému diskrétního logaritmu. Nejznámějšími systémy pracujícími s tímto problémem jsou systémy El Gamal, DSA a Diffie-Hellmanův.

Diffie-hellmanova funkce vznikla počátkem 70. let a uveřejnili ji pánové Diffie a Hellman, po nichž dostal tento kryptografický protokol jméno. Základ tvoří funkce $y = \mathrm{f}(x) = g^{\mathrm{x}} \bmod p$. Při znalosti hodnot p (velké prvočíslo) a g základu mocniny je výpočet hodnoty funkce y pro argument x relativně snadný, avšak inverzní výpočet (diskrétní logaritmus) je prakticky nemožný. Používá se k bezpečnému vytvoření klíčů pro symetrické kryptosystémy přes přenosový kanál.

DSA [22] (Digital Signature Algorithm) se roku 1994 stal americkým vládním standardem. Byl navržen institutem NSA (National Security Agency) pouze pro účely digitálního podpisu. Jeho nevýhodou je, že oproti RSA či kryptosystémech založených na problému eliptických křivek ho nelze využít k šifrování. DSA využívá tajný klíč velikosti 160 bitů a veřejný o velikosti 1024 bitů. Vzhledem k velmi malé velikosti tajného klíče je tento systém vhodný pro použití v čipových kartách. Výhodou tohoto systému je jeho volná šiřitelnost a bezpečnost založená na problému diskrétního logaritmu.

2.1.3 Systémy eliptických křivek

Na použití eliptických křivek pro kryptografické účely se přišlo roku 1985. Nezávisle na sobě na to přišli pánové Neil Koblitz (University of Washington) a Victor Miller (IBM). Systémy eliptických křivek využívají operace umocňování ve velkých konečných matematických grupách. Kryptografická síla těchto systémů je dána složitostí řešení úloh diskrétního logaritmu v těchto grupách. Obvykle jsou využívány grupy ze Z_{p} (celá čísla modulo nějaké prvočíslo), ale v těchto systémech je možné využít i jiných možností grup. Doposud jsou známy algoritmy pro některé varianty eliptických křivek. Více v [20].

2.2 Symetrické kryptosystémy

Symetrické (konvenční) šifrování je založeno na principu použití pouze jednoho klíče jak pro šifrování zprávy nebo informace, tak pro její dešifrování. Symetrické šifry jsou na rozdíl od těch asymetrických velmi rychlé a stejně jako jejich protějšek zaručují důvěrnost a autentičnost.

Při šifrování konvenční metodou se používají funkce, u kterých platí, že i při znalosti vstupního a zakódovaného textu je velmi obtížné vygenerovat příslušný klíč. Míra obtížnosti zjištění klíče je závislá zejména na délce použitého klíče. Velikost běžně používaného klíče se v dnešní době pohybuje okolo 128 bitů. Jedním z hlavních požadavků, které jsou kladeny na symetrické šifry, je, že zpráva, která je jimi zakódovaná, musí odolat útoku hrubou silou, jenž předpokládá vyzkoušení všech možných variant klíčů.

Výhodou této metody šifrování je její rychlost, s jakou je zpráva s použitím klíče zašifrována a dešifrována. Metoda se velmi dobře dá použít při šifrování dat, která se nikam neposílají. Naopak velmi velkou nevýhodou této metody je předání klíče použitého při komunikaci protější komunikující straně přes přenosový kanál. Další nevýhodou je pak, že při vyšším počtu komunikujících entit dochází k problému se správou klíčů.

Mezi symetrické kryptografické systémy patří algoritmy: DES (délka klíče 56 bitů), 3DES (s délkou klíče 168 bitů), Blowfish (klíč 256 bitů) a další jako IDEA (128 bitů), CIFER (16 bitů).

Symetrické šifry dělíme na [3]:

- proudové šifry,
- blokové šifry.

Více informaci o symetrických šifrách v [3], [4] a [14].

2.3 Hashovací funkce

Hashovací funkce (ang. Hash) se využívá u asymetrických kryptosystémů ke zrychlení činnosti šifrování a dešifrování. Jedná se o jednocestnou kompresní funkci, která ze zprávy o proměnlivé délce vygeneruje kód o pevné délce několika desítek bitů (128 b, 160 b, 192 b nebo 256 b) tzv. Hash, neboli kontrolní součet. Výpočet hashe není složitý, ale zjistit z něj původní zprávu by mělo být v reálném čase nemožné.

Požadavky na Hash [3]:

- aby pravděpodobnost existence dvou zpráv se stejným hašem byla prakticky nulová,
- pro nějakou danou hodnotu haše musí být prakticky nemožné najít zprávu se stejnou hodnotou haše.

Hashovaní funkce musí zajistit, změní-li se vstupní řetězec byť pouze o jeden bit, změní se úplně výstupní řetězec. Nejznámější hashovaní funkce jsou MD5 (16 B), SHA-1 (20 B), SHA-2 (64 B). Příklad změny řetězce při použití hashovaní funkce MD5 viz Tab. 2.1.

Tab. 2.1: Příklad funkce MD5

Heslo	Funkce MD5
Token123	2c81b0a10a352201d7d360adb4215e49
token123	1fc34072660678ab6395a990ca908258

Z tabulky je patrné, že i malá změna hesla úplně změní výstupní řetězec.

3 AUTENTIZACE PŘEDMĚTEM

V této kapitole se zaměříme na dva nejpoužívanější předměty při užití autentizace předmětem, a to autentizaci čipovými kartami (Smart karty) a USB Tokeny.

3.1 Druhy Tokenů

Svým vzhledem připomínají USB flash disk, ale jejich architektura je totožná s popsanými čipovými kartami (některé tokeny mají stejný čip jako modely Smart karet). USB token slouží jako úložiště soukromých klíčů, certifikátů a jiných tajných informací. Jeho úkolem je zajistit, aby nebyly tyto tajné informace zkopírovány nebo jinak zneužity. Proto se při podepisování např. emailové zprávy posílají podepisovaná data do tokenu, kde se zašifrují tajným klíčem. Před zneužitím cizí osobou jsou chráněny PINem.

Velikost paměti u USB tokenů se pohybuje nejčastěji okolo 8 kB, 16 kB, 32 kB a výjimečně i 64 kB. Pro komunikaci využívá token USB port, který se dnes nachází v každém počítači a nepotřebuje, tak jako čipové karty, speciální čtečky s příslušnými ovladači. Postačí ovladače pro USB port. Tokeny bývají chráněny i proti mechanické manipulaci (mechanickému napojení na obvody tokenu). Nejčastěji zalepením obvodu (viz obr. 3.1), zalitím epoxidem, ty dražší se po mechanickém otevření skořápky, tvořící tělo USB tokenu, rozpadnou. Můžeme se také setkat i s nijak nechráněnými

Obr. 3.1: Otevřený USB token

levnějšími typy. Úlohou skořápky je také chránit čip před mechanickým poškozením, lidským potem, rozlitou tekutinou a jinými vnějšími vlivy.

Více informací naleznete v [12] a [24].

Tab. 3.1: USB tokeny a jejich parametry

	Paměť pro data	Max. délka klíčů	Algoritmy	Cena/ks
Ikey 4000	64 kB	RSA 2048 b	RSA, 3DES, AES(128,192,256) DH, SHA-1	1765 kč/1 ks
Aladdin eToken klíčů	64 kB	RSA 2048 b	RSA, DES, SHA1, 3DES, SHA-256	209 kč/100 ks
Feitian Technologies ePass 2000	32 kB	RSA 2048 b	RSA, DES, 3DES, SHA-1	456 kč/100 ks
A-Key 3600	128 kB	RSA 2048 b	AES (128b,256b), RSA, SHA-1	570 kč/100 ks
Gemalto Smart Enterprise Guardian	2 GB	RSA 2048 b	RSA, DES, 3DES, HMAC, SHA-1, SHA-2, MD5, AES 256	1145 kč/1 ks
Ikey 3000	32 kB	RSA 1024 b	RSA, MD5, MD2, SHA-1, MD160, RC2, RC4, DES, 3DES	1540 kč/1 ks

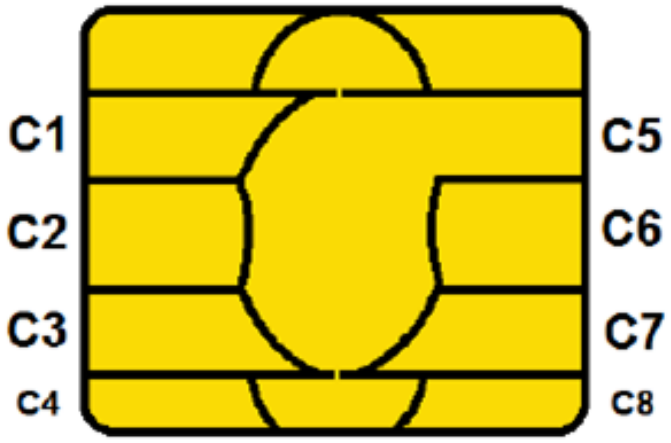
3.2 Druhy čipových karet

Existuje plno druhů čipových karet, které jsou poměrně malé a přenosné. Často jsou v podobě plastových karet, vyrobených z polyvinylchloridu (PVC), akrylonitrilbutadienstyrenu (ABS) nebo polykarbonátu.

