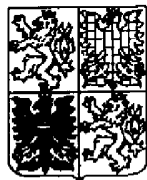


PŘIHLÁŠKA VYNÁLEZU

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

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **26.02.1998**
(32) Datum podání prioritní přihlášky: **28.02.1997**
(31) Číslo prioritní přihlášky: **1997/19708189**
(33) Země priority: **DE**
(40) Datum zveřejnění přihlášky vynálezu: **12.01.2000**
(Věstník č. 1/2000)
(86) PCT číslo: **PCT/DE98/00569**
(87) PCT číslo zveřejnění: **WO98/38826**

(21) Číslo dokumentu:

1999 - 3074

(13) Druh dokumentu: **A3**

(51) Int. Cl. ⁷:
H 04 Q 7/38
H 04 Q 7/22

(71) Přihlašovatel:
DETEMOBIL DEUTSCHE TELEKOM MOBILNET
GMBH, Bonn, DE;

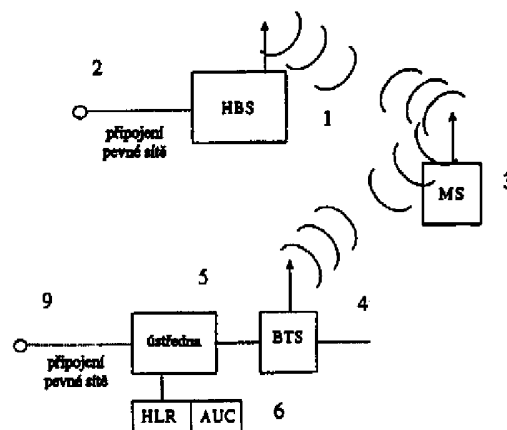
(72) Původce:
Ljungström Patrik, Bonn, DE;
Mohrs Walter, Bonn, DE;
Pernice Frieder, Gross-Zimmern, DE;

(74) Zástupce:
Všetečka Miloš JUDr., Háfkova 2, Praha 2,
120 00;

(54) Název přihlášky vynálezu:
**Bezdrátový komunikační systém kompatibilní
s veřejným mobilním komunikačním
systémem**

(57) Anotace:

Bezdrátový komunikační systém, který je na radiovém rozhraní v podstatě kompatibilní s veřejným mobilním komunikačním systémem, který má alespoň jednu funkci k autentizaci, přičemž základní stanice bezdrátového komunikačního systému je vybavena zařízeními ke čtení a zapisování informace z/na identifikační moduly a disponuje vhodným programovým vybavením, a spolu s daty, uloženými na identifikačním modulu, dává k dispozici funkce domovského registru /HLR/ popř. opravňovací ústředny /AUC/. Na identifikačních modulech se mimoto nemanipulovatelným způsobem ukládají ještě veškeré inicializační parametry bezdrátových základních stanic, které chce provozovatel sítě držet pod kontrolou.





BEZDRÁTOVÝ KOMUNIKAČNÍ SYSTÉM KOMPATIBILNÍ S VEŘEJNÝM MOBILNÍM KOMUNIKAČNÍM SYSTÉMEM

Oblast techniky

Vynález se týká bezdrátového komunikačního systému podle druhové části patentového nároku 1, kompatibilního s veřejným komunikačním systémem.

Dosavadní stav techniky

U dnešních mobilních komunikačních systémů existuje jasné rozlišení mezi veřejnými mobilními radiovými systémy, jako např. GSM - systémem, a soukromými bezdrátovými komunikačními systémy, které pracují například podle digitálního DECT-standardu. Toto vedlo k odlišným přístrojovým systémům, které jsou vhodné buď pro mobilní radiový provoz nebo bezdrátový provoz.

Byly již prováděny pokusy, konstruovat koncové přístroje, zejména mobilní koncové přístroje, které jsou vhodné k provozu ve dvou různých mobilních komunikačních systémech. Na základě nekompatibility různých standardů toto vede ale k relativně uživatelsky nepřívětivým a drahým řešením.

Jiný výchozí bod spočívá v tom, zřídit základní stanici bezdrátového komunikačního systému takovým způsobem, že tato je kompatibilní s veřejným mobilním komunikačním systémem,



tzn. může komunikovat s běžnými mobilními koncovými přístroji veřejného mobilního komunikačního systému. Chybí ale vhodné návrhy k realizování, např. potřebných bezpečnostních funkcí. Problém přitom spočívá v tom, že základní stanice bezdrátového komunikačního systému je spojena s pevnou sítí s propojenými vodiči, takže není možné přímé ovlivnění základní stanice přes mobilní komunikační systém.

Úkolem vynálezu proto je, navrhnout bezdrátový komunikační systém s bezpečnostními funkcemi, který je kompatibilní s veřejným mobilním komunikačním systémem a umožňuje použití příslušných mobilních koncových přístrojů. Další úkol spočívá v tom, že bezdrátový komunikační systém přes svou povahu soukromého systému má mít možnost, být zřizován a provozován pod kontrolou příslušného provozovatele mobilní komunikační sítě.

Podstata vynálezu

Řešením daného úkolu je vynález, vyznačující se znaky nároku 1.

Podstata vynálezu spočívá v tom, že základní stanice bezdrátového komunikačního systému se vybaví vhodným čtecím/zapisovacím zařízením, se kterým se mohou přečíst a popsat informace běžných identifikačních modulů, pod kterými se rozumí např. čipové karty, SIM's (Subscriber Identity Modules), všeobecně všechny aktivní nosiče dat, které informace ukládají a zpracovávají. Ve spojení s vhodným programovým vybavením a s daty, uloženými na identifikačním modulu, je základní stanice bezdrátového komunikačního



systému nyní s to převzít funkce základní stanice mobilní komunikační sítě s autentizační funkcí, přesněji, funkce domovského registru (HLR: Home Location Register) popř. opravňovací ústředny (AUC: Authentication Center). Tím se může každý mobilní koncový přístroj, oprávněný k používání, přihlásit u základní stanice bezdrátového komunikačního systému a komunikovat přes pevnou síť.

