(19) Országkód

HU

MAGYAR KÖZTÁRSASÁG

MAGYAR SZABADALMI HIVATAL

SZABADALMI LEÍRÁS

(11) Lajstromszám:

216 231 B

(21) A bejelentés ügyszáma: P 96 01870
(22) A bejelentés napja: 1995. 01. 13.
(30) Elsőbbségi adatok:
08/181,859 1994. 01. 13. US
08/272,203 1994. 07. 08. US
(86) Nemzetközi bejelentési szám: PCT/US 95/00531
(87) Nemzetközi közzétételi szám: WO 95/19672

(51) Int. Cl.[6]

H 04 L 9/08
H 04 L 9/32

(40) A közzététel napja: 1997. 05. 28.
(45) A megadás meghirdetésének a dátuma a Szabadalmi Közlönyben: 1999. 05. 28.

(72) Feltaláló:
Sudia, Frank W., New York, New York (US)

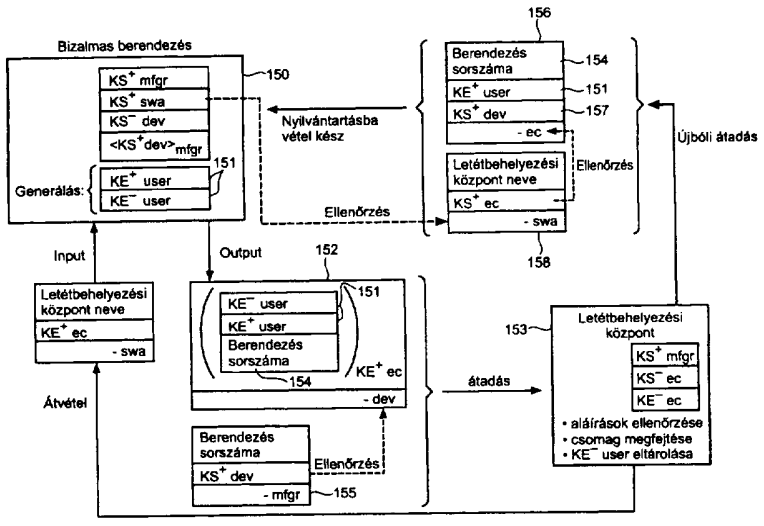
(73) Szabadalmas:
CERTCO, LLC, New York, New York (US)

(74) Képviselő:
Gödölle, Kékes, Mészáros & Szabó Szabadalmi és Védjegy Iroda, Budapest

(54) **Eljárás titkosított kommunikáció létrehozására**

KIVONAT

A találmány egyrészt eljárás ellenőrizhetően bizalmas kommunikáció létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál (153) nagyszámú felhasználó által alkalmazandó nagyszámú, titkos, aszimmetrikus rejtjelkulcsot helyeznek letétbe. A találmány szerint a letétbe helyezési központnál (153) a rejtjelkulcsokat ellenőrzik, a rejtjelkulcsokat ellenőrzéskor hitelesítik, és a hitelesítéstől függően az egyes felhasználóktól a nagyszámú rejtjelkulcs közül egy megfelelővel kommunikációt kezdeményeznek. A találmány másrészt eljárás ellenőrizhetően bizalmas kommunikációk létrehozására



15. ábra

A leírás terjedelme 70 oldal (ezen belül 28 lap ábra)

HU 216 231 B

nagyszámú felhasználó között szelektív kívülálló fél általi hozzáféréssel, illetve eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során külső behatás ellen védett logikával vezérelt elektronikus hardverberendezéseket alkalmaznak. A találmány továbbá eljárás ellenőrizhetően bizalmas, folyamirányított kommunikációk létrehozására nagyszámú felhasználó között, valamint eljárás bizalmas berendezés firmware-ének frissítésére.

A találmány eljárás titkosított kommunikáció létrehozására.

A bonyolult számítástechnika és az elosztott adatfeldolgozó rendszerek fejlődése és elterjedése a digitális információátvitel gyors növekedéséhez vezetett. Ezen információkat pénzügyi és banki területen, elektronikus postai, elektronikus adatcsere és egyéb adatfeldolgozó rendszerekben használják. Az ilyen információk nem biztonságos vagy nem védett kommunikációs csatornákon történő átvitelekor fennáll az a veszély, hogy az információkat lehallgatják vagy megváltoztatják. A titkosító kommunikációs rendszerek azáltal őrzik meg az adatátvitelek titkosságát, hogy megakadályozzák, hogy a nem biztonságos csatornán átvitt üzeneteket illetéktelen személyek lehallgassák. A titkosító kommunikációs rendszerek az átvitelek integritását is biztosítják azzal, hogy a nem biztonságos csatornán átvitt üzenetek információinak illetéktelen személyek általi megváltoztatását megakadályozzák. A titkosító kommunikációs rendszerek továbbá biztosíthatják az átvitel integritását és érvényességét azáltal, hogy felismerhető, hamisíthatatlan és dokumentumfüggő digitális aláírásokat alkalmaznak, amelyekkel megakadályozható, hogy egy küldő fél saját üzenetét letagadja.

A titkosítórendszerek kódolják vagy titkosítják a digitális adatátvitelt, beleértve a digitalizált hang- vagy képátviteleket is, hogy az csak a szándékolt vevő fél számára legyen érthető. A digitalizált hangot, betűket és/vagy számokat tartalmazó kódolatlan üzenetet numerikusan kódolják, majd összetett matematikai algoritmussal titkosítják, amely algoritmus a kódolt üzenetet egy rejtjelkulcsnak is nevezett szám- vagy számjegykészlet alapján átalakítja. A rejtjelkulcs az alkalmazott algoritmustól vagy titkosítórendszertől függően véletlenszerűen választott vagy speciális matematikai jellemzőkkel rendelkező adatbitsorozat. A számítógépeken használt bonyolult titkosítóalgoritmusok több száz vagy több ezer bit hosszúságú számokat tudnak átalakítani és kezelni, és ellenük bármilyen ismert illetéktelen megfejtési eljárás hatástalan. A titkosítóalgoritmusoknak két alapvető csoportja van: a szimmetrikus rejtjelkulcsos algoritmusok és az aszimmetrikus rejtjelkulcsos algoritmusok.

A szimmetrikus rejtjelkulcsos algoritmusok azonos rejtjelkulcsot alkalmaznak az üzenet küldője általi titkosításra és az üzenet vevője általi megfejtésre. A szimmetrikus rejtjelkulcsos algoritmusok a két fél kölcsönös bizalmára épülnek, akik egymással megosztják a rejtjelkulcsot, hogy nem bizalmas harmadik felekkel szemben védekezzenek. A legjobb ismert szimmetrikus rejtjelkulcsos algoritmus a Nemzeti Adattitkosító Szabvány (Nationai Data Encryption Standard, DES) algoritmusa, amelyet először a Nemzeti Szabvány és Technológiai Intézet ismertetett a Federal Register 1975. március 17-én megjelent 40. kötet 52. számában és az 1975. augusztus 1-jén megjelent 40. kötet 149. számában. A rejtjelkulccsal ellátott, küldő titkosítóberendezés (a DES rejtjelkulcs 56 bit hosszú) a DES algoritmust alkalmazza az üzenet titkosítására a kommunikáció adott szakaszára (szakaszrejtjelkulcs). A vevő titkosítóberendezés inverz DES algoritmust alkalmaz a titkosított üzenet megfejtésére, ha el van látva ugyanazzal a rejtjelkulccsal, amelyet a titkosításra használtak. A szimmetrikus rejtjelkulcsos titkosítórendszerek alkalmasságát azonban általában megkérdőjelezik, mert a küldőnek és a vevőnek a kívánt kommunikáció előtt a rejtjelkulcsot olyan biztonságos csatornán kell kicserélnie, amelyhez nincs harmadik illetéktelen félnek hozzáférése. Ez a folyamat, amelyben először biztonságosan kicserélik a rejtjelkulcsokat, és csak azután titkosítják a kommunikációt, gyakran lassú és fáradságos, és ezért nem alkalmazható olyan helyzetekben, amelyekben spontán vagy önkéntes kommunikációra, illetve egymás számára ismeretlen felek közötti kommunikációra van szükség. Ezenkívül, ha a rejtjelkulcsot illetéktelen harmadik fél lehallgatja, lehetővé válik számára, hogy a titkosított beszélgetést mindkét oldalon lehallgassa.

A titkosítóalgoritmusok második csoportjánál, az aszimmetrikus rejtjelkulcsos algoritmusoknál, különböző rejtjelkulcsot alkalmaznak a titkosításra és a megfejtésre. Az aszimmetrikus rejtjelkulcsos algoritmust alkalmazó titkosítórendszerekben a felhasználó a titkosító rejtjelkulcsot nyilvánosságra hozza, a megfejtési rejtjelkulcsot pedig titokban tartja, amely egyéni megfejtési rejtjelkulcsot nem lehet levezetni a nyilvános titkosító rejtjelkulcsból. Ezáltal bárki, aki ismeri egy meghatározott felhasználó nyilvános rejtjelkulcsát, képes üzenetet titkosítani a felhasználónak, de csak a nyilvános rejtjelkulcsnak megfelelő egyéni rejtjelkulcsot birtokló felhasználó tudja az üzenetet megfejteni. A nyilvános/egyéni rejtjelkulcsokat tartalmazó rendszert először Diffie és Hellman ismertette „A titkosítás új irányvonalai" című cikkében az IEEE Transactions on Information Theory 1976. novemberi számában és az US 4 200 770 számú szabadalmi leírásban.

Az aszimmetrikus rejtjelkulcsos algoritmusok egyik korai típusa azáltal tesz lehetővé biztonságos kommunikációt egy nem biztonságos csatornán, hogy a kommunikáló felek interaktív módon rejtjelkulcsot állítanak elő a kommunikáció adott szakaszára. A két, egymással kapcsolatban álló felhasználó az aszimmetrikus rejtjelkulcsos algoritmussal egyidejűleg és függetlenül biz-

tonságos, lehallgató által nem levezethető rejtjelkulcsot generál, amellyel szimmetrikusan kódolják a felhasználók közötti kommunikáció adott szakaszát. A biztonságos rejtjelkulcs generálásának interaktív eljárását Diffie és Hellman ismertette a fent említett 1976. évi cikkben. Ebben az ismert, interaktív Diffie–Hellman-rendszer néven ismert eljárásban, amelyet a 2. ábra ábrázol, az A és a B felhasználók véletlenszerűen egy-egy 21, 22 titkos számot választanak, majd egy-egy 23, 24 közbenső számot számítanak két nyilvánosan ismert szám és a felhasználók által választott 21, 22 titkos számok segítségével. A felhasználók ezután elküldik egymásnak a 23, 24 közbenső számokat, és kiszámítják a titkos (szimmetrikus) 25 rejtjelkulcsot saját 21, 22 titkos számaik és a másik felhasználótól megkapott 23, 24 közbenső számok felhasználásával. Az interaktív módon generált 25 rejtjelkulcsot ezután mindkét felhasználó szimmetrikusan, DES vagy más szimmetrikus rejtjelkulcsos algoritmus rejtjelkulcsaként használja az egyébként nem biztonságos csatornán folyó kommunikáció adott szakaszának titkosítására és megfejtésére. Ez az interaktív folyamat csak néhány másodperc valós időt igényel, és a digitális kommunikációk, beleértve a digitalizált hang vagy kép átvitelét is, adott kommunikációs szakaszban a szakasz megkezdésénél az interaktív rejtjelkulcs-kicserélő folyamatot elindító gomb megnyomásával titkosíthatók. Mivel az interaktív Diffie–Hellman rejtjelkulcs-generáló rendszerben választott számok nagyon nagyok, a számításokat nem lehet invertálni, így a titkos rejtjelkulcsot nem tudja lehallgató kiszámítani, ami által a kommunikáció titkos marad. Mivel a számításokat nem lehet invertálni, minden felhasználó tudja, hogy az ezzel az algoritmussal kapott üzeneteket nem változtatták meg, és azokat csak a másik felhasználó küldhette, ami által megmarad a kommunikáció integritása és érvényessége. Ez az interaktív rejtjelkulcs-kicserélő eljárás azonban a felek valós idejű interaktív kapcsolatát igényli a rejtjelkulcs létrehozására, és nem használható önkéntes kommunikáció vagy egymás számára ismeretlen felek esetén. Az interaktív Diffie–Hellman rejtjelkulcs-generáló rendszer különösen nem alkalmazható tároló-továbbító elektronikus postai üzenetküldésnél vagy elektronikus adattároló rendszerben történő, hosszú idejű dokumentumtárolásnál, mert a vevő nincs online kapcsolatban a szakaszrejtjelkulcs kialakítására.

Ha a kommunikáló felek nincsenek egymással online kapcsolatban, a Diffie–Hellman-rendszer egy módosított, nem interaktív, hitelesített Diffie–Hellman-rendszer néven ismert formája alkalmazható. A hitelesített Diffie–Hellman rejtjelkulcs-generáló rendszer kiindulási, hitelesítési lépése a 3. ábrán látható. Az a felhasználó, aki a vevő fél lesz, véletlenszerűen választ egy titkos 31 számot (az egyéni rejtjelkulcsát), majd egy közbenső 33 számot számít két nyilvánosan ismert 32 számmal és az általa választott titkos 31 számmal. A felhasználó azután a 34 nyilvános rejtjelkulcsot képző, közbenső 33 számot és két nyilvános 32 számot azonosításra elküldi egy hitelesítő hatóságnak, amely kibocsát a hitelesítő hatóság digitális 36 aláírásával ellátott nyilvános rejtjelkulcs 35 igazolást, amely a felhasználó azonosságát a felhasználó Diffie–Hellman nyilvános rejtjelkulcs információjához köti. A felhasználó által nyilvánosságra hozott 34 nyilvános rejtjelkulcs ugyanaz marad, amíg a felhasználó el nem határozza új rejtjelkulcs bevezetését, és másik egyéni rejtjelkulcsot nem választ. A hitelesített Diffie–Hellman-eljárással történő üzenetküldés a 4. ábrán látható. A vevő felhasználóhoz menő üzenet átviteléhez a küldő felhasználó először megkapja a vevő felhasználó 35 igazolását, és ellenőrzi a hitelesítő hatóság 36 aláírását. A küldő ezután kiszámítja a kommunikáció azon szakaszára vonatkozó 42 szakaszrejtjelkulcsot a vevő közbenső 33 számával (ami a vevő igazolásából származik) és a küldő saját titkos 41 számával (az egyéni rejtjelkulcsával), amelyet véletlenszerűen választ. A küldő ezután a 42 szakaszrejtjelkulccsal 43 üzenetet titkosít, és saját közbenső 40 számát titkosítatlanul az üzenet elejére helyezi. Az üzenet vételével a vevő kiszámítja a 42 szakaszrejtjelkulcsot a küldő titkosítatlan közbenső 40 számával és saját titkos 31 számával (vagy egyéni rejtjelkulcsával), majd a 42 szakaszrejtjelkulccsal megfejti az üzenetet. Ugyanúgy, mint az interaktív Diffie–Hellman-rendszernél, a hitelesített Diffie–Hellman-rendszerben generált 42 szakaszrejtjelkulcs használatával is mindkét fél hagyományos szimmetrikus, például DES algoritmussal titkosítja, illetve fejti meg az egyébként nem biztonságos csatornán keresztül folyó adott kommunikációs szakaszt. A hitelesített Diffie–Hellman-rendszernél azonban szükséges, hogy egy bizalmas személy vagy hitelesítő hatóság aláírja a vevő felhasználó nyilvános rejtjelkulcsának 35 igazolását, hogy a küldő felhasználó megbízhasson a benne levő információk pontosságában. Ráadásul a küldő által véletlenszerűen választott 41 egyéni rejtjelkulcsnak, amellyel mind a 42 szakaszrejtjelkulcsot, mind a kommunikáció 40 közbenső számát számítja, nem szabad megegyeznie a küldő saját nyilvános rejtjelkulcs-igazolásához kapcsolódó egyéni rejtjelkulccsal. Azért, hogy mások ne tudják meg a küldő állandó egyéni rejtjelkulcsszámait (amelyek megfelelnek a hitelesített nyilvános rejtjelkulcsszámoknak), el kell különítenie azokat a csak meghatározott üzenetekhez generált egyéb ideiglenes egyéni rejtjelkulcsoktól vagy közbenső számoktól.

Az US 4 405 829 szabadalmi leírásban egy másik aszimmetrikus, a feltalálókról (Rivest, Shamir és Adleman) RSA-nak nevezett algoritmust ismertetnek, amely két nagy prímszám szorzataként előállt szám tényezőkre való felbontását tartalmazza. Az interaktív Diffie–Hellman-rendszerhez hasonlóan az RSA algoritmus is viszonylag egyszerűen számítható, de gyakorlatilag nem lehet invertálni. Mivel a nyilvános rejtjelkulcsból az egyéni rejtjelkulcsot nem lehet levezetni, a kommunikáció titkossága nem sérül. Ha az RSA algoritmussal egy üzenetet nyilvános rejtjelkulccsal titkosítanak, akkor azt csak az egyéni rejtjelkulccsal lehet megfejteni, és fordítva. A hitelesített Diffie–Hellman-rendszerhez hasonlóan az RSA algoritmus is igényel bizalmas személyt, hogy hitelesítse és nyilvánosságra hozza a felhasználók nyilvános rejtjelkulcsait. A két Diffie–Hell-

man-rendszerrel ellentétben azonban az RSA algoritmus nem állít elő a felek által szimmetrikusan alkalmazandó szakaszrejtjelkulcsot. Ehelyett egy meghatározott felhasználó nyilvános titkosító rejtjelkulcsa közvetlenül titkosítja a felhasználóhoz menő üzeneteket, amelyeket a felhasználó egyéni megfejtési rejtjelkulcsa fejt meg. Így az RSA algoritmus tisztán aszimmetrikus rejtjelkulcsos algoritmus.

Mivel azonban az RSA algoritmus összetett, és az üzenet nagyon nagy számokkal történő hatványra emelését tartalmazza, a titkosítás és a megfejtés még közepes hosszúságú üzeneteknél is sok időt vesz igénybe. Ezért sokkal egyszerűbb, gyorsabb és hatékonyabb az RSA algoritmust egy szimmetrikus algoritmusban alkalmazott DES rejtjelkulcs átvitelére használni. Ez az ismert eljárás RSA rejtjelkulcsátvitel néven ismert, és az 5. és 6. ábrán látható. Amint az az 5. ábrán látható, egy felhasználó véletlen DES 51 rejtjelkulcsot generál, és azzal 52 üzenetet titkosít. A felhasználó ezután titkosítja a DES 51 rejtjelkulcsot egy szándékolt vevő felhasználó nyilvános RSA 53 rejtjelkulcsával, és a DES-sel titkosított 54 üzenetet az RSA-val titkosított DES 55 rejtjelkulccsal együtt elküldi a vevő felhasználónak. Miután a vevő megkapja az üzenetet, a vevő megfejti az 51 DES rejtjelkulcsot az egyéni RSA megfejtési 56 rejtjelkulcsával, majd a DES 51 rejtjelkulccsal megfejti az 52 üzenetet. Mivel a DES algoritmus számítása sokkal kevesebb időt és költséget igényel, mint az RSA algoritmus, az aktuális üzenetet a szimmetrikus DES rejtjelkulccsal titkosítják és fejtik meg, míg a szimmetrikus DES rejtjelkulcs titkosítására és megfejtésére az aszimmetrikus RSA rejtjelkulcsokat használják.

Az RSA nyilvános/egyéni rejtjelkulcsos titkosítórendszer mind az üzenettől, mind az aláírótól függő digitális „aláírást" is szolgáltat, amely annak igazolására használható, hogy a kapott üzenetet valójában a küldő küldte, és hogy az üzenetet változatlan formában kapták meg. Az RSA digitális aláírás az RSA azon járulékos tulajdonságán alapszik, hogy azonkívül, hogy a felhasználó egyéni rejtjelkulcsa csak a felhasználó nyilvános rejtjelkulcsával titkosított kommunikációkat tudja megfejteni, a felhasználó egyéni rejtjelkulcsával csak olyan üzeneteket lehet titkosítani, amelyeket csak a felhasználó nyilvános rejtjelkulcsával lehet megfejteni. Mivel az egyéni rejtjelkulcs kizárólag a felhasználó tulajdona, az egyéni rejtjelkulccsal történő titkosítás a származás igazolását teszi lehetővé, amelyet bárki ellenőrizhet, aki hozzáfér a felhasználó nyilvános rejtjelkulcsához. A gyakorlatban a küldő először egyéni rejtjelkulcsával az üzenet szövegét olyan aláírt üzenetté kódolja, amely bárki által megfejthető, de csak a küldőtől jöhet. Amennyiben szükséges, a küldő adott esetben a küldendő aláírt üzenetet a vevő nyilvános rejtjelkulcsával titkosíthatja. A titkosított szöveg vételekor, amennyiben szükséges, a vevő megfejti azt egyéni megfejtési rejtjelkulcsával, és az aláírt üzenetet dekódolja a küldő nyilvános titkosító rejtjelkulcsával. Mivel csak a küldő ismeri egyedi, egyéni rejtjelkulcsát, a konkrét „aláírt" üzenetet csak a küldő küldhette; az aláírás így ellenőrzi a küldő személyét. Mivel pedig a vevő csak a küldő nyilvános rejtjelkulcsával rendelkezik, a küldő nem reklamálhat, hogy a vevő vagy harmadik illetéktelen fél megváltoztatta vagy meghamisította az üzenetét; az aláírás ezáltal megakadályozza, hogy a küldő az üzenetét letagadja. Ezen túlmenően, mivel csak a küldő egyéni rejtjelkulcsa alakítja át az eredeti üzenetet, és csak a küldő ismeri egyedi egyéni rejtjelkulcsát, sem a vevő, sem illetéktelen harmadik személy nem tudja megváltoztatni az üzenetet; az aláírás így igazolja az üzenet integritását.

Az RSA algoritmus egy másik típusú digitális aláírást is szolgáltat, amely darabolófüggvénnyel minden dokumentumra nézve egyedi, rövid üzenetkivonatot hoz létre. A 7. és 8. ábra az RSA aláírás darabolófüggvénnyel történő létrehozását és ellenőrzését mutatja. A darabolófüggvény egy másik összetett matematikai algoritmus, amely „egyirányú", azaz a darabolófüggvény eredményéből nem lehet a dokumentumot rekonstruálni, és „ütközésmentes", vagyis nem lehet másik olyan dokumentumot létrehozni, amelyből a függvény ugyanazt a kivonatot darabolja. Amint az a 7. ábrán látható, a küldő a 72 üzenetet a 74 üzenetkivonat létrehozására először egy 73 darabolóalgoritmuson viszi keresztül, majd a 74 üzenetkivonatot titkosítja RSA egyéni 75 rejtjelkulcsával, ami által a 72 üzenethez csatolt, tömör 76 digitális aláírást alakít ki. Miután a vevő a 8. ábrán látható módon megkapja a 72 üzenetet és az üzenetkivonatot, a küldő RSA nyilvános 77 rejtjelkulcsával megfejti a küldő RSA-val titkosított üzenet kivonatát (a 76 digitális aláírást). A vevő ugyanazt a 73 darabolóalgoritmust használja a kapott üzenetből 74 üzenetkivonat előállítására. A vevő által végrehajtott két transzformációból kiadódó két üzenetkivonatnak azonosnak kell lennie; ez igazolja, hogy a küldő írta alá az üzenetet.

A küldő ellenőrzésére egy másik, DSA-nak (Digital Signature Algorithm) nevezett algoritmus is használható. A DSA algoritmust az US 07 738 431 szabadalmi bejelentésben ismertették. A DSA algoritmusnak az RSA algoritmushoz annyiban hasonló tulajdonságai vannak, hogy a küldő az üzenetet egy darabolóalgoritmuson vezeti keresztül üzenetkivonat létrehozására, és azután az üzenetkivonatot saját egyéni rejtjelkulcsával titkosítja vagy aláírja, a vevő pedig a küldő nyilvános rejtjelkulcsával ellenőrzi a titkosított kivonatot. Az RSA aláírási algoritmustól eltérően azonban, amely az eredeti üzenetkivonatot adja vissza, miután a vevő megfejti az aláírási blokkot, a DSA ellenőrzési algoritmus csak az aláírás hitelességének pozitív megerősítését eredményezi, és így egy szándékolt vevő nyilvános rejtjelkulcsával titkosított kommunikációk később nem állíthatók vissza a vevő megfelelő egyéni rejtjelkulcsával történő megfejtéssel. Ezért a DSA algoritmus viszonylag jól alkalmazható digitális aláírásokra, de nem alkalmazható rejtjelkulcs átvitelére vagy közvetlen üzenettitkosításra.

Hogy a nyilvános/egyéni rejtjelkulcsrendszer hatékonyan működjön, a felhasználóknak meg kell bízniuk egy központi rejtjelkulcs-hitelesítő hatóságot, amely a nyilvános titkosító rejtjelkulcsok listájának nyilvánosságra hozataláért és frissítéséért felel. A felhasználónak,

vagyis a küldőnek és a vevőknek meg kell bízniuk a rejtjelkulcs-hitelesítő hatóságban, hogy az a felhasználónak a helyes, nyilvános rejtjelkulcsokat szolgáltatja, és így nem szándékolt vevőkhöz nem történik üzenetátvitel. Ebből a célból, amint azt az előzőekben kifejtettük és a továbbiakban kifejtjük, a hitelesítő hatóság a felhasználók név- és nyilvános titkosítórejtjelkulcs-információit szolgáltatja, és a szolgáltatott információkhoz azok hibátlanságának hitelesítésére hozzácsatolja saját digitális aláírását. Amikor azonban egynél több személy vagy személyek hierarchiája vesz részt a hitelesítési folyamatban, számos különböző módszer vagy „bizalmassági modell" létezik annak meghatározására, hogy a felhasználó hogyan dolgozza fel az igazolásokat. A három fő modell a tiszta hierarchikus modell (1), a több hierarchia közötti kereszthitelesítést alkalmazó modell (2), és a „helyi bizalmassági" modell (3). Ezeket a modelleket részletesen ismertetik az X9.30 számú, „Irreverzibilis algoritmusokkal történő, nyilvános rejtjelkulcsos titkosítás a pénzügyi szolgáltatóipar számára" című Amerikai Nemzeti Szabvány „Igazolás kezelése a DSA-hoz" című 3. fejezetében (American Bankers Assn., Washington, D. C., 1992). Bár még nincs általános egyetértés abban, hogy a fent említett három bizalmassági modell közül melyik a legjobb, a leírásunkban feltételezzük, hogy megfelelő, általánosan elfogadott hitelesítési bizalmassági modellről van szó, ha az egynél több személy által kibocsátott igazolásokat tartalmaz.

A fent leírt nyilvános/egyéni rejtjelkulcsrendszer azon felhasználók titkossági érdekeire koncentrál, akik titkosan akarnak üzeneteket küldeni és venni. Ezenkívül azonban figyelembe kell venni a kormányok törvényes ellenőrzési és nemzetbiztonsági érdekeit is. Meg kell tartani a kormány azon képességét, hogy törvényes ellenőrzési és nemzetbiztonsági célokból lehallgasson másülönben titkos elektronikus üzeneteket, hogy gyanúsított bűnözők, terroristák és külföldi kémek ne tudjanak a törvény tudta nélkül összeesküvést szőni. Jóllehet a telefonbeszélgetések lehallgatással figyelemmel kísérhetők, a titkosítóalgoritmusok a titkosított adatot még a nagy teljesítményű kódfejtő számítógépek számára is megfejthetetlenné teszik. A fejlett algoritmusokkal titkosított digitális és digitalizált átvitelek volumenének és arányának növekedése ezért lehetetlenné teszi és kiszorítja ezen kommunikációk törvényes kormányi elektronikus felügyeletét, különösen, ha titkosítóberendezéseket széles körben alkalmaznak telefonokban, számítógépekben, telefaxokban és más adatkezelő berendezésekben.

Egyik lehetséges módja annak, hogy lehetővé tegyük a kormány vagy felhatalmazott nyomozók számára gyanúsított bűnözők üzeneteinek lehallgatását az, hogy a titkosított kommunikációk minden felhasználójától megköveteljük, hogy egyéni megfejtési rejtjelkulcsát helyezze letétbe egy titkos hatóságnál vagy a kormánynál, vagyis megengedjük a titkos hatóságnak vagy a kormánynak, hogy a felhasználók egyéni megfejtési rejtjelkulcsainak bizalmas gondnoka legyen. Amikor a felügyelet megköveteli, a kormánynak hozzáférése lesz, vagy képes lesz a hozzáférést nyerni az egyéni rejtjelkulcsokhoz, hogy minden titkosított kommunikációt figyelhessen. Ez a módszer azonban nem alkalmazható, mert nem tartalmaz elég garanciát a kormány egyéni rejtjelkulcsokkal való visszaélése ellen, valamint annak lehetősége ellen, hogy az egyéni megfejtési rejtjelkulcsok kiszivárogjanak illetéktelen harmadik felekhez a kormánytól vagy a titkos hatóságtól történő lopással, illetve a kormány vagy a titkos hatóság személyzetének megvesztegetése folytán.

A felhasználói titkossági érdekeket és a törvényes ellenőrzés biztonsági érdekeit egyéni megfejtési rejtjelkulcs-letétbehelyezésével kielégítő további eljárást ismertetnek a CRYPTO 92 keretében 1993. márciusában Silvio Micali által indítványozott és a Massachusettsi Technológiai Intézet Számítógép Tudományok Laboratóriuma által 1993. október 13-án közreadott „Előnyös nyilvános, rejtjelkulcsos titkosítórendszerek" című cikkben, valamint az US 5 276 737 szabadalmi leírásban. Ebben a 9–11. ábrákon látható eljárásban nyilvános rejtjelkulcsát titkosítási célokra hitelesíteni kívánó felhasználónak a következőképpen kell egyéni rejtjelkulcsát letétbe helyeznie. Amint a 9. ábrán látható, a felhasználó egyéni 91 rejtjelkulcsát több 92 „darabra" bontja, amelyek 90 ellenőrzés keretében egyenként ellenőrizhetők, hogy vajon érvényes részeit képzik-e a teljes egyéni 91 rejtjelkulcsnak. Az egyéni 91 rejtjelkulcs csak a 92 darabok mindegyikének ismeretében vagy meghatározott számú 92 darab ismeretében rekonstruálható. A felhasználó ezután a 93 műveleti lépésben a darabokat különböző letétbe helyezési 94 ügynökökhöz vagy ügynökségekhez küldi, amelyek a 10. ábrán látható módon, 95 műveleti lépésben speciális algoritmussal az egyéni 91 rejtjelkulcs részeként ellenőrzik a darabokat, és az ellenőrzés eredményét 96 műveleti lépésben átadják egy fő letétbe helyezési központnak. A 11. ábrán látható módon, miután a fő letétbe helyezési központ megkapta a 96, 97 műveleti lépések ellenőrzési eredményét, hogy az egyéni 91 rejtjelkulcs részei helyesek, 98 igazolást bocsát ki a felhasználó nyilvános 99 rejtjelkulcsa számára, amely 98 igazolás lehetővé teszi, hogy a 99 rejtjelkulcsot titkos rendszerben használják azzal a biztosítékkal, hogy amennyiben szükséges, és kizárólag jogosultsági vagy bírósági rendnek megfelelően, a törvényes ellenőrzési ügynökségek képesek legyenek megszerezni az egyéni rejtjelkulcs titkos darabjait a felhasználó választott letétbe helyezési ügynökeitől, és azokat összeállítva lehallgathassák a felhasználó kommunikációit. Ezzel a rendszerrel a felhasználók számára biztosítjuk titkosított üzeneteik titkosságát, és a kormány számára biztosítjuk a titkosított üzenetekhez szükség esetén történő hozzáférés lehetőségét. Mivel normális esetben egyetlen személynek sincs hozzáférése a teljes egyéni rejtjelkulcshoz, és mivel a felhasználó olyan személyeket választ, akikben megbízik, a törvénytelen vagy korrupt cselekmények esélyei nagymértékben csökkennek. Továbbá a személyek nagyobb köre választható letétbe helyezési ügynöknek, ezért a minden letétbe helyezési ügynök egyidejű megvesztegetésének, és ezáltal a bizalmi viszonyok megszűnésének esélye méginkább lecsökken.

A fő letétbe helyezési központ, amely megbízott hatóságként hitelesíti a felhasználó nyilvános rejtjelkulcsának valódiságát, időközönként nyilvánosan hozzáférhető igazolást bocsát ki a nyilvános titkosító rejtjelkulcs és a tulajdonosát azonosító információ közötti kapcsolat tanúsítására vagy hitelesítésére. Az érvényesség igazolása biztosítja a küldőt, hogy a megnevezett nyilvános rejtjelkulccsal rendelkező felhasználóhoz menő üzenetet ténylegesen csak a szándékolt vevő kapja meg és olvassa el. Az igazolás általában nemzetközileg elismert elektronikus formában van, például az X.509 CCITT ajánlásban meghatározott és a Nemzetközi Szabványügyi Szervezet (ISO) által nemzetközi szabványként kibocsátott formában. A 12. ábrán egy nyilvános titkosító rejtjelkulcs-letétbehelyezési igazolása formátumának egy példája látható. Az igazolás többek között tartalmazza az igazolást létrehozó szervezet vagy rejtjelkulcskezelő központ (a kibocsátó) 121 nevét, a tulajdonos nyilvános 122 rejtjelkulcsát, a tulajdonost azonosító 126 információt, az igazolás 123 sorszámát, valamint az érvényesség kezdetének és végének 124 dátumait. A kibocsátó 125 digitális aláírása „lepecsételi" az igazolást, és megakadályozza annak megváltoztatását.

Az Amerikai Egyesült Államok kormánya azonban kormány (és valószínűleg ipari) szabványként más eljárást ajánlott az egyéni megfejtési rejtjelkulcsok letétbe helyezésének és a kommunikációk megfigyelésének lehetővé tételére. Az Amerikai Egyesült Államok kormánya kifejlesztett egy mikroáramkört, úgynevezett „Clipper chipet", amely beépíthető kormány tulajdonában lévő, valamint a kereskedelemben gyártott telefonokba és számítógépes berendezésekbe. A Clipper chip alacsony költségű chip, amely nagy mennyiségű titkosításra és rejtjelkulcskezelésre alkalmazható. A Capstone chip a Clipper chip tökéletesített változata, amely rendelkezik digitális aláírási és üzenetkivonatolási képességekkel. Más titkosítórendszerekhez hasonlóan, a Clipper chip szimmetrikus titkosítóalgoritmust alkalmaz, mégpedig a Skipjack-nek nevezett titkos algoritmust, amely a DES-hez hasonló módon rejtjelezi a telefonos és digitális számítógépes adatkommunikációkat, de 80 bites rejtjelkulcsot alkalmaz. Minden Clipper chip rendelkezik egyedi sorszámmal, egy minden Clipper chipre közös családi rejtjelkulccsal, és egy saját szimmetrikus, egyéni berendezés-rejtjelkulccsal, amely nélkül a felhatalmazott kormányügynökségek nem tudják a chipet tartalmazó berendezéssel kódolt üzenet dekódolni. A chipet tartalmazó berendezés gyártásakor az egyedi, egyéni berendezés-rejtjelkulcsot két összetevőre bontják (úgynevezett „rejtjelkulcsszeletekre"), és azokat egymástól elkülönítve elhelyezik a kormányon belül létrehozott két rejtjelkulcs-letétbehelyezési adatbázisban vagy ügynökségnél. A törvényes ellenőrzési ügynökök hozzáférést nyerhetnek ezekhez az egyéni berendezés-rejtjelkulcsokhoz oly módon, hogy felhatalmazást vagy más törvényi meghatalmazást kapnak a kommunikációk lehallgatására vagy megfigyelésére, és a felhatalmazást a két letétbe helyezési ügynökségnél bemutatják.

Amikor Clipper chipes berendezések felhasználói kommunikálni akarnak egymással, először megegyeznek a kommunikáció titkosítására szolgáló szimmetrikus szakaszrejtjelkulcsban. A szimmetrikus szakaszrejtjelkulcs létrehozására bármilyen eljárás alkalmazható, például az interaktív Diffie–Hellman rejtjelkulcslétrehozási folyamat, és a DES szakaszrejtjelkulcs felhasználók közötti átvitelére is bármilyen eljárás alkalmazható, például az RSA átvitel. A kommunikációk kezdetén a felhasználók a másik felhasználóhoz egy Törvényes Ellenőrzési Hozzáférési Mezőt (LEAF, Law Enforcement Access Field) küldenek, amely elegendő információt tartalmaz ahhoz, hogy lehetővé tegye a törvényes ellenőrzési ügynököknek a kommunikáció lehallgatását vagy megfigyelését. A Clipper LEAF valószínű formája 13. ábrán látható (megjegyezzük, hogy a LEAF-formátum pontos részletei, annak létrehozása és ellenőrzése az Amerikai Egyesült Államok kormánya által jelenleg „titkos" osztályozást kapott, ezért ennek leírása és a 13. ábra bizonyos mértékig spekulatív). A LEAF kialakítására a szakaszrejtjelkulcsot először az egyéni berendezés-rejtjelkulccsal titkosítják, majd a berendezés-rejtjelkulccsal titkosított szakaszrejtjelkulcsot, a küldőberendezés sorszámát és az eredeti titkosítatlan szakaszrejtjelkulcs ellenőrző összegét (ellenőrző értékét) együtt titkosítják a Clipper családi rejtjelkulccsal. Az üzenetet ezután a választott szakaszrejtjelkulccsal titkosítják. A szakaszrejtjelkulccsal titkosított üzenetet és a családi rejtjelkulccsal titkosított LEAF-et együtt átküldik a vevőhöz. A kommunikáció vétele után a vevő felhasználó először betölti a vett LEAF-et a Clipper chipbe annak ellenőrzésére, hogy a LEAF érvényes-e, és hogy a LEAF-ben lévő titkosított szakaszrejtjelkulcs megegyezik-e az előzőleg megkapott szakaszrejtjelkulccsal. Ha a LEAF érvényes, a Clipper chip megfejti az üzenetet az előzőleg megkapott, választott szakaszrejtjelkulccsal.

A kommunikációt törvényesen lehallgató vagy megfigyelő törvényes ellenőrzési ügynök azonban nem ismeri a szakaszrejtjelkulcsot, és ezért először meg kell fejtenie a LEAF-et. Az ügynök először lehallgatja a kívánt LEAF-et, megfejti azt a Clipper családi rejtjelkulccsal, és a chip LEAF-ből származó sorszámát, valamint a bírósági végzésen nyugvó felhatalmazást vagy más törvényes meghatalmazást a két kormányzati letétbe helyezési ügynöknek bemutatja, ami után megkapja a lehallgatott felhasználó egyéni berendezés-rejtjelkulcsának két rejtjelkulcsszeletét. Az ügynök a letétbe helyezett berendezés-rejtjelkulcs két összetevőjét összeilleszti, és a kiadódó berendezés-rejtjelkulccsal a LEAF-ből megfejti a berendezés-rejtjelkulccsal titkosított szakaszrejtjelkulcsot. A szakaszrejtjelkulccsal ezután megfejthetők a kommunikáció aktuális üzenetei. Az a követelmény, hogy mind a küldőnek, mind a vevőnek LEAF-et kell létrehoznia, és ellenőriznie kell a másik LEAF-jét, a törvényes ellenőrzési ügynököknek reális esélyt biztosít a LEAF lehallgatására, mivel mindkét LEAF várhatóan ugyanazon a kommunikációs médiumon keresztül halad a két felhasználó között. A rendszer lehetővé teszi továbbá a törvényes ellenőrzés számára, hogy a felhasználó által generált LEAF megfejtésével szelektíven csak egy gyanúsított felhasználót fi-

gyeljen meg, függetlenül attól, hogy melyik felhasználó kezdeményezte a kommunikációt.

Sajnálatos módon sok technikai probléma merül fel a kormány Clipper chip ajánlásával kapcsolatban, amelyek leginkább abból a tényből fakadnak, hogy a letétbe helyezendő egyéni rejtjelkulcsokat a gyártás alatt a Clipper chipekbe permanensen beágyazzák. Mivel egy adott berendezés egyéni titkosító rejtjelkulcsa megváltoztathatatlanul van beégetve a chipbe, veszélyeztetettség esetén a chipet és valószínűleg az azt tartalmazó egész berendezést le kell selejtezni. Egy meghatározott berendezés felhasználója számára előnyös, ha veszélyeztetés gyanújának felmerülésekor, vagy szabályos időközönként a potenciális veszélyeztetés megelőzésére, bármikor képes a berendezést új rejtjelkulccsal ellátni, a rejtjelkulcsot újra letétbe helyezni és újra hitelesíteni. Azonkívül, hogy a felhasználó nem képes új rejtjelkulcsot bevezetni és azt újra letétbe helyezni, a Clipper berendezés felhasználójának továbbá nincs választási lehetősége a kormány által egyéni rejtjelkulcsának felügyeletére alkalmazott rejtjelkulcs-letétbehelyezési ügynökök számát vagy személyét illetően. Ehelyett az egyéni rejtjelkulcsszeletek két kormány által létrehozott letétbe helyezési adatbázisban vagy ügynökségnél kerülnek elhelyezésre. A felhasználók nem bízhatnak a Clipper chipet tartalmazó berendezésekben, mert fennáll annak a veszélye, hogy a kormány visszaél a berendezésen keresztül történő bármiféle átvitelhez vagy tranzakcióhoz való teljes hozzáférésével, illetve a hozzáférést megvesztegetik. A felhasználók azt is kívánhatják, hogy rejtjelkulcsaikat a kormány által biztosítottnál több bizalmasnál is letétbe helyezhessék, hogy egyéni rejtjelkulcsuk még nagyobb biztonságban legyen. Amennyiben a rejtjelkulcs-letétbehelyezésének koncepciója nagy jelentőséggel bír, a felhasználóknak képesnek kell lenniük a kívánt bizalmassági szint alapján saját bizalmasaik kiválasztására, akiknél letétbe helyezhetik egyéni rejtjelkulcsaikat.

Úgy hisszük továbbá, hogy a kormány Clipper rendszere csak szimmetrikus és valós idejű kommunikációt tesz lehetővé a felhasználók között, és nem támogatja közvetlenül a tároló-továbbító elektronikus postai üzenetküldést. A kommunikáció titkosítása előtt a küldőnek és a vevőnek először meg kell egyeznie a kommunikáció titkosítására szolgáló szimmetrikus szakaszrejtjelkulcsban. Ezt a rejtjelkulcs-kicserélést általában az interaktív Diffie–Hellman-rendszerben végzik, amely szerintünk az egyetlen Clipper chip által támogatott rejtjelkulcs-kicserélési eljárás. Ily módon a felhasználók, hacsak nem állítanak fel saját rejtjelkulcskezelő rendszert, egyidejű interaktív kommunikációra, például valós idejű hang- vagy telefax-kommunikációra vannak korlátozva. Ahhoz, hogy egy felhasználó tároló-továbbító elektronikus postai üzenetküldést tudjon használni, még akkor is képesnek kell lennie a szándékolt vevő nyilvános rejtjelkulcsához hozzáférni, például hitelesített Diffie–Hellman- vagy hitelesített RSA rejtjelkulcs-továbbítási rendszerrel, ha a szándékolt vevő nem elérhető interaktív, valós idejű kommunikációra. Mivel úgy hisszük, hogy a kormány Clipper rendszere ezt nem teszi lehetővé, az azzal történő tároló-továbbító üzenetküldés nehézkes. A kormány tervezett szabványos rendszere így a felhasználók kommunikációs lehetőségeit a valós idejű interakcióra korlátozza.

A kormány rendszerében továbbá a felhasználók alkalmazói nem férnek hozzá alkalmazottaik titkosított adataihoz vagy átviteleihez. Az olyan alkalmazóknak, akiknek a nevében alkalmazottak bizalmas vagy magánjellegű adatot fejlesztenek, közölnek vagy küldenek, biztosítani kell a jogot alkalmazottaik adatához vagy átviteleihez való hozzáféréshez. Sokféle olyan helyzet állhat elő, amelyben a titkosított információ közvetlenül csak a titkosítórendszerekkel dolgozó alkalmazottak számára hozzáférhető, és nem hozzáférhető a menedzsment vagy az igazgatótanács számára, akik felelősek alkalmazottaikért, és akik a vállalati adatforrások tulajdonosai. Adat- vagy kommunikációtitkosítással az alkalmazottak új programokat, termékeket és technológiákat fejleszthetnek vagy tulajdoníthatnak el, illetve jogellenes cselekményeket és tranzakciókat végezhetnek az alkalmazóik tudta nélkül. A beosztottak mozgása vagy újraszervezése, valamint a tárolóeszközök változásai nagy mennyiségű olyan információ elvesztéséhez vezethetnek, amelyek elég fontosak voltak ahhoz, hogy azokat titkosítsák. Ezt ismertette Donn B. Parker „A titkosítás és az üzleti információs anarchia megelőzése" című előadásában (meghívott előadó az Első Évenkénti AC Számítógép és Kommunikáció Biztonsági Konferencián, 1993. november 3–5., Reston, VA). Az adat létrehozóján vagy az átvitel küldőjén kívül a Clipper chip csak a kormány számára teszi lehetővé az átvitelekhez való hozzáférést. Bár az alkalmazók kérhetnek bíróság által kibocsátott felhatalmazást alkalmazottaik kommunikációjának figyelésére, az alkalmazók belső hivatalnokaikat diszkrétebb módon is kívánhatják megfigyelni, minthogy gyanú felmerülése esetén szövetségi nyomozást kezdeményezzenek.

Ezen túlmenően egy olyan titkos algoritmus kijelölése, amely be van ágyazva a chipbe, és ezáltal csak hardverben és csak a kormány által felhatalmazott chipgyártónál hozzáférhető, a kormányt a kommunikáció és a számítógéphardver gyorsan változó és nagy versenyben lévő piacára taszítja. Egy kormányügynökség vagy kormány által felhatalmazott gyártó az egyéni gyártókkal ellentétben képtelen vagy kelletlen lehet az adott szervezetekre speciálisan szabott, továbbfejlesztett berendezések és termékek tervezésére és forgalmazására. Ha a kormány csak meghatározott kereskedőket hatalmaz fel a titkos algoritmust tartalmazó chip gyártására, a versengés csökken, és a technológia nem kerül bele más termékekbe. Ezen túlmenően, mivel a Skipjack algoritmus részleteit nem hozták nyilvánosságra, felmerült a gyanúja annak, hogy az algoritmus tervezői tévedése miatt, vagy a kormány által szándékosan bevezetett csapda miatt nem biztonságos. A titkosítórendszerek tervezésének egyik fontos szempontja, hogy a titkosított üzenetek titkossága és biztonsága a megfelelő rejtjelkulcsértékektől, és ne a rendszer részleteinek titkosságától függjön.

Ezért kívánatos olyan kereskedelmi rejtjelkulcs-letétbehelyezési rendszer kialakítása, amely nyilvános-

ságra hozott algoritmusokat alkalmaz, működése elnyeri a felhasználók bizalmát, és megoldja a nemzetbiztonsági és törvényes ellenőrzési kívánalmak által támasztott problémákat.

Kívánatos még olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely a felhasználó akarata szerint vagy szabályos időközönként megváltoztatható egyéni rejtjelkulcsokat használ.

Kívánatos továbbá olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely lehetővé teszi a felhasználó számára, hogy egyéni rejtjelkulcsa vagy annak különálló részei felügyeletére megválaszthassa a rejtjelkulcs-letétbehelyezési ügynököket.

Kívánatos még olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely biztosítékokat tartalmaz a kormány korlátlan hozzáférésével szemben, de lehetővé teszi a felhasználók alkalmazóinak hozzáférését, vagy azon országok hozzáférését, amelyeknek a külföldi felhasználók polgárai.

Az is kívánatos, hogy olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszert alakítsunk ki, amely alternatívát kínál az Amerikai Egyesült Államok Kormánya által ajánlott Clipper chip rendszerre.

A találmány ismertetése

A találmány egyik célja olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely nyilvánosságra hozott algoritmusokat alkalmaz, működésével elnyeri a felhasználók bizalmát, és megoldja a nemzetbiztonsági és törvényes ellenőrzési kívánalmak által támasztott problémákat.