Velikost těchto karet je standardizována podle normy ISO - 7810 typ ID-1 s rozměry $85,60 \times 53,98 \times 0,76\,\text{mm}$. Integrovaný obvod provádí příjem, zpracování dat a vrací požadované informace. Pod standardem ISO jsou označovány jako IIC (Integrated Circuit Card).

Ty obsahují integrovaný obvod s procesorem a chráněným paměťovým prostorem, kam lze uložit soukromý klíč s certifikátem. Ty jsou zalisovány v kartě a s vnějším okolím mohou komunikovat třemi způsoby, dotykově, bezdotykově nebo tzv. hybridním způsobem.

Při komunikaci za pomocí dotyku se využívá kontaktních plošek umístěných na kartě (viz obr. 3.2). U kontaktních karet je nutné pro umožnění komunikace vložit kartu do čtecího zařízení, čímž dojde k fyzickému propojení čtecího zařízení a kontaktů karty. Každý z kontaktů má svůj specifický význam, který je následující: C1 = VCC (vstupní napájení), C2 = RST (reset signálů), C3 = CLK (poskytuje hodinový signál kartě), C5 = GND (zem), C6 = VPP (programovací napětí), C7 = I/O (Sériový vstup a výstup), C4 a C8 jsou volný pro budoucí použití. Nevýhodou tohoto typu komunikace je, že po jisté době dochází k opotřebování kontaktů. Výhodou je bezpečnější komunikace, proto se tohoto typu karet využívá při peněžních transakcích, typicky při použití platební karty.



Obr. 3.2: Rozložení pinů čipové karty

Bezdotykové, neboli také bezkontaktní typy karet, nevyužívají ke své činnosti kontaktu s čtecím zařízením, ale stačí, aby se nacházely v jeho blízkosti. K tomuto

účelu komunikace musí obsahovat i vestavěné antény, které zprostředkovávají bezkontaktní komunikaci. Tyto bezkontaktní karty, je možné rozpoznat několika způsoby, buďto podle tvaru kontaktních plošek, které jsou obdélníkové, nebo podle kružnice, která kopíruje obvod čipové karty. Tento typ karty řeší problém u předchozího typu s opotřebením kontaktů a využívá se tam, kde je potřebná rychlá manipulace, např. při vchodu do budovy, místnosti, ale také v poslední době i hromadné dopravě.

Třetím a posledním typem jsou tzv. hybridní karty, které jsou kombinací obou předešlých typů. Tento typ karty řeší situace, kdy je zapotřebí, aby karta sloužila k provádění hned několika služeb zároveň. Příkladem jejich využití může být případ u nás na VUT, kdy je tuto kartu možné využít jako platební, využívá se dotykový způsob komunikace a zároveň i jako kartu sloužící pro umožnění vstupu do laboratoří, kopírování na kopírce, jídelní kartu a knihovnickou průkazku. Základní dělení čipových karet je následující:

- **paměťové čipové karty** - obsahují integrovaný obvod sloužící pouze k ukládání dat a nemá zabezpečující mechanismy,
- **procesorové čipové karty** - konstrukce je stejná jako u paměťových čipových karet, navíc obsahují procesor, bývají označovány jako Smart karty,
- **kryptografické čipové karty** - obsahují oproti procesorovým čipovým kartám ještě navíc kryptografický koprocesor sloužící ke zpracování kryptografických výpočtů, které by musel provádět procesor a provádí je efektivněji nežli procesor.

Čipové karty slouží k ověření identity uživatele a používají se v mobilních telefonech (SIM karty), bankovních systémech (platební karty), dále umožňují přístup do budovy, místností, přihlášení k počítači atd. Podrobnější informace naleznete v [21].

Tab. 3.2: Smart karty a jejich parametry

	Paměť pro data	Max. délka klíčů	Algoritmy	Koprocesor	Cena/ks
Gemalto Classic TPC IS v2	32 kB	RSA 2048 b	RSA, 3DES, SHA-256 SHA-1	ANO	203 kč/100 ks
Gemalto Classic TPC IM CC	64 kB	RSA 2048 b	RSA, 3DES, SHA-1, SHA-256	ANO	350 kč/100 ks
Smart Card 400	64 kB	RSA 2048 b	RSA, DSA, DES, DH, SHA-1	ANO	374 kč/100 ks
Smart Card 360	32 kB	RSA 2048 b	DES, 3DES, RSA, SHA-1, DSA, DH	ANO	358 kč/100 ks
Mifare Smart MX	20 - 144 kB	RSA 5024 b	RSA, DES, SHA-224, SHA-1,DH, SHA-256, ECC, AES,	ANO	
Mifare DESFIRE 4K	4 kB	DES 168 b	DES (56 b, 112 b, 168 b), 3DES, AES (128 b)		55 kč/100 ks

4 ROZBOR A POROVNÁNÍ ČIPOVÝCH KARET

Tato kapitola se zabývá rozborem a porovnáním technických parametrů programovatelných smart karet, především pak Java a .NET kartami, které jsou dnes nejrozšířenější.

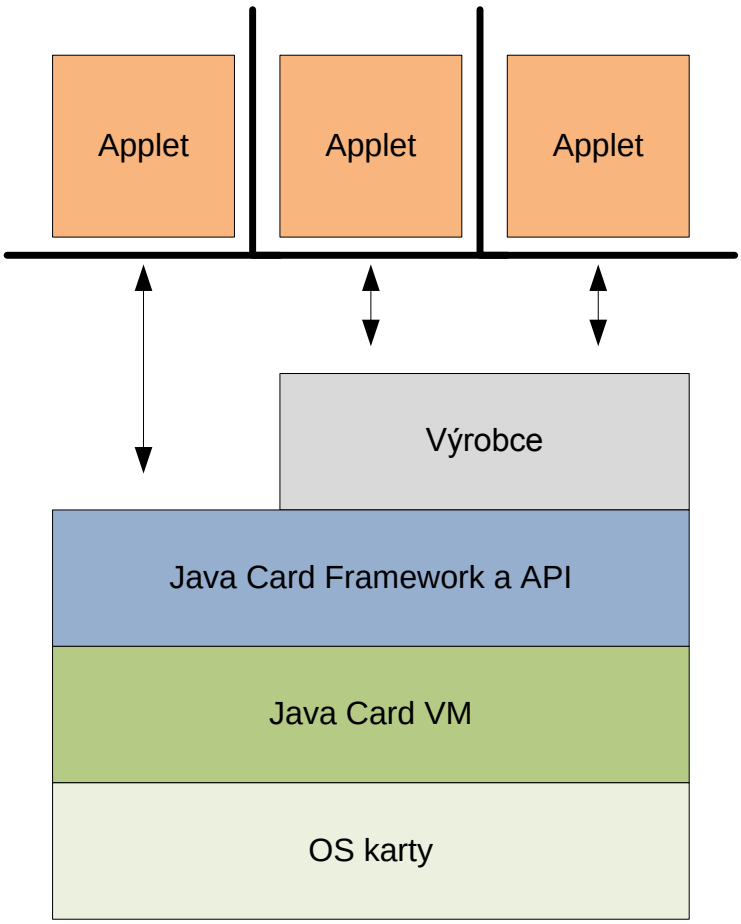
4.1 Java karty

Technologie Java Card [9] umožňuje využívat čipové karty a další jiná zařízení, s omezenou pamětí a výpočetní schopností, pro spuštění tzv. appletu (program napsaný v jazyce Java). Tato technologie poskytuje čipovým kartám výrobců bezpečnou platformu s možností vzájemné spolupráce různých systémů (aplikací), které si poskytují vzájemně služby a dosahují tak vzájemné součinnosti. Z předchozí věty vyplývá, že tato technologie umožňuje umístnění více appletů na daném zařízení tzv. Multifunkčnost.

