PATENTOVÝ SPIS

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: 1997 - 881

(22) Přihlášeno: 27.10.1994

(30) Právo přednosti:
27.10.1994 WO 1994/EP9403542

(40) Zveřejněno: 14.11.2001
(Věstník č. 11/2001)

(47) Uděleno: 26.09.2001

(24) Oznámeno udělení ve Věstníku: 14.11.2001
(Věstník č. 11/2001)

(86) PCT číslo: PCT/EP94/03542

(87) PCT číslo zveřejnění: WO 96/13920

(11) Číslo dokumentu:

289 189

(13) Druh dokumentu: **B6**

(51) Int. Cl.[7]:
H 04 L 9/32
H 04 Q 7/38

(73) Majitel patentu:
INTERNATIONAL BUSINESS MACHINES CORPORATION, Armonk, NY, US;

(72) Původce vynálezu:
Tsudik Gene, Thalwil, CH;

(74) Zástupce:
Kalenský Petr JUDr., Hálkova 2, Praha 2, 12000;

(54) Název vynálezu:

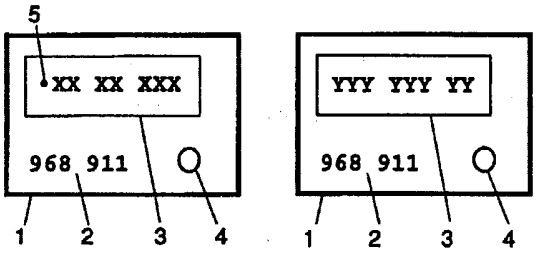
Způsob zajištění identifikace pohyblivého uživatele v komunikačním systému a přenosný vstupní přístroj k provádění tohoto způsobu

(57) Anotace:

Způsob zajištění identifikace pohyblivého uživatele U v komunikačním systému s rozptýlenými uživateli seskupenými do oblastí D_X, D_Y v systému, přičemž každý uživatel má identifikátor A_U a předávací slovo nebo jiný tajný autentizátor PW_U, kde identifikátor A_U a předávací slovo PW_u se uloží v uživatelově místní oblasti D_X, kterýžto způsob obsahuje indikaci synchronizace, přednostně používající indikaci intervalu T_U času, synchronizující vstup uživatele U v cizí oblasti D_Y s jeho místní oblastí D_X. Způsob obsahuje po sobě následující kroky:

- zašifrování pod tajnou funkcí, zvláště jednocestnou funkcí, indikátoru A_U, indikace synchronizace intervalu T_U času a uživatelova předávacího slova PW_u nebo jiného tajného autentizátoru a vyvinutí zašifrovaného dynamického identifikátoru SUid uživatele,
- oznámení místní oblasti D_X uživatele cizí oblasti D_Y, ze které má uživatel U úmysl komunikovat,
- vyslání zašifrovaného identifikátoru SUid do místní oblasti D_X uživatele,
- vyhodnocení zašifrované zprávy v místní oblasti D_X uživatele U a určení správné identity uživatele.

Řešení dále vytváří přenosný vstupní přístroj obsahující programovatelnou kartu (1) k provádění způsobu definovaného výše s rozptýlenými uživateli seskupenými do oblastí D_X, D_Y, dále obsahuje procesor (60) zašifrované zprávy SUid, hodiny (61) připojené k procesoru (60), displej (3), připojený k procesoru (60) a přepínač (4) modu připojený k displeji (3).



CZ 289189 B6

Způsob zajištění identifikace pohyblivého uživatele v komunikačním systému a přenosný vstupní přístroj k provádění tohoto způsobu

Oblast techniky

Vynález se týká komunikace mezi pohyblivými uživateli v počítačové síti. Vynález se dále týká přenosného vstupního přístroje k provádění tohoto způsobu.

Dosavadní stav techniky

V současných komunikačních sítích se pohyblivost uživatele stale velmi rychle významným a populárním činitelem, zejména v bezdrátových nebo buňkových sítích. Ačkoliv je to užitečné a žádoucí, tato zvýšená pohyblivost uživatele vede ke množství významných problémů týkajících se bezpečnosti. Jeden z problémů je schválení nebo přijetí uživatele. Jiným problémem je stopování pohyblivého uživatele.

Typická situace jednotka, t.j. některý uživatel anebo přístroj zaregistrovaný v určité místní oblasti se objeví v jiné, to znamená v cizí oblasti. Cílem uživatele je obdržet určitou službu, když je v cizí oblasti. Protože tento uživatel není známý v cizí oblasti, musí být autentizován a jeho solventnost nebo dobrý stav musí být oznámen úřadu cizí oblasti. V následujícím popise je tento proces označen jako „autentizace“, což je v oboru obvyklé. Jediná jednotka, která je schopna zjistit identitu uživatele a jeho běžný stav, je úřad v jeho místní oblasti. Je několik známých řešení tohoto problému popsaných v dosavadní literatuře, z nichž některé jsou dále uvedeny. Autentizace však není problém, který řeší předložený vynález.

Zde je však zájem o jiný problém, týkající se bezpečnosti a vznikající jako následek pohyblivosti uživatele. Je to důvěryhodnost identity uživatele a jeho pohybů. Ideálně by měl být informován o chování pohyblivého uživatele pouze úřad místní oblasti uživatele. V dalším textu tento proces zjištění identity pohyblivého uživatele, to jest určení, kdo se pokouší získat službu z určité oblasti, se označuje jako „identifikace“.

Ideálně jednotka jiná než uživatel sám a odpovědný úřad v místní oblasti uživatele, to znamená dílčí síť nebo část sítě, ve které uživatel typicky pracuje, by měla znát skutečnou identitu a běžné umístění pohyblivého uživatele. Běžná prostředí umožňující pohyblivost uživatele buď neřeší problém celkově nebo zakládají svá řešení na možnostech technických prostředků uživatelova osobního přístroje.

Obecně je možno říci, že známá řešení tohoto problému daná běžným stavem oboru architektur pohyblivých a buňkových sítí buďto přiměřená nebo jsou příliš specifická pro bezpečné uchování identifikace v tajnosti, jak je dále podrobně vysvětleno.

Jedno ze současně dostupných řešení, které podal M.Rahnema v publikaci (1) v tomto t.zv. GSM systému je, že pohyblivý uživatel je označen jako dočasná jednotka (TMSI v jazyku GSM), když se objeví v cizí oblasti. Nicméně TMSI je pouze označení po počáteční autentizaci pohyblivého uživatele v cizí oblasti, v procesu prováděném uživatelem, uživatelova skutečná identita (IMSI v jazyku GSM) je komunikována v prostředí a může tedy být zachycena vetřelcem a zneužita.

Jiné řešení je popsáno v publikaci (2) na systému „Cellular Digital Packet Data“ (CDPD). Provedení podle systému CDPD je mnohem bezpečnější než výše uvedené řešení GSM. V systému CDPD před tím, než pohyblivý uživatel sdělí svou identitu, vstoupí do klíčovaného protokolu Diffie–Hellman s místním, to znamená s úřadem cizí oblasti. tento protokol popsali W.Diffie a M.Hellman v publikaci (3). Následkem toho obě strany získají možnost sdílení tajného klíče.Rozšifrováním v tomto klíči potom pohyblivý uživatel vyšle svou identitu do úřadu

cizí oblasti. Ač je mnohem bezpečnější než GSM, má toto řešení dvě velké nevýhody. První spočívá v tom, že místní, t.zn. úřad cizí oblasti, odkryje skutečnou identitu pohyblivého uživatele v kontextu CDPD, což není jeho vlastní problém. Nicméně, ideálně by identita pohyblivého uživatele neměla být sdělena úřadu místní oblasti. Pro určení vlastní identity a běžného stavu postačí, když je ověřen nebo potvrzen úřadem místní oblasti. Druhý problém spočívá v podstatě klíče výměnného protokolu Diffie–Hellman. Jeho účelem je sestavit tajný klíč. To umožňuje nějakému vetřelci vydávat se za úřad místní oblasti a spojit se tedy v protokolu výměny klíče s pohyblivým uživatelem a získat sdílený klíč. Když potom pohyblivý uživatel vysílá svou skutečnou identitu zašifrovanou se stejným klíčem, vetřelec bude jednoduše dešifrovat vysílání.

