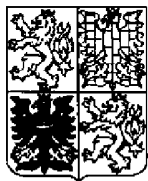


PŘIHLÁŠKA VYNÁLEZU

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

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **16.11.1998**

(32) Datum podání prioritní přihlášky: **20.11.1997**

(31) Číslo prioritní přihlášky: **1997/9714578**

(33) Země priority: **FR**

(40) Datum zveřejnění přihlášky vynálezu: **13.09.2000**
(Věstník č. 9/2000)

(86) PCT číslo: **PCT/FR98/02431**

(87) PCT číslo zveřejnění: **WO99/27505**

(21) Číslo dokumentu:

2000 - 1833

(13) Druh dokumentu: **A3**

(51) Int. Cl. ?

G 07 F 7/10

G 06 K 7/06

(71) Přihlašovatel:

NONNEMACHER, BERNARD, GEMPLUS S. C. A.,
Gémenos Cedex, FR;

(72) Původce:

Beaujard Olivier, Neuilly, FR;
Imbert Patrick, Marseille, FR;

(74) Zástupce:

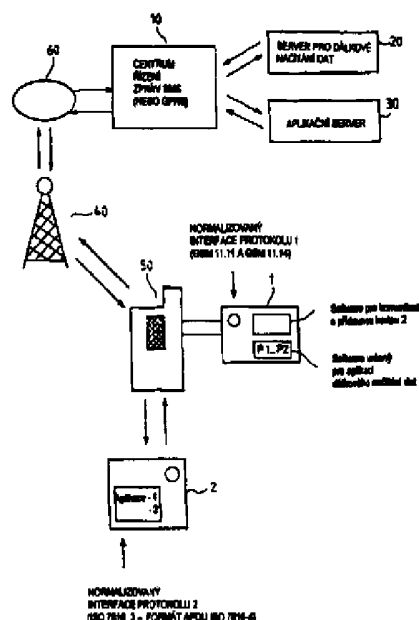
Holas Antonín Ing., Křižová 4, Brno, 60300;

(54) Název přihlášky vynálezu:

**Způsob, čipová karta a terminály pro provádění
transakcí přes telekomunikační síť**

(57) Anotace:

Řešení se týká způsobu pro provádění transakcí přes telekomunikační síť (60) s pomocí čipových karet (1, 2) a telekomunikačních terminálů (50) vybavených přinejmenším dvěma interface ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta (1), určenou k telefonii, druhým pro vkládání přídatné čipové karty (2), určené k jednomu či více užití jinému než telefonickému. Řešení je charakteristické tím, že prostředky pro komunikaci jsou vkládány do identifikační karty abonenta, aby pilotovaly aplikační katru (2) přes telekomunikační terminál (50).



Způsob, čipová karta a terminály pro provádění transakcí přes telekomunikační síť

Vynález se týká způsobu pro provádění transakcí přes telekomunikační síť pomocí čipové karty a telekomunikačních terminálů.

Zároveň se týká čipových karet a terminálů umožňujících uvedení výše uvedeného způsobu do provozu.

Najde četné využití v peněžních transakcích, v používání elektronických peněženek a transakcích spojených se zdravotní péčí či sázkovými hrami.

Dotyčné telekomunikační sítě jsou způsobilé být využívány telefonními abonenty ke styku s jinými účastníky telefonní sítě či k přístupu k různým službám.

Z těchto sítí můžeme jmenovat například telefonní síť, komutovanou síť nebo integrovanou síť komunikačních služeb a síť mobilních telefonů.

Nová generace telekomunikačních terminálů předpokládá, že tyto budou vybaveny dvěma interfaci ke čtení čipových karet, jeden ke komunikaci s identifikační čipovou kartou abonenta určenou k telefonii typu například SIM karty (Subscriber Identity Module) v případě systému mobilní telekomunikace a druhý pro čipovou kartu (aplikační kartu) sloužící k jednomu či více použití jinému než telekomunikačnímu. Mohlo by se jednat například o kartu elektronické peněženky.

