PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **05.01.2010**

(40) Datum zveřejnění přihlášky vynálezu: **10.08.2011**

(Věstník č. 32/2011)

(21) Číslo dokumentu:

2010-5

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

G06K 19/07	(2006.01)
G06K 19/10	(2006.01)
G06Q 90/00	(2006.01)

(71) Přihlašovatel:

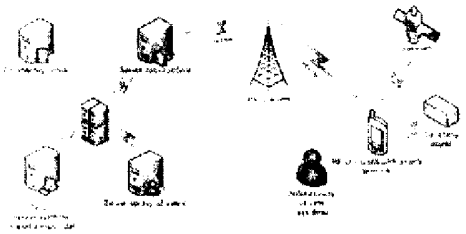
Vojtěch Lukáš Ing. Bc., Nahořany nad Metují, CZ
Fiala František, Kaplice, CZ

(72) Původce:

Vojtěch Lukáš Ing. Bc., Nahořany nad Metují, CZ

(74) Zástupce:

Ing. Václav Kratochvíl, patentový zástupce, Táborská 758/33, Mladá Boleslav, 29301



(54) Název přihlášky vynálezu:

Způsob zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace a zařízení k provádění tohoto způsobu

(57) Anotace:

Vynález se týká způsobu zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace. Produkt se opatří bezpečnostním prvkem obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedené ověření jeho pravosti. Jejich datové obrazy se uloží ve vzdálených databázích umístěných v databázovém serveru spravujícím identifikační čísla, jim odpovídající jednorázová hesla, korektní odpovědi na správně provedené transakce ověření pravosti a archivujícím údaje o provedených kontrolách. Dále se vynález týká zařízení k provádění tohoto způsobu, které je tvořeno bezpečnostním prvkem s parametrickou dobou odolnosti a s bezkontaktním přenosem informace obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedené ověření jeho pravosti, propojeným s databázovým serverem pro správu identifikačních čísla a jim odpovídajícího jednorázového hesla a obrazů korektních odpovědí a pro archivaci údaje o provedených kontrolách.

CZ 2010 - 5 A3

05.01.10
2010-5

Způsob zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace a zařízení k provádění tohoto způsobu.

Oblast techniky

Řešení se týká způsobu zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace a zařízení k provádění tohoto způsobu. Jedná se o univerzální bezpečnostní prvek sloužící jako náhrada stávajících cenin, pečetí, plomb, hologramů, kolků a jiných prostředků sloužících k ověření pravosti daného objektu či prostředky osvědčující zaplacení předepsaného poplatku nebo zamezující padělání či pozměňování úředních listin apod.

Dosavadní stav techniky

Fenomén nelegální ekonomiky představuje celosvětový problém. Výroba a distribuce nelegálních kopií značkových výrobků a léků, krácení poplatků a daní, prodej nekvalitních napodobenin a v důsledcích i obchod s lidmi jako levnou pracovní silou, to je jen základní výčet nelegálních aktivit, které lze pod nelegální ekonomiku zahrnout. Ověřování pravosti produktů v oblasti obchodních vztahů má rostoucí tendenci a objem těchto požadavků se bude geometricky zvyšovat.

Jednou z metod boje proti distribuci plagiátů jsou tradičně využívané bezpečnostní prvky, mezi něž patří nejrůznější pečetě, papírové ceniny či hologramy.

S rozvojem vědy a techniky však roste dostupnost speciálních výrobních technologií, použitelných k výrobě bezpečnostních prvků, široké technické veřejnosti. Následkem je jejich zneužívání nelegálními skupinami při výrobě napodobenin bezpečnostních prvků. Tyto metody zabezpečení, založené na optických a mechanických principech, tak přestávají plnit svou funkci.

Současné moderní metody zabezpečení elektronických dat využívají matematických a fyzikálních principů, které nabízí možnosti nastavení požadované míry bezpečnosti při jí odpovídajících finančních nákladech za realizované zabezpečení. Jednou z technologií, kterou

lze pro realizaci takovýchto bezpečnostních aplikací použít, je technologie radiofrekvenční identifikace RFID (Radio Frequency IDentification).

Každá změna dlouhodobě používaných a hojně rozšířených technologií představuje složitý technicko-ekonomický problém. Nechuť k inovacím a především finanční náklady spojené s inovací a provozem nové technologie jsou hlavními příčinami omezení technologického růstu obecně. Totéž platí i pro využití technologie RFID při vývoji a nasazení moderních bezpečnostních prvků. Ceny RFID identifikátorů tj. transpondérů s implementovanými bezpečnostními procedurami, které nabízí světové trhy, jsou stále nevyhovující. Výsledkem porovnání nákladů aplikací stávajících bezpečnostních prvků a prvků na bázi technologie RFID je zjištění, že dnes nabízené elektronické bezpečnostní prvky RFID jsou příliš nákladné, než aby mohly být nasazeny v širokém spektru použití.

Existující publikované či realizované nízkonákladové metody zabezpečení představují na první pohled perspektivní cesty realizace nízkonákladových bezpečnostních protokolů pro systémy RFID. Nízká spotřeba a relativně nízká náročnost jejich hardwarové implementace je jen zdánlivě předurčují k nejrůznějším bezpečnostním aplikacím.