Další řešení uvedli R.Molva a spol. v publikaci (4) a M.Beller a spol. v publikaci (5). Jedna přidružená myšlenka týkající se rozdělení klíčů je popsána v PCT přihlášce vynálezu PCT/EP93/01989 (6) přihlašovatele předmětné přihlášky vynálezu, jiná přidružená myšlenka týkající se klíčového slova nebo změny klíče je popsán v PCT přihlášce vynálezu PCT/EP93/02540 (7) přihlašovatele předmětné přihlášky vynálezu. Souhrnně lze říci, že jsou zde v podstatě tři otázky týkající se problému identity a pohybu pohyblivého uživatele.

Ústřední úloha zachování tajné identity spočívá v zamezení, aby kdokoliv objevil souvislost mezi pohyblivým uživatelem a uživatelem registrovaným ve zvláštní místní oblasti, jinými slovy ústřední úkol spočívá v zachování identity uživatele v tajnosti. Nejsnadnější, spíše intuitivní řešení je přiřazení pohyblivých označení ke každému pohyblivému uživateli nebo přístroji, když se nachází mimo místní oblast. Jak je uvedeno dále, toto označení může být pevné nebo proměnlivé. Hlavním úkolem vynálezu je tudíž vytvořit způsob a zařízení umožňující použití takových označení.

Druhé významné opatření je udržet cizí oblasti „v temnu“. Není–li závazné pro cizí oblast znát skutečnou identitu uživatele, mohlo by postačit libovolné označení. V největším počtu případů musí být takové označení ověřeno úřadem místní oblasti. Je proto dalším úkolem vynálezu navrhnout způsob a zařízení umožňující tok informací v síti bez odhalení identity uživatele cizí oblasti. Ať jsou nebo nejsou označení použita, mohou zde býti důvody, proč úřad cizí oblasti vyžaduje znalost skutečné identity uživatele. V tomto případě může úřad místní oblasti držet identitu uživatele v tajnosti za předpokladu, že dva úřady mají předem vytvořený prostředek pro zajištění komunikace. Nicméně i v takovém případě úřad cizí oblasti nezná identitu uživatele.

Třetí otázka zvláštního zájmu spočívá v zabránění stopování identity nebo korelace. I když pohyblivý uživatel přijme označení pohybu, jeho pohyby mohou být stopovány cizím vetřelcem. To je zejména možné, když označení je statické, to znamená pevné pro danou oblast uživatele nebo permanentně připojené k uvedenému uživateli. Označení tohoto posledního typu je podobné dlouhému klíčovému slovu. Když byly jednou objeveny identita a pohyby uživatele, mohou býti kompromitovány na základě dlouhého výrazu. Je proto dalším úkolem vynálezu zabránit stopování tím, že se systém vytvoří tak, aby byla možná častá změna označení bez potlačení toku informací.

Odkazy:

(1) Rahnema „Overviw of the GSM System and Protocol Architecture“, IEEE Communications Magazine, Duben 1993, sv. 31, Č. 4, str. 92–101.

(2) „Cellular Digital Packet Data (CDPD) System Specification“, release 1.0, 19 Červenec 1993, CDPD Industry Input Coordinator, Costa Mesa, California, USA.

(3) W. Diffie a M. Hellmann: „Nex Directions in Cryptography IEEE Transactions of Information Theory“, Listopad 1976, Sv. 22, Č. 6 str. 644–654.

(4) R. Molva, D. Samfal, G.Tsudik: „Authentication of Mobile Users“, IEEE Network Special Issue on Mobile Communications, jaro 1994, str. 25–35.

(5) M. Beller l. Chang, Y. Yacobi: „Privacy and Authentication on a portable Communications System“, IEEE JSAC, Special Issue on Wireless Personal Communications, Srpen 1993, Sv. 11, Č. 6, str. 821–829.

(6) Přihláška vynálezu PCT/EP93/01989 o názvu „Method and Apparatus for Providing Secure Key Distribution in a Communication System, přihlašovatel IBM Corporation a P.Janson, G.Tsudik.

(7) Přihláška vynálezu PCT/EP93/02540 o názvu Method and system for Changing an Authorization Password or Key in a Distributed Communication System“, přihlašovatel IBM Corporation a R. Hauser, P. Janson, R. Molva, G. Tsudik, E. van Herreweghen.

(8) US National Bureau of Standards: „Federal Information Processing Standards, publikace 46, 1977.

(9) R. Rivest: „The MD5 Message Digest Algorithm“, Internal RFC 1321, Internal Activities Board, Duben 1992.

(10) R. Molva a G. Tsudik: „Authentication Method with Impersonal Token Cards“, 1993 IEEE Symposium on Research in Security and Privacy, Květen 1993, pojednání zveřejněná IEEE Computer Society Press, Los Alamitos, California, USA.

(11) Security Dynamics Technologies, Inc., Cambridge, Massachusetts, USA: „The ACE System Access Control Encryption“, Product information, 1992.

Podstata vynálezu

Předložený vynález obsahuje řešení výše popsaných úkolů. Pro omezení na minimum nebo zabránění možnosti stopování a identifikace pohyblivého uživatele je vytvořen způsob záznamu dočasných jednoduchých označení pro pohyblivé uživatele, který je účinný a není specifický pro zvláštní technické prostředky. Předložený vynález umožňuje jednoduše jednoznačnou a prakticky okamžitou identifikaci pohyblivého uživatele jeho místním úřadem a dále umožňuje, že nepověřená strana není schopna identifikovat pohyblivého uživatele nebo stopovat jeho pohyby.

Ačkoliv vynález vytváří rozumné řešení všech tří výše diskutovaných otázek, je zde určité omezení, které lze těžko obejíti. jedno takové omezení je například potřeba úřadu cizí oblasti poznání identity místní oblasti pohyblivého uživatele. To je pravděpodobně důvod pro řadu prostředí pohyblivých uživatelů, protože náklady vynaložené „vanku“ musí být případně převedeny do místní oblasti. Dále, jak bylo uvedeno výše, pouze místní oblast může objasnit běžný stav uživatele.

(Pro řešení tohoto zvláštního problému by mohlo být zajištěno prostředí systému, kde komunikace mezi úřady oblasti je „anonymizována“ centrální zúčtovací bankou. V tomto případě by bylo výhodné přidělit označení oblastem tak, aby se pohyblivý uživatel mohl obracet na svou místní oblast nějakým označením. Pak by bylo úkolem ústřední zúčtovací banky rozlišit označení oblastí).

Způsob podle vynálezu se pokouší sjednotit dva protichůdné požadavky, autentizaci a identitu současně. Pro autentizaci nějaké jednotky musí nejprve vyžadovat určitou identitu a potom ukázat nebo dokázat, že zná něco, co může mít pouze skutečný nositel této identity.

Důvěryhodnost identity na druhé straně vyžaduje, aby táž identita byla utajena. To má za následek určitou paradoxní situaci, která musí být vyřešena.

Podstata nové metody spočívá ve výpočtu krátkých pohyblivých označení, která dále budou označena jako „dynamické identifikátory uživatele". Uživatel pohybující se mimo svou oblast může předpokládat takové označení a utajit jakýkoli vztah k vlastní identitě. To je také případ, kdy cizí oblast (nebo nepověřená strana) provádí činnost pro odhalení klíčového slova pohyblivého uživatele.

