SLOVENSKÁ REPUBLIKA

(19) **SK**

ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PATENTOVÁ PRIHLÁŠKA

(22) Dátum podania prihlášky: **28. 6. 2002**
(31) Číslo prioritnej prihlášky: **101 31 254.7**
(32) Dátum podania prioritnej prihlášky: **1. 7. 2001**
(33) Krajina alebo regionálna organizácia priority: **DE**
(40) Dátum zverejnenia prihlášky: **5. 10. 2004**
Vestník ÚPV SR č.: **10/2004**
(62) Číslo pôvodnej prihlášky v prípade vylúčenej prihlášky:
(86) Číslo podania medzinárodnej prihlášky podľa PCT: **PCT/DE02/02348**
(87) Číslo zverejnenia medzinárodnej prihlášky podľa PCT: **WO03/005307**

(11), (21) Číslo dokumentu:

1627-2003

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7] :

G07B 17/00,
G07D 7/00,
G07D 7/20

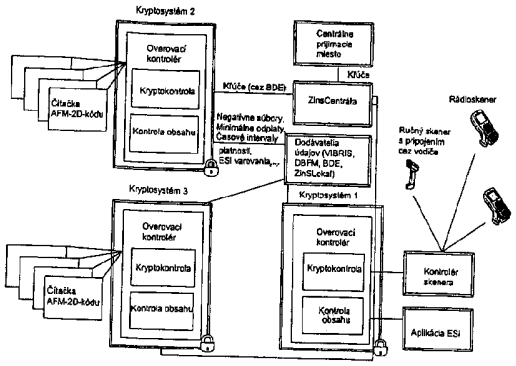
(71) Prihlasovateľ: **DEUTSCHE POST AG, Bonn, DE;**

(72) Pôvodca: **Delitz Alexander, Bonn, DE;**
Fery Peter, Zwingenberg, DE;
Helmus Jürgen, Bonn, DE;
Höhl Aloysius, Fulda, DE;
Meier Gunther, Reinheim, DE;
Robel Elke, Bonn, DE;
Stumm Dieter, Grossefehn, DE;

(74) Zástupca: **Holoubková Mária, Ing., Bratislava, SK;**

(54) Názov: **Spôsob kontroly platnosti digitálnych výplatných znakov**

(57) Anotácia:
Spôsob overenia pravosti výplatného znaku, umiestneného na poštovej zásielke. Podľa tohto vynálezu sa kryptografická informácia, nachádzajúca sa vo výplatnom znaku, dekóduje a použije na overenie pravosti výplatného znaku. Spôsob podľa tohto vynálezu je charakterizovaný tým, že čítacia jednotka graficky nasníma výplatný znak a prenesie ho do kontrolnej jednotky a kontrolná jednotka riadi postupnosť čiastkových kontrol.



SK 1627-2003 A3

Spôsob kontroly platnosti digitálnych výplatných znakov

Oblasť techniky

Vynález sa týka spôsobu kontroly platnosti digitálnych výplatných znakov.

Doterajší stav techniky

Je známe, že sa poštové zásielky vybavujú digitálnymi výplatnými znakmi.

Aby sa odosielateľom poštových zásielok uľahčilo vytvorenie výplatných znakov, je napríklad pri frankovacom systéme, ktorý používa Deutsche Post AG, možné vytvoriť výplatné znaky v systéme zákazníka a cez ľubovoľné rozhranie ich dodať na tlačiareň.

Aby sa zabránilo zneužitiu tohto spôsobu, digitálne výplatné znaky obsahujú kryptografické informácie, napríklad o identite systému zákazníka, ktorý riadi vytvorenie výplatného znaku.

Vynález má za úlohu vytvoriť spôsob, ktorým sa dá pravosť výplatných znakov rýchlo a spoľahlivo skontrolovať. Najmä má byť tento spôsob vhodný na kontrolu v nasadení pre veľké série, najmä v listových alebo prepravných centrách.

Podstata vynálezu

Táto úloha je podľa tohto vynálezu vyriešená tým, že čítacia jednotka graficky nasníma výplatný znak a zašle ho kontrolnej jednotke, a že kontrolná jednotka riadi priebeh čiastkových kontrol.

Je zvlášť účelné, keď jedna z čiastkových kontrol zahrnuje dekódovanie kryptografických informácií, nachádzajúcich sa vo výplatnom znaku.

Zahrnutím dekódovania kryptografických informácií do procesu kontroly sa umožní zistiť pravosť výplatných znakov okamžite, takže sa môže uskutočniť kontrola online - najmä v priebehu spracovania poštovej zásielky v stroji na jej spracovanie.

Ďalej je výhodné, keď jedna z čiastkových kontrol zahrnuje porovnanie dátumu vytvorenia výplatného znaku s aktuálnym dátumom. Zahrnutie dátumu vytvorenia výplatného znaku - najmä v zakódovanej forme - zvyšuje bezpečnosť údajov, pretože porovnaním dátumu vytvorenia výplatného znaku s aktuálnym dátumom sa zabráni viacnásobnému použitiu výplatného znaku na prepravu poštových zásielok.

Na ďalšie zvýšenie rýchlosti kontroly je výhodné, keď si čítacia jednotka a kontrolná jednotka vymieňajú informácie pomocou synchrónneho protokolu.

V inej, tiež účelne výhodnej forme uskutočnenia vynálezu komunikujú čítacia jednotka a kontrolná jednotka navzájom cez asynchrónny protokol.

Pritom je zvlášť výhodné, keď čítacia jednotka pošle kontrolnej jednotke údajový telegram.

Tento údajový telegram výhodne obsahuje obsah výplatného znaku.

Ďalšie výhody, zvláštnosti a účelné ďalšie varianty vynálezu vyplývajú z podnárokov a nasledujúceho opisu výhodných príkladov uskutočnenia pomocou výkresov.

Na výkresoch znázorňujú

Obr. 1 principiálne znázornenie systémových komponentov systému na zabezpečenie odplaty;

Obr. 2 zvlášť výhodnú formu uskutočnenia systému na zabezpečenie odplaty, ručný skener a PC na zabezpečenie odplaty;

Obr. 3 principiálne znázornenie vytvárania a kontroly výplatných znakov;

Obr. 4 prehľad komponentov kryptosystému;

Obr. 5 výhodnú formu uskutočnenia spôsobu kontroly;

Obr. 6 ďalšiu zvlášť výhodnú formu uskutočnenia spôsobu kontroly so zvlášť výhodným priebehom čiastkových kontrol;

Obr. 7 výhodný priebeh rozdelenia kľúčov medzi centrálnym prijímacím miestom (Postage Point - poštové miesto) a jednotlivými kryptografickými kontrolnými jednotkami (Cryptoserver - kryptoserver).

V ďalšom znázorníme vynález na príklade PC-frankovacieho systému. Kroky spôsobu, ktoré slúžia na zabezpečenie odplaty, sú pritom nezávislé od systému, použitého na vytvorenie výplatných znakov.

Znázornená decentralizovaná kontrola na jednotlivých kontrolných miestach, najmä v listových centrách, je zvlášť výhodná, ale rovnako je možná centralizovaná kontrola.

V prvej forme uskutočnenia vynálezu sa výhodne uskutoční kontrola pravosti výplatných znakov náhodným spôsobom jednotlivými skenermi.

Na tento účel vhodný kontrolný systém obsahuje výhodne komponenty, ktoré sú znázornené na obr. 1.

Na obr. 1 je znázornené, s ktorými čiastkovými systémami je kryptosystém v nejakom vzťahu. Tieto sú ďalej stručne opísané.

Skenery

Skenery slúžia na načítanie frankovacieho znaku PC-frankovania. Pri frankovacích znakoch ide o 2D-kódy vo forme údajovej matice s použitou opravou chyby ECC200. Podľa typu skenera sa údaje prenášajú rádiom alebo káblom, pričom rádioskenery majú viacmiestny displej a tým možnosť výstupu a dotykovú obrazovku, resp. klávesnicu na základné vstupy. Rozhranie medzi skenermi a ostatnými systémami výhodného PC-frankovacieho systému na zabezpečenie odplaty tvoria ako komponenty kontrolér skenera a overovací kontrolér. Zatiaľ čo kontrolér skenera riadi frontu maticových kódov, ktoré, prichádzajúc cez ručný skener, čakajú na kontrolu a v podstate udržiava styk so skenermi, s ostatnými systémami je v styku len cez overovací skener (kontrolér).

Kontrolér skenera/overovací kontrolér

Kontrolér skenera, resp. overovací kontrolér slúžia ako rozhranie medzi skenermi a ďalšími systémami na kontrolu 2D-čiarového kódu. Im sa sprostredkuje z optického snímania konvertovaný a na chyby opravený obsah 2D-čiarového kódu, a tie potom dajú podnet na kontrolu a v prípade rádioskenerov sa postarajú o výstup výsledku čítania a kontroly a slúžia ako rozhranie medzi prípadne

nevyhnutným manuálnym dodatočným spracovaním a kontrolami kontrolóra a ostatnými systémami.

Kryptosystém

Kryptosystém sa stará o obsahovú a kryptografickú kontrolu obsahu 2D-čiarového kódu, ako aj o chránené zapamätanie údajov a algoritmov, podstatných z hľadiska bezpečnosti. Jednotlivé komponenty uvedieme ďalej.

Miesto prijímania obnosov na poplatky (Postage Point)

Miesto prijímania obnosov na poplatky (Postage Point) je centrálnym systémom v rámci PC-frankovania. Slúži ako rozhranie k systémom zákazníkov. Z neho môžu zákazníci vyberať obnosy z predplatného na následné frankovanie. V mieste prijímania obnosov na poplatky (Postage Point) sa generujú kľúče na zabezpečenie spôsobu. Ďalej slúži ako rozhranie k zúčtovacím systémom. Pre výhodný systém na zabezpečenie odplaty na PC-frankovanie sa vytvoria nasledujúce rozhrania:

- informácie o zásielke cez 2D-čiarový kód,
- symetrické kľúče,
- kmeňové údaje, ako napríklad obnosy predplatného, stavy účtov.

Výhodné centrálne systémy na zabezpečenie odplaty

Vo výhodnom centrálnom systéme na zabezpečenie odplaty sa zberajú informácie, ktoré sa týkajú zásielok, a dajú sa k dispozícii iným systémom. Tu sa uskutočňuje vytváranie prevádzkových správ, ktoré zasa vedú k vytvoreniu negatívnych súborov. Centrálny systém na zabezpečenie odplaty ďalej dostane od miesta prijímania obnosov na poplatky (Postage Point) aktuálne údaje o kľúčoch a tieto prevedie do jednotlivých kryptoserverov.

Dodávatelia údajov

Na kontrolu obsahu 2D-čiarového kódu je potrebný rad kmeňových údajov, ako napríklad negatívne súbory, minimálne odplaty, časové intervaly platnosti vo

vzťahu k produktu a kódy varovania na zabezpečenie odplaty a kódy ďalšieho spracovania. Tieto údaje pripravujú rôzne systémy (BDE, VIBRIS, lokálny systém na zabezpečenie odplaty).

Aplikácia zabezpečenia odplaty

S aplikáciou zabezpečenia odplaty má AGB-kontrolór, ktorý musí dodatočne spracovať vyradené zásielky z PC-frankovania, možnosť detailne skontrolovať frankovanie, pri ktorom zobrazenie výsledkov kontroly nebude obmedzené ohraničenými výstupnými možnosťami skenera. Naviac tu môže kontrolór zohľadniť aj ďalšie údaje, ako napríklad časový interval platnosti obnosu poštovného, na ktorý sa aktuálna zásielka vzťahuje, ako aj obnos a požadované frankovanie.

Automatické snímanie 2D-čiarového kódu

Automatické snímanie 2D-čiarového kódu sa uskutočňuje v rámci SSA. Na tento účel sa obrazové informácie prevedú na čítačku AFM-2D-kódu. Tam sa uskutoční konverzia obrazu na obsah kódu údajovej matice. V nadväznosti na to sa obsah 2D-čiarového kódu sprostredkuje na kontrolu kryptosystému, ktorý vyhodnotí vrátený výsledok kontroly a sprostredkuje ho optickému snímaciemu systému (IMM) na zakódovanie zásielky. Výhodné súčasti takto rozšíreného spôsobu kontroly sú znázornené na obr. 2.