Čipové karty sloužící k jednomu či více použití jinému než telekomunikačnímu mohou být vydávány zcela nezávislými operátory a komunikace s aplikačními kartami je navazována na základě rozdílných protokolů.

Z předchozího se jeví nezbytným, aby tato nová generace telekomunikačních terminálů podporovala sady aplikačního ovládání různých typů těchto užitkových karet (s použitím například jako bankovní či věrnostní karta).

Výše uvedené skutečnosti jsou velmi závazné pro poskytovatele služeb, kteří se z těchto důvodů budou muset spojovat s výrobcí těchto terminálů, aby je mohli svým klientům nabízet k používání.

Toto navíc implikuje nutnost určité limitace v nabídce užitečných karet použitelných v daném telekomunikačním terminálu na ty, které budou původně k tomuto určeny, v opačných případech by bylo nutno měnit terminálové softwary.

Tento vynález umožňuje zdárné vyřešení všech těchto problémů.

Vynález sleduje jako hlavní cíl to, aby nebyly dále přetěžovány logické komunikační interfaci terminálu, ale aby tyto zároveň mohli akceptovat jakoukoliv užitečnou kartu a to tak, že vkládá komunikační prostředky do každé identifikační karty abonenta určené k telefonii tak, aby abonentovi bylo umožněno používat jakoukoliv užitečnou kartu přes telekomunikační terminál.

Vynález se týká obzvláště způsobu pro provádění transakcí přes telekomunikační síť s použitím čipových karet a telekomunikačních terminálů pro vstup na síť vybavených přinejmenším dvěma interfaci ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta určenou k telefonii, druhým pro vkládání přídatné čipové karty určené k jednomu či více použití jinému než telekomunikačnímu výše uvedenému, jehož podstata je v tom, že identifikační čipová karta abonenta komunikuje s přídatnou kartou přes terminál pomocí sad ovládačů určených k pilotáži výše uvedené přídatné karty, přičemž tyto příkazy jsou předformátovány identifikační kartou abonenta podle formátu komunikačního protokolu přídatné karty a předávány přes terminál podle jeho přenosového protokolu.

Vynález taktéž zahrnuje identifikační telefonickou čipovou kartu abonenta, pojatou tak, že obsahuje prostředky pro komunikaci s přídatnou kartou určenou k jednomu či více



využití jinému než telekomunikačnímu, a to přes telekomunikační terminál vybavený přinejmenším dvěma interfaci ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta určenou k telefonii, druhým pro vkládání přídavné čipové karty, přičemž tyto prostředky zahrnují i sadu příkazů určených k pilotování přídavné karty a s tím, že výše uvedené příkazy jsou předformátovány identifikační kartou abonenta podle formátu (APDU) komunikačního protokolu přídavné karty a předávány přes terminál podle jeho přenosového protokolu.

Vynález zahrnuje taktéž telekomunikační terminál pro vstup na síť vybavený přinejmenším dvěma interfaci ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta určenou k telefonii, druhým pro vkládání přídavné čipové karty určené k jednomu či více použití jinému než telekomunikačnímu, jehož podstata spočívá v tom, že zahrnuje:

- prostředky uzpůsobené k přijímání příkazů vysílaných identifikační kartou abonenta podle přenosového protokolu výše zmíněného terminálu a určené k pilotáži přídavné karty tak, že výše zmíněné příkazy jsou předformátovány identifikační kartou abonenta podle formátu komunikačního protokolu přídavné karty,
- prostředky k předávání v rámci těchto příkazů příkazů „zaslání příkazu vstup/výstup karta 2“ předformátované přídavné kartě,
- prostředky k vykonání v rámci těchto příkazů příkazů „Zapnuta/vypnuta karta 2“,
- prostředky pro vyslání příkazu „karta 2 přítomna“ identifikační kartě abonenta.

