73.275/KÖ

Kivonat

Mobil készülékek alkalmassá tétele törvénykövetelményekkel való egyezésre

Eljárás és mechanizmus egy mobil eszköz kommunikációval kapcsolatos műveleteinek dinamikus vezérléséhez, a mobil eszköz aktuális elhelyezkedési területén, és a vele kommunikáló számítástechnikai eszköz elhelyezkedési területén érvényes törvényi követelményeknek megfelelően, valamint a kommunikációs kapcsolat mindkét végén érvényes alkalmazói program kommunikációs követelményeinek megfelelően. A találmány alkalmas arra, hogy biztosítsuk egy mobil eszköz kommunikációjának a különböző országok kriptográfiai követelményeivel való egyezését, még abban az esetben is, ha a mobil eszköz átlép egy országhatárt kommunikáció közben.

P 0200571

S.B.G. & K.
Szabadalmi Iroda
[illegible]

73.275/KÖ

BEJELENTÉSI PÉLDÁNY

Mobil készülékek alkalmassá tétele törvénykövetelményekkel való egyezésre

Találmányunk tárgya mobil számítástechnikai eszköz, különösen a különböző országok olyan törvényességi követelményeinek, mint például kriptográfiai korlátozásoknak vagy más terület specifikus követelményeknek megfelelő működésmódosítást lehetővé tévő mechanizmus mobil eszközök számára, az országhatár átlépése esetében.

Különböző országokban különböző törvények érvényesek a megengedett kriptográfia erősségre és/vagy típusra vonatkozóan, beleértve az európai országokat, ahol néhány hivatalos szerv biztosítani akarja, hogy a jogosult jel elfogás technikailag megvalósítható maradjon. Például, van olyan ország, ahol megengedett az 512 bites kulcsokkal rendelkező RSA kriptográfiai algoritmus használata, de az 1024 bit hosszúságú kulcs használata nem. Vagy van olyan ország, ahol megengedett a DES használata, de nem megengedett a 3DES vagy bármilyen kriptográfiai algoritmus használata 128 bit hosszúságig. Vannak olyan esetek is, amikor bizonyos országok egy tilos listán vannak, ami azt jelenti, hogy nem megengedett az országban lévő vállalkozásokkal való titkosított adatok cseréje.

A mobil készülékek, például a cellatelefonok és a kommunikációra alkalmas Személyi Digitális Asszisztensek (Personal Digital Assistants/PDAs) a hang adatcserén kívül képesek alkalmazói programok futtatására, és a cella telefonokat gyakran használják hordozható számítógép mechanizmusaként egy hálózathoz való csatlakozáshoz, hogy adatcserét tegyünk lehetővé más számítógépekkel. (Az általunk használt cella telefon kifejezés bármilyen, cellarendszerű hálózatban alkalmazható telefonos eszközt jelent.) Bár az adatvédelmi kódolás/dekódolás előnyös az érzékeny tranzakciók, például egy on-line hitelkártya beszerzés vagy bizalmas információcsere lebonyolítása során, az adatfolyamok titkosítása különösen fontos a rádiós kommunikáció esetében, mivel a rádióval továbbított hírközlést könnyebb elfogni, mint a vezetékes kapcsolaton küldötteket.

Bármely vállalkozás vagy magánszemély, akik mobil környezetben, titkosított adatokat szeretnének kicserélni, csakúgy, mint a mobil számítástechnikai eszközöket forgalmazó vállalkozások, szembesülnek azzal a problémával, hogy hogyan biztosítható a mobil számítástechnikai eszközöket használó felek számára az adatcsere úgy, hogy az a kommunikációs kapcsolat mindkét végén megfeleljen az adott ország törvényes kriptográfiai követelményeinek. Ez egy különleges probléma, mivel a mobil eszközök mozgathatók az országhatárokon keresztül, így egy statikus megoldás nem lenne megfelelő. A probléma jelentkezik például olyan, hálózatba kapcsolt számítógépekkel rendelkező bankok esetében, amelyek lehetővé teszik a kommunikációt a mobil eszközökön futó alkalmazói programok és a bank számítógépes rendszerének alkalma-

zói programja között, és ugyanakkor szembesülnie kell ezzel a problémával a mobil eszköz felhasználójának is. A banknak egy olyan mechanizmusra van szüksége, amely biztosítja a különböző nemzeti törvényekkel való egyezést, ha a nemzetközi üzleti tevékenységét a megfelelő ország szabályozó hatóságának jóvá kell hagynia.

Az US 5781628 szabadalom ismertet egy eljárást, amelynek során szelektív adatátviteli titkosítás korlátozást végeznek egy telekommunikációs hálózaton belül, adott országok esetében, a titkosítási tiltásoknak megfelelően. Az említett szabadalom azonban csak a titkosítási lehetőség kiiktatásával foglalkozik, amikor az szükséges, és nem veszi figyelembe azokat a finomabb kriptográfiai követelményeket, amelyek sok országban érvényesek. Ilyenek lehetnek például, amint azt az előzőekben elmondtuk, hogy a kriptográfiai algoritmusok használata megengedett, ha a kulcs bit hosszúsága nem nagyobb egy meghatározott maximális értéknél, vagy amikor csak bizonyos kriptográfiai algoritmusok tiltottak.

Ezen felül, az US 5781628 szabadalom nem ismertet olyan mechanizmust, amely lehetővé teszi a kriptográfiai komponensek kiválasztását a kommunikációs eszközökön futó kommunikációs alkalmazói programok specifikus követelményeire vonatkozóan. Nem tartalmaz ismertetést olyan mechanizmusról, amely figyelembe veszi, hogy ténylegesen szükség van-e titkosításra. Az US 5781628 szabadalomban ismertetettek alapján lényegtelennek tűnhet, hogy az összes kriptográfiai funkciót ki kell-e iktatni az élőszavas hívások esetében (néhány ország szigorú törvényi követelményeinek

megfelelően), és nem biztosít megfelelő támogatást az olyan kommunikációs alkalmazói programok esetében, amelyek egy szükséges minimális biztonsági szinttel rendelkeznek. Az US 5781628 szabadalom nem teszi lehetővé a vonatkozó kriptográfiai korlátozások és alkalmazási követelmények megfontolását, és annak eldöntését, hogy vajon meg kell-e szakítani a kommunikációs kapcsolatot, vagy egy korlátozott kriptográfiai szintet használva kell-e folytatni.

A kriptográfiai követelmények egy a különböző országok törvényei közötti különbségek példái közül, és mint ilyen, a törvényi követelmények egy olyan példája, amely hasznosíthat egy, a mobil eszközökre vonatkozó különböző törvényekkel való egyezés biztosításához szolgáló eljárást és mechanizmust. Egy másik példa szerint, a törvénykezés megtilthatja, hogy egy számítástechnikai eszköz felhasználója tiltott országokon belül egy bizonyos technológiát használjon (például, ha az a technológia a védelemre vonatkozik). Egy további példa szerint, a törvénykezés megszabhatja, hogy egy pénzügyi intézmény elektronikai tranzakciójához milyen nyelvet kell használni.