Čítačka AFM-2D-kódu

Na jeden čítací stroj (ALM/ILVM) existuje jedna čítačka AFM-2D-kódu, ktorá dostane obrazové údaje cez optický snímací systém (IMM) a na účely zabezpečenia odplaty ich ďalej spracuje. V rámci výhodného PC-frankovania na zabezpečenie odplaty to v prípade rozpoznaného 2D-kódu znamená, že z obrazových údajov sa extrahuje kód 2D-údajovej matice a pomocou spôsobu ECC200 na opravu chýb ho premení na reťazec bajtov, ktorý predstavuje obsah 2D-čiarového kódu.

Tento reťazec bajtov sa odovzdá na kontrolu overovaciemu kontroléru. Výsledok kontroly sa následne cez rozhranie optického snímacieho systému prevedie ďalej a tam sa použije na kódovanie.

Kryptosystém pre čítačku AFM-2D-kódu

Podľa vlastností kryptokariet sa dá počítať napríklad s asi 27 kontrolami za sekundu. Pretože rýchlosť čítacích strojov je asi 10 prečítaných zásielok za sekundu, nezdá sa byť účelným kombinovať každú čítačku AFM-2D-kódu s kryptosystémom. K tomu si treba uvedomiť, že sa tiež nedá vychádzať z predpokladu, že sa PC-F-zásielky budú stopercentne vytvárať na všetkých strojoch súčasne. Preto sa zdá byť účelným kryptosystémy oddeliť a viaceré PC-F-čítačky prevádzkovať s jedným kryptosystémom. Riešenie by sa pritom malo zvoliť tak, aby sa dalo odstupňovať, teda aby boli možné viaceré kryptosystémy na jedno listové centrum. To je napríklad významné pre listové centrá s vysokým výskytom zásielok a vysokým počtom čítacích strojov, pri ktorých sa na začiatku môže vytvoriť druhý kryptosystém. Okrem toho sa neskôr v prevádzke pri zodpovedajúcej potrebe môže zvýšiť počet serverov.

Príslušná architektúra sa pritom na zníženie zložitosti môže výhodne zvoliť tak, aby jednotlivé čítacie stroje boli pevne priradené jednému kryptosystému a prípadne sa ešte môže rozšíriť o prídavnú záložnú konfiguráciu, ktorá sa v prípade chyby pokúsi prejsť na iný kryptosystém.

Oddelenie kryptosystému a čítačiek AFM-2D-kódu okrem toho prináša výhodu, že tak strojové čítanie, ako aj kontrola ručným skenerom sa môžu uskutočniť s tým istým kryptosystémom, a preto sa rovnaká funkcia nemusí implementovať dvojmo, čo ponúka naviac aj podstatné výhody pri implementácii vynálezu.

Výhodné kroky spôsobu na vybavenie poštovej zásielky digitálnym výplatným znakom po vybratí obnosu na poplatok z centrálneho prijímacieho miesta (Postage Point) a vytvorenie výplatného znaku lokálnym PC, ako aj následné dodanie poštovej zásielky a kontrola výplatného znaku, naneseného na poštovú zásielku, sú znázornené na obr. 3.

Nezávisle od rozdelenie kľúčov prebieha tento postup tak, že zákazník najprv zloží obnos poštovného vo svojom PC. Na označenie požiadavky sa pritom vygeneruje náhodné číslo. Na mieste prijímania obnosov na poplatky (Postage Point) sa vytvorí zákazníkovi nový obnos poštovného a zo sprostredkovaného náhodného čísla, ďalších informácií k identite systému zákazníka (identifikačné údaje o systéme zákazníka, v ďalšom označené ako Postage ID) a k obnosu poštovného sa vytvorí takzvaný kryptoreťazec, ktorý sa zakóduje tajným symetrickým kódom, existujúcim na mieste prijímania obnosov na poplatky (Postage Point).

Tento kryptoreťazec a zodpovedajúci obnos poštovného sa následne prenesú do PC zákazníka a spolu s náhodným číslom sa uložia do jeho "Safe-Box", bezpečného pred nežiaducimi prístupmi.

Keď potom zákazník v nadväznosti na tento postup ofrankuje získaným obnosom poštovného poštovú zásielku, zasielacie údaje, významné pre 2D-čiarový kód, okrem iného kryptoreťazec, dátum frankovania a obnos frankovania, rozšírené o náhodné číslo a Postage ID v nezakódovanej forme, sa zhromaždia a vytvorí sa kontrolný pseudosúčet, ktorý jednoznačne označuje obsah.

Pretože náhodné číslo v zakódovanej forme existuje v kryptoreťazci, ako aj v nezakódovanej forme v kontrolnom pseudosúčte, zabezpečí sa, že údaje o zásielke sa nemôžu zmeniť, resp. ľubovoľne generovať, a je možné zistiť ich tvorcu.

Relevantné údaje o zásielke sa potom následne pretransformujú na 2D-čiarový kód a ako zodpovedajúci frankovací znak sa tlačiarňou zákazníka vytlačia na zásielku. Hotová zásielka sa potom môže odovzdať do poštového obehu.

Pri zvlášť výhodnej forme uskutočnenia zabezpečenia odplaty sa 2D-čiarový kód načíta v listovom centre čítačkou AFM-2D-kódu, resp. ručným skenerom a následne sa skontroluje. S tým spojené kroky procesu sú zreteľné z obrázka pod číslami postupu 5 - 8. Na kontrolu správnosti 2D-čiarového kódu odovzdá čítačka AFM-2D-kódu kompletné údaje o zásielke kryptosystému. Tam sa kryptografická informácia, obsiahnutá v zasielacích údajoch, najmä v kryptoreťazci, dekóduje, aby sa zistilo náhodné číslo, použité na vytvorenie kontrolného pseudosúčtu.

Následne sa zistí kontrolný pseudosúčet (nazývaný aj Message Digest) k údajom o zásielke, vrátane dekódovaného náhodného čísla, a skontroluje sa, či je výsledok identický s kontrolným pseudosúčtom, nachádzajúcim sa v 2D-čiarovom kóde.

Okrem kryptografického overenia sa uskutočnia ešte ďalšie kontroly obsahu (číslo postupu 7b), ktoré napríklad vylúčia dvojnásobné použitie 2D-čiarového kódu, resp. skontrolujú, či sa zákazník nestal nápadným pokusmi o podvod, a preto je uvedený v negatívnom súbore.

Zodpovedajúci výsledok kontroly sa potom sprostredkuje PC-F-čítačke, ktorá výsledok odovzdá optickému snímaciemu systému (IMM) na zakódovanie čiarového kódu. Čiarový kód sa následne nastrieka na list a zásielky sa pri negatívnom výsledku kontroly vyradia.

Architektúra kryptosystému

Prehľad komponentov

Obr. 4 prináša prehľad čiastkových komponentov kryptosystému, pričom popísané šípky predstavujú prúdy vstupných a výstupných údajov k externým systémom. Pretože výhodný centrálny systém zabezpečenia odplaty sa používa ako otáčavý kotúč pri rozdeľovaní kľúčov miesta prijímania obnosov na poplatky (Postage Point) na kryptosystémy lokálnych systémov zabezpečenia odplaty a tieto údaje sa medzitým musia zapamätávať, treba tiež vytvoriť komponent kryptosystému, pri ktorom sa však spravidla nepoužije overovací kontrolér.

Čiastkové komponenty kryptosystému v ďalšom opíšeme podrobnejšie.

Overovací kontrolér

Overovací kontrolér predstavuje rozhranie na kontrolu kompletného obsahu 2D-čiarového kódu. Kontrola 2D-čiarového kódu pozostáva z obsahovej a kryptografickej kontroly. Na tento účel treba načítaný obsah 2D-čiarového kódu v skeneroch poslať cez kontrolér skenera do overovacieho kontroléra.

Pretože sa zodpovedný kontrolér skenera pre káblom pripojený skener a overovací kontrolér nachádzajú v rôznych počítačových systémoch, predpokladá sa medzi nimi komunikácia na základe TCP/IP, pričom namiesto čistého Socket-programovania ponúka výhody použitie na ňu nasadeného protokolu. V rámci kryptosystému tu prichádzajú do úvahy v rámci zberu prevádzkových údajov (BDE) používaný riadiaci program pre telegramy, alebo v rámci optického snímacieho systému používaný protokol, ako napríklad Corba/IIOP.

Overovací kontrolér spustí jednotlivé kontrolné programy, ktoré mu zasa späť sprostredkujú výsledky svojej kontroly.

Pretože budú súčasne v činnosti viacerí AGB-kontrolóri s rôznymi skenermi, overovací kontrolér sa musí dimenzovať ako "multisession"-schopný. To znamená, že musí byť schopný spracovať súčasné požiadavky na kontrolu a zodpovedajúci výstup nasmerovať na správny skener. Okrem toho by mal byť dimenzovaný tak, aby bol schopný súčasne spracovať viaceré požiadavky na kontrolu, ako aj paralelne s tým časť kontrolných krokov, napríklad kontrolu kontrolného pseudosúčtu a kontrolu minimálnej odplaty.

Na začiatku relácie sa kontroléru oznámi, s akým typom skenera komunikuje, a dostane priradenú možnosť aktivovať CallBack-metódou programy na výstup a na manuálnu kontrolu. Podľa druhu prevádzky a typu skenera sa výsledky potom pošlú buď rádioskeneru alebo systému zabezpečenia odplaty, ako aj sa zaznamenajú výsledky manuálnej kontroly.

Kryptokarta

Zvláštnu problematiku predstavuje uchovávanie kľúča, ktorým je zakódovaný kryptoreťazec v 2D-čiarovom kóde a na kontrolu sa opäť musí dekódovať. Tento kľúč zaručuje bezpečnosť 2D-čiarového kódu proti sfalšovaniu a preto nesmie byť možné ho vypátrať. Preto sa musí špeciálnymi bezpečnostnými opatreniami zaručiť, aby tento kľúč nebol nikdy v nešifrovanom texte na disku, v pamäti alebo pri prenose viditeľný a naviac musí byť zabezpečený účinným kryptografickým spôsobom.

Riešenia, ktoré sa zakladajú len na softvéri, tu neprinášajú spoľahlivú bezpečnosť, pretože na nejakom mieste systému sa kľúč predsa len objaví v nešifrovanom texte, alebo by sa kľúč dal v dekódovanom texte v pamäti prečítať nejakým debuggerom (ladiacim programom). Toto nebezpečenstvo spočíva predovšetkým aj v tom, že systémy sa dajú spravovať vzdialeným spôsobom, prípadne by sa za účelom opravy mohli dostať mimo vlastnej budovy.

Okrem toho kryptografické postupy predstavujú veľké zaťaženie pre procesor systému, ktorý vzhľadom na operácie, ktoré má vykonať, nie je optimalizovaný.

Preto sa odporúča použiť kryptoprocesorovú kartu s nasledujúcimi znakmi:

- špeciálny kryptoprocesor na zrýchlenie kryptografického postupu,

- uzavretý Black-Box systém na zabránenie prístupu k údajom a postupom, ktoré sú z bezpečnostného hľadiska kritické.

Pri kartách, ktoré spĺňajú tieto znaky, ide o autarkné (sebestačné, uzavreté) systémy, ktoré sú podľa vyhotovenia spojené s počítačom cez PCI- alebo ISA-zbernicu a komunikujú cez ovládač so softvérovými systémami na počítači.

Popri batériou napájanej hlavnej pamäti majú tieto karty energeticky nezávislú pamäť ROM, do ktorej sa dá zapamätať individuálny kód použitia. Priamy prístup do hlavnej pamäte kariet nie je z externých systémov možný, v dôsledku čoho je zaručená veľmi vysoká bezpečnosť, pretože tak ku kľúčovým údajom, ako aj ku kryptografickému postupu na uvoľnenie bezpečnosti sa nedá pristupovať ináč než cez zabezpečený ovládač.