A találmány másik célja olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely a felhasználó akarata szerint vagy szabályos időközönként megváltoztatható egyéni rejtjelkulcsokat használ.

A találmány további célja olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely lehetővé teszi a felhasználó számára, hogy egyéni rejtjelkulcsa vagy annak különálló részei felügyeletére megválaszthassa a rejtjelkulcs-letétbehelyezési ügynököket.

A találmány célja még olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszer kialakítása, amely biztosítékokat tartalmaz a kormány korlátlan hozzáférésével szemben, de lehetővé teszi a felhasználók alkalmazóinak hozzáférését, vagy azon országok hozzáférését, amelyeknek a külföldi felhasználók polgárai.

A találmány célja az is, hogy olyan kereskedelmi rejtjelkulcs-letétbehelyező rendszert alakítsunk ki, amely alternatívát kínál az Amerikai Egyesült Államok Kormánya által ajánlott Clipper chip rendszerre.

A találmány tehát egyrészt eljárás ellenőrizhetően bizalmas kommunikáció létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál nagyszámú felhasználó által alkalmazandó nagyszámú, titkos, aszimmetrikus rejtjelkulcsot letétbe helyezünk. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és a hitelesítéstől függően az egyes felhasználóktól a nagyszámú rejtjelkulcs közül egy megfelelővel kommunikációt kezdeményezünk.

A találmány másrészt eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál az egyes felhasználókhoz rendelt titkos, aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, valamint egy kezdeményező felhasználó és egy vevő felhasználó rejtjelkulcsainak hitelesítésétől függően a kezdeményező felhasználótól a vevő felhasználóhoz biztonságos kommunikációt kezdeményezünk.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között szelektív kívülálló fél általi hozzáféréssel, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt titkos, aszimmetrikus rejtjelkulcsokat helyezünk letétbe, ahol az egyes felhasználók legalább egy rejtjelkulcshoz és legalább egy, a felhasználó kommunikációihoz hozzáféréssel rendelkező, első választható kívülálló félhez vannak rendelve. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy küldő felhasználótól egy vevőhöz az első kívülálló fél számára a kommunikációhoz való hozzáférést megengedő módon kezdeményezzük a bizalmas kommunikációt.

A találmány továbbá eljárás biztonságos kommunikációra legalább egy kommunikáló féllel és a kommunikációban részt nem vevő fél által visszafejthető üzenetrejtjelkulccsal rendelkező rendszerben, amely eljárásban minden felhasználót ellátunk számítógépes hardverberendezéssel. A találmány szerint a berendezés felhasználójától különböző berendezéstulajdonos által meghatározott ellenőrzési információ szerint egy központban a hardverberendezéseket nyilvántartásba vesszük, a hardverberendezéseket hitelesítjük, amely hitelesítések egy központot, egy felhasználót és egy hardverberendezést egymáshoz rendelő igazolást generálnak, valamint egy üzenetrejtjelkulcs alkalmazásával egy kezdeményező felhasználótól egy vevőhöz a tulajdonosnak a kommunikációhoz való hozzáférést megengedő módon biztonságos kommunikációt kezdeményezünk.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között harmadik fél általi hozzáféréssel, amelynek során nagyszámú letétbe helyezési központ közül legalább egynél az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat letétbe helyezünk. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy ellenőrzött rejtjelkulccsal bizalmas kommunikációt kezdeményezünk egy küldő felhasználótól egy vevő felhasználóhoz, amely kommunikáció tartalmaz a kezdeményező felhasználó rejtjelkulcsának és a vevő felhasználó rejtjelkulcsának visszanyerésére szolgáló információt.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során külső behatás ellen védett

logikával vezérelt elektronikus hardverberendezéseket gyártunk. A találmány szerint egy kezdeményező berendezéstől egy vevőhöz biztonságos kommunikációt kezdeményezünk, amely kommunikáció tartalmaz a kezdeményező berendezés által aláírt, egy kívülálló félnek a kommunikációhoz való hozzáférését megengedő hozzáférési információt.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikáció létrehozására nagyszámú felhasználó között. A találmány szerint egy első felhasználó elektronikus hardverberendezésében biztonságos kommunikációt hozunk létre, amely biztonságos kommunikáció tartalmaz egy kívülálló fél által a biztonságos kommunikációhoz való hozzáférést megengedő hozzáférési információt, a biztonságos kommunikációt az első felhasználó elektronikus hardverberendezése egy aláíróchipjének chipspecifikus egyéni aláírási rejtjelkulcsával aláírjuk, amely chipspecifikus egyéni aláírási rejtjelkulcsot az első felhasználó aláíróchipjéhez rendelt, illetéktelen hozzáférés ellen védett memóriába beágyazzuk, mielőtt az elektronikus hardverberendezést az első felhasználóhoz juttatjuk, a biztonságos kommunikációhoz igazolást csatolunk, amely igazolás tartalmaz az első felhasználó aláíróchipje egyéni aláírási rejtjelkulcsának megfelelő nyilvános aláírási rejtjelkulcsot, amely nyilvános aláírási rejtjelkulcs egy bizalmas hatóság egyéni aláírási rejtjelkulcsával alá van írva, valamint a biztonságos kommunikációt egy második felhasználóhoz továbbítjuk.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy letétbe helyezési központnál az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevő felhasználóhoz kommunikációt kezdeményezünk a kezdeményező felhasználó bizalmas, a küldő és vevő felhasználók rejtjelkulcsainak hitelesítését jóváhagyó berendezésétől függően.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és a kommunikációban alkalmazott rejtjelkulcs hitelesítésétől függően egy kezdeményező felhasználótól egy vevő felhasználóhoz kívülálló fél kommunikációhoz való hozzáférését megengedő hozzáférési információt tartalmazó kommunikációt kezdeményezünk.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat és felhasználókhoz rendelt bizalmas berendezéseket ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevőhöz kommunikációt kezdeményezünk a kommunikációban alkalmazott rejtjelkulcs hitelesítése és a kezdeményező felhasználóhoz rendelt bizalmas berendezés ismertetőjeleinek jóváhagyása után.

A találmány továbbá eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során bizalmas letétbe helyezési központoknál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központok egyik része egy első csoporthoz, másik része egy második csoporthoz tartozik, a letétbe helyezési központoknál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy első felhasználó és egy második felhasználó között attól függően kommunikálunk, hogy a küldő és vevő felhasználók letétbe helyezési központjai mely csoporthoz tartoznak.

A találmány továbbá eljárás ellenőrizhetően bizalmas, folyamirányított kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevő felhasználóhoz titkosított, folyamirányított kommunikációt hozunk létre a kezdeményező felhasználó titkosító rejtjelkulcsával, amely kommunikáció tartalmaz egy kívülálló fél számára a folyam megfejtését lehetővé tevő hozzáférési információt tartalmazó kezdeti csomagot, valamint egymás után következő csomagok folyamát, ahol az egymás után következő csomagok tartalmaznak a folyamhoz tartozó, soron következő csomagot azonosító információt, és ahol az egymás után következő csomagok közül legalább egy nem tartalmazza a hozzáférési információt.

A találmány továbbá eljárás ellenőrizhetően bizalmas, folyamirányított kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe. A találmány szerint a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy vevő felhasználónál egy első titkosított, folyamirányított kommunikációt veszünk egy kezdeményező felhasználótól, amely kommunikáció a kezdeményező felhasználó titkosító rejtjelkulcsával van titkosítva, és amely első kommunikáció tartalmaz egy kívülálló fél számára a folyam megfejtését lehetővé tevő hozzáférési információt tartalmazó kezdeti csomagot, valamint egymás után következő csomagok folyamát, ahol az egymás után következő csomagok tartalmaznak a folyamhoz tartozó, soron következő csomagot azonosító információt, és ahol az első folyam egymás után következő csomagjai közül legalább egy nem tartalmazza a hozzáférési információt.

A találmány továbbá eljárás bizalmas berendezés firmware-ének frissítésére. A találmány szerint a bizalmas berendezésbe a firmware kibocsátójához rendelt rejtjelkulcsot ágyazunk be, a firmware-t kommunikáció keretében a bizalmas berendezéshez továbbítjuk, amely kommunikáció a firmware kibocsátója által a beágyazott rejtjelkulccsal jóváhagyható módon van módosítva, és a kommunikáció beágyazott rejtjelkulccsal történő jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

A találmány továbbá eljárás bizalmas berendezés firmware-ének frissítésére, amelynek során a bizalmas berendezésnél firmware-t tartalmazó kommunikációt veszünk. A találmány szerint a kommunikáció kibocsátóját egy, a bizalmas berendezésbe beágyazott rejtjelkulccsal jóváhagyjuk, amely rejtjelkulcs a kommunikáció kibocsátójához van rendelve, valamint a kommunikáció kibocsátójának jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

A találmány továbbá eljárás bizalmas berendezés firmware-ének frissítésére, amelynek során a bizalmas berendezésnél firmware-t tartalmazó kommunikációt veszünk. A találmány szerint a kommunikáció kibocsátóját egy, a bizalmas berendezésbe beágyazott rejtjelkulccsal jóváhagyjuk, amely rejtjelkulcs egy bizalmas személyhez van rendelve, ahol is a jóváhagyás során ellenőrizzük, hogy a kommunikáció tartalmaz-e a bizalmas személy egyéni aláírási rejtjelkulcsával aláírt frissítési igazolást, ahol a frissítési igazolás tartalmazza a firmware kibocsátójának nyilvános aláírási rejtjelkulcsát, továbbá a firmware kibocsátójának nyilvános aláírás-ellenőrzési rejtjelkulcsával ellenőrizzük, hogy a kommunikáció alá lett-e írva a firmware kibocsátójának egyéni aláírási rejtjelkulcsával, valamint a firmware kibocsátójának jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

A találmány továbbá eljárás titkosított kommunikációhoz kommunikáló feleket és a kommunikációban részt nem vevő fél által visszanyerhető üzenetrejtjelkulcsot tartalmazó rendszerben, amelynek során a felhasználókat ellátjuk számítógépes hardverberendezésekkel, amely berendezések legalább egy hozzájuk rendelt rejtjelkulccsal rendelkeznek. A találmány szerint nagyszámú központ közül legalább egy kiválasztott központnál a hardverberendezéseket nyilvántartásba vesszük, a hardverberendezéseket hitelesítjük, amely hitelesítés a berendezés számára igazolást állít elő, és egy üzenetrejtjelkulccsal egy kezdeményező felhasználótól egy vevőhöz biztonságos, az üzenetrejtjelkulcs visszanyerésére a központ rejtjelkulcsával titkosított hozzáférési részt tartalmazó kommunikációt kezdeményezünk.

A találmány továbbá eljárás bizalmas berendezés meghatalmazására egy első felhasználó és egy második fél közötti elektronikus tranzakció levezetésére, amelynek során biztosítjuk, hogy a bizalmas berendezés előre meghatározott, a felhasználó által nem megváltoztatható szabályok szerint kapcsolódik be az elektronikus tranzakcióba. A találmány szerint a bizalmas berendezéstől harmadik félhez elektronikusan továbbítunk az elektronikus tranzakcióba való bekapcsolódásra vonatkozó, a bizalmas berendezés azonosítását tartalmazó meghatalmazási kérelmet, a harmadik féllel eldöntjük, hogy a bizalmas berendezés meghatalmazható-e a tranzakcióba történő bekapcsolódásra legalább részben annak vizsgálatával, hogy a bizalmas berendezés kizárólag a szabályok szerint fog-e működni, a harmadik féltől a bizalmas berendezéshez elektronikusan a tranzakcióba történő bekapcsolódásra vonatkozó meghatalmazást továbbítunk, amely meghatalmazás a harmadik fél általi kibocsátásra vonatkozó igazolást tartalmaz, az igazolást a bizalmas berendezéstől a második félhez elektronikusan továbbítjuk annak biztosítékaként, hogy a bizalmas berendezés meghatalmazással rendelkezik az elektronikus tranzakcióba való bekapcsolódásra, és hogy ezt kizárólag a szabályok szerint teszi meg, valamint a bizalmas berendezéstől a második félhez a szabályok szerint elektronikusan tranzakciós adatot továbbítunk.

A rajzok rövid leírása

A találmány előnyös kiviteli alakjait a következőkben rajzok alapján részletesen ismertetjük, amelyekben az azonos részek azonos hivatkozási számmal vannak jelölve, és ahol az

1A-1G ábrák a találmány ábráiban használt jelek és rövidítések listája, a

2. ábra az ismert, interaktív Diffie–Hellman rejtjelkulcs-levezetési eljárás lépéseinek blokkdiagramja, a

3. ábra az ismert, hitelesített Diffie–Hellman-eljárás hitelesítési része lépéseinek blokkdiagramja, a

4. ábra az ismert, hitelesített Diffie–Hellman-eljárás üzenetküldési része lépéseinek blokkdiagramja, az

5. ábra az ismert RSA rejtjelkulcs átviteli eljárással történő titkosítás lépéseinek blokkdiagramja, a

6. ábra az ismert RSA rejtjelkulcs átviteli eljárással történő megfejtés lépéseinek blokkdiagramja, a

7. ábra az ismert RSA eljárással történő aláírás létrehozás lépéseinek blokkdiagramja, a

8. ábra az ismert RSA eljárással történő aláíráshitelesítés lépéseinek blokkdiagramja, a

9–11. ábrák együtt az ismert Micali rejtjelkulcs-letétbehelyezési folyamat lépéseinek blokkdiagramját mutatják, a

12. ábra egy ismert, nyilvános, titkosító rejtjelkulcs-letétbehelyezési igazolásának példája, a

13. ábra a Clipper berendezés Törvényes Ellenőrzési Hozzáférési Mezője (LEAF) vélt formátumának példája, a

14. ábra a találmány szerinti berendezés gyártói által kibocsátott berendezés igazolásformátumának példája, a

15. ábra rejtjelkulcsnak egyetlen letétbe helyezési ügynöknél történő, ellenőrizhető letétbe helyezési eljárása lépéseinek blokkdiagramja, a

16. ábra kizárólag a bizalmas berendezésen alapuló, ellenőrizhető rejtjelkulcs-letétbehelyezési eljárás lépéseinek blokkdiagramja, a

17. ábra titkosított üzenet üzenet-ellenőrző fejrésszel (MCH, Message Control Header) együtt történő küldési eljárás lépéseinek blokkdiagramja, a
18. ábra az MCH példája az RSA rejtjelkulcs-átviteli formátumban, a
19. ábra MCH-val ellátott titkosított üzenet vételi eljárási lépéseinek blokkdiagramja, a
20. ábra egy MCH dekóderdoboz példája és működésének blokkdiagramja, a
21. ábra önhitelesítő, bizalmas időbélyegző berendezés példája, a
22. ábra a találmány szerinti berendezés gyártója által kibocsátott berendezés tulajdonlásiigazolás-formátumának példája, a
23. ábra a találmány szerinti berendezés tulajdonosa által végrehajtott, ismételt rejtjelkulcs-letétbehelyezési eljárás lépéseinek blokkdiagramja, a
24. ábra a találmány szerinti bizalmas berendezés bizalmas harmadik félnél történő nyilvántartásba vételi eljárása lépéseinek blokkdiagramja.
25. ábra az MCH kialakítása arra az esetre, amikor több vevőnek küldjük ugyanazt az üzenetet, a
26. ábra a tulajdonos nyilvános utasítási rejtjelkulcsára vonatkozó tulajdonosi igazolás több berendezéshez történő kibocsátásának blokkdiagramja, a
27. ábra új rejtjelkulcs bevezetésére vonatkozó, ismételt letétbe helyezésre vonatkozó, vagy tulajdon átruházásra vonatkozó utasítások kiadásának blokkdiagramja, a
28. ábra tulajdonátruházási utasítás kiadásának blokkdiagramja, a
29. ábra nemzetközi titkosított üzenet továbbításakor a küldőberendezés működésének blokkdiagramja, és a
30. ábra nemzetközi titkosított üzenet továbbításakor a vevőberendezés működésének blokkdiagramja.

A találmány részletes leírása

A nyilvános rejtjelkulcsos titkosítórendszerek, beleértve a digitális aláírások alkalmazását is, potenciálisan sarokkövei lehetnek a nemzeti, sőt globális, papír nélküli, elektronikus dokumentációs rendszereknek. Ezen rendszerek alkalmazása a költségcsökkentést illetően hatalmas gazdasági jelentőségű. Az ilyen rendszerek fejlődésének és széles körű elfogadásának kritikus eleme az azok alapjául szolgáló titkosítórendszerek, valamint a kormányok, bankok, vállalatok és más felhasználók – az egyéni felhasználókat is beleértve – digitális aláírásainak megbízhatósága. A megbízhatóságnak nem az egyes felhasználók saját belső rendszerei vagy más felhasználók belső rendszerei iránti bizalmából kell fakadnia, hanem inkább a felhasználók nyilvános rejtjelkulcsos titkosítórendszer iránti, valamint az azáltal szolgáltatott hitelesítési mechanizmus iránti bizalmából. A találmány kereskedelmi titkosítórendszere kielégíti ezeket a megfontolásokat önhitelesítő, és ezért bizalmas titkosítóberendezések alkalmazásával.

A találmány egy előnyös kiviteli alakjában a titkosítást, megfejtést és a digitális úton történő aláírást végző, külső behatás ellen védett chipbe vagy a chipet tartalmazó, külső behatás ellen védett bizalmas berendezésbe van ágyazva egy nem megváltoztatható, a chipre nézve egyedi, nyilvános/egyéni aláírásirejtjelkulcs-pár, valamint egy „gyártói igazolás". A beágyazott gyártói igazolás lehetővé teszi a chipet tartalmazó berendezés számára, hogy saját egyéni berendezése aláírási rejtjelkulcsával digitálisan „aláírjon" dokumentumokat és kommunikációkat („adatstruktúrákat"), ezzel bizonyítva, hogy azok egyedileg a berendezésből származnak, valamint hogy a dokumentumokhoz és kommunikációkhoz a gyártói igazolást hozzácsatolva bizonyítsa, hogy az adatstruktúrák bizalmasak, mivel a származási berendezés ismert és bizalmas típusú, és bizalmas gyártó gyártotta. A gyártói igazolás gyakorlatilag a következőt állítja: „A berendezés, amelynek egyéni rejtjelkulcsa egybevág az itt hitelesített nyilvános rejtjelkulccsal, XXX típusú. Aláírás, gyártó." Mivel az egyéni aláírási rejtjelkulcs külső behatás ellen védett módon be van ágyazva, és mivel a gyártó bizalmas, a berendezés által kibocsátott és az egyéni rejtjelkulccsal aláírt dokumentumok és kommunikációk szintén bizalmasok lesznek.

A találmány egyik előnyös kiviteli alakjának alkalmazása nyolc fő fázist tartalmaz: a berendezésben lévő chip létrehozása vagy legyártása, a berendezés titkosító rejtjelkulcsának letétbe helyezési ügynököknél való nyilvántartásba vétele, a felhasználói üzenetek normál titkosítása és megfejtése, kommunikációk meghatalmazott törvényes ellenőrzési ügynökök általi dekódolása, a berendezés új rejtjelkulccsal való ellátása és frissítése a tulajdonos vagy az alkalmazó által, a törvényes ellenőrzési lehallgatások felülvizsgálása, folyamirányított adat titkosítása, és nemzetbiztonsági garanciák.

A bizalmas berendezés előállítása

A találmány szerinti bizalmas berendezések előállítása a következő általános elemekkel történik:

(1) Beágyazott mikroprocesszor (vagy mikrovezérlő), mikroszámítógép, amely minden külső hozzáférést közvetít és különböző számítási és programozási műveleteket hajt végre;

(2) Opcionális titkosító társprocesszor, amely a szabványos matematikai titkosítási és megfejtési műveleteket az általános célú mikroprocesszornál sokkal nagyobb sebességgel képes elvégezni, és amely előnyösen tartalmaz hardver zajforrást, például dióda zajforrást a titkosító rejtjelkulcs generálásához a szükséges, hitelesíthetően véletlen számok előállításához;

(3) Input/output interface vagy alrendszer a mikroprocesszorhoz menő és attól jövő adat áramlásának kezeléséhez, amely tartalmazhat állapotkijelzőt vagy monitort; valamint

(4) Memória-alrendszer, amely potenciálisan többféle típusú tárolási technológiát tartalmaz, amelyek mindegyike különböző teljesítmény- és hozzáférési jellemzőkkel rendelkezik, úgymint csak olvasható memóriát (ROM), amely állandó, nem megváltoztatható programokat és adatokat tartalmazhat, villamosan törölhető és programozható csak olvasható memóriát (EEPROM)

vagy FLASH memóriát, amely félig állandó programokat és adatokat tartalmazhat, amelyek megváltoztathatók, de nem vesznek el, ha a berendezés tápfeszültsége kiesik vagy azt lekapcsolják, valamint véletlen hozzáférésű memóriát (RAM) amely időszakos számításokhoz és időszakos adattároláshoz használható, de amelynek tartalma elvész, ha a tápfeszültséget kikapcsolják.

A teljes berendezés úgy van kialakítva és legyártva, hogy minden eleme, beleértve különösen az állandó és félig állandó memóriaterületeket, le vannak védve az olyan külső behatások ellen, amelyekkel tartalmuk megtudható vagy működésük megváltoztatható. A berendezés elemeinek külső behatás elleni levédésének egyik módja speciális borítások alkalmazása, amelyeket nehéz eltávolítani a borítás alatt lévő információ megsemmisítése nélkül. Ezen túlmenően a memóriát más lehetőségekkel is ki lehet törölni, ha bármelyik memóriaterület fizikai burkának megváltoztatását kísérlik meg, vagy ha külső behatási kísérletet jelző gyanús események történnek, például a berendezés abnormálisan alacsony hőmérsékletre hűtése a berendezés belső védelmi mechanizmusai deaktiválásának megkísérlésére. Ezen védelmi jellemzők állandó tápforrást igényelnek, hogy a berendezés villamos műveleteket végezhessen a fontos adat törlésére külső behatás gyanúja esetén. A találmány nem határoz meg konkrét előnyös eljárást a berendezés külső behatás elleni védelmének kialakítására, hanem inkább létező vagy jövőbeli technológiákon alapszik, amelyek általánosan úgy tekinthetők, hogy elfogadható védelmi szintet szolgáltatnak az illetéktelen feltárás vagy a berendezésekben lévő adat megváltoztatása ellen. Az ilyen jellemzőkkel rendelkező berendezést általában külső behatás ellen védett modulnak nevezik (TSRM, tamper-resistant secure module), amelyre példa az előzőekben leírt, a Mykotronx Inc. vállalat révén a kereskedelemben hozzáférhető Clipperl/Capstone berendezés.

A chip gyártója bármelyik lehet a számítógépmikroprocesszor-chipet előállító több nagy gyártó közül. A gyártónak előnyösen ismertnek kell lennie a titkosítóiparban, és megbízhatónak kell lennie a chip minőségét és biztonságát, valamint gyártási folyamatának integritását illetően.

A találmány egyik kiviteli alakjában történő alkalmazásra gyártott chip a következő képességekkel rendelkezik. A chip először tartalmaz egy beágyazott berendezés nyilvános/egyéni rejtjelkulcspárt a berendezés által kibocsátott berendezés-aláírásokhoz, amely egyéni aláírási rejtjelkulcs nem olvasható, és külső behatás ellen védett. A titkosító aláírási rejtjelkulcsok bármilyen elfogadható titkosító, például RSA típusúak lehetnek. Mivel azonban az RSA titkosítási és aláírási képességekkel is rendelkezik, és mivel kívánatos az aláírási és titkosítási folyamatok különválasztása, az aláírási rejtjelkulcs előnyösen DSA típusú. A chip szintén tartalmaz beágyazott, külső behatás ellen védett gyártói igazolást a berendezés aláírási rejtjelkulcsához, amelynek formátumára a 14. ábra mutat példát. A chipet tartalmazó berendezés ezt az igazolást az aláírásaihoz fűzheti annak bizonyítására, hogy az aláírások ismert és bizalmas típusú berendezéstől származnak, amelynek jellemzőit az alábbiakban ismertetjük.

A találmány egy másik kiviteli alakjához gyártott chip tartalmazza a gyártó nyilvános aláírás ellenőrzési rejtjelkulcsát is, amely a chipbe külső behatás ellen védett módon van beágyazva. A felhasználó a gyártó nyilvános aláírási rejtjelkulcsával ellenőrizni tudja a másoktól vett utasításokat oly módon, hogy ellenőrzi, hogy azok rendelkeznek-e hozzájuk csatolt érvényes, a gyártó egyéni aláírási rejtjelkulcsával létrehozott digitális aláírással, és így el tudja dönteni, hogy az utasítások a gyártótól vagy annak bizalmasától származnak-e. A chip tartalmazhat beágyazott és külső behatások ellen védett nyilvános utasítási rejtjelkulcsot is a másoktól kapott utasítások felhasználó általi ellenőrzéséhez. A nyilvános utasítási rejtjelkulcs lehet a gyártó által kiválasztott valamely más bizalmas személy, például a Bankers Trust Co. nyilvános rejtjelkulcsa, vagy egy bizalmas nemzeti vagy globális szintű hatóság nyilvános rejtjelkulcsa, és az egyfajta „egyszerűsítésként" a gyártó által opcionálisan be lehet ágyazva a chipbe, hogy elkerüljük a bizalmas személy gyártó általi igazolásának felesleges ellenőrzését. A gyártó különböző minősített rejtjelkulcs-letétbehelyező házak számos utasítási rejtjelkulcsát beágyazhatja, amely rejtjelkulcs-letétbehelyező házakat a gyártó választja ki, ha azokat alkalmasnak és bizalomra méltónak találja.

Ezen túlmenően a találmány egyik kiviteli alakjában alkalmazott chip képes nyilvános/egyéni rejtjelkulcspár generálására az egyes felhasználók adatainak és kommunikációinak titkosításához és megfejtéséhez. A titkosító rejtjelkulcsok típusa bármilyen elfogadható aszimmetrikus titkosító lehet, például RSA. A titkosító rejtjelkulcsok azonban előnyösen Diffie–Hellman-típusúak, vagyis a felhasználó titkos száma az egyéni rejtjelkulcs és a felhasználó nyilvánosságra hozott közbenső száma a nyilvános rejtjelkulcs, amelyeket a hitelesített Diffie–Hellman-rendszerben együtt alkalmaznak a kommunikációk titkosítására és megfejtésére szolgáló szakaszrejtjelkulcs generálására. Az így létrehozott egyéni rejtjelkulcsot a chipben nem kiolvashatóan és külső behatás ellen védetten tároljuk. Ezen túlmenően a chip rendelkezik azzal a képességgel is, hogy a berendezéshez a már egyszer létrehozott nyilvános/egyéni titkosítórejtjelkulcs-pár helyett új nyilvános/egyéni titkosítórejtjelkulcs-párt hozzunk létre. Amint azt a továbbiakban kifejtjük, egy másik kiviteli alakban az interaktív Diffie–Hellman rejtjelkulcs-generálás is alkalmazható, amivel biztosítjuk, hogy minden küldő és vevő új véletlen számokkal járul hozzá az üzenet-szakaszrejtjelkulcsok generálásához.

A találmány előnyös kiviteli alakja szerinti bizalmas berendezés csak akkor képes titkosított kommunikációkat megfejteni, ha két feltétel teljesül. Az első feltétel az, hogy a berendezésbe a titkosított átvitel vétele előtt mind a küldő-, mind a vevőberendezésekre vonatkozó, érvényes, fő letétbe helyezési központtól származó igazolásokat kell betáplálni. Az igazolás akkor érvényes, ha egy fő letétbe helyezési központ aláírásával igazolja, hogy a berendezés egyéni megfejtési rejtjelkulcsa egy vagy

több minősített letétbe helyezési ügynöknél letétbe van helyezve, mégpedig előnyösen kettő vagy több Micali-típusú ügynöknél, akik ellenőrizhető rejtjelkulcs-darabolási protokollt alkalmaznak. A fő letétbe helyezési központ ezen igazolását a gyártó által kibocsátott, a megnevezett fő letétbe helyezési központot érvényes letétbe helyezési ügynöknek nyilvánító igazolásnak kell kísérnie, vagy az igazolást annak a harmadik félnek (bizalmas nemzeti vagy globális, egész rendszerre kiterjedő hatóságnak) kell aláírnia, aki a gyártó által a chipbe ágyazott nyilvános utasítási rejtjelkulcs birtokosaként van megnevezve. A megfejtés második feltétele az, hogy a megfejtendő üzenetet érvényes üzenet-ellenőrző fejrész (MCH) adatmezőnek kell megelőznie (amelynek formátumát a későbbiekben ismertetjük), hogy a törvényes ellenőrzési ügynöknek vagy az alkalmazó biztonsági alkalmazottjának elegendő adata legyen a vevő letétbe helyezett egyéni rejtjelkulcsának megszerzéséhez, és ezzel a kommunikáció megfigyeléséhez.

A találmány egy másik kiviteli alakjában a chip rendelkezik azzal a képességgel is, hogy a berendezés-aláírásokhoz használatos beágyazott rejtjelkulcspár mellett felhasználói aláírásokhoz használatos nyilvános/egyéni rejtjelkulcspárt generáljon. A berendezési aláírásirejtjelkulcs-párhoz hasonlóan a titkosító felhasználói aláírási rejtjelkulcsok bármilyen elfogadható titkosító típusúak, például RSA típusúak lehetnek, de azok előnyösen DSA típusúak, hogy itt is megelőzzük az üzenet titkosításra használt rejtjelkulcsok összekeverésének lehetőségét. A felhasználó aláírási egyéni rejtjelkulcsának nem kiolvashatónak és külső behatás ellen védettnek kell lennie. A felhasználó ezt az aláírási egyéni rejtjelkulcsot üzeneteinek aláírásával küldőellenőrzési és letagadásmegelőzési célokra használja. A találmány egy másik kiviteli alakjában a chip rendelkezik azzal a képességgel is, hogy a berendezés-aláírási rejtjelkulcsot a chip által a felhasználó számára generált nyilvános aláírási rejtjelkulcs hitelesítésére való kérelem aláírására használja, amivel bizonyítja, hogy külső behatások ellen védett tulajdonságokkal rendelkező berendezés generálta a felhasználó aláírásirejtjelkulcs-párját, és őrzi az egyéni rejtjelkulcsot. A találmány további kiviteli alakjaiban a chip rendelkezhet hardver zajforrással, például dióda zajforrással, hogy a rejtjelkulcs-generáláskor véletlen számokat generáljon, valamint egyedi fizikai berendezés-sorszámmal, hogy lehetővé tegyük a berendezésnek vagy a berendezés működésének nyomon követését a könyvelésben, hálózatkezelésben és leltárrendszerekben. Ebben a kiviteli alakban a berendezés aláírása nemcsak a felhasználó berendezésének külső behatások ellen védett tulajdonságait igazolja, hanem azt is, hogy a berendezés által minden esetben újonnan generált rejtjelkulcsot vagy véletlen számot jó minőségű véletlenszám-generátor, előnyösen dióda zajforrás generálta.

A találmány szerinti chipet tartalmazó bizalmas berendezés előállításakor a chip memóriáját legalább három általános területre osztjuk, mégpedig a gyártás alatt a chipbe beágyazott adatot és firmware-t tartalmazó állandó és nem megváltoztatható memóriaterületre, egy félig állandó és megváltoztatható memóriaterületre, amely a felhasználó egyéni titkosító és aláírási rejtjelkulcsait tartalmazza, amelyeket a chip a felhasználó részére generál és a felhasználó számára bizalmasan kezel, és amely adattal és rejtjelkulcsokkal a chip digitális aláírásokat készíthet, vagy a felhasználó nevében üzeneteket fejthet meg, de amelyek soha nem kerülnek nyilvánosságra a rendszeren kívül, valamint egy nem állandó, ideiglenes memóriaterületre, amely különböző adatfeldolgozási műveletek bemeneteinek, közbenső eredményeinek és végeredményeinek munkaterületét tartalmazza. A kialakítástól függően ez a három általános terület más-más típusú memóriatároló rendszerben helyezkedhet el, például az állandó adat ROM-ban, a bizalmasan kezelt felhasználói adat EEPROM-ban vagy FLASH memóriában, és az ideiglenes adat RAM-ban. Egy másik megközelítés lehet FLASH memória alkalmazása mind az állandó, mind pedig a nem állandó adat tárolására. További lehetőség lehet olyan mikroprocesszoros operációs rendszer használata, amely a mikroprocesszor memóriáját objektumok könyvtárának használatával kezeli. Ennél a megközelítésnél a memória egy részét a memóriában lévő egyéb adatok táblájának vagy könyvtárának szentelhetjük, amely minden objektum számára szabványos információt tartalmazhat, például:

- logikai név (például „a gyártó nyilvános rejtjelkulcsa"),
- típus (például rejtjelkulcs, igazolás, programkód-eljárás stb.),
- az adat kezdőcíme és hossza (bájtokban), – az utolsó változtatás dátuma (opcionális),
- a védettség szintje (állandó, felhasználói vagy ideiglenes),
- a nyilvánosság szintje (kívülről kiolvasható vagy kívülről nem kiolvasható).

Ily módon, amíg az egész memória egyformán védett külső behatások ellen, nem kell a védett és nem védett adat számára speciális területeket meghatározni, mivel a mikroprocesszor a kívánt védettségi szintet a könyvtár adott belépési pontjában lévő kód alapján az adatobjektum számára érvényesíteni tudja. Ez a rendszer majdnem ugyanolyan könnyen alkalmazható firmwareprogramkód-eljárásokhoz mint adathoz, és előnyösen alkalmazható akkor, amikor a bizalmas firmwareprogramkód-eljárásokat frissítjük vagy kicseréljük anélkül, hogy szükséges lenne a berendezés vagy memória moduljainak fizikai cseréje.

A találmány szerinti berendezés előnyös kiviteli alakjának védett memóriaterületei a következő típusú információkat tartalmazhatják, beleértve mind az adatot mind pedig a firmware-programkódot.

A. A gyártó által permanensen beágyazva

1. Kívülről hozzáférhető

a) az egész rendszerre kiterjedő hatóság nyilvános rejtjelkulcsa (opcionális)

b) a gyártó nyilvános rejtjelkulcsa

c) a gyártó igazolása az egész rendszerre kiterjedő hatóságtól

d) a berendezés nyilvános rejtjelkulcsa

e) a berendezés igazolása a gyártótól
f) a berendezés egyedi sorszáma
g) a firmware verziószáma
h) a bizalmas bank nyilvános utasítási rejtjelkulcsai
2. Kívülről nem hozzáférhető
a) a berendezés egyéni aláírási rejtjelkulcsa
3. Firmware
a) operációs rendszer és fájlrendszer
b) alapvető titkosító könyvtárrutinok
c) a letétbe helyezési rendszer rutinjai
d) más bizalmas alkalmazások programkódjai
B. Felhasználói műveletekkel generált, és a felhasználó számára bizalmasan kezelt adatok
1. Kívülről hozzáférhető
a) a felhasználó nyilvános titkosító rejtjelkulcsa
b) a felhasználó nyilvános titkosító rejtjelkulcsának letétbe helyezési igazolása
c) a felhasználó nyilvános aláírási rejtjelkulcsa
d) a felhasználó nyilvános aláírási rejtjelkulcsának igazolása
2. Kívülről nem hozzáférhető
a) a felhasználó egyéni megfejtési rejtjelkulcsa
b) a felhasználó egyéni aláírási rejtjelkulcsa
C. Más nem felejtő, írható-olvasható tároló (opcionális)
a) a kommunikációs partner aláírási igazolásai
b) a kommunikációs partner letétbe helyezési igazolásai
c) a kommunikációs partner berendezés igazolásai (az MCH ellenőrzéséhez)
D. Munkatároló (lehet felejtő)
Nyilvános rejtjelkulcsok (minden típus), igazolások (minden típus), kivonatértékek, aláírásblokkok, más feldolgozott adatstruktúrák.

A rejtjelkulcs-letétbehelyezésének folyamata

A találmány szerinti chip előállítása után, és a chip titkosításra vagy megfejtésre való felhasználása előtt a felhasználó nyilvános titkosító rejtjelkulcsát nyilvántartásba kell venni egy fő letétbe helyezési központnál, vagy a chip gyártója által elfogadott letétbe helyezési ügynököknél. Ezt a műveletet vagy maga a felhasználó végzi, vagy kezdeményezheti a gyártó is, és a gyártás alatt a chipet egy letétbe helyezési ügynöknél nyilvántartásba véve megszabadíthatja a felhasználót attól a tehertől, hogy rejtjelkulcsait maga helyezze letétbe. A gyártó azonban meghagyhatja a felhasználónak azt a lehetőséget, hogy később önmaga új rejtjelkulcsot vezethessen be. Sok egyéni felhasználó számára megfelelő, ha a gyártó számára lehetővé tesszük, hogy új rejtjelkulcs bevezetésének lehetőségével vagy anélkül nyilvántartásba vegye a chipet. Ezen túlmenően a vásárlók nagy valószínűséggel megbíznak a gyártó által választott letétbe helyezési ügynökökben. Vállalatok vagy más alkalmazók beprogramozhatják saját chipjeiket és alkalmazottaik chipjeit, és azokat az általuk kiválasztott letétbe helyezési ügynöknél nyilvántartásba vetethetik. A vállalatok azonban általában nem engedhetik meg alkalmazottaiknak, hogy új rejtjelkulcsot vezessenek be, mert ez a fent leírtak szerint a vállalati információk és tulajdon feletti ellenőrzés csökkenését eredményezi.

Megfejtési rejtjelkulcs előállítására és nyilvántartásba vételére a felhasználó (vagy a műveletet végző személy) lehív egy a chipbe beágyazott firmware-programot, amely a chipet a Micali rejtjelkulcs-letétbehelyezési eljárás vagy az adott alkalmazott rejtjelkulcs-letétbehelyezési eljárás konkrét műveleteinek végrehajtására utasítja. Ezen lépések a 9–11., 15. és 16. ábrákon láthatók. Bármilyen eljárást is alkalmazunk az egyéni rejtjelkulcs egy vagy több letétbe helyezési ügynöknél történő letétbe helyezésére, a chip először véletlenszerűen generál vagy kiválaszt egy titkos számot, amely a felhasználó egyéni megfejtési rejtjelkulcsa lesz (ugyanígy generálja a chip a többi szükséges nyilvános számot, ha azok más megelőző véletlen generálással még nem lettek előállítva). A chip az egyéni rejtjelkulcsot nem kiolvashatóan és külső behatások ellen védetten tárolja. Amint az a 15. ábrán látható, az egyéni megfejtési rejtjelkulcsot egyetlen letétbe helyezési ügynöknél is letétbe lehet helyezni. A bizalmas 150 berendezés először nyilvános/egyéni titkosító 151 rejtjelkulcspárt állít elő a felhasználó számára, majd egy 153 letétbe helyezési központnak elküld egy titkosított és aláírt 152 üzenetet, amely tartalmazza a titkosító 151 rejtjelkulcspárt, a berendezés 154 sorszámát és a gyártó 155 igazolását az aláírás ellenőrzésére. A 153 letétbe helyezési központ ellenőrzi az aláírásokat, megfejti az üzenetcsomagot, és eltárolja a felhasználó egyéni megfejtési rejtjelkulcsát. A 153 letétbe helyezési központ a felhasználónak egy aláírt 156 igazolást is küld, amely tartalmazza a felhasználó berendezésének 154 sorszámát, a felhasználó nyilvános titkosító rejtjelkulcsát, a berendezés nyilvános aláírás-ellenőrzési 157 rejtjelkulcsát és a 153 letétbe helyezési központ 158 igazolását az aláírás ellenőrzésére. Amint a felhasználó 150 berendezése ellenőrzi a 153 letétbe helyezési központ aláírását, a nyilvántartásba vétel befejeződik.

Ha az egyéni rejtjelkulcsot egynél több letétbe helyezési ügynöknél kell letétbe helyezni, akkor a chip az egyéni rejtjelkulcsot meghatározott képlet szerint több darabra, úgynevezett szeletekre hasítja. Az előzőekben leírt és a 9. ábrán látható Micali letétbe helyezési eljárást és algoritmust alkalmazva a chip ezután a speciális Micali-algoritmussal meghatározott értékeket számít oly módon, hogy minden érték az egyéni rejtjelkulcs egy-egy 92 darabjának matematikai transzformációján alapszik. A chip ezután a felhasználó által megnevezett mindegyik bizalmas fél vagy letétbe helyezési 94 ügynök számára kialakít egy részcsomagot, amely tartalmazza a felhasználó berendezésének egyedi sorszámát, egy egyéni rejtjelkulcsszeletet és egy meghatározott értékekből álló készletet, amely az adott bizalmas fél számára lehetővé teszi annak ellenőrzését, hogy a kapott egyéni rejtjelkulcsszelet a teljes rejtjelkulcs érvényes része-e anélkül, hogy a bizalmas fél tudomására hozná a teljes rejtjelkulcsot. Amint azt a későbbiekben kifejtjük, ha a felhasználó nem a berendezés tulajdonosa, hanem például az alkalmazó-tulajdonos alkalmazottja, a bizalmas fél részcsomagja tartalmazni fogja a berendezés tulajdonosának egyedi azonosítószámát és a berendezés tulajdonosának igazolását is, és így az alkalmazó-tulaj-

donos megszerezheti az alkalmazott-felhasználó egyéni rejtjelkulcsát anélkül, hogy előzőleg meghatalmazást kellene kapnia. A chip ezután az egyedi, egyéni berendezés-aláírási rejtjelkulccsal aláírja a bizalmas felek részcsomagjait, és csatolja a gyártó küldő chipre vonatkozó igazolását, amivel tanúsítja, hogy az átvitt információ ismert és bizalmas típusú berendezésből származik. Végül a chip kiadja az aláírt bizalmas részcsomagokat, amelyeket a felhasználó bizalmas letétbe helyezési ügynökhöz kézbesít.

A fő letétbehelyező központ a Micali-eljárás használata nélkül, csupán a bizalmas berendezésre hagyatkozva is ellenőrizheti a különálló rejtjelkulcsszeleteket.

Ennél a 16. ábrán látható, rejtjelkulcsszeleteket ellenőrző eljárásnál a chip az egyéni titkosító rejtjelkulcs minden szeletéhez egy véletlen számot generál. A chip ezután minden a felhasználó által megnevezett bizalmas vagy 163 letétbe helyezési ügynök számára egy 161 részcsomagot alakít ki, amely tartalmazza a felhasználó berendezésének egyedi számát, egy rejtjelkulcsszeletet és egy véletlen számot. A chip aláírja a bizalmasok 161 részcsomagjait az egyedi, egyéni berendezés-aláírási rejtjelkulccsal, valamint csatolja a gyártó küldőchipre vonatkozó 162 igazolását, amivel tanúsítja, hogy az átvitt információ ismert és bizalmas típusú berendezésből származik. Ugyanúgy, ahogy a Micali-eljárásnál is, a chip kiadja az aláírt bizalmas 161 részcsomagokat, amelyeket a felhasználó bizalmas 163 letétbe helyezési ügynökökhöz kézbesít. Ezen túlmenően a chipnek létre kell hoznia egy (titkosított) 164 üzenetet a 165 fő letétbe helyezési központ számára, amely többek között tartalmazza a felhasználó nyilvános titkosító rejtjelkulcsát és a felhasználó által megnevezett letétbe helyezési ügynökök neveit a megfelelő letétbe helyezési ügynöknek a rejtjelkulcsszelettel együtt adott véletlen szám kíséretében.

Lehetséges azonban, hogy mivel a bizalmasok részcsomagjai tartalmazzák az egyéni rejtjelkulcs egy-egy szeletét, a felhasználótól a letétbe helyezési ügynökökhöz menő kommunikációhoz hozzáférő harmadik fél kiolvassa a felhasználó részcsomagjainak tartalmát, és összeállítja a teljes egyéni rejtjelkulcsot a részcsomagokban lévő egyéni rejtjelkulcs szeleteinek kombinálásával. Ezután a harmadik fél az egyéni rejtjelkulccsal üzeneteket tud megfejteni és titkosítani a felhasználó nevében. Ennek megakadályozására a legjobb módszer az, hogy titkosított kommunikációs rendszert alkalmazunk a felhasználóktól a letétbe helyezési ügynökökhöz menő részcsomagok küldéséhez. A felhasználó megkapja az egyéni rejtjelkulcsának letétbe helyezésére kiválasztott letétbe helyezési ügynökök nyilvános titkosító rejtjelkulcsainak 166 igazolásait, amely igazolásokat a fő letétbe helyezési központ aláírja, és ezzel igazolja, hogy a meghatározott letétbe helyezési ügynököt a fő letétbe helyezési központ megbízta egy rejtjelkulcsrészcsomag átvételére és tárolására. Ezután a felhasználó a berendezés gyártójától (vagy az egész rendszerre kiterjedő hatóságtól) kapott igazolással vagy előre beágyazott utasítási rejtjelkulccsal ellenőrzi a fő letétbe helyezési központ aláírását. A berendezés ezután minden letétbe helyezési ügynök számára az adott ügynök hitelesített, nyilvános titkosító rejtjelkulcsa alapján titkosít egy üzenetet, amely tartalmazza a felhasználó egyéni rejtjelkulcsának részcsomagját. Adott esetben a gyártó a chipbe számos bizalmas letétbe helyezési ügynök nyilvános titkosító rejtjelkulcsát beágyazhatja a megfelelő utasítási rejtjelkulcsokkal a korábban leírtak szerint, hogy a felhasználó egyéni rejtjelkulcsának szeleteit az utasítási rejtjelkulcsok birtokosa – általában a fő letétbe helyezési központ – által megbízott letétbe helyezési ügynökökhöz küldje. Ily módon a fő letétbe helyezési központ vagy a gyártó letétbe helyezési ügynökeinek „családjában" mindegyik ügynök képes lesz felhasználói letétbe helyezési kérelmek megfejtésére, mialatt a felhasználót megszabadítjuk attól a tehertől, hogy a letétbe helyezési ügynökök nyilvános titkosítórejtjelkulcs-igazolásait megszerezze.

Miután az egyes 163 letétbe helyezési ügynökök vagy megbízottak megkapják a megfelelő 161 részcsomagot a felhasználótól vagy felhasználó berendezésétől, a megbízott megvizsgálja a felhasználó berendezésétől kapott megbízotti 161 részcsomagban lévő egyéni rejtjelkulcsszeletet, és a 165 fő letétbe helyezési központtal együtt ellenőrzi, hogy az a teljes egyéni rejtjelkulcs érvényes és hibátlan része-e. Szükséges az, hogy a letétbe helyezési ügynökök és a fő letétbe helyezési központ megbízható eszközzel rendelkezzenek annak ellenőrzésére, hogy a felhasználói, egyéni titkosító rejtjelkulcs szeletei ténylegesen elhelyezésre kerültek-e. Kívánatos, hogy a rejtjelkulcsszeletek ellenőrzését a letétbe helyezési ügynökök és a fő letétbe helyezési központ úgy végezze, hogy magukat a szeleteket soha ne vizsgálják vagy kezeljék, illetve hogy azokat ne hozzák össze egy helyre. A Micali-féle „előnyös" letétbe helyezési rendszer rendkívül megbízható módot szolgáltat a rejtjelkulcsszeletek különálló elhelyezésének letétbe helyezési központ általi ellenőrzésére. A 10. és 11. ábrán látható Micali-eljárásban az ellenőrzés azzal a meghatározott értékekből álló készlettel történik, amelyet a felhasználó chipje speciális Micali-algoritmussal számít a részcsomag elkészítése közben, és amely a rejtjelkulcs szelettel együtt a letétbe helyezési ügynökhöz menő részcsomagban van. A Micali-algoritmus és rejtjelkulcsszeletének ellenőrzése ismertek a szakterületen, így azokat itt nem részletezzük. A megbízottak ezután a berendezés gyártójának igazolását későbbi megfejtésre való használatra eltárolják, és jóváhagyják a rejtjelkulcsszeletet oly módon, hogy a fő letétbe helyezési központnak megfelelő aláírt üzenetet küldenek felhasználói névvel és berendezésigazolással együtt, valamint hogy a rejtjelkulcsszeletet aláírják és eltárolják. A megbízott a birtokában lévő egyéni megfejtési rejtjelkulcsszeletet (vagy szeleteket) csak akkor fedi fel, ha (a) meghatalmazást vagy bírósági végzést, illetve ha (b) a berendezés törvényes tulajdonosától származó aláírt kérelmet mutatnak be.

