

(19)



(10)

LT 4561 B

(12)

PATENTO APRAŠYMAS

(11) Patento numeris: **4561**

(51) Int. Cl.⁶: **H04Q 7/32**

(21) Paraiškos numeris: **99-002**

(22) Paraiškos padavimo data: **1999 01 04**

(41) Paraiškos paskelbimo data: **1999 05 25**

(45) Patento paskelbimo data: **1999 10 25**

(86) Tarptautinės paraiškos numeris: **PCT/FR97/01089**

(86) Tarptautinės paraiškos padavimo data: **1997 06 17**

(85) Nacionalinės procedūros pradžia: **1999 01 04**

(31, 32, 33) Prioritetas: **96/07697, 1996 06 20, FR**

(72) Išradėjas:

Rafaeel Alos, FR
Jean-Marc Dimech, FR
Marc Porato, FR
Francis Sykes, FR

(73) Patento savininkas:

SAGEM SA, 6, avenue d'Iena, F-75116 Paris, FR

(74) Patentinis patikėtinis:

Marius Jakulis-Jason, 3, A.A.A.Baltic Service Company
Rūdninkų g. 18/2-12, 2001 Vilnius, LT

(54) Pavadinimas:

Mobiliaus radiotelefono terminalas su naudojimo kontrole

(57) Referatas:

Mobiliaus radiotelefono terminalas turi radijo priemonės (7), pritaikytas būti aktyvuotomis mokėjimo kortele (10), mokėjimo kortelę (10), turinčią atmintinę (12) su abonento identifikavimo žodžiu (PIN, IMSI) ir sujungtą su komparatoriaus (11) įvestimi, dar terminalas turi priemonės (4) priimti kortelę (10), kurios sujungtos su radijo priemonėmis (7), priemonės (2) įvedimui konkretaus identifikavimo žodžio (PIN, PINUT), susieto su kortele (10), ir skirtas sujungti su kita komparatoriaus (11) įvestimi, be to, terminalas turi priemonės (3,522,6) jo

suderinimui su kortele (10), kuri skirta valdyti radijo priemonių (7) aktyvavimą pagal abonento identifikavimo žodį, ypač priemones (3) įvesto žodžio (PINUT) perkodavimui.

Mobilaus radiotelefono terminalai yra įprasto vartojimo terminalai, pateikti su skaitliu abonento identifikavimo modulio (SIM) mokėjimo kortelės, identifikuojančios vartotoją ir patvirtintinančios mokėjimą abonentinio mokesčio, susijusio su radijo tinklu. Tokiu būdu mokėjimo kortelė sudaro terminalo elektroninį raktą.

EP 0 639 486 aprašytas radiotelefono terminalas, valdomas SIM kortele, susidedantis iš komparatoriaus įėjimo kodinio vardo patvirtinimui, palyginant su žodžiu SIM kortelės atmintinėje prieš suaktyvinant terminalą.

Toks terminalo vartojimas, be abejo, turi nepatogumų.

Visų pirma, bet koks abonentas, turintis pasisavintą terminalą galėtų kai kuriais atvejais panaudoti jį su savo nuosava SIM kortele. Padaryta nuostata įvesti per terminalo klaviatūrą kodinį identifikavimo žodį kiekvienam abonentui, vadinamą personaliniu identifikavimo numeriu (PIN), bet jis gali kontroliuoti tik jungtinės SIM kortelės vartotoją ir tokiu būdu būti neefektyviu prieš nesąžiningą terminalo vartotoją.

Kitas atvejis galėtų būti terminalo skolinimas neapibrėžtam laikui, pagal dienotvarkę arba ribotam efektyvaus panaudojimo laikotarpiui, pavyzdžiui, viešbučio klientui. Tai turėtų apsaugoti SIM kortelės ir terminalo panaudojimą po šio laikotarpio.

Šio išradimo tikslai - išspręsti šias problemas.

Pagaliau išradimas susijęs su mobilaus radiotelefono terminalu, apimančiu radijo priemones, pritaikytas, kad būtų aktyvuotos mokėjimo kortele, mokėjimo kortelę, turinčią atmintinę su abonento identifikavimo žodžiu ir sujungtą su komparatoriaus įvestimi, terminalas turi priemones kortelės priėmimui, kurios sujungtos su radijo priemonėmis, priemonės įvedimui atitinkamo identifikavimo žodžio, susieto su kortele, ir išdėstytas taip, kad būtų sujungtos su kita komparatoriaus įvestimi, pasižymi tuo, kad

terminalas turi priemones jo suderinimui su kortele, kuri pritaikyta valdyti radijo priemonių aktyvinimą pagal abonento identifikavimo žodį.

5 Tokiu būdu, terminalo - kortelės rinkinio dvi sudedamosios dalys su žodžiu, kurį reikia įvesti, negali būti naudojamos atskirai viena nuo kitos. Neteisėtai pasisavinta arba negaliojanti kortelė negali būti panaudota kitame terminale ir, priešingai, pavogtas terminalas negali būti valdomas jokia kortele.