Ostatní zvláštnosti a výhody vynálezu vyjdou na zřetel při četbě následujícího popisu, který je přiložen jako ilustrativní a nevyčerpávající příklad vedle obrázků, na kterých je:

- na obrázku 1 schématicky znázorněn celkový pohled na telekomunikační síť pro uplatnění principu vynálezu,
- na obrázku 2 zobrazena více detailněji schématickým způsobem identifikační karta abonenta a přídavná karta,
- na obrázku 3 přiblíženy detailním způsobem výměny mezi jednotlivými prvky systému v případě vstupního či výstupního příkazu v souladu s postupem,
- na obrázku 4 přiblíženy obecnějším způsobem výměny mezi jednotlivými prvky pro všechny příkazy.

Jak již bylo řečeno, princip vynálezu je uplatnitelný na všechny typy telefonních sítí, komutovaných telefonních sítí, ISDN a sítí mobilních telefonů (GSM). Avšak následující popis je určen pro síť mobilní telekomunikace, jejímiž terminály jsou mobilní radiotelefony.

Podle tohoto příkladu ilustrovaném na obrázku 1 systém zahrnuje:

- řídicí centrum 10 zpráv SMS (Short Message Service Center) nebo GPRS (Global Packet Radio Service),
- stahovací server 20 obsahující programy určené k uvedení aplikace do provozu,
- aplikační server 30 : elektronická peněženka, banka, body za věrnost udělované obchodníky,
- síť GSM 60 zahrnující alespoň jeden mobilní terminál 40. Každý terminál umožňuje uživateli připojení se k síti operátora,
- mobilní telefon 50 uživatele. Mobilní telefon se skládá z přijímací antény, baterie, displeje, klávesnice, jednoho nebo více interfaců na karty a mikroprocesoru obsahujícího systémový software.

V uvedeném vynálezu je mobilní telefon vybaven dvěma interfaci na čipové karty.



- identifikační karta abonenta 1 nazývaná SIM karta. Tato karta je umístěna v mobilním telefonu uživatele a umožňuje mu být identifikován operátorem mobilních telefonů.
- přídatná karta 2 nazývaná uživatelská karta, neboť je určena k užití jiného typu nežli je použití SIM karty. Tímto použitím může být využita karta jako elektronické peněženky, banky, karty věrnostních bodů.

Obrázek číslo 2 představuje jednotlivé části obsažené v SIM kartě 1 a v přídatné kartě 2, které jsou nezbytné k uvedení vynálezu do provozu.

SIM karta 1 se skládá z mikroprocesoru, čtecí paměti (ROM), zapisovací paměti (RAM) a paměti typu EEPROM. Čtecí paměť (ROM) a paměť EEPROM obsahují softwary a data umožňující fungování SIM karty. Jedná se zejména o systémový software a o jeden (či více) dálkově zaváděný P1-P2 program, které jsou určeny ke spuštění aplikací přídatnou kartou. Každý program sloužící ke spuštění aplikace obsahuje jednu či více aplikací pro přídatnou kartu. Tyto aplikace korespondují s řízením rozhraní stroj - uživatel, k řízení komunikace s přídatnou kartou a řízení komunikace s aplikačním serverem 30 vázaným na přídatnou kartu.

Komunikační software SIM karty používá sadu příkazů, kterou SIM karta potřebuje ke komunikaci s přídatnou kartou 2 přes terminál.

Tato sada příkazů se skládá z předformátovaných příkazů podle formátu APDU (ISO 7816-4), který je formátem komunikačního protokolu karty číslo 2. Tyto příkazy jsou sestavovány SIM kartou dle přenosového protokolu GSM 11.14 a předávány dle tohoto protokolu terminálem (povel vysílaný SIM kartou jsou čteny terminálem).

Ještě přesněji, SIM karta má čtyři následující příkazy:

- a) – „karta 2 zapnutá“
- b) – „karta 2 vypnutá“
- c) – „vyslání vstupního příkazu do karty 2“
- d) – „vyslání výstupního příkazu do karty 2“

První dva, a) a b) jsou vykonávány terminálem, zbývající dva c) a d) jsou ve formátu APDU sdělovány kartě číslo 2.