A 16. ábrán ábrázolt, kizárólag a bizalmas berendezésre hagyatkozó, előnyös letétbe helyezési és ellenőrzési eljárásban minden megbízott átad egy 167 üzenetet a 165 fő letétbe helyezési központnak, amely azonosítja

a felhasználó nevét, nyilvános titkosító rejtjelkulcsát, berendezése számát és a kapott véletlen számot. Ezen túlmenően a felhasználói berendezés a 165 fő letétbe helyezési központ nyilvános titkosító rejtjelkulcsával titkosított csomagot is küld a 165 fő letétbe helyezési központnak, amely tartalmazza az egyéni rejtjelkulcs szeleteinek ellenőrzésére szolgáló véletlen számokat. A 165 fő letétbe helyezési központ átveszi a 164, 167 üzeneteket a felhasználói berendezéstől és a megbízottaktól, és ellenőrzi, hogy az egyes megbízottaktól kapott véletlen szám megegyezik-e azzal a számmal, amelyet a felhasználói berendezés szerint a felhasználói berendezés a megbízottnak adott. Megjegyezzük, hogy ennél az eljárásnál a 163 letétbe helyezési ügynökök és a 165 fő letétbe helyezési központ kizárólag a bizalmas berendezés 161 részcsomagon lévő aláírására hagyatkoznak, amikor megbizonyosodnak afelől, hogy a letétbe helyezés megfelelő. Ez a letétbe helyezési és ellenőrzési eljárás nem tesz szükségessé másodlagos matematikai műveleteket annak ellenőrzésére, hogy a letétbe helyezés megfelelő, vagy hogy a hitelesítéshez bemutatott nyilvános rejtjelkulcs megegyezik-e az elhelyezett rejtjelkulcsszeletekkel. Bár a nyilvánosság, a felhasználó vagy az egész rendszerre kiterjedő megbízhatóság szempontjából kívánatos lehet ellenőrizhető rejtjelkulcs-letétbehelyezési algoritmus, például a Micali-algoritmus alkalmazása, de ez nyilvánvalóan nem szükséges akkor, ha az ilyen eljárás alkalmazásának járulékos költsége nem igazolható. Ezen túlmenően ezzel a módszerrel, amelyben kizárólag a bizalmas berendezésre hagyatkozunk, nincs korlátja a kigondolható rejtjelkulcs-szeletelő rendszerek komplexitásának, mivel nincs szükség komplex másodlagos algoritmusok kigondolására az adott rendszer megfelelő működésének ellenőrzésére. Elégséges csak a firmware-kódot beágyazó berendezés gyártójának integritásában bízni, valamint abban, hogy a berendezés ellenáll a külső behatásoknak.

Miután a fő letétbe helyezési központ ellenőrizte a felhasználó minden egyéni rejtjelkulcsszeletét, jóváhagyja azt a nyilvános titkosító rejtjelkulcsot, amely megfelel a felhasználó megbízottai által jóváhagyott egyéni megfejtési rejtjelkulcsnak. A 165 fő letétbe helyezési központ a nyilvános rejtjelkulcsot egy aláírt 168 igazolással (amelyet fő letétbe helyezési központ igazolásnak, nyilvános titkosítórejtjelkulcs-igazolásnak, vagy egyszerűen a letétbe helyezési igazolásnak nevezünk) hagyja jóvá, amellyel igazolja, hogy a hitelesítendő nyilvános rejtjelkulcsnak megfelelő egyéni rejtjelkulcsot megfelelő formában már letétbe helyezték. A felhasználó berendezésének nyilvános aláírási rejtjelkulcsa, amelyet a berendezés gyártójának igazolásából kapunk meg, szintén behelyezhető a fő letétbe helyezési központ igazolásába, és ezzel szükségtelenné tesszük a berendezés gyártója igazolásának elküldését vagy újbóli ellenőrzését a folyamat későbbi szakaszaiban. A fő letétbe helyezési központ igazolásának formátuma a következő lehet:

Verziószám
Letétbe helyezési igazolás sorszáma
Fő letétbe helyezési központ országkódja
Fő letétbe helyezési központ neve
Fő letétbe helyezési központ nyilvános titkosító rejtjelkulcsa (a LEAF létrehozására)
Felhasználó által választott név
Felhasználó nyilvános titkosító rejtjelkulcsa (az itt hitelesítendő)
Felhasználói berendezés nyilvános aláírás-ellenőrző rejtjelkulcsa (a berendezés aláírásának ellenőrzésére)
Érvényesség dátuma (kezdet/vég)
Fő letétbe helyezési központ aláírása
[Fő letétbe helyezési központ egész rendszerre kiterjedő igazolása]

A fő letétbe helyezési központ által kibocsátott, nyilvános titkosítórejtjelkulcs-igazolásokat elterjesztjük, és azokat a berendezés tulajdonosa a titkosított üzenetek származásának visszakeresésére használhatja, vagy használhatják mások a felhasználó nyilvános/egyéni titkosítórejtjelkulcs-párját tartalmazó berendezés tulajdonosához menő üzenetek titkosítására.

A találmány nem igényel egynél több letétbe helyezési ügynököt a felhasználó egyéni rejtjelkulcsa szeleteinek átvételére, és néhány esetben elegendő lehet csupán egy letétbe helyezési ügynöknél (vagy letétbe helyezési központnál) elhelyezni a felhasználó egyéni megfejtési rejtjelkulcsát. Hogy a felhasználók és a nyilvánosság részéről nagyobb bizalmat érjünk el a rendszerrel kapcsolatban, kívánatos a felhasználó egyéni megfejtési rejtjelkulcsának több letétbe helyezési ügynök közötti szétszeletelése oly módon, hogy mindegyik rejtjelkulcsszelet vagy azok közül meghatározott számú szükséges a felhasználó rejtjelkulcsának összerakásához és kommunikációjának megfejtéséhez. Kívánatos továbbá, hogy a letétbe helyezési ügynökök független, bizalmas üzleti működésűek legyenek, vagyis a tudás feldarabolódjon, és így korrupció, megvesztegetés, erőszak vagy visszaélés megkísérlése esetén nehezebb lesz jogtalanul megszerezni a felhasználó egyéni megfejtési rejtjelkulcsát, mint amikor az egyéni rejtjelkulcs egyetlen személynél van eltárolva. Az is kívánatos, hogy a személyek földrajzilag elkülönüljenek, hogy még inkább lekorlátozzuk a felforgatási vagy korrupciós lehetőségeket.

A kommunikációk titkosítása

Annak a felhasználónak, aki titkosított üzenetet akar küldeni egy másik felhasználónak, rendelkeznie kell egy letétbe helyezési igazolással saját berendezése számára, és egy letétbe helyezési igazolással a szándékolt vevő nyilvános titkosító rejtjelkulcsa számára, mivel a találmány szerinti berendezés sem titkosítani, sem megfejteni nem fog, ha valamelyik hiányzik. A küldőnek először be kell töltenie saját igazolását a berendezésbe, általában akkor, amikor azt a fő letétbe helyezési központtól megkapja. Ezután a szándékolt vevő nyilvános rejtjelkulcs-igazolása megszerezhető közvetlenül a szándékolt vevőtől, nyilvános rejtjelkulcs-igazolásokat listázó tárolószolgálattól, vagy az üzenet küldőjének helyi fájljából, például olyan felhasználók fájljából, akikkel a küldő előzőleg titkosított kommunikációt folytatott. A találmány egyik kiviteli példájában, mivel a küldő berendezése nem titkosít, és a vevő berendezése nem fejt meg, ha a

vevő nyilvános titkosító rejtjelkulcsa nem „érvényes", azért, hogy a vevő berendezése megfejtse a titkosított üzenetet, a vevő nyilvános titkosító rejtjelkulcsának igazolását alá kell írnia (a) a vevő berendezésegyártójának (ez nem valószínű eset, mert a berendezésgyártók nagy valószínűséggel nem fognak letétbe helyezni felhasználói egyéni rejtjelkulcsokat), (b) a fő letétbe helyezési központnak, és az igazolást kísérnie kell egy gyártói igazolásnak, amely a fő letétbe helyezési központot érvényes megbízottként jóváhagyja, vagy (c) olyan megbízottnak vagy fő letétbe helyezési központnak, amelynek utasítási rejtjelkulcsa gyártás alatt a berendezésbe beágyazásra került. A szándékolt vevő hitelesített, nyilvános titkosító rejtjelkulcsával, amely a vevő nyilvános titkosító rejtjelkulcsának igazolásából származik, a küldő felhasználó a kommunikáció titkosításához és megfejtéséhez szakaszrejtjelkulcsot generál mind a küldő, mind pedig a vevő számára. A szakaszrejtjelkulcsot előnyösen a hitelesített Diffie–Hellman-eljárással, vagy adott esetben más megfelelő rendszerrel állíthatjuk elő. A hitelesített Diffie–Hellman-eljárásban a felhasználó először véletlenszerűen előállítja az üzenetre vonatkozó ideiglenes egyéni rejtjelkulcsát, majd saját egyéni rejtjelkulcsa és a vevő nyilvános rejtjelkulcsa alapján kiszámítja a szakaszrejtjelkulcsot (vagyis a vevő nyilvános titkosítórejtjelkulcs-igazolásában lévő közbenső számot és két nyilvános számot). Ezután a küldő a szakaszrejtjelkulccsal titkosítja a vevő felhasználónak küldendő üzenetet.

Annak eldöntésekor azonban, hogy a küldő küldjön-e titkosított üzenetet a szándékolt vevőnek, a küldő nem képes ellenőrizni a vevő nyilvános titkosító rejtjelkulcsának igazolását vagy az azon lévő digitális aláírást, ha a küldő berendezését és a vevő berendezését különböző gyártó gyártotta. Az a tény, hogy a vevő berendezését másik gyártó gyártotta, megnehezíti a küldőberendezést abban, hogy ellenőrizze a gyártó aláírását vagy a gyártói igazolást (amelyet a vevő rejtjelkulcsának letétbe helyezési igazolását aláíró fő letétbe helyezési központ hitelesített), amelyek alátámasztják a fő letétbe helyezési központ érvényességét és a gyártó általi jóváhagyását. Ugyanígy a vevő chipje is képtelen ellenőrizni ezeket a küldő igazolására vonatkozó feltételeket a megfejtés előtt. Ekkor mindkét fél esetében letétbe helyezési korlátozást kell eszközölni ahhoz, hogy törvényes ellenőrzési ügynökök számára lehetővé tegyük egy adott gyanús felhasználó által küldött és vett üzenetek törvényes lehallgatását és megfejtését anélkül, hogy szükséges lenne megszerezni a másik, nem megfigyelt fél egyéni megfejtési rejtjelkulcsát, amivel hozzáférhetünk a nem megfigyelt fél nem ide vonatkozó üzeneteihez is.

A probléma egyik lehetséges megoldása, mialatt egynél több gyártónak is megengedjük titkosítóberendezések gyártását, hogy a berendezésbe vagy a felhasználó fő letétbe helyezési központja, illetve a chip gyártója által kibocsátott igazolásba be kell ágyazni egy bizalmas nemzeti személy, például a Federal Keserve Bank (FRB) nyilvános rejtjelkulcsát, amely az FRB által a különböző fő letétbe helyezési központok vagy gyártók számára kibocsátott további igazolás ellenőrzésére használható. Ez az FRB által aláírt igazolás igazolja egy meghatározott fő letétbe helyezési központ vagy gyártó megbízhatóságát. Egy küldő felhasználó ezután megszerezheti egy szándékolt vevő nyilvános titkosító rejtjelkulcsának igazolását, és megbízhat az igazolást kibocsátó fő letétbe helyezése központban, mivel a fő letétbe helyezése központot a chip gyártója helyett az FRB bízta meg, amint azt az FRB nyilvános rejtjelkulcsa vagy igazolása igazolja. Egy meghatározott berendezés aláírása is megbízható lesz, mivel a berendezést hitelesítő másik gyártót az FRB bízta meg, amint azt az FRB igazolása vagy nyilvános rejtjelkulcsa igazolja. Annak érdekében, hogy kevésbé helyi, egyesült államokbeli szinten gondolkodjunk, és nemzetközi, egész világot átfogó rendszerhez jussunk, egy bizalmas globális személy, például a svájci Nemzetközi Befektetések Bankja nyilvános rejtjelkulcsát beágyazhatjuk a bizalmas berendezésbe, az FRB igazolásába, a fő letétbe helyezése központ igazolásába vagy a gyártói igazolásba (az alkalmazott bizalmassági modelltől függően), amely az FRB rejtjelkulcsához hasonló módon működhet a fő letétbe helyezési központok és gyártók egész világra kiterjedő akkreditálására. Másik lehetséges módja annak, hogy a berendezés a más gyártó által hitelesített fő letétbe helyezési központokban egyesült államokbeli vagy világméretű hatóság nélkül megbízzon az, hogy a berendezésgyártók vagy fő letétbe helyezési központok egymást keresztbe hitelesítik. Ez lehetővé teszi a küldő berendezése számára a vevő letétbe helyezési korlátozásainak kikényszerítését azáltal, hogy lehetővé teszi a küldő berendezése számára a vevő letétbe helyezési igazolása útjának visszaellenőrzését a vevő berendezése gyártóján vagy fő letétbe helyezési központon keresztül magáig a vevőig. Az előnyös kiviteli alakban bizalmas, egész rendszerre kiterjedő személy nyilvános rejtjelkulcsa van beágyazva a bizalmas berendezésbe a fő letétbe helyezési központok és gyártók egész rendszerre kiterjedő akkreditálására, amely rejtjelkulcs a fent ismertetett módon, az FRB vagy globális hatóság rejtjelkulcsával megegyezően működik.

Amikor egy felhasználó, személy vagy berendezés digitálisan aláírt „igazolást ellenőriz", legyen az hitelesítő hatóság vagy gyártó által kibocsátott gyártói igazolás, illetve letétbe helyezési igazolás, a legtöbb jelenlegi és tervezett, nyilvános rejtjelkulcsok igazolásait kezelő rendszerekben általános gyakorlat (és a leírásban is feltételezzük), hogy a felhasználó, személy vagy berendezés azt is megvizsgálja, hogy létezik-e megfelelő „igazolás-visszavonási lista" (CRL, certificate revocation list), annak eldöntésére, hogy a hitelesítő hatóság vagy más kibocsátó terjesztett, propagált vagy másképpen hozzáférhetővé tett-e megfelelő biztonsági politika szerint frissített, visszavont igazolásokból álló listát, valamint hogy a kibocsátó neve és az igazolás száma szerinti igazolást visszavonták-e. Adott felhasználó számára kibocsátott igazolást vissza lehet vonni elhalálozás, név, illetve alkalmazotti viszony megváltozása vagy az egyéni rejtjelkulcsot tartalmazó berendezés (a személyi intelligens mikrokártya) elvesztése, ellopása vagy megsemmisülése esetén. Egy vállalat számára kibocsátott

igazolást vissza lehet vonni az üzleti tevékenység szüneteltetése, névváltoztatás vagy az egyéni rejtjelkulcsot tartalmazó berendezés elvesztése, ellopása, illetve megsemmisülése esetén. Egy berendezés számára kibocsátott igazolás visszavonható a berendezés elvesztése, ellopása, működésből történő kivonása vagy megsemmisülése esetén. A CRL-ek igazolás-ellenőrzés közbeni vizsgálatát részletesen ismertették a nyilvános irodalomban (például ANSI X9.30 – 3. fejezet), ezért ez további fejtegetést nem igényel. A felhasználók, személyek és berendezések általában hozzáféréssel rendelkeznek a megfelelő távközlési szolgáltatásokhoz, így a CRL-eket megkereshetik, illetve a fent leírt módon informálódhatnak. A találmány szerint feltételezzük, hogy minden CRL-t kibocsátó személy hozzáférhetővé teszi azokat az érdekelt felek számára.

Az üzenet-ellenőrző fejrész formátuma

Titkosított üzenet küldésekor a küldő felhasználónak ki kell alakítania egy megfelelő üzenet-ellenőrző fejrész (MCH) mezőt is, amely a következő információkat tartalmazza:

(1) A küldő titkosított üzenetre vonatkozó közbenső számát, amelyet a küldő az üzenetet titkosító szakaszrejtjelkulcs számítására is használt, véletlenszerűen generált, ideiglenes egyéni rejtjelkulccsal számít. A vevő felhasználónak rendelkeznie kell ezzel a közbenső számmal, hogy az üzenet megfejtéséhez ki tudja számítani a szakaszrejtjelkulcsot.

(2) A küldő fő letétbe helyezési központjának nevét és országkódját.

(3) A vevő fő letétbe helyezési központjának nevét és országkódját, amelyek a vevő nyilvános rejtjelkulcsának igazolásából származnak.

(4) A küldő letétbe helyezési igazolásának számát, amely a küldő fő letétbe helyezési központjának nyilvános rejtjelkulcsával titkosítva van (amely rejtjelkulcs a küldő letétbe helyezési igazolásából származik), hogy azt csak a küldő fő letétbe helyezési központja tudja megfejteni.

(5) A küldő azon közbenső számát (amely különbözik a küldő előző közbenső számától), amellyel a küldő kiszámította azt az ideiglenes szakaszrejtjelkulcsot, amellyel a küldő igazolási száma titkosításra került a küldő fő letétbe helyezési központja számára. A küldő fő letétbe helyezési központjának rendelkeznie kell ezzel a számmal, hogy ki tudja számítani a küldő igazolási számának megfejtésére szolgáló ideiglenes rejtjelkulcsot.

(6) A titkosított üzenet szakaszrejtjelkulcsát, amely a küldő saját nyilvános rejtjelkulcsával (a közbenső szám a küldő saját nyilvános igazolásából) titkosítva van, és így a küldő az üzenet-szakaszrejtjelkulcsot gyakorlatilag saját magához küldi. A törvényes ellenőrzés akkor nyerhet hozzáférést ehhez az üzenet-szakaszrejtjelkulcshoz, ha a küldő letétbe helyezési ügynökeitől megkapta a küldő egyéni rejtjelkulcsának komponenseit.

(7) A küldő azon közbenső számát (amely különbözik a küldő két megelőző közbenső számától), amellyel a küldő kiszámította azt az ideiglenes rejtjelkulcsot, amellyel az üzenet-szakaszrejtjelkulcsot saját magához titkosította. A törvényes ellenőrzésnek rendelkeznie kell ezzel a számmal, hogy a küldő fő letétbe helyezési központjától megkapott egyéni rejtjelkulcsát (a titkos számát) is felhasználva kiszámíthassa az ideiglenes rejtjelkulcsot az üzenet-szakaszrejtjelkulcs megfejtésére.

(8) A vevő igazolási számát, amely a vevő fő letétbe helyezési központjának nyilvános titkosító rejtjelkulcsával van titkosítva (és amelyet a vevő letétbe helyezési igazolásából kapunk meg), és így azt csak a vevő fő letétbe helyezési központja tudja megfejteni.

(9) A küldő közbenső számát (amely különbözik a küldő három megelőző közbenső számától), amellyel a küldő kiszámította azt az ideiglenes rejtjelkulcsot, amellyel a vevő letétbe helyezési igazolási száma titkosítva volt a vevő fő letétbe helyezési központja számára. A vevő fő letétbe helyezési központjának rendelkeznie kell ezzel a számmal, hogy kiszámíthassa a vevő igazolási számának megfejtésére szolgáló ideiglenes szakaszrejtjelkulcsot.

(10) Időbélyeget (opcionálisan) követési célokra, és lehetőség szerint a meghatalmazás dátum és időbeli korlátozásainak ellenőrzésében való segítségre.

(11) A küldő berendezésének aláírását.

(12) A küldő nyilvános rejtjelkulcsának letétbe helyezési igazolását, amelyet a küldő fő letétbe helyezési központja bocsátott ki. A küldő letétbe helyezési igazolása tartalmazza a küldő berendezésének nyilvános aláírási rejtjelkulcsát, amelyet a fő letétbe helyezési központ előre leellenőrzött, majd azután kimásolt a küldő berendezésének gyártói igazolásából.

(13) A fő letétbe helyezési központ igazolását az FRB-től, a gyártótól vagy más bizalmas, egész rendszerre kiterjedő hatóságtól a küldő letétbe helyezési igazolásához csatolva, ha a vevő chipjét más gyártó gyártotta. A gyártó, az FRB vagy az egész rendszerre kiterjedő hatóság igazolására csak a felek közötti első kommunikációkor van szükség. Az igazolás lehet a vevő gyártójától vagy fő letétbe helyezési központjától származó kereszthitelesítés is.

Az MCH ezáltal a következőképpen foglalható össze:

A küldő közbenső száma (az üzenet vevő általi megfejtésének lehetővé tételére)

A küldő fő letétbe helyezési központjának országkódja

A küldő fő letétbe helyezési központjának neve

A vevő fő letétbe helyezési központjának országkódja

A vevő fő letétbe helyezési központjának neve

A küldő letétbe helyezési igazolásának száma a küldő fő letétbe helyezési központja számára titkosítva

A küldő közbenső száma (a küldő igazolási számának titkosítására)

Az üzenet szakaszrejtjelkulcsa a küldő számára titkosítva

A küldő közbenső száma (az üzenet-szakaszrejtjelkulcs titkosítására a küldő számára)

A vevő letétbe helyezési igazolásának száma, amely a vevő fő letétbe helyezési központja számára van titkosítva

A küldő közbenső száma (a vevő igazolási számának titkosítására)

Időbélyeg
A küldő berendezésének MCH-aláírása
[A küldő letétbe helyezési igazolása]
[A letétbe helyezési központ igazolása]

A 17. ábra titkosított 176 üzenet 172 MCH-val történő küldésének folyamatát ábrázolja. Az egész 172 MCH (a csatolt 173, 174, 175 igazolások gyakorlatilag nem részei a 172 MCH-nak) alá van írva a küldő 171 berendezése által a 171 berendezés egyéni DSA aláírási rejtjelkulcsával, amely rejtjelkulcshoz (a küldő letétbe helyezési 173 igazolásában) csatolva van a gyártó beágyazott igazolása a 171 berendezés nyilvános aláírási rejtjelkulcsának hitelesítésére. Ez biztosítja, hogy az egész 172 MCH érintetlenül továbbítódik a vevőhöz és hogy a vevő chipje könnyen ellenőrizheti, hogy a 172 MGH-t nem változtatták-e meg. A gyártó igazolását kísérheti egy nemzeti (FRB) vagy világhatósági igazolás, hogy hitelesítse a küldő chipje gyártójának hitelességét abban az esetben, ha a vevő berendezését más gyártó gyártotta.

A találmány egy másik kiviteli alakjában egy második, rövidebb MCH formátum használható abban az esetben, ha a teljes titkosság nem rendkívüli fontosságú. Ebben az MCH-ban sem a küldő igazolási száma, sem a vevő igazolási száma nincs titkosítva a megfelelő fő letétbe helyezési központ számára. Az igazolási számok nem titkosítása időt és helyet takarít meg az MCH létrehozásakor. A találmány egy további kiviteli alakjában egy harmadik, még rövidebb MCH formátum használható abban az általános esetben, amikor a küldő és a vevő mindketten ugyanazt a fő letétbe helyezési központot alkalmazzák rejtjelkulcs-letétbehelyezési célokra, vagyis amikor EC1 és EC2 megegyezik. Az MCH lényegesen rövidebb lehet, ha abban nincs szükség a második fő letétbe helyezési központra vonatkozó azonosítóinformációra, valamint speciális közbenső számra a vevő igazolási számának a második fő letétbe helyezési központ számára történő titkosításához. Az MCH mérete tovább csökkenthető RSA típusú rejtjelkulcsátvitel alkalmazásával az üzenet, valamint a három titkosított belső LEAF-komponens DES rejtjelkulcsának titkosítására. Ezen eljárás szerint a küldő közbenső számait helyettesítjük egy kisebb, RSA-val tömörített DES rejtjelkulccsal. Ezáltal a küldő RSA-val titkosíthatja az üzenet-szakaszrejtjelkulcsot a vevő számára, ami szükségtelenné teszi az MCH-ban az első közbenső számot. A küldő RSA-val titkosíthatja a saját magához menő üzenet-szakaszrejtjelkulcsot is (valójában a törvényes ellenőrzés általi későbbi megfejtéshez), és ezáltal szükségtelenné teszi az MCH-ban a harmadik közbenső számot. A küldő továbbá RSA-val titkosíthatja saját és a vevő igazolási számát is, és ezáltal szükségtelenné teszi az MCH-ban a második és negyedik közbenső számokat. Amint azt a 18. ábra mutatja, a négy közbenső szám és az azokkal kapcsolatos titkosítás elhagyása, valamint a közbenső számok kisebb, RSA átvitellel titkosított 181 számokkal való felváltása az MCH méretéből jelentős helyet takarít meg.

A véletlen összetevő közreműködése

Úgy gondolhatnánk, hogy a kizárólag az RSA rejtjelkulcs-átviteli eljárással vagy a hitelesített Diffie–Hellman-rendszerrel kicserélt üzenet-szakaszrejtjelkulcs nem elegendően biztonságos, mivel mindkét eljárásnál mind a küldő, mind pedig a vevő információt szolgáltat, de az üzenet-szakaszrejtjelkulcsot csak a küldő generálja. A biztonságos kommunikációra vonatkozó katonai szabványok szerint azonban mind a küldőnek, mind a vevőnek véletlen összetevővel kell hozzájárulnia a szakaszrejtjelkulcs egyes kommunikációs szakaszok előtti generálásához, nyilvánvalóan azért, hogy lecsökkenjen annak az esélye, hogy a küldő gyenge rejtjelkulcsot használ vagy ismételten ugyanazt a rejtjelkulcsot használja, és ezzel a vevőt akarata ellenére nemkívánatos biztonsági veszélynek tegye ki. A bizalmas berendezések találmány szerinti rendszere kétféle módon tudja ezt a félelmet eloszlatni. Először is a rendszer biztosíthatja, hogy a küldőberendezés az egyes rejtjelkulcsokat beépített hardver zajforrás – például fordítva előfeszített dióda – zajából levezetett véletlen számokkal generálja, amint azt a korábbiakban ismertettük. Másodszor, ha a berendezés aláírja az MCH-t, a vevő biztosítva van, hogy a szakaszrejtjelkulcsok és az azok generálására szolgáló véletlen számok erősek és egyediek. Ha valaki azonban mégis ragaszkodik a nagyobb biztonsághoz, kívánhatja mindkét résztvevőtől a kommunikációhoz véletlen összetevővel történő hozzájárulást, amint azt a titkos információkra szolgáló, 1. típusú katonai rendszerekre előírják.

A leírásban a küldőt eddig úgy írtuk le, mint aki a vevő letétbe helyezési igazolásában lévő nyilvános titkosító rejtjelkulcsa alapján generálja az üzenet-szakaszrejtjelkulcsokat, de nem használ fel a kommunikáció felállási fázisa alatt a vevőtől kapott véletlen összetevőt. Az olyan elrendezés azonban, amelyben a küldő a generáláshoz a vevőtől hozzájárulást kap, új problémát vet fel. A vevő számára nem lehet egyszerűen megengedni, hogy saját maga Diffie–Hellman közbenső számot generáljon, és azt a küldőnek üzenet-szakaszrejtjelkulcs generálásához elküldje, mivel a vevő ezután már nem használná a bizalmas berendezésében lévő, letétbe helyezett egyéni rejtjelkulcsot üzenetek megfejtésére, és a kommunikációt a törvényes ellenőrzés nem figyelhetné meg. A letétbe helyezési rendszer sikere megkívánja, hogy sem a küldő, sem a vevő ne legyen képes üzenet elolvasására nyilvántartásba vett bizalmas berendezés használata nélkül.

Annak lehetővé tételére, hogy mind a küldő, mind pedig a vevő a kommunikáció előtt véletlen összetevővel járuljon hozzá az üzenet-szakaszrejtjelkulcshoz, a kezdeti rejtjelkulcs-kicserélési protokollt megváltoztathatjuk úgy, hogy a leendő vevő berendezésének lehetővé tesszük, hogy a vevő letétbe helyezett egyéni rejtjelkulcsától különböző, új ideiglenes Diffie–Hellman titkos számot generáljon, amellyel új közbenső számot számítunk, és amelyet az üzenet titkosítására szolgáló üzenet szakaszrejtjelkulcs számításához a vevőnek elküldünk. Az (MCH-ban lévő) közbenső számokat, valamint az MCH különböző részeinek titkosítására szolgáló ideiglenes szakaszrejtjelkulcsokat továbbra is a vevő letétbe helyezett egyéni rejtjelkulcsával generáljuk. Ez a változtatás azonban azt kívánja, hogy az új titkos szám generá-

lása a leendő vevő berendezésében történjen, hogy ez az új titkos szám a bizalmas berendezés belsejében maradjon, és hogy az új közbenső számot a leendő vevő berendezése aláírja a küldő berendezéséhez történő elküldés előtt annak igazolására, hogy az új ideiglenes titkos szám valóban biztonságosan van a vevő berendezésébe zárva. A korábbiakhoz hasonló módon a küldő berendezése új titkos számot generál, amely különbözik a küldő letétbe helyezett egyéni rejtjelkulcsától, és az új titkos számmal, valamint a vevő új közbenső számával generálja az üzenet megfejtésére szolgáló üzenet-szakaszrejtjelkulcsot. A küldő berendezése a küldő új titkos számával szintén generálja a küldő új közbenső számát, amelyet lehallgatási célokra az MCH részeként a vevő berendezésének elküld. Ebben az eljárásban ezért az üzenet szakaszrejtjelkulcsa a küldő és a vevő által szolgáltatott véletlen összetevőket is tartalmaz.

Ebben a rejtjelkulcs-kicserélési protokoll változatban azonban, mivel a vevő és a küldő gyakorlatilag mindig új Diffie–Hellman-típusú egyéni rejtjelkulcsot használ az egyes üzenetek számára, a letétbe helyezési tulajdonság „eltűnik", és a törvényes ellenőrzés, valamint a vállalati vezetés nem lesz képes megszerezni ezeket az ideiglenes üzenet-szakaszrejtjelkulcsokat a letétbe helyezési ügynököktől. Ezért a letétbe helyezési rendszerrel szemben támasztott igények és az érdekelt felek azt kívánják, hogy az üzenet-szakaszrejtjelkulcsot – ugyanúgy, mint a korábbi megoldásoknál – az MCH-ban küldjük. A lehallgatás egyenlőségének biztosítására az MCH minden előzőekben leírt mezője gyakorlatilag megmarad. Az üzenet-szakaszrejtjelkulcsot a küldőhöz továbbító mezőnek (amely a küldőt lehallgató törvényes ellenőrzési ügynökök egyetlen lehetősége az üzenet elolvasására) továbbra is az MCH-ban kell lennie, hogy megőrizzük a lehallgatás egyenlőségének elvét. Az MCH-ban lévő üzenet-szakaszrejtjelkulcsot a korábbi megoldásokhoz hasonlóan a küldő nyilvános titkosító rejtjelkulcsával titkosítjuk, amelyhez a törvényes ellenőrzés hozzáfér. A küldő új közbenső számát az MCH első elemeként a vevőhöz küldjük, mint azelőtt, hogy a törvényes ellenőrzésnek lehetővé tegyük a vevő lehallgatását és az üzenet-szakaszrejtjelkulcs kiszámítását. Ily módon, hogy megvalósítsuk az interaktív Diffie–Hellman rejtjelkulcs-kicserélési technikát, a protokoll szükségessé teszi, hogy a leendő vevő új közbenső számát a berendezésén belül generáljuk és írjuk alá, valamint hogy az MCH-hoz csatoljuk a küldő új közbenső számát, amelyet az előzőleg ismertetett rejtjelkulcs-átviteli eljárásokban nem alkalmazunk, mivel ez az egyetlen lehetőség arra, hogy az érdekelt felek (törvényes ellenőrzés, alkalmazók és mások) el tudják olvasni az üzenetet. Ez az eljárás azonban nem gazdaságos az online telefonos, hálózati, illetve hívási tranzakciókon kívüli tranzakciók esetén, mivel a berendezésnek túl sok dologra – a felek speciális közbenső számaira – kell emlékeznie. Ez az eljárás előnyösen alkalmazható cellarendszerű telefon, hálózati bejelentkezés stb. esetén, amikor is tisztán valós idejű interaktív kommunikációs szakaszokra van szükség.

Az érdekelt felek fejrészei

Az MCH-t általában üzenetfejrészként a titkosított üzenet elé helyezzük. Sok jelenlegi elektronikusposta- és dokumentációs rendszerben több vevő számára engedélyezik egy kódolt üzenet elolvasását az MCH fent ismertetett RSA-átviteles kialakításával oly módon, hogy az üzenet-szakaszrejtjelkulcsot az egyes vevők nyilvános titkosító rejtjelkulcsával RSA-titkosítják. Vagyis ha egy adott titkosított üzenetet több vevőnek szándékozunk elküldeni, az MCH fejrész tartalmazhatja minden szándékolt vevőre a szándékolt vevő nevét, valamint az adott vevő nyilvános titkosító rejtjelkulcsával RSA-titkosított üzenet-szakaszrejtjelkulcsot. Ezáltal minden szándékolt vevő megtalálhatja saját belépési pontját az MCH fejrészbe, megfejtheti a saját üzenet-szakaszrejtjelkulcs másolatát, és elolvashatja az üzenetet. Az MCH hibátlansága több szándékolt vevő esetén is vizsgálható a kommunikáció mindkét végén: a küldő végén a kimeneti MCH-t a küldő berendezésének belső logikája ellenőrzi, amikor is megvizsgálja, hogy érvényes MCH-t hozott-e létre egy adott üzenet titkosítása előtt, a vevő végén pedig a vevő berendezése az MCH helyességét a küldőberendezés digitális aláírásának vizsgálatával ellenőrzi. Amint azt korábban megjegyeztük, mivel a vevők üzenetrejtjelkulcs-másolatai az MCH integrális részét alkotják, a vevők az üzenetet csak a változtatás nélküli MCH küldése és vétele esetén tudják megfejteni, ellentétben a Clipper rendszerrel, amelyben az MCH nem kapcsolódik a rejtjelkulcs-átviteli rendszerhez.

Ennél az MCH kialakítási koncepciónál az MCH a 25. ábrán látható módon foglalható össze. Az előző MCH formátumokhoz hasonlóan az MCH érvényességét a küldő berendezésének digitális 258 aláírása igazolja. Ezen túlmenően, az előzőekhez hasonlóan, a küldő és a vevő letétbe helyezési igazolásainak 251, 252 számai megfelelő fő letétbe helyezési központjaik nyilvános titkosító rejtjelkulcsaival titkosítva vannak. Ebben a formátumban azonban a küldő berendezése által aláírt MCH módosított „vevők listájává" válik, amely rugalmasabb és könnyebben megérthető, mint a mai titkosított elektronikus postai rendszerek működése. A küldő és a vevő 253, 254 neveit (illetve rendszerazonosítóikat vagy címeiket) például itt az MCH titkosítatlanul mutatja. Bár ez sérti a küldő és a vevő anonimitását, de gyakorlati okokból nehézkes az elektronikus postai rendszerben üzenetek küldése anélkül, hogy az üzeneteken feltüntetnénk a küldők vagy a vevők neveit és címeit, így elmondhatjuk, hogy a titkosság kismértékben csökken. Ezen túlmenően a küldő és a vevő alkalmazóinak 255, 256 nevei (illetve az egyedi azonosítójuk, például adószámuk vagy DUNS számuk) szintén titkosítatlanul látszanak, ami nagymértékben segíti az alkalmazó biztonsági személyzetét az adott alkalmazott által küldött és kapott üzenetek megtalálásában. Adott esetben ahelyett, hogy a küldő, a vevő és az alkalmazó neveinek blokkját titkosítatlanul hagyjuk, a mezők tartalma lehet „küldő", „címzett", „küldő alkalmazója" és „vevő alkalmazója" (vagy ezek megfelelői) titkosítatlanul, és az aktuális azonosítók az előzőekhez hasonlóan a titkosított területeken lehetnek. Ekkor a

kommunikáció szándékolt vevője az MCH-ben megkeresi az azonosító titkosítatlan rövidítést, és ily módon az MCH csak olyan részeit kísérli meg megfejteni és elolvasni, amelyek neki lettek címezve és titkosítva.

Ezen túlmenően a 25. ábrán ábrázolt MCH formátum lehetővé teszi az alkalmazó szervezetében lévő esetleges alegységek hozzáférését azáltal, hogy másodlagos alkalmazói vonalakat (a, b stb.) definiál. A titkosságot szem előtt tartó alkalmazók esetén az MCH lehet titkosítatlanul „küldő b alk. alegység", amint azt a korábbiakban ismertettük, és a vállalati egység aktuális azonosítóját a titkosított terület tartalmazhatja. Mivel az MCH minden bejegyzése meg van címkézve, nincs korlátja annak, hogy az alkalmazói hozzáférésnek hány szintje lehet; azok mindegyike bizonyos értelemben az üzenet felhatalmazott „vevője" lesz. Továbbá az előző MCH formátumokkal ellentétben, ez az MCH formátum tartalmazhatja a közvetlenül az alkalmazóhoz titkosított üzenet szakasz 257 rejtjelkulcsot, és így az alkalmazónak nem kell a fő letétbe helyezési központhoz és ügynökökhöz mennie, hogy az üzenet megfejtésére megszerezze az üzenet-szakaszrejtjelkulcsot. Ez a formátum ütközhet az alkalmazottak munkahelyi titkossági várakozásaival, de lehetővé teszi az alkalmazóknak alkalmazottaik fájljainak minimális erőfeszítéssel történő vizsgálatát vagy visszaállítását.

Azért hogy a küldő üzenet küldése előtt ilyen formátumú MCH-t hozzon létre, először meg kell kapnia a szándékolt vevők és alkalmazóik szükséges neveit/kódjait, valamint nyilvános rejtjelkulcsait. Ez az információ a vevő letétbe helyezési igazolásából és a küldő saját letétbe helyezési igazolásából gyűjthető össze. A megközelítés általánosításához, és hogy az üzenetet küldeni kívánó felhasználó számára az információt hozzáférhetővé tegyük, a fő letétbe helyezési központoknak – amint azt a korábbiakban kifejtettük – minden felhasználó szabványos letétbe helyezési igazolásába bele kell helyezniük mind a felhasználó alkalmazója, mind a lehetséges alkalmazói alegységek egyedi azonosítószámát vagy kódszámát, valamint nyilvános titkosító rejtjelkulcsát. A letétbe helyezési igazolást ismétlődő alcsoportokkal alakíthatjuk ki az érdekelt felek változó számának hatékony kezelésére. Minden érdekelt fél bejegyzésének van egy egyedi azonosítószáma, egy nyilvános titkosító rejtjelkulcsa és lehetőleg egy utasítási kódja (vagy célkitűzési kódja, amint azt a továbbiakban ismertetjük), amely utasítja a küldő berendezését a fél MCH bejegyzésének kódolását illetően. Ez az utasítási kód tartalmazhat választható elemeket, amelyek megadják a küldőberendezésnek azt a lehetőséget, hogy az (1) tartalmazza a fél egyedi azonosítószámát titkosítatlanul vagy álnéven, például „a-alk", (2) hogy tartalmazza vagy ne tartalmazza az üzenet-szakaszrejtjelkulcsot a kódolt területen, (3) hogy tartalmazza vagy ne tartalmazza a tag egyedi azonosítószámát a kódolt területen, és (4) hogy tartalmazza vagy ne tartalmazza a kódolt terület elején az időbélyeget vagy véletlen számot. Ezek az utasítási (és esetlegesen más) kódok bitmaszk flegjeiként definiálhatók. A felek listája (és/vagy kódjaik), nyilvános titkosító rejtjelkulcsaik és az utasítási flegek tudatják a küldő berendezésével, hogy hogyan alakítsa ki az MCH érdekelt felekre vonatkozó részeit az egyes felek részleges vagy teljes anonimitásra vonatkozó kívánságai szerint. Feltételezzük, hogy a gyakorlatban sok érdekelt fél nem fog törődni az anonimitással, mivel sokkal könnyebb számukra alkalmazottaik üzeneteinek megkeresése és azonosítása, ha azok nevüket és azonosítási számukat titkosítatlanul hagyják.

A vevők általi megfejtés

Amikor a szándékolt vevő megkapja a titkosított 191 üzenetet és a 192 MCH-t tartalmazó mezőt, a 19. ábrán látható módon számos dolgot kell megtenni ahhoz, hogy a vevő elolvassa az üzenetet. A vevőnek először be kell töltenie 190 chipjébe saját érvényes letétbe helyezési 193 igazolását, mert a találmány előnyös kiviteli alakjában a chip enélkül nem végzi el a megfejtést. A vevő letétbe helyezési igazolása ekkor már általában a berendezés memóriájában előre ellenőrzött állapotban van eltárolva. A vevő ezután 190 chipjébe betölti a 192 MCH-t és a küldő letétbe helyezési 194 igazolását, amely tartalmazza a küldő berendezésének nyilvános aláírás-ellenőrzési rejtjelkulcsát is (szükség esetén a megfelelő egész rendszerre kiterjedő, nemzeti vagy világhatóság 195 igazolásával). A vevő 190 chipje megvizsgálja a küldő letétbe helyezési 194 igazolását, hogy ellenőrizze, hogy a küldő egyéni megfejtési rejtjelkulcsa letétbe van-e helyezve. Ezt úgy hajtja végre, hogy a gyártó nyilvános rejtjelkulcsával ellenőrzi a gyártó aláírását a berendezésigazoláson, illetve szükség esetén az egész rendszerre kiterjedő hatóság aláírását a letétbe helyezési központ igazolásán, valamint megvizsgálja, hogy a küldő letétbe helyezési igazolásán érvényes-e a letétbe helyezési központ aláírása. Az előnyös kiviteli alakban az egész rendszerre kiterjedő hatóság nyilvános aláírási 196 rejtjelkulcsa a letétbe helyezési 195 igazolás közvetlen ellenőrzésére szolgál. A vevő chipje a továbblépés előtt ezután az MCH aláírásának vizsgálatával ellenőrzi, (1) hogy a küldőberendezés bizalmas-e, (2) hogy a küldő rejtjelkulcsa letétbe van-e helyezve, amint azt a küldő is ellenőrzi, és (3) hogy a 192 MCH érvényes-e, vagyis hogy az MCH megfelelő formátumú és minden kívánt információt tartalmaz. Ezt a küldő berendezése aláírásának, a küldő berendezése gyártói igazolásán lévő aláírásnak és szükség esetén a gyártó egész rendszerre kiterjedő hatóságtól származó igazolásának vizsgálatával végezzük. A gyártó és az egész rendszerre kiterjedő hatóság nyilvános rejtjelkulcsait az ellenőrzési folyamat megkönnyítésére a vevő 190 chipjébe beágyazhatjuk. A legegyszerűbb esetben a vevőnek csak egyszer kell ellenőriznie a küldő letétbe helyezési 194 igazolásának hitelességét a saját beágyazott gyártói nyilvános rejtjelkulcsával vagy egész rendszerre kiterjedő bizalmas személy utasítási rejtjelkulcsával történő összehasonlítással. Ha azok adott küldőre nézve egyszer már érvényesnek bizonyultak, a vevőnek az MCH aláírást csak a küldő berendezésének előre megvizsgált nyilvános rejtjelkulcsával kell ellenőriznie, aminek eredményeképp üzenetenként csak egyetlen aláírás ellenőrzését kell végrehajtani. Ha a küldő 194 igazolása vagy a 192 MCH érvénytelen, a vevő chipje az üzenetet nem fogja megfejteni. Ezen igazo-

lások és aláírások ellenőrzése után a vevő végül a küldő MCH-ban lévő közbenső száma alapján kiszámítja az üzenet-szakaszrejtjelkulcsot, valamint a vevő nyilvános titkosító rejtjelkulcs 193 igazolásában ismertetett nyilvános rejtjelkulcsának megfelelő vevői egyéni rejtjelkulcsot. A szakaszrejtjelkulccsal a vevő megfejti a küldő felhasználó által küldött üzenetet.

A törvényes ellenőrzés általi megfejtés

Egy meghatározott felhasználótól származó, valamint a hozzá jövő üzenetek lehallgatására és megfejtésére a törvényes ellenőrzésnek bírósági felhatalmazással vagy meghatalmazással kell rendelkeznie. A bírói meghatalmazás minden valószínűség szerint tartalmaz (1) „lehallgatás kezdete" dátumot és időpontot, amelytől a törvényes ellenőrzés elkezdheti a felhasználó kommunikációjának figyelését, (2) „lehallgatás vége" dátumot és időpontot, amely után a törvényes ellenőrzés nem hallgathatja le a felhasználó kommunikációját, és valószínűleg (3) a „lehallgatás vége" dátum utáni haladékot, amely alatt a törvényes ellenőrzés megtarthatja a felhasználó egyéni rejtjelkulcsát az előzőleg lehallgatott kommunikációk megfejtésére, de ekkor törvényes ellenőrzés a felhasználó további kommunikációját már nem hallgathatja le és nem fejtheti meg. A küldő felhasználó kommunikációjának megfigyelésekor a törvényes ellenőrzés lehallgatja a kommunikációt, és az MCH-ból azonosítja a küldő fő letétbe helyezési központjának nevét és országát annak meghatározására, hogy kitől kell kérnie a küldő egyéni megfejtési rejtjelkulcsát. A törvényes ellenőrzés ezután a küldő fő letétbe helyezési központjának bemutatja a bírói meghatalmazást és a lehallgatott kommunikáció MCH-ját, amely fő letétbe helyezési központ saját egyéni rejtjelkulcsával megfejti a küldő MCH-ban lévő titkosított igazolási számát. A küldő igazolási számának segítségével a küldő fő letétbe helyezési központja megkeresi a küldő felhasználó nevét, valamint a küldő letétbe helyezési ügynökeinek neveit, és átadja azokat a törvényes ellenőrzési ügynöknek a küldő berendezésének gyártói igazolásával együtt, amelyre a törvényes ellenőrzésnek a későbbi dekódolás során lesz szüksége. A törvényes ellenőrzési ügynök ezután kapcsolatba lép a küldő letétbe helyezési ügynökeivel, bemutatja nekik a küldő nevét és a meghatalmazást, és az egyes letétbe helyezési ügynököktől megkapja a küldő által rájuk bízott rejtjelkulcsszeleteket. Mivel a titkosított kommunikációk törvényes ellenőrzés általi előnyös lehallgatási és megfejtési eljárásában a találmány szerint a következőkben ismertetésre kerülő dekóderdobozt alkalmazzuk, a törvényes ellenőrzés letétbe helyezési ügynökökhöz menő kérelme a törvényes ellenőrzés dekóderdobozán nyilvános titkosító rejtjelkulcsát is tartalmazza, és így a rejtjelkulcsszeleteket a törvényes ellenőrzési ügynökök helyett közvetlenül a törvényes ellenőrzés dekóderdobozához lehet küldeni. A letétbe helyezési ügynökök a küldő birtokukban lévő rejtjelkulcsszeleteit a törvényes ellenőrzés dekóderdoboznak titkosított üzenetként küldik el, amely üzenet rendelkezik „lehallgatás kezdete" dátummal, „lehallgatás vége" dátummal, és adott esetben „haladékkal", hogy a dekóderdoboz a meghatalmazás paramétereit ellenőrizhesse. A dekóderdoboz ezután megfejti a titkosított rejtjelkulcsszeleteket tartalmazó üzeneteket, összeállítja a rejtjelkulcsszeleteket, és a küldő összeállított egyéni rejtjelkulcsával kiszámítja a kommunikációra vonatkozó szakaszrejtjelkulcsot, amelyet a küldő az MCH-ban önmagának küldött üzenetként titkosított. A dekóderdoboz ezután csak a meghatalmazásban meghatározott lehallgatási időtartam alatt hallgathatja le a küldőhöz jövő és a tőle elmenő üzeneteket, és a lehallgatott kommunikációt csak a meghatalmazásban meghatározott haladék végéig fejtheti meg.

