BEZPEČNÁ VÝMĚNA DOKUMENTŮ NA PŘÍKLADĚ VIRTUÁLNÍHO PODNIKU

Jan Čapek
Ústav systémového inženýrství a informatiky, FES, Univerzita Pardubice

Abstrakt: *Předkládaný příspěvek se zabývá problematikou bezpečné výměny dokumentů ve virtuálním podniku. Problémy jsou vzhledem k možnému rozsahu příspěvku spíše jen naznačeny s poukázáním na možná úskalí při předávání informací. Je diskutován sdílený datový sklad, různé formy digitálního podpisu, je zmíněn systém PGP, jakož zásady bezpečnostní politiky firmy.*

Abstract: *The contribution deals with safety exchange documents problem within the virtual enterprise. These problems are in view of possible dimension of this contribution only just indicated with highlight of possible pitfalls by information transmission. The shared warehouse, different forms of the digital signature, system of PGP and principle of the security firm's politics was discussed.*

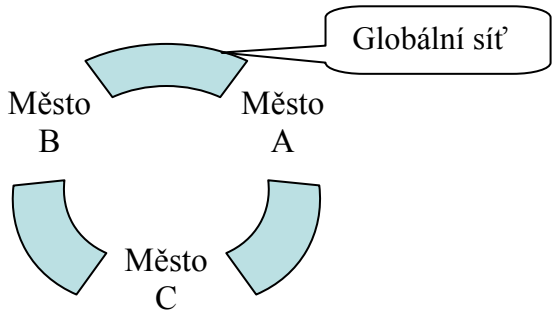
Klíčová slova: *virtuální podnik, globální síť, digitální podpis, bezpečnost dokumentů*

Key words: *virtual enterprise, global network, digital signature, document security*

1. Úvod

V poslední době stále více se dostává do popředí problematika virtuálních podniků, jejich vnitřní fungování (tj. vzájemná spolupráce zaměstnanců virtuálního podniku) jakož i spolupráce s vnějším prostředím. Může existovat mnoho různých definicí virtuálního podniku, pro náš případ přijměme následující výklad.

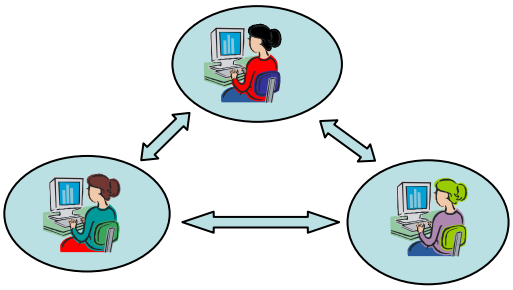
Virtuální podnik je podnik, jehož zaměstnanci spolu nesdílí společné prostory a komunikují spolu a s vedením prostřednictvím informačních a komunikačních technologií (ICT).



Obr.1 Příklad virtuálního podniku rozmístěného ve třech městech a spojeného globální sítí
Zdroj: vlastní

2. Virtuální podnik

Předmět podnikání umožňuje rozptýlenost zaměstnanců a vedení podniku. Příkladem může být SW firma. Podmínkou úspěchu virtuálního podniku (distribuované firmy) je bezpečné propojení jednotlivých částí podniku, jednotlivých pracovišť pomocí globální sítě. Příklad propojení jednotlivých pracovišť je na obr. 2.



Obr. 2 Příklad propojení jednotlivých pracovišť
Zdroj: vlastní

Z hlediska vnějšího zabezpečení virtuálního podniku se nejvíce využívají firewally. Firewall selektivně zajišťuje komunikaci sítí organizace s Internetem tak, aby:

- zvenku byly přístupné právě ty zdroje určené bezpečnostní politikou pevně definované skupině uživatelů,
- uživatelé mohli bezpečně využívat zdroje Internetu.

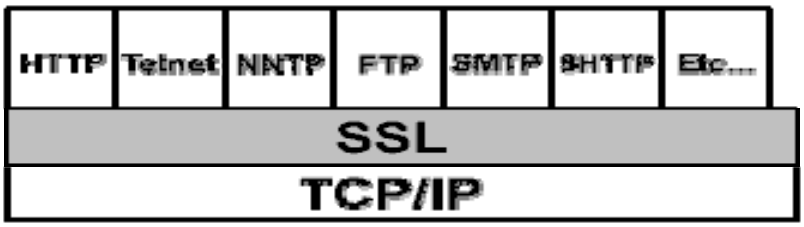
Firewall tedy zabezpečuje komunikaci vnitřních a vnějších sítí oběma směry, umožňuje jemné odstupňování práv uživatelů, soustřeďuje řízení přístupu do jednoho bodu, blokuje nepřátelské mapování vlastního prostoru a obchází chyby v implementaci některých programů.