V následujícím se pojem "základní stanice" vztahuje, pokud není udáno jinak, na základní stanici bezdrátového komunikačního systému.

V následujícím se popisuje jedna z mnoha možností myšlenky vynálezu na příkladu mobilního komunikačního systému GSM. Vynález ale není na mobilní komunikační systémy GSM omezen.

Implementováním jedné nebo několika čteček/zapisovačů čipových karet a běžné SIM - čipové karty v základní stanici bezdrátového komunikačního systému se dosahuje, že provoz základní stanice je v činnosti pod kontrolou příslušného provozovatele sítě GSM, a že účastníkovi se v "bezdrátovém provozu GSM" nabízejí bezpečnostní znaky, jako např. autentizace a kódování hovorových dat, jako při provozu v mobilní radiové síti GSM. Důležité je, že čipová karta, potřebná k provozu základní stanice, se vydává provozovatelem sítě, jak je i běžné u mobilních koncových přístrojů GSM.

Čipová karta, použitá v základní stanici, přebírá přitom spolu s vhodným programovým vybavením, implementovaným v základní stanici, funkci domovského registru (HLR), popř. opravňovací ústředny (AUC), to

znamená, že mobilní koncový přístroj se nyní autentizuje vůči základní stanici bezdrátového systému, a ne, jak je obvyklé, vůči radiové telefonní síti. Přitom se na základě implementovaného programového vybavení generuje v základní stanici náhodné číslo, které se s K_i - klíčem, identicky uloženým v obou čipových kartách, čipové kartě základní stanice a čipové kartě mobilního koncového přístroje, a algoritmu A3, specifického pro systém GSM, přeměňuje na SRES - odpověď (výsledek autentizace). Při souhlasu obou výsledků autentizace - základní stanice a mobilního koncového přístroje - je autentizace úspěšná. Tato procedura autentizace je stejná jako u systému GSM.

Ze stejného náhodného čísla se K_i - klíčem a algoritmem A8 odvozuje známým způsobem klíč K_c , který slouží ke kódování komunikace na radiovém rozhraní v bezdrátovém provozu (jako u systému GSM).

Na SIM základní stanice mohou být vedle běžných dat, specifických pro osobu, uložena ještě dodatečná data tak, aby se s nimi nedalo manipulovat, jako např. povolené kmitočty, maximálně přípustné výstupní výkony pro základní stanici a mobilní koncový přístroj, přístupné služby (telefonie, přenos dat, fax atd.) a všechny ostatní inicializační parametry, na které chce provozovatel sítě mít vliv a které smí základní stanice používat. Toto odpovídá, alespoň pro služby, známé správě oprávnění v domovském registru (HLR) mobilní radiové sítě GSM.

Vhodným řízením klíče se může dosáhnout, že několik účastníků, např. příslušníků rodiny, může komunikovat přes jednu a tu samou základní stanici. K tomu je jako první možnost navrženo, že každý účastník, který chce použít



základní stanici, má svou vlastní druhou SIM - kartu, která se může zastrčit do základní stanice. Základní stanice pro to potřebuje několik přístrojů na čtení karet.

Další možnost spočívá v tom, že na SIM - kartě základní stanice jsou uložena data a klíč pro několik účastníků. Dále je možno si představit skupinový klíč v základní stanici, který umožňuje autentizaci několika individuálních účastníků.

Důležité je, že čipová karta, použitá v základní stanici, obsahuje v základní oblasti identické informace, jako čipová karta koncového přístroje GSM, která se má provozovat se základní stanicí. Jenom když na obou kartách souhlasí osobní data uživatele, zejména bezpečnostní funkce, může se mobilní koncový přístroj u základní stanice autentizovat a přihlásit.

Při zrušení regulérního GSM - účastnického poměru se v SIM - kartě mobilního koncového přístroje, přednostně přes radiové rozhraní GSM, maže oprávnění ke komunikaci se základní stanicí. Tím už není další provoz základní stanice na příslušných kmitočtech, uvolněných specifickým provozovatelem sítě, rozumně možný, protože se mobilní koncový přístroj už nemůže u základní stanice autentizovat.

Možné provedení mimoto navrhuje, že základní stanice obsahuje časovací jednotku (timer), která je provozovatelem sítě programována na určitý čas, a při používání základní stanice účastníkem se vždy automaticky vynuluje. Pokud se základní stanice nepoužívá, např. po zrušení okolností spojení, ztrácí základní stanice po uplynutí naprogramované doby oprávnění, uvádět vysílač do provozu na kmitočtech



mobilního komunikačního systému. Pokud se základní stanice nepoužívá po delší dobu, může funkce časovací jednotky zamrznout pomocí vypnutí základní jednotky.

Pokud účastník např. před nástupem na dlouhou dovolenou zapomněl vypnout základní stanici a tato se automaticky deaktivovala, je uvnitř definovaného časového okénka navržena možnost nouzového pokračování v činnosti.

K realizování GSM - kompatibilní základní stanice je ji třeba vybavit nejdříve čtečkou karet pro GSM - SIM - karty. Základní stanice dále musí být s to, vysílat a přijímat na GSM - standardních kmitočtech. Řízení funkce základní stanice se uskutečňuje pomocí vhodného programového vybavení, jaké se např. používá v GSM - koncových přístrojích a které provádí a řídí autentizaci běžnou u GSM a další funkce.

Vlastní mobilní koncový přístroj vyžaduje pouze malou programově - technickou modifikaci.

Přehled obrázků na výkresech

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

obr. 1 schematicky příkladnou fyzikální konstelaci systému podle vynálezu;

obr. 2 schematicky příkladnou logickou konstelaci systému podle vynálezu.

