PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:
2003 - 1357

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
G 07 B 17/00

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **15.11.2001**

(32) Datum podání prioritní přihlášky: **15.11.2000**

(31) Číslo prioritní přihlášky: **2000/10056599**

(33) Země priority: **DE**

(40) Datum zveřejnění přihlášky vynálezu: **17.12.2003**
(Věstník č. 12/2003)

(86) PCT číslo: **PCT/DE01/04258**

(87) PCT číslo zveřejnění: **WO02/041261**

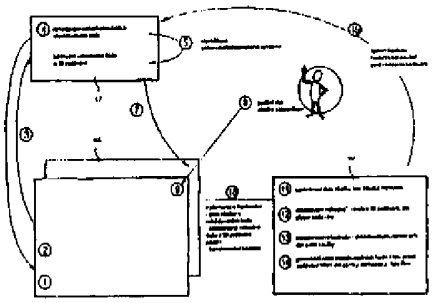
(71) Přihlašovatel:
DEUTSCHE POST AG, Bonn, DE;

(72) Původce:
Lang Jürgen, Bergisch Gladbach, DE;
Meyer Bernd, Königswinter, DE;

(74) Zástupce:
Všetečka Miloš JUDr., Hálkova 2, Praha 2, 12000;

(54) Název přihlášky vynálezu:

Způsob opatřování poštovních zásilek záznamy o frankování



(57) Anotace:

Zákaznický systém zavádí od střediska přenosu hodnoty přes datové vedení poplatek a řídí tisk záznamů o frankování na poštovní zásilky. Středisko přenosu hodnoty zasílá na zákaznický systém datový balík. Podle řešení způsob uvádí, že středisko přenosu hodnoty vytváří kód a kód přenáší na zákaznický systém. V zákaznickém systému se vytvářejí data, která se kódem kódují tak, že středisko přenosu hodnoty může tato dekódovat. Data se od zákaznického systému posílají ke středisku přenosu hodnoty. Středisko přenosu vytváří náhodné číslo a následovně data spolu s náhodným číslem kódujc znovu jak s kódem neznámým zákaznickému systému, tak i s kódem známým bezpečnostnímu modulu zákaznického sytému. Takto kódovaná data následně přenáší na zákaznický systém. Řešení se dále týká zákaznického systému ke frankování poštovních zásilek a střediska přenosu hodnoty pro použití ve způsobu frankování.

CZ 2003 - 1357 A3

JUDr. Miloš Věstěnka
advokát
120 00 Praha 2, Hálkova 2

ZPŮSOB OPATŘOVÁNÍ POŠTOVNÍCH ZÁSILEK ZÁZNAMY O FRANKOVÁNÍ

Oblast techniky

Vynález se týká způsobu opatřování poštovních zásilek záznamy o frankování, přičemž zákaznický systém zavádí přes datové vedení od střediska přenosu hodnoty poplatek, přičemž zákaznický systém řídí tisk záznamů o frankování na poštovních zásilkách a přičemž středisko přenosu hodnoty posílá datový balík na zákaznický systém.

Dosavadní stav techniky

Způsob takového druhu je znám z mezinárodní patentové přihlášky WO 98 14907.

Další způsob je znám z německého patentového spisu DE 31 26 785 C2. U tohoto způsobu se uskutečňuje vytvoření opětovně zaváděného signálu, určeného pro frankování poštovních zásilek, v separátní oblasti střediska přenosu hodnoty, provozovaného poštovním přepravním podnikem.

Neuveřejněná německá patentová přihláška 100 20 566.6/53 se týká rovněž způsobu opatřování poštovních zásilek záznamy o frankování.

U tohoto způsobu zavádí zákaznický systém přes datové vedení od střediska přenosu hodnoty poplatek na způsob

datového balíku, který zákaznický systém používá k vytvoření záznamů o frankování. Tento způsob se vyznačuje tím, že v zákaznickém systému se vytvářejí data, která jsou tak kódovaná, že středisko přenosu hodnoty tato může dekódovat, že data se vysílají od zákaznického systému ke středisku přenosu hodnoty a že středisko přenosu hodnoty data dekóduje a následně data znovu kóduje kódem, neznámým zákaznickému systému, a takto zakódovaná data následně přenáší na zákaznický systém. Přednostní provedení tohoto způsobu se vyznačuje tím, že kódování se v zákaznickém systému uskutečňuje při použití náhodného čísla, které slouží jako autentifikační kód. Způsob se mimo jiné vyznačuje tím, že náhodné číslo se vytváří v bezpečnostním modulu, ke kterému nemá uživatel zákaznického systému žádný přístup.

Protože taková náhodná čísla, která slouží jako autentifikační kód, hrají důležitou úlohu vzhledem k zabezpečení ohledně manipulace celého systému, má velký význam kvalita popř. „náhodnost", se kterou se vytvářejí náhodná čísla. Z toho v praxi vyrůstá problematika, že bezpečnostní moduly, které se ve velkém počtu nacházejí v zákaznickém systému a z důvodů hospodárnosti nabízejí místo jen pro omezené interní funkčnosti a algoritmy, musejí vyhovovat vysokým požadavkům na kvalitu náhodného čísla.

Zejména se musí zabraňovat, aby neoprávněné osoby nezískali znalost náhodného čísla, protože pomocí znalosti náhodného čísla by bylo možné, vytvářet za účelem zneužití, bez finanční úhrady, platně se jevící záznamy o frankování i bez použití bezpečnostního modulu.

Vynález má za úkol, provádět způsob podle úvodu tak, že se zabraňuje vytvářet záznamy o frankování za účelem

zneužití.

Podstata vynálezu

Podle vynálezu se tento úkol řeší tím, že středisko přenosu hodnoty vytváří kód a kód přenáší na zákaznický systém, že v zákaznickém systému se vytvářejí data, která se kódem kódují tak, že je středisko přenosu hodnoty může dekódovat, že se data vysílají od zákaznického systému ke středisku přenosu hodnoty a že středisko přenosu hodnoty data dekóduje a následně data znovu kóduje kódem, zákaznickému systému neznámému a ta, takto kódovaná data, následně přenáší na zákaznický systém.

Aby se pomocí možné předpověditelnosti kvalitativně špatných náhodných čísel, která se tvoří v bezpečnostním modulu, zabránilo zneužití, vytváří se náhodné číslo také centrálně ve středisku přenosu hodnoty pro všechny bezpečnostní moduly při každém procesu zavádění. V rámci elektronické datové komunikace mezi střediskem přenosu hodnoty a příslušným bezpečnostním modulem v zákaznickém systému se kód přenáší zakódován a digitálně signován. Příprava kvalitativně vysoce jakostního náhodného čísla se může lépe zaručovat v centrálním středisku přenosu hodnoty než v bezpečnostním modulu v zákaznickém systému.

Zvlášť přednostní způsob provedení způsobu podle vynálezu se vyznačuje tím, že v zákaznickém systému se vytvářejí data k identifikaci a autentifikaci jakož i k požadované akci, která jsou kódovaná tak, že středisko přenosu hodnoty je může dekódovat, že data se vysílají od zákaznického systému ke středisku přenosu hodnoty a že

středisko přenosu hodnoty data dekóduje a následovně data znovu kóduje kódem, zákaznickému systému neznámým, a takto kódovaná data následně spolu s dalšími, nově přistupujícími kódovanými daty, která se ale mohou dekódovat zákaznickým systémem, přenáší na zákaznický systém.

Přednostní způsob provedení způsobu podle vynálezu se vyznačuje tím, že kódování ve středisku přenosu hodnoty se uskutečňuje při použití náhodného čísla.

Je účelné, že náhodné číslo se kóduje spolu s kódem relace, vydaným zákaznickým systémem a veřejným kódem zákaznického systému. Způsob se dále vyznačuje tím, že středisko přenosu hodnoty signuje data privátním kódem.

Dále je výhodné, že dekódování se uskutečňuje v bezpečnostním modulu v zákaznickém systému, ke kterému nemá zákaznik žádný přístup.

Další výhodný způsob provedení způsobu se vyznačuje tím, že dekódované náhodné číslo se ukládá v bezpečnostním modulu zákaznického systému, ke kterému nemá zákazník žádný přístup.

Zákaznický systém je přednostně konstruován tak, že není s to úplně dekódovat data, vyslaná od střediska přenosu hodnoty, ale dopisové středisko, ve kterém se poštovní zásilky kontrolují ohledně správného frankování, může tato data dekódovat.

Středisko přenosu hodnoty může být konstruováno různými způsoby. Pojem středisko přenosu hodnoty zahrnuje jak známá střediska přenosu hodnoty, tak i nové formy středisek

přenosu hodnoty.

Vynález se týká zejména takových středisek přenosu hodnoty, přes která se může bezprostředně přistupovat na datové komunikační vedení, jako na internet nebo na datový server, připojený na telefonní vedení.

Výhodný způsob provedení způsobu a přednostní provedení střediska přenosu hodnoty se vyznačují tím, že kódování se uskutečňuje ve středisku přenosu hodnoty při použití náhodného čísla.

Je účelné, že náhodné číslo se vytváří v bezpečné oblasti střediska přenosu hodnoty.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že náhodné číslo se kóduje kódem relace, vydaným střediskem přenosu hodnoty, a veřejným kódem bezpečnostního modulu zákaznického systému.

Je účelné, že středisko přenosu hodnoty signuje data privátním kódem.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že privátní kód je uložen ve zvláště zabezpečené oblasti střediska přenosu hodnoty.

Je účelné, že data se s každým požadavkem poplatku přenášejí od zákaznického systému na středisko přenosu hodnoty.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že středisko přenosu hodnoty se identifikuje podle předávaných dat zákaznického systému.

Je účelné, že středisko přenosu hodnoty posílá na zákaznický systém data jím zakódovaná.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že data, posílaná střediskem přenosu hodnoty na zákaznický systém mají první složku, která se nemůže zákaznickým systémem dekódovat a že data dále mají druhý podíl, který se může zákaznickým systémem dekódovat.

Je účelné, že část dat, dekódovatelná v zákaznickém systému, obsahuje informace o identitě zákaznického systému.

Je účelné, že část dat, dekódovatelná v zákaznickém systému, obsahuje náhodné číslo, tvořené ve středisku přenosu hodnoty.

Přednostní způsob provedení způsobu, přednostní provedení zákaznického systému, a střediska přenosu hodnoty se vyznačují tím, že podíl dat, dekódovatelný zákaznickým systémem, obsahuje informace o výši poplatku.

Je účelné, že vysílání dat od zákaznického systému na středisko přenosu hodnoty se uskutečňuje pouze tehdy, když se v zákaznickém systému má zavést obnos v minimální výši.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se

vyznačují tím, že ve středisku přenosu hodnoty se vytváří transformační hodnota.

Je účelné, že transformační hodnota se tvoří při zahrnutí údajů o datech zásilky.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že transformační hodnota se tvoří při zahrnutí přijatého a přechodně uloženého náhodného čísla.

