

UŽITNÝ VZOR

(11) Číslo dokumentu:

16100

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(21) Číslo přihlášky: **2005 - 16930**

(22) Přihlášeno: **22.08.2005**

(47) Zapsáno: **02.01.2006**

(13) Druh dokumentu: **U1**

(51) Int. Cl.:

G01V 15/00 (1995.01)

G09F 3/03 (1968.09)

(73) Majitel:

Jansa Jaroslav Ing. CSc., Praha, CZ

Kašpar Jiří Ing., Říčany, CZ

Zeman Daniel Ing., Hudlice, CZ

(72) Původce:

Jansa Jaroslav Ing. CSc., Praha, CZ

Kašpar Jiří Ing., Říčany, CZ

Zeman Daniel Ing., Hudlice, CZ

(74) Zástupce:

Ing. Jarmila Loskotová, K Závětinám 727, Praha 5, 15500

(54) Název užitého vzoru:

Identifikační digitální pečeť

CZ 16100 U1

Identifikační digitální pečeť

Oblast techniky

Technické řešení se týká řešení identifikace předmětu, přiřazeného k dalším subjektům, týkající se zejména vozidel.

5 Dosavadní stav techniky

10 Označování předmětů pro jejich identifikaci se v současné době provádí nejrůznějšími způsoby, například systémem čárových kódů a to jednorozměrnými nebo i dvourozměrnými. Čárové kódy obsahují jednoznačná unikátní čísla a kódy dvourozměrné i řadu dalších informací o předmětu. Problémem však je u čárových kódů, že se dají snadno zfalšovat, neboť jde pouze o tisknutelné symboly.

Pro označování předmětů se také používají etikety samolepicího charakteru s řadou grafických symbolů, jako jsou například dálniční známky pro vozidla. I když jsou vybaveny ochrannými prvky typu hologramů, i tato označení se dají běžně zfalšovat. Ani dělení etikety, takzvané "nařezání", znemožňující znovunalezení, není vždy spolehlivé.

15 V poslední době se rozvíjejí systémy radiofrekvenčních čipů, ať už pasivních nebo aktivních. Radiofrekvenční čipy RFID (Radio Frequency Identification - identifikace radiofrekvenčním čipem) odpovídají na vyslaný impuls a sdělují čtecímu zařízení své jedinečné identifikační číslo. Při použití 64 bitových čipů je množství použitelných čísel v miliardách miliard a tudíž tvorba celosvětové klasifikace subjektů realizovatelná. Tento systém se používá k označování zboží v obchodech. Při použití této identifikace předmětu však není zaručena neoddělitelnost čipu od předmětu.

Čipy se také používají v různých typech identifikačních karet a dokonce se uvažuje o jejich implantaci zvířatům a s trochou nadsázky i lidem. Speciální třída těchto čipů jsou čipy třídy DSRC (Dedicated Short Range Communication - definovaná komunikace krátkého dosahu), které 25 umožňují i komunikaci mezi sebou a daleko vyšší rychlostí než čipy RFID, které pracují v režimu klient-server, používané k označování vozidel v systémech elektronického mýtného a parkovného. Tento systém označování bude velmi nákladný.

V mnoha aplikacích pro označování se používají kontaktní nebo bezkontaktní čipové karty. Čipová karta je však spojena s osobou, která ji přenáší, čímž je spolehlivost systému takovouto 30 kartu využívající značně ovlivněna "lidským faktorem".

U žádného dosud používaného systému identifikace předmětů však není zaručena neoddělitelnost identifikátoru od předmětu.