Seznam použitých symbolů

D_X	jméno oblasti,
AS_X	úřad oblasti D_X, typicky autentizační server,
U	pohyblivý uživatel domovem v oblasti D_X,
U_X	skutečné jméno pohyblivého uživatele U,
A_u	znamení nebo identifikátor pohyblivého uživatele U,
PW_U	klíčové slovo uživatele U,
SUid	dynamický identifikátor uživatele,
δ_X	časový interval oblasti x,
T_u	indikátor časového intervalu, t.zn. současný čas uživatele U zaokrouhlený na nejbližší hodnotu δ_X.

Přehled obrázků na výkresech

Vynález je znázorněn na výkresech, kde obr. 1 je programovatelná karta použitelná pro tento vynález v obou jejích modech, obr. 2 je příklad pro tok informací z programovatelné karty do místního úřadu uživatele, obr. 3 je síť se dvěma oblastmi pro předvedení použití vynálezu, obr. 4 je příklad pro organizaci procesu místního úřadu a obr. 5 je příklad pro proces u pracoviště cizího vstupu nebo terminálu.

Příklady provedení vynálezu

Na začátku je každý pohyblivý uživatel U označen identifikátorem A_U přídavně k jeho stále identitě. V zásadě by identifikátor A_U uživatele U neměl být odlišný od skutečného jména U_X uživatele. Bezpečnost schématu nezávisí na identifikátoru A_U uživatele, které je tajné. V prostředí, kde každý uživatel U je vybaven programovatelnou kartou nebo podobným přístrojem, identifikátor A_U uživatele může být pouze sériové číslo nějakého jiného jednotného identifikátoru uživatelova přístroje. Seznam těchto pohyblivých identifikátorů A_U je udržován úřadem AS_X místní oblasti D_X a obsahuje předávací slova PW_u a popřípadě jiné informace o uživateli U.

Pro každou místní oblast D_X je zvolen interval δ_X prázdného času oblasti. Tento časový interval δ_X může být poměrně dlouhý, například několik hodin nebo dnů.

Když se uživatel U, jehož místní oblast je D_X, pohybuje do cizí oblasti D_Y, je nejprve třeba, aby byl identifikován (a autentizován). Potom pro něj může být proveden dočasný záznam v cizí oblasti D_Y, aby byly usnadněny následující přístupy v této cizí oblasti D_Y. Jinými slovy, když uživatel plánuje setrvání v cizí oblasti D_Y po určitou dobu, může být výhodné vytvořit pro něho určitý dočasný „domov", místo aby se provedlo spojení s uživatelovou místní oblastí D_X při každém přístupu. To je však právě jedna z dalších možností. Hlavním cílem předloženého vynálezu je identifikace uživatele U.

Podrobný popis protokol pro autentizaci uživatele U může být nalezen v publikaci (4) (Molva). Přesný formát toků autentizace není důležitý v souvislosti s předloženým vynálezem. Bez ohledu na specifika autentizace musí být identita uživatele U sdělena jeho úřadu AS_X místní oblasti D_X. Protože uživatel U nemůže přímo komunikovat s úřadem AS_X místní oblasti D_X, veškerá komunikace má procházet přes cizí úřad AS_Y. To je znázorněno na obr. 2, který bude dále popsán.

Protokol autentizace může předcházet záměna klíče podle Diffie–Hellmana, jak je popsána ve výše uvedené publikaci (2) (CDPD System Specification). V tomto případě se celá procedura stane odolnou proti pasivním vetřelcům, protože všechny zprávy mohou být zašifrovány použitím nového klíče.

Obecně musí tok identifikace obsahovat dynamický identifikátor SUid uživatele U. To je pravdivé jak pro (první) tok z uživatelovy programovatelné karty do cizího úřadu AS_Y, tak i pro (druhý) tok z cizího úřadu AS_Y do uživatelova místního úřadu AS_X. Dynamická identifikace uživatele může spočívat na přímém odbočení dynamického identifikátoru SUid uživatele U nebo na zašifrované verzi dynamického identifikátoru SUid uživatele U.

Myšlenka protokolu s ohledem na důvěryhodnost uživatelovy identity je výpočet dynamického identifikátoru SUid uživatele U.

Vypočítá se jako

$$SUid = F(A_U, T_U, PW_U)$$

kde F je silná jednocestná funkce. Příklady jsou DES popsané v Publication 46 úřadu National Bureau of Standards, viz (8) výše pod „odkazy“ nebo MD5, jež publikoval Rivest v (7). V případě DES nebo jiné funkci na bázi zašifrování je důležité uvést, že není nutný přídavný tajný klíč pro výpočet funkce F, protože předávací slovo PW_U uživatele U je pro tento účel dostačující. Indikátor časového intervalu T_U je běžný čas zaokrouhlený na nejbližší hodnotu δ. Není–li uživatel U vybaven přístrojem podobným programovatelné kartě, vstoupí svým předávacím slovem PW_U do veřejného pracoviště nebo jiného podobného terminálu, to znamená do vstupního přístroje k cizímu úřadu AS_Y cizí oblasti D_Y. Pro uživatele vázaného programovatelnou kartou může být předávací slovo PW_u uživatele U buď 1. silný klíč v programovatelné kartě (pro takové programovatelné karty, které nemají klávesnici nebo jiný prostředek pro vstup), nebo 2. kombinace klíče programovatelné karty a předávajícího slova PW_u uživatele U (pro programovatelné karty s možnostmi vstupu).

Jak bylo uvedeno, hodnota dynamického identifikátoru SUid uživatele U není pro úřad AS_Y cizí oblasti D_Y přístupná. Jediná informace, kterou cizí úřad AS_Y může získat je skutečnost, že pohyblivý uživatel U je zaznamenán v místní oblasti D_X. Ve druhém toku cizí úřad AS_Y cizí oblasti D_Y vysílá dynamický identifikátor SUid uživatele U (s jinou, například autentizační informací) místnímu úřadu AS_X místní oblasti D_X žádaného uživatelem.

Otázka je, jak místní úřad AS_X místní oblasti D_X určí, že dynamický identifikátor SUid uživatele U odpovídá místně zaznamenanému uživateli U. To se provádí udržováním datové tabulky, která pro každého uživatele U zaznamenává příslušnou hodnotu dynamického identifikátoru SUid. Tento předklad tabulky vztahů se vypočítává po každém intervalu δ_X. Protože místní úřad AS_X místní oblasti D_X již ukládá identifikátor A_U pohyblivého uživatele U a předávací slovo PW_U pro každého uživatele U, má všechny nutné informace pro výpočet překládacích tabulek dat.

Je třeba poznamenat, že jestliže dynamické identifikátory SUid nezávisí na běžném umístění uživatele U, překládací tabulky mohou být předem vypočítány mimo linku a v budoucnosti použity. To je zejména v tom případě, kdy je použita poměrně velká hodnota intervalu δ_X například 1 hodina nebo 1 den, jak bylo uvedeno výše.

Vytvoření „skutečné“ identity pohyblivého uživatele U je pouze polovina činnosti. Místní úřad AS_X místní oblasti D_X musí potom ověřit informaci autentizace přiváděnou v druhém toku. To však se stávajícím problémem nesouvisí. jak bylo uvedeno výše, Molva a spol. popisující příklad v publikaci (4).