Je účelné, že transformační hodnota se tvoří při zahrnutí identifikačního čísla procesu zavádění.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že záznam o frankování obsahuje logická data.

Je účelné, že záznam o frankování obsahuje informace o datech zásilky.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že logická data obsahují informace o kódovaném náhodném čísle.

Je účelné, že logická data obsahují informace o kódovaném identifikačním čísle procesu zavádění.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že logická data obsahují informace o transformační hodnotě.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že záznam o frankování obsahuje jak informaci přenášenou od střediska přenosu hodnoty, tak i data, zadávaná zhotovitelem dokumentu.

Je účelné, provádět způsob tak, popřípadě zákaznický systém nebo středisko přenosu hodnoty konstruovat tak, že záznam o frankování obsahuje transformační hodnotu, která se tvoří z kombinace hodnoty, přenášené ze střediska zadávání a hodnoty, zadávané zhotovitelem dokumentu.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že zahrnují následující kroky způsobu: zákaznický systém nebo bezpečnostní modul, spojený se zákaznickým systémem, inicializuje proces zavádění, přičemž se na středisko přenosu hodnoty předává identita zhotovitele dokumentu a/nebo jím použitého zákaznického systému.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že ve středisku přenosu dat se tvoří náhodné číslo.

Je účelné, způsob provádět tak, popřípadě zákaznický systém nebo středisko přenosu hodnoty konstruovat tak, že středisko přenosu hodnoty tvoří identifikační číslo zavádění a spolu s vytvořeným náhodným číslem jednak tak kóduje, že jenom dopisové středisko tyto může dekódovat a následovně vytváří identifikační číslo zavádění.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že středisko přenosu hodnoty vytvořené identifikační číslo zavádění spolu s vytvořeným náhodným číslem kóduje takovým způsobem na jiné, že jenom bezpečnostní modul v zákaznickém systému může tyto dekódovat.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že ve zvláště zabezpečené oblasti střediska přenosu hodnoty se z identifikačního čísla zavádění a dalších dat tvoří transformační hodnota.

Je účelné, provádět způsob tak, popřípadě zákaznický systém a/nebo středisko přenosu hodnoty konstruovat tak, že záznam o frankování je vytvořen tak, že obsahuje transformační hodnotu.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že platnost záznamů o frankování se kontroluje v dopisovém středisku.

Je účelné, provádět způsob tak, popřípadě zákaznický systém nebo středisko přenosu hodnoty konstruovat tak, že kontrola v dopisovém středisku se uskutečňuje analýzou dat, obsažených v záznamu o frankování.

Výhodný způsob provedení způsobu, přednostní provedení zákaznického systému a střediska přenosu hodnoty se vyznačují tím, že kontrolní místo tvoří z dat, obsažených v záznamu o frankování, transformační hodnotu a kontroluje,

zda se tato transformační hodnota shoduje s transformační hodnotou, obsaženou v záznamu o frankování a v případě neshody registruje záznam o frankování jako padělany.

Přehled obrázků na výkresech

Vynález bude blíže vysvětlen prostřednictvím konkrétních příkladů provedení znázorněných na výkresech, na kterých představuje

obr. 1 principiální znázornění způsobu podle vynálezu,

obr. 2 principiápní znázornění, znázorněné na obr. 1, s vyzdvižením stran, zúčastněných na procesu frankování,

obr. 3 rozhraní frankovacího systému, znázorněného na obr. 1 a obr. 2 a

obr. 4 principiální zobrazení bezpečnostních mechanismů, použitých ve způsobu.

Příklady provedení vynálezu

Následující příkladné provedení popisuje vynález podle navrženého použití v oblasti Deutsche Post AG. Je ale samozřejmě stejně možné, použít vynález pro frankování jiných dokumentů, zejména pro použití v oblasti jiných zasílatelských podniků.

Vynález dává k dispozici možný nový způsob frankování,

se zákazníky při použití běžného PC s tiskárnou a dodatečným soft- a popřípadě hardware, jakož i internetového přístupu, moci tisknout na dopisy, korespondenční lístky atd. digitální záznamy o frankování.

Zaplacení k vyrovnání hodnot frankování, vytištěných zákazníkem, se může dít různými způsoby. Například se zmenšuje uložené aktivum. Toto aktivum je přednostně uloženo digitálně. Digitální uložení se uskutečňuje například na speciální zákaznické kartě, standardizované peněžní kartě nebo ve virtuální paměti, která se nachází například v počítači uživatele. Obnos aktiva se přednostně zavádí dříve než se uskuteční tisky hodnot frankování. Zavádění obnosu aktiva se uskutečňuje ve zvláště přednostním provedení postupem při vystavování vrubopisu.

Na obr. 1 je znázorněn principiální průběh, podle vynálezu, frankování poštovních zásilek. Způsob zahrnuje více kroků, které se přednostně mohou doplňovat na celý cyklus. Toto je sice zvláště účelné, ale ne nutné. Následovně znázorněný počet osmi kroků je stejně přednostní, ale rovněž není nutný.

1. Pomocí PC zavést zákazníkům zasílatelského podniku (popřípadě při použití dodatečného soft-/hardware, například mikroprocesorové čipové karty) přes internet cenný obnos.

2. O cenném obnosu se uskutečňuje inkaso, například pomocí odúčtování z konta zákazníka.

3. Z cenného obnosu, který je u zákazníka uložen v elektronické peněžence, se mohou vhodnou

tiskárnou tak dlouho tisknout platné frankovací hodnoty v libovolné výši, až je aktivum spotřebováno.

4. Zákazníkem vytištěný záznam o frankování obsahuje čitelné údaje jakož i strojově čitelný čárový kód, který se ze strany Deutsche Post používá ke kontrole platnosti.

5. Ofrankovaná poštovní zásilka se může podávat pomocí možností, poskytnutých ze strany Deutsche Post, například poštovních schránek nebo poštovních poboček.

6. Čárový kód, uvedený v záznamu o frankování, přednostně 2D-čárový kód, se v dopisovém středisku čte pomocí stroje na čtení adres. Během zhotovení se uskutečňuje kontrola platnosti na logické bázi věrohodnosti.

7. Data, čtená v záznamu o frankování, se mimo jiné přenášejí na pomocný systém k zajištění finanční úhrady.

8. Mezi zavedenými zúčtovacími obnosy a produkovanými zásilkami se k rozpoznání zneužití provádí porovnání.

Na způsobu frankování se přednostně podílí několik stran, přičemž zvláště účelné rozdělení stran je znázorněno na obr. 2.

Znázorněné strany jsou zákazník, zákaznický systém a

zasílatelský podnik.

Zákaznický systém zahrnuje hard- a software, které se zákazníkem používají k PC-frankování. Zákaznický systém řídí v interakci se zákazníkem zavádění a ukládání zúčtovaných obnosů a vytisknutí záznamu o frankování. Podrobnosti k zákaznickému systému regulují předpoklady pro registraci.

Zasílatelský podnik přebírá produkci zásilek a provádí požadované zajištění finanční úhrady.

Středisko přenosu hodnoty může být provedeno různými způsoby:

- Provoz střediska přenosu hodnoty dělá ve spojení bezpečnostní architekturou PC-frankování možným použití symetrických kódovacích způsobů v záznamu o frankování. Tím se značně redukuje potřebný čas na kontrolu platnosti záznamu o frankování. Pro použití symetrického způsobu je potřebný provoz střediska přenosu hodnoty a dopisového střediska stejnou organizací. Takové zrychlené zhotovení není při použití asymetrických bezpečnostních členů v záznamu o frankování možné.

- Realizace všech potřebných bezpečnostních požadavků, mimo jiné k zabránění interních a externích manipulací: Jinak než při volném razítkování odesílatelem se uskutečňuje komunikace přes otevřený a potenciálně nebezpečný internet. Útoky na komunikační cesty a internetové servery jakož i interní možnosti manipulace vyžadují vyšší bezpečnostní opatření.

- Pomocí centrálního řízení kryptografických kódů, předem daného zasílatelským podnikem, je možné zlepšení zabezpečení. Kódy, relevantní při zhotovení v dopisovém středisku, se mohou kdykoliv vyměňovat a mohou se měnit délky kódů.

- Kontroly k zajištění finanční úhrady jsou možné podle jednotného kontrolního způsobu a v každém okamžiku se nechají provádět.

- Noví smluvní účastníci a změny ve smlouvách se mohou rychle sdělovat všem požadovaným systémům zasílatelského podniku.

Zajištění finanční úhrady se přednostně uskutečňuje při evidenci součástí záznamů o frankování.

K tomu se na systém předávají z centrální databáze data o dohodě (zákaznická data/data zákaznického systému), což je zapotřebí pro kontrolu řádného zajištění finanční úhrady.

Rozsah dat, která je třeba ukládat, stanovuje zasílatelský podnik, zejména provozovatel poštovní služby při zohlednění zákonných ustanovení jako vyhláška o ochraně dat podniky poštovní služby (PDSV). V zásadě se mohou potom ukládat všechna data, která jsou potřebná pro řádné stanovení, vyúčtování a vyhodnocení jakož i k prokázání správnosti dodatečné finanční úhrady. V zásadě jsou to všechny informace o zásilce bez jména příjemce a případně domovního čísla/čísla poštovní přihrádky příjemce.

Pomocný systém kontroluje, zda obnosy aktiva, obsažené v zákaznickém systému, se skutečně zmenšují ve výši

poplatků, které se tisknou jako záznamy o frankování.

Pro sběr smluvních dat je přednostně navržen sběrný systém.

Smluvní data k PC-frankování s příslušnými kmenovými daty zákazníků a zákaznického systému (např. bezpečnostní modul-ID) se například poskytují a spravují přes databázi, která se nechá například použít i k jiným způsobům frankování.

Při použití existující databáze frankování se například v databázi implementuje separátní dílčí oblast k PC-frankování. Data se poskytují ve středisku přenosu hodnoty a v systému zajištění finanční úhrady v dopisovém středisku. Je zvláště účelné, že systém obsahuje rozhraní, která umožňují výměnu dat a informací s dalšími systémy.

Na obr. 3 jsou znázorněna tři rozhraní.

Rozhraní jsou označena „Zadávání", „Záznam o frankování" a „Inkaso". Přes zúčtovací rozhraní se mezi zákaznickým systémem a vedoucím zásilkové služby vyměňují zúčtovací data. Přes zúčtovací rozhraní se například může zavádět peněžní obnos.

Frankovací rozhraní stanovuje, jak vypadají záznamy o frankování, aby se mohly číst a kontrolovat v dopisových, popřípadě přepravních střediscích.