Podstata technického řešení

35 Výše uvedené nevýhody odstraňuje a daleko vyšší spolehlivost přináší označování předmětů identifikační digitální pečeti, jejíž podstata spočívá v tom, že identifikační digitální pečeť je jednoznačně přiřazena předmětu, na kterém je pevně uspořádána, například nalepením a sdružuje v sobě více prvků, které jsou integrované v jednom celku a to:

- prvky opticky rozeznatelné, například hologramy, alfanumerické a grafické znaky, čárové kódy apod. označující a identifikující předmět, a/nebo
- 40 - elektronické prvky - bezkontaktní radiofrekvenční čipy RFID s výhodou typu DSRC, čip zajišťující bezdrátovou komunikaci, případně úložiště s kryptografickým klíčem či dokonce kryptografický procesor a podobně, a dále
- 45 - připevňovací prvky - zajišťující dostatečně pevné spojení pečeti s předmětem, například samolepicí vrstvu,

- zabezpečující prvky - zajišťují ochranu proti snahám o neoprávněnou manipulaci (odlepení pečeti), tak, že dochází k destrukci optických a/nebo elektronických prvků pečeti též i v součinnosti s připevňovací vrstvou.

5 Zásadní výhodou použití identifikační digitální pečeti podle technického řešení je nutno spatřovat v jednoznačném svázání této pečeti s předmětem, na který je například nalepena.

Identifikační digitální pečeť v některé z výše uvedených kombinací, zajišťuje snadné označování předmětů jak optickými, tak elektronickými prvky, které zvyšují nejen bezpečnost a spolehlivost, ale přináší i další zvýšení užité hodnoty a aplikovatelnosti.

10 Připevněním, například nalepením této pečeti na předmět zájmu je možné v kombinaci s dalšími zařízeními využívat těchto schopností:

Identifikace předmětu - jak optická, tak elektronická. Kód pečeti identifikuje celý předmět. Elektronická identifikace vyžaduje zařízení komunikující například s RFID čipem. Identifikace může sloužit k mnoha rozmanitým aplikacím. Navíc běžné optické prvky identifikace mohou používat známých klasických metod (písmo, čárový kód).

15 Autentizace předmětu - RFID čip může navíc obsahovat kryptografický klíč. Klíč pečeti je tak klíčem patřícím k celému předmětu, na který je pečeť nalepena.

20 Další identifikační aplikace jsou například zajištění nepřemístitelnosti předmětu. Jeden z dalších efektů využití identifikace či dokonce autentizace je využití principu trvalého či náhodného zjišťování přítomnosti "identifikační digitální pečeti" v dosahu kontrolního modulu. Toho lze využít v mnoha případech.

25 Technické řešení identifikační digitální pečeti slučuje výhody označování předmětů pomocí čárových kódů a elektronických čipů, které doposud společně nebyly využívány. Systém umožňuje současně originální způsob zabezpečení pomocí destrukce elektronických a/nebo optických prvků, proto může být využit i u aplikací, vyžadujících vysokou bezpečnost a ochranu proti zneužití. V případě vyšší verze identifikační digitální pečeti s kryptoprocесorem v elektronickém čipu je možno považovat subjekt označený touto samolepicí pečeti za "digitálně podepsaný", tím je možno tuto technologii použít i v náročnějších e-aktivitách (aktivity spojené s využitím komunikace po Internetu).

30 Zásadní výhodou tohoto systému při použití identifikační digitální pečeti k identifikaci předmětu je v jejím jednoznačném svázání s tímto předmětem, na který je pečeť připevněna.

35 Další velkou výhodou je zabezpečovací prvek, například destrukční systém optických a/nebo elektronických prvků identifikační digitální pečeti, který má nesrovnatelně vyšší stupeň zabezpečení proti zneužití, než například jednoduché systémy "naříznutých" samolepek, používané např. u dálničních známek České republiky. V systému se po destrukci objeví nesmazatelný záznam o pokusu o odlepení identifikační digitální pečeti.

Přehled obrázků na výkresech

40 Technické řešení je blíže objasněno na přiložených výkresech, kde na obr. 1 je schematicky znázorněn příklad uspořádání jednotlivých dílů identifikační digitální pečeti, na obr. 2 je znázorněn systém komunikace a kontroly mytného identifikační digitální pečeti umístěné na vozidle a na obr. 3 je znázorněna varianta identifikační digitální pečeti s použitím identifikačního klíče, na obr. 3a při použití jedné pečeti a vyhodnocovacího obvodu se shodným identifikačním klíčem a na obr. 3b je znázorněno použití páru identifikačních digitálních pečeti se shodným identifikačním klíčem.