Následující část popisuje výhodné uspořádání, aby se snížil „přebytek výpočetních operací“. V prostředí, kde se pohybuje pouze malý počet uživatelů mimo jejich místní oblast, může být velmi neúčinné a dokonce škodlivé předem vypočítávat, udržovat a prohlížet na čase závislé tabulky pro všechny uživatele. V tomto případě cesta ke snížení přebytku výpočetních operací spočívá v tom, že se obecně na uživateli U žádá, aby informoval místní úřad AS_X své místní oblasti D_X o budoucím předpokládaném pohybu. Místní úřad AS_X musí stopovat pouze ony uživatele, kteří se běžně pohybují. To nezahrnuje nutnost, aby uživatel U popisoval všechny své budoucí pohyby. Musí pouze zaznamenat začátek každé cesty „ven“, totiž do cizí oblasti D_Y. Po zaznamenání místní úřad AS_X místní oblasti D_X zapíše pohyblivého uživatele U do zvláštního seznamu, který je používán pro výpočet dynamického identifikátoru SUid na bázi času. není však nutné, aby uživatel informoval místní úřad AS_X místní oblasti D_X o dokončení každé cesty, místní úřad AS_X místní oblasti D_X může dedukovat, že určitý uživatel U se vrátil do místní oblasti D_X, když se tento uživatel U pokusí navázat komunikaci se svým skutečným, to je místním uživatelem ID u místního úřadu AS_X místní oblasti D_X.

V následující části je popsána synchronizace hodin mezi místním úřadem AS_X místní oblasti D_X a cizím úřadem AS_Y cizí oblasti D_Y. Předpoklad o uživateli U udržujícím primární hodiny volně synchronizované s místním úřadem AS_X místní oblasti D_X je jistě reálný pro většinu prostředí. je jasné, že uživatel U vybavený programovatelnou kartou se může spolehnout na hodiny programovatelné karty pro udržování indikátoru intervalu Tu času. Pro „nevybaveného“ uživatele postačí hodiny nějakého pracoviště. je také možné, aby uživatel zadal čas ručně z nástěnných nebo náramkových hodin. Zrnitost δ_X je rozhodující. Nehledě na toto jednoduché udržování indikátoru intervalu T_U času uživatele je zřejmé, že v některých případech udržování stopování indikátoru časového intervalu T_U uživatele není z nějakých důvodů možné.

Pro ovládnutí této situace může být protokol modifikován tak, že 1. cizí úřad AS_Y místní (t.zn. cizí) oblasti D_Y zajišťuje indikátor časového intervalu T_U, nebo 2. místní úřad AS_X uživatelovy místní oblasti D_X jej zajišťuje v každém případě, kdy musí být zaveden čas do uživatelova přístroje a priori, to znamená ve zvláštním toku předcházejícímu první tok popsaný výše. To může býti provedeno v otevřeném, to znamená v jasném textu, protože čas T_X není tajná hodnota.

V souhrnu, jak bylo ukázáno výše, nejvýznamnější činitel v pohybu inkognito je mít často proměnlivé a náležité nezávislé označení, t.j. dynamické identifikátory SUid uživatele U. Používají–li se stále nebo dlouhé identifikátory, umožní se korelace identity a stopování. V ideálním případě je dynamický identifikátor SUid plně použitelný pouze jednou. Způsob podle vynálezu není úplně v souladu s uvedenou normou, protože umožňuje opětně používat označení uvnitř uspořádaného časového intervalu δ_X. Jestliže tedy uživatel U prochází několika oblastmi v jediném intervalu δ_X, je vystaven určitému omezenému stopování identity.

Aby se tomu předešlo, vytváří vynález dva alternativní přístupy.

1. Označení jsou závislá na navštívené oblasti, nebo

2. Je udržována těsná synchronizace mezi uživatelem U a místním úřadem AS_X jeho místní oblasti D_X.

Je–li jméno cizí oblasti D_Y zahrnuto do výpočtu dynamického identifikátoru SUid uživatele U, korelace identity není možná, protože pohyb uživatele z jedné cizí oblasti D_Y do jiné cizí oblasti

D_Y (i ve velmi krátkém čase, t.j. v jediném časovém intervalu δ_X) se provede při nezávislých dynamických identifikátorech SUid uživatele U. Hlavní nedostatek tohoto přístupu spočívá v tom, že vyžaduje více času. Protože v tomto případě místní úřad AS_X místní oblasti D_X není schopen předvídat pohyby uživatele U, nemůže předem vypočítat překládací tabulky. Když je tedy místní úřad AS_X místní oblasti D_X seznámen s dynamickým identifikátorem Sud uživatele U a se jménem cizího úřadu AS_Y cizí oblasti D_Y, není schopen bezprostředně určit dynamický identifikátor SUid uživatele U a přímo odpovědět, protože zde není předem vypočítaná uložená překládací tabulka. Pro každého registrovaného uživatele U místní úřad AS_X místní oblasti D_X musí vypočítat příslušnou hodnotu dynamického identifikátoru SUid uživatele U použitím jména cizí oblasti D_Y jako jednoho vstupu. To způsobuje podstatné zatížení místního úřadu AS_X místní oblasti D_X.

Jiná možnost je udržovat těsnou synchronizaci mezi uživatelem (či spíše osobním přístrojem uživatele) a místním úřadem AS_X místní oblasti D_X. tato synchronizace může být na bázi času, tajné posloupnosti čísel nebo identicky nasazených generátorů náhodných čísel. tento přístup dává nejvyšší úroveň bezpečnosti, protože zaručuje, že nějaké označení nebo dynamický identifikátor SUid uživatele U není nikdy opětně použit. Tento přístup však trpí stejným nedostatkem jako označení závislá na oblasti. Dále vyžaduje, aby každý uživatel U měl spolehlivý přístroj bezpečný proti poruchám.

Popsaná označení na bázi času mohou být uskutečněna v prostředích orientovaných na přístroj, například programovatelné karty, buňkové telefony nebo v tradičních prostředích, kde pohyblivý uživatel U má pouze nějaké předávací slovo PW_u pro autentizaci. V druhém případě nemá uživatel U možnost protiopatření proti napadení veřejnými pracovišti nebo jinými neosobními koncovými uživatelskými zařízeními, která jsou použitelná pro přístup do sítě. Dále je uveden jeden přednostní příklad použití vynálezu.

Zvláště výhodné použití vynálezu je ve spojení s programovatelnými kartami. Nejjednodušší možná programovatelná karta je taková, která má pouze malý displej a jeden zapínací a vypínací přepínač. Uvnitř bezpečnostního obalu má programovatelná karta hodiny a tajný klíč jednotný pro každou kartu. Tento typ programovatelné karty popsali R. Molva a spol. v publikaci (10). Komerční výrobek, který by mohl být přizpůsoben pro práci v tomto modu je Secure ID popsaný v publikaci (11).

Obr. 1 až obr. 5 znázorňují provedení vynálezu s programovatelnými kartami v grafické formě. Následující popis udává podrobnosti.

Programovací karta 1 znázorněná na obr. 1 obsahuje sériové číslo 2, které je obvykle připojeno pevně k programovatelné kartě 1 a je jednotné. Programovatelná karta 1 rovněž obsahuje procesor 60 a displej 3, často malý displej s tekutým krystalem. Všechny tyto přístroje jsou napájeny z baterie. Jak bude vysvětleno dále, programovatelná karta 1 má dva odlišné mody. Pro provádění dynamické identifikace uživatele U metodu založenou na čase jsou učiněna tato opatření:

1. Programovatelná karta 1 je programována pro spínání buď samočinně nebo na žádost mezi dvěma mody, jedním „modem autentizace“, ve kterém programovatelná karta 1 znázorňuje na displeji 3 autentizátor (zde nevýznamný, jak bylo vysvětleno výše) a „modus ID uživatele“, ve kterém programovatelná karta 1 zobrazuje dynamický identifikátor SUid uživatele U. Samočinné spínání nastává ve stejných časových intervalech, například vždy za 10 sekund. Automaticky spínaná programovatelná karta 1 je zvláště výhodná, protože nevyžaduje žádné povrchové úpravy nebo modifikace technických prostředků jako současně dostupné programovatelné karty. Alternativně přepínač 4 modu může být vytvořen tak, že umožňuje uživateli U přepínání mezi dvěma mody.