U implementace rozhraní, znázorněné na obr. 3, jsou zúčtovací rozhraní a inkasní rozhraní od sebe oddělená. Je ale také rovněž možné, že zúčtovací rozhraní a inkasní

rozhraní jsou shrnuty domrmady, například při zúčtování přes peněžní karty, kreditní karty nebo digitální peníze, zejména digitální mince. Inkasní rozhraní stanovuje, jak se uskutečňuje zúčtování poplatků, předávaných přes zúčtovací rozhraní. Ostatní parametry způsobu frankování nezávisí na zvoleném inkasním rozhraní, ale pomocí účinného inkasního rozhraní se zvyšuje účinnost celkového systému. Přednostními inkasními možnostmi jsou vrubopisy a účty.

V dalším se zobrazuje, jak se pomocí aplikačně specifických, obsahu se týkajících, bezpečnostních požadavků, dosahuje bezpečnostních cílů způsobu frankování.

Ohnisko této koncepce je přitom směřováno na technickou specifikaci bezpečnostních požadavků na systém. Procesy, které nejsou bezpečnostně relevantní, jako při-, od- a přehlášení zákazníků, které se nemusí uskutečňovat přes zákaznický systém, se mohou stanovovat separátně. Technické procesy mezi zákaznickým systémem a zhotovitelem zákaznického systému se stanovují přednostně tak, že odpovídají zde znázorněnému bezpečnostnímu standardu.

Způsobem podle vynálezu se dosahuje následovně uvedených bezpečnostních cílů.

- Fantazijní a podvodné známky, tedy frankovací záznamy, které neobsahují žádné věrohodné údaje k zásilce nebo jsou z jiných důvodů nečitelné, se rozpoznávají jako neplatné.

- Dublety, tedy exaktní kopie platných záznamů o frankování s hodnověrnými údaji k zásilce, se mohou rozpoznávat zpětně.

- Zamezuje se zvýšení obnosu aktiva, který je k dispozici zákaznickému systému. Změny obnosu aktiva jsou rozpoznatelné zpětně a mohou se přednostně dodatečně prokazovat podle seznamu protokolu.

- Rozpoznávají se neoprávněná použití a oprávněnému uživateli se v případě neoprávněného použití třetí stranou nevrubopisují.

- K tomu se počítá zneužité zpeněžení řádně přenášených elektronických dat nebo platných, řádně vytvořených frankovacích záznamů o frankování bez vědomí řádného uživatele.

- K tomu se počítá zneužité použití zákaznického systému pomocí změn v programu.

- K tomu se počítá zneužité použití zákaznického systému cizími softwarovými vyzvědači přes internet.

- K tomu se počítá vyzkoumání PIN pomocí útočného software (trojské koně).

- K tomu se počítají napadení z přetížení (Denial-of-Service-Attacks, DoS), například předstíráním identity střediska přenosu hodnoty nebo manipulací procesu zavádění na způsob, že se peníze odúčtují, ale nezřídí se žádné aktivum.

- Neoprávněné zavedení zúčtovacích obnosů se pomocí technických opatření ve středisku přenosu hodnoty činí nemožným. Neoprávněné zavedení zúčtovacích obnosů by se

např. mohlo uskutečňovat:

- Předstíráním identity poštovního střediska přenosu hodnoty ke zvýšení vlastní peněženky v zákaznickém systému zákazníkem.

- Předstíráním certifikovaného zákaznického systému pomocí manipulovaného nebo vymyšleného zákaznického systému takovým způsobem, že pachatel nabyl znalost bezpečnostně kritických tajemství bezpečnostního modulu a poté může nepozorovaně zhotovit padělky.

- Přerušením řádné komunikace mezi zákaznickým systémem a střediskem přenosu hodnoty a opakování této komunikace v úmyslu zneužití (Replay-Attacke).

- Manipulací komunikace, existující mezi zákaznickým systémem a střediskem přenosu hodnoty, v reálném čase (datové proudy, vcházející a vycházející v zákaznickém systému), způsobem, že zákaznický systém vychází z vyššího zavedeného cenného obnosu než středisko přenosu hodnoty.

- Zneužitím čísla identifikace zákazníka způsobem, že třetí osoby zavádějí na náklady zákazníka cenné obnosy.

- Neúplnou realizací storna.

První dva z těchto bezpečnostních problémů se v podstatě řeší systémovým konceptem a opatřeními v celkovém

systému, tři poslední se přednostně řeší implementací soft- a hardware bezpečnostního modulu.

Přednostní provedení hardware, zvyšujícího bezpečnostní standardy, jsou znázorněna následovně:

- Základní vlastnosti hardware

1. Všechna kódování, dekódování, překódování, výpočty signatur a kryptografické kontrolní procedury se provádějí ve zvláště proti neoprávněným přístupům chráněných oblastech kryptografického bezpečnostního modulu v zákaznickém systému a/nebo v bezpečné oblasti střediska přenosu hodnoty. Příslušné kódy jsou rovněž odložené v takových bezpečných oblastech.

2. Bezpečnostně relevantní data a průběhy (například kódy, programy) se chrání proti neoprávněným změnám a tajná data (například kódy, PINy) proti neoprávněnému přečtení. Toto se přednostně zaručuje následujícími opatřeními:

   - Konstrukcí bezpečnostního modulu, eventuálně ve spolupráci s bezpečnostními mechanismy software bezpečnostního modulu,
   - Zavedením programu do bezpečnostních modulů jen při zhotovení nebo kryptografickém zajištění procesu zavádění,
   - kryptografickým zajištěním zavádění bezpečnostně relevantních dat, zejména kryptografických kódů.
   - Také před přečtením pomocí napadení, které počítá se zničením modulu, musí být tajná data chráněna v bezpečnostních modulech.

a. Ochrana dat a programů vůči změně, popřípadě přečtení v bezpečnostním modulu, musí být tak vysoká, že během životnosti modulu nejsou možná napadení s vynaložením úměrných nákladů, přičemž náklady, potřebné pro úspěšnou obranu, je třeba uvážit v porovnání s užitkem, z tohoto plynoucím.

b. Nežádoucí funkce se nesmějí nechat zabezpečovacím modulem provést.

- Zabraňuje se nežádoucím vedlejším funkcím a dodatečným datovým kanálům, zejména rozhraním, které nechtěně předávají dále informace (Side Channels).

Konstrukcí bezpečnostního modulu se zajišťuje, že útočník nemůže číst informace o v tajnosti udržovaných datech a kódech přes rozhraní, která jsou určena pro jiné účely.

Existence Side Channels se kontroluje příslušnými testy. Typické možnosti, které se kontrolují, jsou:

1. Single Power Attack (SPA) a Differential Power Attack (DPA), která zkoušejí ze změn proudové spotřeby během kryptografických výpočtů usuzovat na tajná data.
2. Timing Attacks, které zkoušejí z doby trvání kryptografických výpočtů usuzovat na tajná data.

Přednostní vlastnosti zpracování dat jsou znázorněna následovně:

- Kontrola chodu:

Je zvláště účelné, že se provádí kontrola chodu. Toto

se může uskutečňovat například pomocí stavového přístroje, například podle standardu FIPS PUB 140-1. Tím se zajišťuje, že se nemůže manipulovat průběhy specifikovaných transakcí a přitom používanými bezpečnostně relevantními daty systému.

Zúčastněné instance, zejména uživatel, se nesmějí bezpečnostním modulem klamat o chodu transakcí.

Když je například proces zavádění cenného obnosu realizován na způsob několika dílčích procesů s jednotlivými zavoláními bezpečnostního modulu, musí kontrola chodu zajistit, že tyto dílčí procesy se provádějí jen v přípustném pořadí.

Stavová data, která se používají pro kontrolu chodu, jsou bezpečnostně relevantní a ukládají se proto přednostně v oblasti bezpečnostního modulu, jištěné proti manipulaci.

- Integrita zpráv:

1. Všechny bezpečnostně relevantní informace ve zprávách se před a po přenosu chrání v komponentách systému vhodnými způsoby proti neoprávněným změnám.
2. Rozpoznávají se změny v bezpečnostně relevantních informacích během přenosu mezi komponentami platebního systému, podporovaného čipovými kartami. Musí následovat příslušné reakce na porušení integrity.
3. Rozpoznává se neautorizované nahrání zpráv. Příslušné reakce musí následovat také na opětovně nahrané zprávy.

Aby se neoprávněné změny a opětovné nahrání zpráv mohlo rozpoznávat, zajišťuje se pro standardní zprávy systému pomocí určení konceptu systému. Software bezpečnostního

modulu zajistil, že rozpoznání se skutečně uskutečňuje a příslušně se reaguje. Pro bezpečnostně relevantní zprávy, specifické pro výrobce (třeba v rámci personalizace údržby bezpečnostního modulu) se stanovují a používají příslušné vhodné mechanismy.

Informace, relevantní pro bezpečí integrity zpráv, se přednostně ukládají v oblasti bezpečnostního modulu, zabezpečené proti manipulaci. Takovými informacemi jsou zejména identifikační znaky a znaky autenticity, sekvenční čítače nebo poplatky.

- Utajení PIN a kryptografických kódů

1. Ačkoliv by se PIN vně bezpečných oblastí neměly přenášet jako nekódovaný text, toleruje se přednostně přenos nekódovaného textu při PC-frankování z důvodu uživatelské přívětivosti celkového systému a použití existujících, nezajištěných hardware komponent v zákaznickém systému (klávesnice, monitor). Lokální systémové komponenty, ve kterých se PIN zpracovávají jako nekódovaný text nebo ukládají, se redukují na minimum. Nezabezpečený přenos PIN se nesmí uskutečňovat.
2. Kryptografické kódy se nesmějí v nekódované podobě přenášet po elektronických přenosových cestách v nezabezpečeném prostředí. Pokud se používají nebo ukládají v systémových komponentách, musejí být chráněné proti neautorizovanému čtení a změnám.
3. Žádná systémová komponenta nesmí nabízet možnost k určení PIN na základě vyčerpávajícího hledání.

- Zaprotokolování

1. Uvnitř zákaznického systému se protokolují všechna

data, která jsou zapotřebí pro rekonstrukci příslušných průběhů. Dále se protokolují také chybné případy, které naznačují podezření na manipulaci.

2. Uložená zaprotokolovaná data musí být chráněna proti neoprávněným změnám a autenticky se mohou přenášet na vyhodnocovací instanci.

- Zpracování ostatních aplikací

Pokud se v bezpečnostních modulech zpracovávají současně jiné aplikace, nesmí se tím ovlivňovat zabezpečení PC-frankovacího systému.

Následujícími opatřeními se může dále zvyšovat zabezpečení dat:

- Mazání tajných dat z dočasných pamětí
- Bezpečná implementace funkcí specifických pro výrobce (např. v rámci personalizace); třeba použití Triple-DES nebo bezpečného symetrického způsobu pro kódování tajných dat personalizace, získání kódů nekódovaného textu na způsob rozdělených tajemství (např. poloviny kódů) podle principu čtyř očí.
- Nesmějí existovat žádné nejisté dodatečné funkce (třeba kódování nebo dekódování nebo signování volně volitelných dat kódy systému); nesmí být možná žádná funkční záměna kódů.