3. Možná ohrožení při e-komunikaci:

Při elektronické komunikaci mohou nastat následující ohrožení výsledků komunikace mezi pracovníky buď virtuálního podniku nebo mezi pracovníky virtuálního podniku a jiného spolupracujícího podniku či fyzické osoby:

- **Modifikace zprávy** - změna po odeslání oprávněným uživatelem,
- **Změna v pořadí zpráv** - zpráva se může ztratit, dojít vícekrát nebo může později odeslaná zpráva dojít dříve,
- **Podvržení zprávy** - zprávu generuje narušitel, který se vydává za oprávněného účastníka,
- **Odmítnutí původu zprávy** - původce zprávy později zapře odeslání,
- **Odmítnutí příjmu zprávy** - příjemce později odmítne příjem zprávy,
- **Zneužití důvěrné informace** - neoprávněná osoba získá obsah zpráv.

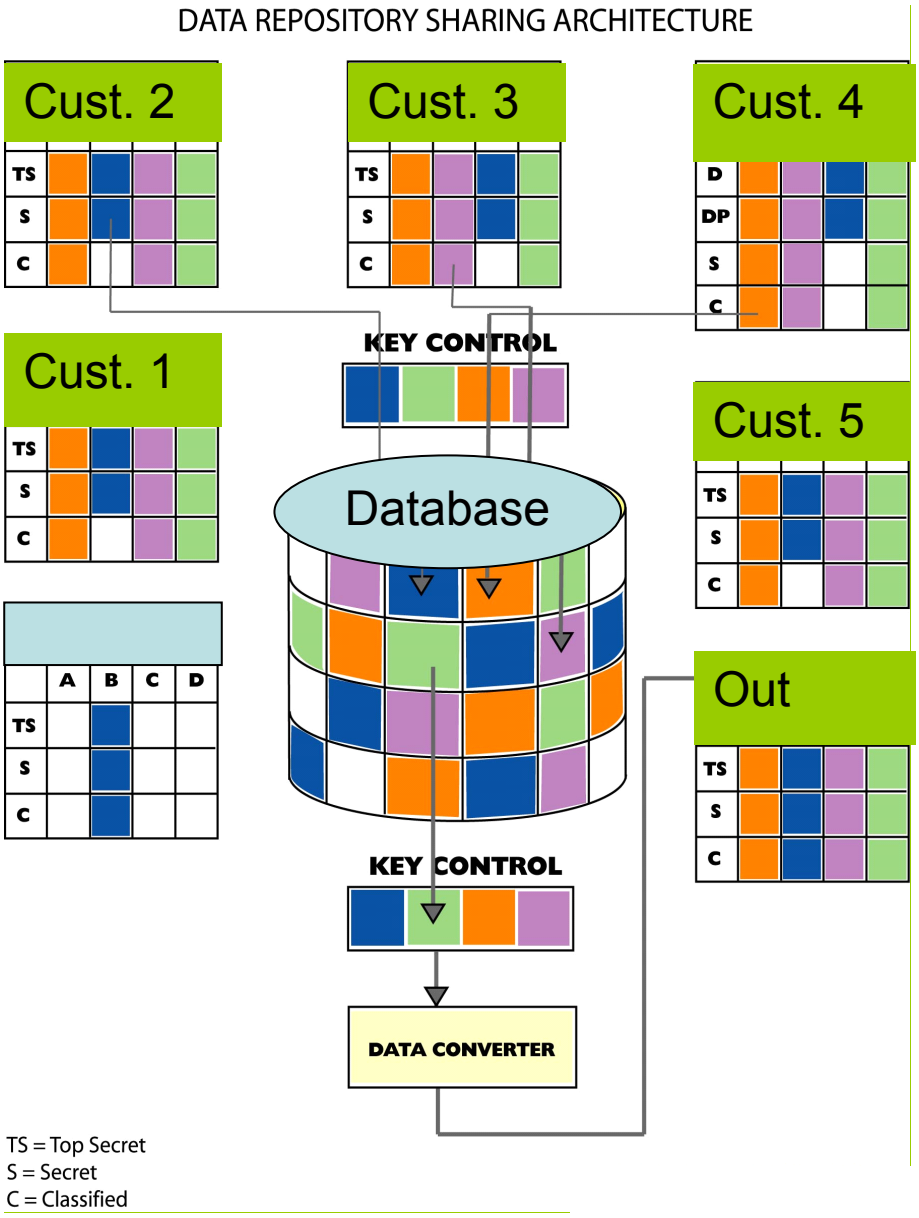
Při elektronické výměně dokumentů je potřeba dodržovat definovaný standard UN/EDIFACT pro elektronickou výměnu zpráv, definované standardní zprávy, které lze šifrovat a/nebo digitálně podepsat, zajistit END-TO END bezpečnost, používat protokol X.400 nebo SMTP. Pro komunikaci po Internetu se používá **SSL - Secure Socket Layer,** který je protokolově nezávislý je podporován Netscape, Microsoftem, viz. Obr. 3.