Jednou stránkou problému jsou technické a technologické požadavky, druhou pak certifikace, normalizační a bezpečnostní požadavky. Drtivá většina publikovaných návrhů bezpečnostních protokolů však postrádá kvalitně provedenou bezpečnostní analýzu. Bezpečnostní analýza je přitom základní požadavek, který je nutný splnit ještě před zavedením identifikačních tj. bezpečnostních systémů do praxe a tuto analýzu musí garantovat odpovídající autorita z oblasti bezpečnosti.

Pro zabezpečené aplikace, například ve státní správě, je bezpodmínečně nutné použít systémů buď normalizovaných, tedy obecně uznávaných, prověřených a schválených, či systémů, u kterých je možné získat osvědčení o jejich bezpečnosti certifikovanou autoritou.

Většina existujících bezpečnostních aplikací RFID je využívána primárně k identifikaci objektů a jejich autentizaci. To se sebou přináší požadavky na vysoké čtecí rychlosti a tím i rychlé bezpečnostní protokoly. Identifikační procedury musí totiž umožňovat automatický sběr dat i u poměrně rychle se pohybujících objektů, a to společně s implementovanou funkcí antikolizního čtení tj. identifikace mnoha objektů v daném souboru či v daném balení.

Aplikace robustních a dostatečně rychlých bezpečnostních protokolů a funkcí má však za následek vysokou potřebu hradel pro jejich implementaci v RFID čipu, čímž rostou i finanční náklady na vyrobený čip. Důsledkem je i nárůst spotřeby elektrického výkonu, který je v čipu k dispozici.

Hlavním důsledkem implementací dostatečně bezpečných a rychlých bezpečnostních protokolů a funkcí je však vysoká spotřeba plochy křemíku čipu a tomu odpovídající nárůst finančních nákladů na jeho výrobu. Ve výsledku tak vznikají sice zabezpečené RFID transpondéry, ale jejich cena neumožňuje nasazení v nízkonákladových aplikacích, jako je například ochrana kusového zboží před paděláním, elektronické ceniny, kolky apod.

Požadavky na vysoké čtecí rychlosti a rychlé komunikační protokoly jsou navíc často velmi zbytečné. To platí i pro implementace antikolizních protokolů v systémech elektronických cenin.

Protože existují aplikace, které umožňují snížení požadovaných rychlostí identifikačních procedur i vyloučení požadavků na antikolizní čtení, vzniká tu prostor pro nízkonákladové bezpečnostní protokoly s parametrizovatelnou pravděpodobnostní bezpečností. Ta může být založena na fyzikální podstatě bezpečnostní funkce a její implementaci do odpovídajícího RFID transpondéru.

Podstata vynálezu

Výše uvedené nedostatky dosud používaných metod jsou do značné míry odstraněny způsobem zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace, podle tohoto vynálezu. Jeho podstatou je to, že produkt se opatří bezpečnostním prvkem obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření jeho pravosti a jejich datové obrazy se uloží ve vzdálených databázích umístěných v databázovém serveru spravujícím identifikační čísla, jim odpovídající jednorázová hesla, korektní odpovědi na správně provedené transakce ověření pravosti a archivujícím údaje o provedených kontrolách.

Při tomto způsobu se řídí a zabezpečuje síťový provoz mezi sítěmi s různou úrovní důvěryhodnosti. Zároveň je možné importovat a exportovat data o nových bezpečnostních prvcích a požadavky na testování pravosti a exportují se výsledky kontrolních aktivit.

Ve výhodném provedení se řídí činnost mobilních kontrolorů postupným zpřesňováním příkazu ke kontrole na dané pozici pro omezení předčasného prozrazení kontrolního místa s tím, že pozice kontrolního místa je lokalizačními systémy zpřesňována postupně, dle utajeného kontrolního plánu, a to až během přesunu oprávněného kontrolora na místo kontroly.

V podstatě se jedná o aplikaci nízkonákladového radiofrekvenčního prvku s parametrickou dobou odolnosti. Daný objekt se opatří NRBP (Nízkonákladový radiofrekvenční bezpečnostní prvek) s bezkontaktním přenosem dat.

Minimalizaci výrobních nákladů na NRBP při zachování potřebné míry bezpečnosti je realizována přesunutím většiny bezpečnostně citlivých procedur do vzdálených serverových aplikací, to znamená do serverů a spolupracujících databází, které jsou zabezpečeny silnými bezpečnostními procedurami. Jejich bezpečnost vždy odpovídá vynaloženým nákladům. Vzdálené databáze lze relativně snadno zabezpečit standardními bezpečnostními postupy a lze je ochránit i fyzicky proti útokům hrubou silou, a to i díky jejich centralizaci.

Každý identifikátor NRBP obsahuje své jedinečné identifikační číslo ROM_ID, umožňující jeho sledování a identifikaci. Dále pak jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření pravosti NRBP. Tato čísla jsou uložena v pevné paměti ROM či (EE)PROM. Jejich obrazy jsou pak uloženy ve vzdálených databázích.

Celý proces identifikace označeného objektu začíná autentizací oprávněného uživatele identifikačního HW – tedy terminálu. Terminál uživatele žádá o své ověření pomocí uživatelského jména a přihlašovacího hesla, přičemž doplňkem pro zvýšení bezpečnosti může být i ověření oprávněného uživatele pomocí čteček otisků prstů atd. K autentizaci terminálu a tím i uživatele je výhodné využít například standardů SSH (Secure Shell) realizujících zabezpečený přenos dat po nezabezpečeném přenosovém kanálu.