Další aspekty

- Mimo bezpečnostních modulů, vložených do zákaznických systémů, je třeba prozkoumat i další bezpečnostní moduly: zejména je třeba prozkoumat bezpečnostní moduly různých certifikačních míst (CAs) u výrobců bezpečnostních modulů.

- Také podíl, na PC straně, zákaznického software je třeba prozkoumat vzhledem ke svým bezpečnostně relevantním úkolům (např. PIN-zadání).
- Výrobcem zákaznického systému je navržen způsob, že se garantuje zabezpečené předávání PIN od bezpečnostních modulů na uživatele (například PIN-zasílání dopisy). Takový koncept je třeba přezkoušet na zabezpečení a zachování.
- Bezpečí prostředí výrobce, zejména získání kódu atd.; osoby pověřené zabezpečením, obecně: připuštění organizačních bezpečnostních opatření výrobců podle pevně stanoveného způsobu. V podrobnostech:

Správa kódů

1. K rozdělení, správě a eventuálně k turnusové výměně a k náhradě kódů je třeba učinit pravidla.
2. Kódy, pro které existuje podezření na kompromitování, se v celkovém systému nesmějí používat.

Přednostní opatření při výrobě a personalizaci bezpečnostních modulů jsou:

1. Výroba a personalizování (první dodání tajných kódů, eventuálně dat, specifických pro zákazníka) bezpečnostních modulů musí existovat v prostředí výroby, které zabraňuje aby
   - se kódy při personalizování kompromitovaly,
   - se proces personalizování prováděl s úmyslem zneužití nebo neoprávněně,
   - se mohl dodávat neautorizovaný software nebo data,
   - se bezpečnostní moduly kradly.

2. Musí být zajištěno, že do systému se nemohou dodat žádné neautorizované komponenty, které provádějí bezpečnostně relevantní funkce.
3. Životní běh všech bezpečnostních modulů musí být kontinuálně zaznamenán.

Výklad:

Záznam životního běhu bezpečnostního modulu zahrnuje přednostně:

- data výroby a personalizace,
- prostorové/časové místo pobytu,
- opravu a údržbu,
- vyjmutí z provozu,
- ztráta popř. krádež pamětí s daty, obsahujících bezpečnostní modul, jako soubory, Dongles, Krypto, server nebo čipové karty
- data výroby a personalizace,
- změna aplikací,
- změna kódů,
- vyjmutí z provozu,
- ztráta popř. krádež.

Bezpečnostní architektura

Pro PC-frankování se navrhuje principiální bezpečnostní architektura, která spojuje přednosti různých existujících přístupů a jednoduchými prostředky poskytuje vyšší míru bezpečnosti.

Bezpečnostní architektura zahrnuje přednostně v podstatě tři jednotky, které jsou představené

s přednostním uspořádání na obr. 4:

- Středisko přenosu hodnoty, ve kterém je známá identita zákazníka a jeho zákaznického systému.
- Bezpečnostní modul, který hard-/software, nemanipulovatelnému zákazníkem, zaručuje bezpečnost v zákaznickém systému (např. Dongle nebo čipová karta u Offline-řešení popř. náhradní server u Online-řešení).
- Dopisové středisko, ve kterém se kontroluje platnost záznamu o frankování, popřípadě se rozpoznávají manipulace na cenném obnosu popř. na záznamu o frankování.

Jednotlivé kroky procesu, které se uskutečňují ve středisku přenosu hodnoty, zákaznickém systému a dopisovém středisku, se v dalším znázorňuji na způsob principiální skici. Přesný technický proces komunikace se naproti tomu odchyluje od tohoto principiálního zobrazení (např. několik komunikačních kroků k dosažení zde znázorněného přenosu). V tomto znázornění se zejména předpokládá důvěrná a celočíselná komunikace mezi identifikovanými a autentifikovanými komunikačními partnery.

Zákaznický systém

0. Uvnitř zaváděcího střediska se vytváří kód a následně se přenáší na zákaznický systém. Přenos kódu se přednostně uskutečňuje kódovaně a popřípadě digitálně signován. Zejména je účelné, že kód se nachází v digitální dopisní obálce.

1. Od bezpečnostního modulu se jednoznačné identifikační číslo (bezpečnostní modul - ID) zákaznického systému

předává takovým způsobem zakódované na středisko přenosu hodnoty, že jen středisko přenosu hodnoty je s to, provádět dekódování. Ve zvláště přednostním provedení se dotaz kóduje veřejným kódem střediska přenosu hodnoty a digitálně se signuje privátním kódem bezpečnostního modulu. Tím se zabraňuje, že dotaz má při každém zavádění zúčtovaného obnosu stejný tvar a může se používat ke zneužitému zavádění zúčtovaných obnosů (Replay-Attack).

2. Kryptograficky ošetřené informace ze zákaznického systému se přenášejí na středisko přenosu hodnoty v rámci zavádění zúčtovaného obnosu. Ani zákazník ani nikdo třetí nemůže tyto informace dekódovat.

V praxi se používá asymetrické kódování s veřejným kódem komunikačního partnera (středisko přenosu hodnoty, popřípadě bezpečnostní modul).

U možnosti předcházející výměny kódů přichází rovněž také do úvahy symetrické kódování.

Středisko přenosu hodnoty

3. Ve středisku přenosu hodnoty se mimo jiné dekóduje identifikační číslo bezpečnostního modulu (bezpečnostní modul - ID).

4. Dotazem v databázi frankování se zákazníkovi Deutsche Post přiřazuje bezpečnostní modul - ID.

5. Ve středisku přenosu hodnoty se vytváří náhodné číslo.

Ve středisku přenosu hodnoty se tvoří identifikační číslo procesu zavádění, které zahrnuje části bezpečnostního modulu - ID, výši zúčtovaného obnosu atd.

6. Identifikační číslo zavádění se spolu s vytvořeným náhodným číslem zaprvé kóduje takovým způsobem, že zákaznický systém není s to je dekódovat. V praxi se uskutečňuje kódování symetrickým kódem podle TDES, který existuje výlučně ve středisku přenosu hodnoty jakož i v dopisových střediscích. Použití symetrického kódování na tomto místě je odůvodněné požadavkem po rychlém způsobu dekódování pomocí produkce.

7. Identifikační číslo zavádění se spolu s vytvořeným náhodným číslem zadruhé kóduje takovým způsobem, že jenom bezpečnostní modul v zákaznickém systému je s to je dekódovat.

8. Rozdílně kódované páry identifikačního čísla procesu zavádění a náhodného čísla se přenášejí na zákaznický systém. Ani zákazník nebo někdo třetí nemůže tyto informace dekódovat. Pomocí výhradní správy poště vlastního, přednostně symetrického kódu ve středisku přenosu hodnoty a v dopisovém středisku se může kód kdykoliv vyměňovat a délky kódů se mohou v případě potřeby měnit. Tím se jednoduchým způsobem zaručuje vysoké bezpečí při manipulaci.

Zákaznický systém

9. V bezpečnostním modulu zákaznického systému se náhodné číslo, které bylo kódováno takovým způsobem, že

bezpečnostní modul je mohl dekódovat, dekóduje a ukládá.

10. Zákazník zachycuje v rámci zhotovení záznamu o kódování informace specifické pro přenos nebo data přenosu (např. porto, způsob zásilky atd.), která se přenášejí do bezpečnostního modulu.

11. Uvnitř bezpečné oblasti střediska přenosu hodnoty se transformační hodnota mimo jiné tvoří z následujících informací
    - výtahy z dat zásilky (např. porto, způsob zaslání, datum, PLZ atd.),
    - přechodně uložené náhodné číslo (které se přijímalo v rámci zavádění zúčtovacího obnosu)
    - a popřípadě identifikační číslo procesu zavádění.

10. Do záznamu o frankování se mimo jiné přebírají následující data:
    - výtahy z dat zásilky v nekódovaném textu (např. porto, způsob zásilky, datum, PLZ atd.),
    - kódované náhodné číslo a kódované identifikační číslo procesu zavádění ze střediska přenosu hodnoty a
    - transformační hodnota tvořená uvnitř bezpečnostního modulu z dat zásilky, přijaté a přechodně uložené náhodné číslo a identifikační číslo procesu zavádění.

Dopisové středisko

11. V dopisovém středisku se zkoušejí napřed data zásilky. Pokud se data zásilky, přejatá do záznamu o frankování,

nesnoduji se zásilkou, existuje buď falešné frankování, fantazijní nebo podvodná známka. Zásilku je třeba dopravit k zajištění úplaty.

12. V dopisovém středisku se náhodné číslo a identifikační číslo procesu zavádění, která se předávala v rámci zúčtovacího obnosu na zákaznický systém, dekódují. K tomu je v dopisovém středisku zapotřebí jen jediný (symetrický) kód. Při použití individuálních kódů by se ale místo něho používal velký počet kódů.

13. V dopisovém středisku se podle stejného způsobu jako v bezpečnostním modulu tvoří transformační hodnota z následujících informací:
    - výtahy z dat zásilky,
    - dekódované náhodné číslo
    - dekódované identifikační číslo procesu zavádění.

14. V dopisovém středisku se porovnávají vlastní vytvořená a přenášená transformační hodnota. Pokud se obě shodují, tak se přenášená transformační hodnota tvořila se stejným náhodným číslem, které se také v rámci zavádění zúčtovaného obnosu předávalo středisku přenosu hodnoty. Proto se jedná nejenom o pravý, platný zúčtovaný obnos, ale i o data zásilky, se kterými byl bezpečnostní modul seznámen (kontrola platnosti). Podle nákladů odpovídají dekódování, tvorba transformační hodnoty a porovnání dvou transformačních hodnot teoreticky kontrole signatury. Na základě symetrického dekódování vzniká ale vůči kontrole signatury časový zisk.

15. Přes křížovou kontrolu v záložním systému se mohou

dodatečně zjišťovat odchylky mezi zavedenými zúčtovanými obnosy a frankovacími obnosy (kontrola chledně dubletů zásilek, tvorba salda v záložním systému).

Znázorněná zásadní bezpečnostní architektura nezahrnuje separátně zabezpečenou správu zúčtovaných obnosů (funkce peněženky), zajištění komunikace mezi zákaznickým systémem a střediskem přenosu hodnoty, oboustrannou identifikaci zákaznického systému a střediska přenosu hodnoty a inicializaci k bezpečnému zahájení provozu nového zákaznického systému.