Találmányunkkal eljárást és mechanizmust biztosítunk egy mobil eszköz működés teljesítményének dinamikus ellenőrzéséhez a mobil eszköz sajátos elhelyezkedésének törvényi követelményeinek megfelelően, és a felhasználói programok követelményeinek megfelelően, a kommunikációs kapcsolat mindkét végénél. Az ellenőrzött működések célszerűen kommunikációval kapcsolatos működések, mint például adatvédelmi kódolás és dekódolás vagy digitális aláírás alkalmazása.

A továbbiakban a mobil számítástechnikai eszköz elnevezést használjuk bármely olyan mobil eszközre vonatkozóan, amely alkalmas adatátvitelre és/vagy adatfeldolgozásra.

Találmányunk egyik célja egy olyan eljárás és mechanizmus biztosítása, amellyel lehetővé válik a kriptográfia erősségének és/vagy típusának automatikus váltása, amikor a mobil számítástechnikai eszközök átlépik az országhatárokat, vagy lehetővé válik a mobil eszköz kapcsolatának ellenőrzött módon való megszakítása.

Meghatározzuk az országot, ahol a mobil számítástechnikai eszköz elhelyezkedik, és azután információt szerzünk az azonosított országban megengedett kriptográfiai erősségek vagy típusok megállapításához. Például, a megengedett kriptográfiai erősségeket vagy típusokat azonosíthatjuk a megengedett vagy tiltott algoritmusok megnevezésével vagy a kulcs bithosszúságával. A megszerzett információ más ország specifikus kommunikációs tiltásokat vagy korlátozásokat is azonosíthat.

Ezután az adat titkosításhoz kiválasztunk egy megengedett algoritmust végrehajtó kriptográfiai komponenst a felhasználói programok követelményeinek megfelelően az adatátvitel mindkét végét illetően, és a kriptográfiai korlátozásokra vonatkozó információnak megfelelően, vagy megszakíthatjuk a kommunikációs kapcsolatot, vagy működésképtelenné tesszük az eszközt vagy megtiltjuk annak kódolási lehetőségét.

Az egyik megvalósításban a találmányt egy első számítástechnikai eszköz felhasználói kiszolgáló komponensében alkalmazzuk. A felhasználói kiszolgáló komponens alkalmas arra, hogy azono-

sítsa legalább azt az országot, ahol az első számítástechnikai eszköz elhelyezkedik, hogy információt szerezzen az azonosított országban, a törvényes előírások megszegése nélkül használható kriptográfiai komponensek meghatározásához. A felhasználói kiszolgáló komponens a megszerzett információnak megfelelően, és az első számítástechnikai eszköz első felhasználói programjának kommunikációs követelményeinek megfelelően vagy kijelöli, vagy érvényesíti egy kriptográfiai komponens kiválasztását az adatvédelmi kódoláshoz és dekódoláshoz.

Ha az első számítástechnikai eszköz kezdeményezi a kommunikációt, akkor célszerűen kezdeményezi a választás érvényesítését annak a második számítástechnikai eszközön telepített második felhasználói program kommunikációs követelményeinek megfelelően, amellyel az adatcserét kíván lebonyolítani. A második felhasználói követelményekre vonatkozó érvényesítés kezdeményezés egyszerűen lehet egy második számítástechnikai eszköznek küldött kérelem egy kommunikációs csatorna létrehozására, vagy lehet egy explicit érvényesítés kérelem.

Akár a megengedett kriptográfiai komponens azonosítására szolgáló információ megszerzése, akár egy kriptográfiai komponens kiválasztása vagy választás érvényesítése, akár a titkosított adat cseréjét megelőzően, az első vagy második számítástechnikai eszközön végzett következő érvényesítés, figyelembe veszi annak az országnak a kriptográfiai követelményeit, amelyben a második eszköz telepítve van, hogy biztosítsuk mind az első, mind a második eszköz telepítésének megfelelő ország követelményeivel való egyezést.

A kriptográfiai funkciók dinamikus kiválasztásában és egy kapcsolat megszakításának mérlegelésében az alkalmazási követelményeket illetően, találmányunk jelentős előnyöket biztosít az olyan mechanizmussal szemben, amely csupán a mögöttes kommunikációs verem eszközeire támaszkodik a kriptográfiai algoritmusok használatának engedélyezéséhez vagy megtiltásához. A találmány szerinti megvalósításban egy választási mechanizmust hajtunk végre a kommunikációs rendszer függvények egy rétegezett modelljének (például az OSI modellnek) az alkalmazói rétegén, és lehetővé tesszük, hogy az alkalmazói programok a követelményeik meghatározásával elősegítsék a kriptográfiai függvények egyeztetését, amely a kommunikációs rétegen végrehajtott választási mechanizmussal nem lenne lehetséges.

Így, az alkalmazói követelmények figyelembe vételével és az alkalmazói programok engedélyezésével, hogy hozzájáruljunk annak egyeztetéséhez, hogy melyik kriptográfiai algoritmust használjuk, vagy hogy megszakítsunk egy kapcsolatot, olyan egyeztetési eredményt érünk el, amely megfelelő az adott alkalmazásokra. Amikor egy kommunikációs eszköz átlép egy országhatáron, néhány alkalmazás lehetővé teszi a folytonos kommunikáció és alkalmazás végrehajtását egy más titkosítási algoritmus használatával vagy úgy, hogy nem használ titkosítást, míg más alkalmazói programok esetében a kapcsolat megszakad, ha a kommunikációs csatornára meghatározott kritériumok nem tarthatók fenn. Más szabályok esetleg az eszköz letiltását követelik meg. Mindegyik esetben, az alkalmazói követelményekre való utalás lehetővé teszi a megfelelő intézkedést.

A kommunikációs rétegen végrehajtott mechanizmusnak szükségszerűen jellemzőnek kell lennie az adott kommunikációs támogatásra (például TCP vagy GSM specifikus), míg találmányunk olyan szolgáltatást biztosít, amely szélesebb körben használható, mivel nem jellemző egy adott kommunikációs támogatás rétegre.

Egy, a találmány szerinti alkalmazás kiszolgáló komponens megvalósítható egy számítógép program termékként, amely egy számítógéppel olvasható adathordozó közegen tárolt, számítógéppel olvasható program kód, vagy egy számítástechnikai eszköz integrál komponenseként.

Találmányunk másik célja a 12. igénypont szerinti mobil számítástechnikai eszköz megvalósítása.

Találmányunk harmadik célja a 11. igénypont szerinti számítástechnikai berendezés megvalósítása.

A találmány előnyös megvalósításában egy kommunikációs csatorna létrehozása magában foglalja egy kriptográfiai komponens első kiválasztását a csatornán keresztül küldött adat kódolásához és dekódolásához. Ezt követően elvégezzük a kriptográfiai függvények érvényességének ellenőrzését passzív műveletként, amelyet bizonyos előre meghatározott események indítanak el. Ilyen esemény lehet a helyzet meghatározás egy országhatár átlépés észlelésekor, amelynek eredményeképpen egy mobil eszköz megszakadását idézzük elő, arra késztetve az alkalmazói programot, hogy ellenőrizze a kriptográfiai komponensek érvényességét az új ország kombináció esetében.

Egy másik megvalósításban egy aktív folyamatot használunk, amelynek során meghatározzuk az ország elhelyezkedését, ezután

megszerezzük és ellenőrizzük a megengedett kriptográfiai függvények listáját (vagy a kriptográfiai korlátozások listáját a megengedett kriptográfiai komponensek azonosításához), amikor az átvitelhez az adatot titkosítani kell.