2. Hodiny 61 programovatelné karty 1 použité v autentizačním modu mají „hrubou strukturu“ když se vypočítává identifikátor SUid uživatele U. Zvláštní hodiny pro modus ID uživatele U nejsou nutné, avšak mohly by být použity.

V modu ID uživatele U programovatelná karta 1 zobrazuje 6 až 8 míst decimálního čísla nebo jiný sled symbolů znázorněný jako XX XX XXX na obr. 1 jako na čase závislý dynamický identifikátor SUid uživatele U. Tento identifikátor SUid uživatele U může obsahovat úvodní značku 5, která oznamuje, že identifikátor SUid uživatele U je zobrazen. Uživatel U nyní vstoupí svým „ID uživatele“ do pracoviště pro vysílání do úřadu AS_Y cizí oblasti D_Y. Jak bude uvedeno dále, tento vstupní krok může být také proveden samočinně. V tomto okamžiku by mělo být jasné, že dynamický identifikátor SUid uživatele U obsahuje identifikaci uživatele U pouze v zašifrované formě, takže žádný vetřelec nebude schopen z ní získat správnou identitu uživatele U. Dále by mělo být jasné, že ačkoliv dynamický identifikátor SUid uživatele U je po určitém časovém intervalu modifikován, jakýkoliv sled dynamických identifikátorů SUid uživatele U není zřejmě v závislosti na žádném jiném a nezpůsobuje žádné viditelné oznámení příslušnosti k témuž uživateli U.

V autentizačním modu programovatelná karta 1 zobrazuje jiných 6 až 8 míst decimálního čísla nebo jiný sled symbolů znázorněný jako YYY YYY YY na obr. 1 jakožto dynamický identifikátor SUid uživatele U. Uživatel U zadává tento identifikátor SUid jako své „předávací slovo PW_u „do terminálu, který jej potom vysílá do úřadu AS_Y cizí oblasti D_Y. (Identifikační proces samotný, jak je uvedeno výše, není součástí tohoto vynálezu a nebude tudíž dále podrobně popisován.)

Taková programovatelná karta 1 by mohla být použita při modifikaci komerčně dostupných programovatelných karet, jako je programovatelná karta SecurID popisovaná v publikaci (11) a obsahující již zřejmě hodiny a procesor. Pro odborníka školeného v oboru by napsání vhodného programového vybavení a v případě potřeby přizpůsobení karty neměl býti problém. Ani zde není nutná fyzická modifikace programovatelné karty, je–li zvoleno samočinné přepínání z modu ID uživatele na modus autentizace.

Obr. 2 znázorňuje vysílání dynamického identifikátoru SUid uživatele U a identifikátoru SUid z programovatelné karty 1 přes úřad 6 cizí oblasti do úřadu 8 místní oblasti uživatele.

Jedna přednostní cesta spočívá v tom, že uživatel přivede na vstup obě hodnoty z programovatelné karty 1, jak jsou zobrazeny. Jiná cesta spočívá v tom, že se programovatelná karta 1 čte v terminálu připojeném k úřadu 6 cizí oblasti. Obvyklé přepážkové psací stroje, jaké se používají v bankovním obchodním styku, by mohly být modifikovány, aby prováděly výše uvedený postup. (pro autentizaci může také uživatel U zavést na vstup předávací slovo PW_u, číslo PIN nebo použít jakýkoliv prostředek systému pro autorizační proces. Jak bylo uvedeno výše, autorizační proces není součástí vynálezu a může být použita jakákoliv metoda.)

Úřad 6 cizí oblasti má informaci o tom který úřad 8 místní oblasti má být adresován. To je přednostně dáno zavedením vhodného úseku do dynamického identifikátoru SUid uživatele U. Podle jiné alternativy může být od uživatele U požadován zvláštní vstup od úřadu 6 cizí oblasti pro identifikaci úřadu 8 místní oblasti.

Z úřadu 6 cizí oblasti jsou data přenášena přes přenosový člen 7, znázorněný na obr. 2 jako kabel, do úřadu 8 místní oblasti. Přenosový člen 7 může být alternativně vytvořen jako rádiový nebo infračervený přenosový systém. Vetřelec vyvíjející data z úřadu 6 cizí oblasti nebo přenosového členu 7 nebude schopen detekovat správnou identitu uživatele U nebo jeho předešlé mít přístupu do systému.

Protože dynamický identifikátor SUid uživatele U je již zašifrován, další zašifrování pro bezpečnější vysílání již není nutné, může však být provedeno.

Obr. 3 znázorňuje síť sestávající z první části 10 sítě a z druhé části 20 sítě, z nichž každá má určitý počet terminálů pro přístup uživatele U. První část 10 má sběrnici 15 spojující její uživatelské terminály 11 až 13 a server 14. Přenosový člen 7 zde znázorněný jako vedení nebo kabel spojuje server 14 s cestou 30 hradel. Některé nebo všechny terminály mají vestavěnou výpočetní jednotku. Také úřad 8 místní oblasti může být rozdělen a nemusí být umístěn v serveru 14.

Druhá část 20 má také určitý počet terminálů 21 až 24, které jsou připojeny k rámcové kruhové síti 25. Alespoň terminál 24 má vestavěnou výpočetní jednotku a je použit jako server pro tuto druhou část 20 sítě. Spoj 26 zde znázorněný jako dvoulinka může být vytvořen jako rádiový nebo infračervený přenosový systém s cestou 30 hradel.

Pohyblivý uživatel U, který chce vstoupit do systému přes terminál 12 a který se nachází „doma" ve druhé části 20, zavede svá data na vstup, to znamená dynamický identifikátor SUid, předávací slovo PW_u atd. do klávesnice nebo jiného vstupního zařízení u terminálu 12, anebo vloží svou programovatelnou kartu 1 do čtecího zařízení v terminálu 12. Jelikož terminál 12 je z hlediska uživatele U částí cizí oblasti, bude vynález, aby zavedl do vstupu jméno své místní oblasti nebo bude toto jméno U_X přečteno z programovatelné karty 1. Buď terminál 12 nebo alternativně uživatelova programovatelná karta 1 vypočítá dynamický identifikátor SUid uživatele U, jak bylo popsáno výše. Úřad 14 cizí oblasti přijímající tento dynamický identifikátor SUid uživatele U není schopen určit jeho hodnotu. Musí však znát místní oblast D_X uživatele U, v daném případě druhou část 20 za účelem nasměrování nebo vyslání zašifrovaných dat do správné místní oblasti D_X přes cestu 30 hradel.

Cesta 30 hradel nebo jiná cesta hradel reléová stanice v cestě má také schopnost vyjádřit správnou místní oblast D_X uživatele U, avšak nemůže číst nebo vyjádřit dynamický identifikátor SUid uživatele U. V daném případě cesta 30 hradel vysílá přijatý zašifrovaný identifikátor SUid uživatele U do úřadu 24 místní oblasti.

Když úřad 24 místní oblasti uživatele přijme dynamický identifikátor SUid svého místního pohyblivého uživatele U, vypočítá předem tabulky dat obsahující dynamické identifikátory SUid uživatele U pro všechny jeho uživatele platné v přítomném časovém intervalu δ_X, tudíž rychlým a snadným prohlédnutím tabulky může úřad 8 místní oblasti zjistit, zdali přijímaný dynamický identifikátor SUid uživatele U je platný a kterému uživateli náleží. To je podrobněji popsáno v souvislosti s obr. 4. Úřad 24 místní oblasti může potom zaslat přiměřenou zprávu terminálu 12 (ze kterého uživatel žádal službu) anebo projít autentizačním procesem.