A vevőhöz jövő és tőle elmenő üzenetek lehallgatására hasonló eljárást alkalmazunk. A lehallgatott kommunikáció MCH-jából a törvényes ellenőrzés azonosítja a vevő fő letétbe helyezési központjának nevét és országát, majd a meghatalmazást és a lehallgatott kommunikáció MCH-ját bemutatja a vevő fő letétbe helyezési központjának, amely egyéni rejtjelkulcsával megfejti az MCH-ban lévő titkosított vevői igazolási számot. A vevő igazolási számával a vevő fő letétbe helyezési központja kikeresi a vevő, valamint a vevő letétbe helyezési ügynökeinek neveit, és azokat a törvényes ellenőrzési ügynöknek átadja. A törvényes ellenőrzési ügynök ezután kapcsolatba lép a vevő letétbe helyezési ügynökeivel és bemutatja nekik a vevő nevét, valamint a meghatalmazást. A letétbe helyezési ügynökök a törvényes ellenőrzési dekóderdoboznak a vevő által rájuk bízott rejtjelkulcsszeleteket titkosított üzenetként küldik el, amely üzenet rendelkezik „lehallgatás kezdete" dátummal, „lehallgatás vége" dátummal és „haladékkal", hogy a dekóderdoboz ellenőrizhesse a meghatalmazás paramétereit. A dekóderdoboz ezután megfejti a titkosított rejtjelkulcsszeleteket, összeállítja azokat, és a vevő kiadódó összeállított egyéni rejtjelkulcsával a küldő MCH elején lévő közbenső számával együtt kiszámítja a kommunikáció szakaszának rejtjelkulcsát. A dekóderdoboz ezután csak a meghatalmazásban meghatározott lehallgatási időtartam alatt hallgathatja le a vevőhöz jövő és a tőle elmenő üzeneteket, és csak a meghatalmazásban meghatározott haladék végéig fejtheti meg a lehallgatott kommunikációt.

A találmány egy másik kiviteli alakjában a letétbe helyezési ügynököktől a törvényes ellenőrzési dekóderdobozhoz menő, titkosított rejtjelkulcsszeletet tartalmazó üzenet formátuma a következő:

Felhasználó igazolási száma
Egyéni rejtjelkulcsszelet: X(i)
Lehallgatás kezdetének dátuma és időpontja
Lehallgatás végének dátuma és időpontja
Bíróság által jóváhagyott haladék (napok/órák)
Dátum és időpont (a rejtjelkulcsszeletet tartalmazó üzeneté)
Letétbe helyezési ügynök aláírása
[Letétbe helyezési ügynök igazolása]

Ebben a formátumban az igazolás számán kívül minden információt titkosítunk a dekóderdoboz titkosító rejtjelkulcsával. Mivel a letétbe helyezési ügynököktől jövő, rejtjelkulcsszeleteket tartalmazó üzenetek az adott dekóderdoboz számára vannak titkosítva, más fel-

használó vagy dekóderdoboz nem tudja azokat elolvasni. Ezen túlmenően a „lehallgatás kezdete" és „lehallgatás vége" dátumok és időpontok utasítják a dekóderdobozt, hogy mikor kezdje a lehallgatást és a kommunikáció dekódolását, valamint hogy mikor fejezze be a lehallgatást. A haladék járulékos időt tesz lehetővé a dekóderdoboz számára, hogy az előzőleg lehallgatott kommunikációt visszamenőleg dekódolja. A haladék letelte után a dekóderdoboznak be kell fejeznie a dekódolást és ki kell törölnie a szóban forgó egyéni rejtjelkulcsot. Így a dekóderdoboz a meghatalmazásban meghatározott dátumig használható a lehallgatott felhasználó kommunikációjának megfejtésére, ami után a dekóderdoboz és annak beépített órája megakadályozza a további megfejtést. A dekóderdoboz megtagadhatja olyan rejtjelkulcsszeleteket tartalmazó üzenetek feldolgozását, amelyeknek üzenetdátumuk és időpontjuk tizenkét óránál (vagy más meghatározott időtartamnál) régebbi, vagy amelyeknek érvényességi dátuma és ideje lejárt.

A dekóderdoboz alkalmazása

A találmány egyik előnyös kiviteli alakjában a törvényes ellenőrzés speciális, külső behatások ellen védett dekóderdobozt alkalmaz a megfigyelt felhasználók kommunikációinak meghatározott és szabályozott feltételek fennállásakor történő lehallgatásához és megfejtéséhez. A dekóderdoboz példaképpeni működését a 20. ábra mutatja. A 200 dekóderdoboz úgy van kialakítva, hogy a találmány szerinti bizalmas berendezések rendszerében azokhoz hasonló bizalmas berendezés legyen, és ezért képes különböző feltételek vizsgálatára a törvényes ellenőrzési ügynökök nem megfelelő akcióinak megakadályozására. A 200 dekóderdoboz rendelkezik a gyártó által beágyazott egyéni berendezés-aláírási rejtjelkulccsal, valamint gyártói nyilvános aláírási rejtjelkulcs 202 igazolással a nyilvános aláírási rejtjelkulcs számára, amely rejtjelkulcs megfelel a berendezés egyéni aláírási rejtjelkulcsának. A gyártói 202 igazoláson kívül a dekóderdoboz rendelkezhet a dekóderdoboz tulajdonosaként a törvényes ellenőrzési hatóság vagy vállalati biztonsági osztály által, illetve nevében kibocsátott 203 igazolással is, amely igazolja a dekóderdoboz és a törvényes ellenőrzés vagy biztonsági hatóság közötti kapcsolatot, valamint azt, hogy a dekóderdoboz az ő kizárólagos tulajdonában van, és irányítása alatt áll. A 200 dekóderdoboz rendelkezhet azzal a képességgel is, hogy a találmány szerinti általános felhasználói chipekhez hasonlóan nyilvános/egyéni rejtjelkulcspárt generáljon a dekóderdobozhoz menő adminisztrációs és vezérlőüzenetek titkosítására és megfejtésére. A 200 dekóderdoboz rendelkezik továbbá azzal a képességgel is, hogy biztonságosan eltárolja egyéni rejtjelkulcsát, és hogy a megfelelő nyilvános titkosító rejtjelkulcsot általa aláírt 201 igazolásban kibocsássa, amelyhez csatolva van a berendezés gyártó által aláírt 202 igazolása. A nyilvános/egyéni rejtjelkulcspár generálásának (és alkalmazásának) képessége egy lehallgatott felhasználó 206 letétbe helyezési ügynökei számára lehetővé teszi, hogy ha törvényes ellenőrzési ügynökök 207 fő letétbe helyezési központnak bemutatják a felhasználó kommunikációinak lehallgatására vonatkozó meghatalmazást, a dekóderdoboz nyilvános titkosító rejtjelkulcsával titkosítva elküldjék a lehallgatott felhasználó 204 rejtjelkulcsszeleteit a dekóderdoboznak, valamint lehetővé teszi a dekóderdoboz számára, hogy saját egyéni megfejtési rejtjelkulcsával a rejtjelkulcsszeleteket megfejtse. A találmány szerinti általános felhasználói chiptől eltérően azonban, amely az üzenetet megfejti és a titkosítatlan eredményt visszaadja a felhasználónak, a dekóderdoboz soha nem adja ki a törvényes ellenőrzési ügynököknek a lehallgatott felhasználó egyéni rejtjelkulcsát. Ehelyett a dekóderdoboz ezt az információt biztonságosan eltárolja a meghatalmazásban és a rejtjelkulcsszeleteket tartalmazó üzenetekben meghatározott haladék végéig, amikor is a dekóderdoboz ezt az információt végérvényesen kitörli.

Ennek megfelelően, hogy a 200 dekóderdoboz bizalmas berendezésként hajtsa végre feladatait és a lehallgatási hatóság által felállított dátum- és időpontkorlátokat betartsa, tartalmaznia kell egy bizalmas, kalibrált és hitelesített dátum/idő 205 órát. A dekóderdoboz gyártója a 205 óra érvényességét és kalibrációját akkor hitelesíti és igazolja, amikor a berendezés ismert jellemzőinek listáját tartalmazó, berendezésre vonatkozó 202 igazolást bocsát ki. Amikor a 200 dekóderdoboz a 206 letétbe helyezési ügynököktől megkapja a 204 rejtjelkulcsszeleteket, amelyek (a meghatalmazás alapján) tartalmazzák azokat az időkorlátokat, amelyek előtt és után a meghatalmazás nem érvényes, a 200 dekóderdoboz a törvényes ellenőrzés meghatalmazásának érvényességét belső 205 órájával ellenőrzi. Ha a meghatalmazás még nem érvényes, a dekóderdoboz nem fogja a lehallgatott felhasználó kommunikációit megfigyelni és megfejteni. Ha a meghatalmazás (és bármiféle alkalmazható haladék) lejár, a lehallgatott felhasználó egyéni rejtjelkulcsa kitörlődik, és a dekóderdoboz nem fogja a meghatalmazás alapján azt újra előállítani (hacsak új érvényességi idejű meghatalmazást ki nem bocsátanak). Megjegyezzük, hogy bár a bizalmas 205 óra opcionális a találmány szerinti általános felhasználói chipben, feltétlenül szükséges azonban ahhoz, hogy a 200 dekóderdoboz ellenőrizhesse a lehallgatási meghatalmazás dátum- és időkorlátait. Az általános felhasználói chip használója mindamellett közreműködhet az időkorlát ellenőrzésében azáltal, hogy chipje óráját kalibráltatja. Ha a felhasználó órája nincsen kalibrálva, a felhasználó berendezése által a kommunikáció közben generált MCH az időbélyegmezőben nulla értéket tartalmaz. Ebben az esetben a kommunikációt lehallgató dekóderdoboz csak a meghatalmazás „lehallgatás vége" dátumát tudja betartani oly módon, hogy a meghatalmazás és a haladékok lejárta után megtagadja a megfejtést. Ekkor a dekóderdoboz nem tudja betartani a „lehallgatás kezdete" dátumot, mivel addig, amíg a meghatalmazás érvényes, a meghatalmazás lehetővé teszi minden nulla értékű időbélyeggel rendelkező MCH megfejtését, még akkor is, ha azok a meghatalmazás „lehallgatás kezdete" dátum és időpont előtt kerültek lehallgatásra. Akkor azonban, ha a felhasználó órája kalibrálva van, a törvényes ellenőrzés dekóderdoboza megtagadja minden olyan MCH megfejtését, amely a lehallgatási meghatal-

mazás kezdetének dátuma és időpontja előtti érvényes és bizalmas időbélyeget tartalmaz. A találmány szerinti dekóderdoboz legelőnyösebben csak olyan kommunikációkat fejt meg, amelyeket a meghatalmazás időtartama közben megbízhatóan időbélyeggel láttak el. Feltételezhető, hogy a meghatalmazás időtartamával való, törvényes ellenőrzés általi potenciális visszaélés ezen pótlólagos akadálya arra motiválja a találmány szerinti chipek felhasználóit, hogy chipjeik kalibrált állapotban legyenek. Ha a rendszert adattároló rendszerben nagyszámú üzenet megfejtésére használjuk, a meghatalmazások vagy felfedezések későbbi rendszerezése miatt különösen kívánatos az időtartamok betartása, mivel máskülönben sok üzenet lehet kitéve nyomozásnak a törvényes rend keretein kívül.

A törvényes ellenőrzés felülvizsgálatának jellemzői

A letétbe helyezéses titkosítórendszereknél fennáll az a probléma, hogy a törvényes ellenőrzési ügynökök könnyen megvesztegethetők olyan titkosító rejtjelkulcsok megszerzésére, amelyek nagy gazdasági értékkel rendelkező adatot védenek. Egy jól megszervezett bűnszövetkezet tagjai például ellophatják egy adott vállalat értékes ipari terveit oly módon, hogy először illegálisan lehallgatják a vállalat kommunikációit abból a célból, hogy néhány üzenetfejrészt és letétbe helyezési ügynök nevét megszerezzék, ezután egy alacsonyan fizetett rendőrségi hivatalnok megvesztegetésével kábítószeres nyomozási meghatalmazást szereznek, hogy a vállalat egyéni megfejtési rejtjelkulcsát a letétbe helyezési ügynököktől megszerezzék, majd végül az egyéni megfejtési rejtjelkulccsal ellopják a terveket. Mivel a titkosítást ma már sok számítógép között folyó biztonságos kommunikációra használják, már nem elfogadható, hogy a törvényes ellenőrzés egy telekommunikációs rendszert minimális biztosítékkal hallgasson le. Sokkal erősebb biztosítékok szükségesek ahhoz, hogy a rendőrségi eljárásokat és ellenőrzéseket a modern vállalati számítógépes biztonság gyakorlatának szintjére hozzuk, és megelőzzük, hogy a fenti eset bekövetkezzen.

A bizalmas berendezés egyik ilyen biztosítéka egy belső számláló az üzenet-ellenőrző fejrészek számlálására, amely számláló értéke az egyes hozzáférések után szekvenciálisan növekszik. Az üzenet sorszáma (MSN, message sequence number) titkosítva az üzenetfejrészbe helyezhető, és így az kívülálló számára nem lesz látható. Ezt úgy valósíthatjuk meg, hogy a számot (1) a küldő üzenet-szakaszrejtjelkulcsának másolatával együtt a küldő nyilvános titkosító rejtjelkulcsával titkosítjuk, (2) vagy a küldő, illetve a vevő letétbe helyezési ügynökének nyilvános titkosító rejtjelkulcsával titkosítjuk, vagy (3) előnyösen legalább a küldő, a vevő és azok letétbe helyezési ügynökei, valamint lehetőleg minden érdekelt fél számára megfejthetően titkosítjuk. A küldő letétbe helyezési ügynöke azonban helyikihasználási okokból és a kis veszély miatt dönthet úgy, hogy megengedi a sorszámok titkosítatlan kijelzését. Az üzenet-ellenőrző fejrészek duplikált sorszámainak elkerülése kritikus fontosságú, és a lehető legnagyobb mértékben kerülendők a számozásban lévő rések is.

További biztosíték lehet, hogy a felhasználó számára az üzenet-ellenőrző fejrészben opcionális „címsor" elhelyezését tesszük lehetővé. Ha a felhasználó félne attól, hogy nem megfelelő meghatalmazásokkal illegálisan lehallgatják, egy rövid cím, például „Terv #123", kódolásával figyelmeztetheti magát és másokat az üzenet tartalmára. Adott esetben a felhasználó egyszerűen megtarthatja a berendezéshez rendelt üzenetsorszámokra és a felhasználóhoz rendelt címekre vonatkozó saját (postai szoftverrendszerhez használatos) logját. Helyikihasználási okokból azokban a valószínűleg gyakori esetekben, ha címet nem írnak be, a címsor nulla hosszúságú lesz.

Harmadik védelmi lehetőségként az üzenet-ellenőrző fejrész aláírt részéhez az üzenet tartalmának egy kivonatát adjuk annak megelőzésére, hogy a felhasználó vagy törvényes ellenőrzés később azt állítsa, hogy a megfejtett üzenet tartalma más volt, mint amit valójában küldtek. Így például a felhasználó nem tud egy előzőleg küldött, kábítószer-kereskedelemmel kapcsolatos üzenetet később ártatlan üzenettel kicserélni, vagy korrupt törvényes ellenőrzési hivatalnokok nem tudnak kábítószer-kereskedelmi vagy ártalmatlan üzenetet a hivatalnokok által lopott értékes ipari tervekkel kicserélni.

Ezek a biztosítékok járulékos biztonsági intézkedésekként alkalmazhatók. Először a küldő berendezése által generált üzenetsorszámmal a küldő a vevő, valamint a törvényes ellenőrzés és a bírósági rendszer nyomon követi az üzenetet. Bár a törvényes ellenőrzés hozzáférésének hatékony kontrollálása nehézkes lehet, különösen bűnözők üldözése közben, és bár a bírósági rendszer nem mindig képes a törvényes ellenőrzési kérelmek gondos elbírálására a lehallgatási felhatalmazások kibocsátása előtt, utólag idézés gyakorolható a lehallgatás eredményének felülvizsgálására minden lehallgatás után, a lehallgatások véletlen mintájánál vagy olyan lehallgatásoknál, amelyek valamilyen tekintetben szokatlannak bizonyulnak. A törvényes ellenőrzési ügynökök bizalmas berendezését, a dekóderdobozt ezért megváltoztatjuk úgy, hogy az tartalmazza az általa megfigyelt és a törvényes ellenőrzés számára olvashatóvá tett üzenetek üzenetsorszámainak és üzenetkivonatainak (valamint adott esetben címsorainak) biztonságos belső naplóját. A lehallgatott felhasználó letétbe helyezési ügynökei által a dekóderdobozhoz küldött, a felhasználó rejtjelkulcsszeleteit tartalmazó elektronikus felhatalmazás tartalmazhatja a meghatalmazást kibocsátó bíróság nyilvános titkosító és aláírási rejtjelkulcsait. A dekóderdoboz ezután kérés esetén képes lesz kinyomtatni az üzenetsorszámok és címsorok naplóját, lehetőleg megfelelően meghatalmazott vevő, például a meghatalmazást kibocsátó bíróság rejtjelkulcsával titkosítva.

Egy másik kiviteli alakban a dekóderdoboz addig nem kezdi meg a megfigyelt kommunikációk megfejtését, amíg nem kap olyan bírósági végzést, amely összhangban van a letétbe helyezési ügynököktől kapott rejtjelkulcsszeletekkel. A letétbe helyezési ügynököktől kapott, és a dekóderdoboz nyilvános titkosító rejtjelkulcsával titkosított, rejtjelkulcsszeleteket tartalmazó üzenetek továbbfejleszthetők például úgy, hogy (minden letétbe helyezési ügynök részéről) tartalmazzák annak a bíróságnak a nyilvános titkosító és aláírási rejtjelkulcsa-

it, amely a meghatalmazást kibocsátotta. Adott esetben a letétbe helyezési ügynökök rejtjelkulcsszeleteket tartalmazó üzeneteikben hivatkozhatnak a meghatalmazás dátumára és számára (ha van ilyen), és a dekóderdoboz a bíróságtól megkaphatja a bíróság nyilvános titkosító és aláírási rejtjelkulcsait, valamint a bíróság nyilvános rejtjelkulcs-igazolását, amelyet az eredeti lehallgatási felhatalmazáshoz csatoltak. A letétbe helyezési ügynökökhöz menő bírósági felhatalmazás továbbfejleszthető például úgy, hogy továbbítsa a következő, rejtjelkulcsszeleteket tartalmazó üzenethez szükséges adatokat:

A fő letétbe helyezési központ neve és azonosítószáma,

A lehallgatott felhasználó igazolási száma,

A bíróság neve vagy azonosítószáma,

A meghatalmazás száma (ha van ilyen),

A meghatalmazás dátuma és időpontja,

„Lehallgatás kezdete" dátum és időpont,

„Lehallgatás vége" dátum és időpont,

Maximális üzenetszám (opcionális),

[Bíró aláírása],

Bíró igazolása,

Bírót hitelesítő igazolás (például bírósági stb.).

A letétbe helyezési ügynökök ezután „újra hitelesíthetik" a bíróság dekóderdobozhoz menő nyilvános titkosító és aláírási rejtjelkulcsait azáltal, hogy a letétbe helyezési ügynököktől a dekóderdobozhoz menő, titkosított rejtjelkulcsszeleteket tartalmazó üzenetek tartalmazzák a következő járulékos információt, amelynek meg kell lennie a letétbe helyezési ügynököktől jövő mindegyik rejtjelkulcsszeletben:

A fő letétbe helyezési központ neve és azonosítószáma,

A lehallgatott felhasználó igazolási száma,

A letétbe helyezési ügynök neve vagy azonosítószáma (aki ezt a rejtjelkulcsszeletet tartalmazó üzenetet küldte),

A bíróság neve vagy azonosítószáma,

A bíróság nyilvános titkosító rejtjelkulcsa,

A bíróság nyilvános aláírási rejtjelkulcsa,

A meghatalmazás száma (ha van ilyen),

A meghatalmazás dátuma és időpontja,

Maximális üzenetszám (opcionális),

A letétbe helyezési ügynök aláírása,

[A letétbe helyezési ügynök igazolása].

A dekóderdobozt ezáltal biztosítjuk afelől, hogy mindegyik rejtjelkulcsszeletet tartalmazó üzenet ugyanattól a bírótól és meghatalmazásból származik.

Az a tény, hogy a dekóderdoboz rendelkezik a bíró nyilvános titkosító és aláírási rejtjelkulcsaival, lehetővé teszi a bíró számára, hogy (bizalmasan) kérje és megkapja a lehallgatási időtartam alatt a dekóderdoboz által lehallgatott és megfejtett üzenetek sorszámait és címsorait, mintegy a törvényes ellenőrzési ügynökök lehallgatás utáni felülvizsgálataként a nem igazságos, törvénytelen vagy korrupt magatartás elleni biztosítékként. Ezen túlmenően a dekóderdoboz addig nem töröl ki vagy használ fel újra lehallgatott üzenet naplójához rendelt memóriát, amíg a dekóderdoboz az előzőleg megkapott nyilvános aláírási rejtjelkulccsal ellenőrzött, külön erre vonatkozó parancsot nem kap a bírótól vagy a bíróságtól. Ilyen parancsot akkor adnak ki, ha a bíróság a dekóderdoboztól az előzőleg kért, lehallgatott üzenetnaplót már megkapta, vagy ha a bíróság elhatározta, hogy az adott esetben nincs szükség felülvizsgálatára. Ha a lehallgatott üzenetek naplójának memóriaterülete megtelik, a dekóderdoboz nem fejt meg további üzeneteket, amíg a naplót el nem küldte a bíróhoz vagy bírósághoz, és a bíróság által aláírt, a dekóderdoboznak a lehallgatott üzenetek naplójának törlését megengedő parancs nem érkezik. A törvényes ellenőrzés folytathatja az új üzenetek lehallgatását a lehallgatott üzenetek naplójának törlése előtt, de az új üzenetek nem kerülnek megfejtésre, amíg a teljes üzenetnapló felülvizsgálatra nem került. A dekóderdoboz rendelkezik azzal a képességgel is, hogy a törvényes ellenőrzést figyelmezteti, ha a lehallgatott üzenetnapló majdnem megtelt, és így a törvényes ellenőrzés kérheti az üzenet-felülvizsgálati napló felküldését, hogy a dekóderdoboz ne hagyja abba a megfejtést. Ezek a tranzakciók és kommunikációk teljesen automatizálhatók, és közel pillanatszerűen folyhatnak.

A felülvizsgálati napló bejegyzései az üzenetkivonatán kívül tartalmazhatnak egy második kivonatot, amelyet (a) az üzenetkivonat és (b) az előző naplóbejegyzés teljes szövege egymáshoz csatolásával és újrakivonatolásával kapunk. Ez megakadályozhatja, hogy tisztességtelen bírósági személyzet a naplóba bejegyzéseket vezessen be, töröljön ki vagy sorszámozzon újra. Ezt a koncepciót az US 5 136 646 és US 5 136 647 szabadalmi leírásokban ismertették.

A bíróság később utótagos ellenőrzésként kérheti a törvényes ellenőrzést, hogy közölje a bíróság által megkapott felülvizsgálati naplóban lévő üzenetfejrészeket és az üzenetkivonatok teljes szövegét. A bíróság lehallgatási felhatalmazásában mesterségesen a lehetségesnél kevesebbre is korlátozhatja az üzenetnapló kapacitását, vagyis a lehallgatott üzenetek azon számát, amelyeket a dekóderdoboz megfejthet, mielőtt a lehallgatott üzenetek naplóját és az üzenetfejrészeket felül kellene vizsgálni. Az ilyen típusú korlátozásnak nincs hatása a törvényes ellenőrzés nyomozási képességére, mivel a napló bírósághoz történő, felülvizsgálat céljára szolgáló letöltése majdnem pillanatszerűen történik, de figyelmeztetheti a bíróságot a szokatlan körülményekre. Olyan meghatározott esetekben, amelyek szigorúbb szabályozást igényelnek, mint pusztán a lehallgatott üzenetnapló bírósághoz történő elküldését, a bíróság a teljesnél kevesebbre korlátozhatja a törvényes ellenőrzés üzenetnaplójának azon kapacitását, amelynek elérése előtt a törvényes ellenőrzésnek új meghatalmazást kell kérnie a további kommunikációk lehallgatására.

Ezáltal ha (1) mind a küldő, mind a vevő nyomon követik az általuk adott és vett üzenetek sorszámait, és vagy címsorokat rendelnek az üzenet-ellenőrző fejrészekhez, vagy helyi szoftverrendszereikben naplózzák az üzeneteket, és ha (2) mind a törvényes ellenőrzés, mind a bíróság rendelkezik a törvényes ellenőrzés által megfejtett üzenetek teljes naplójával, valamint ha (3) minden üzenetfejrész tartalmaz üzenetkivonatot, amely

megakadályozza, hogy valamelyik fél később megváltoztassa az üzenetet tetteinek elleplezésére, akkor egy lehallgatás utáni hiteles felülvizsgálat megállapíthatja, hogy történt-e visszaélés vagy korrupt cselekmény a törvényes ellenőrzési ügynökség részéről. Bár a rendszer a priori nem tudja megakadályozni az ellopott terv fent említett esetét, a bűnszövetkezet azon tudata, hogy tetteik a bíróság vagy a szóban forgó felhasználó által teljes mértékben felülvizsgálhatók, a jogellenes rendőrségi cselekmények lényeges korlátozását eredményezi. Azt is szabályozhatjuk, hogy a törvényes ellenőrzési ügynökség jegyezzen fel és mutasson be a bíróságnak a meghatalmazással lehallgatott minden üzenetet, és lehetővé tehetjük a lehallgatott feleknek, hogy lehallgatási felülvizsgálatot kérjenek, különösen ahol üzleti vállalkozásról van szó, és a lehallgatás alapján nem emelnek bűnvádat.

Folyamirányított adat

Folyamirányított adatokat tartalmazó kommunikációkban, például telefonhívásokban, ahol az egyes kommunikációk kettő vagy több felhasználótól származó nagyszámú üzenetcsomag folyamából állnak, nem lehetséges, hogy a küldőberendezés az MCH részeként kivonatolja és aláírja a teljes üzenetet. Bár fennáll a lehetősége annak, hogy minden kommunikációs csomaggal egy MCH-t küldjünk, de ez nagyon költséges lenne a feldolgozási időt és a hálózat sávszélességét illetően. Az MCH-t ezért csak egyszer kellene átvinni, méghozzá a hívás létrejöttekor. A titkosított adat folyamatos folyamait előnyösen úgy kezeljük, hogy a hívó felhasználót kinevezzük „küldőnek", és a kommunikáció kezdetén a korábbiakhoz hasonlóan létrehozzuk az MCH-t, amely tartalmazza az üzenet sorszámát (MSN) és az első csomag berendezés által aláírt kivonatát (ha van ilyen). A küldő berendezése ezután egyedi csomagsorszámból (PSN, packet sequence number) álló sorozatot generál, amely minden kommunikáció elején 0-tól kezdődik. A soron következő csomagok esetén a berendezésnek csak a meghatározott csomagot kell kivonatolnia és aláírnia, és a csomaghoz csatolnia kell a kivonatot (és alá kell írnia), az MSN-t (amely ugyanaz az egész üzenet során), valamint a PSN-t. A hívott hasonló műveleteket végez az egyes csomagokkal, vagyis hivatkozik a hívó kommunikációjának MSN-jére, 0-tól kezdődően sorban számozza csomagjait, és a hívott berendezésével aláíratja csomagkivonatból, a hívott MSN-jéből és a hívó PSN-jéből álló csoportot, amivel egy „csomag ellenőrző fejrészt" (PCH, packet control header) hoz létre. A berendezések opcionálisan beilleszthetik a kommunikáció kezdete óta eltelt aktuális időt (másodpercben vagy tizedmásodpercben), amely az előzőekben ismertetett MCH változatokban már megtalálható. Ez lehetővé teszi hívás valósághűbb visszaadását.

Azért, hogy a kommunikáció után megkülönböztethessük a hívó és a hívott csomagjait, kívánatos, hogy egyszerű kódolási rendszerű hívási résztvevő kódot (CPC, call party code) hozzunk létre, amely rendszerben számokat rendelünk a kommunikáció résztvevőihez, például hívó=0, hívott=1, és ugyanazon titkosított szakasz további résztvevői nagyobb számokat kapnak. Adott esetben a CPC helyett használható egyedi azonosítószám, például a berendezés sorszáma, a berendezés sorszáma plusz a berendezés gyártójának azonosítószáma, vagy a megelőző kivonat.

Ezek az eljárások általánosíthatók többrésztvevős szakaszrejtjelkulcs-generálási eljárásként is. Egy hívó például szakaszrejtjelkulcsot generálhat, és ugyanazzal a rejtjelkulccsal RSA rejtjelkulcs átvitelt alkalmazva több hívottal egyidejűleg kezdeményezhet hívásokat. Ekkor az első két résztvevő (hívó és hívott) után minden fél számára külön MCH-t alakítunk ki. A hívó berendezése a többrésztvevős hívást kezelheti különálló hívásokként vagy ugyanazon szakaszrejtjelkulccsal, de többszörös CPC-vel rendelkező egyszeri hívásként. Ekkor a hívók felelősek azért, hogy a hívó MSN-jét használják, és hogy létrehozzák saját CPC és PSN számaikat. Adott esetben, általános kétrésztvevős szakaszrejtjelkulcs-generálási eljárások (például Diffie–Hellman-eljárások) alkalmazását feltételezve, olyan konferenciahívások alakíthatók ki, amelyekben egy központi fél (például rendszeroperátor) létrehozza a hívásokat és a résztvevők csomagjait a többi résztvevő számára valós időben megfejti és újratitkosítja. A központi résztvevő lehet az a személy is, aki a következő hívott féllel történő összekapcsolást végzi, amikor is a hívott fél csomagjait a központi résztvevő berendezése megfejti, majd a hívott fél által más résztvevőkkel való kommunikálásra használt szakaszrejtjelkulccsal (rejtjelkulcsokkal) újratitkosítja. Ezt ismertetik B. Schneider Alkalmazott titkosítás (J. Wiley 1994., 276. oldal) c. írásában, ahol a Diffie–Hellman-módszert három vagy több fél esetére alkalmazzák.

A csomag-ellenőrző fejrész a következőképpen alakítható ki:

Az eredeti hívó MSN-je,

A felhasználó hívási résztvevő kódja (CPC) (hívó=0 stb.),

Felhasználói csomag sorszáma (PSN),

Hívás kezdete óta eltelt idő (ms),

Kivonat (a csomagé),

[Berendezés aláírása].

A kommunikáció minden egyes csomagjával előnyösen nem küldünk PCH-t, mert ez a rövid csomagokat alkalmazó rendszerekben túlzsúfoltságot eredményezhet, hanem a PCH-t csak periodikusan küldjük. Ez rokon a hálózati kommunikáció ismert „csúszóablakos" technikájával, ahol a csomagküldési szekvencia és a csomag újbóli elküldése nem az egyes csomagokra, hanem nagyszámú csomagra hajtódik végre. Az ilyen rendszerek általában az átviteli vonal zaja alapján dinamikusan hangolják az „ablakot", vagyis a hibavizsgálatok között küldött csomagok számát, amikor is az ablak nagy lesz tiszta vonal esetén, de kicsi a sok újraküldést okozó zajos vonal esetén. Ha gyakran lép fel hiba, a kis ablakméret miatt a felhasználónak csak kis mennyiségű adatot kell újból elküldenie; ha viszont ritkán történik hiba, a vizsgálat is ritkábban végezhető, amikor azonban hiba esetén az elveszett adat nagy költséggel küldhető el újra. A csomagellenőrző fejrészeket közvetlenül a kommunikációs rendszer csúszóablakos rendszerébe lehet integrálni, ami által csomag szinten elérjük a ki-

ván kapacitást a törvényes ellenőrzési akciók felülvizsgálására, mialatt a modern kommunikációs hálózatokban maximális rendszerátvitelt teszünk lehetővé.

A lehallgatási folyamat felülvizsgálhatóságának további szigorítására a kommunikáció szakaszának végét előnyösen speciális csomaggal jelöljük meg. Ezt a csomagot e berendezések a szétkapcsolás előtt a felhasználók tudta nélkül a többi berendezés felé küldjük annak megakadályozására, hogy a felhasználók vagy a törvényes ellenőrzési ügynökök később azt állítsák, hogy a kommunikáció befejeződött, illetve nem fejeződött be, amikor valójában annak az ellentéte történt meg. Ezt úgy valósíthatjuk meg, hogy a berendezéseket a felhasználótól jövő „be akarom fejezni" parancs elfogadására utasítjuk, amelyre válaszul a berendezés „készülj a szétkapcsolásra" csomagot küld, ami azután a másik berendezés(eke)t is erre készteti. A berendezések) adatfolyamaikat egy „végső" csomaggal zárják, amely nem tartalmaz újabb adatot, azonban előnyösen tartalmazza az összes küldött és vett csomag számát, a hívás időtartamát stb.

Időbélyegző berendezés

A találmány előnyös kiviteli alakjának további jellemzője, hogy – amint azt a fentiekben a dekóderdoboz kapcsán kifejtettük – tartalmaz bizalmas és külső beavatkozásokkal szemben védett időbélyegző berendezést, amely önmagát hitelesítve digitálisan aláírt, harmadik fél által megbízhatónak tekinthető időbélyegeket (vagy ilyen időbélyegeket tartalmazó adatstruktúrákat) bocsát ki vagy csatol. Ilyen időbélyeg-berendezéseket ismertetnek az US 5 001 752 és US 5 136 643 számú szabadalmi leírásokban. A 21. ábrán látható 210 időbélyegző berendezés (vagy alrendszer) előnyös kiviteli alakját csak bizalmas hatóság, például a gyártó vagy a gyártó megbízottja kalibrálhatja és helyezheti üzembe oly módon, ahogyan postai mérleget is csak az Egyesült Államok Postaszolgálatának helyi fiókja állíthat be, ami után azt a társadalom megbízhatónak tekinti, és a postai rendszer csak az előre fizetett összegért fog postai mérleg bélyegeket felszámítani. A kalibrálás után a 210 időbélyegző berendezés (vagy alrendszer) „időállítás" 211 utasításra (vagy újrakalibrálásra) csak akkor fog reagálni, ha az utasítást a gyártó, a gyártótól származó 212 igazolást csatoló személy vagy a gyártó megbízottja aláírta, amely aláírás igazolja, hogy a személy meg van bízva a gazdaberendezés 210 időbélyegző berendezésének (vagy alrendszerének) állítására vagy kalibrálására. Az időállító 211 utasítást személyesen a berendezést fizikálisan birtokló időállító hatóságnak kell végrehajtania, és az időállító 211 utasítást azonnal ki kell törölnie annak megakadályozására, hogy a berendezés tulajdonosa megtudja az utasítást, és azt későbbi időpontban a berendezés órájának visszaállítására újból kiadja.

A kalibrálás után a 210 időbélyegző berendezés – amíg meg nem zavarják – belső óramechanizmusa alapján 213 időbélyegeket vagy strukturált adatmezőkben lévő komplett időbélyegadatot szolgáltat, a kiadódó adtstrukturákat egyéni berendezés rejtjelkulcsával 214 aláírja, és ellátja gyártójának 215 igazolásával. Ha a gazdaberendezésnek elmegy a tápfeszültsége, megbolygatják vagy deaktiválási utasítást kap, az időbélyegek kibocsátását abbahagyja. Azért, hogy elkerüljük más, valószínűleg hasznos, bizalmas időbélyegeket nem feltétlenül kívánó funkciók elrontását, az időbélyegző berendezés azt a szabályt alkalmazza, hogy egy előre meghatározott, „nulla" értékkel tölti fel az időbélyegmezőt, amely lehet csupa bináris nulla vagy bináris egy (vagy ezzel ekvivalens szabály), amikor egy strukturált adatmező időbélyeg beírását kéri. Amikor azonban egy strukturált adatmező vagy a gazdaberendezés aktuális időbélyeg kibocsátását kéri, ahogy például törvényes ellenőrzési dekóderdoboz esetében is történik, ha az időbélyegző berendezés abbahagyta az időbélyegek kibocsátását, a gazdaberendezés időbélyeget igénylő funkciói nem működnek, dekóderdoboz esetében például a doboz megtagadja a lehallgatott kommunikáció megfejtését. Azért, hogy elkerüljük vagy minimalizáljuk a gazdaberendezés tápfeszültségének megszűnését, a bizalmas időbélyegző berendezések előnyösen el vannak látva saját különálló, hosszú életű, kizárólag az óra által használt 216 elemmel, „alacsony elemfeszültség" jelzéssel az időbélyegző készülék tápjának az elem kicserélése előtti megszűnésének megakadályozására, valamint az elemcsere alatt megfelelő villamos töltést biztosító eszközzel (például kondenzátorral, második elemházzal vagy opcionális külső tápellátással).

Az időbélyegző berendezés által kibocsátott minden időbélyeghez tartozhat egy gyártó (vagy más időállító hatóság) által kibocsátott időbélyegzőberendezés-igazolás, amely igazolja az időbélyegző óra minőségét és bizalmasságát, az utolsó állítási időt, valamint az idő várható eltolódását. Amikor egy vevő felhasználó a gazdaberendezés által digitálisan aláírt adatstruktúrát kap, érvényes értéket tartalmazó időbélyegmező esetén tudni fogja, hogy az idő a berendezés aláírásával és igazolásával igazoltan hibátlan volt az adatstruktúra létrehozásakor, aláírásakor és kibocsátásakor. Ez az igazolás (1) az időbélyegző órát legutóbb kalibrált hatóság megbízhatóságán, (2) a gyártó által a berendezésigazolásban állított óraeltolódás tűrésén, és (3) az óra azon képességén alapszik, hogy bolygatás vagy tápellátás megszűnése esetén deaktiválja magát. A vevő továbbá tudja azt, hogy ha az időbélyegmező „nulla" értéket tartalmaz, az időbélyegző órája az adatstruktúra berendezés általi létrehozásának, aláírásának és kibocsátásának idején nem volt megbízhatóan kalibrált állapotban. Ezt az információt, amely az időbélyegző berendezésnek, valamint belső óramechanizmusának bizalmassági jellemzőire vonatkozik, előnyösen megfelelő minőség-érték kódolási rendszerrel közvetlenül a berendezés igazolásába kódolhatjuk. Ez az információ azonban következhet a gyártó nevéből és a berendezés típusából is, amelyeket a gyártó a berendezési igazolás kibocsátásával egyidőben az „irányelvi állásfoglalás" részeként a specifikációban és teljesítményigazolásban közzétesz.

Ilyen időbélyegeket a berendezés az MCH-létrehozási és dekódolási műveleteken kívüli üzenetkezelési műveletek részeként is kibocsáthat. Ezek az időbélyegek a berendezés felhasználójának személyes aláírása

mellé csatolhatók, amikor a felhasználó a berendezésben biztonságosan elhelyezett saját aláírási rejtjelkulcsával más dokumentumot vagy tranzakciót ír alá. A berendezés aláírja, illetve társaláíróként aláírja a felhasználó aláírásának időbélyegelemét, vagy adott esetben aláírja a felhasználó teljes aláírási blokkját (amely tartalmazza a felhasználó által aláírt időbélyeget és a dokumentum kivonatolási eredményét). A berendezés ezután csatolhatja igazolását, hogy az időbélyeget hihetővé és hitelessé tegye a gyártó nyilvános rejtjelkulcsát ismerő harmadik fél számára.

Bizalmas frissítés, csere és új rejtjelkulcs bevezetése

A találmány további jellemzője olyan külső behatás ellen védett bizalmas berendezés, amely beágyazva tartalmaz gyártói nyilvános rejtjelkulcsot, védett, nem felejtő memóriaterületet és biztonságos központi processzort (CPU, central processor unit), és amely a gyártó által beágyazott firmware-t bizalmas módon képes frissíteni vagy kiegészíteni. A bizalmas berendezés a frissítést vagy kiegészítést olyan adatblokkinput átvételével végzi, amely az adott típusú berendezésnek megfelelő, a gyártó aláírásával digitálisan aláírt új vagy kiegészítő firmware-kódot tartalmaz, amely aláírás biztosítja a berendezést afelől, hogy az új firmware-kódot a gyártó fejlesztette, tesztelte és hagyta jóvá, valamint hogy a berendezésnek ezért (a) egy vagy több pillanatnyilag beágyazott firmware-rutint az új firmware-kóddal felül kell írnia, vagy (b) az új firmware-kódot egy vagy több új rutinként a védett memória pillanatnyilag nem használt területén el kell helyeznie. Az előnyös kiviteli alakban a védett memória FLASH típusú, amely tápellátás nélkül végtelen ideig megtartja a benne tárolt információt, amelyet azonban a berendezés kívánság szerint (viszonylag lassan) ki is törölhet és ismét felhasználhat. A védett memória tartalmazhat továbbá bármiféle külső behatások ellen védett vagy nem védett adattároló területet (például lemezmeghajtót), amelyben a frissítendő vagy kiegészítendő kód titkosított formában tárolható, és amelynek megfejtési rejtjelkulcsát csak a bizalmas berendezés ismeri. A programok titkosított formában való tárolásával a berendezés hatékonyan megakadályozza, hogy azokat a megfejtési rejtjelkulcs ismerete nélkül bárki módosítsa. Amikor a berendezés ilyen új firmware- (vagy szoftver-) kódot tartalmazó, aláírt blokkot kap, a felhasználó a kódot a gyártó aláírásával együtt betáplálja, és a berendezésnek „firmware-frissítés" utasítást ad. A berendezés ezután a gyártó aláírását a gyártó gyártás alatt berendezésbe ágyazott nyilvános aláírási rejtjelkulcsával ellenőrzi. Ha a gyártó aláírása megfelelő, a kód elfogadásra kerül, és a berendezés végrehajtja a kívánt frissítést.

A bizalmas berendezés firmware-ének fent leírt bizalmas frissítése kiegészíthető továbbá oly módon, hogy helyet adjon meghatalmazott harmadik feleknek, akik a velük kapcsolatos berendezésfunkciókra vonatkozó firmware-rutinokat frissíteni kívánják, amilyen funkció például a pillanatnyi rejtjelkulcs-letétbehelyezési rendszer is, amelyet a bizalmas berendezés gyártójától függetlenül nagyobbrészt egy banki fő letétbe helyezési központ alakíthat ki és adminisztrálhat. Harmadik fél által történő frissítéskor a gyártó a firmware-t szolgáltató harmadik fél nyilvános rejtjelkulcsát tartalmazó firmware-frissítési igazolást ír alá, és azt a harmadik félnek kibocsátja. A harmadik fél ezután a firmware-rutinokat kifejleszti, leteszteli, jóváhagyja azok kicserélését vagy kiegészítését, aláírja azokat a harmadik fél egyéni aláírási rejtjelkulcsával, valamint csatolja a gyártótól származó frissítési igazolást. Ilyen frissítés átvételekor a felhasználó a berendezésbe betölti az aláírt szoftverkódrutinokat és a gyártó frissítési igazolását, majd ezután kibocsát egy „harmadik fél firmware-frissítésének végrehajtása" utasítást. A berendezés ezután a harmadik fél új szoftverkódrutinokon lévő aláírását a gyártó frissítési igazolásával ellenőrzi, majd ellenőrzi a frissítési igazolást a gyártó nyilvános aláírási rejtjelkulcsával, amelyet a gyártás alatt a berendezésbe ágyaztak. Ha mindkét aláírás rendben van, a frissítés elfogadásra kerül, és a berendezés végrehajtja a kívánt frissítést.

Azon túlmenően, hogy a külső behatások ellen védett berendezés elfogadja a berendezés firmwarerutinjainak frissítésére vagy kiegészítésére vonatkozó utasításokat, elfogadja a gyártás alatt beágyazott „utasítási" rejtjelkulcsok cseréjére vagy kiegészítésére szolgáló utasításokat is. Amint azt korábban ismertettük, a bizalmas berendezés a gyártó gyártáskor beágyazott rejtjelkulcsain kívül is rendelkezhet nyilvános rejtjelkulcsokkal. Az ilyen „utasítási" nyilvános rejtjelkulcsok között a találmány ismertetésében leírtak szerint lehetnek egy vagy több fő letétbe helyezési központ rejtjelkulcsai is. Ezek a beágyazott rejtjelkulcsok, beleértve a gyártó vagy más bizalmas harmadik fél rejtjelkulcsait is, különféle igazolások, például letétbe helyezési igazolások, berendezés igazolások, frissítési igazolások, időállítóutasítás-igazolások, valamint a berendezésnek adott egyéb végrehajtandó utasítások ellenőrzésére használhatók. A berendezés ezen túlmenően nemcsak a gyártás alatt beágyazott nyilvános rejtjelkulcsokra hagyatkozik, hanem elfogadhat olyan külső utasításokat, amelyek új nyilvános rejtjelkulcsok beágyazására vagy a meglévők cseréjére vonatkoznak. Abból a célból, hogy a berendezés egy bizalmas harmadik fél nyilvános aláírási rejtjelkulcsát elfogadja és nem nyilvános területen eltárolja, a gyártó az új nyilvános rejtjelkulcsot egy általa aláírt utasítási adatcsomagba (vagy igazolásba) helyezi, amelyben arra utasítja a berendezést, hogy dobja el a körülvevő igazolást, és tárolja el az abban lévő, megnevezett nyilvános utasítási rejtjelkulcsot. A speciális csomag arra is utasíthatja a berendezést, hogy milyen típusú tranzakciókra van az új rejtjelkulcs megbízva (például rejtjelkulcs-letétbehelyezési műveletnél, személygépkocsi bérlésénél, orvosi adatokkal kapcsolatos alkalmazásnál, vagy más alkalmazásoknál). Amikor a berendezés ilyen, nyilvános rejtjelkulcsot tartalmazó adatcsomagot kap a gyártótól, a berendezés először ellenőrzi a gyártó aláírását, majd azután az új nyilvános rejtjelkulcsot annak korlátozásaival együtt elfogadja és eltárolja.

A gyártó a gyártáskor vagy utasítási adatcsomag részeként történő későbbi beágyazáskor megnevezheti egy harmadik fél nyilvános utasítási rejtjelkulcsát is, amely jóváhagyja a gyártó saját benn lévő nyilvános aláírás-ellenőrzési rejtjelkulcsának cseréjére vonatkozó

tranzakciókat. Bár a gyártó saját nyilvános aláírási rejtjelkulcsának cseréjére szinte soha nincsen szükség, megvan annak a lehetősége, hogy a gyártó megfelelő egyéni aláírási rejtjelkulcsát (amely berendezésigazolások és egyéb berendezésnek szóló utasítások kibocsátására szolgál) ellopják. A gyártó egyéni aláírási rejtjelkulcsának ellopásával a tolvajnak lehetősége nyílik arra, hogy látszólag érvényes utasításokat adjon ki új (kétséges megbízhatóságú) letétbe helyezési központok és új időállító hatóságok jóváhagyására. Előfordulhat az a valószínűbb eset is, hogy a gyártó egyéni aláírási rejtjelkulcsa egyszerűen elveszik vagy megsemmisül, amivel lehetetlenné válik további érvényes utasítások kibocsátása. A számítástechnikai rendszerek viszonylatában ezen események bármelyike „katasztrófának" számít, és a gyártó összes berendezésének visszavonásához vezethet. A találmánnyal azonban egy ilyen visszavonás költsége megelőzhető vagy csökkenthető azáltal, hogy harmadik fél számára lehetővé tesszük a gyártó kompromittált aláírási rejtjelkulcsának kicserélését. Ha a gyártó a gyártás során, vagy később az utasítási adatcsomaggal egy vagy több bizalmas harmadik fél utasítási rejtjelkulcsait beágyazta, és a harmadik fél nyilvános utasítási rejtjelkulcsa által jóváhagyható tranzakciók közé saját nyilvános rejtjelkulcsának kicserélését is felvette, a gyártó a harmadik félhez fordulhat azzal a kéréssel, hogy a gyártó minden berendezéséhez bocsásson ki a gyártó nyilvános aláírási rejtjelkulcsának cseréjét eredményező utasítási adatcsomagot, ami által megvédi magát és felhasználóit a berendezések fizikai cseréjének feltételezhetően óriási költségétől. Ekkor a gyártó által kibocsátott berendezésigazolásokat is ki kell cserélni, amit úgy bonyolíthatunk le, hogy minden berendezéssel kibocsáttatunk egy kérelmet a berendezés saját nyilvános berendezés-aláírási rejtjelkulcsára vonatkozó igazoláshoz. Ha a gyártó egyéni rejtjelkulcsa elvész vagy megsemmisül, és nem kompromittálódik, akkor minden megelőző aláírás érvényes marad, amikor is a felhasználónak csak be kell mutatnia régi berendezésigazolását, hogy új berendezésigazolást bocsáttasson ki ugyanarra a gyártó új aláírási rejtjelkulcsával aláírt információra. A gyártó ezután új berendezésigazolásokat juttat vissza (leginkább online vagy elektronikus postai tranzakció keretében). Bár még ez is drága, mégis sokkal olcsóbb és kevésbé árt a gyártó elismertségének, mint a gyártó terepen lévő bizalmas berendezéseinek teljes fizikai cseréje.