Příklad provedení technického řešení

45 Identifikační digitální pečeť 1, znázorněná na obr. 1 sestává ze zóny 2, která obsahuje prvky označující a identifikující předmět, například obrazové prvky, identifikační záznamy, ochranné

tiskové prvky, čárový kód a podobně, dále z modulu 3, obsahující elektronické prvky, například bezkontaktní pasivní radiofrekvenční čip RFID s výhodou typu DSRC, čip zajišťující bezdrátovou komunikaci, případně úložiště s kryptografickým klíčem či dokonce kryptografický procesor například čip s elektronikou RFID, kryptografický klíč a podobně, dále ze zabezpečovacího prvku 4, například samodestrukční vrstvy a připevňovací části 5, zajišťující dostatečně pevné spojení identifikační digitální pečeti 1 s předmětem, například samolepicí vrstvu a podobně, přičemž všechny části identifikační digitální pečeti 1 tvoří jeden nedělitelný celek. Zabezpečovací prvek 4 zajišťuje v součinnosti s připevňovací částí 5 ochranu proti snahám o neoprávněnou manipulaci, například odlepení identifikační digitální pečeti 1 tak, aby došlo k destrukci optických i elektronických prvků pečeti.

Při aplikaci identifikační digitální pečeti 1 do systému kontroly mýtného se identifikační digitální pečeť 1 nalepuje na okno vozidla, stejně jako dnes dálniční známka. Vozidlová jednotka 8 elektronického mýtného, označovaná jako OBU (On Board Unit - vozidlová a palubní jednotka daného elektronického dopravního systému), je doplněna o vyhodnocovací modul 7 s identifikátorem, komunikující s identifikační digitální pečeti 1, čímž je logicky zajištěno "zapečetění" vozidlové jednotky 8 elektronického mýtného ve vozidle a jednoznačné spojení vozidlové jednotky 8 elektronického mýtného s vozidlem. Kontrola pak probíhá jednak opticky pracovníkem 10 kontroly a elektronicky kontrolním modulem 9. Vozidlová jednotka 8 elektronického mýtného může být nejen identifikována s vozidlem, ale identifikační digitální pečeť 1 může dokonce kryptograficky podepisovat zaznamenávaná data.

Identifikační digitální pečeť 1 je nalepena na předmět identifikace a tím je jednoznačně svázána s tímto předmětem.

Vysoký stupeň zabezpečení věci proti zneužití identifikační digitální pečeti 1 zaručuje zabezpečovací prvek 4 identifikační digitální paměti 1, který zajistí v součinnosti s připevňovací vrstvou 5 identifikační digitální paměti 1 ochranu proti snahám o neoprávněnou manipulaci, například odlepení identifikační digitální pečeti 1 tak, aby došlo k destrukci optických i elektronických prvků pečeti, čímž bude identifikační paměť znehodnocena, což bude identifikováno kontrolním systémem.

Při aplikaci v systému čerpání pohonných hmot se identifikační digitální pečeť 1 nalepuje rovněž na okno vozidla, stejně jako dnes dálniční známka.

Vyhodnocovací modul 7 s identifikátorem na čerpacím stojanu identifikuje vozidlo a umožní čerpání a případně i zaplacení.

Při aplikaci v systému parkování nebo vjezdu do myčky se identifikační digitální pečeť 1 rovněž nalepuje na okno vozidla, stejně jako dnes dálniční známka. Vyhodnocovací modul 7 s identifikátorem na vstupu parkoviště nebo vjezdu do myčky identifikuje vozidlo a umožní poskytnutí služby a případně i zaplacení.

S výhodou lze identifikační digitální pečeť 1 kombinovat s párem privátních klíčů, kdy privátní identifikační klíč je obsažen v identifikační digitální pečeti 1 a druhý párový identifikační klíč je obsažen ve vyhodnocovacím modulu 7.