Další akce mohou být podmíněny testováním polohy terminálu, například pomocí systému GPS a až poté, co je terminál dopraven na správné místo, může započít kontrolní činnost.

Příkaz ke kontrole na dané konkrétní pozici tj. v dané provozovně, může sloužit k omezení předčasného prozrazení kontrolního místa. Pozice může být navíc systémem zpřesňována postupně, dle utajeného kontrolního plánu, a to až během přesunu uživatele na místo kontroly - kontrolovanou provozovnu.

Po úspěšné autentizaci terminálu i uživatele a dosažení zadané GPS polohy místa pro inspekci mohou být započaty procedury identifikace objektů a následné verifikace jejich původu.

Jak je v bezdrátových identifikačních technologiích obvyklé, čtečka umístěná v terminálu začne vysílat modulovaný VF (vysokofrekvenční) signál na frekvenci nosného kmitočtu. Tato VF energie je přijata anténou transpondéru NRBP a slouží pro napájení vnitřních obvodů. Pokud je přijatá energie dostatečná, začne NRBP vysílat své identifikační číslo ROM_ID. Tato data jsou terminálem zaslána do vzdáleného serveru, který jako odpověď vrátí základní popis objektu tj. například informaci o tom, že identifikovaný objekt je lahev daného typu alkoholu, objemu, výrobní šarže či výrobce.

Tato veřejná data mohou být použita pro základní orientaci v souboru testovaných objektů, ale mohou sloužit i pro necertifikované aplikace obchodního charakteru u výrobců, prodejců, dodavatelů či zákazníků.

Následovat může vlastní verifikační transakce, která je dostupná pouze autentizovanému terminálu a uživateli provádějícímu inspekční činnost.

Odezvu NRBP na verifikační transakci je možné prodloužit použitím přídavného umělého zpoždění, a to jeho implementací přímo do procedury testující shodu datových řetězců ID&JH s ROM_ID&ROM_HESLO.

Parametr bezpečnostní odolnosti totiž souvisí s velikostí vyčítané paměti a také celkovou dobou realizace vyčítání. Podle bezpečnostního protokolu, který je využit, lze

celkovou dobu odolnosti vypočítat jako součin doby běhu jednoho dotazu na pravost NRBP a počtu možných kombinací, kterými je možné se ptát na pravost NRBP. Tím je definována bezpečnostní odolnost NRBP vůči útokům hrubou silou.

Protože celková doba zpoždění má přímou souvislost s odolností vůči útoku hrubou silou, je zřejmé, že implementace přídavného umělého zpoždění může snížit spotřebu paměťových buněk NRBP. Proceduru „čekej dobu t" lze obvodově realizovat standardním synchronním čítačem s dekodérem adresy, nebo ještě výhodněji pomocí frekvenční děličky. Jejich hardwarová implementace zabere jistou plochu křemíkového čipu taktéž.

K uvedenému způsobu slouží zařízení tvořené bezpečnostním prvkem s parametrickou dobou odolnosti a s bezkontaktním přenosem informace obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření jeho pravosti propojeným s databázovým serverem pro správu identifikační čísla a jim odpovídajícího jednorázového hesla a obrazů korektních odpovědí a pro archivaci údaje o provedených kontrolách.

Zařízení s výhodou obsahuje server zabezpečení pro řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti. Dále může obsahovat server správy systému pro import a export dat a server správy uživatelů pro řízení činnosti mobilních kontrolorů.

Zařízení je s výhodou připojeno k bezdrátovým komunikačním sítím pro komunikaci mezi vzdálenými serverovými systémy a terminály mobilních inspektorů. Bezpečnostní prvek může být tvořen radiofrekvenčním prvkem opatřeným anténní strukturou vytvářenou přímo na křemíkovém čipu.

Zvolená doba odolnosti bezpečnostního prvku je dána součinem všech možných kombinací ROM_HESLA a dobou nutnou k realizaci jednoho testu ověření pravosti. Zařízení využívá k zajištění požadované doby bezpečnostní odolnosti implementace modulů umělého přídavného zpoždění a omezené velikosti paměti pro hardwarovou realizaci bezpečnostních procedur. Bezpečnostní prvek může být v podobě náhrady a/nebo doplňku papírových kolků a jiných cenin a/nebo pečetí.

Jádrem NRBP je tedy elektronický čip, jehož hlavní částí je paměť ROM uchovávající uložená data veřejná (ROM_ID) i neveřejná (ROM_heslo a ROM_OK). Z pohledu bezpečnostní odolnosti NRBP lze uvažovat především o útoku hrubou silou, kdy útočník může provádět útok na jednorázové heslo JH pomocí jeho hádání, tzn. zkoušení různých kombinací. Maximální potřebná doba nutná pro uhodnutí odpovídající odpovědi na JH je dána součinem počtu potřebných pokusů tj. počtem jednotlivých možných variant JH a doby realizace jednoho pokusu.

Při minimalizaci hardwarové náročnosti NRBP s parametrickou dobou odolnosti lze uvažovat o dvou možných způsobech zajištění požadované nízké hodnoty pravděpodobnosti uhodnutí hodnoty ROM_heslo. První metodou je zvětšování velikosti paměti ROM, druhou je prodlužování doby odezvy NRBP.

