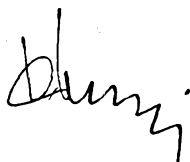


ELJÁRÁS PÉNZ- VAGY ÉRTÉKEGYSÉGEK BIZTONSÁGOS KEZELÉSÉRE
ELŐRE FIZETETT ADATHORDOZÓKKAL

K i v o n a t

Az eljárás pénz- vagy értékegységek biztonságos kezelésére vonatkozik előre fizetett adathordozókkal, amelyeket kártyakiadóval (I.A.) állítunk ki, elsősorban elektronikus könyvelési rendszerekhez, telefonkártyarendszerekhez és elektronikuspénztárca-rendszerekhez. Az adathordozót (II.A.) egy ismertetőjegy alapján egyértelműen azonosítjuk egy végkészülék és/vagy háttérrendszer(ek) (I.B.) felé, majd az adathordozóhoz (II.A.) hozzárendelt pénz- vagy egységértéket egy eladott, ill. megvásárolt árunak vagy szolgáltatásnak megfelelően a háttérrendszerben (I.B.) automatikusan csökkentjük és könyveljük, és a kommunikációt a végkészülékek és a hálózati csomópontok háttérrendszere ~~NY~~ között folytatjuk. Egy ügyfél vagy felhasználó által előre kifizetett adathordozót (II.A.) egyetlen egyértelmű ismertetőjeggyel vagy azonosítójellel, például sorszámmal, kriptogrammal, rejtjelkulccsal vagy hasonlóval látunk el. Az ismertetőjegyhez vagy azonosítójelhez egy értéket rendelünk hozzá, és a kettőt együtt egy kommunikációs úton (III.B.) eljuttatjuk a háttérrendszerbe (I.B.). A háttérrendszerben (I.B.) letétbe helyezett, egyetlen meghatározott adathordozóhoz (II.A.) tartozó titkos kulcsot biztonsági felülvizsgálathoz használjuk fel válaszatok visszafejtésével. Az adathordozónak (II.A.) küldött felszólítás és az onnan kapott válasz egyezésekor az adathordozót (II.A.) hitelesnek minősítjük.

(1. ábra)



ELJÁRÁS PÉNZ- VAGY ÉRTÉKEGYSÉGEK BIZTONSÁGOS KEZELÉSÉRE
ELŐRE FIZETETT ADATHORDOZÓKKAL

A találmány tárgya eljárás pénz- vagy értékegységek biztonságos kezelésére előre fizetett adathordozókkal, elsősorban elektronikus könyvelési rendszerekhez, telefonkártya-rendszerekhez és elektronikuspénztárca-rendszerekhez.

Már évek óta fejlesztik és használják a csipkártyás elektronikus pénztárcákat. A csipkártyán kívül többnyire ezek alkotórésze a csipkártya és a számítógép- és átviteli rendszerek közötti együttműködésnél, valamint a csipkártyával végrehajtott tranzakciók elszámolásánál alkalmazott biztonságtechnika. Erre a célra mind nemzeti, mind nemzetközi szinten számos koncepciót dolgoztak ki. Néhány országban elektronikuspénztárca-rendszereket vezettek be; ezek közé tartoznak például a következők:

- Feldversuch Eisenstadt, Ausztria, 1994. decembere óta
- Avantcard, Finnország
- Danmond, Dánia
- Mondex, Swinton, Anglia
- ezenkívül CIN TC224 WG10 jelzéssel szabványosítottak elektronikus pénztárcát (intersect electronic purse).

