PŘIHLÁŠKA VYNÁLEZU

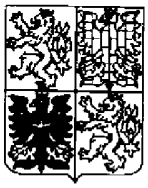
zveřejněná podle § 31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:
2000 - 309

(13) Druh dokumentu: **A3**

(51) Int. Cl. [7]:
H 04 Q 7/00

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **25.05.1999**

(32) Datum podání prioritní přihlášky: **26.05.1998**

(31) Číslo prioritní přihlášky: **1998/19823532**

(33) Země priority: **DE**

(40) Datum zveřejnění přihlášky vynálezu: **14.06.2000**
(Věstník č. 6/2000)

(86) PCT číslo: **PCT/DE99/01531**

(87) PCT číslo zveřejnění: **WO99/62275**

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

(72) Původce:
Dupré Michael, Sankt Augustin, DE;

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

(54) Název přihlášky vynálezu:

Způsob řízení modulu identifikace uživatele (SIM) v mobilním radiotelefonním systému

(57) Anotace:

Způsob spočívá v tom, že mobilní radiotelefonní síť vysílá na modul identifikace uživatele jednu nebo několik řídících hodnot, které v modulu identifikace uživatele spouštějí určité akce nebo procesy, přičemž jako řídící hodnoty se používají určitá náhodná čísla (řídící RAND), vysílaná mobilní radiotelefonní sítí na modul identifikace uživatele kvůli řádné autentifikaci.

CZ 2000 - 309 A3

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

ZPŮSOB ŘÍZENÍ MODULU IDENTIFIKACE ~~ÚČASTNÍKA~~ UŽIVATELE (SIM) V MOBILNÍCH RADIOTELEFONNÍCH SYSTÉMECH

Oblast techniky

Vynález se týká způsobu řízení modulu identifikace účastníka (SIM) v mobilním radiotelefonním systému podle úvodní části patentového nároku 1.

Dosavadní stav techniky

Mobilní stanice se skládají z mobilního radiotelefonního koncového přístroje, který je příslušný pro všechny radiově a přenosově technické úkoly, a z modulu identifikace uživatele (SIM: Subscriber Identity Module), který se s ním nechá spojit, většinou na způsob čipové karty, která zakládá poměr účastníka k provozovateli mobilní radiotelefonní sítě. Na SIM se ukládají důležitá individuální data účastníka, která umožňují využití služeb mobilní radiotelefonie. SIM obsahuje identifikaci mezinárodního uživatele (IMSI), individuální a tajný kód účastníka (Ki), autentifikační algoritmus (A3), algoritmus pro generování šifrovacího klíče (A8), osobní identifikační číslo (PIN) a jiná permanentní jakož i dočasná data. SIM se v takzvaném centru personalistiky provozovatele mobilní radiotelefonní sítě spolu s IMSI, Ki atd. přidělují a odevzdávají účastníkům. Změna dat, permanentně uložených na SIM kartě, např. pro update-procedury nebo zlepšení ohledně bezpečnosti, potom už obecně není možná, nebo nanejvýše

ještě v centru personalistiky. Pokud je třeba změnit SIM-data velkého počtu účastníků, je to velmi pracovně a finančně nákladné.

Podstata vynálezu

Úkol vynálezu spočívá v tom, navrhnout způsob k řízení modulu identifikace uživatele (SIM) v mobilním radiotelefonním systému, který splňuje vysoké požadavky na bezpečnost a nechá se jednoduše realizovat.

Úkol se řeší znaky patentového nároku 1.

Vynález spočívá v tom, že mobilní radiotelefonní síť vysílá na modul identifikace účastníka jednu nebo několik řídicích hodnot, které spouští určité akce nebo procesy v modulu identifikace účastníka, přičemž jako řídicí hodnoty se používají určitá náhodná čísla (řídicí RAND), která se vysílají mobilní radiotelefonní sítí na modul identifikace uživatele kvůli řádné autentifikaci.