Útoky na bezpečnostní architekturu

Popsaná bezpečnostní architektura je pomocí následujícího bezpečná proti útokům:

- Třetí strany nemohou v internetu přerušenou (kopírovanou) úspěšnou komunikaci mezi zákaznickým systémem a střediskem přenosu hodnoty použít k podvodným účelům (Replay-Attacke).
- Třetí strany nebo zákazníci nemohou vzhledem ke středisku přenosu hodnoty předstírat použití řádného zákaznického systému pomocí manipulovaného zákaznického systému. Pokud třetí strana nebo zákazník předstírá přenos náhodného čísla a Safe-Box-ID, které nebyly vytvořené uvnitř bezpečnostního modulu, nýbrž mu jsou známé, ztroskotává zavádění zúčtovaných obnosů buď na separátně provedené identifikaci řádného zákazníka pomocí jména uživatele a hesla, nebo na znalosti privátního kódu bezpečnostního modulu, který nesmí být zákazníkovi za žádných okolností znám. (Proto je vhodné provádět inicializační proces k vytvoření kódu

v bezpečnostním modulu a certifikování veřejného kódu pomocí poskytovatele zákaznického systému).

- Třetí strana nebo zákazníci nemohou s předstíraným střediskem přenosu hodnoty zavádět do zákaznického systému platné zúčtované obnosy. Pokud třetí strana nebo zákazník předstírají funkčnost střediska přenosu hodnoty, nedaří se tomuto předstíranému středisku přenosu hodnoty vytvořit zakódované identifikační číslo procesu zavádění, které se v dopisovém centru může řádně dekódovat. K tomu se certifikát veřejného kódu střediska přenosu hodnoty nemůže falšovat.
- Zákazníci nemohou při obejití střediska přenosu hodnoty zhotovit záznam o frankování, jehož identifikační číslo procesu zavádění je zakódované takovým způsobem, že by se mohlo v dopisovém středisku dekódovat jako platné.

Ke zvýšení bezpečí dat, zejména při hledání, se ke tvorbě transformační hodnoty přibírá vysoký počet náhodných čísel.

- Délka náhodného čísla je proto co možná největší a je přednostně alespoň 16 byte (128 bit). Použitá bezpečnostní architektura je pomocí možnosti používat kódy specifické pro zákazníka aniž by bylo nutné, mít v místech určených pro dekódování, zejména dopisových střediscích, připravené kódy, silnější než známé způsoby. Toto přednostní provedení představuje podstatný rozdíl ke známým systémům podle Information-Based Indicia Program (IBIP).

Výhody bezpečnostní architektury

Následující znaky vyznačují popsanou bezpečnostní

architekturu vuči IBIP-Modell z USA.

- Vlastní bezpečnost se zaručuje v systému Deutsche Post (středisko přenosu hodnoty, dopisové středisko, systém zajištění finanční úhrady, a je tím plně v oblasti vlivu Deutsche Post.
- V záznamu o frankování se nepoužívají žádné signatury, nýbrž technicky rovnocenná a rovněž bezpečná (symetricky) zakódovaná data a transformační hodnoty. K tomu se v nejjednoduššim případě používá jenom symetrický kód, který sám leží v oblasti vlivu Deutsche Post a tím se nechá lehce vyměnit.
- V dopisovém středisku je možná kontrola všech záznamů o frankování (ne pouze namátková kontrola).
- Bezpečnostní koncept je založen na jednoduchém, do sebe uzavřeném kontrolním cyklu, který je v souladu se záložním systémem tomu přizpůsobeným.
- Systém sám dělá jinak sotva zjistitelné dublety patrnými.

- Neplatné fantazijní známky jsou tímto způsobem rozpoznatelné s vysokou přesností.

- Vedle kontroly platnosti se může u všech záznamů o frankování uskutečnit kontrola identifikačního čísla procesu zavádění v reálném čase.

Typy zásilek

S PC-frankováním se mohou poskytovatelem zasílatelské služby frankovat všechny produkty poskytovatele zasílatelské služby jako například „Brief national" (včetně dodatečných služeb) a „Direkt Marketing national" podle předcházejícího ustanovení.

Použití pro jiné způsoby zasílání jako balíkové a expresní zásilky je rovněž možné.

Poplatek, který se může maximálně zavádět přes středisko přenosu hodnoty, se určuje na vhodný obnos. Obnos se může volit podle požadavku zákazníka a potřeby poskytovatele poštovní služby ohledně bezpečnosti. Zatímco pro použití v oblasti soukromých zákazníků je zejména účelný poplatek maximálně několika set DM, pro použití u velkých zákazníků se navrhují podstatně vyšší poplatky. Obnos v řádu přibližně DM 500,- se hodí jak pro náročné soukromé domácnosti tak i pro příslušníky svobodných povolání a menší podniky. Hodnota uložená v peněžence by neměla přednostně systematicky překračovat dvojnásobnou hodnotu cenného obnosu.

Špatně frankované zásilky

Špatně frankované a nevhodné k přepravě, již potištěná psaní, obálky atd. s platným záznamem o frankování se dobropisují zákazníkovi.

Vhodnými opatřeními, například razítkováním zásilek, přijímaných v dopisovém středisku, se nechá zjistit, zda zásilka již byla dopravena. Tím se zamezuje, aby zákazníci dostali zpět od příjemce již dopravené zásilky a tyto podávali k dobropisování u provozovatele poštovní služby, například Deutsche Post AG.

Vrácení na centrální místo poskytovatele zasílací služby, například Deutsche Post, umožňuje vysokou míru zajištění odměny pomocí kompenzace dat se zúčtovacími obnosy

a znalost o nejčastějších důvodech zasílání. Tím existuje popřípadě možnost dodatečného řízení změnou dovažecích předpokladů s cílem redukování kvóty vracení.

Platnost hodnot frankování

Zákazníky koupené hodnoty zúčtování jsou z důvodů zajištění finanční úhrady platné například jen 3 měsíce. Příslušné upozornění je třeba zaznamenat v dohodě se zákazníkem. Aby se hodnoty frankování nemusely spotřebovat do 3 měsíců, musí se zákaznickým systémem zahájit kontaktování střediska přenosu hodnoty k nové výrobě záznamů o frankování. U tohoto kontaktování se, jako u řádného zavádění zúčtovaných obnosů, přiřazuje zbytkový obnos starého zúčtovaného obnosu nově vydávanému zúčtovacímu obnosu a pod novým identifikačním číslem procesu zavádění se dává k dispozici zákazníkovi.

Zvláštní provozní úpravy

Záznamy o frankování mohou v zásadě mít libovolný tvar, ve kterém se mohou reprodukovat v nich obsažené informace. Je ale účelné, vytvářet záznamy o frankování tak, že mají alespoň částečně tvar čárových kódů. U znázorněného řešení 2D-čárového kódu a z něho vyplývajícího zajištění finanční úhrady je třeba v produkci zohlednit následující zvláštnosti:

PC-frankované zásilky se mohou doručovat pomocí všech možností doručování, také přes dopisní schránky.

Stanovením předpokladů pro povolení pro výrobce součástí systému frankování, relevantních pro rozhraní,

zejména pro výrobce a/nebo provozovatele zákaznických systémů, se dále zvyšuje dodržování znázorněných bezpečnostních opatření.

Nadřazené normy, standardy a úkoly International Postage Meter Approval Requirements (IPMAR).

Přednostně nalézají předpisy nejaktuálnějšího vydání dokumentu International Postage Meter Approval Requirements (IPMAR), UPU S-30, rovněž použití pro všechny normy a standardy, ke kterým se odkazuje v tomto dokumentu. Dodržení všech tam uvedených „Requirements" je, pokud možno, pro zákaznický systém smysluplné.

Digital Postage Marks: Applications, Security & Design

V zásadě nacházejí předpisy aktuálního vydání dokumentu Digital Postage Marks: Applications, Security & Design (UPU: Technical Standards Manual) rovněž použití jako všechny normy a standardy, ke kterým se odkazuje v tomto dokumentu. Dodržení „normativního" obsahu jakož i široké respektování „informativního" obsahu tohoto dokumentu je, pokud možno, pro zákaznický systém smysluplné.

Přednostně nacházejí rovněž použití úpravy a ustanovení podniku poskytujícího zasílatelské služby.

Povolením jenom takových systémů, které rovněž splňují všechna zákonná ustanovení jako všechny normy a standardy poskytovatele zasílatelských služeb, se rovněž zaručuje bezpečnost dat a spolehlivost systému jako jeho uživatelská přívětivost.

Další zákony, směrnice, předpisy normy a standardy.

V zásadě nacházejí použití všechny zákony, vyhlášky, směrnice, předpisy, normy a standardy právě platného znění, kterých je třeba dbát k vývoji a k provozu technického zákaznického systému v konkrétním případě.

Systémově technická interoperabilita

Systémově technická interoperabilita se vztahuje na funkčnost rozhraní zákaznického systému, popřípadě na dodržení úkolů, specifikovaných v popisech rozhraní.

Rozhraní Zúčtovaný obnos
Komunikační cesta, protokoly

Komunikace přes rozhraní Zúčtovaný obnos se přednostně uskutečňuje přes veřejný internet na bázi protokolů TCP/IP a HTTP. Výměna dat se může volitelně kódovat pomocí HTTP přes SSL (https). Zde je znázorněn požadovaný proces požadovaného přenosu.

Výměna dat se uskutečňuje přednostně, pokud je možné, přes HTML- a XML- kódované databáze. Textové a grafické obsahy HTML-stránek je možné znázornit v zákaznickém systému.

Je účelné, sahat u komunikačních stránek po osvědčené HTML-verzi a zříci se použití Frames, vložených objektů (Applets, ActiveX atd) a popř. animovaných GIFs.

Přihlášení k zavádění zúčtovaného obnosu (první přenos od bezpečnostního modulu ke středisku přenosu hodnoty)

V rámci prvního přenosu od bezpečnostního modulu ke středisku přenosu hodnoty se certifikát bezpečnostního modulu jakož i indikátor A akce přenášejí nekódovaně a nesignovaně.

Zpětné hlášení k přihlášení (první odpověď od střediska přenosu hodnoty k bezpečnostnímu modulu)

Zpětné hlášení střediska přenosu hodnoty obsahuje vlastní certifikát střediska přenosu hodnoty, kódovaný kód relace a digitální signaturu kódovaného kódu relace.

Druhý přenos od bezpečnostního modulu ke středisku přenosu hodnoty

V rámci tohoto přenosu vysílá bezpečnostní modul nově kódovaný kód relace a kódovaný záznam s užitečnými daty (výše předem zavedeného zúčtovaného obnosu, zbývající hodnota aktuálního zúčtovaného obnosu, vzestupný registr všech zúčtovaných obnosů, poslední identifikační číslo procesu zavádění) na středisko přenosu hodnoty (všechno symetricky kódované veřejným kódem střediska přenosu hodnoty). Bezpečnostní modul zároveň vysílá digitální signaturu těchto kódovaných dat na středisko přenosu hodnoty. Zákaznický systém zároveň může posílat další, nezakódované a nesignované protokoly využití nebo profily využití na středisko přenosu hodnoty.

Je účelné, že data využití se zanášejí do protokolu využití a že protokol využití a/nebo v něm zaznamenané zápisy se digitálně signují.