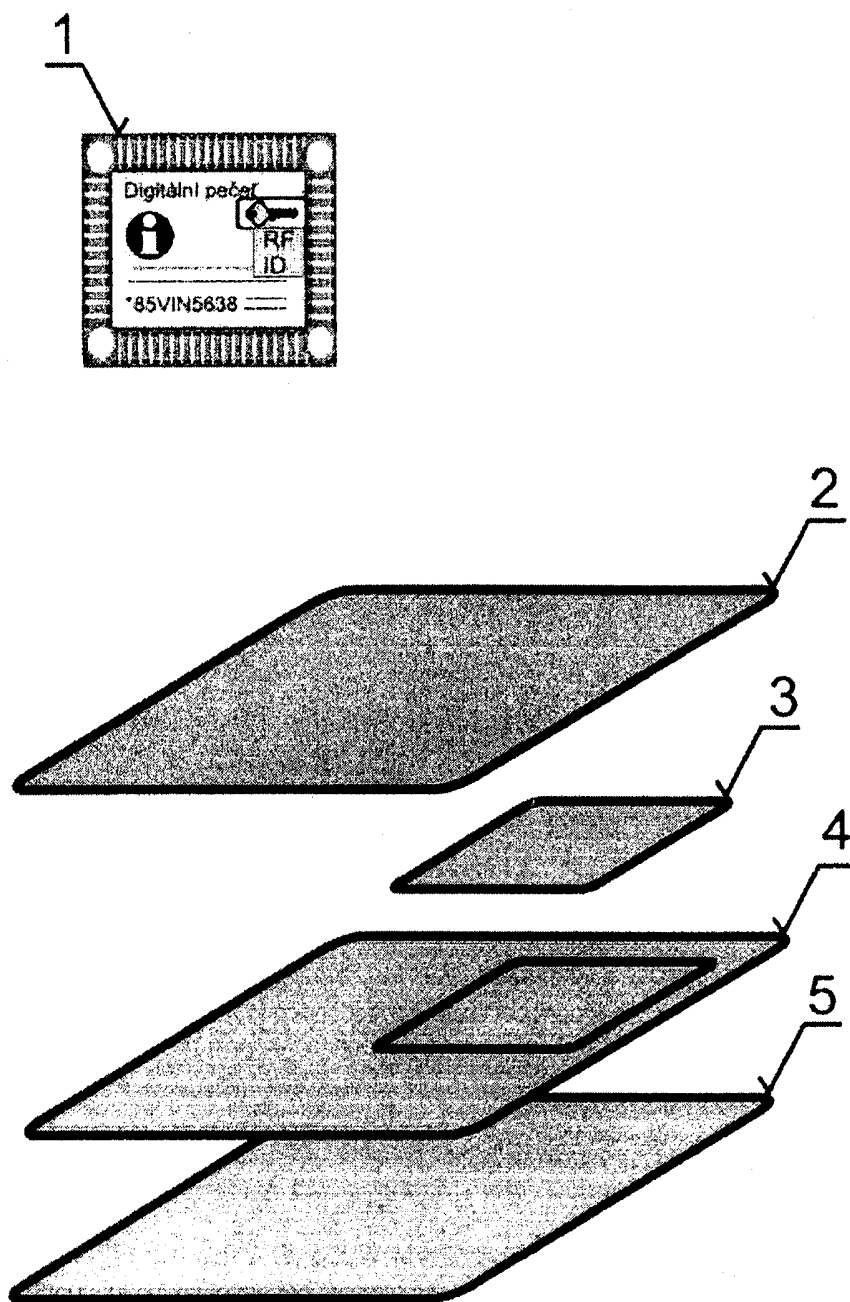
Další možnost použití identifikační digitální pečeti 1 s vysokým stupněm zabezpečení je použití dvojice až n-tice identifikačních digitálních pečeti 1, tzv. pečtní pár, podle možnosti až n-tice identifikačních digitálních pečeti 1 a případně ještě v kombinaci s privátním klíčem, kdy identifikační privátní klíč je právě obsažen ve dvojici, či n-tici, který se při identifikaci musí shodovat. Řídicí modul 6 páru identifikačních digitálních pečeti 1, případně i s veřejným klíčem, oslovuje jednotlivé pečeti a vyhodnocuje, zda pár patří k sobě.