Java Card API (Application Programming Interface) umožňuje přenositelnost aplikace, která je určena pro smart kartu i na jiné platformy, např. USB tokeny, které byly vyvinuty s využitím technologie Java Card, stejně jako u Java appletů běžících na různých počítačích. Stejně jako v Javě je to provedeno za pomoci Java Card VM (Virtual Machine) a runtime knihovny [10]. Objektově orientované programování umožňuje vývojářům vytvářet, testovat a nasazovat aplikace a služby rychle a zároveň bezpečně. Což v konečném důsledku snižuje náklady na vývoj, větší konkurenceschopnost produktu na trhu a zvyšuje význam pro zákazníky. Další důležitou výhodou je kompatibilita Java Card API s mezinárodními standardy ISO/IEC 7816 (poslední aktualizace proběhla v r. 2005). Tato norma [8] definuje různé aspekty čipových karet, včetně jejich fyzikálních vlastností, fyzických kontaktů, elektronický signálů, přenosových protokolů, příkazů, bezpečnostní architektury, identifikátorů aplikací a společných datových prvků. Další výhodou je její dynamičnost. Tato vlastnost umožňuje bezpečnou instalaci nových aplikací i po vydání karty, čímž je možné reagovat na měnící se potřeby zákazníků [9].

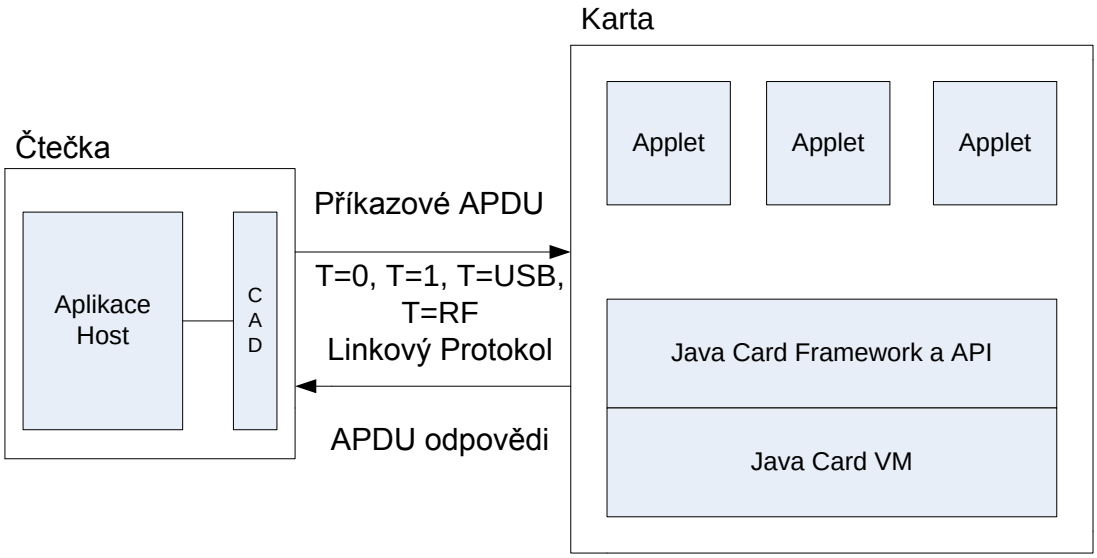
Bezpečnost je určena už samotnou architekturou této technologie obr. 4.1, která k ochraně tajných informací využívá metodu zapouzdření dat, kdy data jsou uložena v samotné aplikaci, která se spouští v izolovaném prostředí (Java Card VM), které je oddělené od základního operačního systému a hardwaru. Další metodou podporující bezpečnost je applet firewall. Ten se využívá na vzájemné oddělení aplikací od sebe, protože Java Card VM většinou spravuje hned několik aplikací, které obsahují citlivá data. Poslední metodu, kterou technologie Java Card využívá, je šifrování. Java Card využívá tak jako i jiné platformy DES, RSA, 3DES, AES a další. Od poslední verze

Java Card 3.0.1 již dokonce podporuje klíče RSA dlouhé 4096 b, algoritmus SHA-2 pro podpisy a další užitečné věci [11].



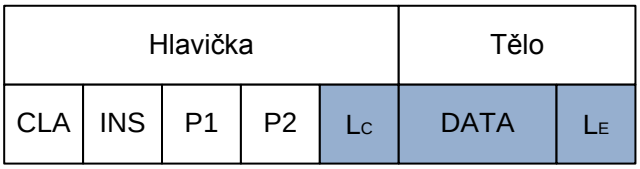
Obr. 4.1: Architektura Java Card [17]

Java karty komunikují s počítačem nebo terminálem prostřednictvím svých datových balíčků APDU (Application Protocol Data Units) přes čtecí zařízení CAD (Card Acceptance Device) viz obr. 4.2. APDU [17] obsahuje buďto příkaz, nebo odpověď. Karta je vždy pasivní, komunikace probíhá podle modelu master-slave. Karta nikdy neinicializuje komunikaci, čeká na příchod příkazu od terminálu, ten zpracuje a odpoví. APDU příkazy a odpovědi jsou mezi terminálem a kartou vyměňovány střídavě.



Obr. 4.2: Komunikace prostřednictvím APDU [17]

Příkazové APDU:



Obr. 4.3: Příkazové APDU [17]

Povinné parametry:

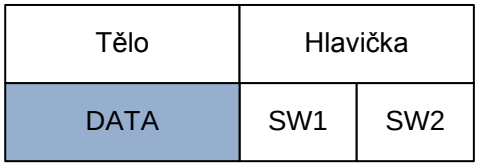
- CLA (Class Byte) - používá se pro identifikaci aplikace,
- INS (Instruction Byte) - identifikuje instrukční kód,
- P1, P2 (Parametr 1, 2) - obsahuje rozdělený příkaz.

Nepovinné parametry:

- L_C (Length of data to be transfered) - udává velikost pole DATA v příkazu,
- DATA - přenášená data,
- L_E (Length of data expected) - očekávaná velikost pole DATA v odpovědi.

Všechna pole kromě pole DATA má velikost 1 Byte, velikost pole DATA udává pole L_C.

Odpověď APDU:



Obr. 4.4: Odpověď APDU [17]

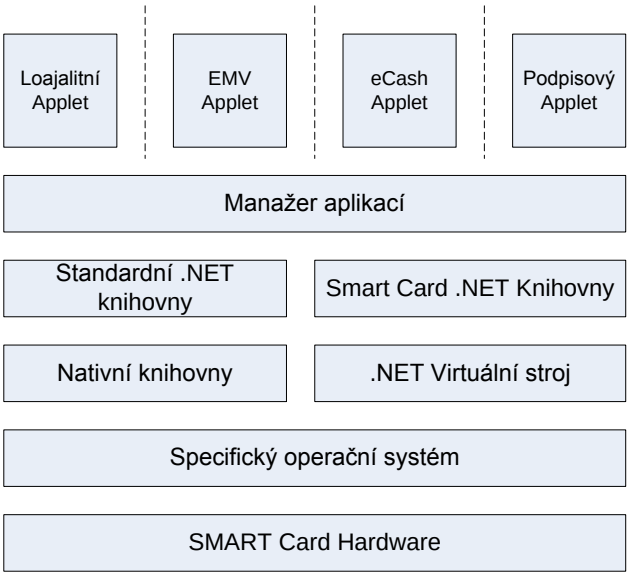
- DATA - pole obsahující data (nepovinné),
- SW1, SW2 (Status Word) - udává stav jak proběhl příkaz na kartě (povinné).

Velikost pole DATA udává pole L_{E} v příkazu APDU a velikost SW1 a SW2 je 1 Byte.

4.2 .NET karty

Technologie .NET je název pro soubor technologií v softwarových produktech, jenž tvoří platformu, která je dostupná pro web, OS Windows, kapesní počítače tzv. pocket PC nebo mobilní telefony s operačním systémem Windows Mobile. Technologie Smartcard .NET [15] vyvinul Hive Minded, jako pokus zavést platformu .NET do čipových karet a dalších zařízení. Tato platforma se vyvíjela v návaznosti na mezinárodní normu ECMA 335 / ISO 23271, která obsahuje specifikace .NET a .NET framework.