Druhá odpověď střediska přenosu hodnoty bezpečnostnímu modulu

Středisko přenosu hodnoty předává symetricky kódované náhodné číslo a symetricky kódované identifikační číslo procesu zavádění na bezpečnostní modul. Středisko přenosu hodnoty mimoto předává identifikační číslo procesu zavádění, zhotovené veřejným kódem bezpečnostního modulu, vytvořené náhodné číslo, Login-informace pro bezpečnostní modul jakož i nový kód relace na bezpečnostní modul. Celková přenášená data se přitom digitálně signují.

Třetí přenos od bezpečnostního modulu ke středisku přenosu hodnoty

V rámci třetího přenosu se od bezpečnostního modulu přenášejí nový kód relace, nové identifikační číslo procesu zavádění spolu s užitečnými daty k potvrzení úspěšné komunikace všech vespolek v kódovaném a digitálně signovaném tvaru na středisko přenosu hodnoty.

Třetí odpověď střediska přenosu hodnoty na bezpečnostní modul

U třetí odpovědi potvrzuje středisko přenosu hodnoty úspěch přenosu bez použití kryptografického způsobu.

Deinstalace

Možnost deinstalace zákaznického systému musí být možná prostřednictvím zákazníka.

Detailní technický popis rozhraní Zúčtovaný obnos se uskutečňuje s koncepcí poště vlastního střediska přenosu hodnoty.

Protokol využití a profil využití

V zákaznickém systému je v rámci každého vytvoření záznamu o frankování třeba vytvořit zápis protokolu, který by měl obsahovat všechny údaje příslušného záznamu o frankování - opatřené digitální signaturou. V protokolu by se měl dále každý chybový status bezpečnostního modulu zaznamenat takovým způsobem, že se manuální mazání tohoto záznamu zpozoruje při kontrole.

Profil využití obsahuje připravené shrnutí dat využití od poslední komunikace se střediskem přenosu hodnoty.

Pokud je zákaznický systém rozdělen na komponentu, nacházející se u zákazníka a na centrální (např. nacházející se v internetu) komponentu, měl by být uživatelský profil přednostně veden v centrální komponentě.

Rozhraní Záznam o frankování
Součásti a vyjádření

Zákaznický systém musí být s to, vytvářet PC-záznamy o frankování, které exaktně odpovídají úkolům Deutsche Post, popřípadě rámci běžných CEN- a CPU-standardů.

PC-záznamy o frankování se přednostně sestávají z následujících tří členů:

- 2-dimenzionálního čárového kódu, barkódu nebo

matrixkódu, ve kterém jsou znázorněné, specifické pro zásilku, informace ve strojově čitelném tvaru. (Účel: automatizace ve výrobě a zajištění finanční úhrady Deutsche Post).

- Textu v nezakódovaném písmu, který reprodukuje důležité části informace čárového kódu v čitelném tvaru. (Účel: kontrolní možnost pro zákazníky jakož i ve výrobě a zajištění finanční úhrady Deutsche Post.)

- Znaku, jako například poštovní trubka, charakterizujícího poskytovatele zasílatelských služeb, například Deutsche Post.

Specifikace datového obsahu

Čárový kód a nezakódované písmo PC-záznamu o frankování obsahují účelným způsobem následující informace:

		v barkódu	v nekódovaném textu	poznámka
1	poštovní podnik (Licensing Post Identifier)	ano	ne	
2	způsob frankování (Licensing Plate Type)	ano	ne	
3	verze a verze ceny/produkty	ano	ne	
4	číslo licence ze Safe-Box-ID (PSD Identifier)	ano	ano	v nekódovaném textu:prvních 5 byte Safe-Box-ID v hexadecimálním znázornění
5	průběžné číslo zásilky (Message Identifier)	ano	ne	vztaženo na Safe-Box
6	Key-indikátor fáze	ano	ne	
7	CryptoString	ano	ne	
8	kód produktu	ano	ne	

9	finanční úhrada	ano	ano	nekódovaný text v ASCII
10	datum frankování	ano	ano	nekódovaný text v ASCII
11	PSČ příjemce	ano	ne	
12	ulice/poštovní schránka příjemce	ano	ne	první a poslední tři místa adresy
13	Truncated transformační hodnota	ano	ne	

Tabulka: obsah PC-záznamu o frankování

Popisuje se zde jenom obsah záznamu o frankování. Předpisy poskytovatele zasílatelských služeb pro obsah adresových údajů si ponechávají neměně svou platnost.

Specifikace fyzikálních vyjádření na papíru (Layout)

Záznam o frankování je přednostně uspořádán v adresovém poli zarovnaný zleva nad adresou na zásilce.

Adresové pole se specifikuje v právě platném vydání norem poskytovatele zasílatelských služeb. Tak se umožňují zejména následující frankování:

- Tisk na dopisní obálku,
- Tisk na nálepkové etikety nebo
- Použití dopisních obálek s okénkem takovým způsobem, že tisk na dopis je plně viditelný skrz okénko.

Pro jednotlivé členy záznamu o frankování platí přednostně:

- Používá se nejdříve čárový kód typu Data Matrix, jehož jednotlivé obrazové body mají mít délku hrany alespoň 0,5 milimetru. Vzhledem na čtenářsky technické předpoklady by se měl přednostně používat 2D-barkód na způsob Data Matrix

s minimální velikostí pixelů 0,5 mm. Popř. účelná možnost spočívá v tom, redukovat velikost pixelů na 0,3 mm.

U velikosti znázornění 0,5 mm na pixel dostáváme délku hrany celého barkódu od cca. 18 do 20 mm, když všechna data přicházejí jak popsáno. V případě, že se podaří, číst v ALM barkódy s velikostí pixelu od 0,3 mm, nechá se délka hrany redukovat na cca. 13 mm.

Dodatečné rozšíření specifikací na použití jiného barkódu (např. Aztec) při stejných obsazích dat.

Přednostní provedení Layout a polohování jednotlivých členů záznamu o frankování je v dalším příkladně znázorněno na obr. 5.

„Nejkritičtější" velikostí je výška znázorněného okénka dopisní obálky s okénkem s velikostí 45x90 mm. Zde se znázorňuje DataMatrix-Code s délkou hrany cca. 13 mm, který je při použití navržených datových polí možný jen při rozlišení pixelu 0,3 mm. Kód s délkou hrany 24 mm nenechává s ohledem k výšce, která je k dispozici, dostatečný prostor pro údaje k adrese.

Kvalita tisku a čitelnost

Odpovědni za bezchybný tisk záznamu o frankování jsou výrobce zákaznického systému v rámci schvalovacího postupu jakož i zákazník v pozdějším provozu. K tomu je zákazník odkazován vhodnými upozorněními v uživatelské příručce a v systému nápovědy. Toto platí zejména pro řádné přilnutí etiket a zamezení sklouznutí (částí) záznamu o frankování vně viditelné oblasti dopisních obálek s okénkem.

Strojová čitelnost záznamů o frankování závisí na použitém rozlišení tisku a na kontrastu. Pokud se mají místo černé používat i jiné barvy, je třeba počítat s menší rychlostí čtení. Je třeba vycházet z toho, že požadovaná rychlost čtení se může u rozlišení 300 dpi („dots per inch") použitém v tiskárně zaručovat při vysokém kontrastu tisku. To odpovídá přibližně 120 obrazovým bodům na centimetr.

Testovací tisky

Zákaznický systém musí být s to, produkovat záznamy o frankování, které odpovídají ve formování a velikosti platným záznamům o frankování, ale nejsou určené pro zasílání, nýbrž slouží pro kontrolní výtisky a jemné nastavování tiskárny.

Zákaznický systém je přednostně vytvořen tak, že testovací tisky se od skutečných záznamů odlišují způsobem, rozpoznatelným pro zasílatelský podnik. K tomu se například ve středu záznamu o frankování umisťuje nápis „VZOREK-nezasílat". Alespoň dvě třetiny barkódu se mají pomocí nápisu nebo jinak dělat nepoznatelnými.

Vedle pravých (zaplacených) záznamů o frankování se mimo zvlášť označených testovacích tisků nesmějí vyrábět žádné bezplatné tisky.

Požadavky na zákaznický systém; základní systém; přehled a funkčnost:

Základní systém slouží jako vazební člen mezi ostatními složkami PC-frankování, jmenovitě střediskem přenosu

hodnoty, bezpečnostním modulem, tiskárnou a zákazníkem. Skládá se z jednoho nebo několika počítačových systémů, například PC, které popř. mohou také být spolu spojené pomocí sítě.

Základní systém zajišťuje také komfortní používání celkového systému zákazníky.

Požadavky na konstrukci a bezpečnost:

Základní systém disponuje přednostně čtyřmi rozhraními:

1. Přes popsané rozhraní Zúčtovaný obnos se uskutečňuje komunikace se střediskem přenosu hodnoty.

2. Přes rozhraní k bezpečnostnímu modulu se vyměňují všechny informace, se kterými se musí seznamovat bezpečnostní modul (zúčtovaný obnos, popřípadě identifikační číslo procesu zavádění, pro zásilku specifická data k jednotlivým frankováním). Přes tato rozhraní se mimoto vyměňují všechna data s bezpečnostním modulem (kryptograficky zpracovávaná data).

3. Přes rozhraní k tiskárně se tato ovládá.

4. Přes rozhraní k uživateli, popřípadě zákazníkovi (Graphical User Interface, GUI), musí tento zařídit všechny relevantní procesy v interakci s největší možnou ergonomií.

V základním systému by se měla mimoto ukládat a zpracovávat následující data:

- nastavení/data specifická pro uživatele,

- detailní protokoly využití a profily využití,
- při použití SSL: výměnné certifikáty, se kterými se může verifikovat platnost SSL-certifikátů a
- všechny relevantní informace o produktech a cenách poskytovatele zasílatelských služeb.

Rozsah funkcí a průběhy

Základní systém podporuje přednostně následující průběhy:

- první instalace s pomocí uživatele,
- identifikace uživatele, zejména vzhledem k bezpečnostnímu modulu; popřípadě s rozdílnými oprávněními pro zavádění zúčtovaných obnosů a výrobu záznamů o frankování,
- popřípadě administrace několika uživatelů,
- podpora uživatele při zavádění zúčtovaných obnosů (přitom podpora reprodukování informací, které se posílají od střediska přenosu hodnoty na způsob HTML-kódovaných souborů),
- podpora uživatele při výskytu problémů při zavádění zúčtovaných obnosů,
- pro uživatele transparentní správa cenného obnosu (přehled o kontu),
- správa protokolů využití, příprava profilů využití a přenos protokolů využití nebo profilů využití,
- podpora uživatele při vytvoření a při tisku záznamu o frankování (znázornění vzor záznamu o frankování, který chceme tisknout, na obrazovce - WYSIWYG),
- platnost zajištěná výpočtem finanční odměny podle Service-Information Deutsche Post,
- elektronický systém nápovědy,
- automatická aktualizace relevantních informací o

produktech a cenách Deutsche Post při změnách jakož i informace zákazníka o existující a ukončené aktualizaci,

- technické podchycení vícenásobného tisku jednoho a toho samého záznamu o frankování a
- deinstalace zákaznického systému.