Schéma detailněji znázorňující různé výměny je vyobrazeno následně pod obrázkem číslo 3.

Přídatná karta 2 (uživatelská karta) se skládá z mikroprocesoru, čtecí paměti (ROM), zapisovací paměti (RAM) a paměti typu EEPROM. Čtecí paměť (ROM) a paměť EEPROM obsahují softwary a data umožňující fungování této uživatelské karty, zejména systémový software a aplikační softwary (kupříkladu software elektronické peněženky a/nebo software ke správě věrnostních bodů ...).

Terminál, kterým je v tomto případě mobilní telefon, umožňuje zavedení dvou karet. K tomuto účelu obsahuje dva interfacé ke čtení čipových karet. První interface umožňuje vkládání SIM karty, která identifikuje uživatele telefonu na síti, ke které je připojený. Interface/y pro přídatné karty umožňuje uživateli vkládat karty jiných typů (bankovní kartu, věrnostní kartu, zdravotní kartu, ...).

Terminál obsahuje mezi jinými i zde neznázorněné součásti jako mikroprocesor a programovou paměť obsahující systémový software a komunikační software.

Tento komunikační software je schopen dle tohoto vynálezu přijímat pokyny vyslané SIM kartou.

Tento software umožňuje mezi jiným předávat kartě 2 pokyny karta 2 vstup/výstup a to předformátované, to znamená předávat je ve formátu APDU, vykonat příkazy vypnout/zapnout kartu 2 a vyslat pokyn „karta 2 přítomna“ SIM kartě, jakmile mobilní

telefon zjistí přítomnost karty 2 ve svém čtecím zařízení. Toto zjištění může být mechanické či elektrické. Tento pokyn je vyslán SIM kartě v komunikačním protokolu GSM 11.14.

Nyní popíšeme více detailněji dialog mezi jednotlivými částmi systému podle obrázku číslo 3 v případě výstupního nebo vstupního příkazu vyslaného SIM kartou přidavné kartě. Typickým vstupním příkazem je příkaz ke psaní určený kartě 2, kdy tento příkaz je doprovázen daty k zaznamenání.

Výstupním příkazem je typicky příkaz ke čtení udělený kartě 2.

. v I. kroku SIM karta sestaví příkaz v APDU formátu (ISO-7816-4) do příkazu SIM TOOLKIT normy GSM 11.14,

. ve II. kroku terminál příkaz APDU přijme a sdělí ho přidavné kartě 2,

. ve III. kroku zašle přidavná karta zpět terminálu návratový kód SW1/SW2 ve formátu APDU. Tento kód, v případě výstupního příkazu, je přiřazen k datům,

. ve IV. kroku připraví terminál „Terminal Response“ TR a vyšle SIM kartě odpověď s návratovým kódem,

. v V. kroku SIM karta v případě zdárného příjmu zpracuje odpověď, v opačném případě se začíná znovu od I. kroku.

Obrázek číslo 4 znázorňuje hlavní příkazy používané k navázání dialogu mezi SIM kartou a přidavnou kartou – kartou 2 – přes terminál.

Příkaz „karta 2 přítomna“ je vyslán terminálem. Čtyři ostatní příkazy jsou vysílány SIM kartou k terminálu, který si je přečte. Příkaz „Karta 2 zapnuta“ je zpracován terminálem a jako příkaz RESET je odeslán kartě číslo 2. Příkaz „Karta 2 vypnuta“ je zpracován terminálem, který následně přestane kartu číslo 2 zásobovat elektrickým proudem.

Příkazy Karta 2 vstup/výstup byly již podrobně rozebrány na schématu obrázku číslo 3.