Ezekben az ismert rendszerekben alapvetően a következő eljárásokat alkalmazzák:

Az első lépés a csipkártya feltöltése pénzürtékegységekkel, amelyek ellenértékét a kártyatulajdonos készpénzzel vagy más módon befizeti az elektronikus-pénztárca-rendszer üzemeltetőjének számlájára (Pool-Konto). Amikor ezt követően a kártyatulajdonos a csipkártyájával fizet, az elektronikus pénztárca tartalmából pénzürtékegységeket vonnak le, és egy biztonsági modul segítségével a szolgáltató termináljához továbbítják. Ott a bevételezett pénzürtékegységeket vagy gyűjtik egy bizonyos összegig, és így számolják el az elektronikus-pénztárca-rendszer üzemeltetőjével, vagy minden egyes fizetésnél benyújtják követelésüket az üzemeltetőnek. Az összegeket vagy az egyes adatsorokat egy ún. kereskedői kártyán gyűjtik, amit a szolgáltatónak be kell nyújtania, vagy egy megfelelően kialakított terminállal online viszik át egy elszámolóhelyre.

Ismeretesebbek továbbá olyan elektronikus pénztárcák, amelyeket mikroprocesszoros kártyával valósítanak meg. Ezek használatát pl. a prEN726-3 szabvány szerinti üzemeltetési rendszerrel vezérlik. Ennél az alkalmazásnál is pénzösszegeket tárolnak a kártyán, amelyekből minden kifizetésnél egy adott összeget vonnak le. Az ismert mikroprocesszoros kártyáknak az az előnyük az ismert memóriakártyákkal szemben, hogy a mikroprocesszoros kártyák képesek a levonást végrehajtó rendszer hitelességének, jogosultságának ellenőrzésére. Ez az ellenőrzés memória-csipkártyával nem lehetséges. Ezenkívül hasonló rendszereket és eljárásokat ismertetnek

az US-A-4,859,837, a WO-A-90 15 382 és a DE 42 43 851 A1 sz. szabadalmi leírások. A DE 196 04 876 C1 sz. szabadalmi leírás egy további eljárást ír le tranzakciók ellenőrzésére elektronikuspénztárca-rendszerekben.

Az US-A-5,777,305 sz. szabadalmi leírásból egy olyan előre fizetett kártya (pre-paid-card) ismeretes, amely egy azonosítójellel van ellátva, és amelyen egy bizonyos követelés van jóváírva. A kártyát egy háttérrendszerben végzett azonosítás után aktiválják vagy deaktiválják. Az azonosítás után a háttérrendszer vezérli a kommunikációt és a további folyamatokat. Az előre fizetett kártyán levő információkat egy végkészülékkel leolvassák. Az elszámolást is a háttérrendszer vezérli. A kártyán tárolt összeg minden használatkor az igénybe vett szolgáltatás ellenértékével csökken.

Az US-A-4,825,050 sz. szabadalmi leírás egy olyan adatvédelmi rendszert ír le, amelyben a pénzügyi tranzakciókhoz kriptográfiai technikákat alkalmaznak.

Az EP-A-0 397 512 sz. szabadalmi leírás egy eljárást ismertet a kártyán tárolt adatok jogosulatlan felhasználásának megakadályozására. Itt a védendő információkat mind a kártyán, mind a háttérrendszerben tárolják, és szükség esetén egymással összehasonlítják. Ez az eljárás azonban az időigényes többszöri összehasonlítási műveletek miatt nem csak hosszadalmas, hanem sok tárhelyet is igényel.

Az US-A-5,477,038 sz. szabadalmi leírás is előre fizetett kártyák vagy hasonló eszközök alkalmazására

vonatkozó eljárást ír le. Ennél a megoldásnál a kártya a kártyát azonosító számon kívül egy banki azonosítószámot és egy számlaszámot is tartalmaz. Ezeket az adatokat a kártyára felvitt mágnescsíkon tárolják. Ez az eljárás a különböző azonosítószámok ellenére nem biztonságos, mivel ezek a kártyáról leolvashatók, és visszaélésre felhasználhatók.