Bezpečnostní modul

Úkol a bezpečnostní úroveň

Bezpečnostní modul zaručuje jako „kryptografický modul" ve smyslu FIPS PUB 140, Security Requirements for Cryptographic Modules, vlastní bezpečnost zákaznického systému. Skládá se z hardware, software, firmware nebo kombinace z nich a přechovává kryptografickou logiku a kryptografické procesy, to znamená, správu a použití kryptografických způsobů jakož i vůči manipulaci bezpečné uložení cenného obnosu. Požadavky, kterým musí postačovat bezpečnostní modul, se

- vzhledem k bezpečnostním standardům definují pomocí vhodných norem, jako například FIPS PUB 140 a
- vzhledem k dodržování poštovních standardů se UPU-publikováním „International Postage Meter Approval Requirements (IPMAR)", opírajícím se o FIPS PUB 140.

K zavedení a k provozu v zákaznickém systému se musí bezpečnostní modul v rámci zaváděcího způsobu příslušně certifikovat jako kryptografický modul podle FIPS PUB 140 - přednostně podle bezpečnostního stupně 3 (Security Level 3)

Procesy bezpečnostního modulu

Bezpečnostní modul by měl přednostně k inicializaci a ke komunikaci se střediskem přenosu hodnoty a deaktivaci podporovat vedle běžných operací v podstatě následující procesy, které se detailně popisují v zadní části dodatku Technický popis zákaznického systému:

- vytvoření kódu
- výdej veřejného kódu
- uložení certifikátu
- vytvoření signatury
- kontrola signatury
- kontrola certifikátu
- dočasné uložení certifikátu
- asymetrické kódování
- asymetrické dekódování
- vytvoření náhodného čísla
- uložení kódu relace
- uložení dvou identifikačních čísel procesu zavádění
- uložení aktuální hodnoty registru zúčtovaných obnosů
- uložení rostoucí hodnoty registru
- identifikace uživatele
- vydání statusu platnosti zúčtovaných obnosů
- vydání statusu hodnoty registru zúčtovaných obnosů
- transformační tvorba dat specifických pro zásilku
- zmenšení hodnot registru zavedených zúčtovaných obnosů
- zaprotokolování chyb
- samočinný test
- deaktivování

Testovací tisky

Bezpečnostní modul se nepoužívá při testovacím tisku a proto se také nekontaktuje.

Tiskárna

Tiskárna může podle pravidla výrobce zákaznického systému být buď na trhu běžná standardní tiskárna nebo speciální tiskárna.

Velká většina dnešních laserových a inkoustových tiskáren by měla být principiálně vhodná pro PC-frankování. Doporučují se tiskárny s rozlišením alespoň 300 dpi (dots per inch).

Procesy uvnitř zákaznického systému

Průběh vytváření záznamů o frankování

Pomocí zákaznického systému zákazník provádí následující dílčí procesy při vytváření záznamů o frankování:

- Výstavba spojení k bezpečnostnímu modulu: přes základní systém se vytváří spojení k bezpečnostnímu modulu.
- Identifikace uživatele: uživatel se identifikuje heslem/PIN osobně u bezpečnostního modulu a tím ho aktivuje.
- Zadávání pro zásilku specifických informací: zákazník zadává, s podporou zákaznického systému, potřebné informace, specifické pro zásilku, do základního systému, který předává podstatná data na bezpečnostní modul.
- Vytvoření záznamu o frankování: základní systém vytváří z dat, specifických pro zásilku, a z kryptograficky zpracovaných dat z bezpečnostního modulu záznam o frankování.
- Protokolování zhotovení záznamů o frankování: každý úspěšný zpětný přenos se zachovává v protokolu využití

základního systému. Při rozdělení zákaznického systému do lokální složky u zákazníka a do centrální složky (např. v internetu) je protokol využití třeba vést v centrální složce.

- Zrušení komunikačního vztahu: pokud byly všechny požadované záznamy o frankování zhotovené, komunikační vztah se opět ruší. Při obnoveném zhotovení záznamů o frankování je třeba - jak je popsáno nahoře - provést identifikaci uživatele.

- Testovací tisky: Alternativně k tomuto postupu je možné, nechat vedení uživatele pokročit tak daleko, že vzor záznamu o frankování může být znázorněn nejenom na obrazovce (WYSIWYG) ale i vytištěn jako (neplatný) testovací tisk. Teprve v pozdějším stadiu by se přitom uskutečnil nahoře uvedený proces integrace bezpečnostního modulu.

Nasazení technického systému se kryje pomocí účelných organizačních opatření, takže se pozoruje technicky registrovatelné vícenásobné zaslání záznamu o frankování jakož i přestupek vůči obchodním podmínkám zasilatele.

Dále je výhodné, navrhnout vhodné technické parametry pro vytisknutí záznamů o frankování, zejména vzhledem ke kvalitě tisku, aby se záznamy o frankování mohly lépe evidovat v automatických evidenčních zařízeních.

Pro kontrolu systémů se mohou brát za základ vhodné systémy zabezpečení kvality, zejména podle norem ISO 9001.

Zastupuje:

Dr. Miloš Všetečka v.r.

advokát
120 00 Praha 2, Hálkova 2

PATENTOVÉ NÁROKY

1. Způsob opatřování poštovních zásilek záznamy o frankování s následujícími znaky:

- zákaznický systém zavádí od střediska přenosu hodnoty přes datové vedení poplatek,
- v zákaznickém systému se jednoznačné identifikační číslo zákaznického systému kóduje tak, že středisko přenosu hodnoty je může dekódovat a přenášet,
- kódované identifikační číslo se přenáší od zákaznického systému na středisko přenosu hodnoty,
- středisko přenosu hodnoty vytváří data neznámá zákaznickému systému,
- středisko přenosu hodnoty definuje identifikační číslo,
- středisko přenosu hodnoty kóduje následovně data neznámá zákaznickému systému kódem, zákaznickému systému neznámým, ale známým kontrolnímu středisku,

vyznačující se tím, že

- ve středisku přenosu hodnoty se tato data mimo jiné kódují kódem známým zákaznickému středisku,
- že středisko přenosu hodnoty data následovně přenáší na zákaznický systém,
- že bezpečnostní modul zákaznického systému data, neznámá zákaznickému systému, dekóduje a ukládá,
- že zákaznický systém řídí tisk záznamů o frankování na poštovních zásilkách, přičemž do záznamů o frankování se integrují data bezpečnostního modulu, neznámá zákaznickému systému, která se mohou dekódovat v kontrolním středisku.

2. Způsob podle nároku 1, ***vyznačující se tím***,

že data neznámá zákaznickému systému se vytvářejí jako náhodné číslo ve středisku přenosu hodnoty a následně se kódují.

3. Způsob podle nároku 2, ***vyznačující se tím***, že náhodné číslo se vytváří v bezpečné oblasti střediska přenosu hodnoty.

4. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že náhodné číslo se kóduje veřejným kódem.

5. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že středisko přenosu hodnoty signuje data privátním kódem.

6. Způsob podle nároku 5, ***vyznačující se tím***, že privátní kód je uložen v bezpečnostním modulu střediska přenosu hodnoty.

7. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že data se s každým požadavkem poplatku přenášejí od zákaznického systému na středisko přenosu hodnoty.

8. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že středisko přenosu hodnoty identifikuje podle přenášených dat zákaznický systém.

9. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že část dat, dekódovatelná zákaznickým systémem, obsahuje informace o

identitě zákaznického systému.

10. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že část dat, dekódovatelná v zákaznickém systému, obsahuje náhodné číslo, tvořené ve středisku přenosu hodnoty.

11. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že podíl dat, dekódovatelný zákaznickým systémem, obsahuje informace o výši poplatku.

12. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že při každém přenosu dat od střediska přenosu hodnoty k zákaznickému systému se přenáší obnos, který postačuje ke zhotovení několika záznamů o frankování.

13. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že ve středisku přenosu hodnoty se vytváří transformační hodnota.

14. Způsob podle nároku 13, ***vyznačující se tím***, že transformační hodnota se vytváří při zahrnutí údajů o datech zásilky.

15. Způsob podle jednoho nebo více z nároků 13 nebo 14, ***vyznačující se tím***, že transformační hodnota se vytváří při zahrnutí přijatého a přechodně uloženého náhodného čísla.

16. Způsob podle jednoho nebo více z nároků 13 až 15, ***vyznačující se tím***, že transformační hodnota se

vytváří při zahrnutí [illegible] čísla [illegible] zavádění.

17. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že záznam o frankování obsahuje informace o datech zásilky.

18. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že záznam o frankování obsahuje jak informace, přenášené od střediska přenosu hodnoty, tak i data zadávaná uživatelem zákaznického systému.

19. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že záznam o frankování obsahuje transformační hodnotu, která se tvoří kombinací hodnoty přenášené od střediska zadávání a hodnoty zadávané zhotovitelem dokumentu.

20. Způsob podle jednoho nebo více z nároků 2 až 19, ***vyznačující se tím***, že středisko přenosu hodnoty obsahuje identifikační číslo zavádění, které je přiřazeno poplatku.

21. Způsob podle nároku 20, ***vyznačující se tím***, že při vytvoření identifikačního čísla zavádění vytvořené náhodné číslo zaniká.

22. Způsob podle nároku 20 nebo 21, ***vyznačující se tím***, že identifikační číslo zavádění se přenáší na bezpečnostní modul zákaznického systému.

23. Způsob podle nároku 22, ***vyznačující se tím***, že v bezpečnostním modulu se z identifikačního čísla

zaváděné z dalších dat vytváří transformační hodnota.

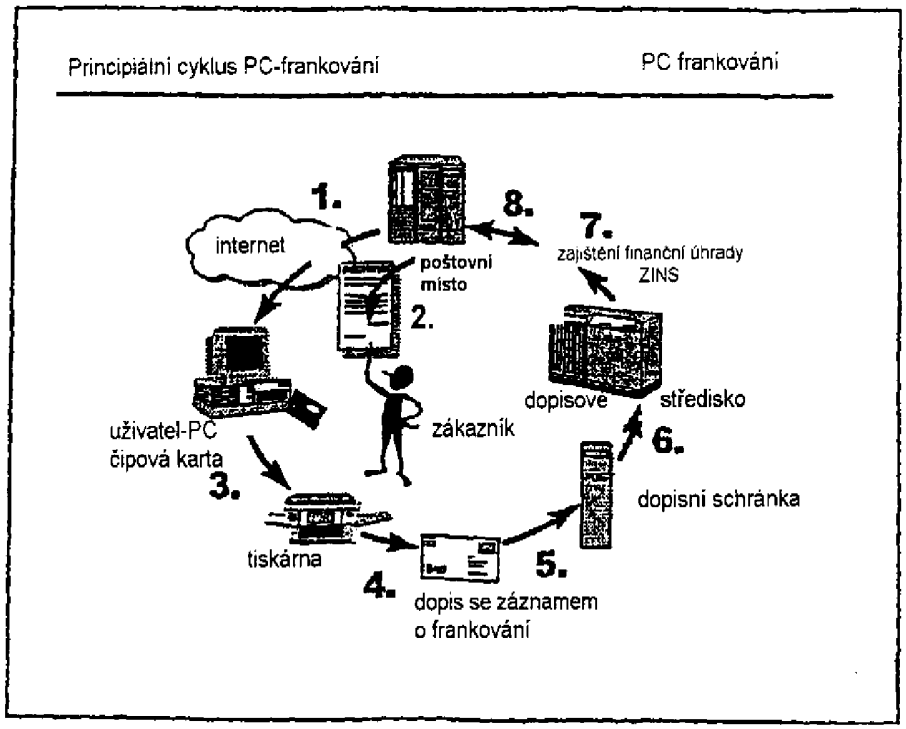
24. Způsob podle nároku 23, ***vyznačující se tím***, že záznam o frankování se vytváří tak, že obsahuje transformační hodnotu.