V modulu identifikace uživatele se přitom před spuštěním akce nebo procesu uskutečňuje přezkoušení těchto doporučených řídicích hodnot (řídicích RAND), přičemž se řídicí hodnoty porovnávají s určitými porovnávacími hodnotami (porovnávací RAND), které jsou k dispozici na SIM. Na SIM je za tím účelem k dispozici alespoň jedna porovnávací hodnota, která je buď uložená jako pevná veličina, nebo se může vypočítat. Řídicí/porovnávací RAND se vyznačují např. tím, že se stanovují podle bezpečnostních algoritmů A3/A8, implementovaných na SIM, jako funkce tajného kódu Ki a/nebo dalších pevně uložených veličin. Aby

se porovnání mohlo provádět rychle, může se porovnávací hodnota ukládat na SIM.

Dále se navrhuje, že se pro každou SIM rezervuje několik řídicích hodnot, které spouští právě určitou akci nebo určitý proces na SIM. Řada přípustných řídicích hodnot se drží na vhodném místě mobilní radiotelefonní sítě, např. v autentifikační ústředně (AC), přičemž tyto řídicí hodnoty jsou přiřazeny vždy určitému SIM a určité akci, kterou je třeba vyvolat.

Ke zvýšení bezpečnosti v mobilní radiotelefonní síti může na SIM být např. uloženo několik různých bezpečnostních algoritmů A3/A8, mezi kterými se může přepínat pomocí příjmu příslušné řídicí hodnoty.

Rovněž je možné, že na SIM-kartě je uloženo několik tajných kódů Ki, nebo se mohou odvodit z jednoho, tam uloženého Ki, a může se mezi nimi přepínat pomocí příjmu příslušné řídicí hodnoty.

Každá akce nebo proces, které je třeba spustit, se přitom mohou spouštět nejenom jediným řídicím RAND, nýbrž také pomocí řídicího RAND ze skupiny několika řídicích RAND. Přitom se používá jenom část řídicích RAND, takže se řídicí RAND, která následují po sobě, od sebe odlišují, ale mají společné řídicí bity.

Předností vynálezu je, že takové "dálkové řízení" akcí nebo procesů se na SIM nemusí přenášet žádné dodatečné řídicí hodnoty, které by se ostatně nechaly lehce identifikovat a zneužít. Použití náhodného čísla, které se přenáší při každé autentifikaci, jako řídicí hodnoty, činí

toto jako takové nerozpoznatelné. Řídicí hodnoty se objevují jako "běžné" RAND-hodnoty, které se vysílají sítí k SIM k autentifikaci. Také není třeba žádná změna GSM-protokolů.

Příklady provedení vynálezu

Vynález bude blíže vysvětlen prostřednictvím konkrétních příkladů provedení. Přitom vychází najevo další znaky a přednosti vynálezu.

Proces autentifikace uvnitř GSM-mobilních radiotelefonních systémů se uskutečňuje tím, že autentifikační ústředna AC mobilní radiotelefonní sítě posílá na SIM náhodné číslo RAND, a tento vypočítá pomocí algoritmu A3/A8 a tajného kódu Ki výsledek SRES´=A3/A8(Ki,RAND) a posílá ho na AC zpět. AC rovněž zná tajný kód Ki. Vypočítá podle stejného algoritmu A3/A8 hodnotu SRES a porovnává tuto hodnotu s hodnotou SRES´, poskytnutou SIM. Při shodě obou hodnot platí SIM za autentifikovaný.

SIM-karta má nyní dva různé, nebo také více algoritmů A3/A8, které mají stejná rozhraní směrem ven, při stejné délce RAND, Ki a SRES. SIM přitom může mít jenom jeden Ki, nebo na jeden algoritmus A3/A8 jeden vlastní Ki.