Minimalistickým uspořádáním NRBP je kombinace implementace omezené paměti ROM a asynchronní děličky, a to v případě požadavku na snížení pravděpodobnosti prolomení zabezpečení pamětí heslem o jeden řád. Implementace metody umělého zpoždění tak může přinést úsporu hardwarových prostředků tj. plochy křemíkového čipu v řádu jednotek až desítek procent – přibližně 2,9 až 35,4 % v porovnání s řešením využívajícím rozšiřování paměti ROM.

Ve výhodném provedení jsou významnou položkou omezení nákladů na kompletní NRBP také anténní struktury vytvářené přímo na křemíkovém čipu OCA (On-Chip Antenna), a to jak pro induktivní napájení NRBP, tak i pro případ NRBP pracujících ve vzdálené zóně. Experimenty ověřily možnost dalšího snižování nákladů na RFID transpondéry pro speciální aplikace o více než 25 %, čímž mohou významně přispět k novým aplikacím NRBP.

Přehled obrázků na výkresech

Vynález bude podrobněji popsán na konkrétním příkladu provedení s pomocí přiložených výkresů. Kde na Obr. 1 je znázorněn telekomunikační řetězec pro systém využívající NRBP. Na Obr. 2 je znázorněn bezpečnostní protokol systému s NRBP. Na Obr. 3 je uveden vývojový diagram funkcionality NRBP s procedurou „čekej_dobu_t" a na Obr. 4 je příklad struktury NRBP s implementovanou anténní strukturou.

05.01.10

Příklad provedení

Příkladem provedení je NRBP (Nízkonákladový radiofrekvenční bezpečnostní prvek s parametrickou dobou odolnosti) sloužící jako náhrada či doplněk papírového kolku pro ochranu jednotlivých balení zboží zatíženého spotřební daní. Mezi tyto výrobky patří například lahve s alkoholickými nápoji či cigaretové krabičky.

V evropské unii se spotřebuje ročně více než 10^{11} kusů lahví s alkoholem a cigaretových krabiček. V případě aplikace NRBP po dobu 20 let je třeba označit počet objektů $2*10^{12}$. Pro takovýto soubor unikátních identifikátorů je nutné využít paměť ROM o kapacitě 41 bitů.

Část paměti ROM_OK postačí o velikosti 8 bitů.

Při požadavku na pravděpodobnostní odolnosti prolomení NRBP, po dobu 20-ti let, danou jevem uhodnutí P(uhodnutí)=$7,17*10^{-8}$ je třeba ROM_HESLO o velikosti 63 bitů.
S využitím standardizované struktury záhlaví a obsahu čipu NRBP dostáváme:

- Záhlaví – indikace typu transpondéru 2 bity
- Výrobce 8 bitů
- ROM_ID 41 bitů
- ROM_HESLO 63 bitů
- ROM_OK 8 bitů
- CRC 8 bitů

V případě využití struktury NRBP s omezenou pamětí ROM_HESLO a asynchronní děličkou lze uspořit plochu čipu v rozmezí 2,9 až 35,4 % podle typu implementace NRBP, což umožní vznik nízkonákladového NRBP a to díky minimalizaci ceny za jeden kus čipu při zachování bezpečnostní odolnosti.

Další snížení nákladů na NRBP lze realizovat řešením anténních systémů NRBP přímo na křemíkovém čipu, což může přinést úsporu nákladů ve výši více než 25%. Takové uspořádání pro kmitočet 9 GHz a rozměry transpondéru NRBP 1.12 x 0.57 mm je uvedeno na obr. 4.

Vzdálené databáze a serverové aplikace uspořádané podle obr. 1 slouží k vykonávání bezpečnostních procedur a jejich vyhodnocování. Databázový server spravuje identifikační čísla NRBP transpondérů a jim odpovídající jednorázová hesla, archivuje údaje o provedených kontrolách tj. čas, datum, identifikaci kontrolora, souřadnice GPS apod.

Server zabezpečení má za úkol provádět standardní funkce firewallu, tedy řídit a zabezpečovat síťový provoz mezi sítěmi s různou úrovní důvěryhodnosti. To vše směrem k GSM sítím, které systém využívá, i směrem k sítím využívaným pro správu systému a vyhodnocování dat.

Server správy systému slouží pro import a export dat, kdy importem jsou především informace o nových bezpečnostních prvcích, které vstupují do systému, a požadavky na testování pravosti. Exportem jsou pak výsledky kontrolních aktivit.

Server správy uživatelů je podpůrným nástrojem pro řízení činnosti mobilních kontrolorů - osob konajících inspekční činnost v terénu.

Síť GSM slouží pro komunikaci mezi vzdálenými serverovými systémy a terminály mobilních inspektorů. Systém GPS je použit jako kontrolní nástroj inspekční činnosti. RFID – GSM/GPRS/GPS terminál je nástrojem pro mobilní inspekci původu aplikovaných bezpečnostních prvků.

Označený objekt je opatřen nízkonákladovým bezpečnostním prvkem a autorizovaný uživatel systému je reprezentován inspektory v terénu.

Každý identifikátor NRBP obsahuje své jedinečné identifikační číslo ROM_ID, umožňující jeho sledování a identifikaci. Dále pak jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření pravosti NRBP. Tato čísla jsou uložena v pevné paměti ROM či (EE)PROM. Jejich obrazy jsou pak uloženy ve vzdálených databázích.