A gyártó nyilvános rejtjelkulcsa vagy bármilyen más bizalmas, nyilvános utasítási rejtjelkulcs kicserélésére vonatkozó mechanizmus találmány szerinti berendezésben történő megjelenése csökkentheti a rendszer azon biztonságossági veszélyeit, amelyeket az egész rendszerre kiterjedő nyilvános rejtjelkulcsok használata jelent. Ez nagyobb megbízhatóságot tesz lehetővé a tisztán hierarchikus bizalmassági modellek számára, amelyek általánosan kevesebb igazolást igénylő, rövidebb és egyszerűbb igazolási utakat, a felhasználandó igazolások meghatározásához kevesebb erőfeszítést, valamint az aláírások ellenőrzésére kevesebb számítási időt igényelnek.

Új rejtjelkulcs tulajdonos által vezérelt bevezetése

Amint azt a korábbiakban ismertettük, a felhasználó rendelkezik azzal a lehetőséggel, hogy új rejtjelkulccsal lássa el a berendezését, vagyis hogy a felhasználó titkosítórejtjelkulcs-párját a gyártás után bármikor megváltoztassa. Ennek végrehajtásához a felhasználó a bizalmas berendezésnek arra vonatkozó firmware-utasítást bocsát ki, hogy az hajtsa végre a rejtjelkulcs-letétbehelyezési eljárás meghatározott műveleteit, vagyis generáljon új egyéni és nyilvános titkosítórejtjelkulcs-párt, küldje el a rejtjelkulcsszeleteket a letétbe helyezési ügynököknek, és végül vegyen át a fő letétbe helyezési központtól egy új letétbe helyezési igazolást. Az is kívánatos, hogy a felhasználó alkalmazója, illetve szponzora (vagy tulajdonosa, ha a felhasználó egy másik berendezés vagy folyamat) ellenőrzése alatt tartsa a rejtjelkulccsal kapcsolatos folyamatokat, valamint az új rejtjelkulcs bevezetésének folyamatát, hogy (a) biztos legyen abban, hogy a felhasználó az alkalmazó által elfogadhatónak vélt letétbe helyezési ügynököket választ, és (b) hogy biztosítva legyen, hogy az alkalmazó a berendezés valódi tulajdonosaként ismert marad a választott letétbe helyezési ügynökök számára, és ezért a letétbe helyezési ügynököktől felhatalmazás vagy bírósági végzés nélkül kérheti a felhasználó rejtjelkulcsának szeleteit. Az alkalmazó sokféle okból igényelheti, hogy meghatározott berendezés rejtjelkulcsaihoz hozzáférjen, például belső felmérést végez, vagy tulajdonában lévő titkosított adatot állít vissza, miután a megfelelő berendezés elveszett, megsemmisült, vagy azt ellopták. Az alkalmazónak számos okból szükséges lehet a berendezés új rejtjelkulccsal történő ellátása is, például ha a berendezés előző titkosító vagy aláírási rejtjelkulcsai kompromittálódtak vagy kitörlődtek, ha a berendezés másik alkalmazotthoz kerül, vagy ha a berendezés tulajdonosi szervezete stratégiai okokból periodikus időnként minden titkosítóberendezést új rejtjelkulccsal lát el.

Az előnyös kiviteli alakban a bizalmas berendezést a gyártó előzőleg úgy állítja be, hogy az nem fog rejtjelkulcs-előállítási és letétbe helyezési folyamatot kezdeményezni, amíg a berendezés 22. ábrán látható, berendezésre vonatkozó tulajdonosi 220 igazolást nem kap, amely igazolás tartalmazza a meghatározott berendezés állandó 221 sorszámát, és amely a gyártó által 225 aláírással alá van írva. A tulajdonosi 220 igazolás, amelyet a gyártó a berendezés vállalati vásárlójának az átadásakor bocsát ki, tartalmazza a vállalat 222 nevét, a vállalat egyedi 223 azonosítószámát (például a belső jövedelmi alkalmazói azonosítószámot (EIN, Internal Revenue Service Employer Identification Number) vagy a Dun & Bradstreet számot (DUNS, Dun & Bradstreet Number)), valamint a vállalat nyilvános aláírásellenőrzési 224 rejtjelkulcsát, amely megfelel a vállalat tulajdonában lévő egyéni aláírási rejtjelkulcsnak, és amellyel a vállalat a berendezésnek adott új rejtjelkulcs bevezetésére vonatkozó vagy más utasításokat ellenőrzi. Az információ átvétele után a berendezés csak olyan új rejtjelkulcs bevezetésére vonatkozó vagy más utasításra fog reagálni, amely a vállalati tulajdonosnak a berendezés tulajdonosi igazolásában lévő nyilvános rejtjel-

kulcsnak megfelelő egyéni aláírási rejtjelkulcsával van aláírva.

A 23. ábrát tekintve, ha az alkalmazó (a berendezés tulajdonosa) a 230 berendezést új rejtjelkulccsal akarja ellátni, a 230 berendezésnek aláírt 231 utasítást bocsát ki, amely tartalmazza (1) a berendezés 232 sorszámát, az egyedi 233 azonosítószámot, (2) a letétbe helyezési ügynökök 235 neveit, a fő letétbe helyezési központ 234 nevét, (3) az új rejtjelkulcs bevezetésére vonatkozó utasítás dátumát és idejét, (4) az új rejtjelkulcs bevezetésére vonatkozó utasítás lejáratának 236 dátumát és idejét, valamint (5) az új rejtjelkulcs bevezetésére vonatkozó utasítás egyedi 237 sorszámát, és aláírja az utasítást az alkalmazó egyéni aláírási 238 rejtjelkulcsával. Érvényes tulajdonosi 239 igazolás és új rejtjelkulcs bevezetésére vonatkozó érvényes 231 utasítás átvételekor a bizalmas 230 berendezésben lévő chip először ellenőrzi a gyártó aláírását a tulajdonosi 239 igazoláson, és az alkalmazó aláírását az új rejtjelkulcs bevezetésére vonatkozó 231 utasításon. Ezután a bizalmas 230 berendezés a korábbiak szerint végrehajtja a rejtjelkulcs-generálási és letétbe helyezési folyamatot, ahol is minden letétbe helyezési részcsomag tartalmazza a tulajdonos egyedi 233 azonosítószámát, és a részcsomagokat csak azoknak a 235 letétbe helyezési ügynököknek küldi el, amelyeket az alkalmazó az új rejtjelkulcs bevezetésére vonatkozó 231 utasításban megnevezett. Ezen (elektronikusan kiadható) utasítások megismétlésének megakadályozására a berendezést úgy alakítjuk ki, hogy a berendezés nem felejtő memóriában eltárolja a legutóbb vett néhány új rejtjelkulcs bevezetésére vonatkozó utasítás sorszámát, és megtagadja az utasítások újbóli végrehajtását. Ha a berendezés órája megfelelően rendben van tartva, az új rejtjelkulcs bevezetésére vonatkozó utasítások megismétlését úgy is korlátozhatjuk, hogy a berendezés óráját az utasítások lejárati dátumának és idejének figyelésére utasítjuk. Egy előnyös kiviteli alakban a kalibrálatlan órával rendelkező berendezés megtagadja az olyan rejtjelkulcs-bevezetési utasítás végrehajtását, amelynél a lejárati dátum/idő nem nulla, nulla lejárati dátum/idő esetén azonban végrehajtja azokat.

Amikor a letétbe helyezési ügynökök és a fő letétbe helyezési központ egy felhasználói berendezéstől megkapják a rejtjelkulcs (vagy új rejtjelkulcs) szeletének egyedi tulajdonosi azonosítószámot tartalmazó részcsomagjait, a letétbe helyezési ügynökök és a fő letétbe helyezési központ az egyedi azonosítószámot felveszik megfelelő adatbázisaikba, majd a tulajdonostól átveszik az egyéni titkosító rejtjelkulcshoz való hozzáférést célzó kérelmezést. Egy előnyös kiviteli alakban a letétbe helyezési ügynökök és a letétbe helyezési központ igényli, hogy az egyedi tulajdonosi azonosítószámot megjelölő rejtjelkulcsszeletet tartalmazó részcsomagot kísérje gyártó által aláírt megfelelő berendezéstulajdonosi igazolás. Ez a berendezéstulajdonosi igazolás lehetővé teszi a letétbe helyezési ügynökök és a fő letétbe helyezési központ számára, hogy válaszoljanak olyan rejtjelkulcskérelmi üzenetek vételére, amelyek a tulajdonos berendezéstulajdonosi igazolásában lévő nyilvános rejtjelkulcsának megfelelő egyéni aláírási rejtjelkulcsával vannak aláírva.

Egy másik kiviteli alakban a bizalmas berendezésnek lehetővé tesszük, hogy külön berendezéstulajdonosi igazolás alkalmazása nélkül új rejtjelkulcs bevezetésére vonatkozó, ismételt letétbe helyezésre vonatkozó, tulajdonosi átruházási vagy egyéb utasításokat fogadjon el a berendezés tulajdonosától. Az a követelmény, hogy a berendezéshez menő utasításoknál különálló tulajdonosi igazolást kell alkalmazni, adminisztratív terhet jelent, mert a tulajdonosnak a tulajdonában lévő berendezésekre vonatkozó igazolás-adatbázist kell fenntartania, és a megfelelő igazolást minden esetben meg kell keresnie, amikor a berendezést új rejtjelkulccsal akarja ellátni, vagy a berendezésnek egyéb utasítást akar küldeni. A probléma egy jobb megközelítését mutatja a 26. ábra, ahol a gyártóval a berendezések egy adott családjához bocsáttatunk ki egyszeri tulajdonosi igazolást a tulajdonos nyilvános utasítási rejtjelkulcsához, az eladónak megengedjük, hogy nyilvános utasítási 261 rejtjelkulcsát a 260 berendezésben a 260 berendezés eladásakor installálja, és ezután olyan rendszert vezetünk be, amely ezen rejtjelkulcsok belső tárolásán alapszik. A 260 berendezés kezdeti eladásakor a 260 berendezés először ellenőrzi a tulajdonos gyártója 262 igazolásának érvényességét a gyártó által a 260 berendezésbe ágyazott nyilvános utasítási 263 rejtjelkulccsal. Ha a 260 berendezésben üres a tulajdonos nyilvános utasítási rejtjelkulcsának 264 memóriaterülete, a 260 berendezés a tulajdonos nyilvános utasítási 261 rejtjelkulcsát a tulajdonos gyártói 262 igazolásából a tulajdonos nyilvános utasítási rejtjelkulcsának 264 memóriaterületére bemásolja. Ha a tulajdonos nyilvános utasítási rejtjelkulcsa már létezik a 260 berendezésben, és az különbözik a 260 berendezés inicializálását megkísérlő tulajdonosétól, a 260 berendezés azt feltételezi, hogy a gyártó a berendezést más személynek adta el. Mivel minden 260 berendezésnek legfeljebb egy elsődleges tulajdonosa lehet, a 260 berendezés tulajdoni helyzetét a korábbi tulajdonosi igazolási koncepcióval ellentétben (vagy azt kiegészítve) a tulajdonos benne lévő nyilvános utasítási rejtjelkulcsának megléte határozza meg.

Ha tulajdonosi nyilvános utasítási rejtjelkulcs nincs installálva, a berendezést olyan egyfelhasználós, eladásra váró berendezésnek tekintjük, amely nincs korlátozva az új rejtjelkulcs bevezetését vagy tulajdon átruházását illetően. Ekkor a tulajdonosi rejtjelkulcs hiánya a berendezésnek azt jelzi, hogy a felhasználó utasításait végrehajthatja anélkül, hogy alkalmaznia kellene a fent leírt új rejtjelkulcs-bevezetési, újra letétbe helyezési és tulajdonátruházási szabályokat. Ha a bizalmas 270 berendezésben installálták a tulajdonos nyilvános utasítási 271 rejtjelkulcsát, amint azt a 27. ábra mutatja, akkor a felhasználó új rejtjelkulcs bevezetésére vonatkozó, ismételt letétbe helyezésre vonatkozó és tulajdonátruházásra vonatkozó 272 utasításai nem kerülnek végrehajtásra, ha az utasítások nincsenek a megfelelő tulajdonosi egyéni aláírási 274 rejtjelkulccsal aláírva. Ha a tulajdonos 273 aláírását a bizalmas 270 berendezés ellenőrizte, végrehajtja az ismételt letétbe helyezési folyamat előzőleg ismertetett lépéseit. Ezáltal a tulajdonosnak a

berendezés utasításakor nem kell olyan tulajdonosi igazolást csatolnia, amely igazolja, hogy adott számú berendezés tulajdonosa. A tulajdonos aláírt utasításait természetesen adott szabálynak vagy mintának megfelelő berendezésszámú berendezésre vagy a berendezések néhány osztályára kell korlátozni annak megakadályozására, hogy az utasítások a tulajdonos összes berendezésébe bekerüljenek.

Ezen túlmenően, a 28. ábrán látható módon, a tulajdonos kiadhat a berendezés tulajdonlásának átruházására vonatkozó utasítást is, amely a tulajdonos eredetileg installált nyilvános utasítás-ellenőrzési rejtjelkulcsának másikkal (a vásárlóéval, a berendezés új tulajdonosáéval) történő kicserélését jelenti. A berendezés tulajdonosa olyan tulajdonátruházási 282 utasítást küld a 280 berendezésnek, amely tartalmazza az új tulajdonos nevét és nyilvános utasítás-ellenőrzési rejtjelkulcsát, és amely alá van írva az aktuális tulajdonos egyéni utasítás-aláírási 283 rejtjelkulcsával. A berendezés az aktuális tulajdonos nyilvános utasítási 281 rejtjelkulcsával ellenőrzi a tulajdonátruházási 282 utasítást, ezt a rejtjelkulcsot az új tulajdonos nyilvános utasítási 284 rejtjelkulcsával kicseréli, és ezután csak az új tulajdonos utasításaira válaszol. A tulajdonos ezen túlmenően második nyilvános utasítási rejtjelkulcs installálásával egy további „másodlagos tulajdonost" is megnevezhet. Ez a második nyilvános utasítás-ellenőrzési rejtjelkulcs rendelkezik egy „jogosultságok" mezővel, amely jelzi, hogy mely műveletekre vonatkozó utasítások elfogadására van felhatalmazva. Ilyen jogosultságok lehetnek például az új rejtjelkulcs bevezetése, újabb tulajdonos hozzáadása, tulajdonos törlése (ugyanaz, mint a feltételes eladás), minden tulajdonos törlése, és megnevezett tulajdonos nélküli, eladásra váró berendezéssé történő visszaalakítás. Ezek a meghatározott jogosultságok az eredeti elsődleges utasítás-ellenőrzési rejtjelkulcshoz képest tartalmazhatnak több, kevesebb, illetve ugyanannyi jogosultságot, beleértve az elsődleges tulajdonos utasítási rejtjelkulcsának cseréjét vagy eltávolítását is.

A berendezés általánosított nyilvántartásba vétele

Az előzőekben ismertetett, egyéni titkosító rejtjelkulcs-letétbehelyezésére és letétbe helyezési igazolás átvételére vonatkozó általános eljárásokat olyan általánosabb esetre is alkalmazhatjuk, amelynek során a bizalmas berendezést bizalmas harmadik félnél nyilvántartásba vesszük, és a berendezés a harmadik féltől más bizalmas berendezésekkel történő kommunikációt lehetővé tevő felhatalmazást vesz át, de amely eset terjedelmében vagy céljában nem szükségszerűen korlátozódik a rejtjelkulcs-letétbehelyezési helyzetre. Ebben a 24. ábrán látható általános folyamatban egy 241 bizalmas harmadik féllel (TTP, trusted third party) kommunikáló, programozható, bizalmas 240 berendezés rendelkezik egyéni aláírási rejtjelkulccsal, és a megfelelő nyilvános aláírási rejtjelkulcsra vonatkozó gyártói 242 igazolással. A 240 berendezés tartalmazza a gyártó és egész rendszerre kiterjedő (vagy globális) hatóság (SWA, systemwide authority) nyilvános rejtjelkulcsainak biztonságos másolatait is – amelyek egymással megegyezhetnek –, valamint tartalmaz biztonságos rendszerszintű firmware-t, amely a leírásban ismertetett módon támogatja a kiegészítő alkalmazásszintű firmware és megfelelő nyilvános rejtjelkulcsok távolról történő installálását. A 240 berendezés nyilvántartásba vehető a potenciálisan korlátlan számú 241 TTP bármelyikénél, amelyek ebben az általános regisztrációs rendszerben az SWA által aláírt meghatalmazási 243 igazolások kibocsátása révén vannak engedélyezve (az SWA a nyilvános rejtjelkulcsos hitelesítési hierarchia ismert elveinek megfelelően kijelölhet egy sor járulékos hitelesítőt is, amelyek a rendszerben TTP-ket engedélyeznek). Miután a felhasználók berendezéseiket egy adott TTP-nél nyilvántartásba vették, más kereskedelmi partnerekkel speciális tranzakciókat kezdhetnek.

A folyamat első lépésében a felhasználó 240 berendezése nyilvántartásba vételére 244 kérelmet intéz egy adott hitelesített 241 TTP-hez. Ez a 240 berendezés által aláírt 244 kérelem tartalmaz a felhasználóra és a nyilvántartásba vételi kérelem természetére vonatkozó 245 információt, és a 244 kérelmet kíséri a gyártó berendezési 242 igazolása, hogy a gyártó kezeskedjen az aláírásért és a berendezés ismert típusáért. A kiválasztott 241 TTP más információt vagy biztosítékot is kérhet a felhasználótól vagy más féltől a felhasználó identitásának, hovatartozásának, hitelességének stb. ellenőrzésére, ami túl van a protokoll terjedelmén, de befolyásolhatja a TTP döntését abban, hogy a tranzakciók végrehajtására való felhatalmazást megadja vagy megtagadja. A 241 TTP a megfelelő nyilvános rejtjelkulcsokkal ellenőrzi a gyártó aláírását a berendezés 242 igazolásán és a berendezés aláírását a felhasználó nyilvántartásba vételi 244 kérelmében lévő 245 információban.

Amikor a felhasználónak megengedjük, hogy az általa kért osztályú tranzakciókba lépjen, a 241 TTP 247 igazolást tartalmazó 246 választ bocsát ki, amely 247 igazolás felhatalmazza a berendezést a felhasználó nevében történő tranzakciók végrehajtására. A 241 TTP berendezést felhatalmazó 247 igazolása általában olyan információt tartalmaz, amely azonosítja a 241 TTP-t, a felhasználót, a felhasználó berendezését, az engedélyezett tranzakciókat, valamint kényelmességi okokból (amint azt a továbbiakban ismertetjük) a felhasználói berendezés nyilvános aláírási rejtjelkulcsának újrahitelesített másolatát, hogy a felhasználónak ne kelljen elküldenie berendezési 242 igazolását a kereskedelmi partnerekkel történő, minden egyes soron következő tranzakciónál. A 241 TTP 246 válasza tartalmazhat letölthető firmware-t és/vagy a felhasználó bizalmas berendezésébe töltendő, a felhatalmazott tranzakciók végrehajtását engedélyező nyilvános rejtjelkulcsokat is. Amikor a 241 TTP 246 válasza a felhasználót az új firmware vagy nyilvános rejtjelkulcsok berendezésébe történő biztonságos betöltésére hívja fel, a 256 válasz tartalmazni fogja a 241 TTP SWA által kibocsátott hatósági 243 igazolását is, amely hitelesíti a 241 TTP nyilvános aláírási rejtjelkulcsát, szállító firmware-ét, és a nyilvános rejtjelkulcs frissítésére szóló felhatalmazását. Amikor a felhasználó bizalmas 240 berendezése megkapja a 241 TTP 246 válaszát, az SWA beágyazott nyilvános aláírási rejtjelkulcsával ellenőrzi a 241 TTP hatósági 243 igazolását, a

241 TTP abban lévő nyilvános aláírási rejtjelkulcsával ellenőrzi a firmware és a nyilvános rejtjelkulcsok 248 frissítéseit, valamint a 241 TTP berendezésének felhatalmazási 247 igazolását.

Ha a 24. ábrán látható módon a felhasználó egy 250 kereskedelmi partnerrel tranzakciót kíván végrehajtani, a berendezése a leírásban ismertetettek szerint kialakítja a tranzakciós 249 adatot a berendezésben (a gyártáskor vagy egy azt követő letöltéskor) installált firmware-programban kialakított szabályoknak megfelelően, és aláírja a tranzakciós 249 adatot, valamint a megfelelő nyilvános rejtjelkulcshoz tartozó igazolást csatol. Ez az igazolás lehet a gyártó berendezésének 242 igazolása, de méginkább a TTP berendezésének felhatalmazó 247 igazolása, amely tartalmazza a berendezés kényelmi okokból újrahitelesített nyilvános rejtjelkulcsának másolatát. A 250 kereskedelmi partner a TTP berendezést felhatalmazó 247 igazolásán lévő aláírását rendszerint a TTP nyilvános rejtjelkulcsával ellenőrzi, majd a berendezés abban lévő nyilvános aláírási rejtjelkulcsával ellenőrzi a berendezés 249 tranzakción lévő aláírását, amivel megerősíti, hogy a berendezés teljesíti a megfelelő firmware által előírt tranzakciós protokoll követelményeit. Abban az esetben, ha a 250 kereskedelmi partner még nem rendelkezik a megfelelő TTP nyilvános aláírás-hitelesítési rejtjelkulcsával, a felhasználó tranzakciójába behelyezheti a TTP SWA-jának felhatalmazó 243 igazolását. Ezt a 250 kereskedelmi partner ellenőrizheti az SWA nyilvános rejtjelkulcsával, amellyel a rendszerben való részvételhez rendelkeznie kell.

Az eddig ismertetett, általánosított folyamat elég általános ahhoz, hogy lehetővé tegye (a) egy egyéni titkosító rejtjelkulcs-letétbehelyezését egy letétbe helyezési központ (TTP) által aláírt letétbe helyezési igazolás ellenében, ahol a felhasználói berendezés igazolásában lévő, vagy abban elrejtett információ azt közli a letétbe helyezési központtal, hogy a berendezés már el van látva olyan firmware-rel, amely képes végrehajtani az itt ismertetett rejtjelkulcs-letétbehelyezési titkosítórendszer speciális funkcióit, vagy (b) ha a berendezés nem rendelkezik ilyen firmware-rel, de azzal ellátható, lehetővé tegye biztonságos szoftverfrissítés letöltését, amelynek installálása lehetővé teszi a berendezés számára a letétbe helyezési rendszer tranzakciós igényeinek kielégítését. A 250 kereskedelmi partnernek küldött tranzakciós 249 adat lehet egy 247 TTP (fő letétbe helyezési központ) által kibocsátott 247 felhatalmazással (a felhasználó letétbe helyezési igazolásával) kísért, üzenet ellenőrző fejrésszel ellátott, titkosított üzenet.

A 24. ábra általánosított rendszere ezért sok olyan felettébb kívánatos tulajdonsággal bír, amely üzleti és kormány általi tranzakciók komplex formáit teszi lehetővé nyílt kommunikációs hálózati környezetben. Így például sok különböző berendezésgyártó létezhet, ahol az egyes berendezések képesek többlépéses tranzakciók biztonságos végrehajtására, firmware letöltésére járulékos típusú, többlépéses tranzakciók biztonságos végrehajtására, valamint az így létrehozott tranzakciók aláírására. Ezenkívül bármennyi bizalmas harmadik fél létezhet, amelyek mindegyike különböző típusú tranzakciós felhatalmazást bocsát ki, valamint eltérő osztályú firmware-alkalmazást hoz létre és hitelesít, például rejtjelkulcs-letétbehelyezést, digitális készpénzkezelést, gépkocsikölcsönzést vagy felhasználói orvosi adatkezelést. Ezáltal, bár a kereskedelmi partnernek hasonlóan kiépített bizalmas berendezést kell alkalmaznia (ezt a felhasználó berendezésének firmware-je és protokolljai kívánják), a berendezést az eredeti felhasználó partnerétől eltérő partner gyárthatja, bocsáthatja ki és szerelheti be, az eredeti felhasználó tranzakciói a rendszer szabályai szerint mégis elfogadásra és feldolgozásra kerülnek, amíg a partner birtokolja az SWA nyilvános aláírás-hitelesítési 247 rejtjelkulcsának másolatát, amely ha az SWA és annak TTP-i által hitelesítve van, minden típusú berendezés és azok programjai számára lehetővé teszi, hogy egymást felismerjék és együtt dolgozzanak. Ez a protokoll például olyan üzleti célokra alkalmazható, amelyekben a rendszereknek tranzakciós követelményeket kell kielégíteniük az (a) ellenőrizhetően letétbe helyezett rejtjelkulcsokkal történő titkosítást, (b) készpénz vagy más nagy értékű dokumentumok digitális reprezentációjának kezelését, és (c) a felhasználó orvosi vagy más személyes információihoz történő hozzáférést és azok használatát illetően.

Egyedi tulajdonosi azonosítószám

A könnyű kezelhetőség és a titkossági jogok közötti egyensúlytól függően az egyedi tulajdonosi azonosítószám opcionálisan megjelenhet a (a) felhasználó letétbe helyezési igazolásában vagy (b) normál kommunikációk alatt kibocsátott MCH-kban, valamint a letétbe helyezése ügynökökhöz menő, rejtjelkulcsszeleteket tartalmazó üzenetekben. Egy kommunikációk megfejtését megkísérlő nyomozó számára kívánatos lenne az, hogy a tulajdonosi azonosítószámot tartalmazó MCH megtekintésével képes legyen megállapítani, hogy abban a kommunikációban részt vevő egy vagy mindkét berendezés, amelyből az MCH származik, adott tulajdonoshoz tartozik-e. Más titkossági érdekek, bizonyos tulajdonosokéit is beleértve azonban azt sugallják, hogy a kommunikációk titkosságának növelésére el kell hagyni az MCH-ból a tulajdonosi azonosítószámot. Olyan esetekben, amelyekben a tulajdonosi azonosítószám csak a berendezés letétbe helyezési igazolásában szerepel, és nem szerepel a kommunikációk MCH-iban, ha egy adott alkalmazó által fizetett nyomozó meg akarja állapítani, hogy egy meghatározott kommunikáció az alkalmazó alkalmazottaitól származik-e, sok olyan MCH-val találkozik, amelynek nincs listázott berendezéstulajdonosa, és egy adott MCH-ban listázott fő letétbe helyezési központnál kell érdeklődnie afelől, hogy az MCH az alkalmazó tulajdonában lévő berendezéstől származik-e. A fő letétbe helyezési központ megfejti az MCH kommunikációban részt vevő fél igazolási számát, amely fél rejtjelkulcsai a fő letétbe helyezési központnál letétbe vannak helyezve, és megvizsgálja, hogy a felhasználói igazolás a nyomozó alkalmazójának lett-e kibocsátva. Amennyiben ez teljesül, és ha a nyomozó kérelme az alkalmazó-tulajdonos aláírási rejtjelkulcsával alá van írva (vagyis a nyomozó rendelkezik felhatalmazással az alkalmazó-tulajdonostól

a nyomozásra), a fő letétbe helyezési központ feltárja ezt az információt. Ha a nyomozó nem rendelkezik felhatalmazással, meghatalmazást vagy bírósági végzést kell szereznie, hogy nyomozhasson az ismeretlen berendezéstulajdonosok MCH-iban tükröződő gyanús tevékenység ügyében. A legtöbb berendezéstulajdonos feltételezhetően nem fogja megtagadni, hogy nyíltan megnevezzék a felhasználói letétbe helyezési igazolásokban és MCH-kban, mivel a legtöbb elektronikus kommunikációs rendszerben nem praktikus a fizikai és logikai hálózati címekre vonatkozó információk elrejtése, amelyek gyakran erősen azonosítják az adott üzenetet küldő és vevő intézményt. Így keveset vesztünk azzal, hogy az egyedi tulajdonosi azonosítószámokat nyilvánosan kezeljük, és sokat nyerünk azzal, hogy gyorsan tudunk üzeneteket átvizsgálni és szétválogatni a küldőberendezés tulajdonosának és vevőberendezés tulajdonosának nevei alapján.

Az egyedi tulajdonosi azonosítószám azonban anélkül is szerepelhet az alkalmazott letétbe helyezési igazolásában vagy a kommunikációk MCH-jában, hogy nyilvánosságra kerülne. Az alkalmazott letétbe helyezési igazolása és MCH-i a fent leírt többi rejtjelkulcs mellett tartalmaznak egy alkalmazói nyilvános titkosító rejtjelkulcsot. Ezek a rejtjelkulcsok általában mind a küldő, mind a vevő letétbe helyezési igazolásában megjelennek (feltételezzük azt, hogy a küldő és a vevő is rendelkezik alkalmazóval). Az MCH kialakításakor a küldő berendezése az MCH-ba az egyik vagy mindkettő alkalmazó egyedi azonosítószámát belehelyezi, amely számok a megfelelő alkalmazó nyilvános titkosító rejtjelkulcsával titkosítva vannak, és így a küldő berendezése gyakorlatilag az MCH segítségével minden alkalmazó-tulajdonosnak egy olyan üzenetet küld, amely a megfelelő alkalmazó-tulajdonos saját – csak általa megfejthető – egyedi azonosítóját tartalmazza. Ez az eljárás hasonló a fent leírthoz, amelyben a küldő az MCH-val küldi a küldő és a vevő igazolási számait, amelyek a megfelelő fő letétbe helyezési központ nyilvános titkosító rejtjelkulcsával vannak titkosítva, valamint az MCH-val küldi az üzenet-szakaszrejtjelkulcsot vevőhöz (az MCH normál funkciója) és a küldőhöz, ami lehetővé teszi mindkét fél lehallgatását. Ez a technika lehetővé teszi az alkalmazó számára annak egyszerű megállapítását, hogy melyik MCH-k tartoznak az alkalmazottaihoz, mialatt a tulajdonos-alkalmazó alkalmazottaihoz tartozó üzenetek nem azonosíthatók könnyen az üzenetek áramlásában, valamint a tulajdonosi azonosítószámok titkosítva vannak, és nem szerezhetők meg egyszerűen.

Ez a megközelítés azonban azzal a hátránnyal jár, hogy az alkalmazó nyilvános titkosító rejtjelkulcsával titkosított egyedi alkalmazói azonosítószáma mindig ugyanazt az értéket eredményezi, amely ezáltal felismerhető. A megközelítés egy jobb megvalósítása az, hogy olyan adatblokkot titkosítunk az alkalmazó nyilvános rejtjelkulcsával, amely aktuális időbélyeget (vagy más véletlen számot) tartalmaz a letétbe helyezési igazolási száma mellett (amelyet az alkalmazónak természetesen jogában áll ismerni), és így az időbélyeg a titkosított adatblokknak nagy változatosságot ad. A titkosított blokkban elkülönülő, „szembeötlő" szöveg, például „ALKALM" (vagy esetleg az alkalmazó egyedi azonosítója, helyköz megengedett) is szerepelhet, hogy a mezőt megfejtő személy számára nyilvánvaló legyen a megfejtés sikeressége (abban az esetben, ha a többi adatrész bináris formájú, amikor is ebben nem lehetünk biztosak). Ebben az esetben az alkalmazó tulajdonosi voltának bizonyítékául csupán az szolgál, hogy képes ezt a mezőt elolvasni. Ezen túlmenően, ha az időbélyeg nem eléggé megbízhatóan különböző az egyes esetekben, a változatosság növelésére újabb véletlen számot adhatunk az adatblokkhoz, amivel az alkalmazói MCH adatblokkokat egyedivé teszünk.

Ezzel a továbbfejlesztett eljárással, amelyet mind a küldő, mind pedig a vevő alkalmazói számára minden elküldött üzenetnél elvégzünk, anélkül hogy minden egyes kommunikációhoz be kellene mutatni a titkosított MCH-t a megfelelő letétbe helyezési központnak, az alkalmazók és más szponzorok megállapíthatják, hogy mely kommunikációkat generálták vagy vették alkalmazottaik, ami által adott esetben jelentős költséget takarítunk meg. Az alkalmazóknak alkalmazottaik egyéni titkosító rejtjelkulcsának megszerzéséhez az előzőekhez hasonlóan kapcsolatba kell lépniük a fő letétbe helyezési központtal és a letétbe helyezési ügynökökkel, és azáltal kell igazolniuk, hogy valóban az alkalmazott berendezésének tulajdonosai, hogy kérelmüket a berendezés gyártója által kibocsátott és tulajdonosi igazolásukban lévő nyilvános aláírás ellenőrzési rejtjelkulcsnak megfelelő egyéni aláírási-rejtjelkulccsal aláírják. Az alkalmazók így azonban megtakarítják a felekhez menő felesleges kérvényekre fordított időt, erőfeszítést és költséget azon kommunikációk MCH-ira vonatkozóan, amelyekről később kiderül, hogy nem a tulajdonukban lévő berendezésektől származtak. Ha egy alkalmazó bűntényt vagy más jogellenes cselekményt sejt a nem tulajdonában lévő berendezésektől származó kommunikációk MCH-ival kísért üzenetekben, az előzőekhez hasonlóan minden esetben kapcsolatba léphet egy megfelelő törvényes ellenőrzési ügynökséggel, elmondhatja az ügynökségnek, hogy miért sejt bűncselekményt, az ügynökségen keresztül a bíróságtól felhatalmazást kaphat azon kommunikációk lehallgatására és/vagy megfejtésére, amelyek olyan bűnözőktől származnak, akik nem az alkalmazó alkalmazásában állnak, vagy esetleg az alkalmazó helyiségeiben tevékenykedő személyektől, akik vagy alkalmazottak, vagy nem, és akik olyan titkosítóberendezéseket használnak, amelyek nincsenek az alkalmazó tulajdonában, és nincsenek az alkalmazó nevén nyilvántartásba véve.

Ez az eljárás, amelyben az MCH-ba titkosított információt helyezünk oly módon, hogy azt csak a felhatalmazott fél tudja elolvasni, a küldőn és a vevőn kívül (akik meg tudják fejteni az üzenet-szakaszrejtjelkulcsot) nyilvánvalóan kiterjeszthető további felekre, mégpedig a felek fő letétbe helyezési központjaira (amelyek meg tudják fejteni megfelelő felhasználójuk igazolási számát) és a felek alkalmazó-tulajdonosaira (akik anélkül, hogy mással kapcsolatba kellene lépniük, meg tudják fejteni alkalmazottjuk igazolási számát vagy saját

egyedi tulajdonosi azonosítószámát, hogy eldönthessék, hogy tulajdonosai-e a kommunikáló berendezésnek, mialatt elkerülik azt, hogy őket minden üzeneten azonosítsák). Ez kiterjeszthető más felekre is, például nagyon nagy vállalatokban lévő divíziókra, vagy olyan külföldi országokbeli, helyi törvényes ellenőrzésre, amelyek nem támasztanak meghatalmazási igényeket. Természetesen az ezekkel a rejtjelkulcsokkal titkosított információkat tisztán, azaz titkosítatlanul is fel lehet tüntetni, mint ahogyan azt korábban kifejtettük, ha a feleknek nincs ellenvetésük az ellen, hogy nyíltan megnevezzék őket, és az üzeneteken rutinszerűen azonosíthatók legyenek. Ezt az információt el is lehet hagyni, ha az adott fél irreleváns, például ha egy felhasználónak nincs alkalmazója. Egyszerűbb eljárást eredményezne, ha minden helyzetben egyazon MCH formátumot alkalmaznánk, és a nem használt mezőket üresen hagynánk. Az előnyös kiviteli alakban azonban ugyanazon rendszeren belül különböző MCH formátumokat alkalmazunk, amely formátumok az első mezőben egyedi verziószámmal vannak azonosítva oly módon, hogy minden MCH-t feldolgozó berendezés képes meghatározni, hogy milyen mezőket kell fogadnia, és az MCH-t ennek megfelelően kezeli. Ez az eljárás végtelen számú érdekelt fél beágyazását teszi lehetővé az MCH-ba, ami a lehető legrugalmasabb rendszert eredményezi. A számítási igényt főként az fogja meghatározni, hogy a mezők közül mennyit kell valójában titkosítani a megfelelő fél nyilvános titkosító rejtjelkulcsával.

Az alkalmazók az MCH-ban lévő információt könnyebben kezelhetik, ha az egyes bejegyzésekhez „iránymutató mezőt" vagy utasítási kódot csatolnak, amely olyan kódot tartalmaz, amely az alkalmazó berendezését az irányban utasítja, hogy milyen információt helyezzen az MCH-ba. A korábbiakhoz hasonlóan az utasítási kód olyan elemeket tartalmazhat, amelyek az alkalmazónak a következő információk beillesztésére adnak lehetőséget: (1) az alkalmazó neve és egyedi azonosítószáma titkosítatlanul vagy álnéven, (2) az „alkalmazó" szó titkosítatlanul és az alkalmazó egyedi azonosítószáma egy MCH-mezőben titkosítva, (3) a felhasználó igazolási száma egy titkosított mezőben, (4) az üzenet-szakaszrejtjelkulcs egy titkosított mezőben, (5) időbélyeg egy titkosított mezőben és (6) egy véletlen zavarószám a többi titkosított mező bármelyikében. Ezen lehetőségek közül egyidejűleg többet is alkalmazhatunk. Ezen túlmenően ezek az irányadó lehetőségek ugyanazok az érdekelt felek számára, a kommunikációs feleket is beleértve, ami lehetővé teszi, hogy a feleket postai vagy rendszer-azonosítójukkal, illetve egyszerűen a megfelelő üres MCH mezőkben a „küldő" vagy „vevő" szóval címkézzék meg.

Több, egyidejűleg letétbe helyezett rejtjelkulcs

A berendezés firmware-rutinjai frissítésének fent leírt jellemzőin és a gyártó nyilvános rejtjelkulcsai kicserélésének jellemzőin kívül a találmány szerinti bizalmas berendezés rendelkezik azzal a képességgel is, hogy egyidejűleg több letétbe helyezett titkosító rejtjelkulcsokból álló készletet tartson fenn és kezeljen. Normális esetben, ha a berendezés belekezd az új rejtjelkulcs bevezetésének ciklusába, vagyis új, egyéni titkosító rejtjelkulcs generálásába és letétbe helyezésébe, továbbá ennek eredményeképp letétbe helyezési igazolást kap a megfelelő új, nyilvános titkosító rejtjelkulcs számára, a berendezés az előző egyéni rejtjelkulcsot törli, hogy a berendezés az újonnan letétbe helyezett egyéni rejtjelkulcsra hagyatkozzon. Adott esetben a berendezés rövid ideig megtarthatja az előző egyéni rejtjelkulcsot, amennyiben szükséges, például amíg az adattárolóban az előző egyéni titkosító rejtjelkulccsal titkosított adatot visszaállítja. Egy másik kiviteli alakban azonban a berendezés elfogadhat és végrehajthat olyan, a fent leírt módon a felhasználótól vagy a berendezés tulajdonosától származó ismételt letétbe helyezésre vonatkozó utasítást, hogy ugyanarra a titkos/nyilvános titkosítórejtjelkulcs-párra második érvényes letétbe helyezési igazolást hozzon létre. Ebben a kiviteli alakban a berendezés a letétbe helyezési folyamatot valószínűleg különböző letétbehelyezésiügynök-listával és különböző fő letétbe helyezési központtal folytatja le, és ugyanarra a nyilvános/egyéni titkosítórejtjelkulcs-párra eltérő, a második fő letétbe helyezési központ által aláírt és kibocsátott érvényes letétbe helyezési igazolást kap, amely az első letétbe helyezési igazolással átválthatóan használható. Ez a nyilvános titkosító rejtjelkulcsra vonatkozó második igazolás olyan esetekben alkalmazható, amikor a berendezés felhasználója külföldi úton van vagy más országokban lévő felekkel levelezik, különösen ha ezek az országok törvényes felügyeletet kívánnak fenntartani az országból induló vagy oda érkező üzenetek fölött. Ezekben az esetekben ugyanazon berendezés-rejtjelkulcs másik országban történő ismételt letétbe helyezésével a felhasználó (vagy a felhasználó alkalmazója) segítheti a másik országbeli jogi kívánalmak teljesítését, mialatt a felhasználó vagy alkalmazó számára megengedi azt a kényelmet, hogy ügyeit (a tulajdonos törvényes lehallgatása, elveszett rejtjelkulcs visszanyerésére stb.) saját országában lévő, eredeti letétbe helyezési ügynökeivel intézheti. Továbbá, hogy a tulajdonos számára lehetővé tegyük alkalmazottaik MCH-inak nyomon követését, elégséges lehet a küldő vagy vevő tulajdonosi azonosítóinak MCH-kban történő feltüntetése, amelyek közlik a tulajdonossal, hogy valóban képes a rejtjelkulcs megszerzésére. Idő és erőfeszítés megtakarítására a tulajdonos az ilyen MCH-t elküldheti a külföldi fő letétbe helyezési központhoz, hogy megszerezze a külföldi letétbehelyezésiigazolásszámot, a megfelelő berendezésszámot és a megfelelő berendezésigazolást, de ezután jelentkeznie kell hazai letétbe helyezési ügynökeinél, akik ellenőrizni tudják a már náluk lévő tulajdonosi igazolást, és kiadják az adott rejtjelkulcs szeleteit. Ez az eljárás felmenti a berendezés tulajdonosát azon járulékos jogi formalitások alól, amelyek szükségesek lehetnek az adott rejtjelkulcs szeleteinek külföldi letétbe helyezési ügynököktől történő megszerzéséhez.

Nemzetbiztonsági exportbiztosítékok

Az Egyesült Államok kormányának jelenlegi politikája az, hogy szabadon lehetővé teszi a titkosítás amerikai állampolgárok általi alkalmazását az Egyesült Álla-

mokon belül, de súlyos megkötéseket és szankciókat helyez kilátásba titkosítóberendezések, szoftver vagy know-how exportálása esetén. A jelenlegi rendszert módosíthatjuk úgy, hogy a titkosítóberendezések viszonylag szabad, magáncélú használatát tesszük lehetővé az Egyesült Államokon belül, mialatt egyidejűleg korlátozzuk azok nemzetközi alkalmazását. Az ilyen rendszer lehetővé teszi olyan különálló, egymással kapcsolatban lévő „területek" létezését, amelyek nyitva állnak a hardver- és szoftverkereskedők számára, és amelyekben a rendszerben használt szabványos üzenetformátumokhoz képest nincsenek kialakításbeli változtatások, illetve azok mértéke minimális. Kívánatos továbbá, hogy lehetővé tegyük egyéni letétbe helyezési ügynökök alkalmazását tisztán vállalaton belüli, egyországos esetekben, ahol a rejtjelkulcs-letétbehelyezési rendszert kizárólag arra használjuk, hogy egy adott vállalat számára lehetővé tegyük alkalmazottai titkosításainak megfigyelését és szabályozását bármiféle nyílt vagy burkolt kötelezettség nélkül, hogy megkönnyítsük a törvényes ellenőrzésnek a vállalat által letétbe helyezett rejtjelkulcsokkal titkosított kommunikációkhoz történő hozzáférést. Előfordulhat, hogy az ilyen vállalatok saját használatukra megveszik a szoftvert és a hardvert, de megtagadják bármiféle nyilvános kötelezettség felvállalását az egyéni rejtjelkulcsokhoz történő hozzáférés rövid időn belüli biztosítását illetően, amint azt a törvényes ellenőrzés bűnözők vagy terroristák üldözése közben kívánhatja.

A rendszer megvalósításához először feltételezzük, hogy a rendszerben lévő berendezések közvetlenül vagy közvetve egy egész rendszerre kiterjedő hatósághoz (SWA) vannak kapcsolva, amely (az előzőekben leírtak szerint) a letétbe helyezési ügynököknek, fő letétbe helyezési központoknak és berendezésgyártóknak igazolásokat bocsát ki, hogy azokat a berendezések érvényesnek és megbízhatónak tekintsék. Egy nemzeti vagy globális kommunikációs rendszernek gyakorlati okokból több, egymással kapcsolatban nem álló fő letétbe helyezési központot és ügynököt kell támogatnia, amelyeknek az SWA által igazoltan hitelesnek kell lenniük. A fő letétbe helyezési központoknak vagy letétbe helyezési ügynököknek kibocsátott igazolásokban az SWA azokat „nyilvánosnak" vagy „egyéninek" minősíti. Egy „nyilvános" fő letétbe helyezési központ vagy letétbe helyezési ügynök úgy van kialakítva és megbízva, hogy azonnal válaszoljon a nemzetbiztonsági vagy törvényes ellenőrzési meghatalmazásokra és idézésekre. Az ilyen ügynököknél letétbe helyezett rejtjelkulcsokkal rendelkező felhasználók számára megengedett, hogy határon kívüli kommunikációt létesítsenek. Egy „egyéni" fő letétbe helyezési központ vagy letétbe helyezési ügynök azokat az egyvállalati vagy egyországos rejtjelkulcsközpontokat öleli fel, amelyek a rejtjelkulcs-letétbehelyezési technológiát saját használatukra helyezték üzembe, és nem vállalnak megbízást nyilvános szintű szolgáltatásra. Az SWA-tól a fő letétbe helyezési központ vagy letétbe helyezési ügynök számára kibocsátott igazolás tartalmaz egy országkódot is. Ezért minden olyan felhasználói letétbe helyezési igazolás, amelyet egy fő letétbe helyezési központ bocsátott ki és írt alá, valamint amelyhez csatolva van a fő letétbe helyezési központ SWA igazolása, szintén tartalmazni fogja a felhasználó országkódját. Megjegyezzük, hogy kényelmi okokból a felhasználó letétbe helyezési igazolásának azt is tudatnia kell, hogy nyilvános vagy nem nyilvános letétbe helyezési ügynöktől származik, bár az SWA nem képes ezen információ helyességének biztosítására. Így a berendezés könnyebben tarthatja be a szabályokat annál, mintha minden esetben kérné a fő letétbe helyezési központ SWA igazolását.

A 29. és 30. ábra nemzetközi titkosított kommunikáció adása és vétele esetére mutatja a letétbe helyezési követelmények betartásának menetét. Amint azt a 29. ábra mutatja, a küldő bizalmas 290 berendezése a rendszert úgy valósítja meg, hogy a küldőtől és a vevőtől kéri a letétbe helyezési 291, 293 igazolásokat, és ha a küldő és vevő nem ugyanannál a fő letétbe helyezési központnál helyezett letétbe, kéri a fő letétbe helyezési központjaik SWA 292, 294 igazolásait a nemzetközi kommunikáció adása előtt. A vevő felhasználó 295 országkódjának és fő letétbe helyezési központja 296 országkódjának egymással meg kell egyezniük, hogy a küldő 290 berendezés üzenetet küldjön. Ezen túlmenően, ha a küldő és vevő különböző országban vannak, és ha valamelyik felhasználó nem nyilvános 298, 299 fő letétbe helyezési központot alkalmaz, a küldőberendezés megtagadja az ahhoz a vevőhöz menő kommunikációt. Amint azt a 30. ábra mutatja, a vevő bizalmas 300 berendezése a rendszert szintén úgy valósítja meg, hogy megtagadja a valamilyen módon keletkezett kommunikáció megfejtését, ha a küldő és a vevő különböző országokban vannak, és ha valamelyik felhasználó nem nyilvános fő letétbe helyezési központot használ. Ezek a szabályok megvalósítják azt a kívánt politikát, hogy nem lehet megengedni a letétbe helyezés nélküli, nemzetközi titkosított kommunikációkat, mivel a fő letétbe helyezési központ nem tudja meghamisítani az SWA által igazolt nyilvános státusát, és még ha a fő letétbe helyezési központ hamisítani is tudná a felhasználó országkódját (hogy a felhasználó külföldi területhez tartozónak látszódjon), a berendezés nem engedi meg az eltérést a felhasználó és a fő letétbe helyezési központ országkódjai között. Bár ez a rendszer nem akadályozza meg a felhasználót abban, hogy bizalmas titkosítóberendezését illegálisan átvigye a nemzeti határon, de a rendszer könnyen megfeleltethető a nemzeti követelményeknek azáltal, hogy lehetővé teszi a felhasználó számára, hogy letétbe helyezett rejtjelkulcsot kapjon az egyes országokban, és hogy csak a megfelelő rejtjelkulcs használatával kommunikáljon az egyes politikai régiókban.