Příklady provedení vynálezu

Na obrázku 1 je schematicky znázorněno několik zařízení veřejného mobilního komunikačního systému. Je k dispozici mobilní koncový přístroj 3, který se nachází ve spádové oblasti základní stanice 4 mobilního komunikačního systému a který s ní může kódovaně komunikovat přes radiové rozhraní. Základní stanice 4 mobilního komunikačního systému je spojena s ústřednou 5, která má přístup k veřejné pevné síti 2. Ústředna 5 je dále v kontaktu s domovským registrem (HLR) a opravňovací ústřednou (AUC) mobilní radiové sítě. Pokud se chce mobilní koncový přístroj 3 přihlásit v mobilní komunikační síti, provádí se známým způsobem autentizace mobilního koncového přístroje 3 uvnitř domovského registru popř. opravňovací ústředny 6.

Dále je znázorněna základní stanice 1 (HBS) bezdrátového komunikačního systému, rovněž spojená s veřejnou, vedeními pospojovanou pevnou sítí 2 (PSTN, ISDN). Na základě nepatrného výstupního výkonu je spádová oblast základní stanice relativně malá. Základní stanice 1 se zpravidla nachází uvnitř spádové oblasti jedné nebo několika základních stanic 4 veřejné mobilní komunikační sítě.

Jak je znázorněno na obrázku 2, mobilní koncový přístroj 3 se autentizuje v mobilním radiovém provozu mobilní radiovou sítí, a sice s pomocí specifického identifikačního klíče (K_i - klíč), který je uložen jednak v SIM - kartě 8 mobilního koncového přístroje 3 a jednak v domovském registru 6 (HLR), popř. opravňovací ústředně (AUC) mobilního komunikačního systému.



Podle vynálezu je nyní základní stanice 1 bezdrátového komunikačního systému vybavena identifikačním modulem 7 (např. rovněž se SIM - kartou) a vhodným programovým vybavením, aby ve spojení s daty, uloženými na identifikačním modulu 7, vnímala jenom ty samé funkce a úlohy, které vnímá domovský registr popř., opravňovací ústředna mobilního komunikačního systému, takže mobilní koncový přístroj 3, pokud se nachází ve spádové oblasti bezdrátového komunikačního systému a má oprávnění k přístupu, se může autentizovat, přihlásit a kódovaně komunikovat u základní stanice 1 bezdrátového systému, která mu přísluší. To je možné pouze, když podstatné rozsahy dat identifikačního modulu 7, použitého v základní stanici 1, jsou identické s daty, uloženými na čipové kartě (SIM) mobilního koncového přístroje 3 s oprávněním k přístupu.

Podle vynálezu je základní stanice 1 bezdrátového systému nyní kompatibilní s mobilním komunikačním systémem, tzn. ve Standby - módu vysílá základní stanice 1 bezdrátového systému periodicky specifickou identifikaci, aby indikovala svoji přítomnost a připravenost k provozu. Mobilní koncový přístroj 3 sleduje kmitočtové pásmo podle specifické identifikace základní stanice 1. Když se mobilní koncový přístroj 3 dostane do spádové oblasti základní stanice 1 a přijme bez rušení její identifikaci, pokusí se mobilní koncový přístroj 3 popsáním způsobem přihlásit u základní stanice 1. K tomu se vyměňují, jako u systému GSM, autentizační a inicializační zprávy mezi základní stanicí 1 a mobilním koncovým přístrojem 3. Pokud byla autentizace úspěšná, může mobilní koncový přístroj 3 komunikovat po pevné síti 2, bez okliky přes mobilní komunikační síť.

Přirozeně je také možné, že několik oprávněných mobilních koncových přístrojů 3 spolu kódovaně komunikuje přes základní stanici 1 bezdrátové komunikační sítě bez spolupůsobení veřejné pevné sítě 2, 2 nebo mobilní komunikační sítě.

Zastupuje:

Dr. Miloš Všetečka v.r.



PATENTOVÉ NÁROKY

1. Způsob provozu bezdrátového komunikačního systému, který je na radiovém rozhraní v podstatě kompatibilní s veřejným mobilním komunikačním systémem, který má alespoň jednu funkci k autentizaci, *vyznačující se tím*, že základní stanice bezdrátového komunikačního systému je vybavena zařízeními ke čtení a zapisování informací z/na identifikační moduly a disponuje vhodným programovým vybavením, aby se ve spojení s daty, uloženými na identifikačních modulech, nechaly připravit funkce domovského registru popř. opravňovací ústředny, takže oprávněné mobilní koncové přístroje, které se nacházejí ve spádové oblasti bezdrátového komunikačního systému, se mohou autentizovat a přihlásit u základní stanice, která je jim příslušná.

2. Způsob podle nároku 1, *vyznačující se tím*, že podstatné rozsahy dat identifikačního modulu, použitého v základní stanici, jsou identické s daty, uloženými na čipové kartě (SIM) mobilního koncového přístroje s oprávněním k přístupu.

3. Způsob podle nároku 1 nebo 2, *vyznačující se tím*, že oprávnění mobilního koncového přístroje k přihlášení u základní stanice bezdrátového komunikačního systému může být zablokováno provozovatelem sítě mobilního komunikačního systému.

4. Způsob podle některého z nároků 1 až 3, *vyznačující se tím*, že na identifikačním modulu jsou

vedle individuálních dat účastníka k autentizaci nemanipulovatelně uložena další data, totiž dovolené kmitočty, maximálně přípustné výstupní výkony pro základní stanici a mobilní koncový přístroj, přípustné služby (telefonie, přenos dat, fax atd.) a všechny ostatní inicializační parametry, na které chce mít provozovatel sítě vliv a které jsou rámcově implicitními hodnotami pro provoz základní stanice bezdrátového systému.