Jedná se o multiaplikační prostředí, které umožňuje, aby na kartě spolupracovalo více aplikací. Aplikace pro tuto platformu mohou být za použití různých programovacích jazyků, jako jsou: C#, C++, Visual Basic, JavaScript, J# a podobně. Dokonce umožňuje kombinací více programovacích jazyků v kódu jedné aplikace, protože je poté stejně následně převedena do .NET kódu. Čipové karty s platformou .NET mají tak jako platforma Java Card k dispozici virtuální stroj (prostředí), který využívá koncept aplikační domény k izolování právě bežících aplikací, a zabraňuje neoprávněnému sdílení dat mezi aplikacemi. Smartcard .NET platforma dokonce podporuje proud celých 64 b čísel ověření kódu karty. Vnitřní architekturu čipové karty .NET můžete vidět na obr. 4.5



Obr. 4.5: Architektura čipové karty .NET

Podstatným rozdílem mezi platformou JavaCard a .NET je, že .NET platforma neumožňuje při komunikaci a programování ovlivnit obsah APDU paketů. .NET čipová karta se navenek chová jako server, se svými URI (Uniform Resource Identifier). Metody naprogramované v kartě se pak volají jako metody daného serveru,

tzn. programátor nevytváří žádné konstrukce příkazů APDU. I když se to navenek nezdá, jsou na platformě .NET APDU příkazy přítomny, ale nacházejí se na nižší vrstvě. Proto, aby vůbec došlo ke komunikaci, dochází při kompilaci programu k vygenerování knihovny, která má pak na starost rozbalování a zabalování volání metod do APDU [23].

4.3 Porovnání

Obě popsané technologie mají své výhody i nevýhody. Záleží proto na každém programátorovi, kterou technologii bude chtít využít k programování. Obě dvě technologie jsou multiaplikačním prostředím, což znamená, že na nich může fungovat hned několik aplikací zároveň. Aplikace (applety) v Javacard jsou psané pouze v jednom programovacím jazyce (java), což má své výhody i nevýhody. Při programování aplikací se většinou pracuje v týmu, kde si mezi sebou programátoři rozdělí, kdo kterou část aplikace naprogramuje. Z toho vyplývá, že všichni programátoři musí znát daný programovací jazyk. Naproti tomu programátorský tým programující s technologií .NET má možnost napsat své části aplikace v různých programovacích jazycích, protože ty jsou stejně následně přeloženy do .NET kódu. Tato výhoda je ale zároveň i nevýhodou, chce-li programátor pochopit, jak pracuje jiná část programu, která není přímo napsána v programovacím jazyce, který ovládá. Výhodou programovat v platformě Javacard je také to, že se jedná o otevřený systém (open source), kdy jsou programátorovi k dispozici všechny kódy, což je výhodné převážně tehdy, když se dotyčný podílí na upgradu nebo vyladění chyb v kódu. Oproti tomu je platforma .NET částečně uzavřeným systémem. Některé jeho části kódu jsou veřejně známé, ale některé spadají pod autorský zákon, takže nejsou obyčejným programátorům k dispozici.

V oblasti použitého hardwaru u čipových karet se tyto technologie od sebe příliš neliší. Obě technologie zvládají 8 b, 16 b a 32 b procesory. V oblasti pamětí je tomu také tak. Ovšem ohledně správy a využití paměti by na tom mohla být o něco lépe .NET technologie mající navíc aplikaci, která by měla zefektivnit přidělení a uvolnění paměti. Toto je jenom moje domněnka, jelikož toto tvrzení není podložené žádným měřením.

5 TECHNOLOGIE NFC

Near Field Communication, zkráceně NFC. Jedná se o komunikační technologii, sloužící pro bezdrátovou komunikaci mezi zařízeními na velmi krátkou vzdálenost 1-4 cm, teoreticky až do 10 cm. Je především určena pro použití v mobilních telefonech, ale lze ji využít také např. v tabletech aj. NFC je rozšířením standardu ISO / IEC 14443, ve které jsou zařazeny technologie RFID (Radio Frequency Identification) a bezkontaktní karty a ISO 18092. RFID je technologie využívající pro komunikaci mezi zařízeními radiofrekvenční vlny, s jejichž pomocí zařízení A dopraví příkaz k zařízení B, které poté, až zpracuje příkaz, odpoví stejným způsobem. Technologie NFC je právě kombinací těchto dvou rozhraní SmartCard a bezdrátového komunikačního zařízení.

Komunikační rozhraní může pracovat v několika režimech. Ty se od sebe liší tím, zda vytváří vlastní radiofrekvenční (RF) pole nebo zda zařízení získává energii z RF pole vytvořeného jiným přístrojem. Generuje-li přístroj vlastní RF pole, říkáme o něm, že je aktivní. Pokud toto pole nevytváří, jedná se o pasivní zařízení. Aktivní zařízení se liší od těch pasivních v tom, že obsahují vlastní napájecí zdroj, zatímco u pasivního zařízení vzniká potřebné napájení působením magnetického pole na anténu, stejně jako u RFID systémů [18]. Pokud spolu vzájemně komunikují dvě zařízení, jsou možné tři druhy konfigurace viz tab. 5.1. Tyto konfigurační režimy

Tab. 5.1: Komunikační konfigurace

Zařízení A	Zařízení B	Popis
Aktivní	Aktivní	Jedná se o P2P komunikaci, kdy zařízení A vysílá data tím, že generuje své RF pole, zařízení B v tu dobu žádné RF pole nevytváří. Pole RF jsou střídavě generována podle toho, jak probíhá komunikace.
Aktivní	Pasivní	RF pole generuje pouze Zařízení A
Pasivní	Aktivní	RF pole generuje pouze zařízení B

jsou důležité, protože to, zda jste aktivní nebo pasivní, určuje, jakým způsobem jsou data přenášena.

Nachází-li se zařízení v aktivním režimu, je základní RF signál (f = 13,56 MHz) modulován s přenášenými daty v závislosti na kódovacím režimu. Rychlost přenosu se pohybuje od 106 kbit/s do 424 kbit/s. Pokud je přenosová rychlost 106 kbit/s, využívá kódovací systém tzv. modifikovaného Millerova kódování. Pokud je přenosová rychlost větší než 106 kbit/s používá se kódovací schéma Manchester. V obou kódových schématech se posílá jediný datový bit v pevném časovém úseku. Tento

časový úsek je rozdělen na dvě poloviny, kterým se říká půl bity. V Millerově kódování je nula kódována s pauzou v první polovině bitu a bez pauzy v druhé polovině bitu. Modifikované Millerovo kódování se tomuto kódování nul vyhýbá a první polovina bitu navazuje přímo na tu druhou bez pauzy. Kódování Manchester je téměř stejné, ale na místo pauzy v první nebo druhé polovině bitu je celá jedna polovina bitu pauza nebo je modulována. Při přenosu závisí vedle systému kódování také na úrovni modulace a na přenosové rychlosti. Pro přenosovou rychlost 106 kbit/s se používá 100 % modulace, což znamená, že v pauze RF signálu je aktuálně nula. V pauze se nevysílá žádný RF signál. Pro přenosovou rychlost větší než 106 kbit/s se používá poměr modulace 10 %, to znamená, že v pauze RF signálu není nula, ale přibližně 82 % úrovně signálu neobsahujícího pauzu. Tento rozdíl je důležitý z bezpečnostního hlediska.

V pasivním režimu jsou data vždy kódována pomocí metody Manchester s modulací 10 %. Pro přenosovou rychlost 106 kbit/s se pro modulaci používá dílčí nosná frekvence, při vyšších přenosových rychlostech než je 106 kbit/s je základní RF signál modulován.

Kromě aktivního a pasivního režimu existují v NFC komunikaci ještě dva další režimy iniciátor a cíl. Komunikace pak vypadá takto: Zařízení A posílá zprávu jinému zařízení B a zařízení B mu odpovídá. Není možné, aby zařízení B zaslalo zařízení A data bez toho, že by předtím zařízení B obdrželo zprávu od zařízení A, na kterou by mohlo odpovědět. V tomto případě se zařízení A, které komunikaci zahájilo, nazývá iniciátor. Role ostatních zařízení je cíl. Při komunikaci mohou zařízení zastávat různé kombinace těchto režimů. Není možná pouze kombinace iniciátor a pasivní režim. Zde je potřeba zdůraznit, že jeden iniciátor může komunikovat s více zařízeními (cíli). Komunikace pak probíhá tak, že všechna cílová zařízení jsou povolena ve stejný moment a před odesláním zprávy iniciátor teprve vybere příslušné zařízení pro příjem jeho zprávy. Ostatní zařízení, až na vybrané, tuto zprávu ignorují. Proto není možné současně ve stejný čas posílat data do více než jednoho cílového zařízení [7].