Obr. 3 Secure Socket Layer
Zdroj:Dostálek L.: Velký průvodce protokoly TCP/IP

4. Sdílený datový sklad

- Při sdílení dat uložených v datovém skladu, není výhodné používat běžných technologií právě z důvodu možnosti průniku nežádoucí osoby do datového skladu, při bezpečnostní chybě pracovníků virtuálního podniku. Proto je výhodná taková konstrukce datového skladu, kde každý zaměstnanec virtuálního podniku má ke svým položkám přístup přes svůj klíč. Viz. Obr. 4.



Obr. 4 Sdílený datový sklad
Zdroj e-Witness

4.1. Digitální podpis

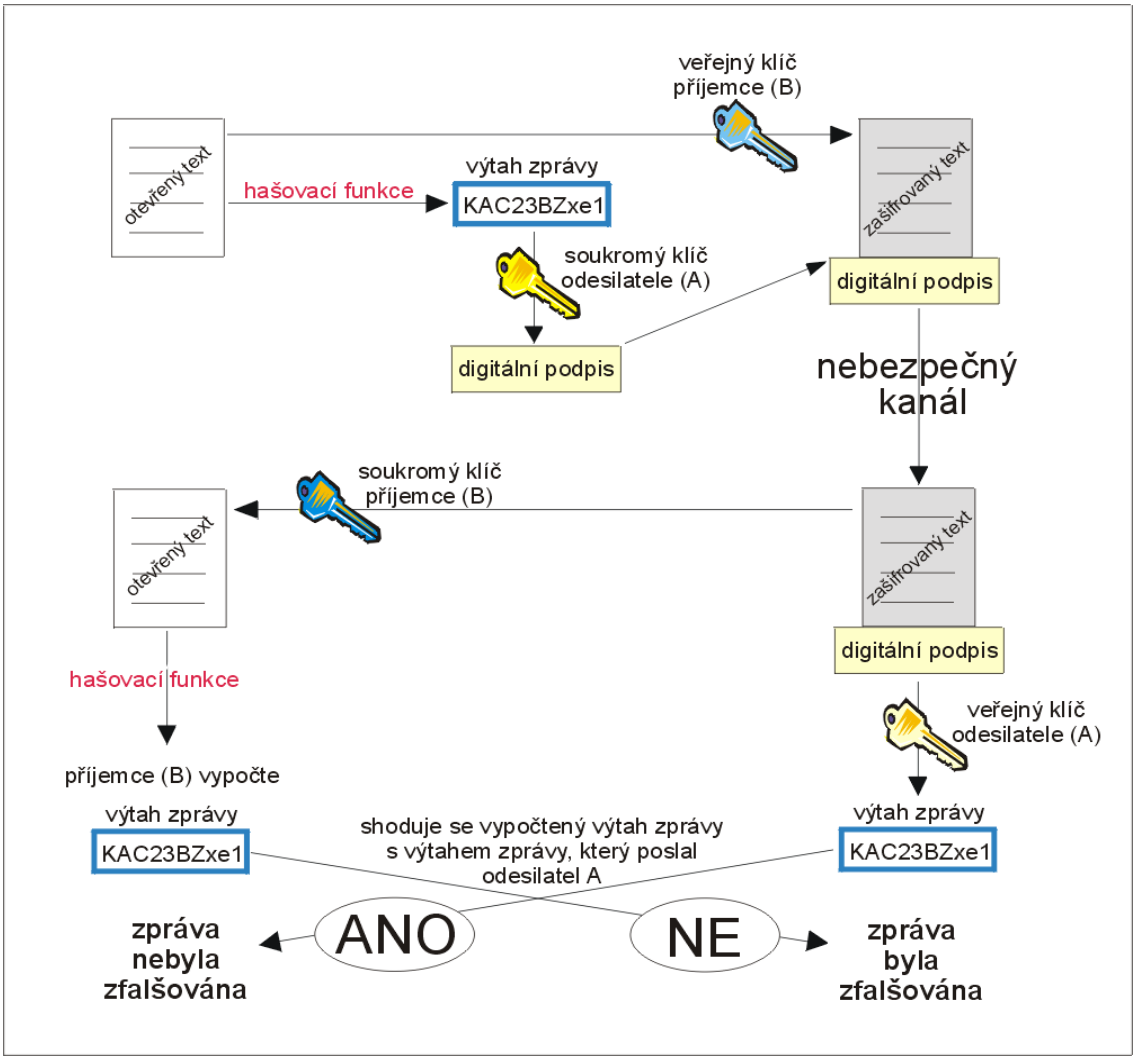
- má všechny vlastnosti psaného podpisu,
- má lepší zabezpečení než klasický podpis,
- zprávu nelze modifikovat,
- zprávu nelze podvrhnout,