Az US-A-5,721,781 sz. szabadalmi leírás egy hitelesítő rendszert és eljárást ismertet intelligens kártyákkal végrehajtott tranzakciókhoz. Az eljárás csak a kártya és egy terminál közötti műveletekre vonatkozik; a rendszer nem tartalmaz háttérrendszert. Az itt leírt háromszoros azonosítás nagyon bonyolult, idő- és tár-igényes, ami miatt a nagy adatfeldolgozó berendezésekkel ellátott nagy könyvelési rendszerekben nem alkalmazható.

Az EP-A-0 654 919 sz. szabadalmi leírásból ismert eljárás egy információátviteli rendszer egy részének azonosítására vonatkozik egy másik rendszerrésszel felhívás-válasz (challenge-response) elv alapján. Ennél az azonosítási eljárásnál először egy hordozható adathordozó elrendezésben blokkolják a számítási műveletek végrehajtását, amit először egy hibaszámláló állásának megváltoztatásával kell feloldani. A végkészülékről felhívásként véletlen adatokat visznek át a hordozható adathordozó elrendezésre, miután a hibaszámláló állását megnövelték, és a blokkolást feloldották. Mind a végkészülékben, mind a hordozható adathordozó elrendezésben a felhívási adatokból legalább egy

algoritmus és titkos kulcsadatok segítségével hitelesítési paramétereket számítanak ki. A végkészülék válaszként a saját hitelesítési paramétereit viszi át a hordozható adathordozó elrendezésre, amely azokat összehasonlítja az ott számított hitelesítési paraméterekkel. Egyezés esetén az értéktároló újra feltölthető és/vagy a hibaszámláló visszaállítható.

A WO 98 521 63 A sz. szabadalmi leírás eljárást és kapcsolási elrendezést ismertet adatok biztonságos átvitelére egy IC-kártyára. Az adatok például alkalmazási programokat tartalmaznak, ahol legalább az adatok egy része titkosítva van egy nyilvános kriptográfiai kulcs alkalmazásával.

Az említett kártyatípusok közül leginkább a telefonkártyák terjedtek el. A telefonkártyák memóriacsipkártyák, amelyeknek azonosító tartományuk és legalább egy számlálótartományuk van. Az Amerikai Egyesült Államokban Virtual Calling Card (VCC) néven olyan szolgáltatást vezettek be, amely lehetővé teszi az ügyfeleknek, hogy egy hozzáférési jel és PIN kód megadásával bármelyik telefont használhassák. Ezek az ún. Calling Card rendszerek általában egy központi vezérlőegységen alapulnak, amely megfelelő adatbankkal és központi számítógéppel van ellátva. A díj elszámolása az egyes ügyfelekhez hozzárendelt számlákon történik. Ez a szolgáltatás Európában is terjed. Ilyen rendszer van leírva a "Deutsche Telekom AG - Vision" c. kiadványban,

1995. február, 44-45. old. (T-Card mit Connect Service der Deutschen Telekom).

A fenti cikk szerint a kártya - telefonkártyától hitelkártyáig - több célra használható. A kiadvány 61. oldalától a 4.1.2.1. fejezetben (Beutelsberger, Kersten és Pfau: "Chipkarten als Werkzeug") le van írva, hogy hogyan vizsgálják a memória-csipkártyák hitelességét az ismert Challenge-Response eljárással. Ezekkel a csipkártyákkal lehetőség van a kártyák azonosítására és elfogadhatóságának vizsgálatára egy terminál vagy kártyaolvasó segítségével. A hitelesítés a terminálba beépített biztonsági modulban történik.

A DE 196 04 349 A1 sz. szabadalmi leírás memória-csipkártyák vizsgálatára alkalmas eljárást ismertet, amely kriptográfiai függvények és egy terminál segítségével két- vagy háromszoros hitelesítést tesz lehetővé.