Aplikace pro technologii NFC dělíme do tří skupin:

- **bezkontaktní tokeny**,
- **platby a ticketing**,
- **spárování zařízení**.

Bezkontaktní tokeny

Tato skupina zahrnuje všechny aplikace používající technologii NFC k přijímání dat od pasivních tokenů (čipová karta, RFID štítek, klíčenka, aj.). U těchto zařízení

můžeme proto předpokládat, že budou mít omezený výpočetní výkon, proto na nich nebude možné spustit žádné složitější protokoly.

Primárním využitím by pro tyto systémy mohlo být ukládání informací do svých pamětí, které by pak mohla číst aktivní zařízení.

Příkladem tohoto využití jsou NFC smart plakáty [16]. Ty se liší od klasických plakátů v tom, že se v jejich těle nebo na povrchu nachází čitelné NFC značky. NFC smart plakát může mít mnoho podob:

- plakát,
- billboard,
- stránka časopisu,
- 3D objekt.

Společným prvkem pro tyto možnosti je, že všechny obsahují NFC tag, v němž jsou uloženy informace ve formátu NDEF (NFC Data Exchange Format). Tento NFC tag je přečten v případě, že se do jeho blízkosti dostane nějaké aktivní NFC zařízení. Abychom předešli problému s hledáním místa na plakátu, odkud je možné tag přečíst, je důležité, aby každý plakát měl toto místo označené tzv. TouchPointem. TouchPoint je označen symbolem, kterému se říká N-MARK.

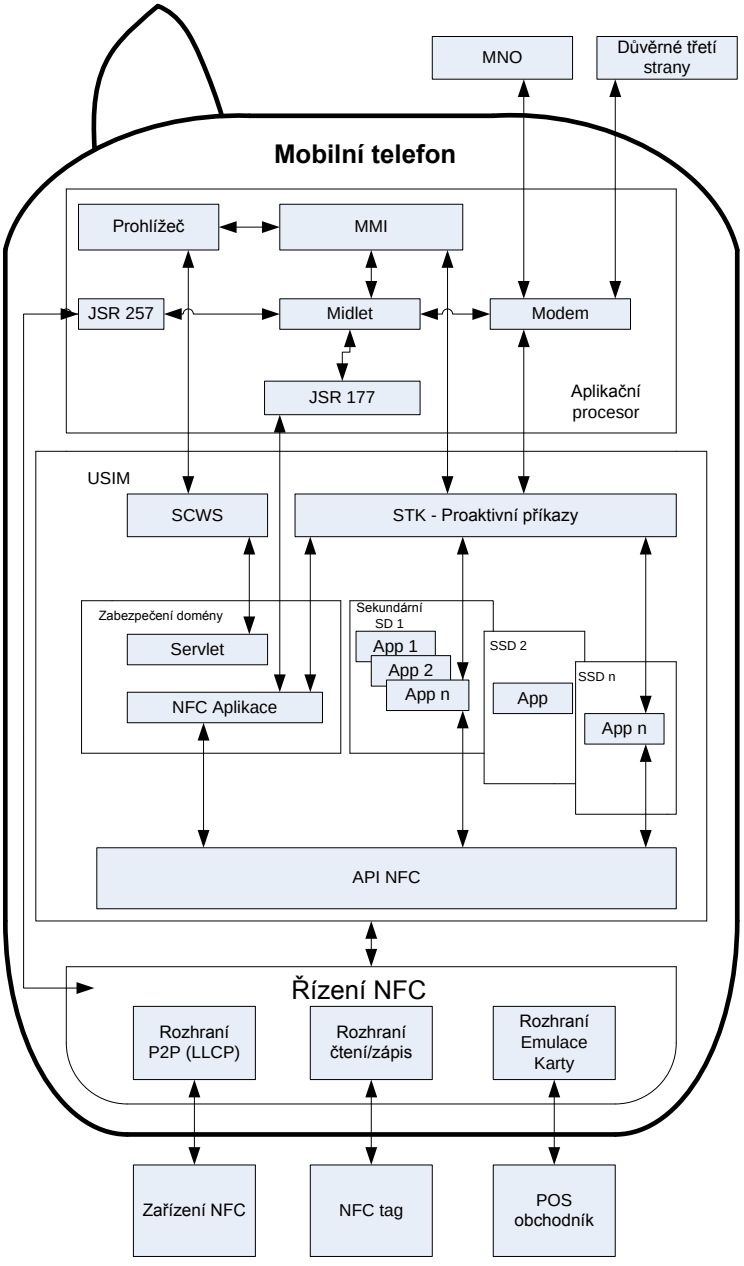
Výhody a obchodní příležitosti pro NCF Smart plakát:

- umožňuje pracovat s koncovými uživateli - poskytnout aktuální informace, prodat službu (vstupenky, vyzvánění...), nebo jim poskytnou prostředky sloužící ke kontaktu pro vlastní pohodlí (např. zde stáhni telefonní číslo pro naši službu),
- dynamicky vybrat nebo aktualizovat obsah přístupný přes plakát,
- pomáhají zjistit, které informace plní svůj účel (převážně v reklamním průmyslu, to je počet lidí, které plakát shlédlo),
- vytvoří okamžité výzvy k stahování (např. hudby),
- nízké náklady ve srovnání s jinými formami dynamického zobrazování (např. LCD televize),
- snadná implementace ve velkých objemech,
- snadno aktualizovatelné (pokud není writeprotected),
- flexibilní velikost a využití.

Platby/Ticketing

V tomto příkladu aplikace se rozhraní NFC využívá k přenosu hodnotné informace. Bývají uloženy v bezpečných zařízeních, jako jsou bezkontaktní platební karty nebo mobilní telefony viz obr. 5.1. Chce-li uživatel provést platbu nebo použít uložený lístek, přepne se do čtecího režimu (jedná se o speciální čtecí protokol pro tento druh aplikací), ve kterém kontroluje přijímané informace o procesu platby nebo

o přijmutí/odmítnutí lístku. U těchto aplikací se můžeme setkat s pojmem „Bezpečné NFC“, který je zavádějící, protože nemá nic společného s bezpečným NFC spojením, ale označuje pouze použitou konfiguraci kombinace hardwarového NFC čipu s čipem SmartCard. Správně se jmenuje „Bezpečná SmartCard a NFC“, bohužel tento název se používá méně častěji. Víc podrobněji se budu těmito aplikacemi zabývat v další kapitole.



Obr. 5.1: Architektura NFC v mobilním telefonu

Spárování zařízení

Princip těchto aplikací spočívá v tom, že spolu komunikují dvě zařízení patřící do stejné skupiny (např. dva mobilní telefony, notebook a fotoaparát, aj.). Komunikace probíhá tak, že obě zařízení se k sobě dostatečně přiblíží. V ten moment se spolu zařízení spojí pomocí NFC, samotný přenos dat pak probíhá přes bluetooth, protože NFC nemá dostatečnou šířku pásma pro přenos obrazových dat. Spárování zařízení pomocí technologie NFC má výhodu v tom, že zařízení stačí k sobě přiblížit na určitou vzdálenost, vyhneme se tak nastavení bluetooth zařízení a zrychlíme komunikaci.

Bezpečnost

Jak již bylo zmíněno dříve, technologie NFC není bezpečná a spoléhá se na kryptografické zabezpečení dané aplikace, která emuluje platební nebo jinou kartu. Tuto technologii ohrožují tři způsoby útoků.

Prvním je odposlouchávání, které je důležité z hlediska toho, že NFC je bezdrátovou komunikační technologií. Odposlech by měl být tedy proveden za pomoci antény, která má za úkol zachytit přenášené signály. Útočník dále potřebuje vědět, jak získat potřebná data z přijatého signálu a poté je ze zachyceného signálu dekódovat pomocí příslušného zařízení pro dekódování RF signálu. Nyní vzniká otázka, jak blízko musí být útočník u cíle, aby se mu podařilo zachytit přenášená data mezi vysílacím a přijímacím zařízením, to může být třeba mobilní telefon a platební terminál v obchodě. Komunikace mezi těmito dvěma zařízeními probíhá na vzdálenosti max. 10 cm a menší, spíš se jedná o 1–4 cm. Na tuto otázku ale neexistuje jednoznačná odpověď, protože je na ní vázáno obrovské množství parametrů, které je potřeba znát:

- RF charakteristika odesílacího zařízení (anténa, geometrie, stínící účinek, prostředí ad.),
- charakteristika útočníkovy antény (anténa, geometrie, možnost změny pozice ve všech 3 rozměrech, aj.),
- kvalita útočníkova přijímače,
- kvalita útočníkova dekodéru RF signálu,
- výběr místa, kde bude útok proveden (případné bariéry, stěny, hluk, kov v okolí, aj.),
- výkon vysílacího zařízení.