Több olyan mechanizmus létezik, amely alkalmas egy mobil eszköz helyzetének azonosítására. A találmány egyik megvalósításában a cella telefonokra vonatkozóan, a telefon egy ország lekérdezést továbbít a cellarendszerű hálózat operációs rendszerének, vagy egy, a telefon mozgását jelző új közvetítő cella azonosító vételének válaszaként, vagy periodikusan, vagy adatcsere esetében. A cellarendszerű hálózat operációs rendszere ezután egy adatbázis visszakeresést hajt végre egy adott országra vonatkozó cella azonosító feltérképezéséhez. Egy másik megvalósításban műholdak lekérdezésével a Globális Helymeghatározó Rendszert (GPS) alkalmazzuk egy eszköz helyének azonosítására, amikor titkosított adatot akarunk kicserélni.

Találmányunk előnyös megvalósítását a csatolt ábrák alapján ismertetjük részletesen.

Az 1. ábrán egy mobil számítástechnikai eszköz és egy második számítástechnikai eszköz között, egy kommunikációs csatornán keresztül történő kommunikáció vázlatos ábrázolását mutatjuk, ahol az egyes számítástechnikai eszközök tartalmaznak egy, a találmány egyik megvalósítása szerinti alkalmazás kiszolgáló komponenst.

A 2. ábra egy folyamatábra, amely egy kriptográfiai komponens kiválasztásának és érvényesítésének lépéseit mutatja a találmány szerinti megoldásban.

Találmányunk egyik előnyös megvalósítása szolgáltatást nyújt mobil számítástechnikai eszközökön, mint például Személyi Digitális Asszisztenseken (PDA), laptopokon és palmtopokon (hordozható és marok számítógépek), járművekbe épített számítástechnikai eszközökön, és a legújabb generációs mobil telefonokon futó alkalmazói programok számára, csakúgy, mint az ezekkel a mobil eszközökkel kommunikáló számítástechnikai eszközökön futó alkalmazói programok számára.

Találmányunk lehetővé teszi a különböző országok törvényi követelményeinek való megfelelést az adatkódoláshoz/dekódoláshoz használható kriptográfiai algoritmusok erősségét és típusát illetően, és lehetővé teszi a helyi törvényekkel való egyezés fenntartását még abban az esetben is, amikor a mobil eszköz átlépi az országhatárokat. Találmányunk egy mechanizmust biztosít a használt kriptográfia erősségének és típusának dinamikus átváltásához, és lehetővé teszi a kapcsolatoknak szabályozott módon való megszakítását. Ismertetésünkben az országra való utalást bármely olyan földrajzi vagy politikai területre vonatkozóan használjuk, amely a kommunikációhoz sajátos kriptográfiai követelményekkel vagy más törvényi követelményekkel rendelkezhet.

Az 1. ábrán egy 10 mobil számítástechnikai eszközt mutatunk, példánkban egy cella telefont, amely alkalmas több installált 20 alkalmazói program futtatására. A mobil eszközön installált szoftver komponensek tartalmaznak egy 30 alkalmazás kiszolgáló komponenst, amely a kommunikációs funkciók rétegelt szervezetének az alkalmazási rétegén vannak elhelyezve (az ilyen rétegelt szervezet, amely a rétegek közötti adatáramlás támogatáshoz spe-

cifikus interfészekkel rendelkezik, általános a kommunikációs eszközök esetében). Az alkalmazási réteg a hétrétegű szabványos nyitott rendszerű összekapcsolás (OSI) modell és a megfelelő funkció réteg modellek legfelső rétege, és így közvetlen kommunikációs vezérlés szolgáltatást biztosít az alkalmazói programokhoz. Az alkalmazási réteg jellemzően az a réteg, amelyen azonosítjuk a kommunikáló partnereket, azonosítjuk az alkalmazói program átviteli sebességét és hibaarány („szolgáltatás minőség" paraméter) követelményeit, és azonosítjuk az adatszintaxis korlátozásokat.

A 30 alkalmazás kiszolgáló komponens lehet egy Java(TM) szoftver komponens, amely a Java Virtuális Gép (JVM) környezetben fut, a társtól társig szolgáltatás biztosításához az alkalmazói program futásideje alatt. A 30 alkalmazás kiszolgáló komponens lehet az alkalmazási rétegen rendelkezésre álló több alkalmazás kiszolgáló komponens közül egy, de az ilyen kiegészítő támogató szolgáltatás a találmány területén kívül esik. Az 1. ábra vázlatosan jelzi a funkciók rétegelt szervezetét, beleértve a 40 JVM-et, az eszköz 50 operációs rendszerét és a mögöttes 60 kommunikáció támogató rétegeket.

Példánkban a 10 mobil számítástechnikai eszköz egy cellarendszerű kommunikációs helyi hálózat 70 hozzáférés csomópontján („bázisállomás") és a 80 hálózaton keresztül kommunikál egy 90 távoli számítástechnikai eszközzel. A távoli rendszer lehet bármilyen kommunikációs eszköz, akár mobil, akár nem mobil, de az első példánkban feltételezzük, hogy a távoli rendszer egy számítógép hálózaton belül fixen elhelyezett vezetékes kapcsolattal

rendelkező számítógép rendszer. Feltételezzük, hogy a mobil telefonon futó 20 program egy bank 90 számítógép rendszerén futó 20' programmal van kapcsolatban. A mobil eszköz kezelője egyik számláról egy másikra való átutalásra ad utasítást. A bank és a mobil eszköz a manipulálás kizárásának biztosításához normálisan titkosítja az adatfolyamot.

Amikor a 10 mobil számítástechnikai eszközön futó 20 alkalmazói program adatcserét kezdeményez egy 90 távoli rendszer 20' alkalmazói programjával, egy kommunikációs csatornát hozunk létre. A csatorna létrehozása során a 100 lépésben (2. ábra) meghatározunk egy paraméter készletet a csatorna számára, beleértve a célcím meghatározást, egy csatorna azonosító kijelölését, az időbélyegezést és egy kriptográfiai komponens, egy kompresszor és egy hitelesítő követelményeinek azonosítását, amelyeket a kommunikáció alatt szándékozunk használni. A csatorna csatlakozik a kompresszorhoz, a hitelesítőhöz és a titkosítóhoz. Az alkalmazói program jellemzően meghatároz egy szolgáltatás minőség követelmény készletet a kommunikációs csatorna számára, és a csatorna csak akkor jön létre, ha a 30 alkalmazás kiszolgáló komponens döntése szerint az alkalmazói követelmények teljesíthetőek.

A titkosítónak, azaz egy kriptográfiai objektumnak az alkalmazás kiszolgáló komponens ellenőrzése alatt és az alkalmazói program követelményei szerint való kiválasztását a 2. ábra alapján ismertetjük részletesen.