5. Způsob podle některého z nároků 1 až 4, *vyznačující se tím*, že radiové rozhraní základní stanice bezdrátového komunikačního systému pracuje v kmitočtovém spektru veřejného mobilního komunikačního systému.

6. Způsob podle některého z nároků 1 až 5, *vyznačující se tím*, že na radiovém rozhraní se používá kódování přenášených dat.

7. Způsob podle některého z nároků 1 až 6, *vyznačující se tím*, že základní stanice obsahuje časovací jednotku (timer), která je provozovatelem sítě naprogramována na určitý čas, a která se při oprávněném použití základní stanice účastníkem vždy automaticky vynuluje, přičemž základní stanice při nepoužití, tzn. po uplynutí doby naprogramované v časovací jednotce ztrácí oprávnění uvádět svůj vysílač do provozu na kmitočtech mobilního komunikačního systému.

8. Způsob podle některého z nároků 1 až 7, *vyznačující se tím*, že při automatickém odpojení základní stanice uplynutím času časovací jednotky je navržena možnost nouzového obnovení provozu.

9. Způsob podle některého z nároků 1 až 8, **vyznačující se tím**, že nouzové obnovení provozu základní stanice je možné jenom uvnitř definovaného časového okénka.

10. Bezdrátový komunikační systém k provádění způsobu podle některého z nároků 1 až 9, **vyznačující se tím**, že základní stanice (1) bezdrátového komunikačního systému je vybavena alespoň jedním čtecím/zapisovacím zařízením, kterým se mohou číst a zapisovat informace běžných identifikačních modulů (7) veřejného mobilního komunikačního systému, a v základní stanici (1) je implementováno vhodné programové vybavení, které čte informace z identifikačního modulu (7), popř. zapisuje informace na identifikační modul a zpracovává je.

11. Bezdrátový komunikační systém podle nároku 10, **vyznačující se tím**, že jako identifikační modul (7) se používají čipové karty (SIM), jako např. podle ISO ID-1, ID-000, DCS 1800, PCS 1900, které se obvykle používají v mobilních komunikačních systémech.

Zastupuje:

Dr. Miloš Všetečka v.r.

Seznam vztahových značek

- | | |
|----------------|---|
| 1 | Základní stanice (HBS) |
| 2 | Pevná síť (PSTN, ISDN) |
| 3 | Mobilní koncový přístroj |
| 4 | Základní stanice |
| 5 | Ústředna |
| 6 | Opravňovací ústředna
(AUC)
Domovský registr (HLR) |
| 7 | Identifikační modul |
| 8 | SIM - karta |
| 9 | Veřejná pevná síť |
| K _i | klíč |

Během řízení o této PCT-přihlášce č. PCT/DE98/00569 bylo (na základě International Preliminary Examination) upraveno znění popisu a patentových nároků. Upravené znění těchto patentových nároků a popisu přikládáme v příloze.

BEZDRÁTOVÝ KOMUNIKAČNÍ SYSTÉM KOMPATIBILNÍ S VEŘEJNÝM MOBILNÍM KOMUNIKAČNÍM SYSTÉMEM

Oblast techniky

Vynález se týká bezdrátového komunikačního systému, kompatibilního s veřejným komunikačním systémem, a způsobu jeho provozu, podle druhové části nezávislých patentových nároků.

Dosavadní stav techniky

U dnešních mobilních komunikačních systémů existuje jasné rozlišení mezi veřejnými mobilními radiovými systémy, jako např. GSM - systémem, a soukromými bezdrátovými komunikačními systémy, které pracují například podle digitálního DECT-standardu. Toto vedlo k odlišným přístrojovým systémům, které jsou vhodné buď pro mobilní radiový provoz nebo bezdrátový provoz.

Byly již prováděny pokusy, konstruovat koncové přístroje, zejména mobilní koncové přístroje, které jsou vhodné k provozu ve dvou různých mobilních komunikačních systémech. Na základě nekompatibility různých standardů toto vede ale k relativně uživatelsky nepřívětivým a drahým řešením.

Jiný výchozí bod spočívá v tom, zřídit základní stanici bezdrátového komunikačního systému takovým způsobem, že tato

je kompatibilní s veřejným mobilním komunikačním systémem, tzn. může komunikovat s běžnými mobilními koncovými přístroji veřejného mobilního komunikačního systému. Chybí ale vhodné návrhy k realizování, např. potřebných bezpečnostních funkcí. Problém přitom spočívá v tom, že základní stanice bezdrátového komunikačního systému je spojena s pevnou sítí s propojenými vodiči, takže není možné přímé ovlivnění základní stanice přes mobilní komunikační systém.

WO-A-95/24106 se zabývá bezpečným osobním komunikačním systémem, založeným na základní stanici, připojené na veřejnou pevnou síť, která umožňuje provoz koncových přístrojů mobilního komunikačního systému. Bezpečnost komunikace se zaručuje použitím autentizačního způsobu, běžného v mobilním komunikačním systému, přičemž základní stanice je spojena přes veřejnou síť s bezpečnostními zařízeními mobilního komunikačního systému a vyměňuje si s nimi bezpečnostní informace, aby se umožnilo přihlášení mobilního koncového přístroje u základní stanice. Tento způsob se zakládá tedy na výměně autentizačních frekvencí jednak mezi mobilním koncovým přístrojem a základní stanicí, a jednak mezi základní stanicí a zařízeními mobilní komunikační sítě.

Z WO-A-95/02927 je znám způsob řízení vysílačích/přijímacích zařízení radiových komunikačních systémů. Přitom je vysílačí/přijímací zařízení vybaveno zařízeními ke čtení takzvané Smart Card, na které jsou uloženy informace o kmitočtech, použitelných vysílačím/přijímacím zařízením, uvolněných provozovatelem radiového komunikačního systému.