Okrem toho karty sledujú prostredníctvom svojich vlastných snímačov, či dochádza k pokusom o manipuláciu (podľa vyhotovenia karty, napríklad teplotné maximá, žiarenie, otvorenie ochranného krytu, napäťové maximá).

Ak dôjde k takému pokusu o manipuláciu, obsah batériou napájanej hlavnej pamäte sa ihneď vymaže a uskutoční sa vypnutie karty.

Pre kryptoserver by sa mali funkcia dekódovania Postage ID, funkcia kontroly kontrolného pseudosúčtu, ako aj funkcia importovania kľúčových údajov nahrať priamo na kartu, pretože tieto programy majú veľký bezpečnostný význam.

Ďalej by mali byť všetky kryptografické kľúče, ako aj konfigurácie certifikátov, ktoré sú nevyhnutné na uskutočnenie autentizácie, tiež zabezpečené v batériou napájanej pamäti karty. Ak karta nemá dostatočnú pamäť, spravidla na karte existuje Master Key, ktorým sa vyššie uvedené údaje dajú zakódovať a následne uložiť na disk systému. To však vyžaduje, aby sa pred použitím týchto informácií tieto údaje najprv opäť dekódovali.

Nasledujúca tabuľka poskytuje prehľad modelov kariet, ktoré prichádzajú do úvahy, od rôznych výrobcov a súčasne uvádza ich osvedčenia.

Kryptokarty na použitie v rámci výhodného systému na zabezpečenie odplaty pre PC-frankovanie

Výrobca	Označenie typu	Osvedčenie
IBM	4758-023	FIPS PUB 140-1 Level 3 a ZKA-eCash
IBM	4758-002	FIPS PUB 140-1 Level 4 a ZKA-eCash (predpoklad 07/2000) CCEAL 5 (podaná žiadosť, v súčasnosti vo fáze certifikácie)
Utimaco	KryptoServer	ITSEC-E2 a ZKA-eCash
Utimaco	KryptoServer 2000 (dostupný v 1. kv./01)	FIPS PUB 140-1 Level 3, ITSEC-E3 a ZKA-eCash (podaná žiadosť)
Racal/Zaxus	WebSentry PCI	FIPS PUB 140-1 Level 4

Popri splnení požiadaviek, kladených na kartu, je kvôli žiaducemu osvedčeniu od BSI tiež veľmi dôležité, ktoré osvedčenia jednotlivé modely v súčasnosti majú a ktoré osvedčenia sa v súčasnosti nachádzajú v procese vyhodnotenia.

Certifikáty, vydané pre tieto výrobky, sa pritom delia na tri stupne, určované rôznymi certifikačnými miestami.

ITSEC je Európskou komisiou zverejnený súbor kritérií na certifikovanie IT-produktov a IT-systémov s ohľadom na ich bezpečnostné vlastnosti. Ohodnotenie dôveryhodnosti sa riadi podľa stupňov E0 až E6, pričom E0 znamená nedostatočnú a E6 najvyššiu bezpečnosť. Ďalším vývojom a harmonizáciou s podobnými medzinárodnými štandardami sú CC (Common Criteria), ktoré sa v súčasnosti nachádzajú v procese štandardizácie pri ISO (ISO norma 15408). Tento regulačný nástroj sa používa na ohodnotenie bezpečnosti systému.

Z vyššie uvedenej tabuľky v súčasnosti neexistuje žiadny výrobok, ktorý by mal certifikát podľa CC. IBM-model 4758-002 sa však v súčasnosti nachádza vo fáze takejto certifikácie.

Štandard FIPS PUB 140-1 je súbor kritérií, vydaných americkou vládou, na hodnotenie bezpečnosti komerčných kryptografických prístrojov. Tento súbor kritérií sa orientuje predovšetkým podľa vlastností hardvéru. Hodnotenie sa uskutočňuje v 4 stupňoch, pri ktorých Level 1 znamená najnižšiu a Level 4 najvyššiu bezpečnosť.

Okrem vyššie uvedeného štandardu hodnotenia existuje ďalší súbor kritérií, ktorý vydáva Centrálny kreditný výbor (Zentral Kreditausschuss - ZKA) a upravuje prevádzku IT-systémov a IT-produktov v oblasti "electronic cash".

Popri už uvedených vlastnostiach kariet a pridelených certifikátoch však existuje ešte rad ďalších výhod, ktoré stručne uvádzame ďalej:

- možnosť vytvorenia vlastného softvéru a jeho prenesenia na kartu,
- integrovaný generátor náhodných čísel (FIPS PUB 140-1 certifikovaný),
- DES, Triple DES a SHA-1 implementované na strane hardvéru,
- vytvorenie RSA-Key a spracovanie Private/Public Key pre kľúče až do dĺžky 2048 bitov,
- funkcie Key Management,
- funkcie správy certifikátu,
- čiastočne možná paralelná prevádzka viacerých kryptokariet v jednom systéme.

Kryptorozhranie

V rámci aplikácie kryptokariet sa funkcie, ktoré sú významné pre bezpečnosť, zapamätajú priamo v karte, a preto sú zvonku prístupné len cez ovládač karty. Ako rozhranie medzi ovládačom a overovacím kontrolérom slúži komponent kryptorozhrania, ktorý prevádza požiadavky na kontrolné programy cez ovládač na kartu.

Pretože sa v rámci jedného počítača môžu použiť viaceré karty, úlohou kryptorozhrania je aj uskutočniť rozdelenie jednotlivých kontrolných požiadaviek podľa zaťaženia. Táto funkcia je účelná najmä vtedy, keď kontrolné programy kryptosystému používajú naviac ešte jedna alebo podľa listového centra viaceré čítačky AFM-2D-kódu.

Ďalšia úloha spočíva v odvíjaní sa komunikácie za účelom rozdelenia kľúčových údajov. V stupni 2 existuje prípadne len základný mechanizmus, ktorý prenáša kľúče, zakódované kvôli bezpečnosti, v rámci signovaného súboru údajov. Požiadavka na kryptorozhranie potom spočíva v tom, aby sa pripravil pomocný program, ktorý umožní importovanie takéhoto súboru údajov.

Funkcie kryptosystému

Priebeh kontroly v overovacom kontroléri

Na kontrolu 2D-čiarového kódu dá overovací kontrolér k dispozícii centrálnu kontrolnú funkciu ako rozhranie k systémom skenerov, resp. čítacím systémom. Táto kontrolná funkcia koordinuje priebeh jednotlivých čiastkových kontrol.

Kódy, sprostredkované z jednotlivých čiastkových kontrol pre prípad zabezpečenia odplaty, sa pomocou vopred definovanej tabuľky, ktorá sa výhodne ošetruje centrálne a prenáša sa na kryptosystém, premenia na kód zabezpečenia odplaty. V rámci tejto tabuľky sa naviac stanovia priority, ktoré regulujú, ktorý kód zabezpečenia odplaty sa priradí, keď sa rozpoznajú viaceré prípady zabezpečenia odplaty.

Tento kód zabezpečenia odplaty sa potom spolu s opisujúcim textom pošle späť ako výsledok kontroly. Podľa systému na ďalšie spracovanie mimo

kryptosystému sa tento výsledok potom vydá rádioskeneru alebo v rámci aplikácie na zabezpečenie odplaty, resp. sa pri automatickej kontrole konvertuje na TIT2-kód a potlačí sa ním zásielka.

Pretože postupy medzi systémami ručných skenerov a automatickými čítacími systémami sú rozdielne, pre oba prípady použitia sa implementuje odlišná funkcia.

Podľa toho, ktorý komunikačný mechanizmus medzí čítacím systémom a overovacím kontrolérom sa použije, sa líši vyvolanie a vrátenie výsledkov. V prípade použitia synchrónneho protokolu na báze RPC, ako napríklad Corba/IIOP, sa kontrolná metóda priamo vyvolá a výsledky kontroly sa odovzdajú po skončení kontroly. Klient, teda kontrolér skenera, resp. čítací systém čakajú v tomto prípade na vypracovanie a vrátenie výsledkov kontroly. V posledne uvedenom prípade sa preto u klienta predpokladá Threadpool, ktorý môže uskutočniť paralelnú kontrolu viacerých požiadaviek.

Pri asynchrónnom mechanizme pomocou TGM kontrolér skenera, resp. čítací systém nevyvolá kontrolnú metódu priamo, ale pošle telegram kryptosystému, ktorý obsahuje požiadavku na kontrolu, obsah 2D-čiarového kódu a ďalšie informácie, ako je aktuálny triediaci program. Pri vstupe tohto telegramu do kryptosystému sa kontrolná funkcia vyvolá, vykoná a výsledky čítania a kontroly sa zasa pošlú späť ako nový telegram. Výhoda pri tomto spôsobe spočíva v tom, že na systéme, ktorý vydal požiadavku, sa proces neblokuje, kým nebude známy výsledok.

Kontrola systémov ručných skenerov

Kontrolný program pre systémy ručných skenerov očakáva ako vstupné hodnoty Session ID, ako aj obsah 2D-čiarového kódu. Ako dodatočný parameter sa očakáva ešte aj ID triediaceho programu. Posledne uvedený parameter slúži na určenie minimálnej odplaty.

Obr. 5 znázorňuje prehľad o priebehu kontroly v rámci overovacieho kontroléra pre prípad, že táto bola vyvolaná systémom ručného skenera. Vychádza sa pritom z kontroly rádioskenerom s následným manuálnym porovnaním adresy s

obsahom 2D-čiarového kódu. Pri skeneri, pripojenom cez vodiče, by bola reprezentácia analogická systému na zabezpečenie odplaty, resp. aplikácii zabezpečenia odplaty.

Výhodný priebeh kontroly s použitím rádioskenera, kontroléra skenera a kontrolnej jednotky (overovací kontrolér) je znázornený na obr. 5.

Kontrolná jednotka riadi pri znázornenom, zvlášť výhodnom príklade uskutočnenia, priebeh čiastkových kontrol, pričom prvá čiastková kontrola zahrnuje načítanie maticového kódu, nachádzajúceho sa v digitálnom výplatnom znaku. Načítaný maticový kód sa najprv prenesie z rádioskenera do kontroléra skenera. Následne sa v oblasti kontroléra skenera uskutoční kontrola maticového kódu, ako aj jeho odovzdanie kontrolnej jednotke. Kontrolná jednotka riadi rozdelenie obsahu kódu. Výsledok čítania sa následne sprostredkuje snímacej jednotke - v znázornenom prípade rádioskeneru. Týmto zistí napríklad užívateľ čítacej jednotky, že bolo možné prečítať výplatný znak a pritom rozpoznať informácie, ktoré obsahovala matica. Následne kontrolná jednotka dekóduje kryptoreťazec, obsiahnutý v maticovom kóde. Na tento účel sa výhodne najprv skontroluje verzia kľúča, pravdepodobne použitého na vytvorenie výplatného znaku. Následne sa skontroluje kontrolný pseudosúčet, obsiahnutý v kryptoreťazci.

Ďalej sa uskutoční kontrola predpokladanej minimálnej odplaty.

Okrem toho sa skontroluje identifikačné číslo (Postage ID) systému zákazníka, ktorý riadi vytvorenie výplatného znaku.

Na to nadväzujúc sa uskutoční porovnanie identifikačných čísel s negatívnym zoznamom.

Pomocou týchto kontrolných krokov je týmto zvlášť jednoduchým a účelným spôsobom možné jednoducho zistiť neoprávnene vytvorené výplatné znaky.

Výsledok zistenia sa odovzdá ako digitálna správa, pričom sa táto digitálna správa dá napríklad odovzdať pôvodnému rádioskeneru. Takto môže napríklad užívateľ rádioskenera zásielku vyradiť z procesu zasielania. Pri automatizovanom uskutočnení tohto variantu postupu je však samozrejme rovnako možné vyradiť zásielku z normálneho postupu spracovania poštových zásielok.

Výhodne sa výsledok kontroly zaprotokoluje v oblasti kontrolnej jednotky.