Először, a mobil eszköz a 110 lépésben meghatározza az aktuális helyzetét. A helyzet meghatározáshoz többféle mechanizmus

áll rendelkezésünkre. Egy cella telefon esetében célszerűen a mobil eszköz alkalmazás kiszolgáló komponensével végezzük, úgy, hogy lekérdezünk egy, a cella rendszerű hálózaton keresztül elérhető adatbázist, amely az ország helymeghatározás információhoz hálózat cella azonosítókat (cella ID-ket) tartalmazó feltérképező információt tartalmaz. A helyi hálózat cellára vonatkozó cella ID-t a telefon lekérdezése tartalmazza, ezt a cella ID-t előzőleg a helyi hálózat hozzáférés csomópont vagy bázisállomás közvetítette. Ez a bázisállomás által való cella ID közlés ismert a technikában, de az információ előzőleg nem volt elérhető a mobil eszközök alkalmazás kiszolgáló komponensével való felhasználásra. A cella rendszerű hálózat az adatbázis lekérdezés eredményeképpen egy ország helymeghatározás azonosítót küld.

Ezután, a 30 alkalmazás kiszolgáló komponens a 120 lépésben ellenőrzi a hálózat hozzáférés csomóponttól kapott cella ID-t, hogy megállapítsa, hogy mikor változik meg a cella ID, mivel ez jelzi, hogy a mobil eszköz elhelyezkedése megváltozott. Ezeket az egymást követő ellenőrzéseket a későbbiekben ismertetjük.

A mobil eszköz alkalmazás kiszolgáló komponense ezután a 140 lépésben ellenőrzi az azonosított ország kriptográfiai követelményeit. A különböző országok kriptográfiai korlátozásainak listáját előnyösen egy, a mobil eszköz nem felejtő memóriájában (például egy cella telefon ROM-jában) lévő táblázatban tároljuk, úgy, hogy egy táblázatból való adat kikereső műveletet végzünk el helyileg, keresési kulcsként az adatbázis lekérdezéssel kapott ország helymeghatározás azonosítót használva, anélkül, hogy egy harmadik félre támaszkodnánk a törvényi követelmények listá-

jának fenntartásához. A találmányunk szerinti, Java környezetben megvalósított példában az azonosított ország kriptográfiai követelményeire vonatkozó kapott információ alkotja a Java helyszín objektum paramétereket.

Az alkalmazás kiszolgáló komponens ezután a 150 lépésben ellenőrzi a rendelkezésre álló kriptográfiai algoritmusok érvényességét, miközben figyelembe veszi a 160 lépésben az alkalmazás specifikus biztonsági követelményeket.

Például, egy alkalmazói program meghatározhatott egy minimális biztonsági szintet vagy egy megkívánt biztonsági szintet, meghatározva például egy adott előírt kriptográfiai algoritmust (úgymint 3DES) vagy az elfogadható kriptográfiai kulcs bithosszúságának tartományát (például 128 bit vagy több). A meghatározott alkalmazási követelményeket a 160 lépésben az alkalmazás kiszolgáló komponens összehasonlítja az adott eszköz elhelyezkedését illető kriptográfiai korlátozások listájával, és a rendelkezésre álló kriptográfiai komponensek kriptográfiai erejével és típusával. Azokat a rendelkezésre álló kriptográfiai komponenseket, amelyek összes alkalmazói program követelményt és törvényi korlátozást kielégítik, érvényesként azonosítjuk a 170 lépésben, és kiválasztunk közülük egyet.

Bizonyos mobil eszközök esetében, például PDA-k esetében, a memória erőforrások olyan korlátozottak lehetnek, hogy célszerű, ha a különböző országok kriptográfiai korlátozásainak listáját nem magában a mobil eszközben tároljuk. Ezért, vagy hogy lehetővé tegyük, hogy ugyanazt a mobil eszközt egy másik felhasználó használhassa a biztonság veszélyeztetése nélkül, vagy hogy lehe-

tővé tegyük az aktuális törvényi követelmények karbantartását anélkül, hogy magát a mobil eszközt aktualizálni kellene, a korlátozások listáját és más kommunikációs szabályokat tárolhatjuk egy, a mobil eszközbe behelyezhető intelligens kártya biztonságos fájljain belül. Az intelligens kártya tartalmazhatja a mobil eszköz felhasználójának nyilvános és magánjellegű kriptográfiai kulcsait, és az előzőleg kijelölt kommunikációs partnerek nyilvános kulcsait.

Az intelligens kártya mellett egy kevésbé előnyös megoldásváltozat, ha a mobil eszköz egy távoli adatbázisról lekérdezi a kriptográfiai korlátozások listáját az eszköz elhelyezkedéseként azonosított országra vonatkozóan, és ezután ennek a listának a használatával végzi el a kriptográfiai komponensek érvényességének ellenőrzését.

Miután kiválasztottunk egy első kriptográfiai komponenst, amely kielégíti a helyi törvényi követelményeket és a helyi alkalmazási követelményeket, az alkalmazás kiszolgáló komponens a 180 lépésben elküldi a csatorna kérelmet egy 70 távoli számítástechnikai eszközön lévő tárgy alkalmazói programnak. Ez a kérelem tartalmazza a különböző meghatározott paramétereket a csatornára vonatkozóan, beleértve az érvényes kriptográfiai komponensek készletéből kiválasztott kriptográfiai komponens azonosítóját, egy kompresszort és egy hitelesítőt, és a küldő nyilvános kriptográfiai kulcsát. A nyilvános kulcsokat jellemzően digitálisan aláírjuk a kicserélést megelőzően, hogy lehetővé tegyük az azt követő hitelesítést.

Példánkban, ahol a távoli tárgy eszköz egy nagy hálózatba kapcsolt számítógép rendszer, a tárgy alkalmazói program lehet egy banki alkalmazás. Az adott példában a tárgy rendszer feltételezhetően nagyobb ellenőrzéseket hajt végre, mint a mobil telefonokon telepített alkalmazói programok közötti társtól társig kommunikáció esetében, már csak az olyan szabályozások miatt is, amelyek az on-line kérelmeket támogató pénzintézetek számára előírtak. Azaz, a bank rendszere várhatóan kötelezővé teszi az érvényes kriptográfiai komponensek kiválasztását a helyi korlátozásokat illetően, a mobil kommunikációs eszközre vonatkozóan, csakúgy, mint a saját elhelyezkedését illető kriptográfiai korlátozásokra vonatkozóan.

Így a találmányunk körébe tartozik egy olyan eljárásmód, amelynek során csak az aktuális eszköz elhelyezkedésre vonatkozó helyi követelményeket és az aktuális alkalmazás követelményeket ellenőrizzük, vagy egy olyan eljárásmód, amelynek során ellenőrizzük az egyik vagy mindkét kommunikációs eszközre vonatkozó törvényi követelményeket, amelyek a kommunikációs kapcsolat mindkét végén érvényesek.

A bank számítógép rendszerén lévő alkalmazás kiszolgáló komponens a mobil eszköztől érkező kommunikációs csatorna létrehozására irányuló kérésre a 190 lépésben meghatározza a mobil kommunikációs eszköz elhelyezkedését, például a cella telefontól érkező kérésben lévő explicit ország helymeghatározás azonosító visszakeresésével, vagy a kérésben lévő cella ID használatával, az adatbázis lekérdezéshez. Ha a kérésben nincs helymeghatározá-

si információ, akkor a vevő alkalmazás kiszolgáló komponens nem fogadja a hívást.