Úkolem vynálezu proto je, navrhnout bezdrátový komunikační systém s bezpečnostními funkcemi, který je kompatibilní s veřejným mobilním komunikačním systémem a umožňuje použití příslušných mobilních koncových přístrojů. Další úkol spočívá v tom, že bezdrátový komunikační systém přes svou povahu soukromého systému má mít možnost, být zřizován a provozován pod kontrolou příslušného provozovatele mobilní komunikační sítě.

Podstata vynálezu

Řešením daného úkolu je vynález, vyznačující se znaky nezávislých patentových nároků.

Podstata vynálezu spočívá v tom, že základní stanice bezdrátového komunikačního systému se vybaví vhodným čtecím/zapisovacím zařízením, se kterým se mohou přečíst a popsat informace běžných identifikačních modulů, pod kterými se rozumí např. čipové karty, SIM's (Subscriber Identity Modules), všeobecně všechny aktivní nosiče dat, které informace ukládají a zpracovávají. Ve spojení s vhodným programovým vybavením a s daty, uloženými na identifikačním modulu, je základní stanice bezdrátového komunikačního systému nyní s to převzít funkce základní stanice mobilní komunikační sítě s autentizační funkčností, přesněji, funkce domovského registru (HLR: Home Location Register) popř. opravňovací ústředny (AUC: Authentication Center). Tím se může každý mobilní koncový přístroj, oprávněný k používání, přihlásit u základní stanice bezdrátového komunikačního systému a komunikovat přes pevnou síť.

V následujícím se pojem "základní stanice" vztahuje,

pokud není udáno jinak, na základní stanici bezdrátového komunikačního systému.

V následujícím se popisuje jedna z mnoha možností myšlenky vynálezu na příkladu mobilního komunikačního systému GSM. Vynález ale není na mobilní komunikační systémy GSM omezen.

Implementováním jedné nebo několika čteček/zapisovačů čipových karet a běžné SIM - čipové karty v základní stanici bezdrátového komunikačního systému se dosahuje, že provoz základní stanice je v činnosti pod kontrolou příslušného provozovatele sítě GSM, a že účastníkovi se v "bezdrátovém provozu GSM" nabízejí bezpečnostní znaky, jako např. autentizace a kódování hovorových dat, jako při provozu v mobilní radiové síti GSM. Důležité je, že čipová karta, potřebná k provozu základní stanice, se vydává provozovatelem sítě, jak je i běžné u mobilních koncových přístrojů GSM.

Čipová karta, použitá v základní stanici, přebírá přitom spolu s vhodným programovým vybavením, implementovaným v základní stanici, funkci domovského registru (HLR), popř. opravňovací ústředny (AUC), to znamená, že mobilní koncový přístroj se nyní autentizuje vůči základní stanici bezdrátového systému, a ne, jak je obvyklé, vůči radiové telefonní síti. Přitom se na základě implementovaného programového vybavení generuje v základní stanici náhodné číslo, které se s K_1 - klíčem, identicky uloženým v obou čipových kartách, čipové kartě základní stanice a čipové kartě mobilního koncového přístroje, a algoritmu A3, specifického pro systém GSM, přeměňuje na SRES - odpověď (výsledek autentizace). Při souhlasu obou

výsledků autentizace - základní stanice a mobilního koncového přístroje - je autentizace úspěšná. Tato procedura autentizace je stejná jako u systému GSM.

Ze stejného náhodného čísla se K_i - klíčem a algoritmem A8 odvozuje známým způsobem klíč K_c , který slouží ke kódování komunikace na radiovém rozhraní v bezdrátovém provozu (jako u systému GSM).

Na SIM základní stanice mohou být vedle běžných dat, specifických pro osobu, uložena ještě dodatečná data tak, aby se s nimi nedalo manipulovat, jako např. povolené kmitočty, maximálně přípustné výstupní výkony pro základní stanici a mobilní koncový přístroj, přístupné služby (telefonie, přenos dat, fax atd.) a všechny ostatní inicializační parametry, na které chce provozovatel sítě mít vliv a které smí základní stanice používat. Toto odpovídá, alespoň pro služby, známé správě oprávnění v domovském registru (HLR) mobilní radiové sítě GSM.

Vhodným řízením klíče se může dosáhnout, že několik účastníků, např. příslušníků rodiny, může komunikovat přes jednu a tu samou základní stanici. K tomu je jako první možnost navrženo, že každý účastník, který chce použít základní stanici, má svou vlastní druhou SIM - kartu, která se může zastrčit do základní stanice. Základní stanice pro to potřebuje několik přístrojů na čtení karet.

Další možnost spočívá v tom, že na SIM - kartě základní stanice jsou uložena data a klíč pro několik účastníků. Dále je možno si představit skupinový klíč v základní stanici, který umožňuje autentizaci několika individuálních účastníků.

Důležité je, že čipová karta, použitá v základní stanici, obsahuje v základní oblasti identické informace, jako čipová karta koncového přístroje GSM, která se má provozovat se základní stanicí. Jenom když na obou kartách souhlasí osobní data uživatele, zejména bezpečnostní funkce, může se mobilní koncový přístroj u základní stanice autentizovat a přihlásit.

Při zrušení regulérního GSM - účastnického poměru se v SIM - kartě mobilního koncového přístroje, přednostně přes radiové rozhraní GSM, maže oprávnění ke komunikaci se základní stanicí. Tím už není další provoz základní stanice na příslušných kmitočtech, uvolněných specifickým provozovatelem sítě, rozumně možný, protože se mobilní koncový přístroj už nemůže u základní stanice autentizovat.

Možné provedení mimoto navrhuje, že základní stanice obsahuje časovací jednotku (timer), která je provozovatelem sítě programována na určitý čas, a při používání základní stanice účastníkem se vždy automaticky vynuluje. Pokud se základní stanice nepoužívá, např. po zrušení okolností spojení, ztrácí základní stanice po uplynutí naprogramované doby oprávnění, uvádět vysílač do provozu na kmitočtech mobilního komunikačního systému. Pokud se základní stanice nepoužívá po delší dobu, může funkce časovací jednotky zamrznout pomocí vypnutí základní jednotky.