Ako vrátená hodnota by sa mali vrátiť kód, patriaci k prípadu zabezpečenia odplaty a príslušné textové hlásenie, ako aj objekt 2D-čiarového kódu.

Postup kontroly pri čítačke AFM-2D-kódu

Ako vstupný parameter pre kontrolný program pre čítačku AFM-2D-kódu sa bude očakávať taktiež Session-ID, ako aj obsah 2D-čiarového kódu a jednoznačné označenie triediaceho programu, ktorý je práve aktívny.

Obr. 6 znázorňuje prehľad priebehu kontroly v rámci overovacieho kontroléra pre prípad, že bola vyvolaná čítacím systémom.

Na obrázku sú na zvýraznenie priebehu uvedené naviac aj optický snímací systém (IMM-systém), ako aj čítačka AFM-2D-kódu, aby sa znázornil celkový kontext kontroly. Podiel kryptosystému sa však obmedzuje len na to, aby skontroloval funkcie medzi 2D-čiarovým kódom a vrátením, ako aj protokolovaním výsledku.

V prípade rozhrania s manažérom telegramov by sa na overovacom kontroléri naštartovali viaceré Service Tasks, ktoré čakajú na telegramy s požiadavkami na kontrolu a obsahom telegramu vyvolajú kontrolný program. Výsledok kontrolného programu sa očakáva a zbalí sa do telegramu a zašle sa späť žiadajúcemu klientovi.

Na obr. 6 je znázornená ďalšia výhodná forma uskutočnenia riadenia priebehu čiastkových kontrol kontrolnou jednotkou (overovací kontrolér). Pri tejto ďalšej výhodnej forme uskutočnenia sa uskutoční snímanie výplatných znakov automatickým optickým rozpoznávacím systémom (Prima/IMM). Údaje zašle optická kontrolná jednotka do čítacej a snímacej jednotky (čítačka AFM-2D-kódu).

Pri forme uskutočnenia postupu na kontrolu platnosti digitálnych výplatných znakov, znázornenej na obr. 6, sa uskutoční načítanie digitálnych výplatných znakov výhodne ešte viac automatizovaným spôsobom, napríklad optickým snímaním miesta poštovej zásielky, na ktorom je výhodne usporiadaný výplatný znak. Ďalšie kroky kontroly sa uskutočňujú v podstate zodpovedajúco priebehu kontroly, znázornenému pomocou obr. 5.

Vrátená hodnota kontrolného programu pozostáva na jednej strane z kódu na zabezpečenie odplaty a príslušného hlásenia, ako aj z konvertovaného a o Postage ID rozšíreného obsahu. Z týchto vrátených hodnôt sa vytvorí telegram a sprostredkuje sa žiadajúcemu čítaciemu systému.

Kontroly obsahu

Rozdelenie a konverzia obsahu 2D-čiarového kódu

Vstup: naskenovaný 2D-čiarový kód

Opis:

V tejto funkcii sa má obsah 2D-čiarového kódu, ktorý pozostáva z 80 bajtov, rozdeliť a prekonvertovať na štruktúrovaný objekt, ktorý budeme v ďalšom označovať ako objekt 2D-čiarového kódu, aby sa dosiahla lepšia možnosť zobrazenia, ako aj efektívnejšie ďalšie spracovanie. Jednotlivé polia a konverzie sú opísané v nasledujúcej tabuľke:

Pri konverzii binárnych a decimálnych čísel treba dávať pozor na to, aby ľavým bajtom postupnosti bajtov bol bajt s najvyššou hodnotou. Ak sa konverzia prípadne nemôže uskutočniť kvôli konfliktu typov alebo chýbajúcim údajom, potom sa má vygenerovať hlásenie prípadu zabezpečenia odplaty "PC-F-čiarový kód sa nedá čítať" a vrátiť ho overovaciemu kontroléru. Ďalšia kontrola obsahu, resp. kryptografická kontrola nemá v tomto prípade zmysel.

Pole	Typ	Prekonvertovať na	Opis
Poštový úrad	ASCII (3 bajty)		Konverzia nie je potrebná
Spôsob frankovania	binárny (1 bajt)	malé celé číslo	
Označenie verzie	binárny (1 bajt)	malé celé číslo	Číslo verzie postupu
Číslo kľúča	binárny (1 bajt)	malé celé číslo	Typ kódu
Kryptoreťazec	binárny (32 bajtov)		Postupnosť bajtov sa má prevziať nezmenená, po dekódovaní sa oddelí Postage ID

Postage ID		text (16 znakov)	Naplní sa po dekódovaní kryptoreťazca
Priebežné číslo zásielky	binárny (3 bajty)	celé číslo	Len kladné čísla
Kľúč produktu	binárny (2 bajty)	celé číslo	Kladné čísla, poukaz na príslušnú referenčnú tabuľku
Odplata	binárny (2 bajty)	floating point??	Konverzia na kladné decimálne číslo, ktoré sa má podeliť 100, údaje v Euro
Dátum frankovania	binárny (3 bajty)	dátum	Po konverzii na kladné decimálne číslo sa dá dátum prekonvertovať podľa formátu YYYYMMDD
Poštové smerové číslo prijímateľa	binárny (3 bajty)	2 hodnoty, jedna pre krajinu, druhá pre PSČ	Po konverzii na kladné decimálne číslo udávajú prvé dve číslice kód krajiny a päť zvyšných číslic PSČ
Ulica/poštový priečinok	ASCII (6 bajtov)	skratka ulice alebo poštový priečinok	U prvých číslic ide o čísla, potom je zakódované PSČ, ináč prvé a posledné tri miesta ulica s číslom domu
Zvyšná suma poštovného	binárny (3 bajty)	floating point + pole meny (text 32 znakov)	Po konverzii na kladné decimálne číslo udáva prvá číslica menu (1 = Euro), nasledujúce štyri číslice miesta pred desatinnou čiarkou a zvyšné dve číslice miesta za desatinnou čiarkou
Kontrolný pseudosúčet	binárny (20 bajtov)		Postupnosť bajtov sa má prevziať nezmenená, slúži na kryptografické overenie frankovania

Vrátená hodnota: objekt 2D-čiarového kódu,
kód varovania 00, pokiaľ je konverzia OK,
ináč varovanie pre prípad zabezpečenia odplaty "PC-F-čiarový kód sa nedá čítať"

Kontrola čísla verzie

Vstup: aktuálny objekt 2D-čiarového kódu
Opis:

Z prvých troch polí sa dá rozpoznať verzia 2D-čiarového kódu. Z toho tiež vidieť, či pri výplatnom znaku vôbec ide o 2D-čiarový kód Deutsche Post a nie o 2D-čiarový kód iného poskytovateľa služieb. Obsahy polí sa musia porovnať s vopred konfigurovaným zoznamom platných hodnôt. Ak sa nezistí žiadna zhoda, vráti sa varovanie zabezpečenia odplaty "PC-F-verzia". Kontrola ďalších obsahových, ako aj kryptografických aspektov potom nemá zmysel a nemala by sa ďalej uskutočňovať.

Vrátená hodnota: kód varovania 00, pokiaľ je kontrola verzie OK,
ináč kód varovania pre prípad zabezpečenia odplaty "PC-F-verzia"

Kontrola Postage ID

Vstup: objekt 2D-čiarového kódu s dekódovaným Postage ID
Opis:

Postage ID, ktoré je obsiahnuté v 2D-čiarovom kóde, je zabezpečené metódou?? kontrolných číslic (CRC 16), ktorá sa má na tomto mieste skontrolovať. Ak táto kontrola nie je úspešná, vráti sa ako výsledok varovanie zabezpečenia odplaty "PC-F podozrenie na falšovanie (Postage ID)". Na kontrolu Postage ID je potrebné predchádzajúce dekódovanie kryptoreťazca.

Vrátená hodnota: kód "00", ak je kontrola OK,
ináč kód varovania pre prípad zabezpečenia odplaty "PC-F

podozrenie na falšovanie (Postage ID)"

Kontrola prekročenia času

Vstup: objekt 2D-čiarového kódu

Opis:

Táto funkcia slúži na automatickú kontrolu časového intervalu medzi frankovaním PC-uvoľnenej zásielky a jeho spracovaním v listovom centre. Medzi oboma dátumami smie byť len určitý počet dní. Počet dní sa pritom riadi podľa produktu a doby jeho prepravy plus jeden čakací deň.

Konfigurácia časového intervalu sa výhodne zapamätá vo vzťahu produkt-čas platnosti a v rámci jednej ošetrovacej masky sa ošetrí centrálne. V uvedenom vzťahu sú ku každému kľúču produktu (pole 2D-čiarového kódu), možnému pre PC-frankovanie, uchované príslušné počty dní, ktoré môžu ležať medzi frankovaním a spracovaním v listovom centre. V zjednodušenom postupe sa vopred nakonfiguruje len údaj o časovom intervale, ktorý sa vzťahuje na štandardné zásielky a uloží sa v systéme ako konštanta.

Na kontrolu sa vytvorí počet dní medzi aktuálnym dátumom testovania pri spracovaní a dátumom, ktorý sa nachádza v 2D-čiarovom kóde, napríklad 02.08. až 01.08. = 1 deň. Ak je zistený počet dní väčší než hodnota, vopred stanovená pre produkt, overovaciemu kontroléru sa vráti kód zabezpečenia odplaty, priradený prípadu varovania "PC-F-dátum (frankovanie)", ináč kód, ktorý dokumentuje úspešnú kontrolu. Keď sa v zjednodušenom postupe porovnáva vždy s hodnotou pre štandardné zásielky, musí po vydaní výsledku kontroly existovať možnosť opraviť tento výsledok kontroly, napríklad manuálne tlačidlom na skeneri, pokiaľ aktuálny produkt pripúšťa dlhší čas prepravy.

Ďalšia kontrola prekročenia času sa vzťahuje na obsah Postage ID. V rámci predplatného zložený obnos poštovného a tým aj Postage ID majú vopred určenú dobu platnosti, v ktorej sa zásielky musia ofrankovať. Postage ID obsahuje okamih, po ktorý je obnos poštovného platný. Ak je dátum frankovania o určitý počet dní

väčší než táto doba platnosti, vráti sa varovný kód zabezpečenia odplaty, patriaci k varovaniu zabezpečenia odplaty "PC-F-dátum (obnos poštovného)".

Vrátená hodnota: kód "00", pokiaľ je kontrola OK,
ináč varovný kód pre prípad zabezpečenia odplaty
"PC-F-dátum (obnos poštovného)" alebo
"PC-F-dátum (frankovanie)"

Kontrola odplaty

Vstup: objekt 2D-čiarového kódu; ID aktuálneho triediaceho programu

Opis:

V rámci tejto funkcie sa uskutoční kontrola odplaty, obsiahnutej v 2D-čiarovom kóde, voči minimálnej odplate, ktorá je definovaná pre zásielky príslušného triediaceho programu. Pri týchto obnosoch ide o Euro-obnosy.

Priradenia sa dodávajú medzi triediacim programom a minimálnou odplatou cez automatické rozhranie.

Zjednodušený postup je podobný ako pri kontrole prekročenia času. Tu sa v konfiguračnom súbore k aplikácii definuje konštantná minimálna odplata, ktorá platí pre všetky zásielky. Preto nie je potrebné odovzdať triediaci program.

Pri následnej kontrole sa porovnáva, či je minimálna odplata, obsiahnutá v 2D-čiarovom kóde, pod touto hodnotou. Ak tento prípad nastane, vráti sa kód, priradený prípadu zabezpečenia odplaty "PC-F podfrankovanie", ináč kód úspešnosti.

Vrátená hodnota: kód "00", pokiaľ je kontrola OK,
ináč varovný kód pre prípad zabezpečenia odplaty
"PC-F podfrankovanie"

Porovnanie s negatívnym súborom

Vstup: objekt 2D-čiarového kódu s dekódovaným Postage ID

Opis:

V rámci tejto funkcie sa uskutoční kontrola, či sa Postage ID, patriaci k 2D-čiarovému kódu, nachádza v negatívnom súbore. Negatívne súbory slúžia na to, aby sa zásielky od zákazníkov, ktorí sa stali nápadnými pokusmi o zneužitie, resp. ktorým ukradli PC, vyňali z procesu prepravy.