Celý proces identifikace označeného objektu, podle protokolu na obr. 2, začíná autentizací oprávněného uživatele identifikačního HW – tedy terminálu. Terminál uživatele žádá o své ověření pomocí uživatelského jména a přihlašovacího hesla tj. doplňkem pro

zvýšení bezpečnosti může být i ověření oprávněného uživatele pomocí čteček otisků prstů atd. K autentizaci terminálu a tím i uživatele je výhodné využít např. standardů SSH (Secure Shell) realizujících zabezpečený přenos dat po nezabezpečeném přenosovém kanálu.

Další akce mohou být podmíněny testováním polohy terminálu, například pomocí systému GPS a až poté, co je terminál dopraven na správné místo, může započít kontrolní činnost.

Příkaz ke kontrole na dané konkrétní pozici tj. v dané provozovně může sloužit k omezení předčasného prozrazení kontrolního místa. Pozice může být navíc systémem zpřesňována postupně, dle utajeného kontrolního plánu, a to až během přesunu uživatele na místo kontroly - kontrolovanou provozovnu. Po úspěšné autentizaci terminálu i uživatele a dosažení zadané GPS polohy místa pro inspekci mohou být započaty procedury identifikace objektů a následné verifikace jejich původu.

Jak je v bezdrátových identifikačních technologiích obvyklé, čtečka umístěná v terminálu začne vysílat modulovaný VF (vysokofrekvenční) signál na frekvenci nosného kmitočtu. Tato VF energie je přijata anténou transpondéru NRBP a slouží pro napájení vnitřních obvodů. Pokud je přijatá energie dostatečná, začne NRBP vysílat své identifikační číslo ROM_ID. Tato data jsou terminálem zaslána do vzdáleného serveru, který jako odpověď vrátí základní popis objektu, například informaci o tom, že identifikovaný objekt je lahev daného typu alkoholu, objemu, výrobní šarže či výrobce. Tato veřejná data mohou být použita pro základní orientaci v souboru testovaných objektů, ale mohou sloužit i pro necertifikované aplikace obchodního charakteru u výrobců, prodejců, dodavatelů či zákazníků.

Následovat může vlastní verifikační transakce, která je dostupná pouze autentizovanému terminálu a uživateli provádějícímu inspekční činnost: autorizovaný terminál žádá vzdálený server o jednorázové heslo JH, které odpovídá danému objektu podle ROM_ID, serverová aplikace otestuje, zdali nebylo již toto heslo v historii použito a pokud ano, pak posoudí místo dříve provedené identifikační a verifikační transakce. Z historie identifikace a případné verifikace daného objektu lze usuzovat na pravděpodobnost zjištění plagiátu daného NRBP. Toto posouzení však citlivě závisí na zaznamenané historii, typu zboží a jeho deklarovaném pohybu na trhu. Pokud nebylo jednorázové heslo JH použito, je zasláno do terminálu. Pokud již použito bylo, může být zasláno taktéž, avšak s odpovídajícím

příznakem vícenásobné verifikace. Následuje komunikační transakce mezi terminálem a NRBP zajišťující vzájemnou synchronizaci datového toku po bezdrátovém médiu na takt vnitřního oscilátoru v NRBP. Terminál žádá NRBP o jeho ROM_ID a synchronizuje svůj takt s taktem oscilátoru NRBP. Terminál vysílá repliku ROM_ID a následně též JH do NRBP. NRBP synchronně porovnává uložené ROM_ID a JH s přijímaným datovým tokem.

Pokud přijímaný datový tok ROM_ID a JH odpovídá datům uloženým v NRBP, pak NRBP v synchronním taktu vysílá odpověď ROM_OK zpět terminálu. Terminál zašle ROM_OK data do vzdáleného serveru k ověření. Serverová aplikace zašle výsledek verifikace autorizovanému terminálu. Uživatel provede další kroky - vizuální nebo fyzická kontrola, řešení nedostatků atd.

Pokud by došlo během realizace identifikační nebo verifikační procedury k chybě v datové komunikaci, mohlo by tím dojít i k omylu při ověření pravosti. Tuto chybu lze eliminovat dvěma základními postupy s rozdílnou hardwarovou náročností jejich implementace (nízkou a vysokou): vícenásobným opakováním identifikační a verifikační procedury nebo aplikací metod zabezpečení přenosu dat - kontrolní součet, parita, atd.

Odezvu NRBP na verifikační transakci je možné prodloužit použitím přídavného umělého zpoždění, a to jeho implementací přímo do procedury testující shodu datových řetězců ID&JH s ROM_ID&ROM_HESLO. Začlenění procedury „čekej dobu T“ do vývojového diagramu NRBP je znázorněno na obr. 3.

Parametr bezpečnostní odolnosti totiž souvisí s velikostí vyčítané paměti a také celkovou dobou realizace vyčítání. Podle bezpečnostního protokolu, který je využit, lze celkovou dobu odolnosti vypočítat jako součin doby běhu jednoho dotazu na pravost NRBP a počtu možných kombinací, kterými je možné se ptát na pravost NRBP. Tím je definována bezpečnostní odolnost NRBP vůči útokům hrubou silou.

Protože celková doba zpoždění má přímou souvislost s odolností vůči útoku hrubou silou, je zřejmé, že implementace přídavného umělého zpoždění může snížit spotřebu paměťových buněk NRBP. Proceduru „čekej dobu t“ lze obvodově realizovat standardním synchronním čítačem s dekodérem adresy, nebo ještě výhodněji pomocí frekvenční děličky. Jejich hardwarová implementace zabere jistou plochu křemíkového čipu taktéž.