A ma túlnyomó részt használt eljárások és rendszerek hátránya az, hogy a mindenkori értéket vagy értékegységeket az adathordozón, például csipkártyán vagy mikroprocesszoros kártyán tárolják. A végkészülékek felismerik az adathordozón tárolt értéket, és azt a vásárolt áru vagy szolgáltatás ellenértékével csökkentik. Mivel nagyszámú előre fizetett adathordozó van forgalomban, általában lemondanak arról, hogy a végkészülékekben és/vagy azok háttérrendszereiben ún. árnyékfolyószámlákat vagy árnyékegyenlegeket vezessenek. Ezért a végkészülékekben és azok háttérrendszereiben nem lehet a használni kívánt adathordozót hitelesíteni. Az adathordozó mani-

pulálásával vagy hamisításával pénz- vagy értékegységeket lehet előállítani, amire egyébként csak a könyvelési rendszer üzemeltetője jogosult. Ennek következtében az üzemeltetőket világszerte hatalmas károk érik.

Az árnyékfolyószámlákat vagy árnyékegyenlegeket vezető rendszereknek elsősorban az a hátrányuk, hogy a rendszerben nagy adattömeget kell átvinni. Ezenkívül sok végkészüléknek nincs online kapcsolata, azaz az adatokat csak időben késve viszik át. Ezért viszont a manipulációkat nem lehet azonnal észlelni.

Célunk a találmánnyal egy eljárás létrehozása pénz- vagy értékegységek biztonságos kezelésére előre fizetett adathordozókkal, például csipkártyákkal, mágneskártyákkal és hasonló eszközökkel elektronikus könyvelési rendszerekben, például telefonkártya-rendszerekben, elektronikuspénztárca-rendszerekben és hasonlóknak, amely eljárással megakadályozhatók a kártyamanipulációk, és az ismert rendszerekhez képest csökken az adatátvitel.

A találmány szerinti eljárás pénz- vagy értékegységek biztonságos kezelésére szolgál előre fizetett adathordozókkal, amelyeket kártyakiadóval állítunk ki, elsősorban elektronikus könyvelési rendszerekhez, telefonkártya-rendszerekhez és elektronikuspénztárca-rendszerekhez; az adathordozót egy ismertetőjegy alapján egyértelműen azonosítjuk egy végkészülék és/vagy háttérrendszer(ek) felé, majd az adathordozóhoz hozzárendelt pénz- vagy egységértéket egy eladott, ill. megvásárolt árunak vagy szolgáltatásnak megfelelően a háttérrend-

szerben automatikusan csökkentjük és könyveljük, és a kommunikációt a végkészülékek és a hálózati csomópontok háttérrendszere(i) között folytatjuk. Az eljárás szerint egy ügyfél vagy felhasználó által előre kifizetett adathordozót egyetlen egyértelmű ismertetőjeggyel vagy azonosítójellel, például sorszámmal, kriptogrammal, rejtjelkulccsal vagy hasonlóval látunk el; az ismertetőjegyhez vagy azonosítójelhez egy értéket rendelünk hozzá, és a kettőt együtt egy kommunikációs úton eljuttatjuk egy háttérrendszerbe; a háttérrendszerben letétbe helyezett, egyetlen meghatározott adathordozóhoz tartozó titkos kulcsot biztonsági felülvizsgálathoz használjuk fel válaszatok visszafejtésével; és az adathordozónak küldött felszólítás és az onnan kapott válasz egyezésekor az adathordozót hitelesnek minősítjük.

Előnyösen a háttérrendszerrel közvetlenül hozzuk létre és ellenőrizzük a kommunikációs összeköttetést; az adathordozók ismertetőjegyeként minden adathordozóhoz egy egyedi, nyilvános kriptográfiai kulcsot alkalmazunk; és a kulcshoz vagy azonosítóhoz egy meghatározott tarifamoddelt rendelünk hozzá.

Célszerűen az illetéktelen leolvasást megnehezítő, bonyolult ismertetőjegyet alkalmazunk.