Negatívne súbory sa pritom udržiavajú centrálne v rámci projektu Databáza uvoľňovania. V rámci rozhrania k tomuto projektu treba určiť postup výmeny údajov so systémami decentralizovaných listových centier.

Keď ešte prípadne použitie ošetrovania, resp. výmena údajov neexistuje, treba vytvoriť prechodný mechanizmus. Ošetrenie týchto údajov by sa prechodne mohlo uskutočniť v Excel-tabuľke, z ktorej sa generuje csv-súbor. Tento šúbor sa zašle elektronickou poštou AGB-kontrolórom a títo ho načítajú cez predpokladaný mechanizmus importovania do systémov. Neskôr sa uskutoční prenos cestou, definovanou v rámci výhodnej IT-jemnej (detailnej, prepracovanej) koncepcie zabezpečenia odplaty.

Postage ID označuje jednotlivé predplatné, ktoré zákazník vyvolá zo systému (Postage Point). Tieto údaje sú zapamätané v v takzvanom safebox-e systému zákazníka. Ide pritom o hardvérový komponent vo forme SmartCard, vrátane čítacieho systému, resp. donglu (ochranného zariadenia). V safebox-e sa obnosy predplatného bezpečne uchovávajú a zákazník z nich môže odoberať jednotlivé frankovacie sumy bez toho, aby bol on-line pripojený na miesto, kde sa prijímajú obnosy poplatkov (Postage Point).

Každý safebox je označený jednoznačným ID. Tento safebox-ID sa zanesie do negatívneho súboru, ak sa príslušné zásielky majú kvôli podozreniu zo zneužitia vyradiť. Safebox-ID sa skladá z viacerých polí. Popri jednoznačnom kľúči sa v safebox-ID nachádzajú aj ďalšie polia, ako je dátum platnosti a kontrolné číslo. Na jednoznačnú identifikáciu safebox-u sú určujúce prvé tri polia safebox-ID. Tieto sa nachádzajú aj v prvých troch poliach Postage ID, v dôsledku čoho sa môže uskutočniť priradenie medzi safebox-om a predplatným. Tieto polia sú opísané v nasledujúcej tabuľke:

Bajt č.	Dĺžka	Význam	Obsah údajov	Komentár

b1	1	Označenie ponúkajúceho	00	nepoužité
			01	Test: ponúkajúci: úrad poštovej prepravy
			FF	Postage-Point-box podniku poštovej prepravy
b2	1	Schválené číslo modelu	XX	Vyplňuje sa pre každého výrobcu 01 (prvý doručený model) · vzostupným spôsobom pre každý novo schválený model
b3, b4, b5	3	Sériové číslo modelu	XX XX XX	Vyplňuje sa pre každý schválený model každého výrobcu od 00 00 01 po FF FF FF vzostupným spôsobom

Ak sú prvé tri polia Postage ID aktuálne kontrolovaného frankovania identické s prvými tromi poliami safebox-u, nachádzajúceho sa v negatívnom súbore, vráti sa prípad zabezpečenia odplaty, priradený zákazníkovi v negatívnom súbore, ináč kód úspešnosti.

Vrátená hodnota: kód "00", pokiaľ je kontrola OK,
ináč varovný kód, priradený zákazníkovi, resp. safebox-u v negatívnom súbore

Porovnanie obsahu 2D-čiarového kódu s nešifrovaným textom zásielky

Vstup: objekt 2D-čiarového kódu

Opis:

Aby sa zabránilo vyhotovovať kópie 2D-čiarového kódu, uskutoční sa porovnanie zasielacích údajov, zakódovaných v 2D-čiarovom kóde, s údajmi, ktoré sú uvedené na liste v nešifrovanom texte. Toto porovnanie je pri rádioskeneroch možné priamo, pretože sú tam k dispozícii dostatočné zobrazovacie a vstupné možnosti. Pri ručných skeneroch s pripojením cez vodiče treba urobiť kontrolu na PC (systém na zabezpečenie odplaty).

Priebeh vyzerá tak, že overovací kontrolér po prebehnutí automatizovaných kontrol vyvolá výstup údajov 2D-čiarového kódu na rádioskener, resp. na PC na zabezpečenie odplaty. Na tento účel má k dispozícii Callback-metódu, ktorá sa na začiatku priradí relácii.

Túto vyvolá s aktuálnym objektom 2D-čiarového kódu. Potom sú za zobrazenie obsahu 2D-čiarového kódu zodpovedné kontrolér skenera, resp. PC na zabezpečenie odplaty, a vracajú ako hodnotu (po spracovaní kontrolórom), vrátenú Callback-metódou, "00", resp. príslušný chybový kód.

Pri úspešnom vyhodnotení sa vráti kód úspešnosti, ináč kód varovania zabezpečenia odplaty "PC-F-nešifrovaný text".

Pri automatickej kontrole nie je táto kontrola potrebná. Tu sa dá táto kontrola uskutočniť výhodne v rámci centrálnych vyhodnotení off-line, resp. pomocou porovnaní obratov, alebo cez porovnanie cieľového poštového smerového čísla s poštovým smerovým číslom, nachádzajúcim sa v 2D-čiarovom kóde.

Vrátená hodnota: kód "00", pokiaľ je kontrola OK,
ináč varovný kód pre prípad zabezpečenia odplaty "PC-F-nešifrovaný text"

Kryptografické kontroly

Kryptografická kontrola pozostáva z dvoch častí:

a) dekódovania kryptoreťazca a

b) porovnania kontrolného pseudosúčtu.

Oba postupy sa uskutočnia v chránenej oblasti kryptokarty, pretože zákazník by pri vypátraní informácie, vznikajúcej pri spracovaní, mohol vytvoriť platné hodnoty pre frankovacie kontrolné pseudosúčty.

Dekódovanie kryptoreťazca

Vstup: objekt 2D-čiarového kódu

Opis:

Ako vstupný parameter táto funkcia obsahuje oddelený objekt 2D-čiarového kódu výsledku skenovania. Pomocou dátumu frankovania a Key-Nr. sa vyhľadá pre tento okamih platný symetrický kód a kryptoreťazec odovzdaného objektu sa pomocou tohto kódu dekóduje postupom Triple DES CBC. To, aká hodnota sa pridelí inicializačnému vektoru, resp. či sa bude pracovať s inner- alebo s outerbound-CRC a s akou dĺžkou bloku, sa rozhodne v rámci rozhrania k systému zabezpečenia odplaty.

Ak by sa kód, ktorý sa nachádza v 2D-čiarovom kóde, nenachádzal v kryptosystéme, vráti sa varovanie zabezpečenia odplaty "PC-F-podozrenie z falšovania (kľúč)" s chybovým hlásením, že kľúč s uvedeným Key-Nr. sa nenašiel.

Výsledok operácie pozostáva z dekódovaného Postage ID, ako aj z dekódovaného náhodného čísla. Dekódovaný Postage ID sa vnesie do zodpovedajúceho poľa objektu 2D-čiarového kódu. Náhodné číslo by sa z bezpečnostných dôvodov nemalo oznámiť, pretože zákazník by so znalosťou tejto informácie mohol vytvárať platné kontrolné pseudosúčty a tak falšovať 2D-čiarové kódy.

V nadväznosti na dekódovanie sa z tejto metódy vyvolá vypočítanie kontrolného pseudosúčtu a vráti sa jeho vrátená hodnota.

Vypočítanie kontrolného pseudosúčtu

Vstup: objekt 2D-čiarového kódu

dekódované náhodné číslo z kryptoreťazca

(dekódované náhodné číslo nesmie byť známe mimo karty)

Opis:

Funkcia výpočtu kontrolného pseudosúčtu zistí z originálneho výsledku skenovania, ktorý sa nachádza v objekte 2D-čiarového kódu, prvých 60 bajtov. Potom sa pripojí dekódovaný Postage ID, ako aj odovzdané dekódované náhodné číslo. Z toho sa metódou SHA 1 vypočíta kontrolný pseudosúčet a porovná sa s kontrolným pseudosúčtom 2D-čiarového kódu, nachádzajúcim sa v objekte 2D-čiarového kódu. Ak sa zhoduje všetkých 20 bajtov, kryptografická kontrola je úspešná a vráti sa zodpovedajúca vrátená hodnota.

Pri nezhode sa overovaciemu kontroléru vráti varovanie zabežpečenia odplaty "PC-F-podozrenie z falšovania (kontrolný pseudosúčet)".

Ako vrátená hodnota sa naviac sprostredkuje vypočítaný kontrolný pseudosúčet, aby sa dal odovzdať spolu s výsledkom kontroly.

Vrátená hodnota: kód "00", pokiaľ je kontrola OK,
ináč varovný kód pre prípad zabezpečenia odplaty
"PC-F-podozrenie z falšovania (kontrolný pseudosúčet)" alebo
"PC-F-podozrenie z falšovania (kľúč)"

Výstup výsledkov

Zobraziť výsledok kontroly a čítania

Opis:

Prostredníctvom Callback-metódy má overovací kontrolér možnosť nasmerovať výstup výsledkov na výstupné zariadenie, ktoré patrí aktuálnej kontrole. Na tento účel odovzdá Callback-metóde objekt 2D-čiarového kódu a zistený varovný kód zabezpečenia odplaty. Ako vrátená hodnota sa môže dodať kód postupu dodatočného spracovania, zvolený AGB-kontrolórom.

Callback-metóda pre výstup sa priradí, taktiež na začiatku relácie, pri prihlásení sa overovacieho kontroléra.

Protokolovanie výsledkov

Vstup: objekt 2D-čiarového kódu, kód výsledku kontroly

Opis:

Protokolovanie výsledkov sa uskutočňuje zjednodušeným spôsobom v súbore na systéme, na ktorom beží overovací kontrolér. Spravidla sa výsledky, resp. opravné súbory, sprostredkujú priamo BDE a cez výhodné rozhranie zabezpečenie odplaty-BDE sa zapíšu do databázy výhodného lokálneho systému na zabezpečenie odplaty.

Výhodne sa zapamätajú Postage ID, priebežné číslo, dátum frankovania, odplata, kľúč produktu, PSČ, výsledkový kód zabezpečenia odplaty, text hlásenia, čas trvania kontroly, čas kontroly, ID skenera, prevádzkový režim skenera, spôsob snímania, ako aj spôsob ďalšieho spracovania. Všetky hodnoty sa odovzdajú od seba oddelené bodkočiarkou v jednom súbore na jednu zásielku a tak sa dajú napríklad v Excel-i ďalej vyhodnocovať.

Ak sa systém nachádza v prevádzkovom režime "prvé snímanie", do rubriky spôsob snímania treba zadať "e", ináč "n" pre dodatočné snímanie.

Príprava kmeňových údajov

Opis:

Na kontrolu obsahu je potrebný rad kmeňových údajov. Pritom ide o:

- PC-F-negatívny súbor
- triediace programy a minimálne odplaty
- všeobecnú minimálnu odplatu
- kľúč produktu PC-F
- maximálnu dobu dodania na jeden kľúč produktu PC-F
- všeobecnú maximálnu dobu dodania
- prípady zabezpečenia odplaty, priority a priradenie k pokynom na ďalšie spracovanie
- pokyny na ďalšie spracovanie

Kmeňové údaje sa môžu v prechodnej dobe s výnimkou PC-F-negatívneho súboru, ako aj kryptografických kódov miesta na prijímanie obnosov predplatného (Postage Point), pevne vopred nakonfigurovať.

Ak je to nevyhnutné, pre časť údajov sa môžu implementovať jednoduché aplikácie spracovania a rozdeľovania. Ošetrenie by sa potom malo uskutočniť v Excel-tabuľke, z ktorej sa generuje csv-súbor. Tento súbor by sa mal poslať elektronickou poštou AGB-kontrolórom a tí by ho mali cez predpokladaný mechanizmus načítať do systémov.