A mobil eszköz helyzet meghatározó információjának megszerzését követően, a tárgy számítógép rendszer alkalmazás kiszolgáló komponense a 190 lépésben visszakeresi a saját ország (helyben tárolt) helymeghatározás információját, és mindkét helyzet meghatározó azonosítót betáplálja egy programba, amely a 200 lépésben adatkikeresést végez egy táblázatból, a törvényes kriptográfiai követelmények azonosításához minkét elhelyezés esetében. Ezt követően, a 210 lépésben ellenőrzést hajtunk végre, hogy biztosítsuk az egyezést a kriptográfiai korlátozások és a tárgy számítógép rendszer alkalmazói program követelményei között, ahogy azt az előzőekben a mobil eszköz esetében ismertettük.

Megjegyezzük, hogy amíg a mobil eszközre vonatkozó helyzet meghatározó információ a tárgy számítógép rendszer rendelkezésére áll, találmányunk szerint egy lehetséges változatban a mobil számítástechnikai eszköz támaszkodhat annak a tárgy számítógép rendszernek az alkalmazás kiszolgáló komponensére, amellyel kommunikációt folytat, ahhoz, hogy elvégezzük e kriptográfiai korlátozások ellenőrzését mindkét elhelyezkedés esetében. Ha a mobil eszköz alkalmazói programjára vonatkozó csatorna kritériumokat elküldjük a tárgy számítógép rendszernek, akkor a tárgy rendszer alkalmazás kiszolgáló komponense elvégezheti a kriptográfiai komponens kiválasztását vagy érvényesítését is. Ebben az esetben, a kiválasztás és érvényesítés funkciókat nem lehet megismételni a mobil eszközön.

Így a mobil eszköz és a tárgy számítógép rendszer alkalmazás kiszolgáló komponense rendelkezik az összes olyan információval, amely szükséges a csatorna paramétereinek egyeztetéséhez, beleértve, hogy melyik kompresszort és hitelesítőt kell használni, és annak a kriptográfiai komponensnek a kiválasztását, amelyik kielégíti mind az alkalmazási követelményeket, mind az elhelyezkedés törvényi követelményeit, vagy hogy az alkalmazás kiszolgáló komponens döntést hozhasson arról, hogy a kapcsolat nem jöhet létre, ha az alkalmazás biztonsági szint követelményei nem teljesülnek, és a vonatkozó kriptográfiai korlátozások nem egyeznek.

Azaz, az alkalmazás kiszolgáló komponens a kommunikációs csatorna mindkét végén együttesen eldönti, hogy:

Dinamikusan megváltoztatja a kriptográfia vagy a kulcs jellemzőit,

Megszakítja a kapcsolatot, vagy

Megbénítja az eszközt.

Ha a kezdetben a mobil eszköz követelményeivel (elhelyezkedés specifikus törvények és alkalmazási követelmények) egyezőként kiválasztott kriptográfiai komponens nem elfogadható a tárgy rendszer számára, akkor a 220 lépésben kísérletet teszünk arra, hogy a rendelkezésre álló kriptográfiai komponensek közül azonosítsunk egyet, amely megfelel a csatorna mindkét végén támasztott követelményeknek. Jellemzően a tárgy rendszer egy olyan kriptográfiai komponens változat azonosításával felel, amely kielégíti annak követelményeit. Ha ez a változat nem elfogadható a mobil eszköz számára, akkor a mobil eszköz al-

kalmazás kiszolgáló komponense elküldi a tárgy rendszernek annak a kriptográfiai komponens készletnek az azonosítóját, amely kielégíti a mobil eszköz követelményeit, így a tárgy rendszer ezután végleges választást végezhet, vagy döntést tud hozni arról, hogy a kommunikáció nem folytatható. Egy másik változatban, a javasolt kriptográfiai komponensek azonosítóinak kicserélése folytatódhat addig, amíg az eszköz érvényes kriptográfiai komponensek listája ki nem merül, vagy befejezhetjük a csatorna paraméterek egyeztetését, ha egy előre meghatározott időn belül vagy egy előre meghatározott számú kommunikációs folyam közben nem kapunk pozitív eredményt.

Az egyeztetési folyamatot a „kézfogásos" egyeztetés más aspektusaival egyidejűleg végezhetjük, beleértve a kompresszor kiválasztását, a hitelesítő kiválasztását, az egyeztetés átviteli sebességet és a kommunikációs protokollt, stb. Az adat titkosítását, tömörítését és hitelesítését ezután a 230 lépésben végezzük el, az adatátvitelt megelőzően, az egyeztetett funkcióknak megfelelően.

A csatorna létrehozás során végrehajtott kiválasztási és érvényesítési folyamaton kívül további érvényesítés szükséges ahhoz, hogy kezelhessük azt az esetet, amikor a mobil eszköz a kommunikáció közben átlépi az országhatárt. A csatorna létrehozást követő érvényesítés végrehajtásának lehetséges módjai a következők:

1. Az első mód egy „aktív" mód, amelynek során a mobil eszköz elhelyezkedésének ellenőrzését (és a kriptográfiai komponensek érvényesítését az ország változtatásakor), amelyet az előző-

ekben a csatorna létrehozással kapcsolatban ismertettünk, a 120 lépésben megismételjük, minden esetben, amikor titkosított adatot küldünk vagy fogadunk. Az adatkódolást vagy dekódolást közvetlenül megelőzően, egy szabály rutint hívunk segítségül, továbbítva egy kriptográfiai típust, a titkosítandó adatot, és bármilyen lényeges kriptográfiai kulcsot. A szabály rutin lekérdezi az elhelyezkedést, felhasználja a helyzet meghatározó információt a hely kommunikációs követelményei listájának eléréséhez, és aktualizálja a helyszín paramétereket, és igazolja, hogy a meghatározott kriptográfiai típus és kulcs hosszúság elfogadható a meghatározott hely esetében.

Ez a mód a hálózati kommunikáció növekedését eredményezi, mivel minden egyes helymeghatározás ellenőrzés, és esetleg a kriptográfiai korlátozások listájához való hozzáférés, hálózati kommunikációt igényel. Az aktív módon történő helymeghatározást követjük, amikor GPS-t használunk, mivel a GPS a műholdak aktív lekérdezését igényli.

2. A második mód a „passzív" mód, amelynek során a 120 hely ellenőrzést és érvényesítést csak akkor végezzük el, amikor egy meghatározott esemény következik be, például az egyik kommunikációs eszköz átlépi az országhatárt. Az előzőekben ismertetett cella telefonos példában ez a 30 alkalmazás kiszolgáló komponens vezérlésével valósítható meg, úgy, hogy az alkalmazás kiszolgáló komponens megvizsgálja a bázisállomásról kapott cella ID-ket, és csak akkor kezdeményez helymeghatározást, amikor változást észlel a cella azonosítás során.

Általában, ha a 130 helymeghatározás lépés során meggyőződünk arról, hogy a mobil eszköz nem lépett ás országhatáron, akkor a találmány azon megvalósításaiban, amelyekben a mobil eszköz csak a saját kommunikációs végét ellenőrzi, nem szüksége további lépéseket tennünk a helyi érvényesítéshez, és a távoli számítástechnikai eszközzel való kommunikáció folytatódik. Mindazonáltal, a mobil számítástechnikai eszköz elküldi a helyzeti információját a távoli számítástechnikai eszköznek minden alkalommal, amikor ezt az információt megszerzi, hogy lehetővé váljék, hogy a távoli számítástechnikai eszköz aktuális információt tartson fenn az eszköz helyzetéről egy beszélgetés egész ideje alatt.