Többfelhasználós berendezésváltozatok

A találmány egy további jellemzője, hogy ugyanazon berendezés használatával képes különböző helyi vagy távoli felhasználóhoz irányuló különböző kommunikációs szakaszok kezdeményezésére és egyidejű kezelésére. Sok nagyobb számítógép támogat több felhasználót, akik gyakran egyidejűleg vannak terminálokon bejelentkezve, és akik a világon más-más személyekkel

akarnak titkosított kommunikációs szakaszokat kezdeményezni. Rendkívüli módon nem lenne hatékony azonban az, ha egy megosztott számítógépen lévő minden egyes felhasználói szakasz számára különálló bizalmas berendezésre lenne szükség, ezért a bizalmas berendezés az egyes kommunikációk számára nyomon követheti az üzenet-szakaszrejtjelkulcsot oly módon, hogy azt egy a szakaszra vonatkozó, egyedi üzenetsorszámmal (MSN, message sequence number) együtt eltárolja. Ekkor az adott MSN-nel rendelkező további üzenetcsomag érkezésekor az üzenetcsomag késedelem nélkül megfejthető és a válasz titkosítható. Ezen túlmenően a berendezés több felhasználó egyéni megfejtési rejtjelkulcsát letétbe helyezheti, mialatt a felhasználók egyéni rejtjelkulcsát a meghatározott felhasználó egyedi azonosítószámával összerendeli, valamint lehetővé teszi, hogy a rejtjelkulcsokat csak megfelelő felhasználói hitelesítés, például kulcsszó, intelligens mikrokártya, PIN, biometria, lekérdezésre adott válasz stb. bemutatásával lehessen használni. Amikor az egyes nyilvános/egyéni rejtjelkulcspárokhoz letétbe helyezés céljára történő generálásukkor felhasználói azonosítószámot és kulcsszót vagy hasonlót rendelünk, az illetéktelen hozzáférés esélyének korlátozására a berendezéssel foganatosíthatjuk a kulcsszavakra vonatkozó, például a hosszúságot, érvényességi időt, próbálgatási kizárásokat és könnyű kitalálhatóságot illető szokásos szabályokat.

Ezáltal rejtjelkulcs-letétbehelyezéses titkosítórendszert és eljárást hoztunk létre. A szakember számára belátható, hogy a találmány az ismertetett példaképpeni kiviteli alakoktól eltérően is megvalósítható, és a találmány oltalmi körét csak a következő szabadalmi igénypontok korlátozzák.

SZABADALMI IGÉNYPONTOK

1. Eljárás ellenőrizhetően bizalmas kommunikáció létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál nagyszámú felhasználó által alkalmazandó nagyszámú, titkos, aszimmetrikus rejtjelkulcsot letétbe helyezünk, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és a hitelesítéstől függően az egyes felhasználóktól a nagyszámú rejtjelkulcs közül egy megfelelővel kommunikációt kezdeményezünk.

2. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál az egyes felhasználókhoz rendelt titkos, aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, valamint egy kezdeményező felhasználó és egy vevő felhasználó rejtjelkulcsainak hitelesítésétől függően a kezdeményező felhasználótól a vevő felhasználóhoz biztonságos kommunikációt kezdeményezünk.

3. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy a biztonságos kommunikáció kezdeményezése előtt a kezdeményező felhasználó bizalmas hardverberendezése a kezdeményező felhasználó és a vevő felhasználó rejtjelkulcsai hitelesítését jóváhagyja.

4. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hitelesítés során a letétbe helyezési központ kibocsát egy letétbe helyezési igazolást, amely hitelesíti a vevő felhasználó rejtjelkulcsát, és a kommunikáció kezdeményezése során a kezdeményező felhasználó ellenőrzi a vevő felhasználó letétbe helyezési igazolását.

5. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy egy felhatalmazó személy első és második letétbe helyezési központnak letétbe helyezési központi igazolást bocsát ki, ahol a vevő felhasználó a második letétbe helyezési központnál helyez letétbe rejtjelkulcsot, az első és második letétbe helyezési központ felhasználói igazolást bocsát ki a kezdeményező és a vevő felhasználó számára, valamint a kezdeményező felhasználó a második letétbe helyezési központ igazolását és a vevő felhasználó igazolását ellenőrzi a biztonságos kommunikáció kezdeményezése előtt.

6. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy egy bizalmas berendezés benne lévő, illetéktelen hozzáférésnek ellenálló logika alkalmazásával jóváhagyja a vevő felhasználó rejtjelkulcsa ellenőrzését.

7. A 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy a letétbe helyezett rejtjelkulcs Diffie–Hellmann-protokoll közbenső száma.

8. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, szelektív kívülálló fél általi hozzáféréssel, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt titkos, aszimmetrikus rejtjelkulcsokat helyezünk letétbe, ahol az egyes felhasználók legalább egy rejtjelkulcshoz és legalább egy, a felhasználó kommunikációihoz hozzáféréssel rendelkező, első választható, kívülálló félhez vannak rendelve, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy küldő felhasználótól egy vevőhöz az első kívülálló fél számára a kommunikációhoz való hozzáférést megengedő módon kezdeményezzük a bizalmas kommunikációt.

9. A 8. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció kezdeményezése során az első kívülálló fél rejtjelkulcsával titkosított hozzáférési információt küldünk.

10. A 8. igénypont szerinti eljárás, *azzal jellemezve,* hogy a letétbe helyezés során egy letétbe helyezési központnál nyilvántartásba veszünk egy bizalmas hardverberendezést, amely egy felhasználóval és az első kívülálló féllel van társítva.

11. A 10. igénypont szerinti eljárás, *azzal jellemezve,* hogy a letétbe helyezés során egy berendezés-előállító kibocsát egy első tulajdonosi igazolást, amely azonosítja a bizalmas hardverberendezést és az első kívülálló felet, valamint a tulajdonosi igazolást letétbe helyezési ügynökhöz továbbítjuk a felhasználó kommunikációihoz hozzáféréssel rendelkező első kívülálló fél azonosítására.

12. A 8. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció kezdeményezése során a kom-

munikációhoz való hozzáférés céljából egy, a vevőhöz tartozó második kívülálló fél számára hozzáférhető információt küldünk.

13. A 8. igénypont szerinti eljárás, *azzal jellemezve,* hogy a vevő egy második kívülálló fél megnevezését és a vevő egy rejtjelkulcsát továbbítja egy letétbe helyezési központnak, és a letétbe helyezési központ a második kívülálló fél megnevezését a vevő rejtjelkulcsával együtt egy igazolásba foglalja.

14. A 13. igénypont szerinti eljárás, *azzal jellemezve,* hogy a vevő felhasználó egy igazolását a küldő felhasználóhoz továbbítjuk, amely igazolás megnevezi a kommunikációhoz hozzáféréssel rendelkező második kívülálló felet.

15. Eljárás biztonságos kommunikációra legalább egy kommunikáló féllel és a kommunikációban részt nem vevő fél által visszafejthető üzenetrejtjelkulccsal rendelkező rendszerben, amely eljárásban minden felhasználót ellátunk számítógépes hardverberendezéssel, *azzal jellemezve,* hogy a berendezés felhasználójától különböző berendezéstulajdonos által meghatározott ellenőrzési információ szerint egy központban a hardverberendezéseket nyilvántartásba vesszük, a hardverberendezéseket hitelesítjük, amely hitelesítések egy központot, egy felhasználót és egy hardverberendezést egymáshoz rendelő igazolást generálnak, valamint egy üzenetrejtjelkulcs alkalmazásával egy kezdeményező felhasználótól egy vevőhöz a tulajdonosnak a kommunikációhoz való hozzáférést megengedő módon biztonságos kommunikációt kezdeményezünk.

16. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során nagyszámú központ közül a tulajdonos által meghatározott információ szerint kiválasztott központnál vesszük nyilvántartásba a berendezést.

17. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során nagyszámú központ közül a felhasználótól különböző személy által a berendezésben elhelyezett információ szerint kiválasztott központnál vesszük nyilvántartásba a berendezést.

18. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során egy berendezést egy első központnál nyilvántartásba veszünk, és nagyszámú központ közül egy, a tulajdonos által meghatározott információ szerint kiválasztott második központnál egy berendezést nyilvántartásba veszünk.

19. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során a berendezést a tulajdonos által meghatározott információ szerint korlátozott számban, többször hitelesítjük.

20. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során a berendezést egy központnál egy első berendezéstulajdonostól különböző második berendezéstulajdonos által meghatározott ellenőrzési információ szerint vesszük nyilvántartásba.

21. A 20. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második berendezéstulajdonos egy felhasználó.

22. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvántartásba vétel során a tulajdonost a központ számára azonosítjuk.

23. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a vevő egy tárolóberendezés.

24. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy az eljárás legalább egy műveleti lépéséhez bizalmas berendezésre van szükség, amely a műveleti lépésbe csak akkor kapcsolódik be, ha tulajdonosi információt helyezünk a bizalmas berendezésbe.

25. A 15. igénypont szerinti eljárás, *azzal jellemezve,* hogy a berendezés az eljárás egy műveleti lépését olyan utasítás hatására végzi el, amely a felhasználótól különböző személynek a berendezésbe beágyazott rejtjelkulcsával meg van erősítve.

26. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között harmadik fél általi hozzáféréssel, amelynek során nagyszámú letétbe helyezési központ közül legalább egynél az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat letétbe helyezzük, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy ellenőrzött rejtjelkulccsal bizalmas kommunikációt kezdeményezünk egy küldő felhasználótól egy vevő felhasználóhoz, amely kommunikáció tartalmaz a kezdeményező felhasználó rejtjelkulcsának és a vevő felhasználó rejtjelkulcsának visszanyerésére szolgáló információt.

27. A 26. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz a küldő felhasználó és a vevő felhasználó rejtjelkulcsainak letétbe helyezési központjait azonosító információt.

28. A 26. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz egy letétbe helyezési központhoz tartozó rejtjelkulccsal titkosított információt.

29. A 26. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá visszanyerünk egy letétbe helyezett rejtjelkulcsot, a visszanyert rejtjelkulcsot egy bizalmas berendezésben kívülről történő kiolvasás ellen védett módon biztonságosan eltároljuk, valamint a bizalmas berendezésben lévő rejtjelkulccsal egy kommunikációhoz hozzáférünk.

30. A 29. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférés során csak korlátozott időtartam alatt férünk hozzá biztonságos kommunikációkhoz, ahol az időtartam korlátozását a bizalmas berendezés végzi.

31. A 26. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá egy letétbe helyezett rejtjelkulcs szeleteit visszanyerjük, és a szeletekből egész rejtjelkulcsot állítunk elő.

32. A 26. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a bizalmas berendezés felülvizsgálati listát tart fenn a lehallgatott kommunikációkról.

33. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során külső behatás ellen védett logikával vezérelt elektronikus hardverberendezéseket gyártunk,

azzal jellemezve, hogy egy kezdeményező berendezéstől egy vevőhöz biztonságos kommunikációt kezdeményezünk, amely kommunikáció tartalmaz a kezdeményező berendezés által aláírt, egy kívülálló félnek a kommunikációhoz való hozzáférését megengedő hozzáférési információt.

34. A 33. igénypont szerinti eljárás, *azzal jellemezve,* hogy felhasználó általi külső behatás ellen védett, az ellenőrizhetően bizalmas kommunikációkat minősítő berendezéseket állítunk elő.

35. Eljárás ellenőrizhetően bizalmas kommunikáció létrehozására nagyszámú felhasználó között, *azzal jellemezve,* hogy egy első felhasználó elektronikus hardverberendezésében biztonságos kommunikációt hozunk létre, amely biztonságos kommunikáció tartalmaz egy kívülálló fél által a biztonságos kommunikációhoz való hozzáférést megengedő hozzáférési információt, a biztonságos kommunikációt az első felhasználó elektronikus hardverberendezése egy aláíró chipjének chipspecifikus egyéni aláírási rejtjelkulcsával aláírjuk, amely chipspecifikus egyéni aláírási rejtjelkulcsot az első felhasználó aláíró chipjéhez rendelt, illetéktelen hozzáférés ellen védett memóriába beágyazzuk, mielőtt az elektronikus hardverberendezést az első felhasználóhoz juttatjuk, a biztonságos kommunikációhoz igazolást csatolunk, amely igazolás tartalmaz az első felhasználó aláíróchipje egyéni aláírási rejtjelkulcsának megfelelő nyilvános aláírási rejtjelkulcsot, amely nyilvános aláírási rejtjelkulcs egy bizalmas hatóság egyéni aláírási rejtjelkulcsával alá van írva, valamint a biztonságos kommunikációt egy második felhasználóhoz továbbítjuk.

36. A 35. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a biztonságos kommunikációt a második felhasználó egy elektronikus hardverberendezésénél vesszük, és a bizalmas hatóság nyilvános aláírási rejtjelkulcsával ellenőrizzük az első felhasználó aláíróchipjének nyilvános aláírási rejtjelkulcsát.

37. A 36. igénypont szerinti eljárás, *azzal jellemezve,* hogy az igazolást az első felhasználó aláíróchipjének illetéktelen hozzáférés ellen védett memóriájába beágyazzuk, mielőtt az elektronikus hardverberendezést az első felhasználóhoz juttatjuk.

38. A 37. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas hatóság nyilvános aláírási rejtjelkulcsa a második felhasználó elektronikus hardverberendezése aláíróchipjének nem olvasható, illetéktelen hozzáférés ellen védett memóriájába be van ágyazva.

39. A 38. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas hatóság az első felhasználó aláíróchipjének gyártója.

40. A 38. igénypont szerinti eljárás, *azzal jellemezve,* hogy nagyszámú bizalmas hatóság nyilvános aláírási rejtjelkulcsa van a második felhasználó aláíróchipjének nem olvasható, illetéktelen hozzáférés ellen védett memóriájába beágyazva.

41. A 35. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá az első felhasználó elektronikus hardverberendezésében felhasználó specifikus nyilvános/egyéni titkosító/megfejtési rejtjelkulcspárt állítunk elő, és a biztonságos kommunikációt az első felhasználó elektronikus hardverberendezésében lévő egyéni titkosító rejtjelkulccsal titkosítjuk.

42. A 41. igénypont szerinti eljárás, *azzal jellemezve,* hogy a nyilvános/egyéni titkosító/megfejtési rejtjelkulcspárt RSA algoritmussal állítjuk elő.

43. A 42. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első felhasználó aláíróchipjének egyéni aláírási rejtjelkulcsát DSA algoritmussal állítjuk elő.

44. A 43. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas hatóság egyéni aláírási rejtjelkulcsát DSA algoritmussal állítjuk elő.

45. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy letétbe helyezési központnál az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevő felhasználóhoz kommunikációt kezdeményezünk a kezdeményező felhasználó bizalmas, a küldő és vevő felhasználók rejtjelkulcsainak hitelesítését jóváhagyó berendezésétől függően.

46. A 45. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezés magában eltárolja a letétbe helyezési központ egy rejtjelkulcsát, és a letétbe helyezési központ eltárolt rejtjelkulcsával jóváhagyja egy letétbe helyezési központ azon igazolását, amely igazolja, hogy egy vevő felhasználó rejtjelkulcsa ellenőrizve van.

47. A 45. igénypont szerinti eljárás, *azzal jellemezve,* hogy a letétbe helyezés, az ellenőrzés és a hitelesítés legalább egy műveleti lépését a bizalmas berendezéstől jövő kérelemre adott válaszként hajtjuk végre.

48. A 45. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezés egy hozzá rendelt rejtjelkulccsal aláír egy adatstruktúrát.

49. A 45. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a bizalmas berendezés generál egy letétbe helyezendő rejtjelkulcsot.

50. A 49. igénypont szerinti eljárás, *azzal jellemezve,* hogy a rejtjelkulcs kommunikációt titkosító rejtjelkulcs.

51. A 49. igénypont szerinti eljárás, *azzal jellemezve,* hogy a rejtjelkulcs aláírási rejtjelkulcs.

52. A 49. igénypont szerinti eljárás, *azzal jellemezve,* hogy legalább egy műveleti lépés bizalmas berendezést tesz szükségessé, és a bizalmas berendezés a műveleti lépést csak akkor hajtja végre, ha a hozzá rendelt felhasználótól különböző harmadik féltől felhatalmazó információt kap.

53. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál az egyes felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és a kommunikációban alkalmazott rejtjelkulcs hitelesítésétől függően egy kezdeményező felhasználótól egy vevő felhasználóhoz kívülálló fél kommunikációhoz való hozzá-

férését megengedő hozzáférési információt tartalmazó kommunikációt kezdeményezünk.

54. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmazza a vevő felhasználó rejtjelkulcsa letétbe helyezési központjának megnevezését.

55. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmazza a küldő felhasználó rejtjelkulcsa letétbe helyezési központjának megnevezését.

56. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmaz egy letétbe helyezési központnál letétbe helyezett rejtjelkulcs visszanyerésére szolgáló visszanyerési információt, amely visszanyerési információ a letétbe helyezési központ rejtjelkulcsával titkosítva van.

57. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz a küldő felhasználó rejtjelkulcsával titkosított üzenetrejtjelkulcsot.

58. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz a vevő felhasználó rejtjelkulcsával titkosított üzenetrejtjelkulcsot.

59. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz egy kommunikációban részt nem vevő fél rejtjelkulcsával titkosított üzenetrejtjelkulcsot.

60. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmaz a kommunikáció idejét jelző időinformációt.

61. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmazza a vevő felhasználó letétbe helyezési központjához tartozó földrajzi terület megnevezését.

62. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmazza a küldő felhasználó letétbe helyezési központjához tartozó földrajzi terület megnevezését.

63. Az 53. igénypont szerinti eljárás, *azzal jellemezve,* hogy a küldő felhasználó bizalmas berendezése egy hozzá rendelt rejtjelkulccsal aláírja a hozzáférési információt.

64. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a felhasználókhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat és felhasználókhoz rendelt bizalmas berendezéseket ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevőhöz kommunikációt kezdeményezünk a kommunikációban alkalmazott rejtjelkulcs hitelesítése és a kezdeményező felhasználóhoz rendelt bizalmas berendezés ismertetőjeleinek jóváhagyása után.

65. A 64. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a letétbe helyezési központ kibocsát egy igazolást egy felhasználó számára, amely igazolás tartalmazza a felhasználó rejtjelkulcsát és egy bizalmas berendezéshez rendelt rejtjelkulcsot.

66. A 64. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a letétbe helyezési központ kibocsát egy igazolást egy felhasználó számára, amely igazolás tartalmaz egy, a felhasználótól különböző, a felhasználót érintő kommunikációkhoz hozzáférő, választható, kívülálló felet megnevező információt.

67. A 64. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a letétbe helyezési központ kibocsát egy igazolást egy felhasználó számára, amely igazolás tartalmazza egy, a felhasználótól különböző, választható, kívülálló fél rejtjelkulcsát.

68. A 64. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a letétbe helyezési központ kibocsát egy igazolást, amely tartalmaz a letétbe helyezési központhoz rendelt földrajzi területet megnevező információt.

69. A 64. igénypont szerinti eljárás, *azzal jellemezve,* hogy a vevő egy tárolóberendezés.

70. Eljárás ellenőrizhetően bizalmas kommunikációk létrehozására nagyszámú felhasználó között, amelynek során bizalmas letétbe helyezési központoknál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központok egyik része egy első csoporthoz, másik része egy második csoporthoz tartozik, a letétbe helyezési központoknál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy első felhasználó és egy második felhasználó között attól függően kommunikálunk, hogy a küldő és vevő felhasználók letétbe helyezési központjai mely csoporthoz tartoznak.

71. A 70. igénypont szerinti eljárás, *azzal jellemezve,* hogy egy letétbe helyezési központ a csoportját egy felhasználó rejtjelkulcsát tartalmazó igazolásban nevezi meg.

72. A 70. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első felhasználó a második felhasználóhoz a második felhasználó egy igazolásában lévő letétbehelyezésiközpont-csoport megnevezése alapján kezdeményez kommunikációt.

73. A 70. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második felhasználó az első felhasználótól jövő kommunikációt az első felhasználó egy igazolásában lévő letétbehelyezésiközpont-csoport megnevezése alapján végzi el.

74. Eljárás ellenőrizhetően bizalmas, folyamirányított kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy kezdeményező felhasználótól egy vevő felhasználóhoz titkosított, folyamirányított kommunikációt hozunk létre a kezdeményező felhasználó titkosító rejtjelkulcsával, amely kommunikáció tartalmaz egy kívülálló fél számára a folyam megfejtését lehetővé tevő hozzáférési információt tartalmazó kezdeti csomagot, valamint egymás után következő csomagok folyamát, ahol az egymás után következő csomagok tartalmaznak a folyamhoz tartozó, soron következő csomagot azonosító információt, és ahol az egymás után következő cso-

magok közül legalább egy nem tartalmazza a hozzáférési információt.

75. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció tartalmaz továbbá a kommunikáció végét jelző információt tartalmazó lezárócsomagot.

76. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy az egymás után következő csomagok tartalmaznak továbbá a csomag sorozatban elfoglalt helyét jelző egyedi információt.

77. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy az egymás után következő csomagok tartalmaznak továbbá időbélyeg-információt.

78. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmazza a kezdeti csomag kivonatát.

79. A 78. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kezdeti csomag a kezdeményező felhasználó titkosító rejtjelkulcsával alá van írva.

80. A 79. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ tartalmaz továbbá üzenetazonosító információt.

81. A 80. igénypont szerinti eljárás, *azzal jellemezve,* hogy az egymás után következő csomagok közül legalább egy tartalmazza az üzenetazonosító információt.

82. A 81. igénypont szerinti eljárás, *azzal jellemezve,* hogy a folyamhoz tartozó, soron következő csomagot azonosító információ csomagsorszám.

83. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a kezdeményező felhasználónál a folyamirányított kommunikációt hordozó kommunikációs csatorna minőségére vonatkozó információt veszünk, és a kommunikációs csatorna minősége által meghatározott frekvenciával szelektív módon helyezünk el üzenetazonosító információt az egymás után következő csomagokban.

84. A 74. igénypont szerinti eljárás, *azzal jellemezve,* hogy a csomagok tartalmaznak azokat a kezdeményező felhasználóhoz rendelő információt.

85. Eljárás ellenőrizhetően bizalmas, folyamirányított kommunikációk létrehozására nagyszámú felhasználó között, amelynek során egy bizalmas letétbe helyezési központnál a nagyszámú felhasználóhoz rendelt aszimmetrikus rejtjelkulcsokat helyezünk letétbe, *azzal jellemezve,* hogy a letétbe helyezési központnál a rejtjelkulcsokat ellenőrizzük, a rejtjelkulcsokat ellenőrzéskor hitelesítjük, és egy vevő felhasználónál egy első titkosított, folyamirányított kommunikációt veszünk egy kezdeményező felhasználótól, amely kommunikáció a kezdeményező felhasználó titkosító rejtjelkulcsával van titkosítva, és amely első kommunikáció tartalmaz egy kívülálló fél számára a folyam megfejtését lehetővé tevő hozzáférési információt tartalmazó kezdeti csomagot, valamint egymás után következő csomagok folyamát, ahol az egymás után következő csomagok tartalmaznak a folyamhoz tartozó, soron következő csomagot azonosító információt, és ahol az első folyam egymás után következő csomagjai közül legalább egy nem tartalmazza a hozzáférési információt.

86. A 85. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a vevő felhasználótól a kezdeményező felhasználóhoz a vevő felhasználó titkosító rejtjelkulcsával második titkosított, folyamirányított kommunikációt állítunk elő, amely második kommunikáció tartalmaz egy kívülálló fél számára a második titkosított folyam megfejtését lehetővé tevő hozzáférési információt tartalmazó kezdeti csomagot, valamint egymás után következő csomagok folyamát, ahol az egymás után következő csomagok tartalmaznak a második folyamhoz tartozó, soron következő csomagot azonosító információt.

87. A 86. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második titkosított folyam hozzáférési információja tartalmazza a második titkosított folyam kezdeti csomagjának egy kivonatát, amely kivonat a vevő felhasználó titkosító rejtjelkulcsával alá van írva.

88. A 87. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második titkosított folyam hozzáférési információja tartalmaz a kezdeményező felhasználótól vett, üzenetazonosító információt.

89. A 86. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második titkosított folyam egymás után következő csomagjai közül legalább egy tartalmaz üzenetazonosító információt.

90. A 89. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második titkosított folyam egy soron következő csomagját azonosító információ csomagsorszám.

91. A 90. igénypont szerinti eljárás, *azzal jellemezve,* hogy a második titkosított folyam csomagjai tartalmaznak azokat a kezdeményező felhasználóhoz rendelő információt.

92. A 86. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a kezdeményező felhasználónál a folyamirányított kommunikációt hordozó kommunikációs csatorna minőségére vonatkozó információt veszünk, és a kommunikációs csatorna minősége által meghatározott frekvenciával szelektív módon helyezünk el üzenetazonosító információt az egymás után következő csomagokban.

93. A 92. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikációs csatorna minőségére vonatkozó információt folyamatosan vesszük, és azt a frekvenciát, amellyel az azonosító információt szelektív módon az egymás után következő csomagokban elhelyezzük, a vett információ alapján dinamikusan beállítjuk.

94. Eljárás bizalmas berendezés firmware-ének frissítésére, *azzal jellemezve,* hogy a bizalmas berendezésbe a firmware kibocsátójához rendelt rejtjelkulcsot ágyazunk be, a firmware-t kommunikáció keretében a bizalmas berendezéshez továbbítjuk, amely kommunikáció a firmware kibocsátója által a beágyazott rejtjelkulccsal jóváhagyható módon van módosítva, és a kommunikáció beágyazott rejtjelkulccsal történő jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

95. A 94. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware kibocsátója aláírja a kommunikációt, és

a bizalmas berendezés a beágyazott rejtjelkulccsal az aláírást ellenőrizve jóváhagyja a kommunikációt.

96. A 94. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware végrehajtható szoftverkódot tartalmaz.

97. A 94. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware titkosító rejtjelkulcsot tartalmaz.

98. A 94. igénypont szerinti eljárás, *azzal jellemezve,* hogy továbbá a firmware jóváhagyására szolgáló, nagyszámú rejtjelkulcsot ágyazunk be.

99. Eljárás bizalmas berendezés firmware-ének frissítésére, amelynek során a bizalmas berendezésnél firmware-t tartalmazó kommunikációt veszünk, *azzal jellemezve,* hogy a kommunikáció kibocsátóját egy, a bizalmas berendezésbe beágyazott rejtjelkulccsal jóváhagyjuk, amely rejtjelkulcs a kommunikáció kibocsátójához van rendelve, valamint a kommunikáció kibocsátójának jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

100. A 99. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezésbe beágyazott rejtjelkulcs a firmware kibocsátójának nyilvános aláírás-ellenőrzési rejtjelkulcsa, és a jóváhagyás során ellenőrizzük, hogy a kommunikáció alá lett-e írva a firmware kibocsátójának egyéni aláírási rejtjelkulcsával.

101. A 100. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware kibocsátója a bizalmas berendezés gyártója.

102. A 101. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware-t tartalmazó kommunikáció tartalmaz egy, a bizalmas berendezés firmware-ébe beágyazandó nyilvános aláírási rejtjelkulcsot.

103. A 99. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezésbe beágyazott rejtjelkulcs egy bizalmas hatóság nyilvános aláírás-ellenőrzési rejtjelkulcsa, és a jóváhagyás során a bizalmas hatóság nyilvános aláírás-ellenőrzési rejtjelkulcsával ellenőrizzük, hogy a kommunikáció tartalmaz-e a bizalmas hatóság egyéni aláírási rejtjelkulcsával aláírt frissítési igazolást, és hogy a frissítési igazolás tartalmazza-e a firmware kibocsátójának egy nyilvános aláírási rejtjelkulcsát.

104. A 103. igénypont szerinti eljárás, *azzal jellemezve,* hogy a jóváhagyás során továbbá a firmware kibocsátójának nyilvános aláírás-ellenőrzési rejtjelkulcsával ellenőrizzük, hogy a kommunikáció alá lett-e írva a firmware kibocsátójának egyéni aláírási rejtjelkulcsával.

105. A 104. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas hatóság a bizalmas berendezés gyártója, a firmware kibocsátója pedig bizalmas harmadik fél.

106. A 105. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware-t tartalmazó kommunikáció tartalmaz egy, a bizalmas berendezés firmware-ébe beágyazandó, nyilvános aláírás-ellenőrzési rejtjelkulcsot.

107. A 99. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware-t tartalmazó kommunikáció tartalmaz egy bizalmas harmadik félhez való, nyilvános aláírás-ellenőrzési rejtjelkulcsot.

108. A 107. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware-t tartalmazó kommunikáció tartalmaz továbbá a bizalmas harmadik fél által végrehajtható tranzakciókat azonosító információt.

109. A 108. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas harmadik fél fel van hatalmazva a firmware kibocsátója nyilvános aláírás-ellenőrzési rejtjelkulcsának kicserélésére.

110. A 109. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware kibocsátója a bizalmas berendezés gyártója.

111. Eljárás bizalmas berendezés firmware-ének frissítésére, amelynek során a bizalmas berendezésnél firmware-t tartalmazó kommunikációt veszünk, *azzal jellemezve,* hogy a kommunikáció kibocsátóját egy, a bizalmas berendezésbe beágyazott rejtjelkulccsal jóváhagyjuk, amely rejtjelkulcs egy bizalmas személyhez van rendelve, ahol is a jóváhagyás során ellenőrizzük, hogy a kommunikáció tartalmaz-e a bizalmas személy egyéni aláírási rejtjelkulcsával aláírt frissítési igazolást, ahol a frissítési igazolás tartalmazza a firmware kibocsátójának nyilvános aláírási rejtjelkulcsát, továbbá a firmware kibocsátójának nyilvános aláírás-ellenőrzési rejtjelkulcsával ellenőrizzük, hogy a kommunikáció alá lett-e írva a firmware kibocsátójának egyéni aláírási rejtjelkulcsával, valamint a firmware kibocsátójának jóváhagyásától függően a firmware-t a bizalmas berendezésbe beágyazzuk.

112. A 111. igénypont szerinti eljárás, *azzal jellemezve,* hogy a firmware-t tartalmazó kommunikáció tartalmaz egy, a bizalmas személyhez való, nyilvános aláírás-ellenőrzési rejtjelkulcsot.

113. A 112. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas személy a bizalmas berendezés gyártója.

114. Eljárás titkosított kommunikációhoz kommunikáló feleket és a kommunikációban részt nem vevő fél által visszanyerhető üzenetrejtjelkulcsot tartalmazó rendszerben, amelynek során a felhasználókat ellátjuk számítógépes hardverberendezésekkel, amely berendezések legalább egy hozzájuk rendelt rejtjelkulccsal rendelkeznek, *azzal jellemezve,* hogy nagyszámú központ közül legalább egy kiválasztott központnál a hardver berendezéseket nyilvántartásba vesszük, a hardverberendezéseket hitelesítjük, amely hitelesítés a berendezés számára igazolást állít elő, és egy üzenetrejtjelkulccsal egy kezdeményező felhasználótól egy vevőhöz biztonságos, az üzenetrejtjelkulcs visszanyerésére a központ rejtjelkulcsával titkosított hozzáférési részt tartalmazó kommunikációt kezdeményezünk.

115. A 114. igénypont szerinti eljárás, *azzal jellemezve,* hogy a központ rejtjelkulcsával titkosított hozzáférési rész tartalmaz egy, a központnál letétbe helyezett rejtjelkulcsot azonosító információt.

116. A 114. igénypont szerinti eljárás, *azzal jellemezve,* hogy az igazolás egy nyilvános/egyéni rejtjelkulcspár nyilvános rejtjelkulcsát tartalmazza.

117. A 114. igénypont szerinti eljárás, *azzal jellemezve,* hogy a hozzáférési információ a nagyszámú központ számára tartalmaz az üzenetrejtjelkulcs visszanyerésére szolgáló információt.

118. A 114. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció során egy bizalmas berendezés a felhasználó által történő illetéktelen hozzáférésnek ellenálló módon tartalmaz hozzáférési információt.

119. A 114. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kommunikáció során egy első központ rejtjelkulcsával titkosítunk hozzáférési információt, és egy második központ rejtjelkulcsával titkosítunk hozzáférési információt.

120. Eljárás bizalmas berendezés meghatalmazására egy első felhasználó és egy második fél közötti elektronikus tranzakció levezetésére, amelynek során biztosítjuk, hogy a bizalmas berendezés előre meghatározott, a felhasználó által nem megváltoztatható szabályok szerint kapcsolódik be az elektronikus tranzakcióba, *azzal jellemezve,* hogy a bizalmas berendezéstől harmadik félhez elektronikusan továbbítunk az elektronikus tranzakcióba való bekapcsolódásra vonatkozó, a bizalmas berendezés azonosítását tartalmazó meghatalmazási kérelmet, a harmadik féllel eldöntjük, hogy a bizalmas berendezés meghatalmazható-e a tranzakcióba történő bekapcsolódásra legalább részben annak vizsgálatával, hogy a bizalmas berendezés kizárólag a szabályok szerint fog-e működni, a harmadik féltől a bizalmas berendezéshez elektronikusan a tranzakcióba történő bekapcsolódásra vonatkozó meghatalmazást továbbítunk, amely meghatalmazás a harmadik fél általi kibocsátásra vonatkozó igazolást tartalmaz, az igazolást a bizalmas berendezéstől a második félhez elektronikusan továbbítjuk annak biztosítékaként, hogy a bizalmas berendezés meghatalmazással rendelkezik az elektronikus tranzakcióba való bekapcsolódásra, és hogy ezt kizárólag a szabályok szerint teszi meg, valamint a bizalmas berendezéstől a második félhez a szabályok szerint elektronikusan tranzakciós adatot továbbítunk.

121. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a meghatalmazás továbbítása során a harmadik féltől a bizalmas berendezéshez a szabályokat továbbítjuk.

122. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezés a meghatalmazás továbbítása előtt már tartalmazza a szabályokat.

123. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a meghatalmazás továbbítása során a harmadik fél digitális aláírását hozzácsatoljuk az igazoláshoz.

124. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a kérelem továbbítása során a bizalmas berendezés azonosítására vonatkozó igazolást továbbítunk, amely igazolás a bizalmas berendezés gyártója által digitálisan alá van írva.

125. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a döntés során a bizalmas berendezés azonosítása alapján eldöntjük, hogy bizalmas berendezés illetéktelen hozzáférés ellen védett-e.

126. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezés rendelkezik hozzá rendelt, egy aszimmetrikus titkosítórendszerhez tartozó nyilvános rejtjelkulccsal és egyéni rejtjelkulccsal, valamint a kérelem továbbítása során a berendezés nyilvános rejtjelkulcsát a harmadik félhez továbbítjuk.

127. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy a bizalmas berendezés rendelkezik hozzá rendelt, egy aszimmetrikus titkosítórendszerhez tartozó első rejtjelkulccsal és második rejtjelkulccsal, valamint a tranzakciós adatnak a második félhez történő továbbítása során a bizalmas berendezés első rejtjelkulcsával létrehozott digitális aláírását a tranzakciós adathoz csatoljuk.

128. A 120. igénypont szerinti eljárás, *azzal jellemezve,* hogy az azonosításra vonatkozó igazolás tartalmazza egy, a bizalmas berendezéshez tartozó nyilvános/egyéni rejtjelkulcspár nyilvános rejtjelkulcsát, és a kérelem továbbítása során a kérelemhez csatoljuk a bizalmas berendezésnek az egyéni rejtjelkulccsal létrehozott digitális aláírását, és így a harmadik fél meg tud bizonyosodni arról, hogy a kérelem a bizalmas berendezéstől jött-e.

129. A 127. igénypont szerinti eljárás, *azzal jellemezve,* hogy a tranzakciós adatnak a második félhez történő továbbítása során a második rejtjelkulcsot továbbítjuk a második félhez.

130. A 127. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első berendezés-rejtjelkulcs egyéni rejtjelkulcs, a második berendezés-rejtjelkulcs pedig nyilvános rejtjelkulcs.

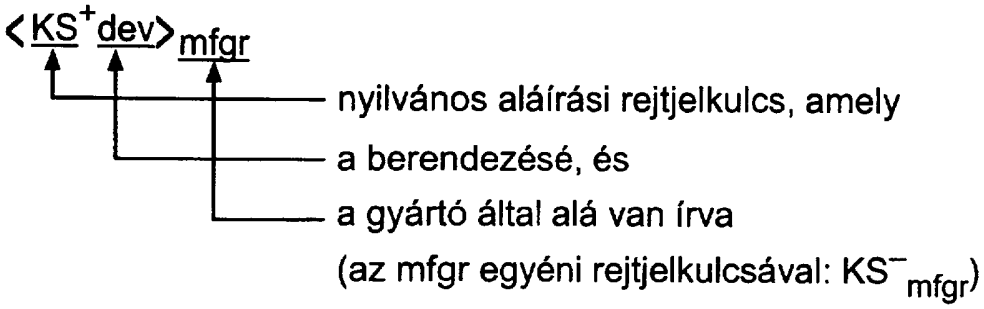
131. A 125. igénypont szerinti eljárás, *azzal jellemezve,* hogy az első berendezés-rejtjelkulcs egyéni rejtjelkulcs, a második berendezés-rejtjelkulcs pedig nyilvános rejtjelkulcs.

X	a vevő egyéni rejtjelkulcsa (exponens)
X1..n	az egyéni rejtjelkulcs számozott szeletei
Xi	a titkos rejtjelkulcs i-edik szelete
y	a küldő ideiglenes egyéni rejtjelkulcsa (exponens)
a	nyilvános alap
p	nyilvános prím kitevő
DHx	közbenső szám = a^x mod p
DHy	közbenső szám = a^y mod p
Kdh	Diffie-Hellman szerinti üzenet rejtjelkulcs
V1..n	Micali közbenső szám = a^{xi} mod p
Kmsg	Véletlen vagy levezetett üzenet rejtjelkulcs
M	titkosítatlan üzenet
C	titkosított üzenet

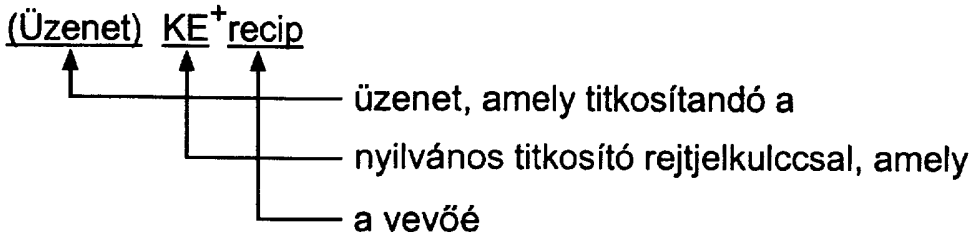
1A ábra

	Nyilvános	Egyéni
Aláírási	KS^+	KS^-
Titkosító	KE^+	KE^-

1B ábra



1C ábra



1D ábra

box		törvényes ellenőrzési dekóder doboz
ca	ca1...n	hitelesítő hatóság (a nyilvános aláírási rejtjelkulcsokhoz)
dev		bizalmas berendezés
ea	ea1...n	letétbehelyezési ügynök
ec	ec1...n	letétbehelyezési központ
mfgr	mfgr1...n	a bizalmas berendezés gyártója
owner		a berendezés tulajdonosa (ha más mint a felhasználó)
recip		az üzenet vevője
sender		az üzenet küldője
swa		egész rendszert átfogó hatóság
user	user1...n	a bizalmas berendezés felhasználója

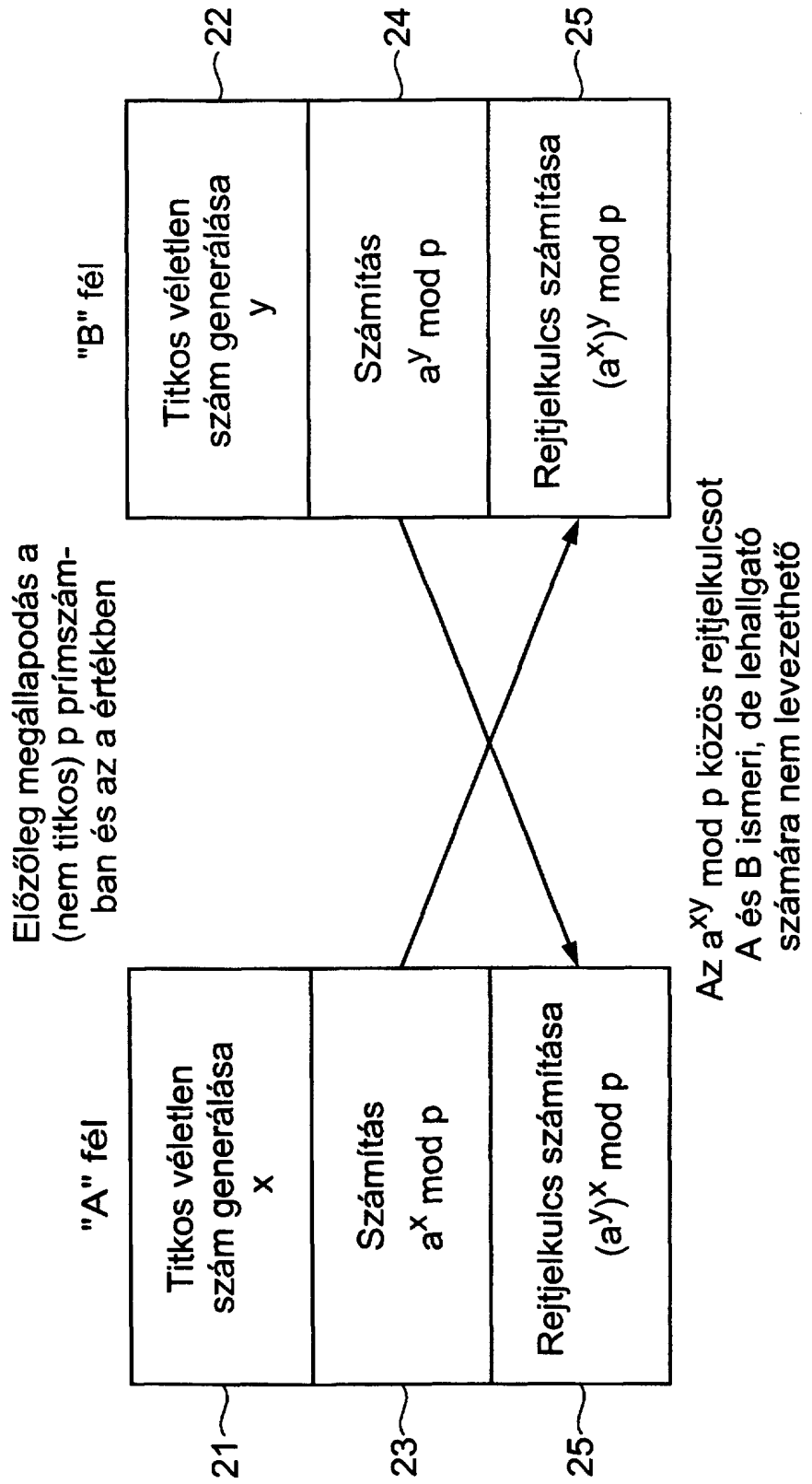
1E ábra

$$\langle adat \rangle_{dev} \text{ (or) } \boxed{adat_{-dev}} = \langle adat \rangle KS^{-}_{dev}$$

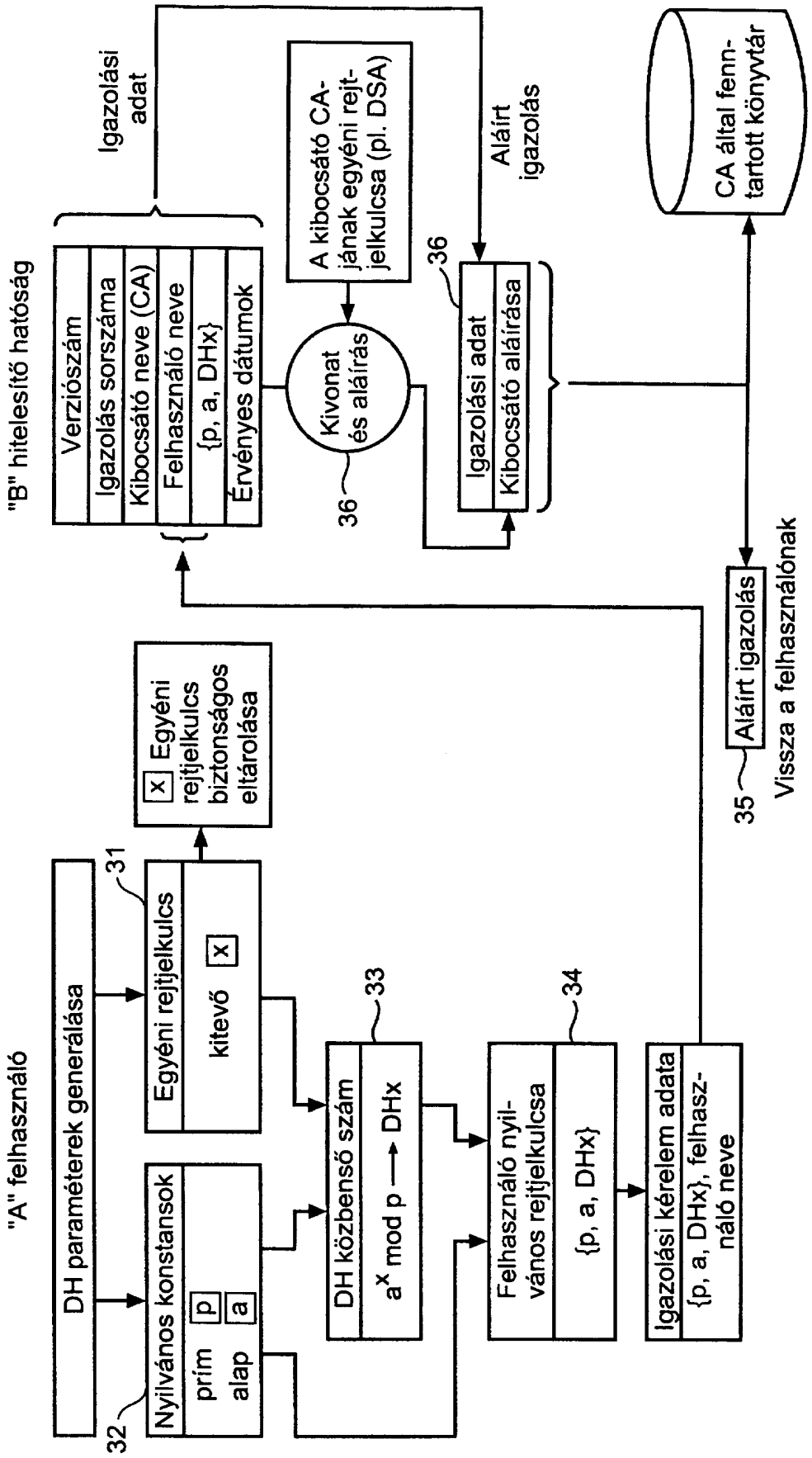
1F ábra

$$(adat)_{sender} = (adat)KE^{+} \text{ sender}$$

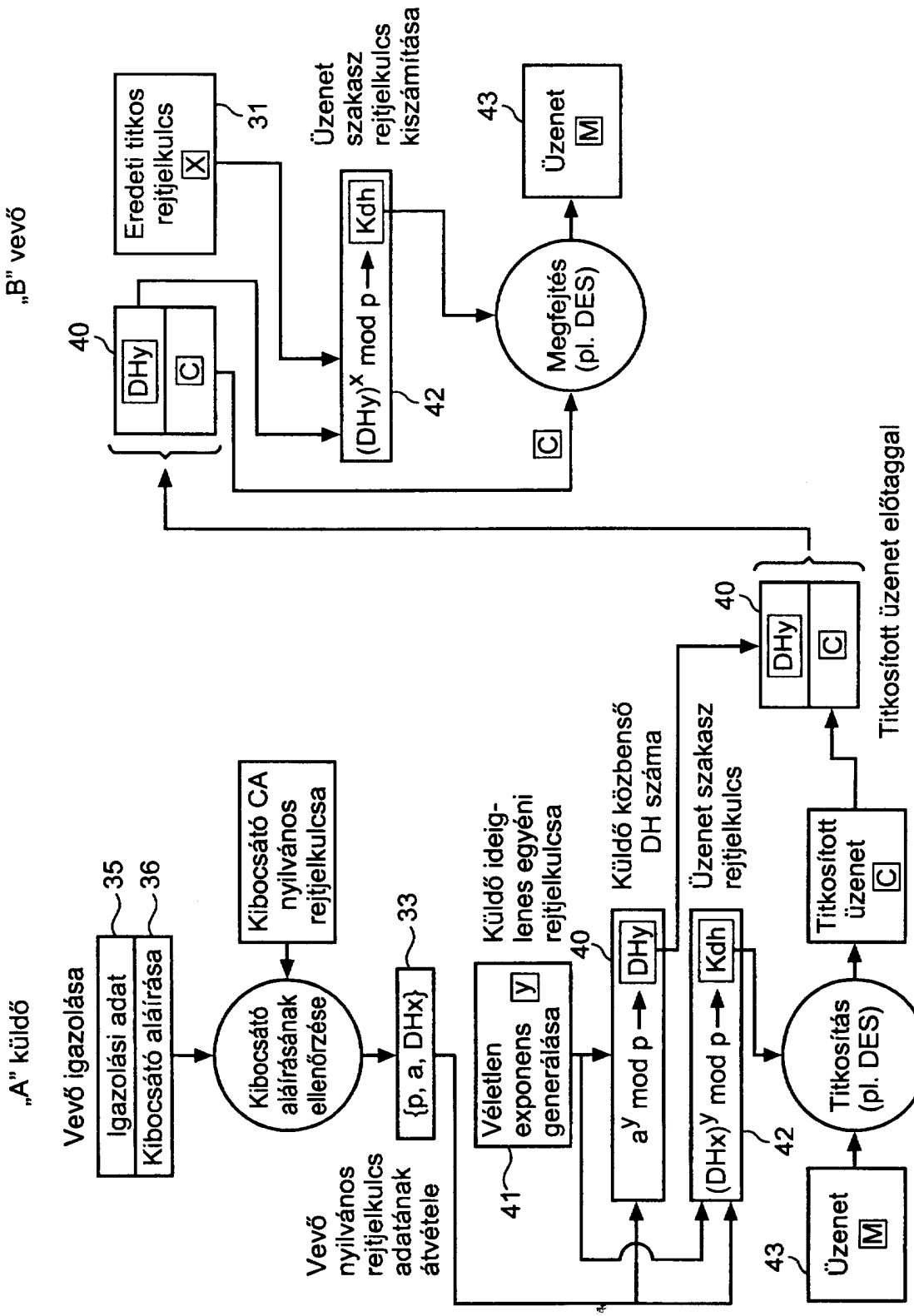
1G ábra


"A" fél
"B" fél
Előzőleg megállapodás a (nem titkos) p prímszámban és az a értékben
Titkos véletlen szám generálása x
Számítás a^x mod p
Rejtjelkulcs számítása $(a^y)^x$ mod p
Titkos véletlen szám generálása y
Számítás a^y mod p
Rejtjelkulcs számítása $(a^x)^y$ mod p
Az a^{xy} mod p közös rejtjelkulcsot A és B ismeri, de lehallgató számára nem levezethető
21
23
25
22
24
25