Jádrem NRBP je elektronický čip, jehož hlavní částí je paměť ROM uchovávající uložená data veřejná (ROM_ID) i neveřejná (ROM_heslo a ROM_OK). Z pohledu bezpečnostní odolnosti NRBP lze uvažovat především o útoku hrubou silou, kdy útočník může provádět útok na jednorázové heslo JH pomocí jeho hádání, tzn. zkoušení různých kombinací. Maximální potřebná doba nutná pro uhodnutí odpovídající odpovědi na JH je dána součinem počtu potřebných pokusů (počtem jednotlivých možných variant JH) a doby realizace jednoho pokusu.

Průmyslová využitelnost

NRBP lze využít v podobě univerzálního bezpečnostního prvku s ambicí nahradit stávající ceniny, pečetě, plomby, hologramy, kolky a jiné prostředky soužící k ověření pravosti daného objektu či prostředky osvědčující zaplacení předepsaného poplatku nebo zamezit padělání či pozměňování úředních listin apod. Tím může tento prvek značně přispět k omezení rozsahu nelegální ekonomiky a posílit fiskální zdroje států nebo unií států bez nutnosti měnit platné zákony. Může rovněž výrazně omezit možnosti pro obcházení nebo porušování platného práva a eliminovat procesy, které jsou deformovány korupcí se všemi negativními následky.

05.01.10
2010-5

PATENTOVÉ NÁROKY

1. Způsob zabezpečení produktů pomocí bezpečnostního prvku s bezkontaktním přenosem informace, ***vyznačující se tím, že*** produkt se opatří bezpečnostním prvkem obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření jeho pravosti a jejich datové obrazy se uloží ve vzdálených databázích umístěných v databázovém serveru spravujícím identifikační čísla, jim odpovídající jednorázová hesla, korektní odpovědi na správně provedené transakce ověření pravosti a archivujícím údaje o provedených kontrolách.

2. Způsob podle nároku 1, ***vyznačující se tím, že*** se řídí a zabezpečuje síťový provoz mezi sítěmi s různou úrovní důvěryhodnosti.

3. Způsob podle nároku 1 nebo 2, ***vyznačující se tím, že*** se importují a exportují data o nových bezpečnostních prvcích a požadavky na testování pravosti a exportují se výsledky kontrolních aktivit.

4. Způsob podle kteréhokoli z uvedených nároků, ***vyznačující se tím, že*** se řídí činnost mobilních kontrolorů postupným zpřesňováním příkazu ke kontrole na dané pozici pro omezení předčasného prozrazení kontrolního místa s tím, že pozice kontrolního místa je lokalizačními systémy zpřesňována postupně, dle utajeného kontrolního plánu, a to až během přesunu oprávněného kontrolora na místo kontroly.

5. Zařízení k provádění způsobu podle kteréhokoli z výše uvedených nároků, ***vyznačující se tím, že*** je tvořeno bezpečnostním prvkem s parametrickou dobou odolnosti a s bezkontaktním přenosem informace obsahujícím své jedinečné identifikační číslo ROM_ID, pro umožnění jeho sledování a identifikaci a jednorázové heslo ROM_HESLO a odpověď ROM_OK na správně provedenou transakci ověření jeho pravosti propojeným s databázovým serverem pro správu identifikační čísla a jim odpovídajícího jednorázového hesla a obrazů korektních odpovědí a pro archivaci údaje o provedených kontrolách.

6. Zařízení podle nároku 5, ***vyznačující se tím, že*** obsahuje server zabezpečení pro řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti.

7. Zařízení podle nároku 5 nebo 6, ***vyznačující se tím, že*** obsahuje server správy systému pro import a export dat.

8. Zařízení podle nároku 5, 6 nebo 7, ***vyznačující se tím, že*** obsahuje server správy uživatelů pro řízení činnosti mobilních kontrolorů.

9. Zařízení podle nároku 8, ***vyznačující se tím, že*** je připojeno k bezdrátovým komunikačním sítím pro komunikaci mezi vzdálenými serverovými systémy a terminály mobilních inspektorů.

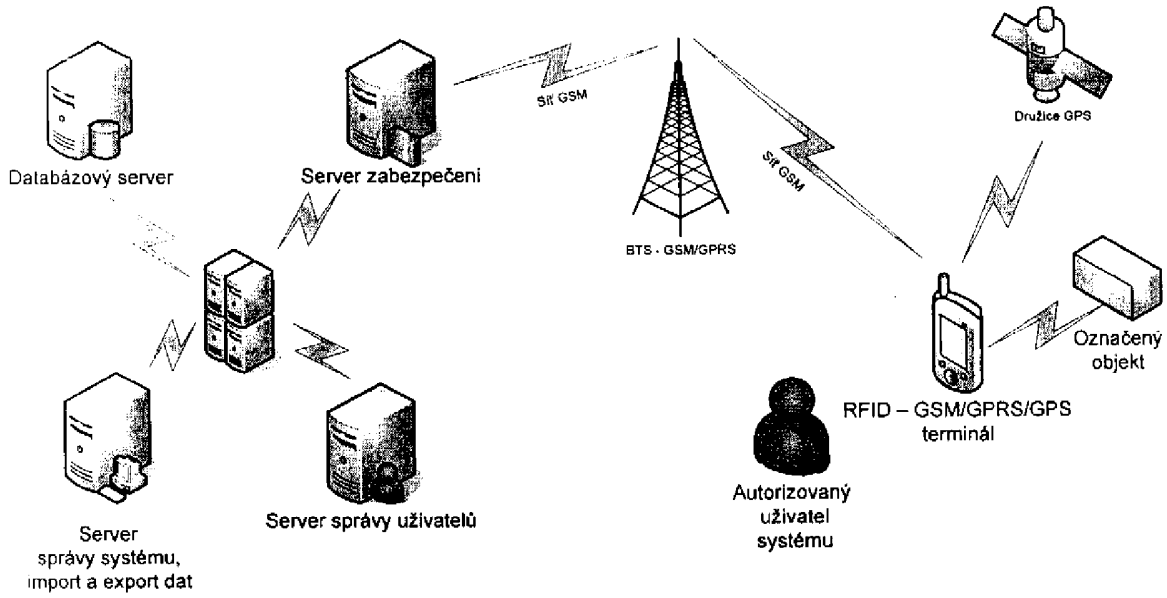
10. Zařízení podle kteréhokoli z předchozích nároků, ***vyznačující se tím, že*** bezpečnostní prvek je radiofrekvenční prvek opatřený anténní strukturou vytvářenou přímo na křemíkovém čipu.