Jak je znázorněno na obr. 4, přijme-li úřad 24 místní oblasti dynamický identifikátor SUid, zvolí vhodnou tabulku 42 označení, například TB_2 ze série 41 předem vypočítaných tabulek TB_1 až TB_n podle běžného časového intervalu δ_X. Potom prohledá zvolenou tabulku při použití dodané hodnoty SUid a identifikuje sériové číslo 2 (nebo některý jiný ID) programovatelné karty 1 nebo uživatelův terminál, který spočítal SUid. Sériové číslo 2 programovatelné karty 1 jednoznačně identifikuje uživatele U. Když je tato identifikace provedena, může být vyvinuta příslušná zpráva z úřadu 24 místní oblasti.

Obr. 5 ukazuje příklad, jak může být uživatelův vstup zpracován ve vstupním terminálu 12 v cizí oblasti D_Y. Uživatel U zavede do vstupu svůj ID nebo identifikátor A_U, své předávací slovo PW_U a dle volby indikátor intervalu T_U času zaokrouhlený na nejbližší časový interval δ_u do terminálu 12 cizí oblasti D_Y. Přijímací obvod 51 obsahující zašifrovač 52 zašifruje uživatelovy vstupy, t.j. i_1 až i_3, které odpovídají PW_U, A_U a T_U, jak je znázorněno na obr. 5. Spojení i_1 a i_2 je zašifrováno pod DES, uvedeným výše v publikaci (8), od klíčem i_3 určujícím SUid, který není poslán do místní oblasti D_X uživatele U. Zde úřad 24 místní oblasti vyhodnotí přijatý dynamický identifikátor SUid uživatele U.

Následuje popis celého procesu po krocích.

KROK 0

Nejprve a přednostně permanentně každý úřad AS_X autentizace (místní oblast D_X), typicky úřad 24 místní oblasti vypočítá tabulky nutné pro proces. To se provádí po určitých časových intervalech, například jednou denně. Tím se vypočítá sled tabulek, například TB_1, TB_2, TB_n, kde n je počet intervalů δ_X v jednom dnu nebo v jiné „dlouhé" časové jednotce. Například, když je δ_X nastaven na jednu hodinu, úřad 24 místní oblasti vypočítá 24 tabulek každý den.

Každá tabulka TB_i obsahuje takový počet řádků, jaký je počet uživatelů v místní oblasti D_X. Každý řádek sestává ze dvou sloupců:

- jméno U uživatele a
- výsledek použití jednocestné funkce $F(A_U,T_U,PW_U)$, kde PW_U je předávací slovo nebo PIN uživatele U a $Ti = T_O i\delta_X$.

T_O je absolutní čas a začátek výpočtu, to znamená když se výpočet provádí každý den, potom T_O se nastaví na půlnoc.

Tím je skončena první část procesu, t.j. výpočet tabulky. Následující druhá část obsahuje určení identity. Pro snadné porozumění bude výpočet popsán v několika krocích.

KROK 1

Uživatel U cestuje do některé cizí oblasti D_Y. U terminálu v této cizí oblasti D_Y, například terminálu 12 první části 10 na obr. 3 se zavede do vstupu ID skutečné jméno uživatele U_X nebo identifikátor uživatele A_U, hodnota δ_X a jeho předávací slovo PW_U (nebo PIN). Ze vstupních hodnot vypočítá terminál dynamický identifikátor SUid uživatele U (programové vybavení nebo technické vybavení)

$$SUid = F(A_U,T_U,PW_U),$$

kde T_U je místní čas terminálu zaokrouhlený na nejbližší hodnotu δ_X, t.j. na sekundy, minuty nebo hodiny v závislosti na tom, jaké jednotky δ_X se měří. Poznamenejme, že v terminálu nemusí být hodiny. V tom případě uživatel zavede do vstupu také čas T_U, např. odpovídající času na jeho hodinkách.

Kromě toho uživatel zavede do terminálu určitou informaci a autentizaci. Není významné pro předložený vynález jaký je obsah této autentizační informace.

KROK 2

Terminál vyšle hodnotu dynamického identifikátoru SUid s autentizační informací do úřadu AS_X místní oblasti D_X uživatele U, například do úřadu 24 v druhé části 20. To může být provedeno nepřímo. Terminál 12 může napřed poslat data do úřadu AS_Y cizí oblasti, například serverem 14 první části 10, který potom pošle data do terminálu AS_X nebo do úřadu 24 místní oblasti.

KROK 3

Když data dojdou do úřadu AS_X, t.j. do úřadu 24 místní oblasti, tento nejprve získá informaci o místním čase T_X. Potom vypočítá

$j = (T_X - T_O)/\delta_X$ užitím dělením celých čísel, a
$k = (T_X - T_O) \% \delta_X$, kde % je modulový operátor.

KROK 4

AS_X, t.j. úřad 24 místní oblasti prohledá tabulku TB_j (předem vypočtenou v kroku 0) použitím dynamického identifikátoru SUid uživatele U jako hledané hodnoty.

KROK 4a

Když je prohledání úspěšné, vstup tabulky ukazuje na uživatele U.

KROK 4b

Když prohledání není úspěšné, úřad AS_X místní oblasti D_X, tj. úřad 24 místní oblasti může (v závislosti na hodnotě k) prohledat buď TB_{j-1} nebo TB_{j+1}.

KROK 5

Když byl uživatel U identifikován, úřad AS_X místní oblasti D_X, tj. úřad 24 místní oblasti, ověří autentizační informaci, která byla přijata s dynamickým identifikátorem SUid, jak je v oboru známo. Podrobnosti tohoto procesu opět nejsou významné pro předložený vynález.

KROK 6

Když úřad AS_X místní oblasti D_X, t.j. úřad 24 místní oblasti zjistí, že dynamický identifikátor SUid odpovídá platnému uživateli U a připojená autentizační informace je správná, odpovídá úřadu AS_Y cizí oblasti D_Y, zde serveru 14 v první části 10, a sdělí mu, že dynamický identifikátor SUid odpovídá právoplatnému uživateli, který je autorizován k získání služby.

Výše popsaný proces nepoužívá programovatelnou kartu. Jestliže se použije programovatelná karta 1, jediná změna nastane v roku 1. Místo vstupu informace do terminálu by mohl uživatel jednoduše přečíst hodnotu zobrazenou na programovatelné kartě 1 v modu ID a zavést ji do terminálu 12. Alternativně může být tato hodnota přečtena strojově terminálem 12. Tato hodnota je dynamický identifikátor SUid právě vypočítaný programovatelnou kartou 1 stejným způsobem jako to provádí terminál ve shora uvedeném kroku 1.

Souhrnně vzato, na konci kroku 6 úřad cizí oblasti AS_Y, zde terminál 12, má jistotu, že uživatel U je legitimní uživatel, ale současně úřad oblasti nezná a nemůže objevit identitu uživatele. Úřad AS_Y oblasti D_Y zná pouze dynamický identifikátor SUid. Shoda mezi dynamickým identifikátorem SUid a skutečným jménem uživatele U_X je známa pouze uživateli U a jeho úřad AS_X místní oblasti D_X.

Je možno se představit mnohé obměny předloženého vynálezu, vycházíme–li z bezdrátového, například rádiového nebo infračerveného vysílání až k multiplexnímu provozu, když služba několika uživatelům současně v bezdrátové oblasti by mohla bát provedena s jediným serverem, jako je kombinovaný vysílač a přijímač a současně s úřadem oblasti. Synchronizace může být například dosaženo hodinami řízenými rádiem nebo jinými synchronizačními přístroji. Programovací karty by mohly obsahovat nějakou účinnou výpočetní kapacitu, aby terminály mohly být provedeny co nejvíce robusně. Všechny tyto obměny by mohly být provedeny použitím základních principů předloženého vynálezu, jak je definován v připojených patentových nárocích.