A találmány szerinti eljárás arra kényszerít egy potenciális csalót vagy támadót, hogy az üzemeltető háttérrendszerét próbálja manipulálni, azaz különböző ismertetőjegyekkel kísérletezzon, hogy hozzájusson egy adathordozó, pl. csipkártya ellenértékéhez. Ez a csaló

számára sokkal nehezebb, mint magának a memóriacsipkártyaként vagy mikroprocesszoros csipkártyaként kialakított adathordozónak a manipulálása. Másrészt az üzemeltető egyszerűbben tudja védeni a biztonságos környezetben elhelyezett központi háttérrendszert a jogosulatlan hozzáférésekkel szemben. Ha például a csalónak sikerül kilesnie az azonosítójegyet, akkor is csak ennek az egyetlen adathordozónak vagy ismertetőjegynek az ellenértékéhez juthat hozzá. A következő ismertetőjegy kikémlélése ismét sok idejébe és fáradságába kerülhet. Fontos, hogy a javasolt eljárás miatt céltalan magát az adathordozót manipulálni. Az adathordozók másolatának vagy szimulációjának értéke szintén az egyetlen eredeti adathordozó viszonylag csekély aktuális értékére korlátozódna. Ezenkívül az is a javasolt eljárás előnye, hogy csökkenti az árnyék-folyószámlákat alkalmazó eddig ismert eljárások nagy adatátviteli igényét. A háttérrendszerben a felismert biztonsági problémákkal kapcsolatos reakcióidők lényegesen rövidebbek, mint az eddigi eljárásoknál, továbbá a szolgáltatások hozzárendelése az azonosításhoz a háttérrendszer központi számítógépében vagy központi vezérlőegységében elvégezhető.

Az alábbiakban még visszatérünk a találmány szerinti eljárás további előnyeire, jellemzőire és alkalmazási lehetőségeire a hálózat üzemeltetőjének és a szolgáltatónak, valamint az adathordozó felhasználójának szempontjából.

A találmányt a továbbiakban kiviteli példa és rajz alapján részletesen ismertetjük. A rajzon az

1. ábra: a találmány szerinti eljárást szemléltető elvi működési diagram.

Mielőtt a találmány szerinti eljárás végrehajtását részletesen leírnánk az 1. ábra alapján, először az alapvető működési elvet és eljárási lépéseket ismertetjük.

Egy ügyfél beszerez egy telefonkártyát. A telefonkártya például egy csipben tárolva csupán a kártya ID azonosítóját (ID 12345...) tartalmazza. Amikor az ügyfél a kártyát behelyezi egy kártyás telefonba, a telefon kiolvassa az ID azonosítót, kapcsolatot létesít a háttérrendszerrel, és közli azzal az ID azonosítót. A háttérrendszer ekkor az ID azonosítóhoz egy értéket rendel hozzá értékegységek formájában vagy valamilyen pénznemben, pl. DM-ben. Az ügyfél megkezdi egy telefonszám tárcsázását. A tárcsázási információkat azonban nem a kártyás telefon értékeli ki, hanem csupán továbbítja a háttérrendszernek. Ez kiértékeli a tárcsázási információkat, a kártyán rendelkezésre álló értéknek megfelelően felépíti az összeköttetést, és amikor a kártya kimerül, azaz a rendelkezésre álló összeg nullára csökken, megszakítja az összeköttetést.

Mivel az összeköttetést egy központi háttérrendszer vezérli (a Calling Card rendszerhez hasonlóan), szinte az összes elképzelhető szolgáltatás felkínálható, és

egyszerűen (mivel központilag) adminisztrálható és továbbfejleszthető.

Az ID azonosító hozzárendelhető például egy meghatározott tarifamodellhez (ha a kártyát pl. akciósan árusították, a kedvezmények egy megfelelő tarifamodellel valósíthatók meg). Ezen a módon a legkülönbözőbb szolgáltatások kapcsolhatók össze.