11. Zařízení podle kteréhokoli z předchozích nároků, ***vyznačující se tím, že*** zvolená doba odolnosti bezpečnostního prvku je dána součinem všech možných kombinací ROM_HESLA a dobou nutnou k realizaci jednoho testu ověření pravosti.

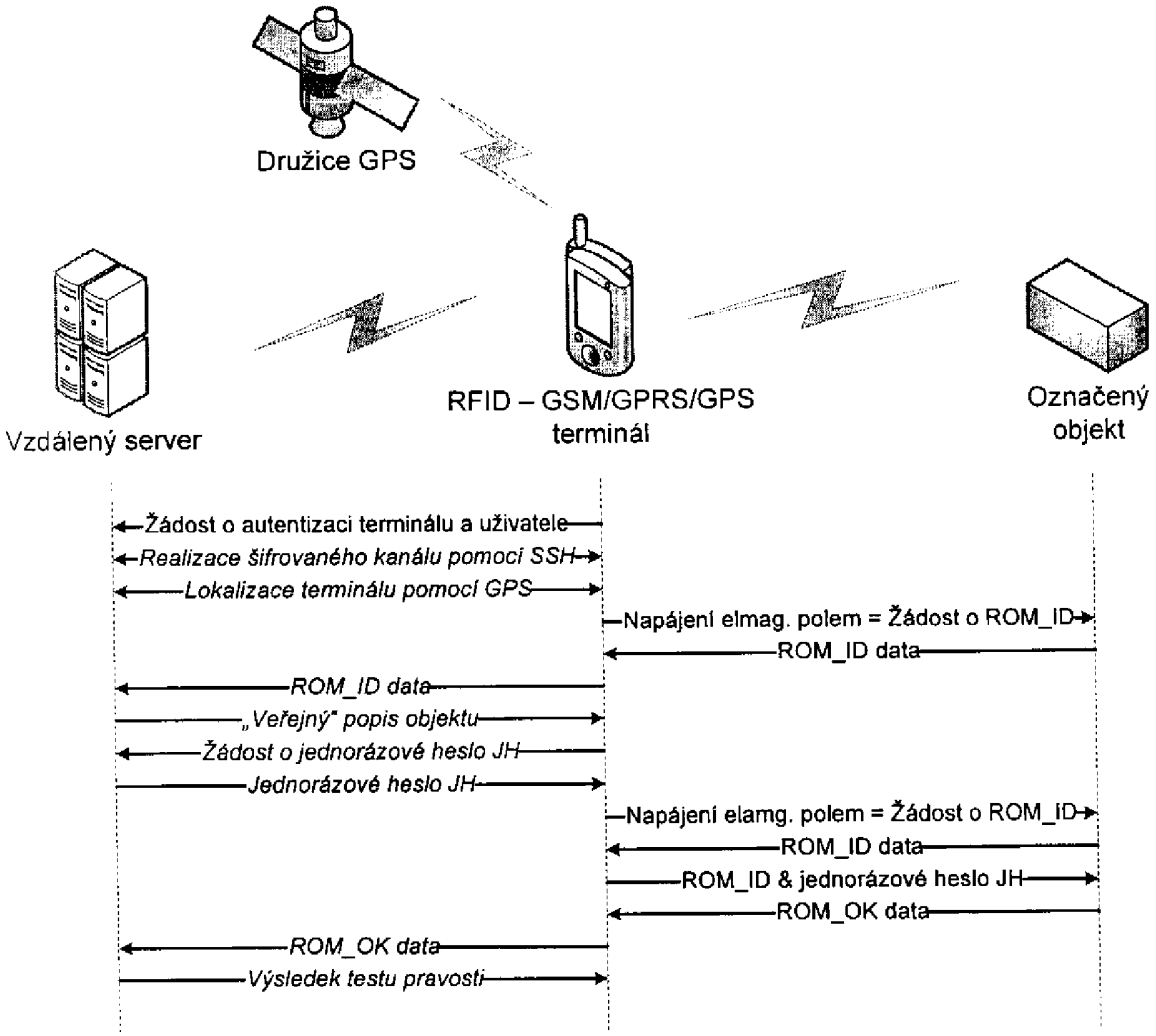
12. Zařízení podle kteréhokoli z předchozích nároků, ***vyznačující se tím, že*** využívá k zajištění požadované doby bezpečnostní odolnosti implementace modulů umělého přídavného zpoždění a omezené velikosti paměti pro hardwarovou realizaci bezpečnostních procedur.