Pokud účastník např. před nástupem na dlouhou dovolenou zapomněl vypnout základní stanici a tato se automaticky deaktivovala, je uvnitř definovaného časového okénka navržena možnost nouzového pokračování v činnosti.

K realizování GSM - kompatibilní základní stanice je ji třeba vybavit nejdříve čtečkou karet pro GSM - SIM - karty. Základní stanice dále musí být s to, vysílat a přijímat na GSM - standardních kmitočtech. Řízení funkce základní stanice se uskutečňuje pomocí vhodného programového vybavení, jaké se např. používá v GSM - koncových přístrojích a které provádí a řídí autentizaci běžnou u GSM a další funkce.

Vlastní mobilní koncový přístroj vyžaduje pouze malou programově - technickou modifikaci.

Přehled obrázků na výkresech

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

- obr. 1 schematicky příkladnou fyzikální konstelaci systému podle vynálezu;
- obr. 2 schematicky příkladnou logickou konstelaci systému podle vynálezu.

Příklady provedení vynálezu

Na obrázku 1 je schematicky znázorněno několik zařízení veřejného mobilního komunikačního systému. Je k dispozici mobilní koncový přístroj 3, který se nachází ve spádové oblasti základní stanice 4 mobilního komunikačního systému a který s ní může kódovaně komunikovat přes radiové rozhraní.

Základní stanice 4 mobilního komunikačního systému je spojena s ústřednou 5, která má přístup k veřejné pevné síti 2. Ústředna 5 je dále v kontaktu s domovským registrem (HLR) a opravňovací ústřednou (AUC) mobilní radiové sítě. Pokud se chce mobilní koncový přístroj 3 přihlásit v mobilní komunikační síti, provádí se známým způsobem autentizace mobilního koncového přístroje 3 uvnitř domovského registru popř. opravňovací ústředny 6.

Dále je znázorněna základní stanice 1 (HBS) bezdrátového komunikačního systému, rovněž spojená s veřejnou, vedeními pospojovanou pevnou sítí 2 (PSTN, ISDN). Na základě nepatrného výstupního výkonu je spádová oblast základní stanice relativně malá. Základní stanice 1 se zpravidla nachází uvnitř spádové oblasti jedné nebo několika základních stanic 4 veřejné mobilní komunikační sítě.

Jak je znázorněno na obrázku 2, mobilní koncový přístroj 3 se autentizuje v mobilním radiovém provozu mobilní radiovou sítí, a sice s pomocí specifického identifikačního klíče (K_i - klíč), který je uložen jednak v SIM - kartě 8 mobilního koncového přístroje 3 a jednak v domovském registru 6 (HLR), popř. opravňovací ústředně (AUC) mobilního komunikačního systému.

Podle vynálezu je nyní základní stanice 1 bezdrátového komunikačního systému vybavena identifikačním modulem 7 (např. rovněž se SIM - kartou) a vhodným programovým vybavením, aby ve spojení s daty, uloženými na identifikačním modulu 7, vnímala jenom ty samé funkce a úlohy, které vnímá domovský registr popř., opravňovací ústředna mobilního komunikačního systému, takže mobilní koncový přístroj 3, pokud se nachází ve spádové oblasti

bezdrátového komunikačního systému a má oprávnění k přístupu, se může autentizovat, přihlásit a kódovaně komunikovat u základní stanice 1 bezdrátového systému, která mu přísluší. To je možné pouze, když podstatné rozsahy dat identifikačního modulu 7, použitého v základní stanici 1, jsou identické s daty, uloženými na čipové kartě (SIM) mobilního koncového přístroje 3 s oprávněním k přístupu.

Podle vynálezu je základní stanice 1 bezdrátového systému nyní kompatibilní s mobilním komunikačním systémem, tzn. ve Standby - módu vysílá základní stanice 1 bezdrátového systému periodicky specifickou identifikaci, aby indikovala svoji přítomnost a připravenost k provozu. Mobilní koncový přístroj 3 sleduje kmitočtové pásmo podle specifické identifikace základní stanice 1. Když se mobilní koncový přístroj 3 dostane do spádové oblasti základní stanice 1 a přijme bez rušení její identifikaci, pokusí se mobilní koncový přístroj 3 popsáním způsobem přihlásit u základní stanice 1. K tomu se vyměňují, jako u systému GSM, autentizační a inicializační zprávy mezi základní stanicí 1 a mobilním koncovým přístrojem 3. Pokud byla autentizace úspěšná, může mobilní koncový přístroj 3 komunikovat po pevné síti 2, bez okliky přes mobilní komunikační síť.

Přirozeně je také možné, že několik oprávněných mobilních koncových přístrojů 3 spolu kódovaně komunikuje přes základní stanici 1 bezdrátové komunikační sítě bez spolupůsobení veřejné pevné sítě 2, 2 nebo mobilní komunikační sítě.

Zastupuje:

Dr. Miloš Všetečka v.r.

P A T E N T O V É N Á R O K Y

1. Způsob provozu bezdrátového komunikačního systému s mobilním koncovým přístrojem (3) veřejného mobilního komunikačního systému, se základní stanicí (1), která je spojená s veřejnou pevnou sítí (2) a která je na radiovém rozhraní kompatibilní s veřejným mobilním komunikačním systémem, který má alespoň jednu funkci k autentizaci, *vyznačující se*

čtením/zapisováním informací z/na alespoň jeden identifikační modul (7) pomocí čtecího/zapisovacího zařízení základní stanicí (1), přičemž rozsahy dat identifikačního modulu (7), použitého v základní stanici (1) jsou identické s daty, uloženými na čipové kartě (SIM) mobilního koncového přístroje (3) s oprávněním k přístupu,

zpracováním přečtených dat pomocí programového vybavení, implementovaného v základní stanici (1),

autentizací mobilního koncového přístroje (3) vzhledem k základní stanici (1) podle dat, čtených a zpracovávaných identifikačním modulem (7), přičemž základní stanice (1) vnímá stejné funkce a úlohy, jako domovský registr popř. opravňovací ústředna mobilního komunikačního systému, a

při úspěšné autentizaci, provozováním mobilního koncového přístroje (3) přes veřejnou pevnou síť (2).