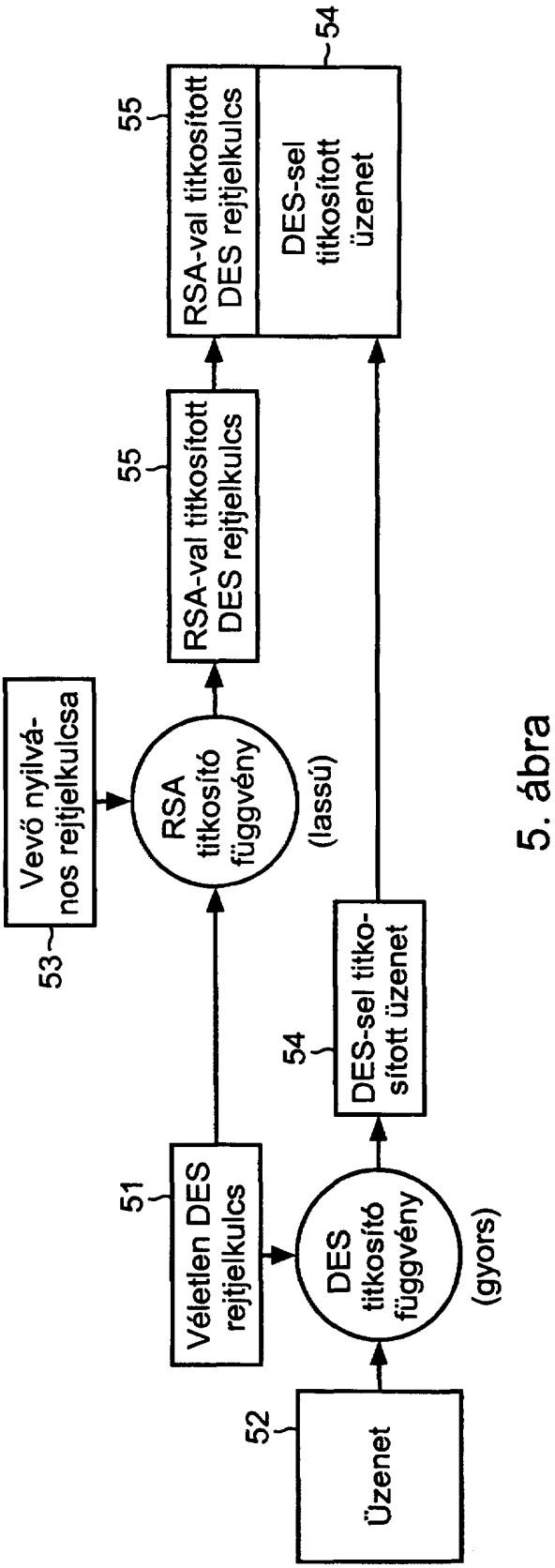
2. ábra


"A" felhasználó
DH paraméterek generálása
Nyilvános konstansok
prím p
alap a
Egyéni rejtjelkulcs
kitevő x
x Egyéni rejtjelkulcs biztonságos eltárolása
DH közbenső szám
a^x mod p → DHx
Felhasználó nyilvános rejtjelkulcsa
{p, a, DHx}
Igazolási kérelem adata
{p, a, DHx}, felhasználó neve
31
32
33
34
35
Aláírt igazolás
Vissza a felhasználónak
"B" hitelesítő hatóság
Verziószám
Igazolás sorszáma
Kibocsátó neve (CA)
Felhasználó neve
{p, a, DHx}
Érvényes dátumok
Igazolási adat
Kivonat és aláírás
36
A kibocsátó CA-jának egyéni rejtjelkulcsa (pl. DSA)
Igazolási adat
Aláírt igazolás
Kibocsátó aláírása
CA által fenntartott könyvtár

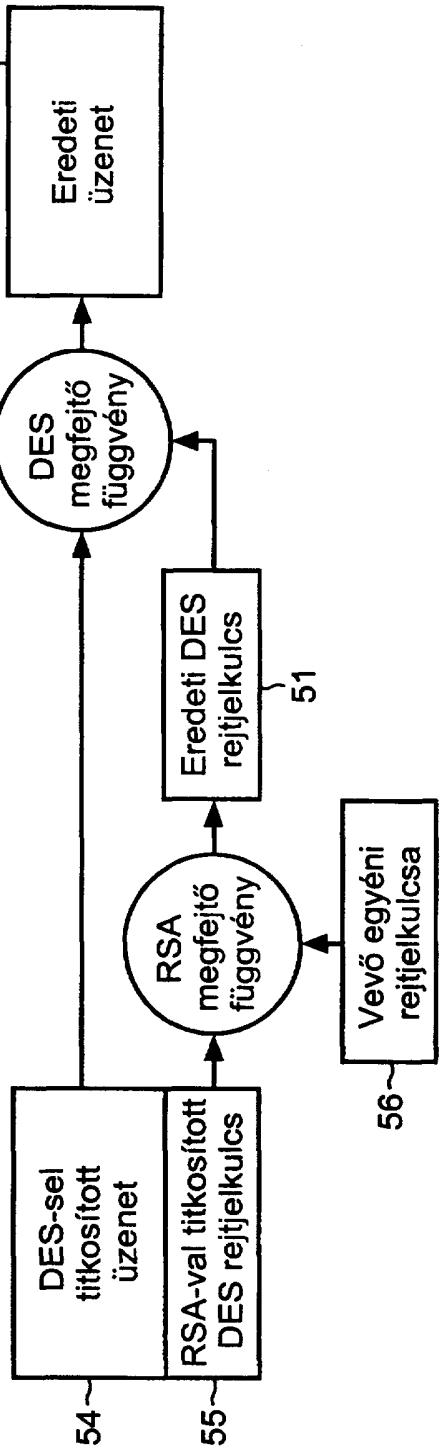
3. ábra


„A" küldő
„B" vevő
Vevő igazolása
Igazolási adat
Kibocsátó aláírása
35
36
Kibocsátó CA nyilvános rejtjelkulcsa
Kibocsátó aláírásának ellenőrzése
33
{p, a, DHx}
Vevő nyilvános rejtjelkulcs adatának átvétele
Véletlen exponens generálása
Y
41
Küldő ideig-lenes egyéni rejtjelkulcsa
40
a^y mod p → DHy
Küldő közbenső DH száma
$(DHx)^y$ mod p → Kdh
Üzenet szakasz rejtjelkulcs
42
Titkosítás (pl. DES)
Titkosított üzenet
C
Titkosított üzenet előtaggal
Üzenet
M
43
Eredeti titkos rejtjelkulcs
X
31
Üzenet szakasz rejtjelkulcs kiszámítása
$(DHy)^x$ mod p → Kdh
Megfejtés (pl. DES)

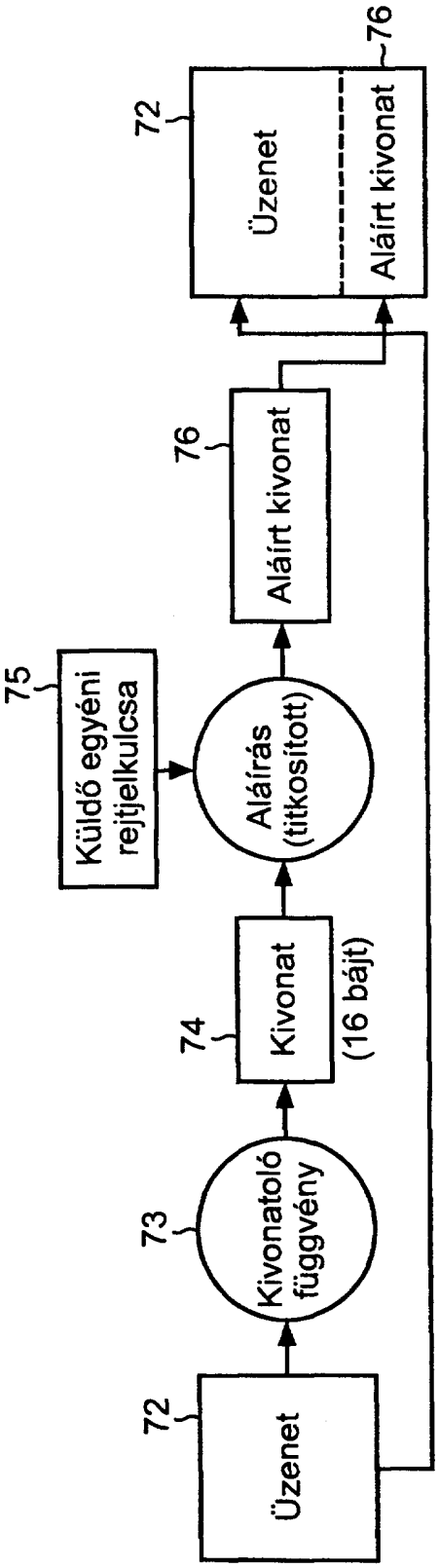
4. ábra


Üzenet
52
Véletlen DES rejtjelkulcs
51
DES titkosító függvény
(gyors)
DES-sel titkosított üzenet
54
Vevő nyilvános rejtjelkulcsa
53
RSA titkosító függvény
(lassú)
RSA-val titkosított DES rejtjelkulcs
55
RSA-val titkosított DES rejtjelkulcs
55
DES-sel titkosított üzenet
54

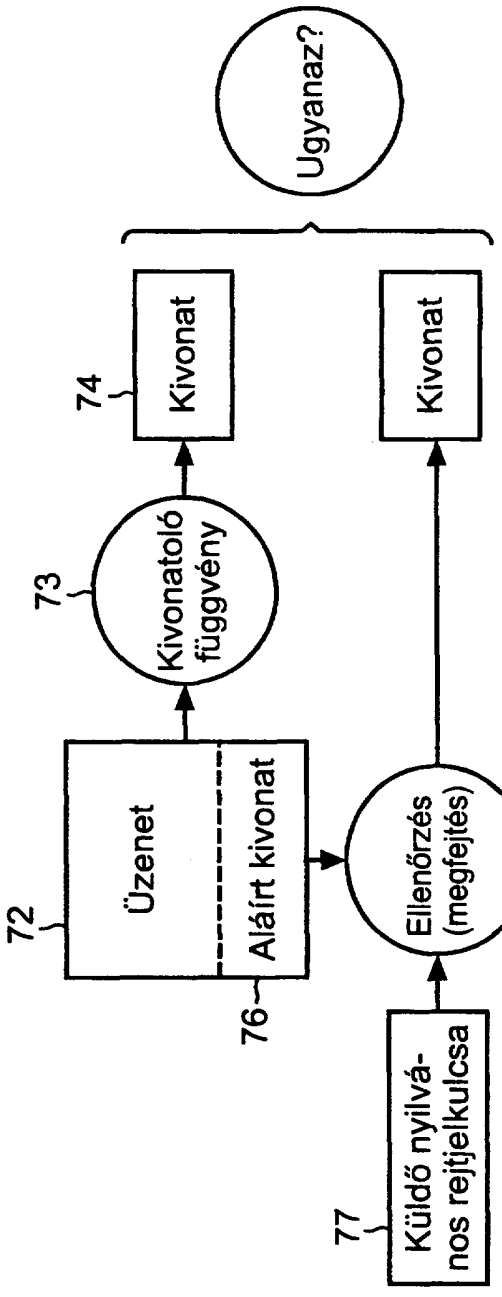
5. ábra


DES-sel titkosított üzenet
54
RSA-val titkosított DES rejtjelkulcs
55
RSA megfejtő függvény
Vevő egyéni rejtjelkulcsa
56
Eredeti DES rejtjelkulcs
51
DES megfejtő függvény
Eredeti üzenet
52

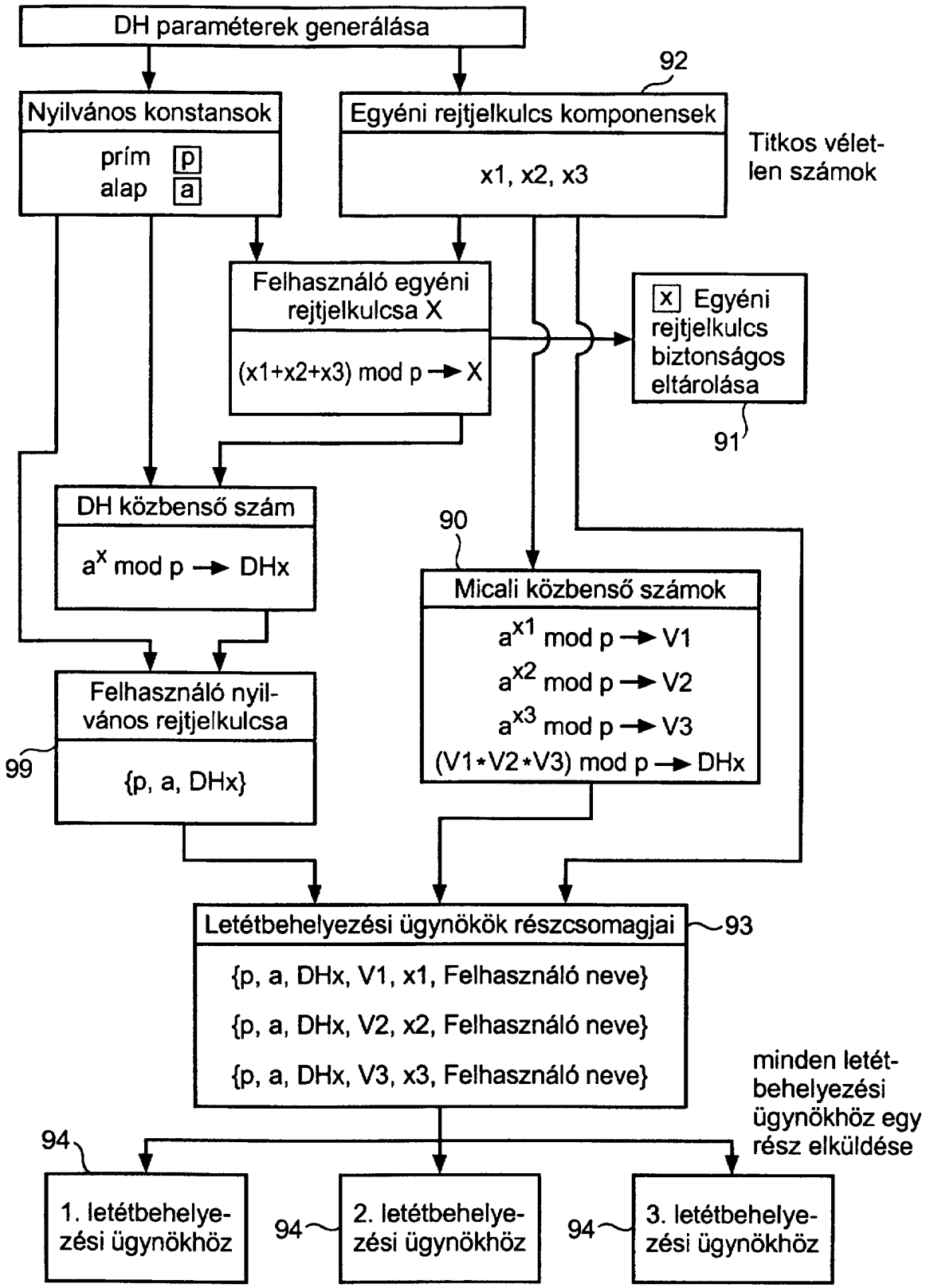
6. ábra


72
Üzenet
73
Kivonatoló függvény
74
Kivonat
(16 bájt)
75
Küldő egyéni rejtjelkulcsa
Aláírás (titkosított)
76
Aláírt kivonat
72
Üzenet
Aláírt kivonat
76

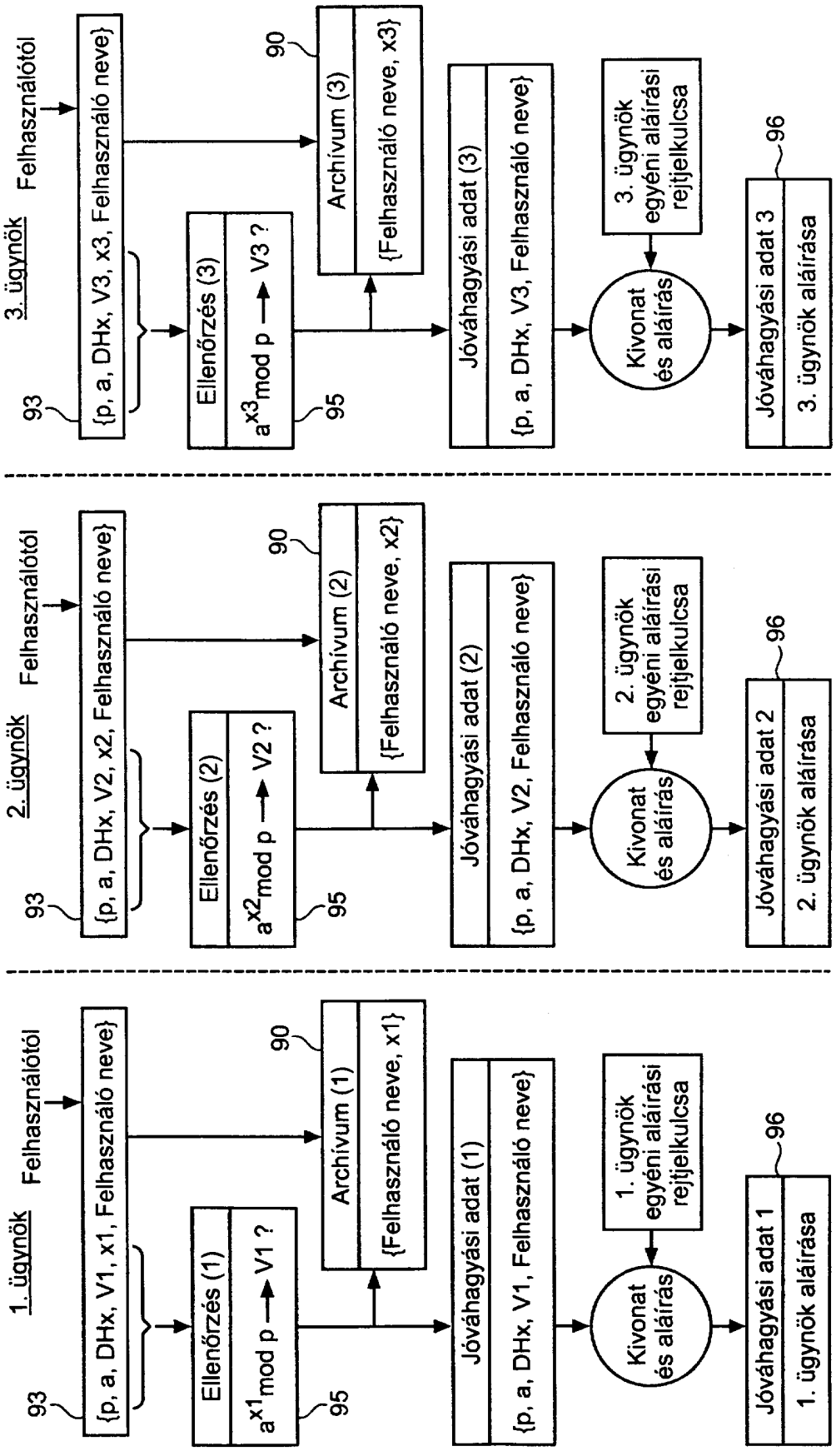
7. ábra


72
Üzenet
Aláírt kivonat
76
73
Kivonatoló függvény
74
Kivonat
Ugyanaz?
Ellenőrzés (megfejtés)
Kivonat
77
Küldő nyilvá-nos rejtjelkulcsa

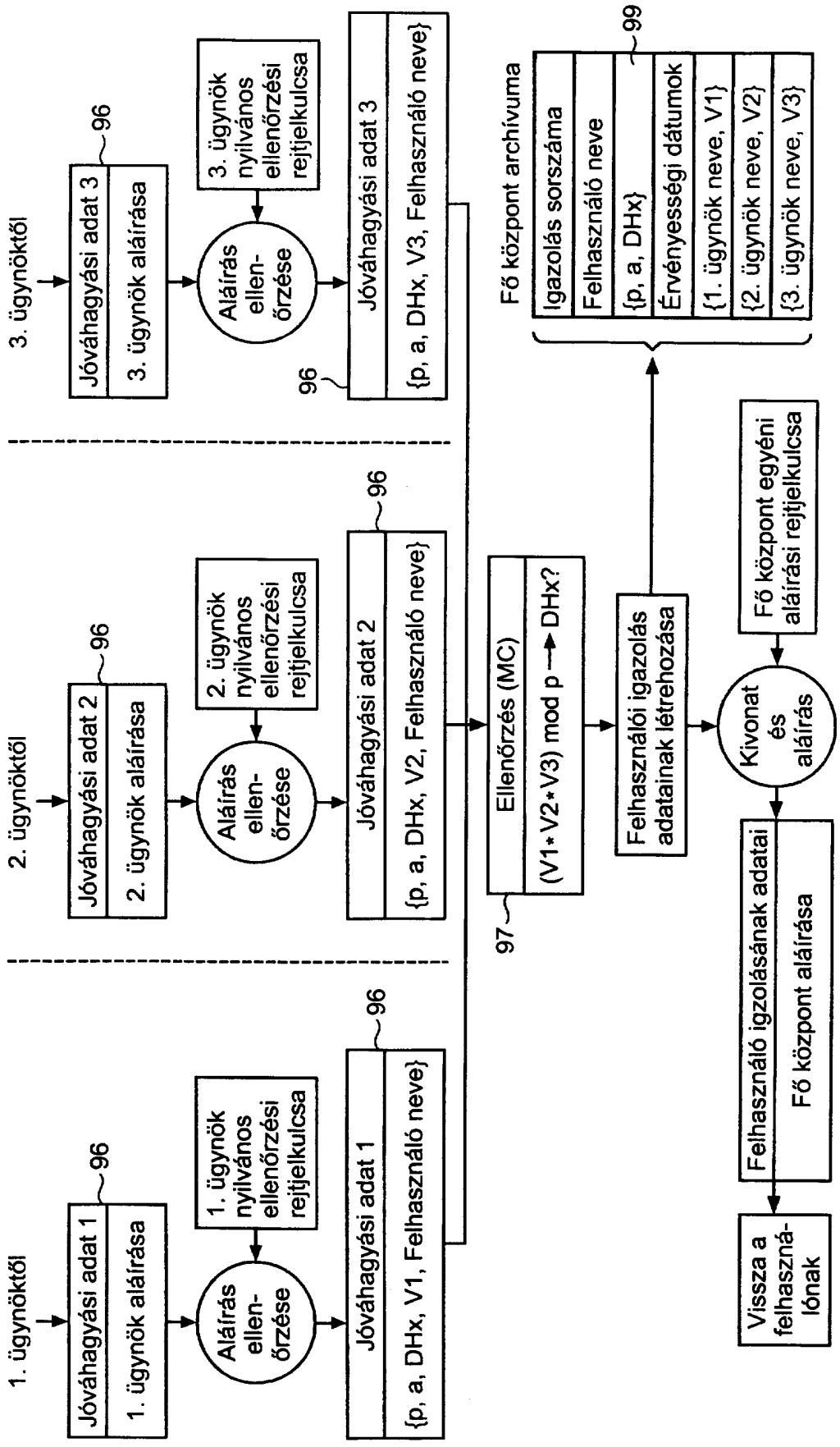
8. ábra


DH paraméterek generálása
92
Nyilvános konstansok
prím p
alap a
Egyéni rejtjelkulcs komponensek
x1, x2, x3
Titkos véletlen számok
Felhasználó egyéni rejtjelkulcsa X
(x1+x2+x3) mod p → X
X Egyéni rejtjelkulcs biztonságos eltárolása
91
DH közbenső szám
a^x mod p → DHx
90
Micali közbenső számok
a^x1 mod p → V1
a^x2 mod p → V2
a^x3 mod p → V3
(V1*V2*V3) mod p → DHx
Felhasználó nyilvános rejtjelkulcsa
99
{p, a, DHx}
Letétbehelyezési ügynökök részcsomagjai
93
{p, a, DHx, V1, x1, Felhasználó neve}
{p, a, DHx, V2, x2, Felhasználó neve}
{p, a, DHx, V3, x3, Felhasználó neve}
minden letétbehelyezési ügynökhöz egy rész elküldése
94
1. letétbehelyezési ügynökhöz
94
2. letétbehelyezési ügynökhöz
94
3. letétbehelyezési ügynökhöz

9. ábra

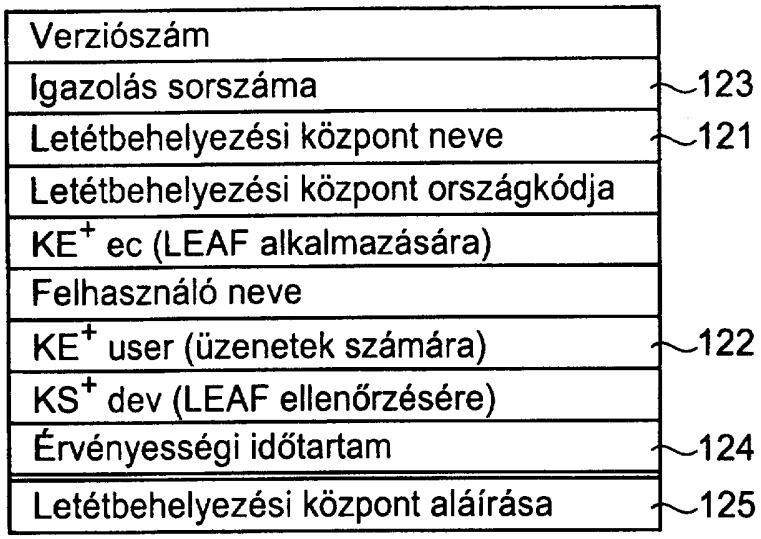

1. ügynök
Felhasználótól
{p, a, DHx, V1, x1, Felhasználó neve}
93
Ellenőrzés (1)
$a^{x1} \bmod p \rightarrow V1$?
95
Archívum (1)
{Felhasználó neve, x1}
90
Jóváhagyási adat (1)
{p, a, DHx, V1, Felhasználó neve}
1. ügynök egyéni aláírási rejtjelkulcsa
Kivonat és aláírás
Jóváhagyási adat 1
1. ügynök aláírása
96
2. ügynök
Felhasználótól
{p, a, DHx, V2, x2, Felhasználó neve}
93
Ellenőrzés (2)
$a^{x2} \bmod p \rightarrow V2$?
95
Archívum (2)
{Felhasználó neve, x2}
90
Jóváhagyási adat (2)
{p, a, DHx, V2, Felhasználó neve}
2. ügynök egyéni aláírási rejtjelkulcsa
Kivonat és aláírás
Jóváhagyási adat 2
2. ügynök aláírása
96
3. ügynök
Felhasználótól
{p, a, DHx, V3, x3, Felhasználó neve}
93
Ellenőrzés (3)
$a^{x3} \bmod p \rightarrow V3$?
95
Archívum (3)
{Felhasználó neve, x3}
90
Jóváhagyási adat (3)
{p, a, DHx, V3, Felhasználó neve}
3. ügynök egyéni aláírási rejtjelkulcsa
Kivonat és aláírás
Jóváhagyási adat 3
3. ügynök aláírása
96

10. ábra

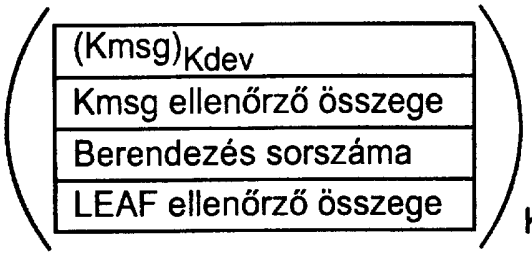

1. ügynöktől
Jóváhagyási adat 1
1. ügynök aláírása
96
Aláírás ellen-őrzése
1. ügynök nyilvános ellenőrzési rejtjelkulcsa
Jóváhagyási adat 1
{p, a, DHx, V1, Felhasználó neve}
96
2. ügynöktől
Jóváhagyási adat 2
2. ügynök aláírása
96
Aláírás ellen-őrzése
2. ügynök nyilvános ellenőrzési rejtjelkulcsa
Jóváhagyási adat 2
{p, a, DHx, V2, Felhasználó neve}
96
3. ügynöktől
Jóváhagyási adat 3
3. ügynök aláírása
96
Aláírás ellen-őrzése
3. ügynök nyilvános ellenőrzési rejtjelkulcsa
Jóváhagyási adat 3
{p, a, DHx, V3, Felhasználó neve}
96
Ellenőrzés (MC)
(V1*V2*V3) mod p → DHx?
97
Felhasználói igazolás adatainak létrehozása
Fő központ archívuma
Igazolás sorszáma
Felhasználó neve
{p, a, DHx}
Érvényességi dátumok
{1. ügynök neve, V1}
{2. ügynök neve, V2}
{3. ügynök neve, V3}
99
Fő központ egyéni aláírási rejtjelkulcsa
Kivonat és aláírás
Felhasználó igzolásának adatai
Fő központ aláírása
Vissza a felhasználónak

11. ábra

12. ábra

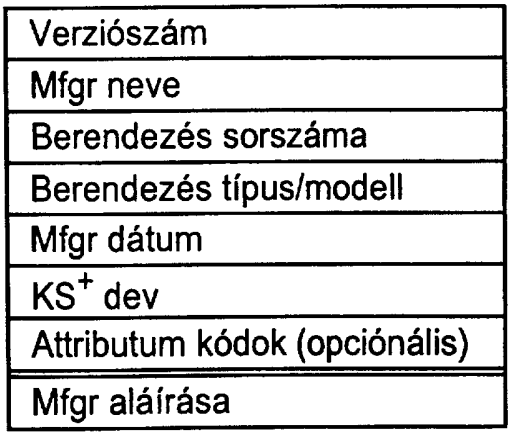


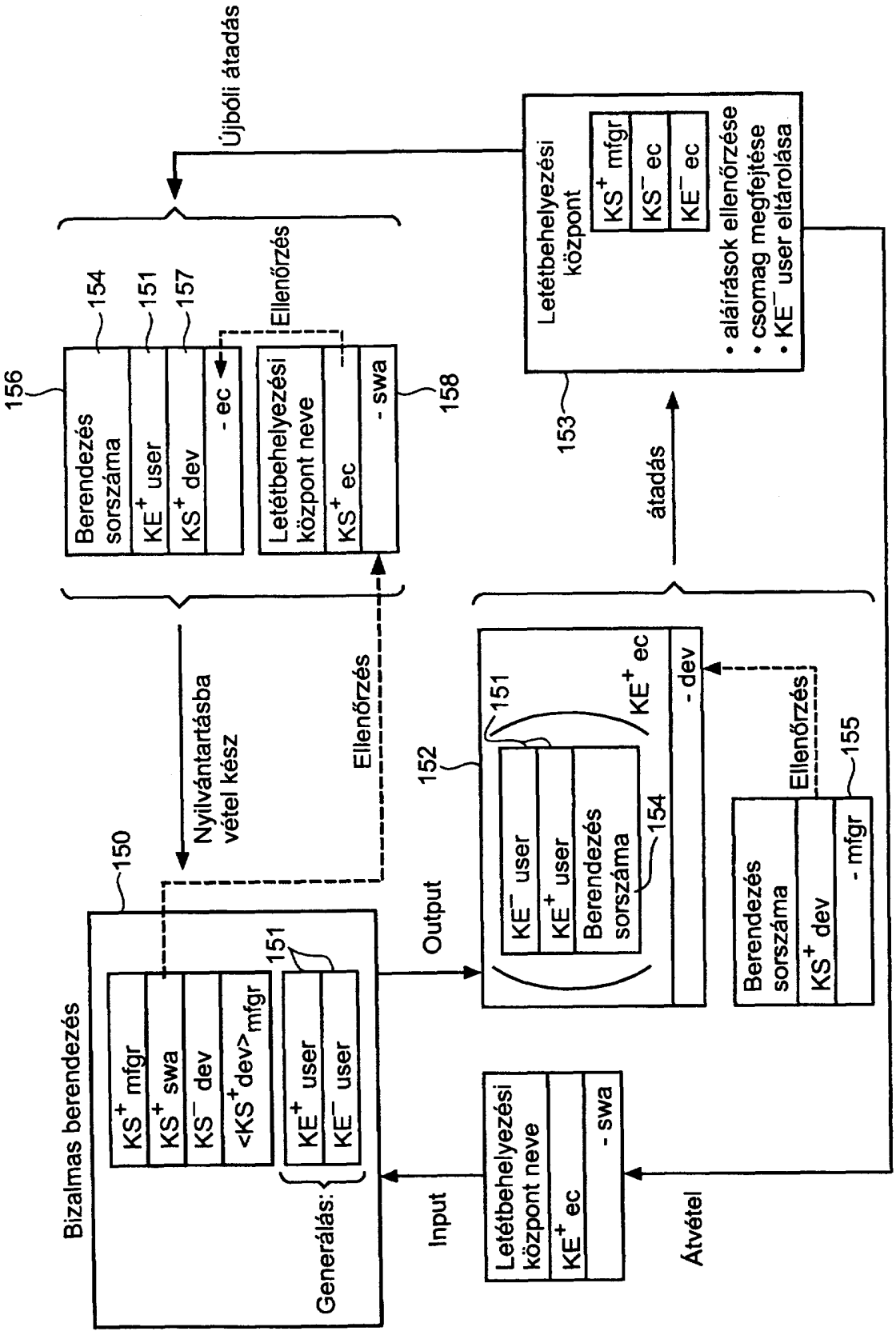
13. ábra



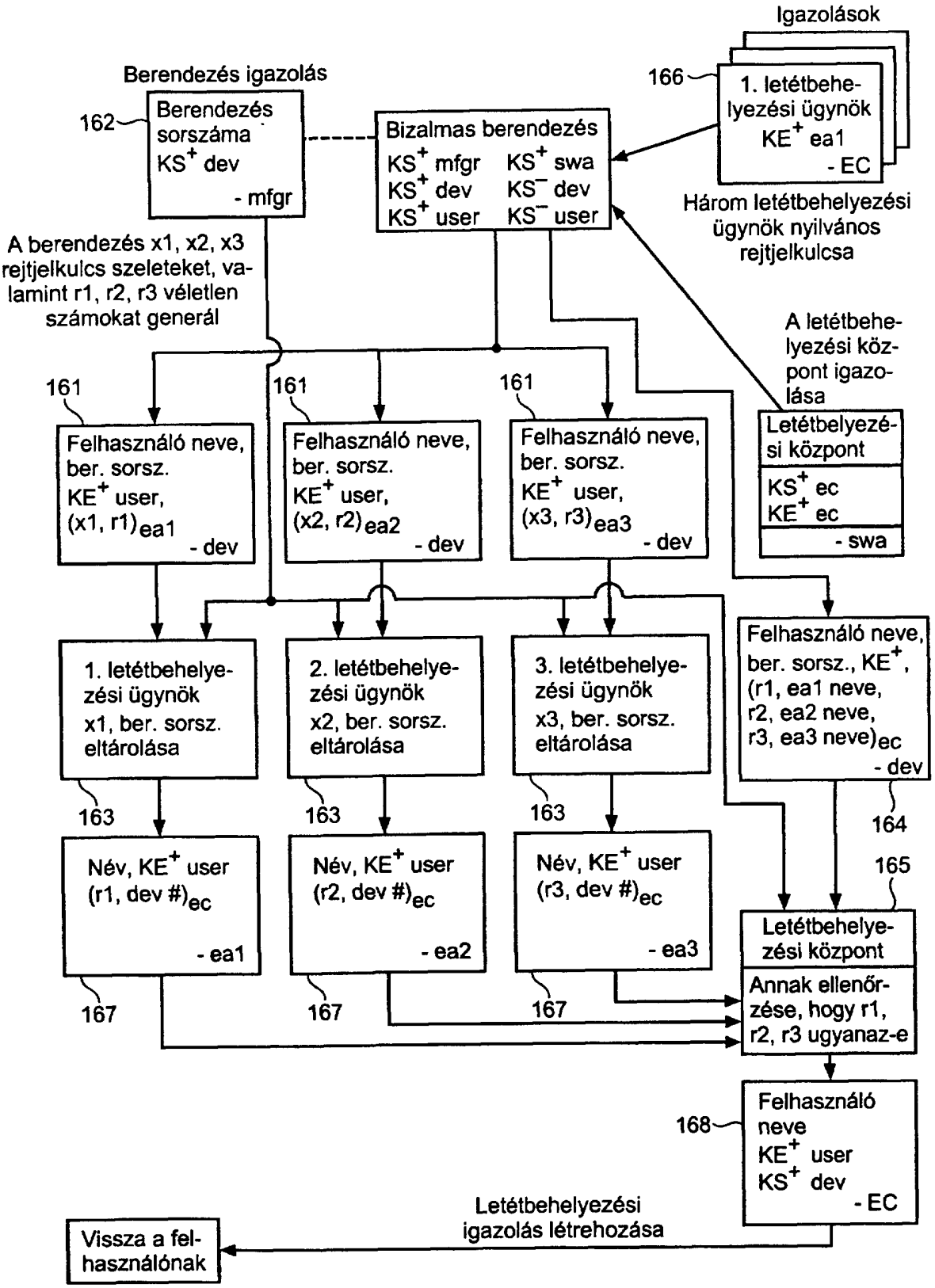
Kmsg	Szimmetrikus üzenet rejtjelkulcs
Kdev	Beágyazott szimmetrikus berendezés rejtjelkulcs
Kfam	Szimmetrikus Clipper család rejtjelkulcs

14. ábra

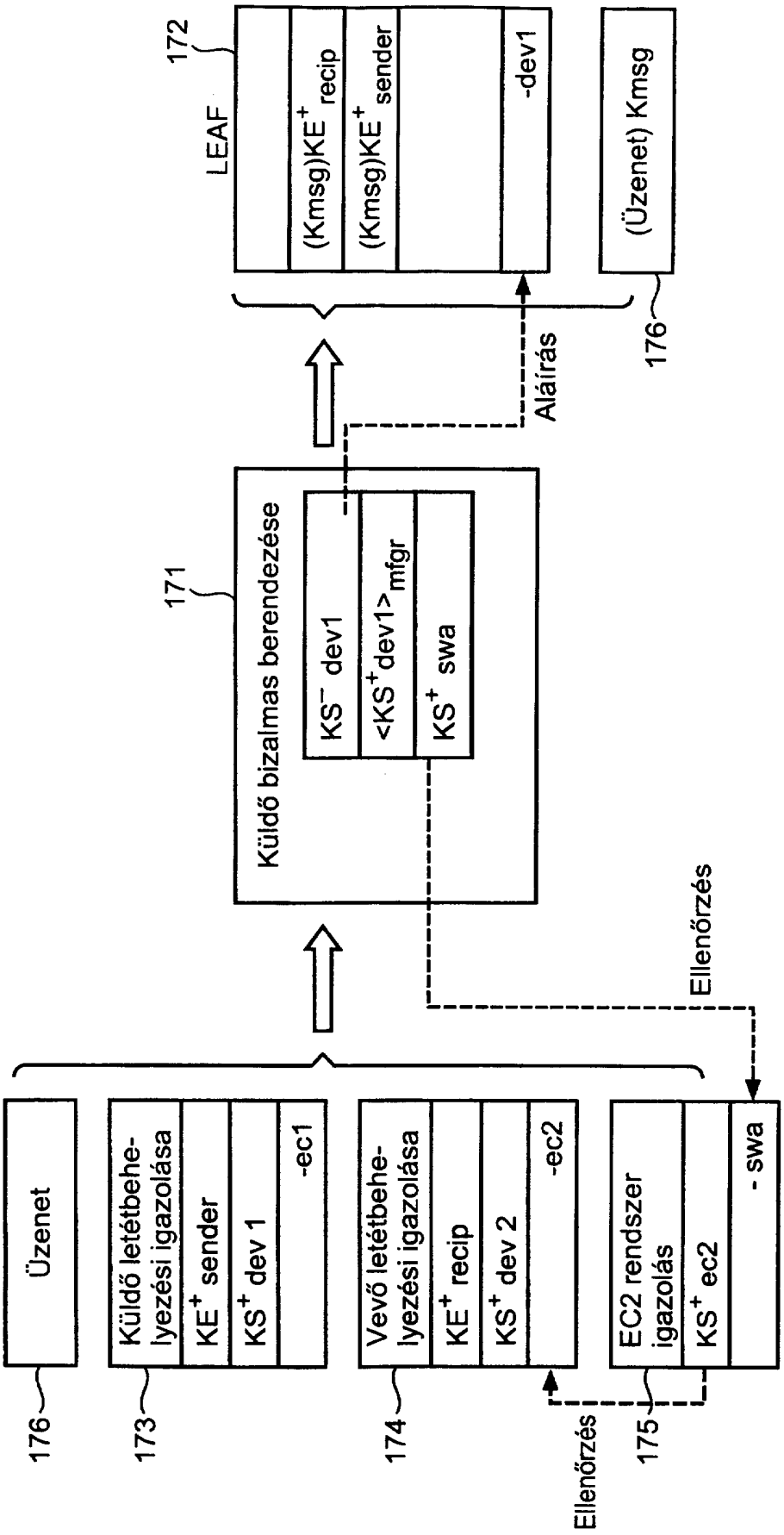



Újbóli átadás
Letétbehelyezési központ
KS+ mfgr
KS− ec
KE− ec
• aláírások ellenőrzése
• csomag megfejtése
• KE− user eltárolása
153
156
Berendezés sorszáma
KE+ user
KS+ dev
- ec
154
151
157
Ellenőrzés
Letétbehelyezési központ neve
KS+ ec
- swa
158
átadás
Nyilvántartásba vétel kész
Ellenőrzés
150
152
151
KE+ ec
- dev
KE− user
KE+ user
Berendezés sorszáma
154
Output
Ellenőrzés
155
Berendezés sorszáma
KS+ dev
- mfgr
Bizalmas berendezés
KS+ mfgr
KS+ swa
KS− dev
<KS+dev>mfgr
151
KE+ user
KE− user
Generálás:
Input
Letétbehelyezési központ neve
KE+ ec
- swa
Átvétel