13. Zařízení podle kteréhokoli z předchozích nároků, ***vyznačující se tím, že*** bezpečnostní prvek je v podobě náhrady a/nebo doplňku papírových kolků a jiných cenin a/nebo pečetí.

05.01.10
2010-5

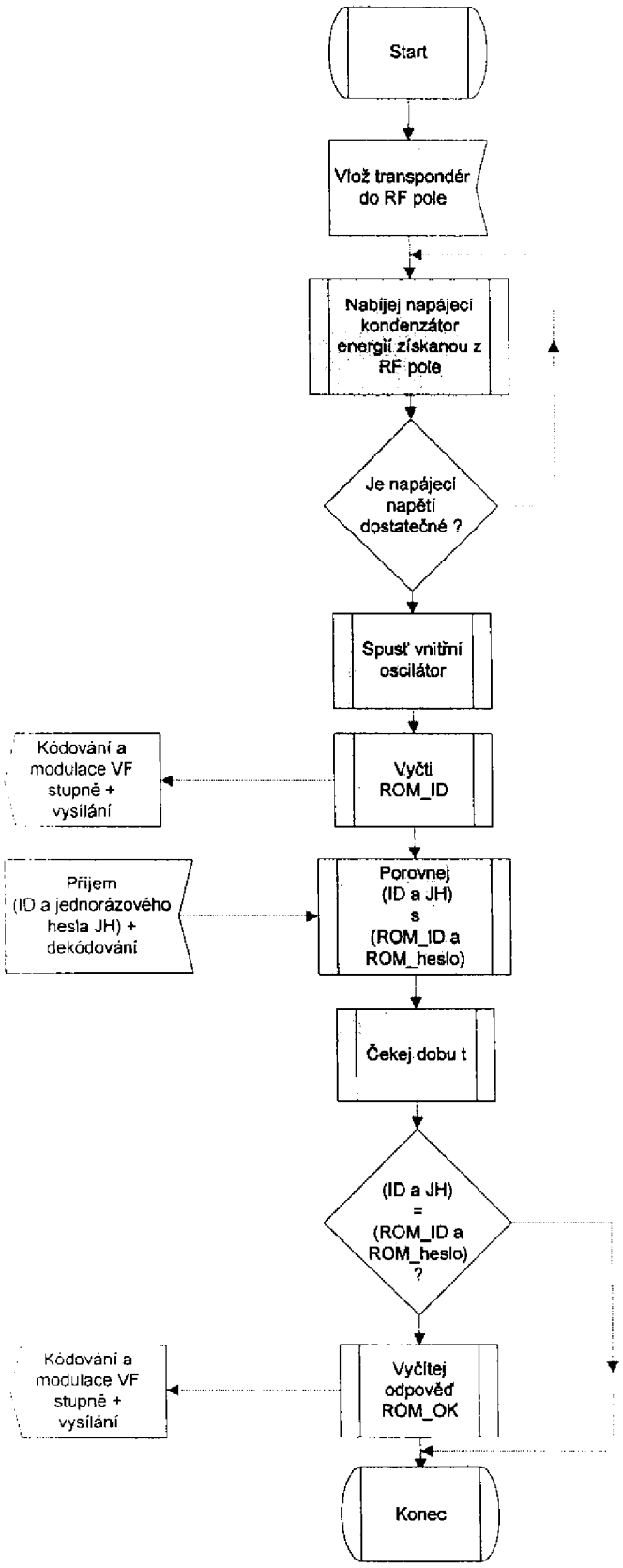


Obr. 1


Družice GPS
Vzdálený server
RFID – GSM/GPRS/GPS terminál
Označený objekt
Žádost o autentizaci terminálu a uživatele
Realizace šifrovaného kanálu pomocí SSH
Lokalizace terminálu pomocí GPS
Napájení elmag. polem = Žádost o ROM_ID
ROM_ID data
ROM_ID data
„Veřejný" popis objektu
Žádost o jednorázové heslo JH
Jednorázové heslo JH
Napájení elamg. polem = Žádost o ROM_ID
ROM_ID data
ROM_ID & jednorázové heslo JH
ROM_OK data
ROM_OK data
Výsledek testu pravosti

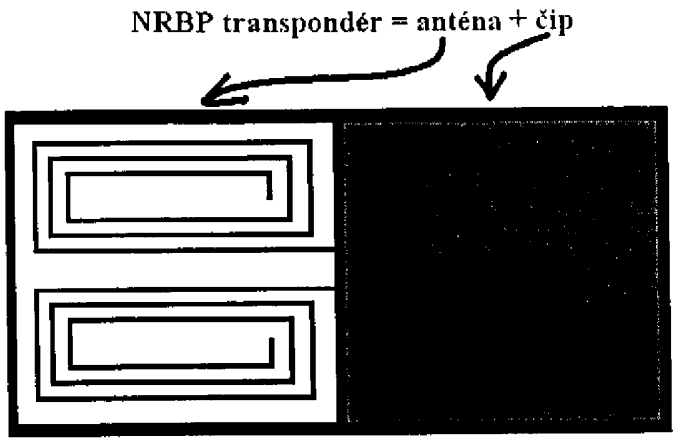
Obr. 2

05.01.10
2010-5



Obr. 3

05.01.10
2010-5



Obr. 4