PATENTOVÉ NÁROKY

1. Způsob zajištění identifikace pohyblivého uživatele v komunikačním systému s rozptýlenými uživateli seskupeními do oblastí D_X, D_Y v systému, přičemž každý uživatel má identifikátor A_U a předávací slovo nebo jiný tajný autentizátor PW_U, kde identifikátor A_U a předávací slovo PW_u se uloží v uživatelově místní oblasti D_X, kterýžto způsob obsahuje indikaci synchronizace, přednostně používající indikaci intervalu T_u, synchronizující vstup uživatele U v cizí oblasti D_Y s jeho místní oblastí D_X, **vyznačující se tím**, že obsahuje po sobě následující kroky:

– zašifrování pod tajnou funkcí, zvláště jednocestnou funkcí, identifikátoru A_U, indikace synchronizace intervalu T_U času a uživatelova předávacího slova PW_u nebo jiného tajného autentizátoru a vyvinutí zašifrovacího dynamického identifikátoru SUid uživatele,

– oznámení místní oblasti D_X uživatele cizí oblasti D_Y, ze které má uživatel U úmysl komunikovat,

– vysílání zašifrovaného identifikátoru SUid do místní oblasti D_X uživatele,

– vyhodnocení zašifrované zprávy v místní oblasti D_X uživatele U a určení správné identity uživatele.

2. Způsob zajištění identifikace podle nároku 1, **vyznačující se tím**, že indikace synchronizace intervalu T_u času se odvozuje z identicky zavedených generátorů náhodného čísla nebo čísel tajného pořadí uložených v místní oblasti D_X uživatele U nebo alespoň v čase spojení s cizí oblastí D_Y.

3. Způsob zajištění identifikace podle nároku 1 nebo 2, **vyznačující se tím**, že zašifrování se provede v cizí oblasti D_Y a zašifrovaný dynamický identifikátor SUid uživatele se vyšle do místní oblasti D_X uživatele U pro vyhodnocení.

4. Způsob zajištění identifikace podle alespoň jednoho z nároků 1 až 3, **vyznačující se tím**, že když je určení úspěšné, vyšle se z místní oblasti D_X potvrzující zpráva zejména do cizí oblasti D_Y, když je určení neúspěšné, oznámí se zamítnutí.

5. Způsob zajištění identifikace podle alespoň jednoho z nároků 1 až 4, **vyznačující se tím**, že tajná funkce je jednoduchá funkce

$$SUid = F(A_U, T_U, PW_U), \text{ a}$$

identifikátor A_U je sekundární identifikátor uživatele U.

6. Způsob zajištění identifikace podle alespoň jednoho z nároků 1 až 5, **vyznačující se tím**, že v místní oblasti D_X před příslušným intervalem času δ_U nebo jiným oznámením intervalu synchronizace se předem vypočítá jedna nebo několik potenciálních zašifrovaných zpráv pro budoucí interval času a uloží se v odkazové/překládací tabulce (42).

7. Způsob zajištění identifikace podle nároku 6, **vyznačující se tím**, že odkazová/překládací tabulka (42) v místní oblasti D_X se vytvoří selektivně, ve zvláštním případě pouze pro zvolené známé pohyblivé uživatele U.

8. Způsob zajištění identifikace podle alespoň jednoho z nároků 1 až 7, **vyznačující se tím**, že pro každou oblast D_X se zvolí časový interval δ_u, zvolený časový interval δ_u trvá jednu nebo více hodin nebo jeden den.

9. Způsob zajištění podle alespoň jednoho z nároků 1 až 8, **vyznačující se tím**, že zašifrování popřípadě vyvíjení náhodného čísla se provede v cizí oblasti D_Y v přenosném vstupním přístroji, přednostně v programovatelné kartě (1) a zašifrovaný dynamický identifikátor SUid uživatele U se zavede do cizí oblasti D_Y.

10. Způsob zajištění identifikace podle nároku 9, **vyznačující se tím**, že alespoň část vstupu do cizí oblasti D_Y se provede přímo z přenosného vstupního přístroje, přednostně jeho strojovým čtením.

11. Přenosný vstupní přístroj k provádění způsobu podle alespoň jednoho z nároků 1 až 10, zejména programovatelná karta (1) k provádění v komunikačním systému s rozptýlenými uživateli seskupenými do oblastí D_X, D_Y, **vyznačující se tím**, že obsahuje procesor (60) zašifrované zprávy SUid, hodiny (61) připojené k procesoru (60), displej (3) připojený k procesoru (60) a přepínač (4) modu připojený k displeji (3).

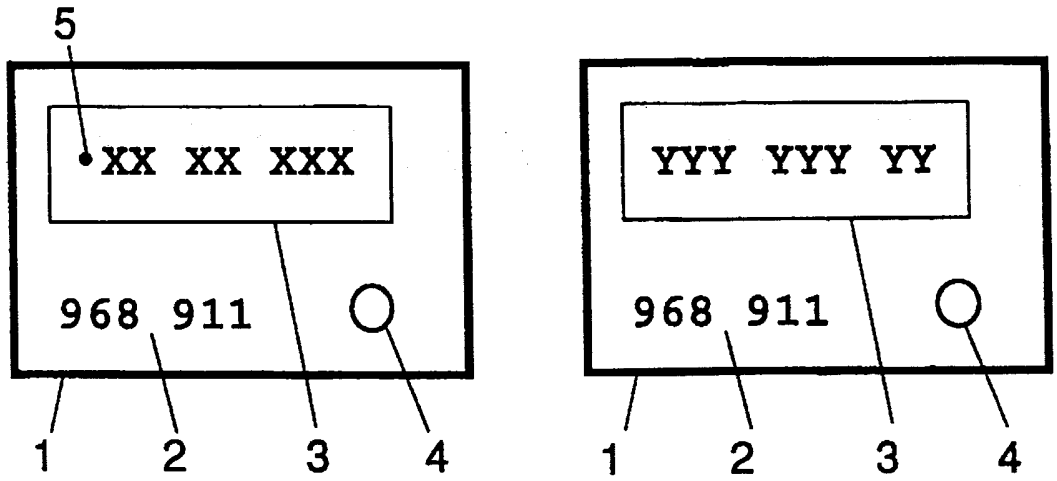
12. Přenosný vstupní přístroj podle nároku 11, **vyznačující se tím**, že dále obsahuje vstupní obvod (62) připojený k procesoru (60).

13. Přenosný vstupní přístroj podle nároku 11, **vyznačující se tím**, že v první části (10) sítě v terminálu (12) je přijímací obvod (51) a zašifrovač (52), a vysílač (16) připojený k první části (10) sítě, a v druhé části (20) sítě je spoj (26).

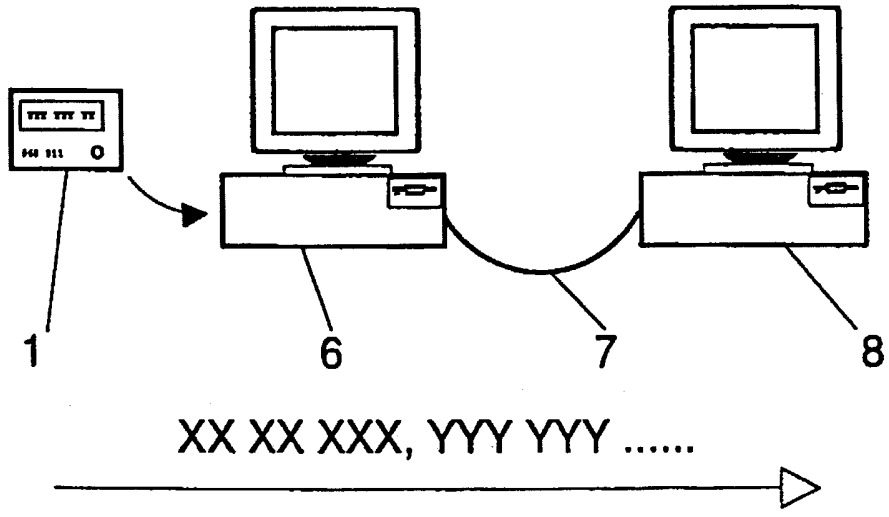
14. Přenosný vstupní přístroj podle nároku 13, **vyznačující se tím**, že úřad AS_Y cizí oblasti nebo identifikační server (14) cizí oblasti AS_Y, nebo úřad AS_X místní oblasti obsahuje server (24) řízení zprávy a zpracování v první části (10) sítě a/nebo v druhé části (20) sítě.