Az eljárás lehetővé teszi, hogy az üzemeltető hatókörén kívül - azaz nem biztonságos környezetben - tartózkodó felhasználó vagy ügyfél adathordozója ne tartalmazza a pénz- vagy egységértéket, hanem csak egy egyértelmű ismertetőjegyet, például egy sorszámot, kriptogramot, rejtjelkulcsot vagy hasonlót. Az ismertetőjegyet a használatnál a végkészülék leolvassa. Az adathordozó az ismertetőjeggyel egyértelműen azonosítja magát a végkészülék és ennek háttérrendszere vagy háttérrendszerei felé. Az adathordozóhoz hozzárendelt pénzértéket vagy egységértéket a vásárolt áru vagy szolgáltatás ellenértékével csökkentjük az üzemeltetők háttérrendszereiben.

Annak érdekében, hogy egy támadó vagy potenciális csaló minél nehezebben ismerhesse meg - pl. leolvasással - az ismertetőjegyet, célszerű bonyolult ismertetőjegyet választani, és ezt titkosítva rögzíteni az adathordozón.

Az ismertetőjegy egy nyilvános kriptográfiai kulcs; minden adathordozóhoz egy saját, egyedi kulcs tartozik. A végkészülék/háttérrendszer egy ún. felhívást (challenge) küld az adathordozónak, amely azt a rajta rögzített krip-

tográfiai kulcs segítségével titkosítja. Az eredmény az ún. válasz (response). Az adathordozó visszaküldi a választ az üzemeltető háttérrendszerének vagy végkészülékének. Az üzemeltető háttérrendszereiben rögzített, az adott adathordozóhoz - és csak ahhoz - tartozó egyedi titkos kulcsot használjuk a válasz visszafejtéséhez. Ha a felhívás és a válasz megegyezik, az adathordozó hiteles. Ezenkívül a pénz- és értékegységek változása az adathordozón is vezethető, tárolható - esetleg titkosítva - az elfogadhatóság ellenőrzéséhez.

Az 1. ábrán látható elvi diagram a nyilvános távközlésben szokásos memóriás vagy mikroprocesszoros csipkártyák használatára vonatkozik. Ezekkel a csipkártyákkal szemben nem támasztunk különösebb biztonsági követelményeket. Csupán a csipkártyák egyedi jellegének megadásánál, személyre szabásánál (perszonifikálásánál) kell ügyelni arra, hogy az azonosítójelet véletlenszerűen válasszunk ki egy több nagyságrenddel nagyobb értéktartományból. Példa: a kiadott kártyák száma = 10^6 darab; értéktartomány = 10^{12} , amiből 12 jegyű kártyaszám adódik. Az 1. ábra szerinti diagram alapvetően az I telekommunikációs infrastruktúrára, a II ügyfelekre és a III kommunikációs utakra van felosztva.

Az eljárást a következőképpen hajtjuk végre: például egy telefonkártya memória- vagy mikroprocesszorcsipjét az I.A. kártyakiadóval állítjuk ki és perszonifikáljuk, azaz egy egyedi, egyértelmű azonosítójellel, pl. kártyaszámmal látjuk el. Ehhez az azonosítójelhez egy értéket (pl. x DM

vagy x egység) rendelünk hozzá, amelyet azonban nem tárolunk a csipben. Az értéket az azonosítójellel együtt az I.B. háttérrendszer rendelkezésére bocsátjuk a III.B. kommunikációs úton keresztül. Az I.B. háttérrendszerben az azonosítójelet az értékkel együtt egy adatbankban tároljuk. A tárolt adatokat először "tiltott" jelzéssel látjuk el.