PATENTOVÉ NÁROKY

1. Způsob pro provádění transakcí přes telekomunikační síť (60) s pomocí čipových karet (1, 2) a telekomunikačních terminálů (50) pro připojení se na síť vybavených přinejmenším dvěma interfacem ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta (1) určenou k telefonii, druhým pro vkládání přídatné čipové karty (2) určené k jednomu či více užití jinému než telefonickému, vyznačený tím, že identifikační čipová karta abonenta komunikovala s přídatnou kartou přes terminál pomocí sady příkazů určených k pilotování výše uvedené přídatné karty s tím, že tyto příkazy jsou předformátovány identifikační čipovou kartou abonenta dle formátu komunikačního protokolu přídatné karty a předávány terminálem dle jeho přenosového protokolu.
2. Způsob pro provádění transakcí podle nároku 1, vyznačený tím, že sada příkazů obsahovala alespoň následující příkazy:
 - zapojení přídatné karty do sítě „karta 2 zapnuta“,
 - odpojení přídatné karty „karta 2 vypnuta“,
 - odeslání dat do přídatné karty „Odeslání vstupního příkazu do karty 2“,
 - příjem dat z přídatné karty „Odeslání výstupního příkazu do karty 2“.
3. Způsob podle nároku 1 nebo 2, vyznačený tím, že komunikace s přídatnou kartou (2) přes terminál obsahovala dodatečný příkaz vyslaný terminálem identifikační čipové kartě abonenta podle jejího komunikačního protokolu, přičemž tento příkaz zní:
 - přítomnost přídatné karty „karta 2 přítomna“.
4. Způsob podle libovolného z předchozích nároků vyznačený tím, že komunikace s přídatnou kartou (2) přes terminál je spouštěna programem nahraným v identifikační kartě abonenta.
5. Způsob podle libovolného z předchozích nároků vyznačený tím, že identifikační karta abonenta (1) byla schopna pilotovat dálkové načítání jednoho či více programů určených ke spouštění aplikací pro přídatnou kartu (2) přes terminál do své vlastní programové paměti, přičemž tyto programy pocházejí ze stahovacího aplikačního serveru přístupného přes terminály pomocí telekomunikační sítě.
6. Způsob podle libovolného z předchozích nároků vyznačený tím, že telefonická síť (60) je sítí radiomobilních telefonů (GSM), terminály jsou radiotelefony a identifikačními kartami abonenta jsou SIM karty.
7. Způsob podle libovolného z nároků 1 až 4 vyznačený tím, že telefonickou sítí je komutovaná telefonická síť nebo integrovaná síť komunikačních služeb (ISDN).
8. Identifikační čipová telefonní karta abonenta vyznačená tím, že obsahuje prostředky pro komunikaci s přídatnou kartou (2) určenou k jednomu či více využití jinému než telefonickému a to přes telekomunikační terminál (50) vybavený přinejmenším dvěma interfacem ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta určenou k telefonii a druhým pro vkládání přídatné čipové karty, přičemž tyto prostředky obsahují i sadu příkazů určených k pilotování přídatné karty (2) s tím, že tyto příkazy jsou předformátovány identifikační kartou abonenta ve formátu (APDU) komunikačního protokolu přídatné karty a přenášeny terminálem dle jeho komunikačního protokolu.



9. Identifikační čipová karta abonenta podle nároku 8, vyznačená tím, že obsahuje programovou paměť včetně programu upraveného k pilotování dálkového načítání dat do této paměti přes terminál (50) z jednoho či více programů určených ke spuštění aplikací pro přídatnou kartu (2), přičemž tyto programy pocházejí ze serveru pro dálkové načítání dat (20) přístupného přes terminály pomocí telekomunikační sítě (60).