Ha a helyazonosítási művelet azt a tényt erősíti meg, hogy országhatár átlépés történt, akkor a mobil eszköz egy megszakítást idéz elő, amely után a 140 lépésben visszakeressük az ország specifikus kriptográfiai korlátozások listáját, és aktualizáljuk a helyszín ország specifikus paramétereit. Ezután ezt a listát összehasonlítjuk a 150, 160 lépésben az alkalmazás követelményekkel a lehetséges kriptográfiai komponensek készletének azonosításához, vagy a kiválasztott kriptográfiai komponens érvényességének igazolásához, ahogy azt az előzőekben ismertettük.

A kriptográfia szinteket és/vagy titkosítás kulcs hosszúságokat ezután dinamikusan újra egyeztetjük a kommunikációs kapcsolat másik végével. Az alkalmazás követelményeitől és az adott törvényi követelményektől függően a kapcsolat megszakítható, vagy az alkalmazás megszüntethető vagy törölhető, vagy az eszköz lezáródik. Kódolás esetén a helyzet információt a kimenő adathoz

csatoljuk. Dekódolás esetén a dekódoló eszköz helyzetét és a bejövő adatba beágyazott helyzet információt egyaránt figyelembe vesszük.

Ezután elvégezzük a tényleges kódolást vagy dekódolást. A feldolgozás során figyelembe vesszük mind az adat eredő helyét, mind a fogadási helyét.

A fentiekben foglaltaknak megfelelően, a mobil eszköz alkalmazás kiszolgáló komponense alkalmas arra, hogy legalább a saját eszköz elhelyezkedésének ellenőrzését elvégezze, és, hogy kiválassza a helyi törvényi korlátozásoknak megfelelő kriptográfiai komponenseket, vagy érvényesítse azok kiválasztását. A csak a saját helyzet figyelembe vétele elegendő lehet olyankor, amikor a mobil eszköz adatot küld egy távoli tárgy eszköz számára, ha számíthatunk arra, hogy a tárgy eszköz elvégzi a saját értékelését a helyi törvényi korlátozásoknak való megfelelést illetően. A kriptográfiai és más kommunikációs korlátozásokkal való egyezés teljesebb ellenőrzése magában foglalja azt az esetet, amikor a mobil eszköz meghatározza a távoli kommunikációs eszköz helyét, csakúgy, mint a saját helyzetét, úgy, hogy egy helyzetlekérdezést küld a távoli eszköz számára. A lekérdezés eredményeit ezután összehasonlíthatjuk az ország specifikus kriptográfiai korlátozások listájával, mint az eszköz saját helyzet információjával. Ehhez az szükséges, hogy mindegyik kommunikációs eszköz elküldje a saját helyzet információját a kommunikációs partnernek, vagy, hogy mindegyik eszköz képes legyen arra, hogy valamilyen módon mindkét eszköz elhelyezkedését azonosítsa.

Hasonló módon, amikor a mobil eszköz titkosított adatot fogad, akkor a mobil eszköz alkalmazás kiszolgáló komponense célszerűen ellenőrzi a kriptográfiai komponensek érvényességét mind a saját elhelyezkedésére, mind az adatküldő eszköz elhelyezkedésére vonatkozóan.

Egy cella telefon helyzet meghatározása többféle módon végezhető el. Például alkalmazhatjuk a Globális Helymeghatározó Rendszert (GPS), amennyiben a műholdas kommunikáció költségei nem jelentenek akadályt. Minden alkalommal, amikor adatot akarunk küldeni, lekérdezzük a műholdakat, és a GPS által szolgáltatott pozíció koordinátákat leképezzük egy adott országra az országhatárok adatbázisát használva. Az országhatárokat kielégítő pontossággal körülírhatjuk sokszögekként, és ezután a koordináták országokra való leképezése viszonylag egyszerű. Ennek ismertetését megtalálhatjuk például az US 5781628 szabadalomban.

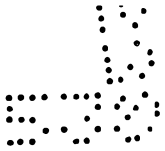
De más helyzet meghatározó mechanizmust is alkalmazhatunk. A cellarendszerű telefonhálózatban például periodikusan jelezhetjük az ország helyzet információt a mobil eszköz számára, úgy, hogy az eszköznek nem kell lekérdezést kezdeményeznie az adatküldést vagy fogadást megelőzően. A hálózat hozzáférési állomások tartalmazhatják az ország helyzet információt a közvetített cella ID-vel.

Mint ahogy az a fenti példa megvalósításából kiderül, a helyzet meghatározási műveletet elvégezhetjük csak az egyik kommunikációs eszközzel, úgy, hogy mindkét eszközre vonatkozóan felhasználjuk a helyzet információt, vagy a kommunikáció mindkét végén elvégezzük a kiválasztást vagy kiválasztás érvényesítést.

A találmány egyik megvalósítását az alkalmazás kiszolgáló komponensre vonatkozóan ismertettük, amely alkalmas arra, hogy a mobil eszközzel folytatott kommunikációt egyeztesse a különböző kriptográfiai törvényekkel. Találmányunkkal lehetővé válik nemcsak a kódolás dekódolás, de a mobil eszközök esetében más műveletek elvégzésének dinamikus vezérlése is, azoknak a törvényi követelményeknek megfelelően, amelyek a mobil eszköz aktuális elhelyezkedési területén érvényesek, és a kommunikációs kapcsolat mindkét végén érvényes alkalmazói program követelményeinek megfelelően.

A találmány más alkalmazásainak példái biztosítják azokkal a törvényekkel való egyezést, amelyek egy adott országon belül megtiltják bizonyos technológiák használatát (például, ha az a technológia a védelemre vonatkozik), és azokkal a törvényekkel való egyezést, amelyek megszabják, hogy milyen nyelvet kell használni, vagy azt a technikai kritériumot, amelynek meg kell felelni a pénzintézetek elektronikus tranzakcióihoz használt digitális aláírás esetében. Az előbbi példában, a helyzet meghatározást annak ellenőrzése követi, hogy a mobil eszköz aktuális elhelyezkedése olyan területen van-e, ahol az eszköz használata tilos. Ebben az esetben az eszköz működésképtelenné válik. A nyelvhasználati követelmény példájában kiválaszthatunk egy fordító szoftver komponenst ahhoz, hogy biztosítsuk az átvitt adatoknak a nyelvi követelményekkel való egyezését.

A digitális aláírás példájában megszerezhetjük a szükséges technikai kritériumokra vonatkozó információt, és azután azt használjuk a specifikus digitális aláírás algoritmus kiválasztá-



sában. Csakúgy, mint a mobil eszköz esetében végzett ország helyzet meghatározás, szükséges lehet, hogy a pénzügyi tranzakció utasítások ön-azonosítóak legyenek, úgy, hogy az ország törvényi követelményeinek ellenőrzését elindíthassuk, amikor egy utasítás egy pénzügyi tranzakció részeként azonosítja magát. Az alkalmazás kiszolgáló komponens végrehajthatja az ilyen szubjektum azonosítókra vagy más programindítókra válaszoló logikát.