25. Způsob podle jednoho nebo více z předcházejících nároků, ***vyznačující se tím***, že platnost záznamů o frankování se kontroluje v dopisovém středisku.

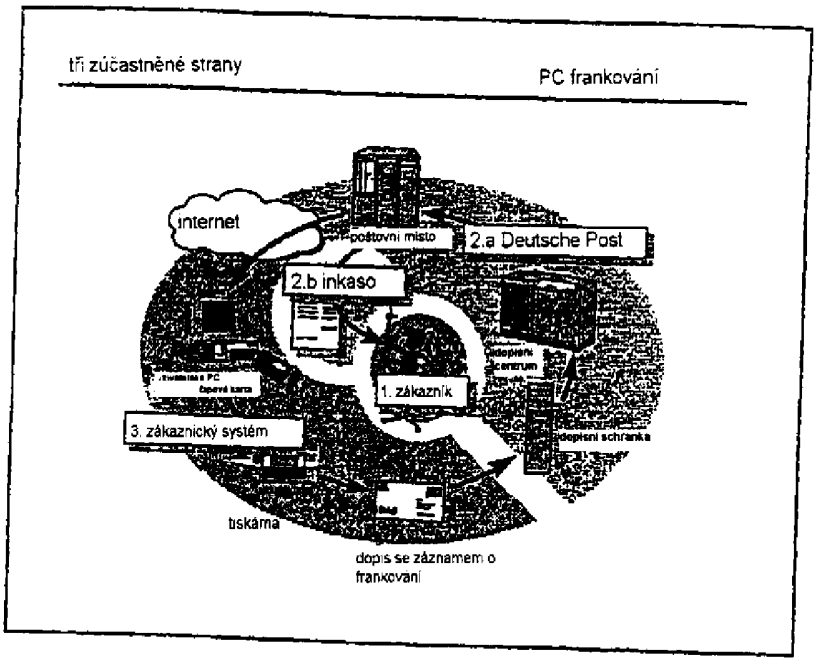
26. Způsob podle nároku 25, ***vyznačující se tím***, že kontrola v dopisovém středisku se uskutečňuje analýzou dat, obsažených v záznamu o frankování.

27. Způsob podle jednoho nebo více z nároků 25 nebo 26, ***vyznačující se tím***, že kontrolní místo dopisového střediska z dat, obsažených v záznamu o frankování, tvoří transformační hodnotu a kontroluje, zda se tato transformační hodnota shoduje s transformační hodnotou obsaženou v záznamu o frankování a v případě neshody registruje transformační hodnotu jako padělanou.

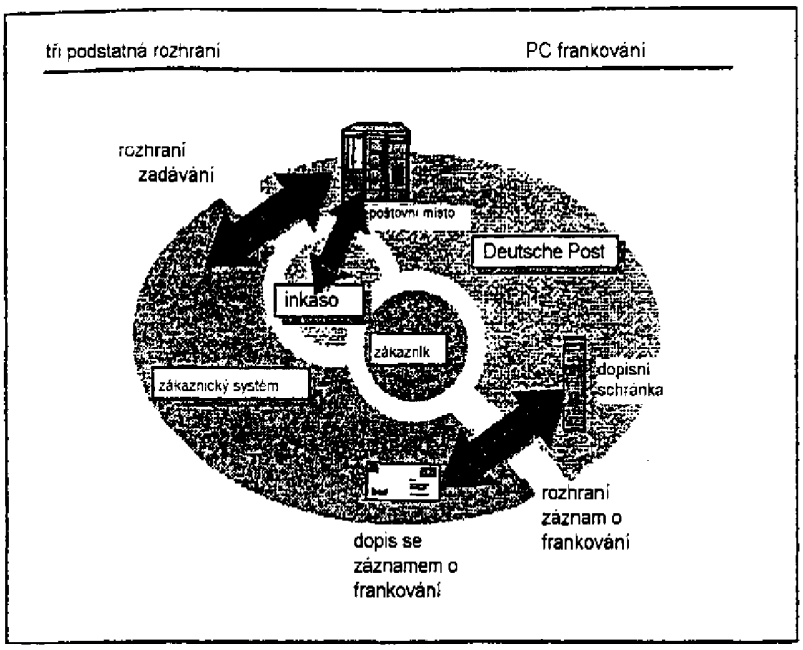
Zastupuje:
Dr. Miloš Všetečka v.r.


Principiální cyklus PC-frankování
PC frankování
1.
8.
7.
internet
poštovní místo
zajištění finanční úhrady ZINS
2.
dopisove
středisko
uživatel-PC
čipová karta
zákazník
6.
3.
dopisní schránka
tiskárna
4.
5.
dopis se záznamem o frankování

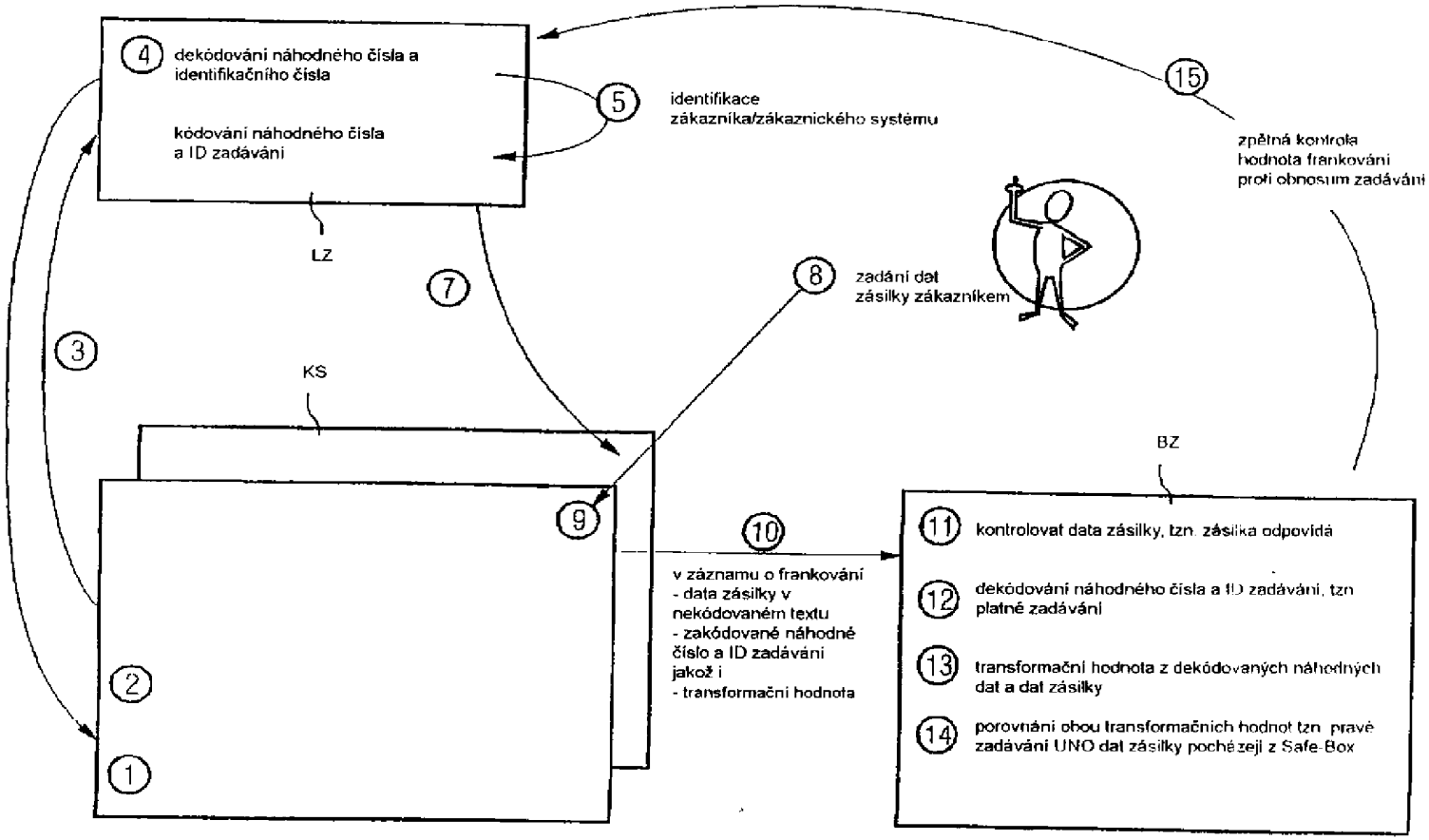
obr. 1


tři zúčastněné strany
PC frankování
internet
poštovní místo
2.a Deutsche Post
2.b inkaso
1. zákazník
3. zákaznický systém
tiskárna
dopis se záznamem o frankování

obr. 2


tři podstatná rozhraní
PC frankování
rozhraní
zadávání
poštovní místo
Deutsche Post
inkaso
zákazník
zákaznický systém
dopisní
schránka
rozhraní
záznam o
frankování
dopis se
záznamem o
frankování

obr. 3


4 dekódování náhodného čísla a identifikačního čísla
kódování náhodného čísla a ID zadávání
5 identifikace zákazníka/zákaznického systému
15 zpětná kontrola hodnota frankování proti obnosům zadávání
LZ
7
8 zadání dat zásilky zákazníkem
3
KS
BZ
9
10
v záznamu o frankování
- data zásilky v nekódovaném textu
- zakódované náhodné číslo a ID zadávání
jakož i
- transformační hodnota
11 kontrolovat data zásilky, tzn. zásilka odpovídá
12 dekódování náhodného čísla a ID zadávání, tzn platné zadávání
13 transformační hodnota z dekódovaných náhodných dat a dat zásilky
14 porovnání obou transformačních hodnot tzn. pravé zadávání UNO dat zásilky pochézejí z Safe-Box
2
1

obr. 4