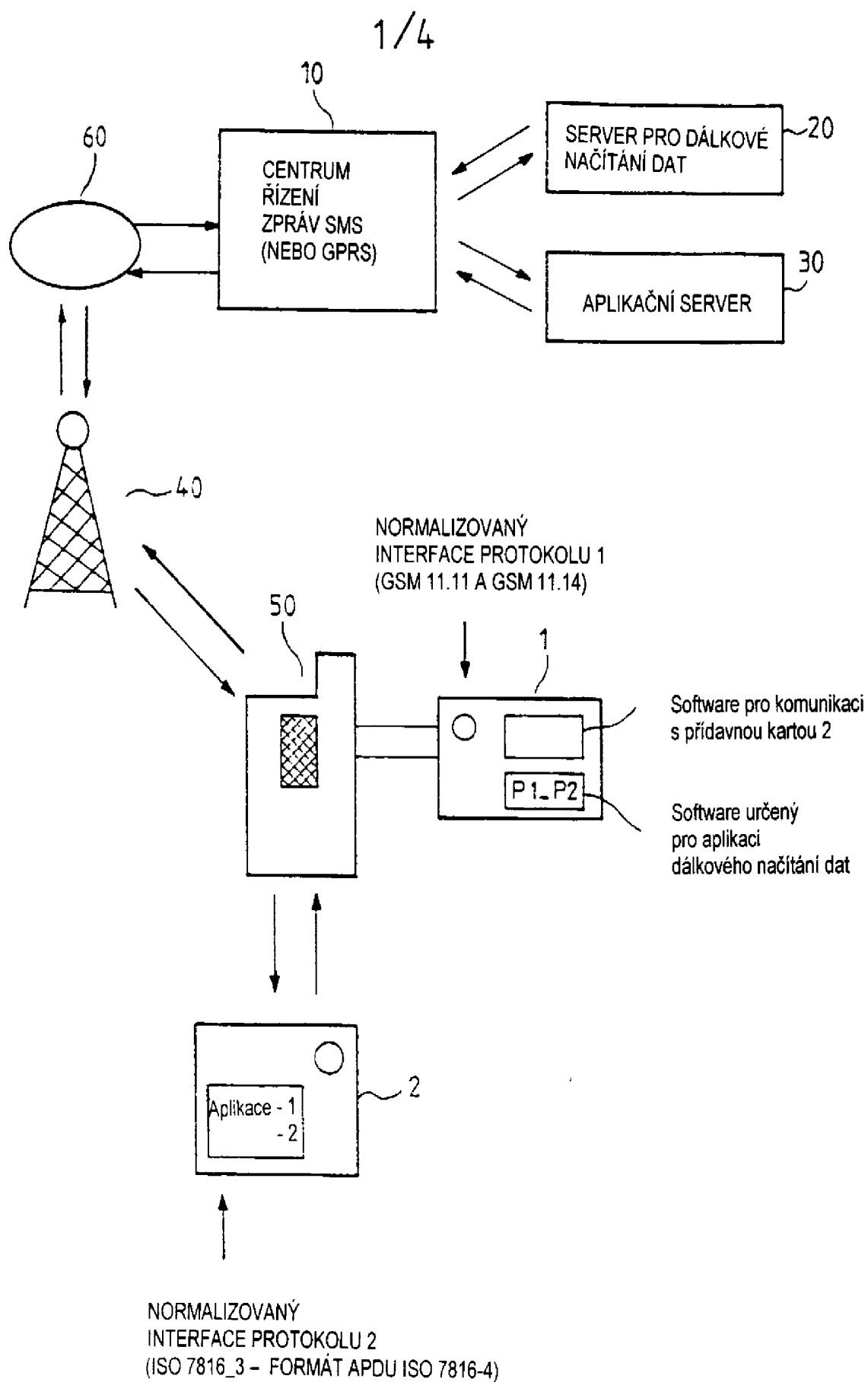
10. Identifikační čipová karta abonenta podle nároku 9, vyznačená tím, že určené programy stažené na identifikační kartu abonenta (1) obsahovaly jednu či více aplikací pro přídatnou kartu (2), přičemž tyto aplikace odpovídají řízení rozhraní stroj - uživatel, řízení komunikace s výše uvedenou přídatnou kartou a řízení komunikace s aplikačním serverem (30) vázaným na přídatnou kartu.