Spravidla sa údaje rozdelia, resp. sa k nim umožní prístup spôsobom, zodpovedajúcim predtým opísanej výhodnej IT-jemnej koncepcii zabezpečenia odplaty.

Príslušné údajové štruktúry sú opísané v údajovom modeli k jemnej koncepcii výhodného zabezpečenia odplaty.

Rozdelenie kľúčových údajov

Symetrické kľúče, ktoré slúžia na zabezpečenie obsahov 2D-čiarového kódu na mieste prijímania obnosov na poplatky (Postage Point) a ktoré potrebuje kryptosystém na overovanie, sa z bezpečnostných dôvodov v pravidelných intervaloch vymieňajú. Pri nasadení vo všetkých listových centrách sa kľúče musia preniesť z Postage Point ku kryptosystémom automaticky a bezpečne.

Výmena by sa pritom mala uskutočniť cez výhodný server zabezpečenia odplaty, pretože na mieste prijímania obnosov na poplatky (Postage Point) by sa nemalo konfigurovať, ktoré výhodné lokálne systémy zabezpečenia odplaty a ktoré kryptosystémy k tomu existujú.

Zvlášť výhodné kroky postupu pre výmenu kľúčov sú znázornené na obr. 7. Výhodná výmena kľúčov sa uskutoční medzi centrálnym prijímacím miestom (Postage Point), centrálnym kryptoserverom a viacerými lokálnymi kryptoservermi.

Pretože symetrické kódy majú pre bezpečnosť proti falšovaniu 2D-čiarového kódu veľký význam, výmena musí byť zabezpečená silnou kryptografiou a jednoznačnou autentizáciou komunikačných partnerov.

Konfigurácia

Základná konfigurácia/správa kľúčov kryptohardvéru

Na základnú konfiguráciu kryptokarty sú potrebné rôzne opatrenia. Mal by ich uskutočniť jeden bezpečnostný správca. Ide pri tom o zhruba o nasledujúce činnosti:

- inštalácia softvérových API na kartu

- generovanie, resp. inštalácia privátnych kľúčov na zabezpečenie správcovských aplikácií a softvéru, ktorý sa má nahrať.

Podľa zvoleného typu a výrobcu karty sú pritom potrebné rôzne opatrenia.

Od aplikácie závislá, pre výhodný systém zabezpečenia odplaty predpokladaná základná konfigurácia kryptokarty pozostáva z nasledujúcich krokov:

- bezpečné zakódovanie a prenos symetrických kľúčov na kartu - napríklad pár RSA-kľúč - za súčasného vytvorenia certifikátu pre Public Key a vydanie kľúča,

- pevne predkonfigurovať certifikát miesta prijímania obnosov na poplatky (Postage Point) na zabezpečenie toho, aby kľúč, ktorý sa má importovať, bol vystavený miestom prijímania obnosov za poplatky (Postage Point).

Základná konfigurácia aplikácie kryptosystému

Každý skener, každý užívateľ a každá kryptokarta v rámci kryptosystému musí byť označená jednoznačným ID. Nakoniec sa musí jednoznačným ID identifikovať aj každá čítačka AFM-2D-kódu.

Login/Logoff

Na začiatku relácie s overovacím kontrolérom sa musí uskutočniť Login. Tento Login obsahuje ako parameter ID skenera, ID užívateľa, ako aj Callback-metódy na manuálnu kontrolu, resp. vydanie výsledkov čítania a kontroly.

Ako vrátená hodnota sa dodá späť Session ID, ktorý sa pri nasledujúcich vyvolávaniach kontroly v rámci relácie má tiež odovzdávať. K Session ID sa v

overovacom kontroléri zapamätá Session Context, v ktorom sú zapamätané odovzdané parametre.

Ak užívateľ počas relácie urobí zmeny v druhu prevádzky, vo vopred definovanom produkte, resp. v ďalších nastaveniach relácie, ktoré sa dajú konfigurovať v jej priebehu, tieto zmeny sa doplnia do premenných, ktoré sú na tento účel priradené v rámci Session Context-u.

Pri Logoff sa Session Context zodpovedajúco vymaže. Následné vyvolávania kontrol s týmto Session ID sa odmietnu.

Správu užívateľov a hesiel treba definovať vo všeobecnej koncepcii správy užívateľov pre výhodné zabezpečenie odplaty, súčasti jemnej koncepcie výhodnej IT zabezpečenia odplaty.

Čítacie systémy sa musia dať pred uskutočním požiadaviek na kontrolu registrovať u overovacieho kontroléra. Ako parameter sa musí odovzdať ID čítacieho systému, ako aj heslo. Ako vrátená hodnota sa pri úspešnom prihlásení taktiež pošle späť Session ID, ktorý sa má pri nasledujúcich požiadavkách na kontrolu zisťovať.

Pri Shutdown vypnutí čítacieho systému sa musí uskutočniť zodpovedajúci Logoff s týmto Session ID.

Rozličné

Špeciálne úlohy užívateľov

V rámci bezpečnostnej koncepcie treba predpokladať dve špeciálne úlohy užívateľov, ktoré majú uskutočniť dve rôzne osoby.

Bezpečnostný správca

Úloha bezpečnostného správcu zahrnuje nasledujúce úlohy:

- vytvorenie príkazových súborov na správu kryptokarty
- signovanie týchto príkazových súborov
- inicializácia a správa kryptokariet
- kontrola softvéru, ktorý sa má nahrať, a príslušnej konfigurácie.

Bezpečnostný správca sa identifikuje svojím Private Key na správu kariet. Tento je zapamätaný na diskete alebo Smart Card a bezpečnostný správca ho musí bezpodmienečne udržiavať pod zámkou.

Na kryptokarte sa dajú vykonať len týmto kľúčom signované správcovské príkazy. Pretože týmto mechanizmom sú chránené postupnosť príkazov a príslušné parametre, vykonanie týchto príkazov sa môže delegovať aj na správcov systémov na mieste. Na tento účel musí bezpečnostný správca dať k dispozícii tieto príkazy a napísať zodpovedajúci návod na postup.

Ďalšia úloha spočíva v správe kryptokariet, pričom pre každú kryptokartu sa uchováva sériové číslo, konfigurácia a systémové číslo systému, v ktorom sú inštalované, ako aj miesto systému. Pri rezervných kryptokartách sa ďalej uchováva informácia, kto je vlastníkom kariet.

Spolu s QS správcom pre bezpečnosť kontroluje zdroje softvéru a príslušnú konfiguráciu softvéru a uvoľňuje ju na inštaláciu.

Okrem toho sa uskutočňuje kontrola softvéru, ktorý sa má inštalovať, resp. je inštalovaný na karte a na kryptoserveri, ako aj uvoľňovanie a signovanie softvéru kariet.

Softvér kariet je treba špeciálne kontrolovať na to, či sa na nejakom mieste niektorý z tajných kľúčov nemôže cez rozhranie ovládača dostať von, resp. či tam nedošlo k pokusom o manipuláciu, ako je napríklad zapamätanie konštantných vopred definovaných kľúčov alebo použitie nie bezpečných postupov kódovania. Okrem softvéru kariet treba skontrolovať aj aplikačný softvér kryptoservera, ktorý je s ním v spojení.

Autentizovanie sa uskutoční presne tak, ako pri bezpečnostnom správcovi pomocou Private Key. Pritom však ide o Private Key na signovanie softvéru.

Je tu však ďalšia bezpečnosť v tom, že na inštaláciu softvéru treba signovať nielen softvér, ale aj príslušný príkaz na inštaláciu. Pretože na toto sú oprávnené dve rôzne osoby (QS správca a bezpečnostný správca) a tým, že príslušné kľúče sa uchovávajú na dvoch rôznych miestach, je tu tiež zaručená vysoká bezpečnosť.

Distribúciu softvéru vykonáva QS správca pre bezpečnosť po dohode s bezpečnostným správcom.

Táto zvlášť výhodná forma uskutočnenia vynálezu takto predpokladá dva rôzne autentizačné kľúče, takže bezpečnosť údajov sa značne zvýši.

Zmenené

PATENTOVÉ NÁROKY

1. Spôsob kontroly pravosti digitálneho výplatného znaku, naneseného na poštovú zásielku, pričom sa kryptografické informácie, nachádzajúce sa vo výplatnom znaku, použijú dekódované a na kontrolu pravosti výplatného znaku, **v y z n a č u j ú c i s a t ý m,** že kontrolná jednotka riadi priebeh čiastkových kontrol, pričom prvá čiastková kontrola zahrnuje načítanie maticového kódu, nachádzajúceho sa v digitálnom výplatnom znaku, že kontrolná jednotka riadi rozdelenie obsahu maticového kódu, že čiastkové kontroly sa uskutočňujú ako kroky kontroly, že kontrolná jednotka môže súčasne vykonávať viaceré požiadavky na kontrolu, ako aj časť krokov kontroly paralelne s tým, že krokmi kontroly sa zistia neoprávnene vytvorené výplatné znaky, že výsledok kontroly sa odovzdá ako digitálna správa a že takto sa zásielka vyradí z normálneho priebehu spracovania poštových zásielok.
2. Spôsob podľa nároku 1,**v y z n a č u j ú c i s a t ý m,** že jedna z čiastkových kontrol zahrnuje dekódovanie kryptografických informácií, nachádzajúcich sa vo výplatnom znaku.

3. Spôsob podľa jedného alebo oboch z nárokov 1 a 2, **v y z n a č u j ú c i s a t ý m,** že jedna z čiastkových kontrol zahrnuje porovnanie medzi dátumom vytvorenia výplatného znaku a aktuálnym dátumom.

4. Spôsob podľa jedného alebo viacerých z predchádzajúcich nárokov, **v y z n a č u j ú c i s a t ý m,** že čítacia jednotka a kontrolná jednotka si vymieňajú informácie pomocou synchrónneho protokolu.

5. Spôsob podľa nároku 4, **v y z n a č u j ú c i s a t ý m,** že protokol je na báze RPC.

6. Spôsob podľa jedného alebo viacerých z nárokov 1 až 5, **v y z n a č u j ú c i s a t ý m,** že čítacia jednotka a kontrolná jednotka navzájom komunikujú cez asynchrónny protokol.

7. Spôsob podľa nároku 6, **v y z n a č u j ú c i s a t ý m,** že čítacia jednotka pošle kontrolnej jednotke údajový telegram.

8. Spôsob podľa nároku 7, **v y z n a č u j ú c i s a t ý m,** že údajový telegram obsahuje obsah výplatného znaku.

9. Spôsob podľa jedného alebo viacerých z nárokov 1 až 8, **v y z n a č u j ú c i s a t ý m,** že údajový telegram obsahuje požiadavku na spustenie kryptografického kontrolného programu.

10. Spôsob podľa jedného alebo viacerých z nárokov 1 až 9, **v y z n a č u j ú c i s a t ý m,** že cez kryptorozhranie sa uskutoční rozdelenie zaťaženia medzi viaceré kontrolné prostriedky.

11. Spôsob podľa jedného alebo viacerých z nárokov 1 až 10, **v y z n a č u j ú c i s a t ý m,** že obsah výplatného znaku sa rozdelí do jednotlivých polí.

12. Spôsob podľa jedného alebo viacerých z predchádzajúcich nárokov, **v y z n a č u j ú c i s a t ý m,** že sa z výplatného znaku zistí identifikačné číslo (Postage ID) systému zákazníka, ktorý riadil vytvorenie výplatného znaku.