10 Technikos lygiu mokėjimo kortelė ir įvedimo priemonės funkcionaliai sudarytos iš autonominio valdymo bloko, valdomo radijo priemonėmis, be bet kokių kitų valdymo priemonių.

Pagal išradimą aukščiau paminėtas blokas nebeturi šios autonomijos, nes terminalas turi suderinimo priemones, kurios valdo mokėjimo kortelės veikimą pagal radijo priemones.
15 Tokiu būdu, terminalas yra pritaikytas asmeniniams poreikiams, ir kortelė yra susieta su juo.

Viename įgyvendinimo variante derinimo priemonės be įvedimo priemonių ir kortelės priėmimo priemonių dar sudaro priemonės įvedamo žodžio perkodavimui.

20 Šiame įgyvendinimo variante valdymo bloko autonomija valdoma tuo, kad identifikavimo žodis, nurodantis vartotoją, iš tikrųjų yra fiktyvus ir tampa realiu, t.y. identišku jam atmintinėje, dėl terminalo perkodavimo priemonių privalumo. Todėl kortelė gali aktyvuoti terminalo radijo priemones tik, jei šis terminalas yra tas, kuris
25 atlieka reikalaujamą perkodavimą.

Apibendrinant, kortelė yra suderinta su terminalu, kuris pats yra suderintas su kortele.

Būtent identifikavimo žodis, esantis mokėjimo kortelėje, lieka paslaptimi bet kuriam vartotojui, įgaliojam arba ne, nes PIN žodis, kurį vartotojas įveda, skiriasi nuo to, kuris
30 yra atmintinėje.

Kitame įgyvendinimo variante derinimo priemonės sudaro atmintinė, turinti duomenis, suderintus su duomenimis, esančiais atmintinėje kortelės, valdančios komparatoriaus priemonės, pritaikytas skaityti kortelės atmintinę ir leisti radijo priemonių aktyvumą tik po to, kai minėtas suderinimas patikrintas.

5

Tokiu būdu, suderinimas valdomas labai paprastai.

Išradimas bus geriau suprastas, pridėdant toliau einantį aprašymą pavyzdžio, apimančio du aukščiau paminėtus išradimo įgyvendinimo variantus, ir remiantis pridedamo
10 brėžinio vienintele figūra, kurioje pavaizduota terminalo blokinė schema pagal išradimą su mokėjimo kortele.

Pavaizduotas terminalas, pažymėtas 1, šiuo atveju yra radijo terminalas, pavyzdžiui, korinio tipo telefonas, pavyzdžiui, GSM, turintis klaviatūrą 2 įvedimui (ir surinkimui)
15 vartotojo identifikavimo žodžio, valdančio perkodavimo arba šifravimo matematinį bloką 3, sujungtą prie išvesties su jungtimi/skaitliu 4, pritaikytu priimti mokėjimo kortelės 10 jungtis 14. Perkodavimas bloke 3 šiuo atveju gali būti nustatytas arba pakeistas klaviatūroje terminalo 1 nuomininko, kuris paskolino jį kitiems vartotojams. Kortelė 10 pavaizduota atskirai nuo terminalo 1, trys brūkšniuotos linijos, jungiančios
20 jungtis 4 ir 14, nurodo ryšį, kuris sudarytas kortelės 10 jungimu.

Kortelė turi komparatorių 11, paprastai mikroprocesorių, sujungtą, kai kortelė 10 prijungta, įvesties takeliu su bloko 3 išvestimi per jungtis 4 ir 14. Antras komparatoriaus 11 įvesties takelis sujungtas su kortelės 10, turinčios vartotojo identifikavimo numerį
25 (PIN), pažymėtą 121, atmintine 12, tuo tarpu, kai kiti to paties tipo duomenys, tokie kaip IMSI (tarptautinis mobilaus abonentų identifikavimas) pažymėti 122. Komparatoriaus 11 išvestis valdo terminalo 1 radijo siųstuvo - imtuvo bloko 7 aktyvumą per jungtis 4 ir 14. Be to, radijo bloko 7 aktyvacija/deaktyvacija valdoma komparatoriumi 6, sujungtu įvestyje, iš vienos pusės, su kortelės 10 atmintinės 12 zona 122 (IMSI) ir, iš kitos pusės, su terminalo 1 atmintinės 5 zona 522, taip pat turinčia IMSI duomenis. Bloko 3 ir
30 komparatoriaus 6 funkcijos praktiškai atliekamos mikroprocesoriumi 9.

Kadangi išradimas gali būti panaudotas įvairių tipų terminalams, nes tai nesusiję su terminalo veikimo esme, šiuo atveju radijumi, bet su informacijos išrinkimo valdymu šiai funkcijai, telefono aparatas ir jo jungimo prie radijo bloko 7 schema neparodyta.

5 Dabar bus paaiškintas terminalo 1 veikimas.

Operatorius, nustatęs perkodavimo arba šifravimo raktą ir įrašęs jį į perkodavimo bloką 3, nustato iš tikro PIN, kurį jis žino ir kuris saugomas kortelėje 10, kitą, faktinį PIN, kurį jis perduoda vartotojui ir kuris bus vadinamas PINUT. PINUT gaunamas PIN pakeitimu
10 atvirkštine tvarka. Vartotojas, įdėjęs kortelę 10 į atitinkamo terminalo 1 jungtį 4, įveda į klaviatūrą 2 PINUT, kuris perkoduojamas bloke 3 į PIN, skirtą ir atpažįstamą komparatoriumi 11, kuris valdo radijo bloko 7 aktyvinimą.