Dalším pro odposlech důležitým parametrem je to, ve kterém režimu se vysílací zařízení zrovna nachází. Zda odesílatel generuje vlastní RF pole (aktivní režim) nebo využívá RF pole jiného zařízení (pasivní režim). Nejtěžším způsobem zachytávání

je pro útočníka případ, kdy se zařízení nachází v pasivním režimu. Předpokládá se totiž, že v aktivním režimu je možné zachytit kvalitní RF signál do vzdálenosti asi 10 m, zatímco v pasivním režimu, který využívají platební karty, to je vzdálenost asi 1 m. V případě mobilního telefonu se NFC zařízení vždy vypne při ztmavení (zamčení) displeje, čímž se předejde neoprávněnému použití této technologie bez našeho vědomí.

Druhým možným útokem je poškození přenášených dat. V tomto případě útoku se útočník snaží poškodit přenášená data tak, aby se stala nečitelná pro přijímací zařízení, a rušit tak probíhající komunikaci. To lze dosáhnout přenosem pevných frekvencí v datovém spektru ve správný čas. Útočník k provedení tohoto úkolu bude potřebovat znalosti o provedené modulaci a kódovacím systému. Tento typ útoku není příliš složitý, ale neumožňuje útočníkovi manipulovat s přenášenými údaji.

Posledním typem útoku je pozměnění (modifikace) dat. Cílem tohoto útoku je, aby komunikující zařízení přijímala pozměněná data, která přijmou jako platná. Proveditelnost tohoto útoku je závislá na použité síle amplitudové modulace, a to proto, že dekódování signálu je rozdílné pro 100 % a 10 % modulaci.

Při 100 % modulaci kontroluje dekodér obě poloviny bitů. Pro to, aby dekodér chápal jedničku jako nulu a naopak, musí útočník zajistit, aby pauza v modulaci byla naplněna nosným kmitočtem, a dále, aby útočníkuv RF signál dokonale překryl původní signál. První část tohoto úkolu se dá provést, ale její druhá část, kdy se má překrýt původní signál, je téměř nemožná. Existují však případy, kdy je možné změnit bit v jedničce do nuly, ne však naopak.

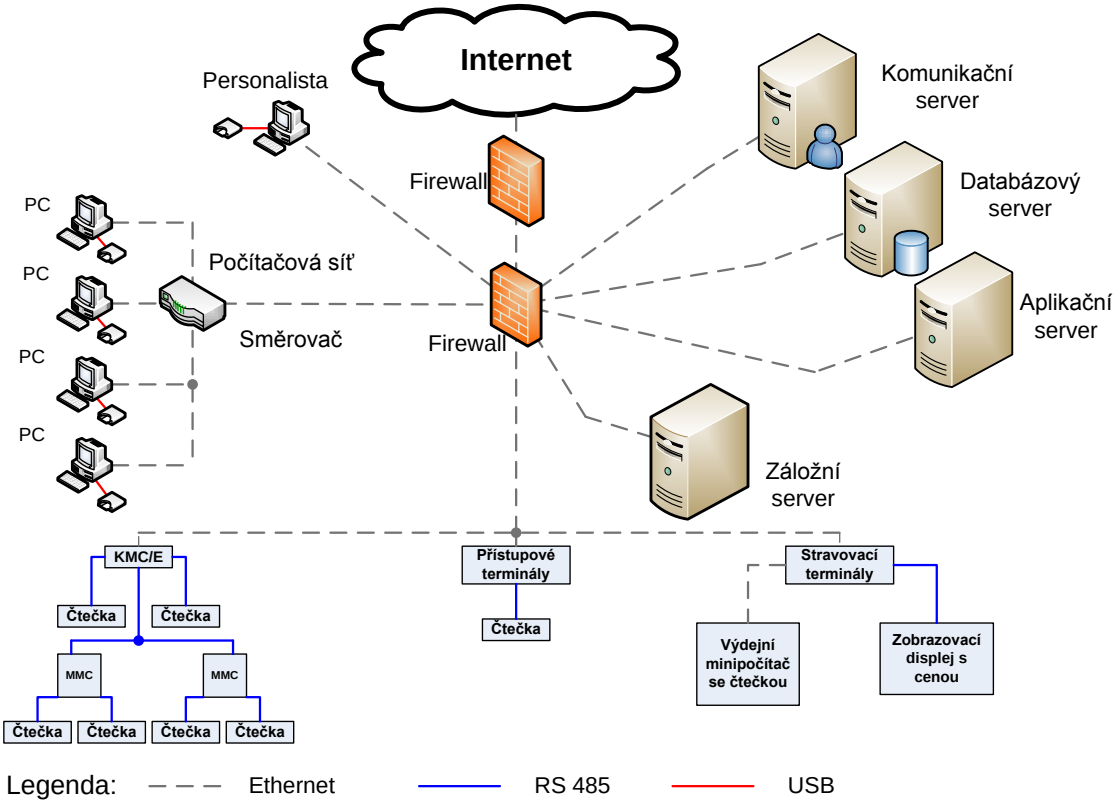
Při 10 % modulaci dochází k porovnání dvou signálů, které má dekodér k dispozici (82 % a plný signál) a porovná je. Nachází-li se oba ve správném rozsahu, zahájí dekódování. Útočník má zde možnost přidat signál do 82 % signálu, ten se poté jeví jako plný signál a plný naopak jako 82 %. To umožňuje změnit všechny hodnoty bitů. Více v [7].

6 BEZPEČNOSTNÍ AUTENTIZAČNÍ PRVKY V LOKÁLNÍ SÍTI

Náplní této kapitoly bude návrh implementace moderních bezkontaktních technologií do lokální sítě. Zejména pak zařízení pracujících na principu technologie NFC aj.

Návrh lokální sítě na obr. 6.1 je rozdělen do několika částí, ve kterých bude rozebrána jejich problematika. Jsou jimi:

- Přístupové a stravovací systémy,
- Lokální síť,
- Serverová část.



Obr. 6.1: Návrh lokální sítě s použitím moderních autentizačních technologií

6.1 Přístupové a stravovací systémy

V této části lokální sítě bude rozebrána problematika přístupových a stravovacích systémů.

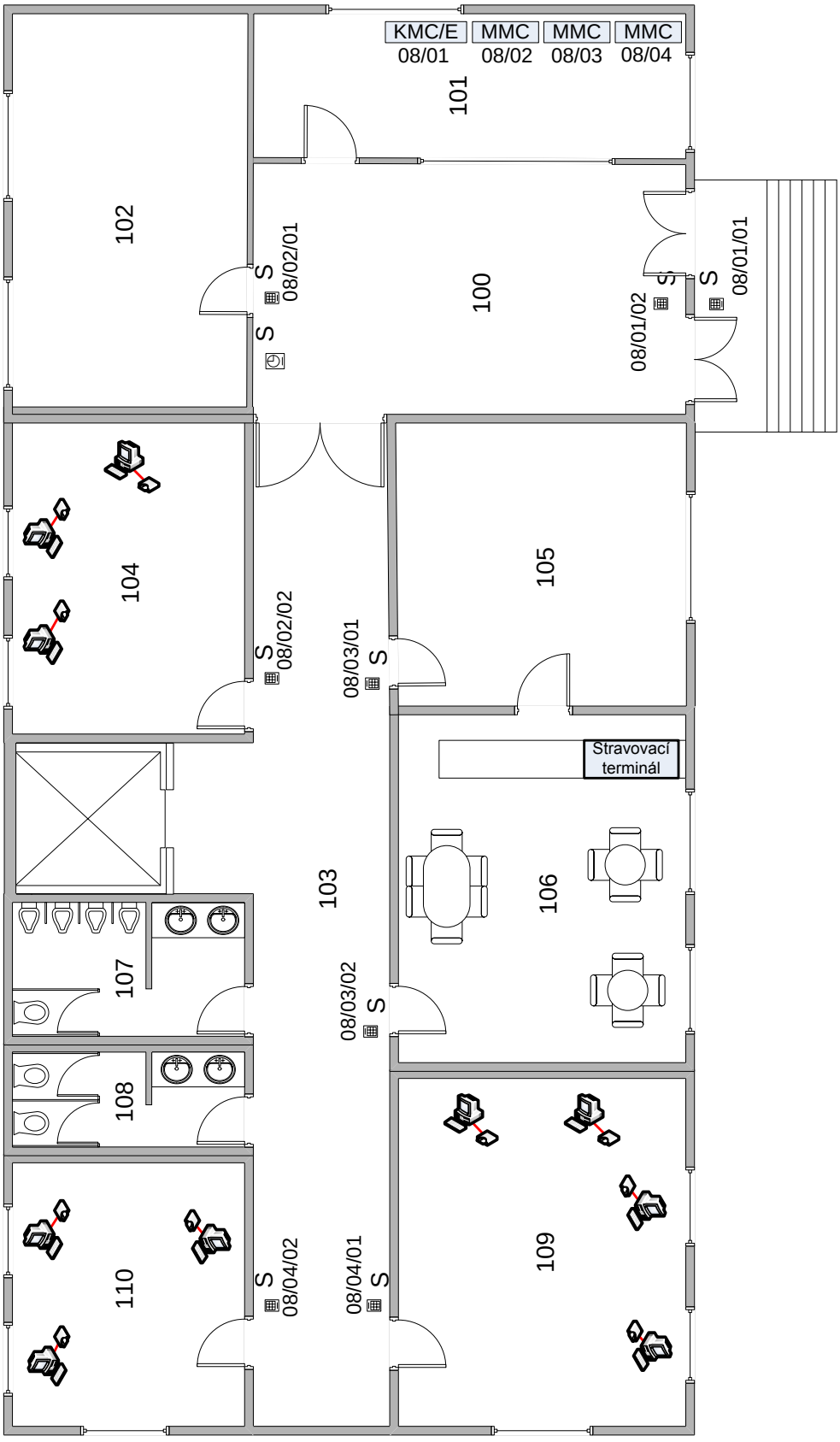
Přístupové systémy budou využívat modulů od firmy Aktion. Tento systém pracuje na principu Master a Slave, kde jako master vystupuje modul KMC/E a slave jsou pro něj moduly MMC.