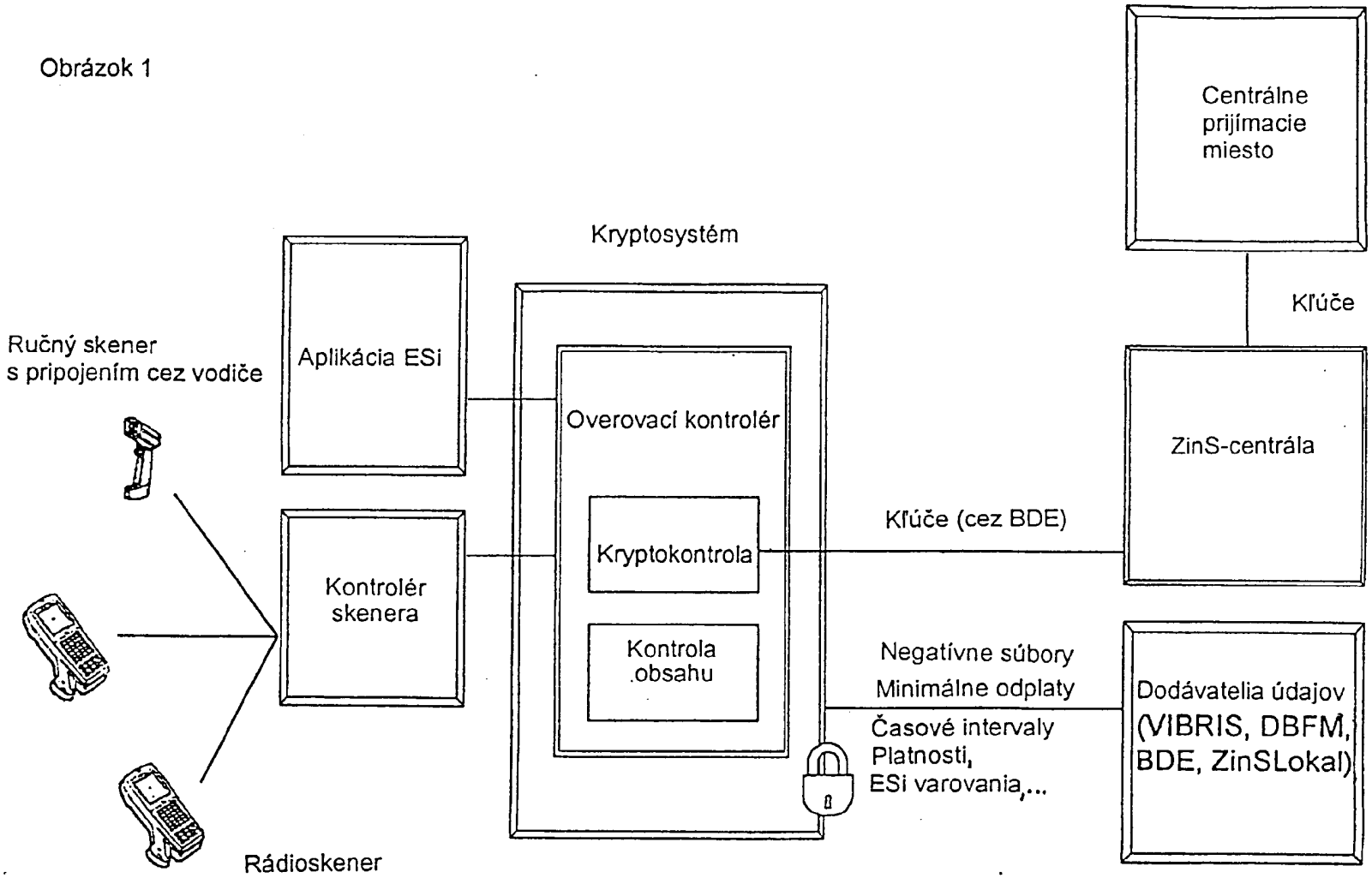
13. Spôsob podľa jedného alebo viacerých z predchádzajúcich nárokov, **v y z n a č u j ú c i s a t ý m,** že jednotlivé identifikačné údaje zákazníckeho systému (Postage ID) sa zachytia v negatívnom súbore a zásielky, ktoré patria k tomuto Postage ID, sa vyradia z normálneho priebehu spracovania poštových zásielok.

14. Spôsob podľa jedného alebo viacerých z predchádzajúcich nárokov, **v y z n a č u j ú c i s a t ý m,** že zakódovaný údaj o adrese prijímateľa, nachádzajúci sa vo výplatnom znaku, sa porovná s adresou prijímateľa, uvedenou na poštovej zásielke, podanej na prepravu.

15. Spôsob podľa jedného alebo viacerých z nárokov 1 až 14, **v y z n a č u j ú c i s a t ý m,** že kontrolné parametre uvedeného spôsobu sa dajú zmeniť.

16. Spôsob podľa nároku 15, **v y z n a č u j ú c i s a t ý m,** že zmena parametrov spôsobu sa uskutoční len po zadaní osobného digitálneho kľúča (Private Key) správcu systému.