V případě aplikaci pro "mýtné" je vydávána dvojice identifikačních digitálních pečeti 1, jedna se lepí na vozidlo, druhá na OBU. Není pak nutné programovat OBU.

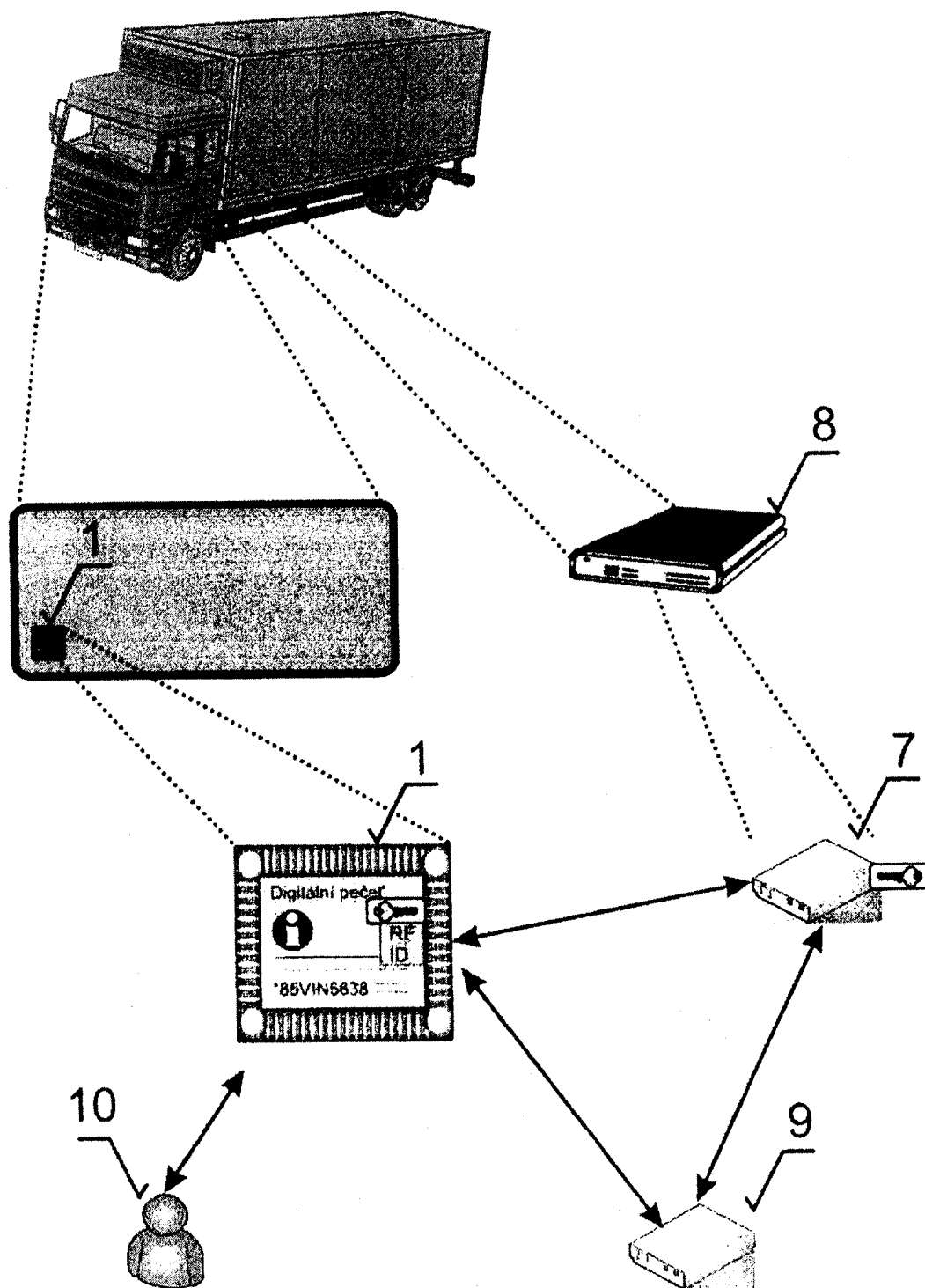
NÁROKY NA OCHRANU

- 5 1. Identifikační digitální pečeť, **v y z n a č u j í c í s e t í m**, že sestává ze zóny (2), která obsahuje označující a identifikující prvky opticky rozeznatelné, zejména hologramy, alfanumerické a grafické znaky, čárové kódy, dále sestává z modulu (3), obsahující prvky elektronicky identifikovatelné, zejména bezkontaktní radiofrekvenční čipy, např. RFID, DSRC, případně úlo-