Modul KMC/E je samostatná řídící jednotka mající na starosti řízení celého přístupového systému. V kombinaci s moduly MMC je lze využít i pro náročnější instalace. Jeden modul KMC/E umožňuje k sobě připojit 15 modulů MMC přes rozhraní RS-485 a ovládat tak až 32 dveří. V jeho paměti se může nacházet až 57 000 záznamů osob a 87 000 záznamů událostí. Modul umožňuje komunikaci se serverem pro aktualizaci záznamů osob a událostí přes Ethernet.

Modul MMC nelze použít jako samostatný řídící modul, ale vždy pouze v kombinaci s modulem KMC/E. MMC nemá žádnou paměť tak jako KMC/E a slouží jako rozšiřující modul. S modulem KMC/E komunikuje prostřednictvím komunikačního režimu RS-485. Tento režim využívá také mimo jiné pro komunikaci se snímací jednotkou.

Komunikace při přístupu do místnosti nebo budovy probíhá následovně: Osoba vlastnící autentizační zařízení (kartu, token, mobil s technologií NFC) ho přiloží ke čtecímu zařízení. Čtečka dekóduje žádost o povolení vstupu, např. do budovy, a upraví zprávu tak, aby ji bylo možné přenášet pomocí protokolu RS-485 do modulu MMC a odtud do řídícího modulu KMC/E, který následně podle záznamů, které má uloženy ve své paměti rozhodne, zda přístup povolí či zamítne. Tato odpověď poté putuje zpět do MMC modulu a čtečky. MMC modul v případě, že je vstup povolen, otevře dané osobě dveře. V opačném případě zůstanou dveře zavřené. Stejnou zprávu obdrží i čtecí zařízení a pokud je přístup povolen, tak se rozezní bzučák, který signalizuje, že je možné projít dveřmi a LED dioda na čtecím zařízení se rozsvítí zeleně. Bzučák i LED diodu může ovládat buďto přímo příslušné čtecí zařízení, nebo jemu nadřazený modul (KMC/E, MMC). Pokud je přístup zamítnut, rozezní se bzučák krátce, což signalizuje zamítavé rozhodnutí a LED dioda se rozsvítí červeně.

Jak už bylo řečeno, KMC/E modul umožňuje být připojený přes Ethernet k serveru. Tato vlastnost je velmi užitečná v případě, kdy je potřeba do systému zavést nového zaměstnance nebo nějak inovovat systém čtecích zařízení. Modul KMC/E provádí vždy po určité době synchronizaci záznamů s ACL (Access Control List), které jsou uloženy na databázovém serveru, a také synchronizaci komunikačních záznamů ADM, které jsou přístupné na komunikačním serveru. Tuto aktualizaci může vyvolat i uživatel (personalista), jenž má na starosti spravovat databázi uživatelů.



Obr. 6.2: Návrh systému pro instituci

Dalším systémem, který se bude nacházet v této instituci, je terminál příchodů a odchodů - tzv. štípačky nebo také docházkový terminál. Tento terminál lze připojit dvěma způsoby: buďto samostatně, přímo prostřednictvím ethernetu k serverům, nebo místo MMC modulu k modulu KMC/E. Výhodnější variantou se mi jeví samostatné připojení tohoto terminálu do sítě, a to hned z několika důvodů: Prvním z nich je, že docházkový terminál nezabírá místo pro připojení dalšího čtecího zařízení k modulu KMC/E. Dalším pak je ten, že terminál musí mnohem častěji komunikovat se serverem než vyžaduje modul KMC/E. Přístupový terminál díky tomu, že komunikuje se serverem, může poskytovat mnohem širší rozmezí služeb než modul KMC/E; kromě záznamu odchodů a příchodů např. umožňuje výběr dovolené, návštěvu doktora aj.

Stejný terminál jako je ten docházkový můžeme použít i na stravovaní, s tím rozdílem, že v něm bude nahraná jiná aplikace určená k výběru jídel. Princip funkce by měl být následující: Strávník si vždy den předem vybere jídlo z nabídky, tím, že přiloží kartu k terminálu, vybere příslušné jídlo a potvrdí svoji volbu. Jeho volba se mu zaznamená na jeho účet a do jídelní aplikace na serveru. Tato aplikace v určitou dobu odešle seznam s objednávkami jídel do kuchyně. Kuchyň se tak může nacházet na druhé straně města a instituce tak ušetří čas i peníze. Nyní se nabízí více variant, jak může strávník zaplatit za svůj oběd. První je vždy na konci měsíce mzdovým oddělením odečtená příslušná částka ze mzdy. Druhou možností je, aby si každý zaměstnanec na svůj zaměstnanecký účet uložil určitou hotovost v podobě kreditu, ze kterého se mu vždy odečte příslušná cena jídla.

6.2 Lokální síť

Lokální síť je v dnešní době součástí každé instituce. Má za úkol sdílení společných prostředků mezi uživateli, usnadnit komunikaci aj. Přihlášení do těchto sítí se většinou provádí tak, že každý zaměstnanec má svůj vlastní účet, za který si odpovídá. Ten je většinou chráněn pomocí nějakého loginu a hesla (autentizace znalostí). V této instituci ale k tomuto účelu budeme využívat kombinaci předmětu a znalosti, to znamená, že před přihlášením do systému zaměstnanec přiloží token (čipová karta, USB token, mobilní telefon) k čtecímu a zadá patřičné heslo pro připojení. Heslo je následně ověřeno v tokenu a výsledek tohoto porovnání je odeslán na server. Ten pak případně načte uživatelův účet i s jeho nastavením. Jedná se o bezpečnější způsob autentizace.

Obr. 6.3: Autentizace pomocí čipové karty k PC

6.3 Servery

Součástí sítě jsou také čtyři servery (komunikační, databázový, aplikační a záložní). Komunikační server má na starosti komunikaci jednotlivých částí sítě a především obsahuje data o struktuře přístupové sítě. Dalším serverem, který se nachází v síti, je aplikační, na kterém jsou nainstalovány aplikace, které mají na starosti chod všech systémů (přístupový systém, docházkový terminál, stravovaní atd.). Aplikační server při vykonávání své činnosti spolupracuje s databázovým serverem, na kterém jsou uložena data o účtech jednotlivých zaměstnanců (práva, která mají v počítačové síti, jaký oběd a kdy si objednal daný zaměstnanec apod.). Čtvrtým a posledním serverem je server, který slouží jako záloha vše tří předchozích (komunikačního, databázového a aplikačního) serverů; to je umožněno díky tomu, že jednotlivé servery jsou na záložním vytvořeny virtuálně.