Közvetlenül a telefonkártya eladása előtt az I.A. kártyakiadóval eltávolítjuk a "tiltott" jelzést az I.B. háttérrendszer adatbankjában. Ettől kezdve az I.B. háttérrendszerben könyvelni lehet a levonásokat a kártya értékéből. Ha egy ügyfél II.A. adathordozóként egy ilyen csipkártyát használ egy nyilvános I.C. telekommunikációs terminálon, akkor a terminál csak az azonosítójelet olvassa le a kártyáról, és azt továbbítja az I.B. háttérrendszernek, azaz III.D. ellenőrző lekérdezést hajt végre. Az I.B. háttérrendszer az azonosítójelhez hozzáfűzi a perszonifikálásnál eredetileg ahhoz hozzárendelt értéket, és - amennyiben van fedezet - engedélyezi a kommunikációt, azaz egy III.E. könyvelési visszaigazolás történik. Eközben a kommunikációs összeköttetést közvetlenül az I.B. háttérrendszer hozza létre és ellenőrzi. Ezáltal az I.B. háttérrendszer - az adatbankjában vezetett könyvelés alapján - a kártya teljes értékének elhasználása után az összeköttetést meg tudja szakítani.

Szabadalmi igénypontok

1. Eljárás pénz- vagy értékegységek biztonságos kezelésére előre fizetett adathordozókkal, amelyeket kártyakiadóval állítunk ki, elsősorban elektronikus könyvelési rendszerekhez, telefonkártya-rendszerekhez és elektronikuspénztárca-rendszerekhez, az adathordozót egy ismertetőjegy alapján egyértelműen azonosítjuk egy végkészülék és/vagy háttérrendszer(ek) felé, majd az adathordozóhoz hozzárendelt pénz- vagy egységértéket egy eladott, ill. megvásárolt árunak vagy szolgáltatásnak megfelelően a háttérrendszerben automatikusan csökkentjük és könyveljük, és a kommunikációt a végkészülékek és a hálózati csomópontok háttérrendszere(i) között folytatjuk,

a z z a l j e l l e m e z v e, hogy

egy ügyfél vagy felhasználó által előre kifizetett adathordozót (II.A.) egyetlen egyértelmű ismertetőjeggyel vagy azonosítójellel, például sorszámmal, kriptogrammal, rejtjelkulccsal vagy hasonlóval látunk el;

az ismertetőjegyhez vagy azonosítójelhez egy értéket rendelünk hozzá, és a kettőt együtt egy kommunikációs úton (III.B.) eljuttatjuk egy háttérrendszerbe (I.B.);

a háttérrendszerben (I.B.) letétbe helyezett, egyetlen meghatározott adathordozóhoz (II.A.) tartozó titkos kulcsot biztonsági felülvizsgálathoz használjuk fel válaszatok visszafejtésével; és

az adathordozónak (II.A.) küldött felszólítás és az onnan kapott válasz egyezésekor az adathordozót (II.A.) hitelesnek minősítjük.

2. Az 1. igénypont szerinti eljárás, a z z a l j e l l e m e z v e, hogy

a háttérrendszerrel (I.B.) közvetlenül hozzuk létre és ellenőrizzük a kommunikációs összeköttetést;

az adathordozók (II.A.) ismertetőjegyeként minden adathordozóhoz egy egyedi, nyilvános kriptográfiai kulcsot alkalmazunk; és

a kulcshoz vagy azonosítóhoz egy meghatározott tarifamodellrel rendelünk hozzá.

3. Az 1. vagy 2. igénypont szerinti eljárás, a z z a l j e l l e m e z v e, hogy

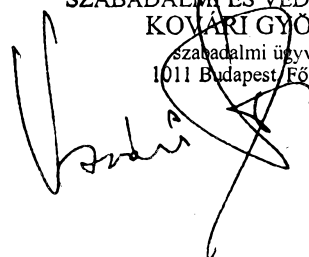
az illetéktelen leolvasást megnehezítő, bonyolult ismertetőjegyet alkalmazunk.

A meghatalmazott:



Alaprajz, labor

ADVOPATENT
SZABADALMI ÉS VÉDJEJY IRODA
KOVÁRI GYÖRGY
szabadalmi ügyvivő
1011 Budapest/Fő u. 19.