Pačios šios komandos nepakanka, šiame pavyzdyje pateikiamos dvi suderinimo
15 priemonės: perkodavimo blokas 3 ir atmintinė 5 su komparatoriumi 6. Tokiu būdu, turi būti aišku, kad kas yra čia nurodyta kaip valdymas komparatoriumi 6 galėtų taip pat būti vadinamas komanda ir kad kituose pavyzdžiuose vienintelės komandos 6 arba 11 pakaktų.

20 Šiuo atveju komparatorius 6 valdo suderinimą tarp atmintinių 522 ir 122 tokiu būdu įgalina radijo bloko 7 aktyvinimą komparatoriumi 11.

Mikroprocesorius 9 taip pat apsaugo nuo bet kokių pasikeitimų PIN arba kitą galimą kodinį žodį valdyti priėjimą prie terminalo.

25

Šiame pavyzdyje mikroprocesorius 9 turi vartojimo skaitytuvą 8 arba skaitiklį, panašų į mokesčio tarifo įrenginį, kuris, pavyzdžiui, skaičiuoja terminalo 1 faktinio panaudojimo trukmę ir kuris palyginimu su ribine reikšme, operatoriaus įvesta į atmintinę 5, neleidžia per kodavimą bloką 3 padaryti skaidriu. Numeris įvestas į klaviatūrą perduodamas į
30 kortelę 10 be pakeitimų.

Tada tik terminalas gali veikti įprastu būdu su kortelės PIN kodu, kuris neprieinamas vartotojui. Kitaip tariant, nuomuotojas sudaro sąlygas grąžinti terminalą 1 į veikimo

būklę be suderinimo, kai terminalas paskolintas, t.y. jis sudaro sąlygas, kad galėtų pats naudoti terminalą, įvedant PIN į atmintinę kortelėje be perkodavimo arba laiko apribojimo.

- 5 Paliekant aukščiau paminėtą uždara būklę, tokiu būdu šiuo atveju nuvedama į paprastą vartojimo veikimo būklę technikos lygiu, kuri gali būti keičiama į būklę su derinimu, aprašytu pradžioje. Perėjimas iš užrakintos būklės į įprasto vartojimo būklę pasiekiamas įvedant tikrą PIN, šis įvedimas nustatomas mikroprocesoriumi 9. Tokiu būdu, terminalo 1 užrakinimas deaktyvuojamas, t.y. terminalas 1 gali veikti su kitomis mokėjimo kortelėmis, perkodavimo blokas 3 tada iš dalies būna permatomas. Tada tuo pačiu būdu 10 mokėjimo kortelė 10 gali veikti su bet kuriuo paprastu vartojimo terminalu.

Išradimo apibrėžtis

1. Mobilaus radiotelefono terminalas, turintis radijo priemones (7), pritaikytas būti
5 aktyvuotomis mokėjimo kortele (10),
- mokėjimo kortelę (10), turinčią atmintinę (12) su abonento identifikavimo žodžiu (PIN, IMSI), sujungtą su komparatoriaus (11) įvestimi,
- terminalas turi priemones (4) priimti kortelę (10), kurios sujungtos su radijo priemonėmis (7), priemones (2) įvedimui konkretaus identifikavimo žodžio (PIN, PINUT), susieto su kortele (10), skirtas sujungti su kita komparatoriaus (11) įvestimi.
10 b e s i s k i r i a n t i s tuo, kad jis turi priemones (3, 522, 6) terminalo derinimui su kortele (10), kuri skirta valdyti radijo priemonių (7) aktyvavimą pagal abonento identifikavimo žodį.
- 15 2. Terminalas pagal 1 punktą, b e s i s k i r i a n t i s tuo, kad derinimo priemonės turi įvedamo žodžio (PINUT) perkodavimo priemones (3), išdėstytas tarp įvedimo priemonių (2) ir kortelės (10) priėmimo priemonių (4).
3. Terminalas pagal 2 punktą, b e s i s k i r i a n t i s tuo, kad perkodavimo priemonės
20 turi mikroprocesorių (9).
4. Terminalas pagal vieną iš 1 - 3 punktų, b e s i s k i r i a n t i s tuo, kad derinimo priemonės turi atmintinę (522), talpinančią duomenis, suderintus su duomenimis (122), esančiais kortelės (10) atmintinėje, ir valdančią komparatoriaus priemones (6).
25 pritaikytas skaityti kortelės (10) atmintinę (12) ir leisti radijo priemonių (7) aktyvinimą tik po to, kai minėtas suderinimas patikrintas.
5. Terminalas pagal vieną iš 2 - 4 punktų, b e s i s k i r i a n t i s tuo, kad mokėjimo tarifo skaitiklis (8) pritaikytas sujungimui su perkodavimo priemonėmis (3).

1/1