11. Telekomunikační terminál přístupu na síť vybavený přinejmenším dvěma interfaci ke snímání čipových karet, jedním pro vkládání identifikační čipové karty abonenta (1) určenou k telefonii a druhým pro vkládání přídatné čipové karty (2) určené k jednomu či více užití jinému než telekomunikačnímu, vyznačený tím, že obsahuje:

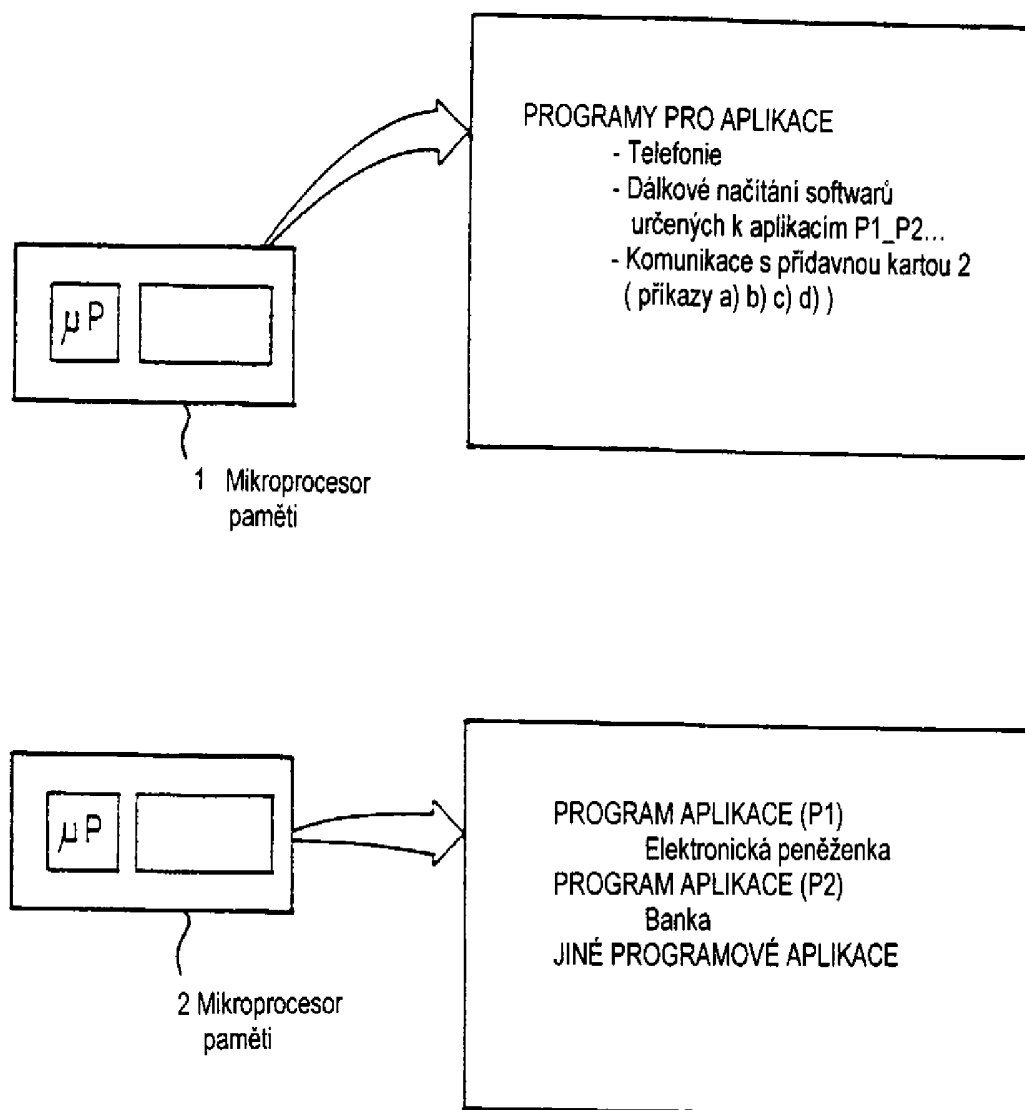
- prostředky adaptované k příjmu příkazů vyslaných identifikační kartou abonenta v přenosovém protokolu výše uvedeného terminálu a určené k pilotování přídatné karty s tím, že tyto příkazy jsou předformátovány identifikační kartou abonenta ve formátu (APDU) komunikačního protokolu přídatné karty,
- prostředky k odeslání z výše uvedených příkazů příkazů „odeslání příkazu vstup/výstup karta 2“ přídatné kartě s tím, že tyto jsou předformátovány,
- prostředky pro vykonání z výše uvedených příkazů příkazů „karta 2 zapnutá/vypnutá“,
- prostředky pro vyslání příkazu „karta 2 přítomna“ identifikační kartě abonenta.