Obrázok 1

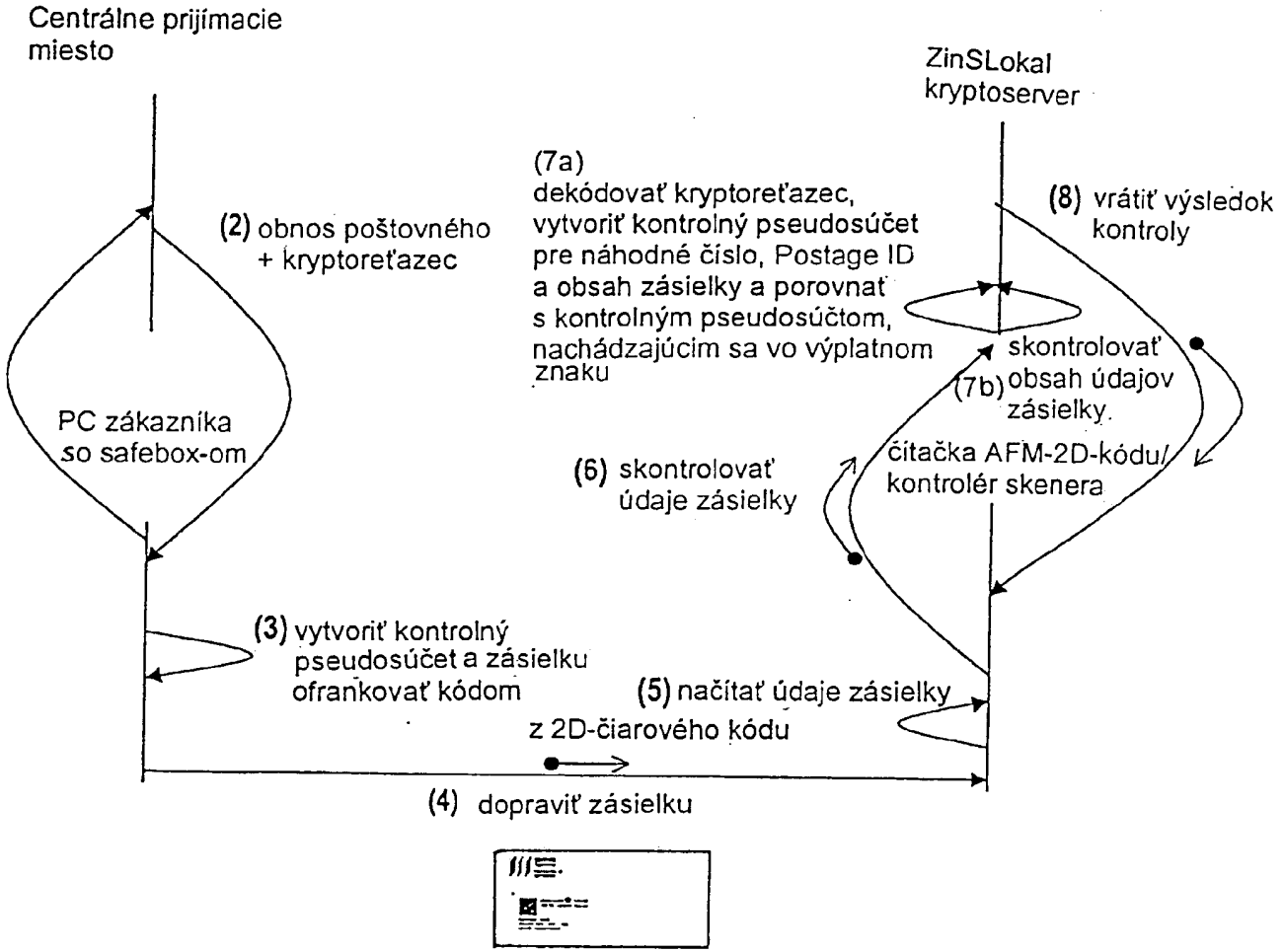


Zmenený

PP 1627 - 2003

Obrázok 2

Zmenený



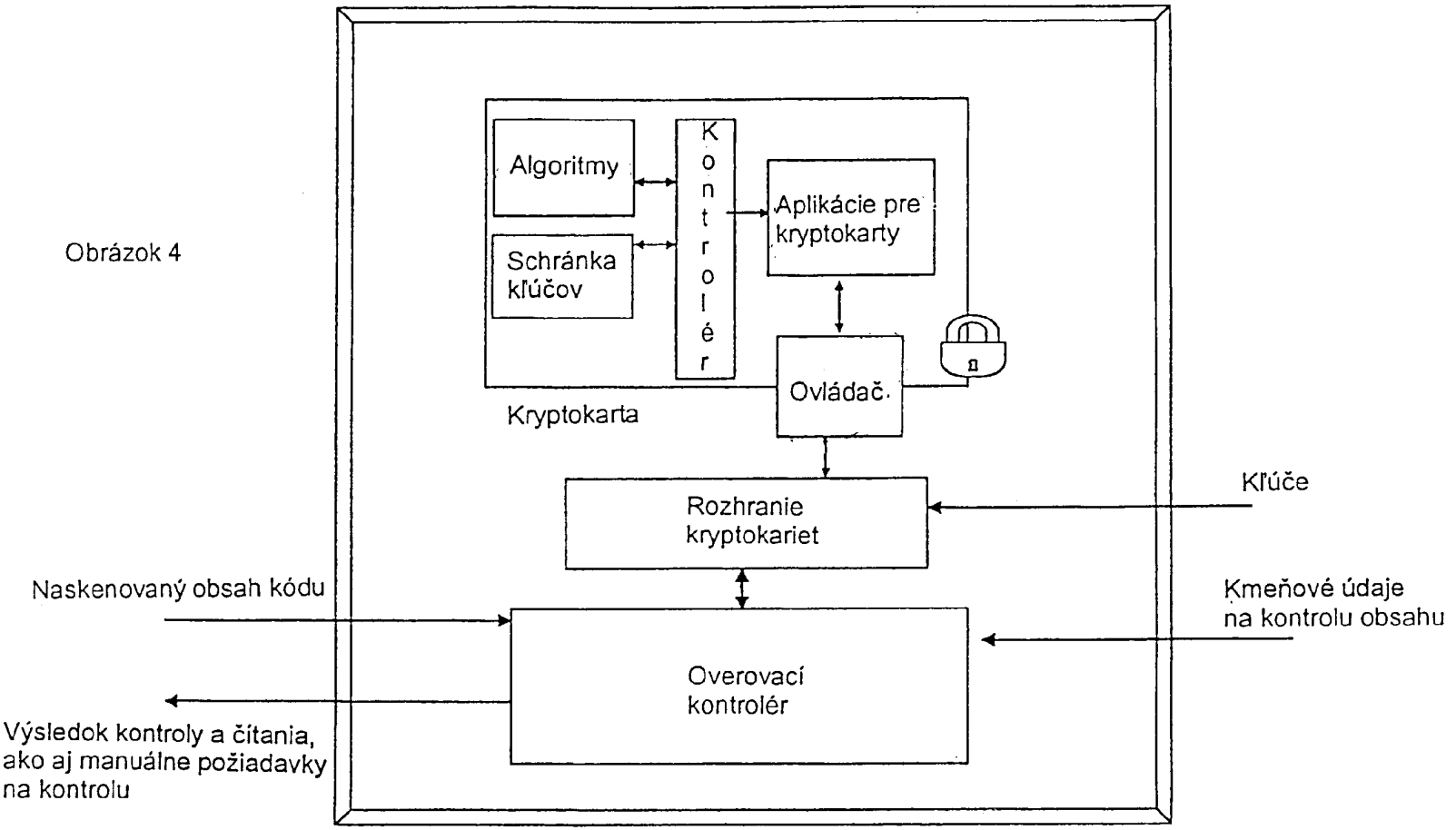
Obrázok 3

Zmenený

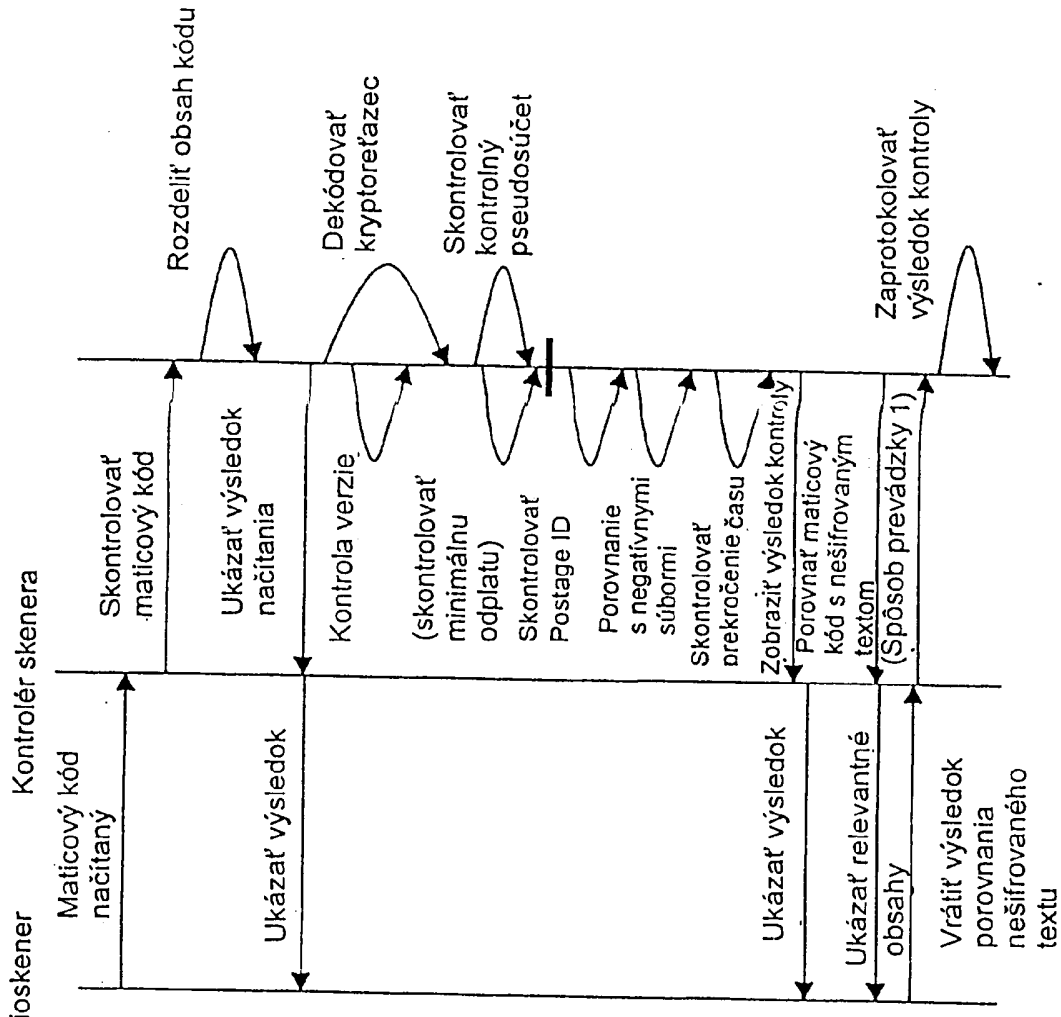
3/1

PP 1624-2003

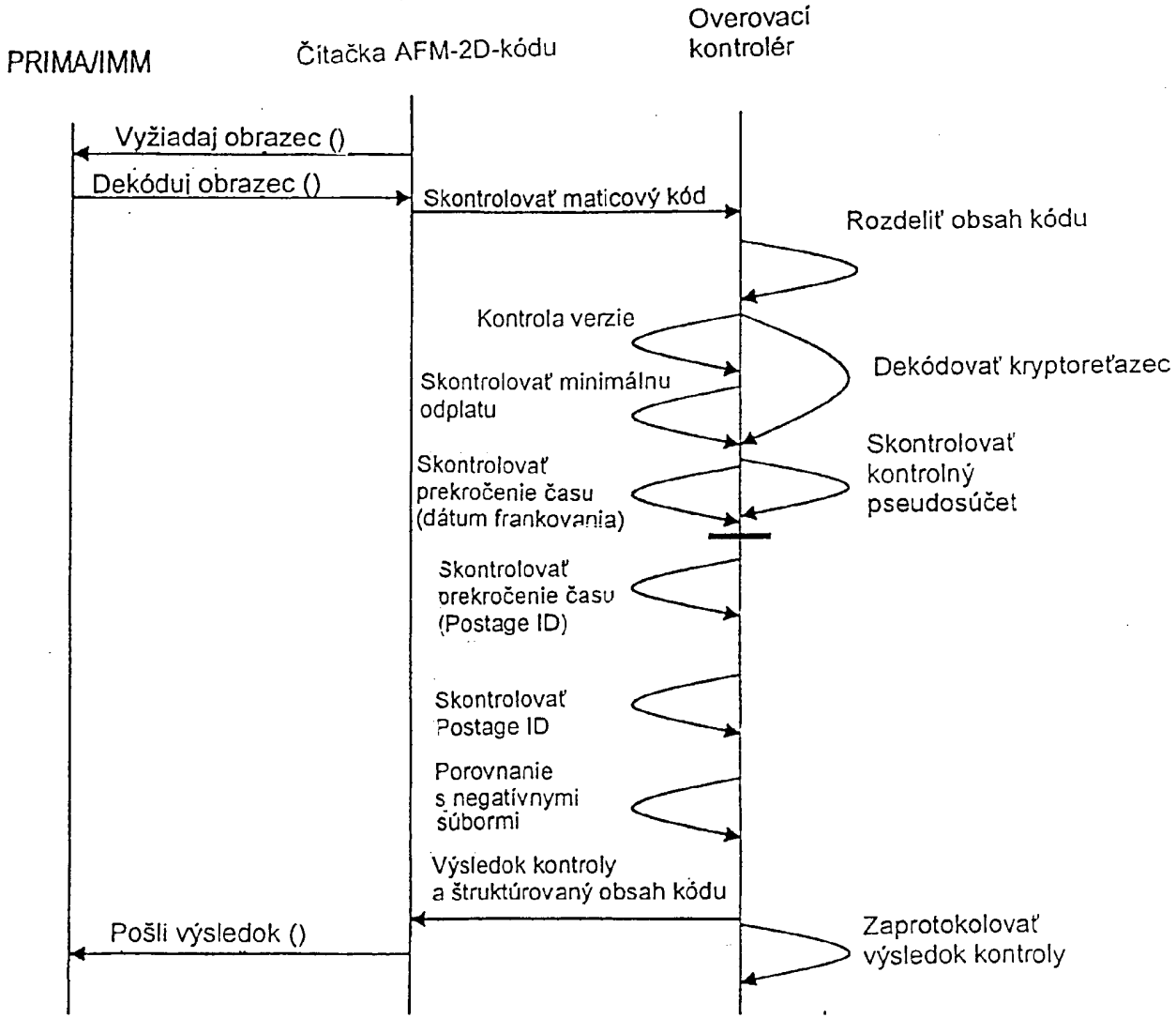
Obrázok 4



Zmenený


Rádioskener
Kontrolér skenera
Maticový kód načítaný
Ukázať výsledok
Ukázať výsledok načítania
Skontrolovať maticový kód
Rozdeliť obsah kódu
Kontrola verzie
Dekódovať kryptoreťazec
(skontrolovať minimálnu odplatu)
Skontrolovať Postage ID
Skontrolovať kontrolný pseudosúčet
Porovnanie s negatívnymi súbormi
Skontrolovať prekročenie času
Zobraziť výsledok kontroly
Porovnať maticový kód s nešifrovaným textom
Ukázať výsledok
Ukázať relevantné obsahy
(Spôsob prevádzky 1)
Zaprotokolovať výsledok kontroly
Vrátiť výsledok porovnania nešifrovaného textu
Maticový kód načítaný
Zmenený

Obrázok 5

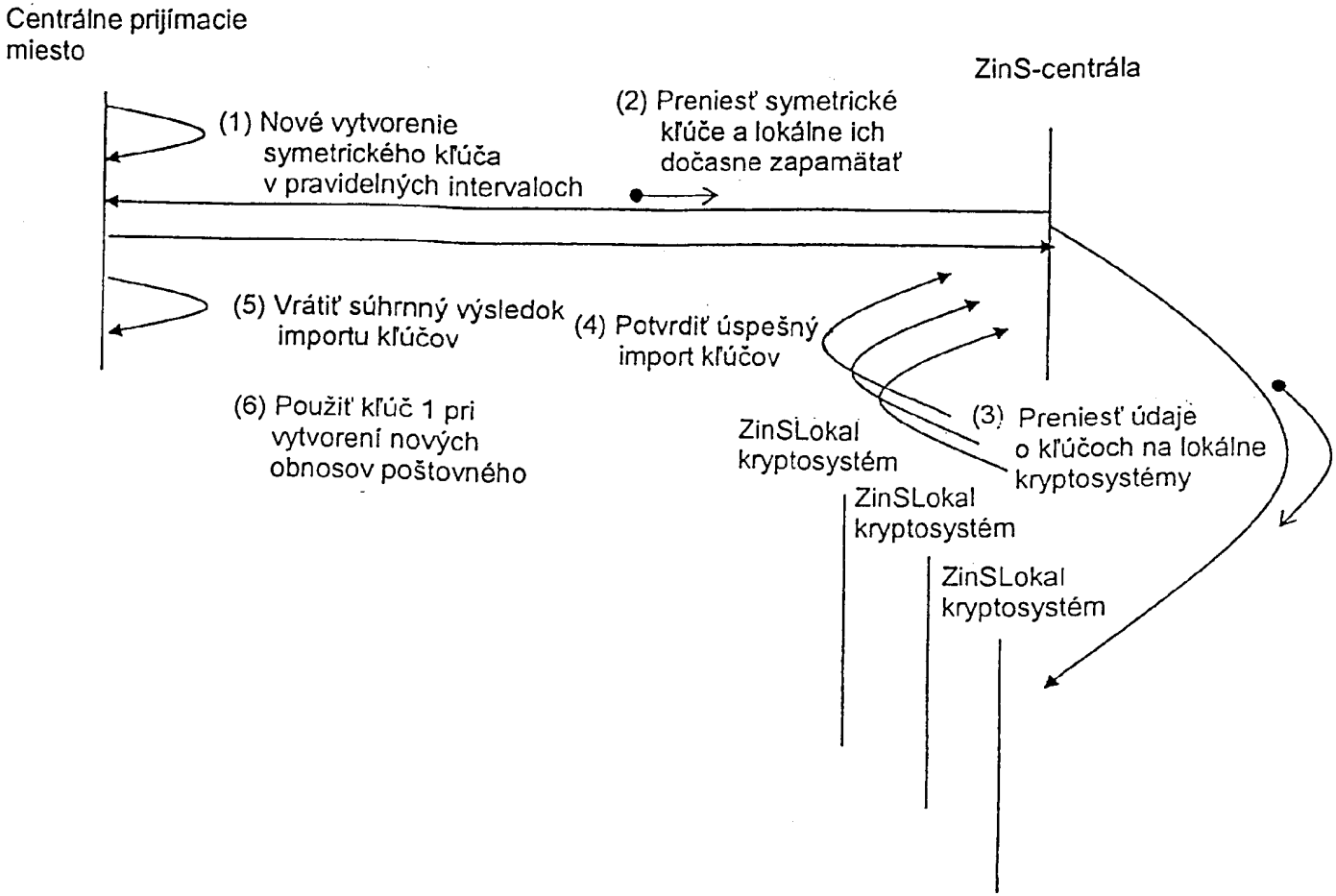


Obrázok 6

6/7

Zmenený

PP 4624-2003



Obrázok 7

Zmenený