2. Způsob podle nároku 1, *vyznačující se tím*, že oprávnění mobilního koncového přístroje (3) k přihlášení

u základní stanice (1) bezdrátového komunikačního systému může být zablokováno provozovatelem sítě mobilního komunikačního systému.

3. Způsob podle nároku 1 nebo 2, *vyznačující se tím*, že na identifikačním modulu (7) jsou vedle individuálních dat účastníka nemanipulovatelně uložena další data k autentizaci, totiž dovolené kmitočty, maximálně přípustné výstupní výkony pro základní stanici (1) a mobilní koncový přístroj (3), přípustné služby a všechny ostatní inicializační parametry, na které chce mít provozovatel sítě vliv a které jsou rámcově implicitními hodnotami pro provoz základní stanice (1) bezdrátového komunikačního systému.

4. Způsob podle některého z nároků 1 až 3, *vyznačující se tím*, že radiové rozhraní základní stanice (4) bezdrátového komunikačního systému pracuje v kmitočtovém spektru veřejného mobilního komunikačního systému.

5. Způsob podle některého z nároků 1 až 4, *vyznačující se tím*, že na radiovém rozhraní se používá kódování přenášených dat.

6. Způsob podle některého z nároků 1 až 5, *vyznačující se tím*, že základní stanice (1) obsahuje časovací jednotku, která je provozovatelem sítě naprogramována na určitý čas, a která se při oprávněném použití základní stanice (1) účastníkem vždy automaticky vynuluje, přičemž základní stanice při nepoužití, tzn. po uplynutí doby naprogramované v časovací jednotce ztrácí oprávnění uvádět svůj vysílač do provozu na kmitočtech mobilního komunikačního systému.

7. Způsob podle nároku 6, *vyznačující se tím*, že při automatickém odpojení základní stanice (1) uplynutím času časovací jednotky je navržena možnost nouzového obnovení provozu.

8. Způsob podle nároku 7, *vyznačující se tím*, že nouzové obnovení provozu základní stanice (1) je možné jenom uvnitř definovaného časového okénka.

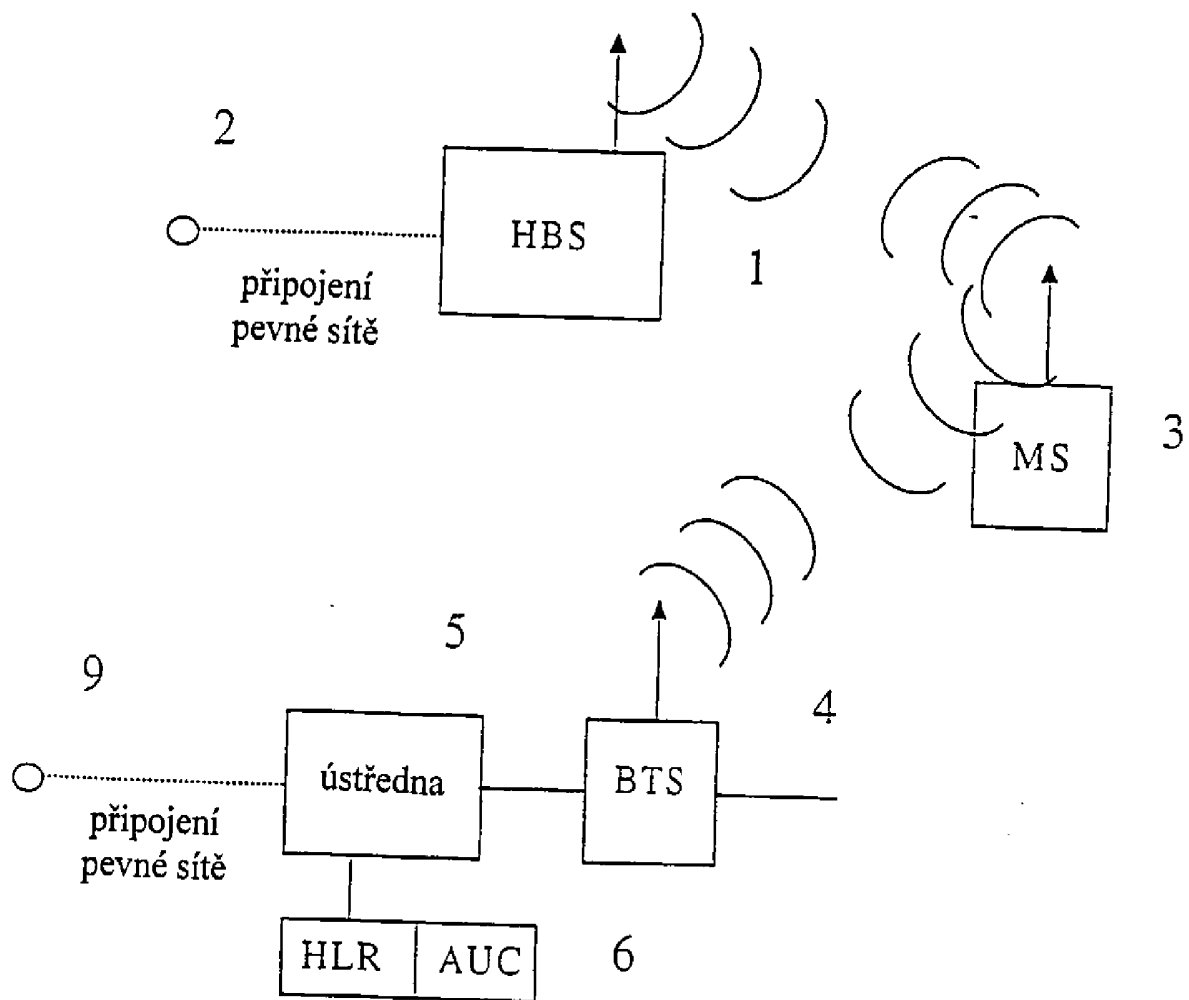
9. Bezdrátový komunikační systém k provozu mobilního koncového přístroje (3) veřejného mobilního komunikačního systému, se základní stanicí (1), která je spojená s veřejnou pevnou sítí (2) a která je na radiovém rozhraní kompatibilní s mobilním komunikačním systémem, který má alespoň jednu funkci k autentizaci, *vyznačující se*