12. Telekomunikační terminál podle nároku 11, vyznačený tím, že příkazy vyslané identifikační kartou abonenta (1) jsou sestaveny dle přenosového protokolu telekomunikačního terminálu, přičemž terminál je schopen sbírat předformátovaná data takto obdržená, aby je mohl dále předávat přídatné kartě dle svého komunikačního protokolu.

13. Telefonní terminál dle nároku 10 vyznačený tím, že transportní protokol mezi terminálem a identifikační kartou abonenta je definován dle normy GSM 11.14 a že komunikační protokol s přídatnou kartou je ve formátu APDU (ISO 7816-4).

**OBR 1**

2/4

**OBR 2**

3/4

SIM KARTAOBR 3

VYSLÁNÍ PŘÍKAZU VSTUP/VÝSTUP

PŘÍKAZ SIMTOOLKIT DLE PROTOKOLU GSM 11.14

FORMÁT PŘÍKAZU
ISO - APDUTELEFON (TERMINÁL)

PŘÍJÍMÁ FORMÁT PŘÍKAZU ISO - APDU

ISO IN/OUT (APDU)

PŘÍDAVNÁ KARTAZPĚTNÉ ODESLÁNÍ NÁVRATOVÉHO KÓDU (+ DAT, JEDNÁ-LI SE O VÝSTUPNÍ
PŘÍKAZ)

SW1 SW2

FORMÁT ISO-APDU

TELEFON (TERMINÁL)PŘIPRAVUJE TERMINAL RESPONSE (TR + NÁVRATOVÝ KÓD)
ODESLÁNÍ TERMINAL RESPONSE

TR SW1 SW2

SIM KARTAZPRACOVÁNÍ PŘIJATÝCH INFORMACÍ V PŘÍPADĚ ŽE JE
PŘÍJEM V POŘÁDKU - V OPAČNÉM PŘÍPADĚ ZAČÍT ZNOVU

4/4

OBR 4

• PŘÍKAZ „KARTA 2 PŘÍTOMNA“

SIM KARTA (1)

TERMINÁL

PŘÍDAVNÁ KARTA (2)

Přídavná karta je zasunuta
do čtecího zařízení
terminálu

Spouští řídicí program
přídavné karty

← Obálka
(Karta 2 přítomna)

• PŘÍKAZ „KARTA 2 ZAPNUTA“

SIM KARTA (1)

TERMINÁL

KARTA (2)

„Karta 2 zapnuta“ →

„Reset“ kartu 2 →

← Odpověď na reset

← Informace z karty 2

• PŘÍKAZ „KARTA 2 VYPNUTA“

SIM KARTA

TERMINÁL

KARTA (2)

„Karta 2 vypnuta“ →

Ukončuje použití karty 2 →

Zakončení použití

• PŘÍKAZ „VYSLÁNÍ PŘÍKAZU KARTA 2 VSTUP“

SIM KARTA

TERMINÁL

KARTA (2)

„Vyslání příkazu karta
2 vstup“ →Vstupní příkaz +
data →← Návratový kód
vstupního příkazu

Zpracování příkazu

← Návratový kód karty 2

• PŘÍKAZ „VYSLÁNÍ PŘÍKAZU KARTA 2 VÝSTUP“

SIM KARTA

TERMINÁL

KARTA (2)

„Vyslání příkazu karta
2 výstup“ →

Výstupní příkaz →

← Návratový kód
výstupního příkazu + Data

ZPRACOVÁNÍ

← Návratový kód + Data