Szabadalmi igénypontok

1. Számítógép program egy első számítástechnikai eszközön futtatott alkalmazói programok kommunikációs szolgáltatásainak biztosításához, azzal jellemezve, hogy az első számítástechnikai eszköz a számítógép program vezérlésével a következő folyamatokat hajtja végre:

reagál legalább az első számítástechnikai eszköz elhelyezkedésének ország azonosítására, az azonosított országban megengedett kriptográfiai komponensek meghatározásához szolgáló információ megszerzésével; és

kiválaszt vagy érvényesít egy kriptográfiai komponens kiválasztást a megszerzett információnak megfelelően, és az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően, az adat kódolásához vagy dekódolásához.

2. Az 1. igénypont szerinti számítógép program, azzal jellemezve, hogy a választás érvényesítést az első számítástechnikai eszköz, vagy egy, az első számítástechnikai eszközzel kommunikáló második számítástechnikai eszköz végzi, a második számítástechnikai eszköz egy második alkalmazói programjának kommunikációs követelményeinek megfelelően.

3. A 2. igénypont szerinti számítógép program, azzal jellemezve, hogy ha nem sikerül olyan kriptográfiai komponenst kiválasztani vagy választást érvényesíteni, amely mind az első, mind a második alkalmazói program követelményeit kielégíti, akkor a kommunikációs kapcsolat megszakad.

4. Az 1-3. igénypontok bármelyike szerinti számítógép program, azzal jellemezve, hogy a választás érvényesítését az első számítástechnikai eszköz vagy egy, az első számítástechnikai eszközzel kommunikáló második számítástechnikai eszköz végzi, a második számítástechnikai eszköz elhelyezkedésének országában megengedett kriptográfiai komponensek meghatározásának megfelelően.

5. Az 1-4. igénypontok bármelyike szerinti számítógép program, azzal jellemezve, hogy kezdeményezi az első számítástechnikai eszköz elhelyezkedésének ország azonosítását, amikor egy kommunikációs kapcsolat jön létre az első számítástechnikai eszköz alkalmazói programja és egy távoli alkalmazói program között.

6. Az 5. igénypont szerinti számítógép program, azzal jellemezve, hogy a kommunikáció közben bekövetkező meghatározott eseményekre való reagálásként ismételten kezdeményezi az elhelyezkedés ország azonosítását.

7. A 6. igénypont szerinti számítógép program, azzal jellemezve, hogy a meghatározott események tartalmazzák az adat kódolásra vagy dekódolásra irányuló utasítás feldolgozását.

8. A 6. vagy 7. igénypont szerinti számítógép program egy telefonos kommunikációs eszköz működésének vezérléséhez, azzal jellemezve, hogy a meghatározott események tartalmazzák egy új cella azonosító fogadását egy cellarendszerű hálózat hozzáférés csomóponttól.

9. A 6-8. igénypontok bármelyike szerinti számítógép program, azzal jellemezve, hogy a megengedett kriptográfiai kompo-

nensek azonosításához való információszerzést és egy kriptográfiai komponens kiválasztását vagy a választás érvényesítését csak akkor ismétli meg, amikor az elhelyezkedés országa megváltozott.

10. Eljárás egy első számítástechnikai eszköz működésének vezérléséhez, azzal jellemezve, hogy az eljárás során:

legalább az első számítástechnikai eszköz elhelyezkedésének ország azonosítására való reagálásként információt szerzünk az azonosított országban megengedett kriptográfiai komponensek meghatározásához, és

kiválasztunk vagy érvényesítünk egy kriptográfiai komponens kiválasztást a megszerzett információnak megfelelően, és az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően, az adat kódolásához és dekódolásához.

11. Számítástechnikai berendezés egy mobil számítástechnikai eszközzel való kölcsönös működéshez, a számítástechnikai berendezés tartalmaz egy vezérlőt a számítástechnikai berendezés működésének vezérléséhez, mind a számítástechnikai berendezés elhelyezkedését, mind a mobil eszköz elhelyezkedését illető törvényi követelményekkel való egyezés biztosítására, azzal jellemezve, hogy a vezérlő tartalmaz:

eszközt a mobil számítástechnikai eszköz elhelyezkedésének ország azonosítására való reagáláshoz, a mobil eszköz elhelyezkedéseként azonosított országban megengedett kriptográfiai komponenseket meghatározó, és a számítástechnikai berendezés elhe-

lyezkedésének országában megengedett kriptográfiai komponenseket meghatározó információ megszerzésével, és

eszközt egy kriptográfiai komponens kiválasztásához vagy a kiválasztás érvényesítéséhez a megszerzett információnak megfelelően, és a mobil számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően, az adat kódolásához és dekódolásához.

12. Mobil számítástechnikai eszköz, amely tartalmaz egy vezérlőt az eszköz működésének vezérléséhez, az eszköz aktuális elhelyezkedését illető törvényi követelményekkel való egyezés biztosítására, azzal jellemezve, hogy a vezérlő tartalmaz:

eszközt legalább a mobil számítástechnikai eszköz elhelyezkedésének ország azonosítására való reagáláshoz, az azonosított országban megengedett kriptográfiai komponenseket meghatározó információ megszerzésével, és

eszközt egy kriptográfiai komponens kiválasztásához vagy a kiválasztás érvényesítéséhez a megszerzett információnak megfelelően, és a mobil számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően, az adat kódolásához és dekódolásához.

13. Az 1. igénypont szerinti számítógép program, azzal jellemezve, hogy a kiválasztott kriptográfiai komponens egy digitális aláírás komponens.

14. A 13. igénypont szerinti számítógép program, azzal jellemezve, hogy a megengedett komponensek meghatározásának és a kiválasztásnak vagy a kiválasztás érvényesítésének végrehajtása egy pénzügyi tranzakció utasítás azonosítóra való reagálás.

15. Az 1-9. igénypontok bármelyike szerinti számítógép program, azzal jellemezve, hogy tartalmaz eszközt egy hitelesítő komponens kiválasztásához vagy kiválasztás érvényesítéséhez, az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően.

16. Az 1-9. vagy 15. igénypontok bármelyike szerinti számítógép program, azzal jellemezve, hogy tartalmaz eszközt egy tömörítő komponens kiválasztásához vagy kiválasztás érvényesítéséhez, az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően.