Pokud by provozovatel sítě chtěl, např. z bezpečnostních důvodů, měnit používaný algoritmus A3/A8, může přimět autentifikační ústřednu AC, aby vytvořila speciální náhodné číslo RAND, které zároveň představuje řídicí hodnotu podle vynálezu, která se dále také označuje jako řídicí RAND. Řídicí RAND spouští přepnutí algoritmu

A3/A8 v SIM-kartě. Hodnoty pro SRES, spočítané AC pro autentifikaci, se již zakládají na novém algoritmu, který se používá na řídicí RAND. Řídicí RAND tedy slouží jednak k regulární autentifikaci SIM a jednak k přepnutí používaných algoritmů kódování A3/A8.

RAND, které slouží jako řídicí RAND, by mělo být individuální pro kartu a bezpečné. Proto se může např. hodnota, která vyplývá z A3/A8(Ki, Ki), používat jako řídicí RAND. Hodnota A3/A8(Ki, Ki) je individuální pro kartu a není známá nikomu, kdo nezná Ki. K vypočítání náhodného čísla RAND pro řídicí funkce se tedy používá Ki, který je znám jenom SIM a síti. Je postačující, řídit Ki jenom jednou částí této hodnoty, aby se nemusely používat všechny bity této hodnoty. Řídicí RAND je potom např. každé RAND, jehož prvních n bitů souhlasí s bity hodnoty A3/A8(Ki, Ki).

Hodnota A3/A8(Ki, Ki) se může vypočítat a bezpečně uložit už při přidělování karty. Před každou autentifikací se u RAND, vysílaného AC, odmaskují nepoužité bity, a výsledek se porovnává s hodnotou řídicího RAND, spočítanou na SIM a popř. tam bezpečně uloženou. Pokud se porovnávací hodnota, vypočítaná kartou, shoduje s přijímaným řídicím RAND, je řídicí RAND autentifikováno a může na SIM spustit přiřazené akce nebo procesy. Pokud je algoritmus A3/A8 již vyměněn, uskutečňuje se normální autentifikační procedura. Ještě jednou přijaté řídicí RAND stejné skupiny řídicích RAND se už jako takové nezohledňuje.

AC zpravidla vytváří náhodné číslo RAND, vysílané na SIM k autentifikaci, čistě náhodně. Pokud je počet n použitých bitů řídicího RAND dostatečně velký, můžeme se zříci zkoušení, zda náhodně vytvořené RAND je rezervované

řídicí RAND, nebo není. Pokud se hodnota n zvolí příliš velká, je potom nepravděpodobné, že AC náhodně vytváří pro každodenní autentifikaci RAND, které souhlasí s rezervovaným řídicím RAND. Pokud se má algoritmus změnit, měla by AC provést autentifikaci několikrát za sebou s řídicími RAND, aby bylo také při problémech se spojením jisté, že SIM také obsahuje toto řídicí RAND.

Pokud se uskutečňuje autentifikace nad registrem cizích lokací VLR, bude tento nejdříve dále používat své staré, od HLR získané autentifikační triplety, a někdy se použije řídicí RAND, předem dané od HLR popř. AC. VLR není známo, že se jedná o řídicí RAND. Teprve potom SIM přepne algoritmus. Okamžik přepnutí v SIM tedy leží podle okolností zřetelně později než okamžik přepnutí v AC. Pokud účastník střídá ve své domovské síti VLR, RAND-/SRES-hodnoty, uložené v posledním VLR se přebírají a dále se používají. Střídání, nebo několikanásobná změna VLR proto není kritická a nezpožďuje přepnutí algoritmu v SIM.

Stejným způsobem se může v SIM střídat i tajný kód Ki. K tomu může být nový Ki už bezpečně uložen na SIM, nebo se může odvozovat ze starého Ki pomocí definovaného způsobu výpočtu.

Řídicí RAND, potřebná k přepínání Ki, se odlišují ve své hodnotě od řídicích RAND pro přepínání algoritmu A3/A8 a mohou se např. odvodit podle jiného matematického postupu. Řídicí RAND se může skládat z prvních n bitů výsledku z A3/A8(Ki, Ki, XOR Z), přičemž Z je libovolná ale pevná hodnota, která je uložena na SIM.