- brání zapření příjmu nebo odeslání.

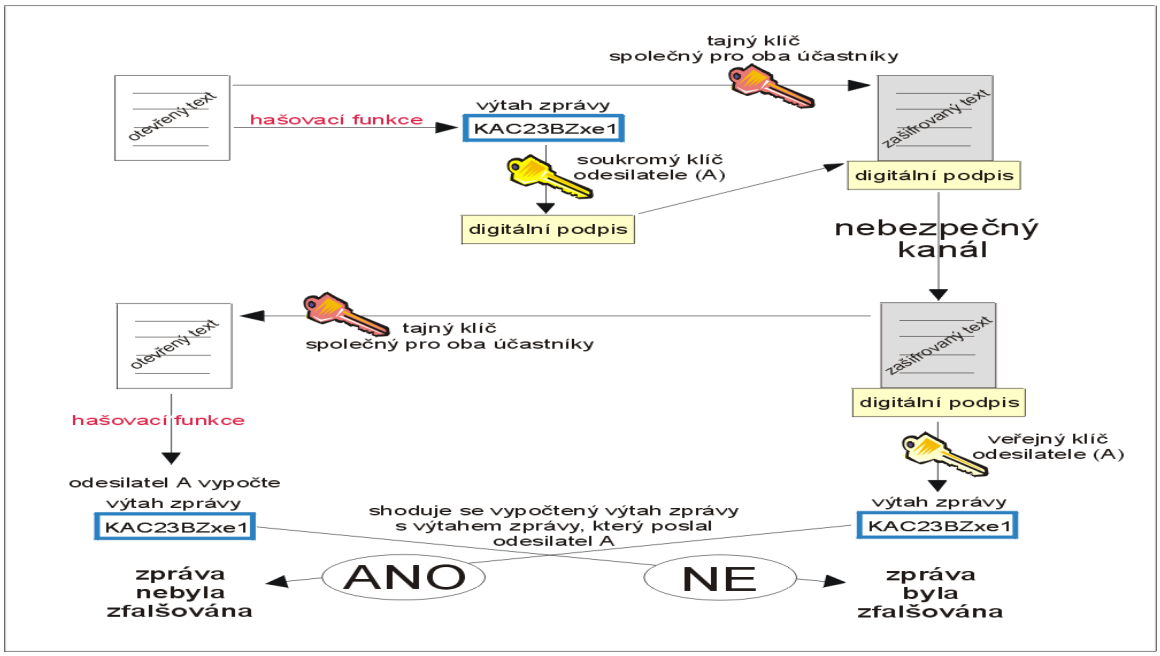
K reálnému použití digitálního podpisu však potřebujeme náš veřejný a soukromý klíč a někoho, kdo ověří pro třetí stranu, naši identitu. Tímto úkolem je pověřena tzv. certifikační autorita.