čtecím/zapisovacím zařízením, umístěným v základní stanici (1), ke čtení /zapisování informací z/na alespoň jeden identifikační modul (7), přičemž rozsahy dat identifikačního modulu (7), použitého v základní stanici (1), jsou identické s daty, uloženými na čipové kartě (SIM) mobilního koncového přístroje (3) s oprávněním k přístupu, a

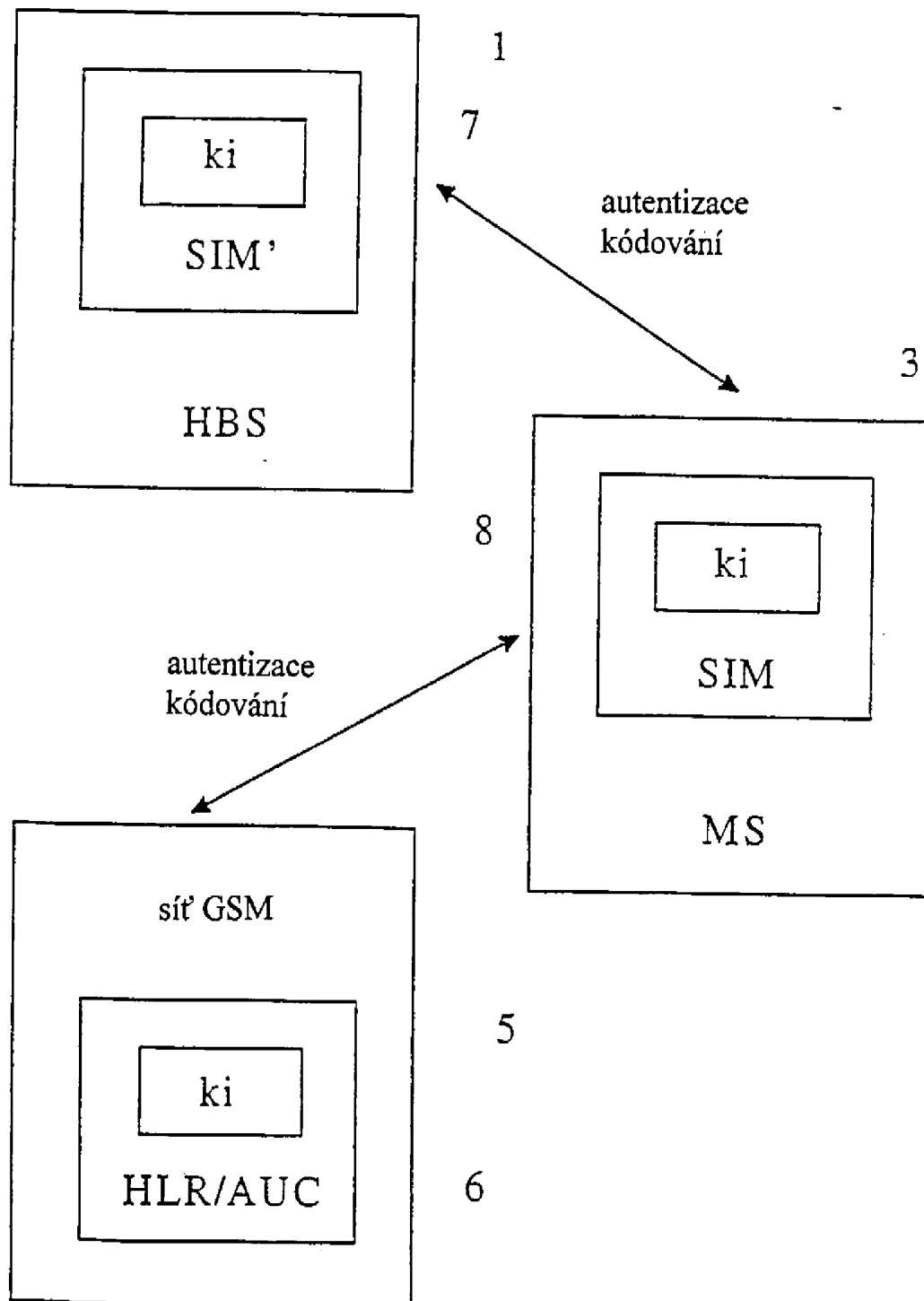
programovým vybavením, implementovaným v základní stanici (1), ke zpracování čtených dat a k autentizaci mobilního koncového přístroje (3) vůči základní stanici (1) na základě dat, čtených a zpracovávaných identifikačním modulem (7), přičemž základní stanice (1) vnímá stejné funkce a úlohy, jako domovský registr popř. opravňovací ústředna mobilního komunikačního systému.

10. Bezdrátový komunikační systém podle nároku 9,

vyznačující se tím, že jako identifikační modul (7) se používají čipové karty (SIM), jako např. podle ISO ID-1, ID-000, DCS 1800, PCS 1900, které se obvykle používají v mobilních komunikačních systémech.



obr. 1



obr. 2