AC musí již po vytvoření prvního řídicího RAND dále pracovat s novou hodnotou Ki, a také SIM používá nový Ki již pro autentifikaci, která se má rovněž provádět s přijímaným řídicím RAND.

Zastupuje:
Dr. Miloš Všetečka v.r.

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

PATENTOVÉ NÁROKY

1. Způsob řízení modulu identifikace uživatele (SIM) v mobilním radiotelefonním systému, ***vyznačující se tím***, že mobilní radiotelefonní síť vysílá jednu nebo několik řídicích hodnot na modul identifikace uživatele, které spouští určité akce nebo procesy v modulu identifikace uživatele, přičemž jako řídicí hodnoty se používají určitá náhodná čísla (řídicí RAND), která se posílají od mobilní radiotelefonní sítě na modul identifikace účastníka kvůli regulérní autentifikaci.

2. Způsob podle nároku 1, ***vyznačující se tím***, že pro spuštění akce nebo procesu se používá skupina rozdílných řídicích hodnot.

3. Způsob podle nároku 1, ***vyznačující se tím***, že řídicí hodnota spouští několik různých akcí nebo procesů.

4. Způsob podle některého z nároků 1 až 3, ***vyznačující se tím***, že v modulu uživatele se před spuštěním akce nebo procesu uskutečňuje přezkoušení těchto přijatých řídicích hodnot (řídicí RAND), při kterém se řídicí hodnoty porovnávají s porovnávacími hodnotami (porovnávací RAND), které jsou k dispozici na SIM.

5. Způsob podle některého z nároků 1 až 4, ***vyznačující se tím***, že porovnávací hodnoty jsou pevně uložené na SIM.

6. Způsob podle některého z nároků 1 až 5,

vyznačující se tím, že porovnávací hodnoty se počítají pomocí dat, uložených na SIM.

7. Způsob podle některého z nároků 1 až 6, ***vyznačující se tím***, že porovnávací hodnota se stanovuje z bezpečnostních algoritmů A3/A8, které jsou implementované na SIM, jako funkce tajného kódu Ki a/nebo dalších, pevně uložených veličin Z.

8. Způsob podle některého z nároků 1 až 7, ***vyznačující se tím***, že pro každý SIM je rezervováno několik řídicích hodnot, které na SIM spouští právě určitou akci nebo určitý proces.

9. Způsob podle některého z nároků 1 až 8, ***vyznačující se tím***, že na vhodném místě mobilní radiotelefonní sítě se udržuje řada přípustných řídicích hodnot, které jsou přiřazeny právě určitým SIM a určitým akcím.

10. Modul identifikace uživatele (SIM) k používání pro způsob podle některého z nároků 1 až 9, ***vyznačující se tím***, že je na něm bezpečně uložena alespoň jedna porovnávací hodnota (porovnávací RAND), nebo se může spočítat pomocí, na něm uložených, dat.

11. Modul identifikace uživatele (SIM) podle nároku 10, ***vyznačující se tím***, že z bezpečnostních algoritmů A3/A8, implementovaných na SIM, se nechá stanovit porovnávací hodnota jako funkce tajného kódu a/nebo dalších, pevně uložených, veličin Z.

12. Modul identifikace uživatele (SIM) podle některého

z nároků 10 nebo 11, ***vyznačující se tím***, že na SIM je uloženo několik různých bezpečnostních algoritmů A3/A8, mezi kterými může pomocí příjmu příslušné řídicí hodnoty docházet k přepínání.

13. Modul identifikace uživatele (SIM) podle některého z nároků 10 nebo 11, ***vyznačující se tím***, že na kartě je uloženo několik tajných klíčů Ki, nebo se z jednoho Ki, tam uloženého, nechá odvodit, mezi kterými má docházet k přepnutí pomocí příjmu příslušné řídicí hodnoty.

Zastupuje:
Dr. Miloš Všetečka v.r.