4.1.1. Výpočet digitálního podpisu

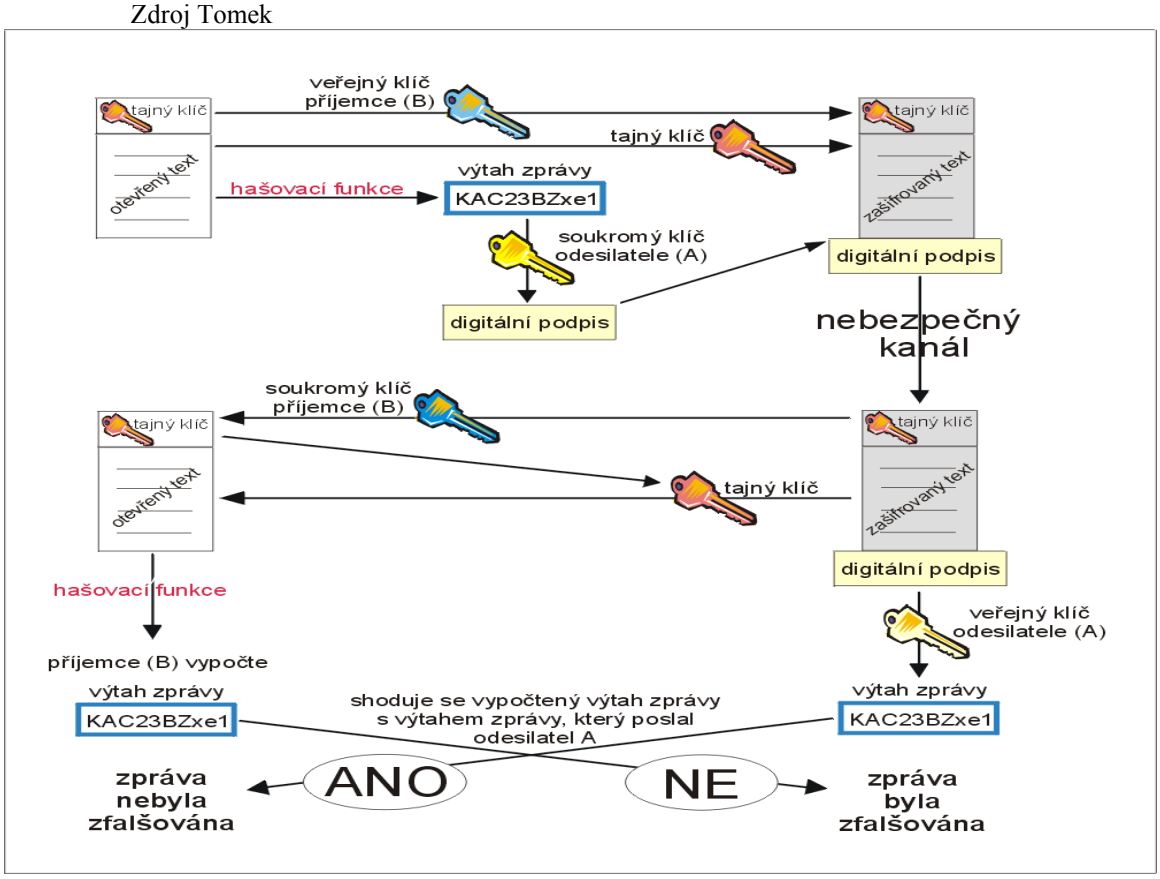
- vypočte se kontrolní součet zprávy (výtah zprávy o konečné - jednotné - délce), který je pro každou zprávu unikátní. (CRC, MD5, SHA1)
- ten se zašifruje tajným klíčem odesílatele a připojí se ke zprávě
- příjemce spočte stejný součet ze zprávy.
- veřejným klíčem odesílatele dešifruje připojený kontrolní blok
- pokud nejsou kontrolní součty zprávy (výtahy zprávy o konečné - jednotné - délce) stejné, je zpráva odmítnuta.