KÖZZÉTÉTELI
PÉLDÁNY

(A2)

1 / 1

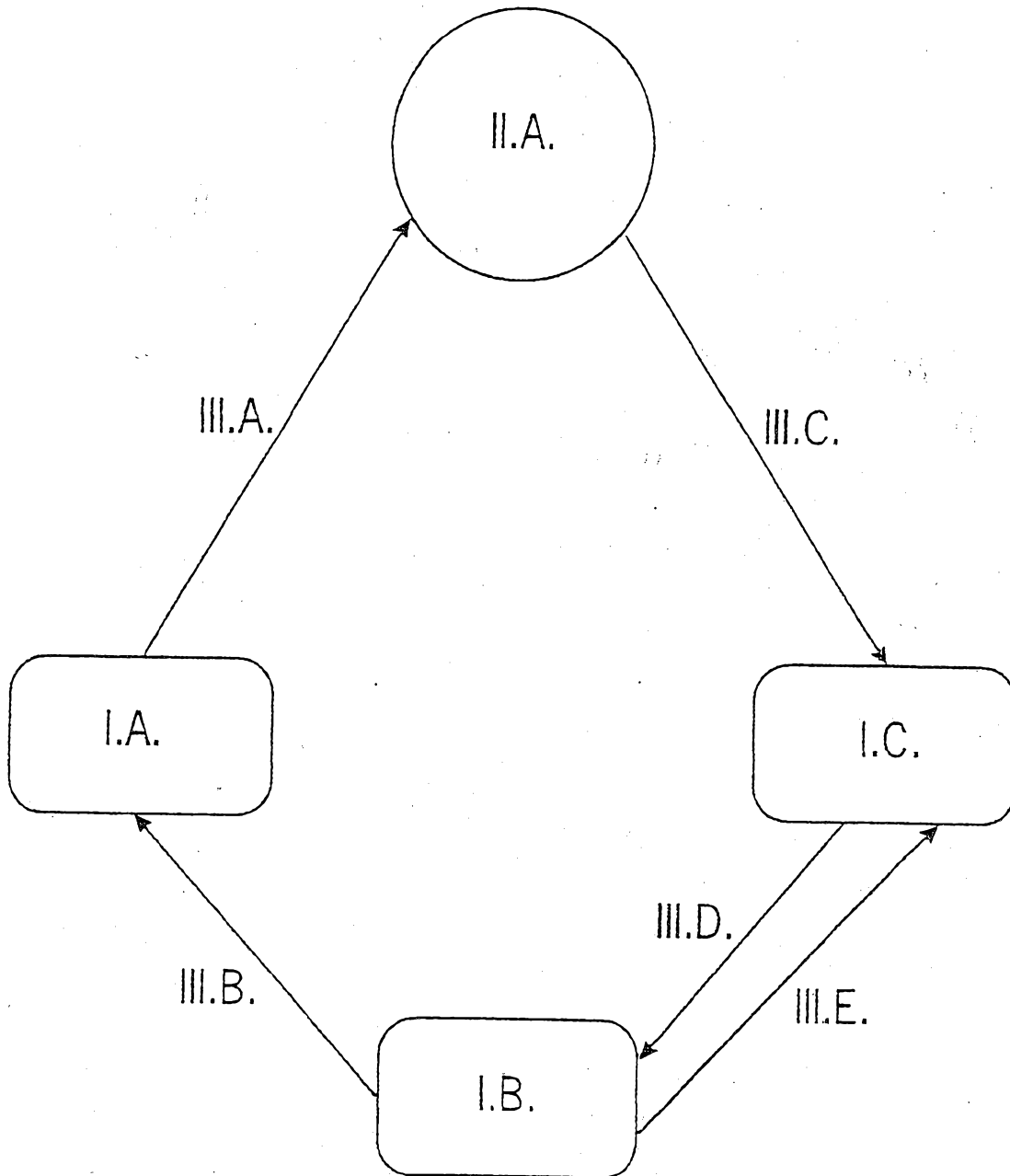


FIG. 1