15. Přenosný vstupní přístroj podle nároku 14, **vyznačující se tím**, že ukládací přístroj (41) překládacích tabulek (42) je umístěn v úřadu AS_X místní oblasti D_X.

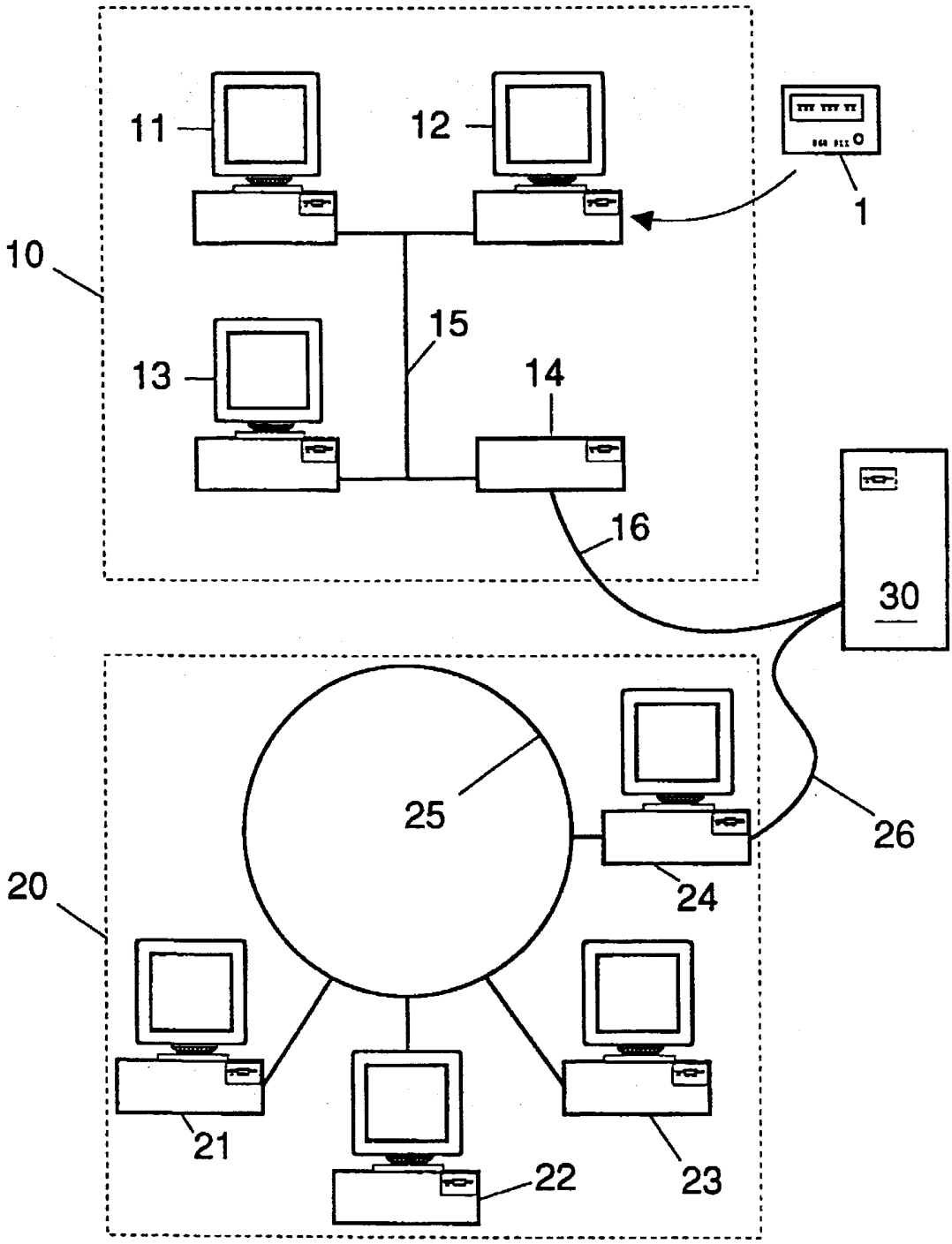
3 výkresy


5
XX XX XXX
968 911
1
2
3
4
YYY YYY YY
968 911
1
2
3
4

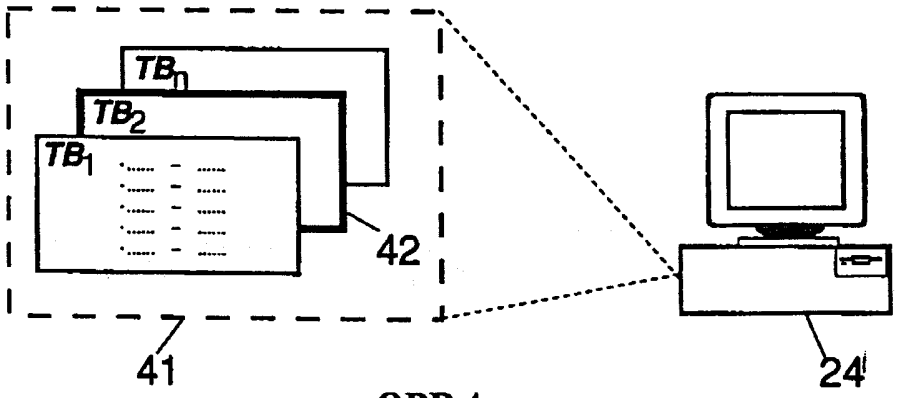
OBR.1


1
6
7
8
XX XX XXX, YYY YYY .....

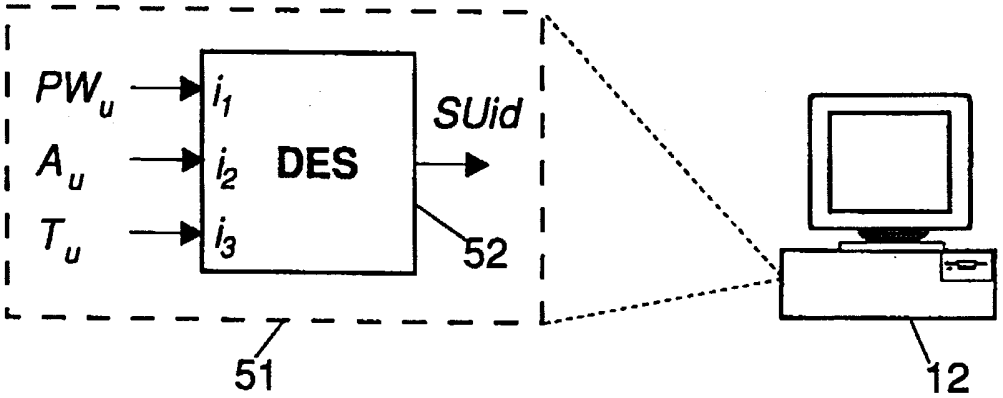
OBR.2



OBR.3



OBR.4



OBR.5

Konec dokumentu