Celou síť chrání dvojice hardwarových firewallů. Hardwarové firewally jsem zvolil, protože jsou odděleny od ostatních serverů a je tak menší riziko, že je může ohrozit některá z aplikací, která se na serveru nachází. Dalším důvodem pak byl

předpoklad, že hardwarový firewall bude rychlejší a flexibilnější při ochraně středně velké instituce.

Cenová dostupnost této sítě se odvíjí od velikosti a míry zabezpečení dané instituce. Cena systému obsahující technologie NFC se určuje velmi těžce, protože ještě nejsou na trhu dostupné některé potřebné prvky, jako jsou čtecí zařízení nebo terminály potřebné pro vedení docházky a stravování. Lze proto jenom dohadovat jejich přibližnou cenu viz tab. 6.1. Více informací naleznete zde [1].

Tab. 6.1: Prvky přístupové sítě

Prvky sítě	Přibližná cena/ 1 ks	Poznámka:
KMC/E	15 000 Kč	
MMC	7 000 Kč	
NFC čtečka pro dveře	4 000 <	Předpoklad je, že cena bude vyšší než u obyčejné RFID čtečky
NFC čtečka pro PC	1 000 Kč	V USA se prodává do 50 přesnou cenu se mi nepodařilo sehnat
Terminál	10 000 <	Předpoklad je, že cena terminálu s NFC technologií bude vyšší než je u klasického RFID

7 ZÁVĚR

Úkolem této práce bylo navrhnout vhodný a zároveň bezpečný způsob implementace moderních autentizačních technologií do lokální sítě imaginární instituce. K tomuto úkolu jsem využil instalační moduly firmy Aktion, pomocí nichž jsem se pokusil navrhnout funkční systém. Při návrhu použitých prvků jsem se snažil dbát na to, aby bylo možné systém vylepšit s příchodem nových bezpečnostních prvků, pracujících na principech technologie NFC. Proto jsem do systému navrhl využití čtecích zařízení, která pracují s protokolem RS-485, protože stejného protokolu by měla využívat i čtecí zařízení pracující s NFC technologií. Celý systém komunikuje se servery, které zajišťují aktuálnost dat potřebných pro bezchybnou funkci systému. Přístupový systém je navíc schopen fungovat i bez aktualizace databází ze serveru. Toho se může využít v případě, že dojde k jejich nečekanému výpadku a nenaběhne záložní server.

Výhodami tohoto systému je bezpečnost, flexibilita a uživatelská přívětivost.

LITERATURA

[1] Aktion.cz [online]. [cit. 2011-05-30]. Aktion. Dostupné z WWW: www.aktion.cz.

[2] *Autentizace: přilož prst.* Clever and Smart [online]. [cit. 2010-12-12]. Dostupný z WWW: www.cleverandsmart.cz/autentizace-priloz-prst.

[3] Burda, Karel. *Bezpečnost informačních systémů.* 1. vydání Brno: FEKT VUT Brno, 2005. s. 1-124.

[4] DRMOLA, Robert. *Základy Šifrování.* [online]. [cit. 2010-12-12]. Dostupný z WWW: www.bobhy.wz.cz/clanky/kryptografie.html.

[5] HAJNÝ, Jan. *Úvod do Zero-knowledge protokolů.* Elektrorevue [online]. 16.10.2008, [cit. 2010-11-28]. Dostupný z WWW: www.elektrorevue.cz/cz/download/uvod-do-zero-knowledge-protokolu. ISSN 1213-1539.

[6] HAJNÝ, Jan; MALINA, Lukáš. *Anonymní Autentizace.* SeCReG [online]. [cit. 2010-12-12]. Dostupný z WWW: secreg.utko.feec.vutbr.cz/cs/content/anonymn%C3%AD-autentizace.

[7] HASELSTEINER, E.; BREITFUB, K. *Security in Near Field Communication.* Philips Semiconductors [online]. 2006, [cit. 2011-05-22]. Dostupný z WWW: www.events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.

[8] *ISO 7816 - Smart Card Standards Overview.* Smartcardsupply.com [online]. [cit. 2011-05-14]. Dostupné z WWW: www.smartcardsupply.com/content/cards/7816standard.htm.

[9] *Java Card Technology Overview.* Oracle.com [online]. Dostupné z WWW: www.oracle.com/technetwork/java/javacard/overview/overview-jsp-135353.html.

[10] *Java Card.* In Wikipedia : the free encyclopedia [online]. 19.5.2005, last modified on 5.5.2011 [cit. 2011-05-14]. Dostupné z WWW: en.wikipedia.org/wiki/Java_Card.

[11] *Release Notes - Java Card 3.0.1 Platform Specification.* Oracle.com [online]. [cit. 2011-05-14]. Dostupné z WWW: www.oracle.com/technetwork/java/javacard/releasenotes-jsp-137685.html.

[12] JELÍNEK, Martin. *Autentizační tokeny v praxi.* IT SYSTEMS [online]. 2008, 10, [cit. 2010-12-12]. Dostupný z WWW: www.systemonline.cz/it-security/autentizacni-tokeny-v-praxi.htm.

[13] KILISKI, Burt. *TWIRL and RSA key Size.* RSA laboratories [online]. 2003, [cit. 2010-11-30]. Dostupný z WWW: www.rsa.com/rsalabs/node.asp?id=2004.

[14] *Vývoj kryptografie.* [online]. 20.04.2009, [cit. 2010-12-06]. Dostupný z WWW: www.bezpecnost.estranky.cz/clanky/zpravodajske-techniky/uvod-do-kryptografie.

[15] MAYES, Keyth E. – MARKANTONAKIS, K. *Smart cards, tokens, security and applications.* 1.vydání. Springer, 2007. ISBN 978-0-387-72197-2. Dostupný z WWW: http://www.scribd.com/doc/44639348/Smart-Cards-Tokens-Security-and-Applications

[16] *Smart Poster.* NFC Forum [online]. 2011,[cit. 2011-05-22]. Dostupný z WWW: www.nfc-forum.org/resources/white_papers/NFC_Smart_Posters_White_Paper.pdf.

[17] ORTIZ, C. Enrique. *An Introduction to Java Card Technology.* Oracle [online]. 29.5.2003, 1, [cit. 2011-05-14]. Dostupný z WWW: www.oracle.com/technetwork/java/javacard/javacard1-139251.html.

[18] PATAUNER, C., et al.*High Speed RFID/NFC at the Frequency of 13.56 MHz.* EURASIP [online]. 2007, 1, [cit. 2011-05-18]. Dostupný z WWW: www.eurasip.org/Proceedings/Ext/RFID2007/pdf/s1p4.pdf.

[19] PINKAVA, Jaroslav. *Úvod do kryptografie* [online]. 1998 [cit. 2010-12-01]. Dostupné z WWW: www.linkpdf.com/ebook-viewer.php?url=http://crypto-world.info/pinkava/uvod/uvod98.pdf.

[20] PRIMAS, Martin. *Nová generace asymetrické kryptografie.* BANKOVNICTVI.IHNED.CZ [online]. 18.10.2010, [cit. 2010-12-12]. Dostupný z WWW: www.bankovnictvi.ihned.cz/?p=900000_d&article[sms_pay]=true&article[id]=47096200.

[21] PUST, Radim. *Čipové karty Mifare a jejich bezpečnost.* Elektrorevue [online]. 1.6.2009, [cit. 2010-12-12]. Dostupný z WWW: www.elektrorevue.cz/cz/download/cipove-karty-mifare-a-jejich-bezpecnost.

[22] Public-Key Cryptography Standards (PKCS): What are DSA and DSS?. RSA laboratories [online]. [cit. 2010-12-05]. Dostupný z WWW: www.rsa.com/rsalabs/node.asp?id=2239.

[23] ŠVENDA, Petr. *.NET smart cards* [online]. Poslední úpravy 18.10.2009 [cit. 2011-05-18]. Dostupný z WWW: `http://www.fi.muni.cz/~xsvenda/dotnetcard.html`.

[24] TOMEK, Lukáš. *USB token: pamatuje si hesla a šifruje. Útok zabere dvě a půl minuty*. Lupa.cz [online]. 10. 9. 2010, [cit. 2010-12-12]. Dostupný z WWW: `www.lupa.cz/clanky/usb-token-pamatuje-si-hesla-sifruje-neni-bezpecny`.

[25] VRÁNA, Jakub. *Bezpečné přihlašování uživatelů.* ROOT.CZ [online]. 12.4.2006, [cit. 2010-11-28]. Dostupný z WWW: `www.root.cz/clanky/bezpecne-prihlasovani-uzivatelu`.