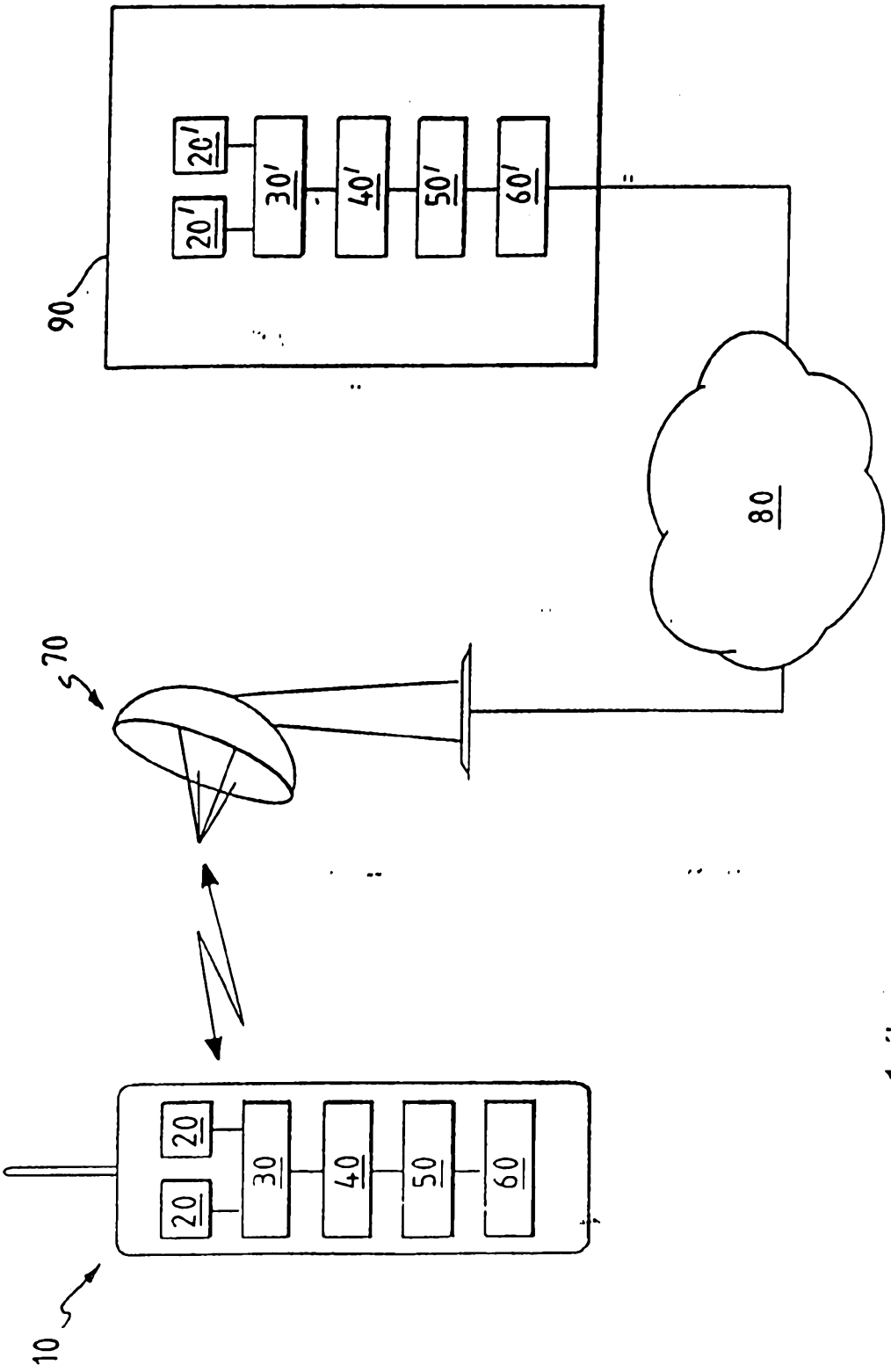
17. A 10. igénypont szerinti eljárás, azzal jellemezve, hogy az eljárás során kiválasztunk vagy érvényesítünk egy hitelesítő komponens kiválasztást az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően.

18. A 10. vagy 17. igénypont szerinti eljárás, azzal jellemezve, hogy az eljárás során kiválasztunk vagy érvényesítünk egy tömörítő komponens kiválasztást az első számítástechnikai eszköz legalább egy első alkalmazói programjának kommunikációs követelményeinek megfelelően.

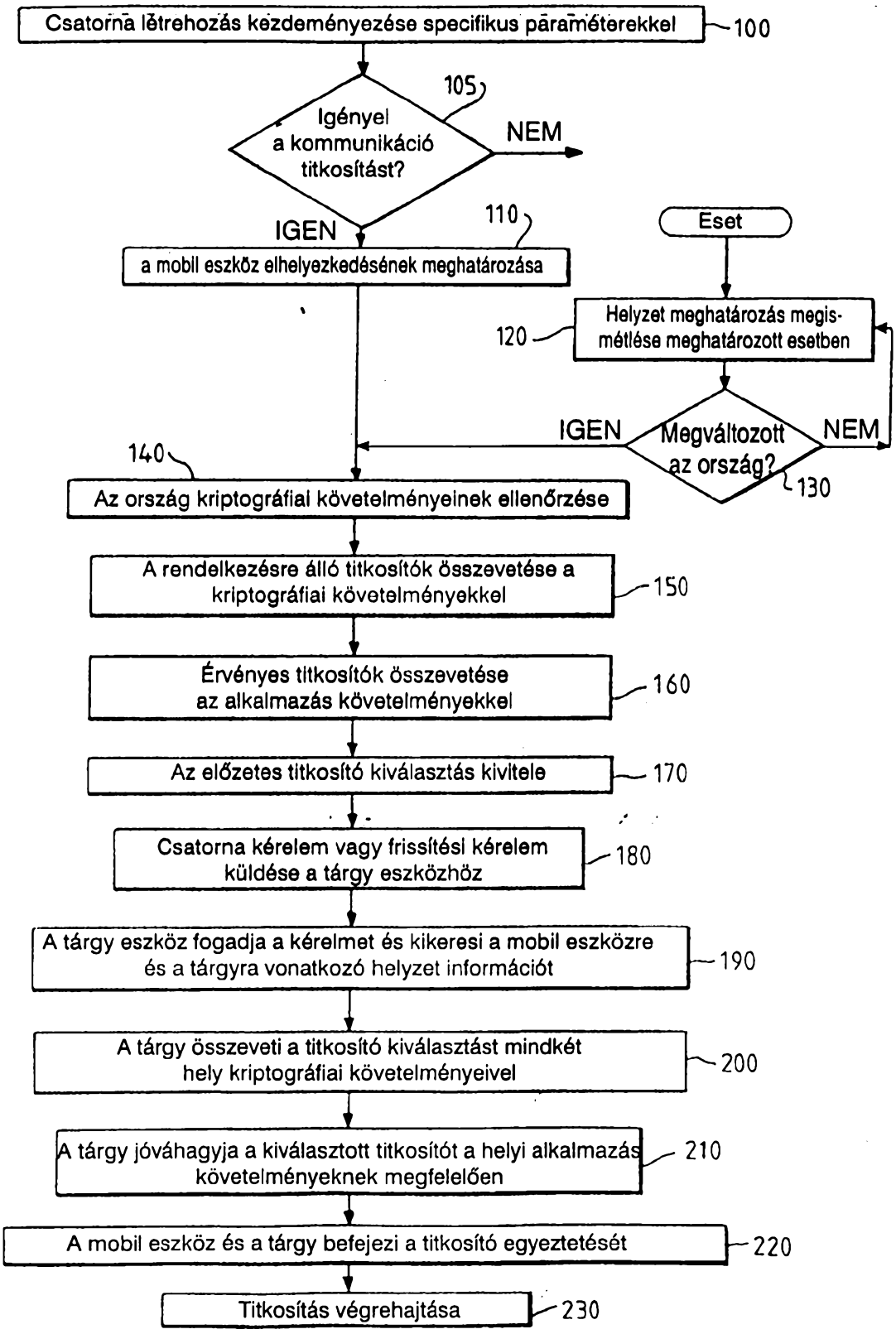
2002. [illegible]

A meghatalmazott

Dr. Köteles Zoltán
szabadalmi ügyvivő
az S.B.G. & K. Szabadalmi Ügyvivői Iroda
tagja
H-1062 Budapest, Andrássy út 113.
Telefon: 461-1000 Fax: 461-1099



1. ábra



2. ábra