Obr. 5 Zpráva je podepsaná a zašifrovaná pomocí kryptografie s veřejným klíčem
Zdroj Tomek



Obr. 6 Zpráva je podepsaná a zašifrovaná pomocí symetrické kryptografie
Zdroj Tomek



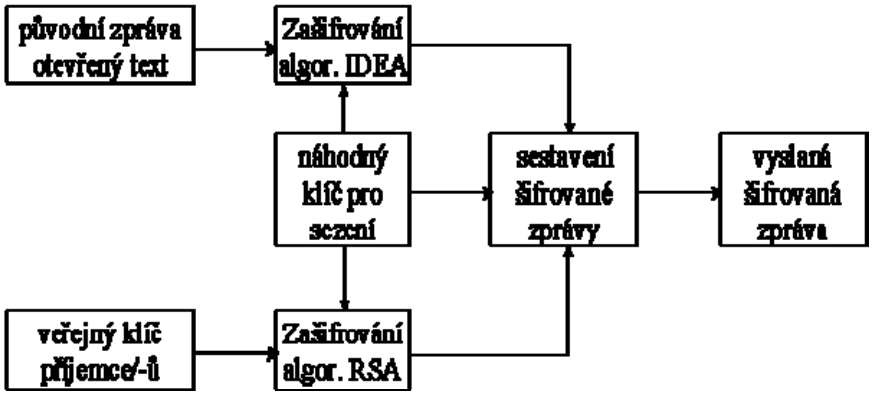
Obr. 7 Zpráva je podepsaná, zašifrovaná pomocí symetrické kryptografie vč. bezpečného přenosu tajného klíče

Zdroj Tomek

4.2. Certifikační autorita

- je základní typ poskytovatele certifikačních služeb, zabývající se vydáváním a správou digitálních certifikátů. Správou digitálních certifikátů rozumíme veškeré činnosti spojené s digitálními certifikáty jako např.:
  - změna údajů uvedených v certifikátu
  - zveřejňování certifikátů
  - verifikace klíčů
  - odvolávání certifikátů
- vydává Seznam odvolaných certifikátů (CRL – Certifikation Revocation List). CRL je seznam veřejných klíčů, které byly odvolány dříve než skončila jejich řádná doba platnosti. Důvodem může být ztráta, odcizení klíče, odchod ze zaměstnání atd.

Pro šifrování e-mailových zpráv není nutné vždy používat systému certifikační autority a jí přidělený digitální podpis. Můžeme použít i **PGP - Pretty Good Privacy.**
PGP je neoficiální světový standard pro e-mail, řeší pouze zašifrování zprávy, ne její distribuci, umožňuje zprávy šifrovat, vytvářet a ověřovat digitální podpisy, volitelná délka klíče až do 2048bitů, kombinuje systém veřejného klíče RSA a symetrické šifry IDEA, zpráva je zašifrována symetrickou šifrou IDEA pomocí náhodného klíče. Ten je pak zašifrován pomocí RSA, který slouží jen jako přepravní obálka. Pro použití v e-poště, má PGP zabudovanou konverzi do tisknutelných znaků. Existuje implementace pro MS DOS, Windows, BSD, AIX,HP-UX,SCO Solaris, Linux, atd. Princip činnosti PGP je na obr. 8.



Obr. 8 Princip činnosti PGP
Zdroj www.PGP.com

5. Bezpečnostní politika

Každý podnik a tedy i virtuální podnik myslí-li to se zabezpečením dokumentů vážně by měl mít vypracovanou svou bezpečnostní politiku. Tedy měl by mít stanovena podniková tajemství, měl by určit možná nebezpečí, stanovit práva uživatelů, navrhnout kontroly systému a v neposlední řadě navrhnout opatření po průniku do systému.

6. Literatura

[1] Zelenka J., Čapek J., Francek J., Janáková H,: Ochrana dat – Kryptologie . Gaudeamus 2003. , 198 s. ISBN 80-7041-737-4

[2] Fabian P. "Design and Developmnet of Educational Multimedia Application for Telelearning" Workshop proceedings TEMPUS INSYPA Huddersfield 1999, pp 88-100. ISBN 80-7194-203-0

[3] Tomek, J.: Bezpečnost a ochrana dat se zaměřením na elektronický podpis. Diplomní práce, UPa, FES 2001.

[4] Dostálek, L.: Velký průvodce protokoly TCP/IP Bezpečnost. Computer Press Praha 2001 ISBN 80-7226-513-X

[5] www.PGP.com

Kontaktní adresa:

prof. Ing. Jan Čapek, CSc.
Ústav systémového inženýrství a informatiky,
Fakulta ekonomicko-správní,
Univerzita Pardubice
Studentská 95
53210 Pardubice
Česká Republika
Tel: +420 466036512,
E-mail: capek@upce.cz