žiště s kryptografickým klíčem nebo kryptografický procesor, dále sestává ze zabezpečovacího prvku (4) a připevňovací části (5), přičemž všechny prvky, tj. zóna (2), modul (3), zabezpečovací prvek (4) a připevňovací část (5) tvoří jeden nedělitelný celek.
- 10 2. Identifikační pečeť podle nároku 1, **v y z n a č u j í c í s e t í m**, že modul (3) obsahuje identifikátor evidovaný nezávislým systémem jako prvek n-tice identifikátorů.

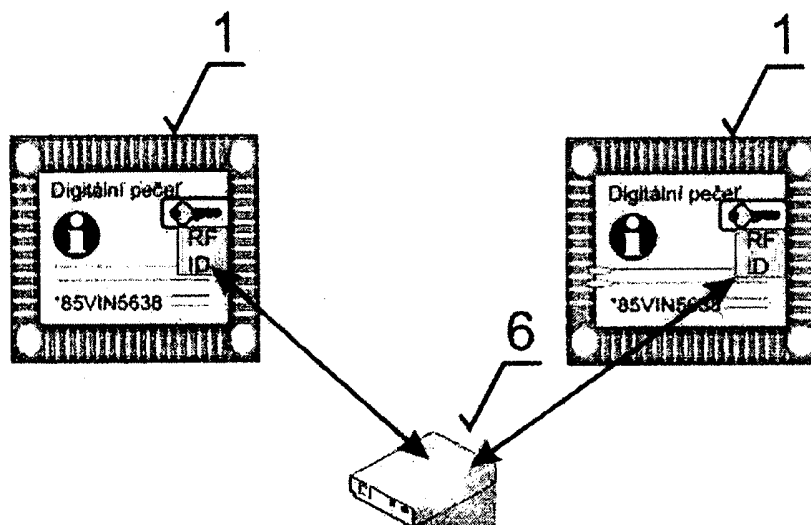
3 výkresy



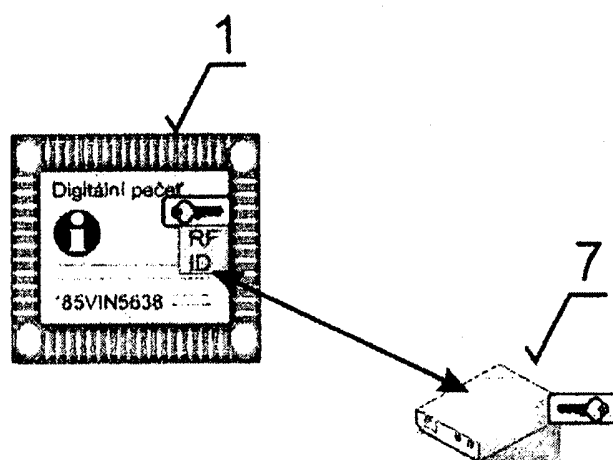
Obr. 1



Obr. 2



Obr. 3a



Obr. 3b

Konec dokumentu