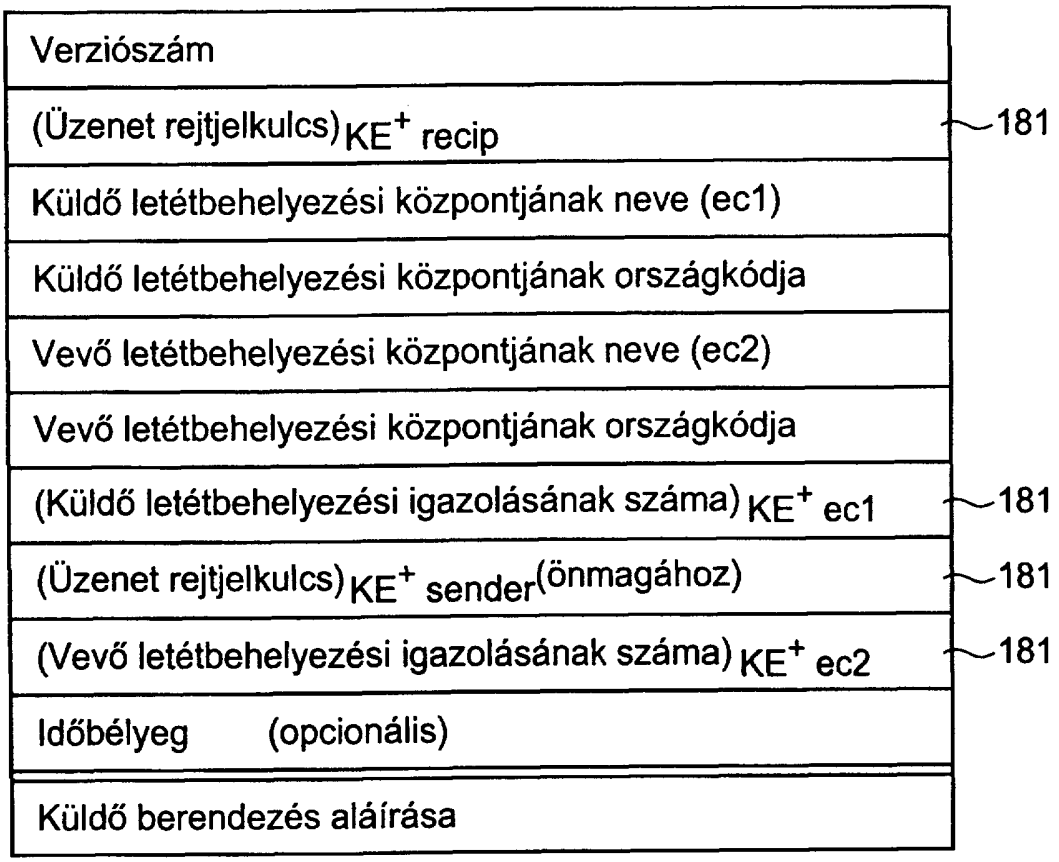
15. ábra


Igazolások
Berendezés igazolás
166
1. letétbehelyezési ügynök KE+ ea1 - EC
162
Berendezés sorszáma KS+ dev - mfgr
Bizalmas berendezés
KS+ mfgr KS+ swa
KS+ dev KS− dev
KS+ user KS− user
Három letétbehelyezési ügynök nyilvános rejtjelkulcsa
A berendezés x1, x2, x3 rejtjelkulcs szeleteket, valamint r1, r2, r3 véletlen számokat generál
A letétbehelyezési központ igazolása
161
161
161
Felhasználó neve, ber. sorsz. KE+ user, (x1, r1)ea1 - dev
Felhasználó neve, ber. sorsz. KE+ user, (x2, r2)ea2 - dev
Felhasználó neve, ber. sorsz. KE+ user, (x3, r3)ea3 - dev
Letétbelyezési központ
KS+ ec
KE+ ec
- swa
1. letétbehelyezési ügynök x1, ber. sorsz. eltárolása
2. letétbehelyezési ügynök x2, ber. sorsz. eltárolása
3. letétbehelyezési ügynök x3, ber. sorsz. eltárolása
Felhasználó neve, ber. sorsz., KE+, (r1, ea1 neve, r2, ea2 neve, r3, ea3 neve)ec - dev
163
163
163
164
165
Név, KE+ user (r1, dev #)ec - ea1
Név, KE+ user (r2, dev #)ec - ea2
Név, KE+ user (r3, dev #)ec - ea3
Letétbehelyezési központ
Annak ellenőrzése, hogy r1, r2, r3 ugyanaz-e
167
167
167
168
Felhasználó neve KE+ user KS+ dev - EC
Letétbehelyezési igazolás létrehozása
Vissza a felhasználónak

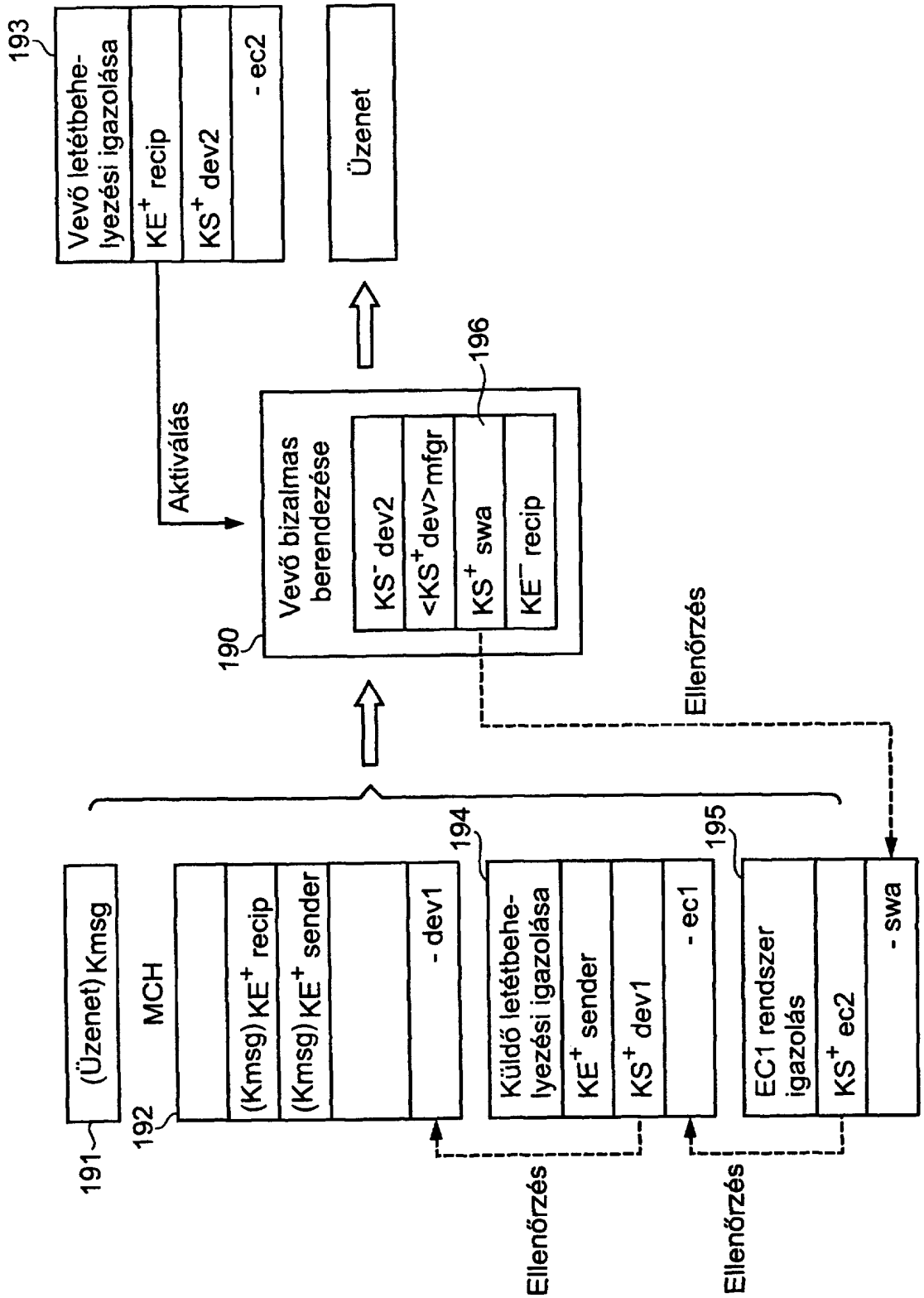
16. ábra


172
LEAF
(Kmsg)KE+ recip
(Kmsg)KE+ sender
-dev1
(Üzenet) Kmsg
176
Aláírás
171
Küldő bizalmas berendezése
KS− dev1
<KS+dev1>mfgr
KS+ swa
Ellenőrzés
Üzenet
Küldő letétbehe-lyezési igazolása
KE+ sender
KS+ dev 1
-ec1
Vevő letétbehe-lyezési igazolása
KE+ recip
KS+ dev 2
-ec2
EC2 rendszer igazolás
KS+ ec2
- swa
176
173
174
Ellenőrzés
175

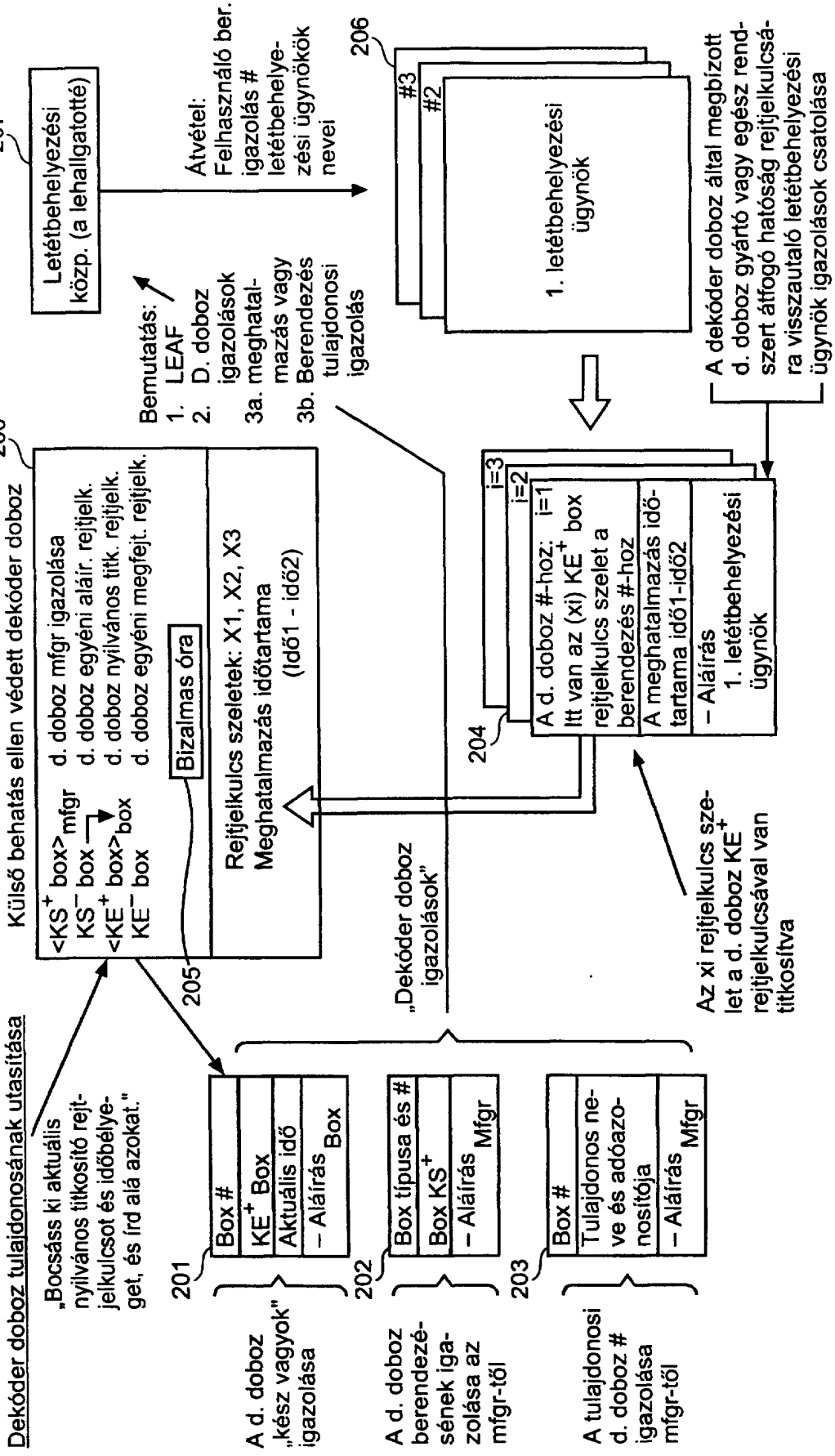
17. ábra


Verziószám
(Üzenet rejtjelkulcs) KE+ recip
181
Küldő letétbehelyezési központjának neve (ec1)
Küldő letétbehelyezési központjának országkódja
Vevő letétbehelyezési központjának neve (ec2)
Vevő letétbehelyezési központjának országkódja
(Küldő letétbehelyezési igazolásának száma) KE+ ec1
181
(Üzenet rejtjelkulcs) KE+ sender(önmagához)
181
(Vevő letétbehelyezési igazolásának száma) KE+ ec2
181
Időbélyeg (opcionális)
Küldő berendezés aláírása

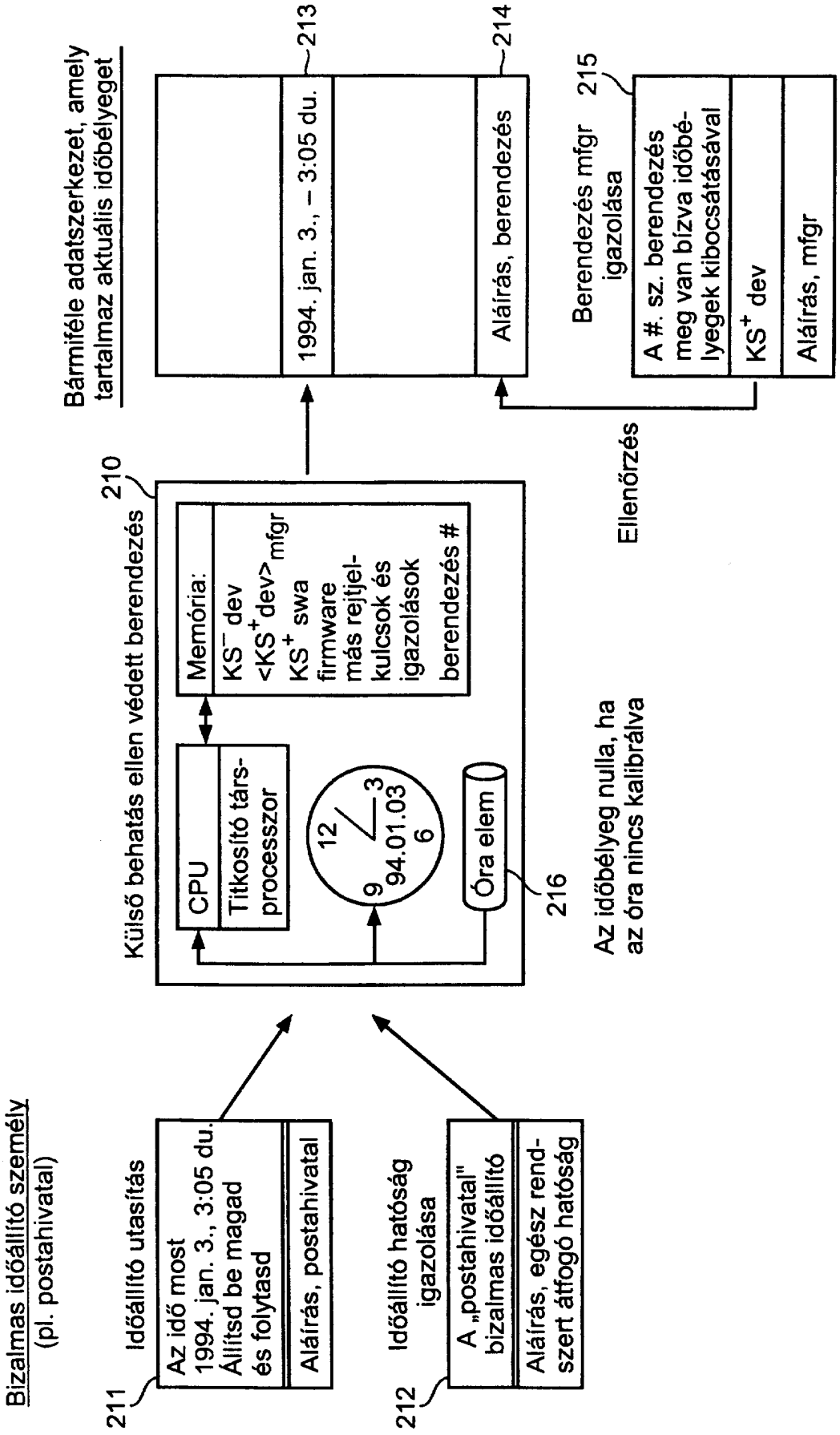
18. ábra


193
Vevő letétbehe-lyezési igazolása
KE+ recip
KS+ dev2
- ec2
Üzenet
Aktiválás
196
Vevő bizalmas berendezése
KS- dev2
<KS+dev>mfgr
KS+ swa
KE- recip
190
Ellenőrzés
(Üzenet) Kmsg
MCH
(Kmsg) KE+ recip
(Kmsg) KE+ sender
- dev1
194
Küldő letétbehe-lyezési igazolása
KE+ sender
KS+ dev1
- ec1
195
EC1 rendszer igazolás
KS+ ec2
- swa
191
192
Ellenőrzés
Ellenőrzés

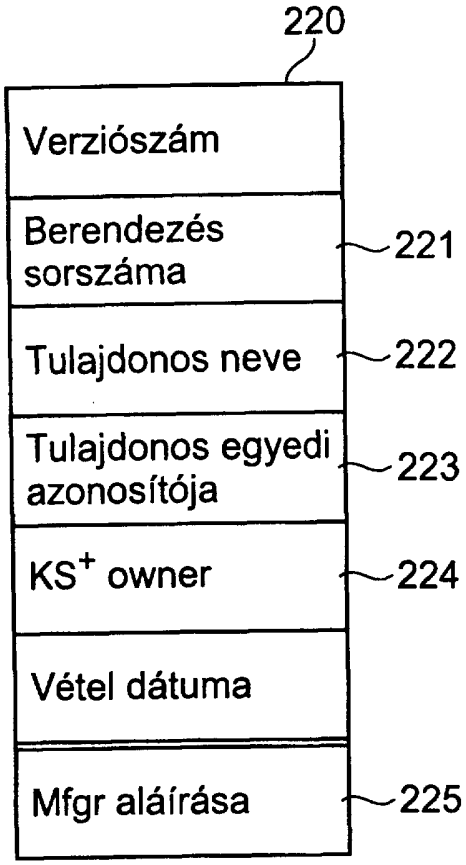
19. ábra


Dekóder doboz tulajdonosának utasítása
„Bocsáss ki aktuális nyilvános titkosító rejtjelkulcsot és időbélyeget, és írd alá azokat."
Külső behatás ellen védett dekóder doboz
200
<KS+ box>mfgr
KS− box
<KE+ box>box
KE− box
d. doboz mfgr igazolása
d. doboz egyéni aláír. rejtjelk.
d. doboz nyilvános titk. rejtjelk.
d. doboz egyéni megfejt. rejtjelk.
Bizalmas óra
205
Rejtjelkulcs szeletek: X1, X2, X3
Meghatalmazás időtartama
(Idő1 - idő2)
Bemutatás:
1. LEAF
2. D. doboz igazolások
3a. meghatalmazás vagy
3b. Berendezés tulajdonosi igazolás
Letétbehelyezési közp. (a lehallgatotté)
207
Átvétel:
Felhasználó ber. igazolás # letétbehelyezési ügynökök nevei
206
#3
#2
1. letétbehelyezési ügynök
A dekóder doboz által megbízott d. doboz gyártó vagy egész rendszert átfogó hatóság rejtjelkulcsára visszautaló letétbehelyezési ügynök igazolások csatolása
i=3
i=2
i=1
A d. doboz #-hoz: itt van az (xi) KE+ box rejtjelkulcs szelet a berendezés #-hoz
A meghatalmazás időtartama idő1-idő2
– Aláírás
1. letétbehelyezési ügynök
204
„Dekóder doboz igazolások"
Az xi rejtjelkulcs szelet a d. doboz KE+ rejtjelkulcsával van titkosítva
201
Box #
KE+ Box
Aktuális idő
– Aláírás Box
A d. doboz „kész vagyok" igazolása
202
Box típusa és #
Box KS+
– Aláírás Mfgr
A d. doboz berendezésének igazolása az mfgr-től
203
Box #
Tulajdonos neve és adóazonosítója
– Aláírás Mfgr
A tulajdonosi d. doboz # igazolása mfgr-től

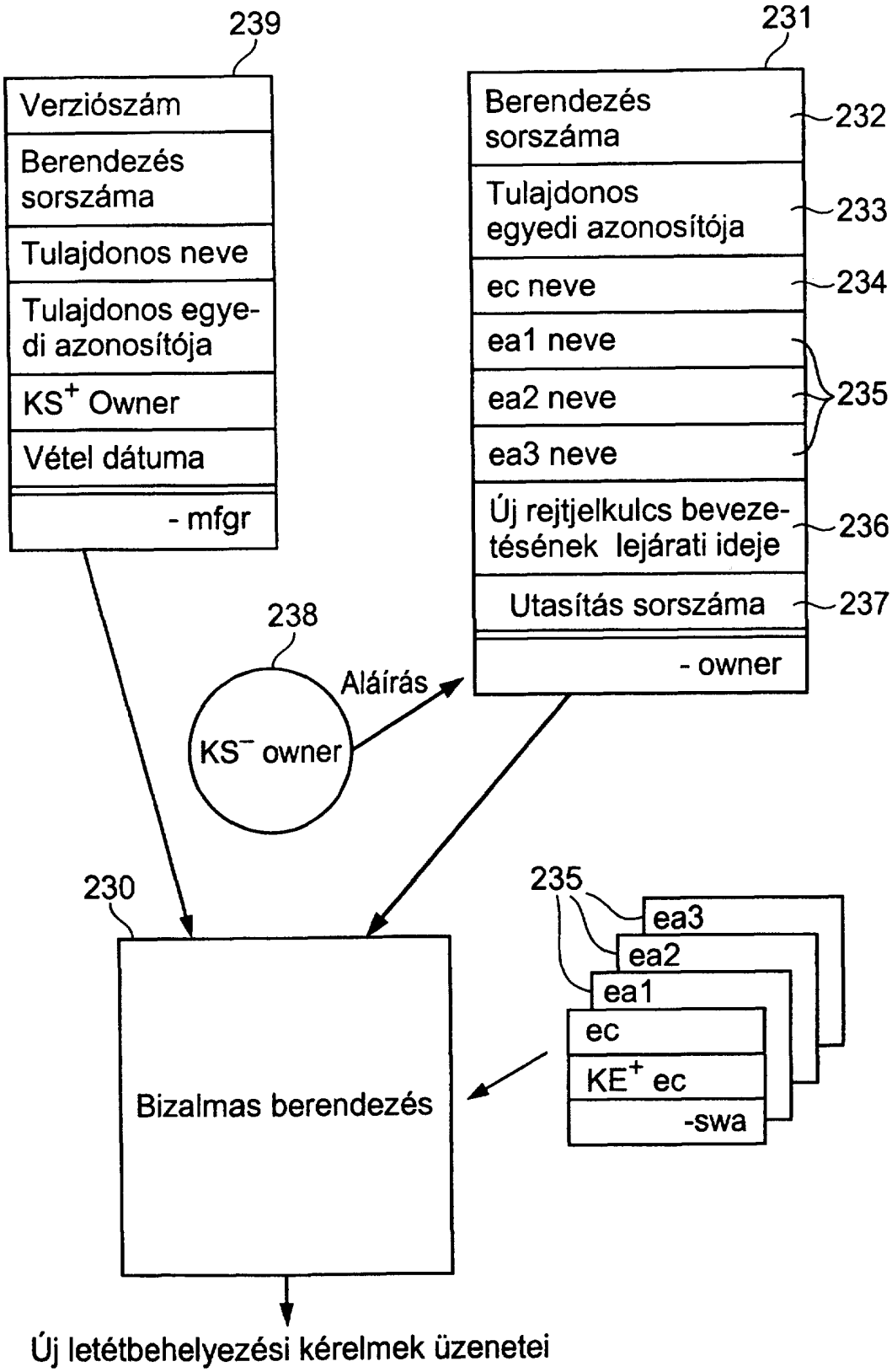
20. ábra


Bizalmas időállító személy
(pl. postahivatal)
211
Időállító utasítás
Az idő most 1994. jan. 3., 3:05 du. Állítsd be magad és folytasd
Aláírás, postahivatal
212
Időállító hatóság igazolása
A „postahivatal" bizalmas időállító
Aláírás, egész rendszert átfogó hatóság
Külső behatás ellen védett berendezés
210
CPU
Titkosító társprocesszor
Memória:
KS⁻ dev
<KS⁺dev>mfgr
KS⁺ swa
firmware
más rejtjelkulcsok és igazolások
berendezés #
12
3
9
6
94.01.03
Óra elem
216
Az időbélyeg nulla, ha az óra nincs kalibrálva
Ellenőrzés
Bármiféle adatszerkezet, amely tartalmaz aktuális időbélyeget
1994. jan. 3., – 3:05 du.
213
Aláírás, berendezés
214
Berendezés mfgr igazolása
215
A #. sz. berendezés meg van bízva időbélyegek kibocsátásával
KS⁺ dev
Aláírás, mfgr

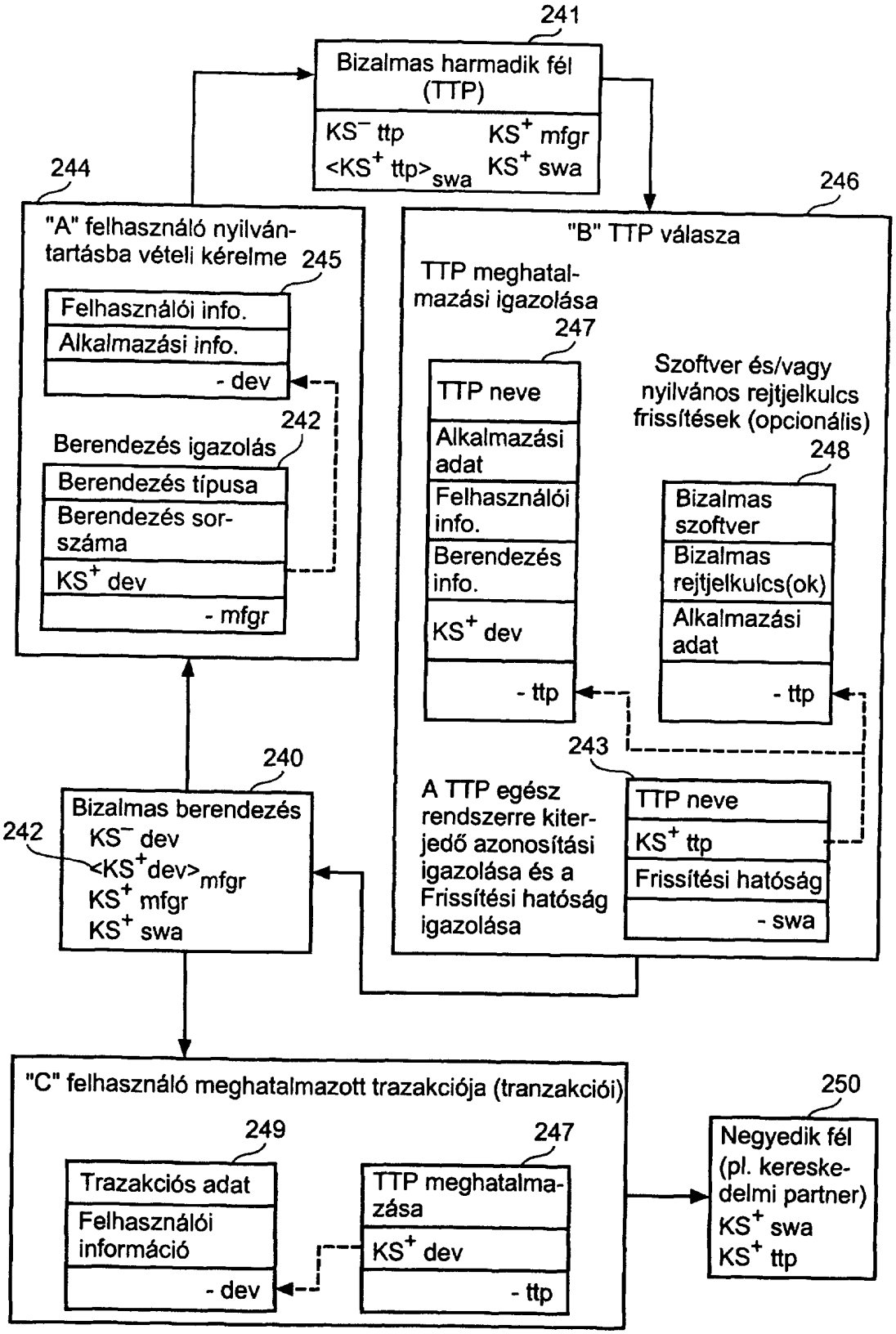
21. ábra


220
Verziószám
Berendezés sorszáma
221
Tulajdonos neve
222
Tulajdonos egyedi azonosítója
223
KS+ owner
224
Vétel dátuma
Mfgr aláírása
225

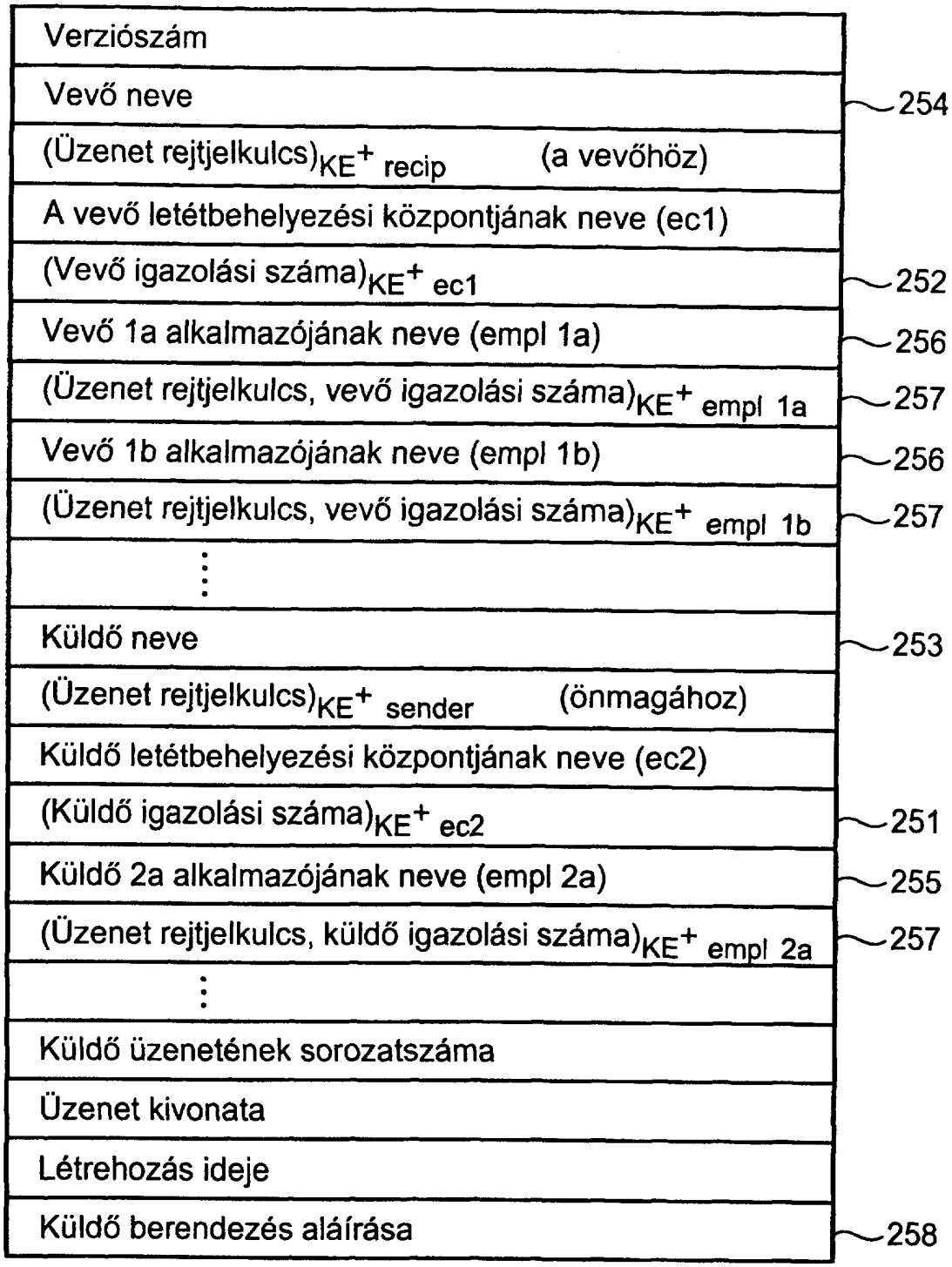
22. ábra


239
Verziószám
Berendezés sorszáma
Tulajdonos neve
Tulajdonos egyedi azonosítója
KS+ Owner
Vétel dátuma
- mfgr
231
Berendezés sorszáma
232
Tulajdonos egyedi azonosítója
233
ec neve
234
ea1 neve
ea2 neve
ea3 neve
235
Új rejtjelkulcs bevezetésének lejárati ideje
236
Utasítás sorszáma
237
- owner
238
Aláírás
KS− owner
230
Bizalmas berendezés
235
ea3
ea2
ea1
ec
KE+ ec
-swa
Új letétbehelyezési kérelmek üzenetei

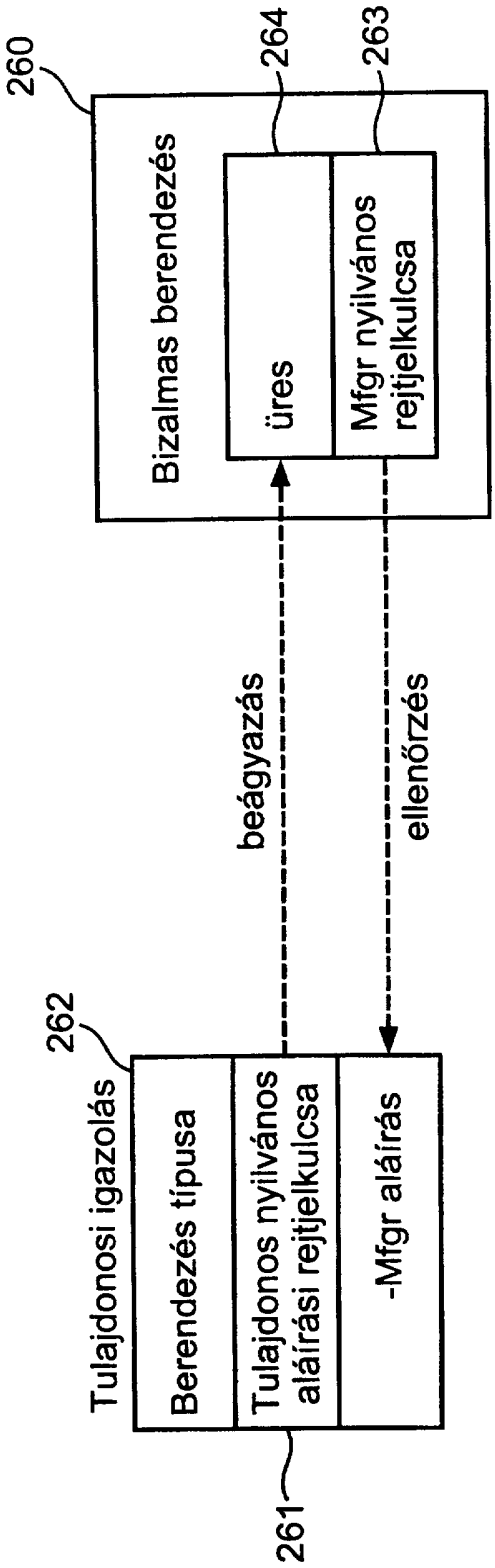
23. ábra


241
Bizalmas harmadik fél (TTP)
KS⁻ ttp
KS⁺ mfgr
<KS⁺ ttp>swa
KS⁺ swa
244
"A" felhasználó nyilvántartásba vételi kérelme
245
Felhasználói info.
Alkalmazási info.
- dev
242
Berendezés igazolás
Berendezés típusa
Berendezés sorszáma
KS⁺ dev
- mfgr
246
"B" TTP válasza
TTP meghatalmazási igazolása
247
TTP neve
Alkalmazási adat
Felhasználói info.
Berendezés info.
KS⁺ dev
- ttp
Szoftver és/vagy nyilvános rejtjelkulcs frissítések (opcionális)
248
Bizalmas szoftver
Bizalmas rejtjelkulcs(ok)
Alkalmazási adat
- ttp
243
A TTP egész rendszerre kiterjedő azonosítási igazolása és a Frissítési hatóság igazolása
TTP neve
KS⁺ ttp
Frissítési hatóság
- swa
240
Bizalmas berendezés
242
KS⁻ dev
<KS⁺dev>mfgr
KS⁺ mfgr
KS⁺ swa
"C" felhasználó meghatalmazott trazakciója (tranzakciói)
249
Trazakciós adat
Felhasználói információ
- dev
247
TTP meghatalmazása
KS⁺ dev
- ttp
250
Negyedik fél (pl. kereskedelmi partner)
KS⁺ swa
KS⁺ ttp

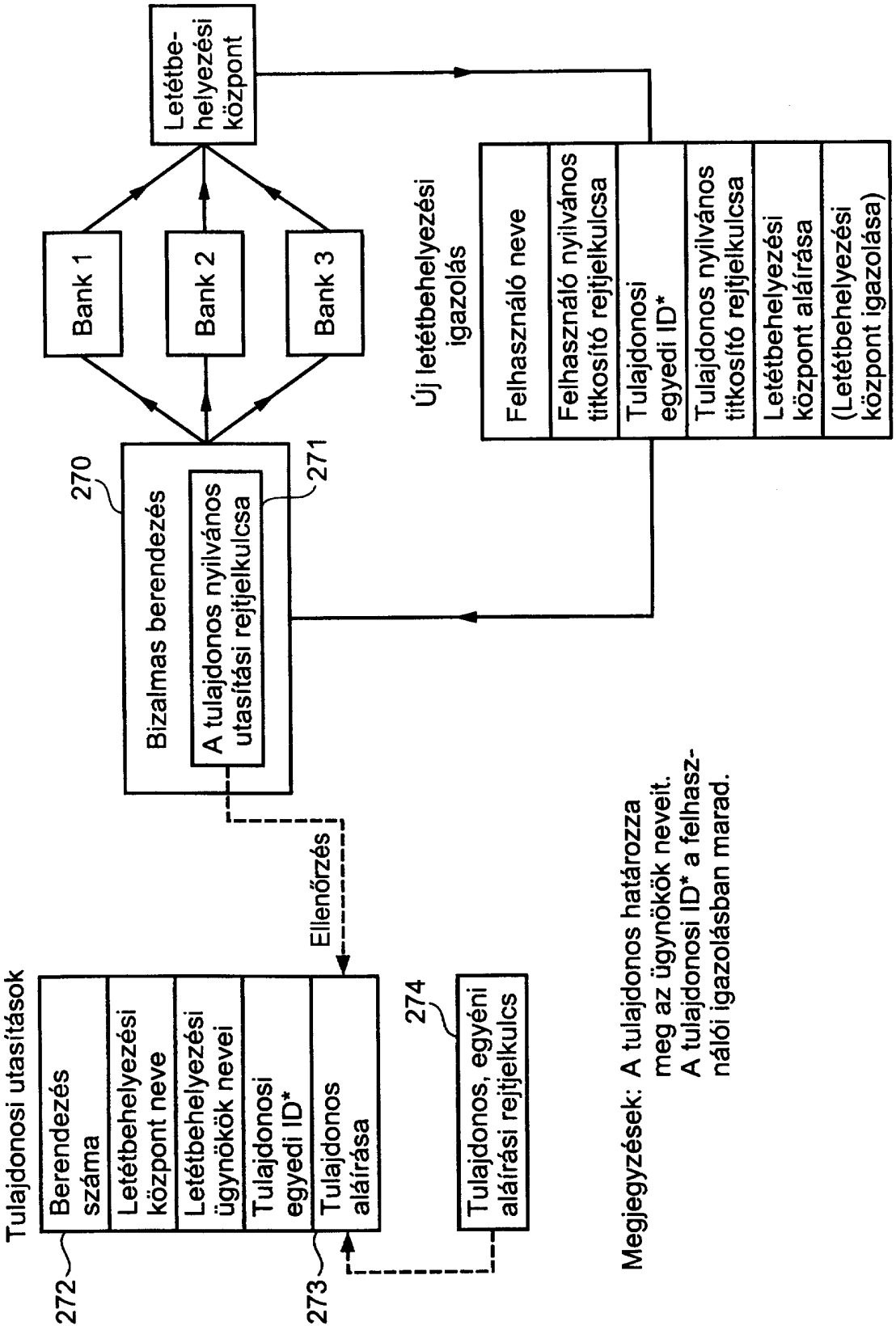
24. ábra


Verziószám
Vevő neve
(Üzenet rejtjelkulcs)KE+ recip (a vevőhöz)
A vevő letétbehelyezési központjának neve (ec1)
(Vevő igazolási száma)KE+ ec1
Vevő 1a alkalmazójának neve (empl 1a)
(Üzenet rejtjelkulcs, vevő igazolási száma)KE+ empl 1a
Vevő 1b alkalmazójának neve (empl 1b)
(Üzenet rejtjelkulcs, vevő igazolási száma)KE+ empl 1b
Küldő neve
(Üzenet rejtjelkulcs)KE+ sender (önmagához)
Küldő letétbehelyezési központjának neve (ec2)
(Küldő igazolási száma)KE+ ec2
Küldő 2a alkalmazójának neve (empl 2a)
(Üzenet rejtjelkulcs, küldő igazolási száma)KE+ empl 2a
Küldő üzenetének sorozatszáma
Üzenet kivonata
Létrehozás ideje
Küldő berendezés aláírása
254
252
256
257
256
257
253
251
255
257
258

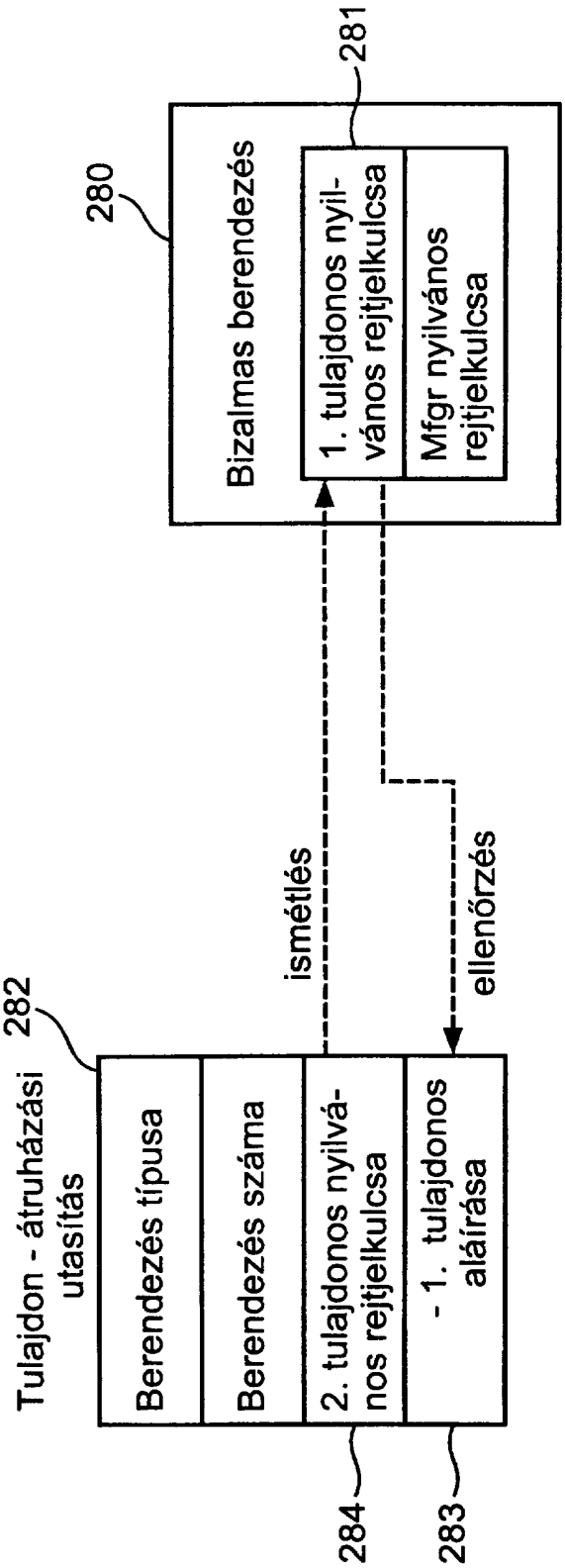
25. ábra


260
264
263
Bizalmas berendezés
üres
Mfgr nyilvános rejtjelkulcsa
beágyazás
ellenőrzés
262
Tulajdonosi igazolás
Berendezés típusa
Tulajdonos nyilvános aláírási rejtjelkulcsa
-Mfgr aláírás
261

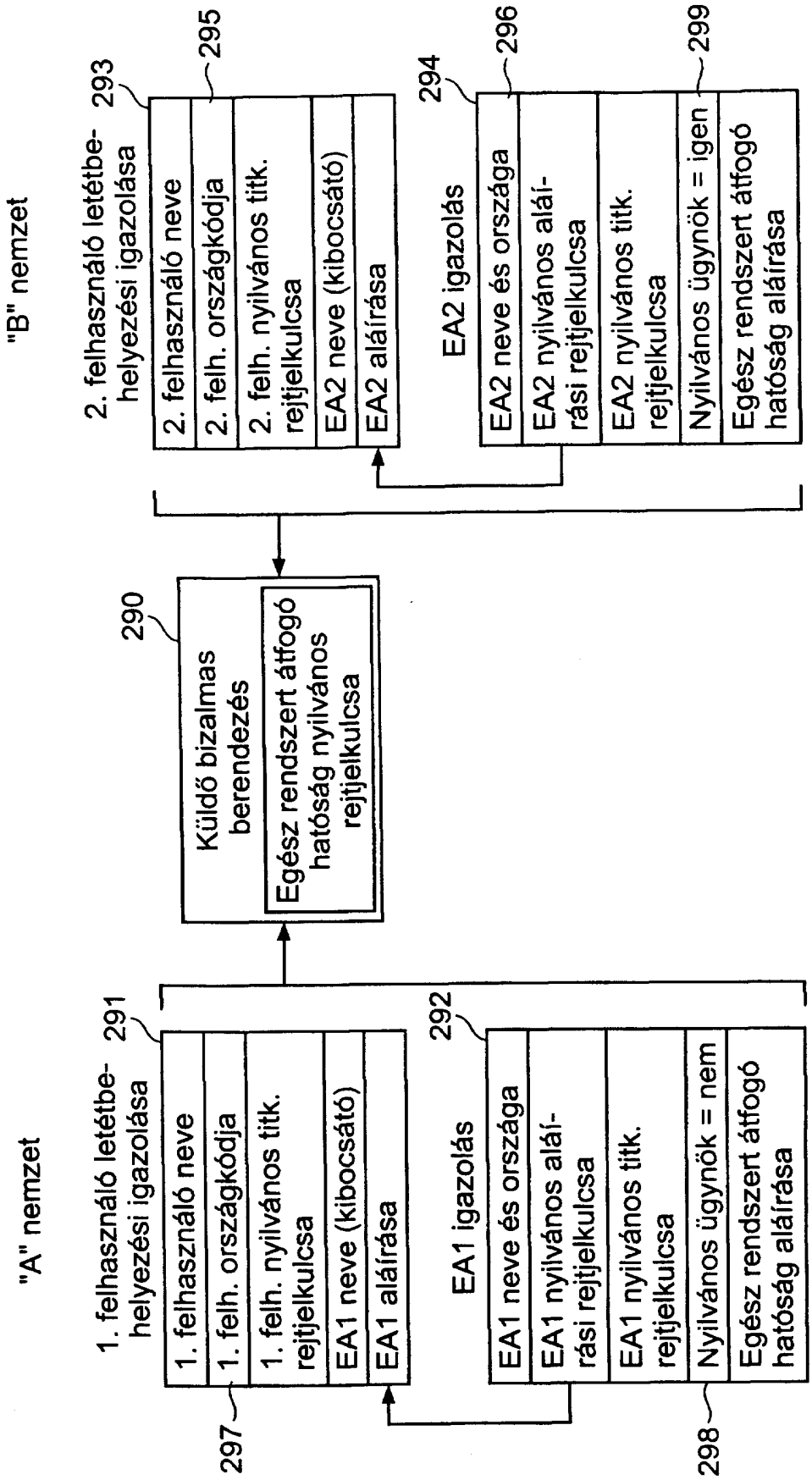
26. ábra


Letétbe-helyezési központ
Bank 1
Bank 2
Bank 3
Új letétbehelyezési igazolás
Felhasználó neve
Felhasználó nyilvános titkosító rejtjelkulcsa
Tulajdonosi egyedi ID*
Tulajdonos nyilvános titkosító rejtjelkulcsa
Letétbehelyezési központ aláírása
(Letétbehelyezési központ igazolása)
270
Bizalmas berendezés
A tulajdonos nyilvános utasítási rejtjelkulcsa
271
Ellenőrzés
Tulajdonosi utasítások
Berendezés száma
Letétbehelyezési központ neve
Letétbehelyezési ügynökök nevei
Tulajdonosi egyedi ID*
Tulajdonos aláírása
272
273
274
Tulajdonos, egyéni aláírási rejtjelkulcs
Megjegyzések: A tulajdonos határozza meg az ügynökök neveit.
A tulajdonosi ID* a felhasználói igazolásban marad.

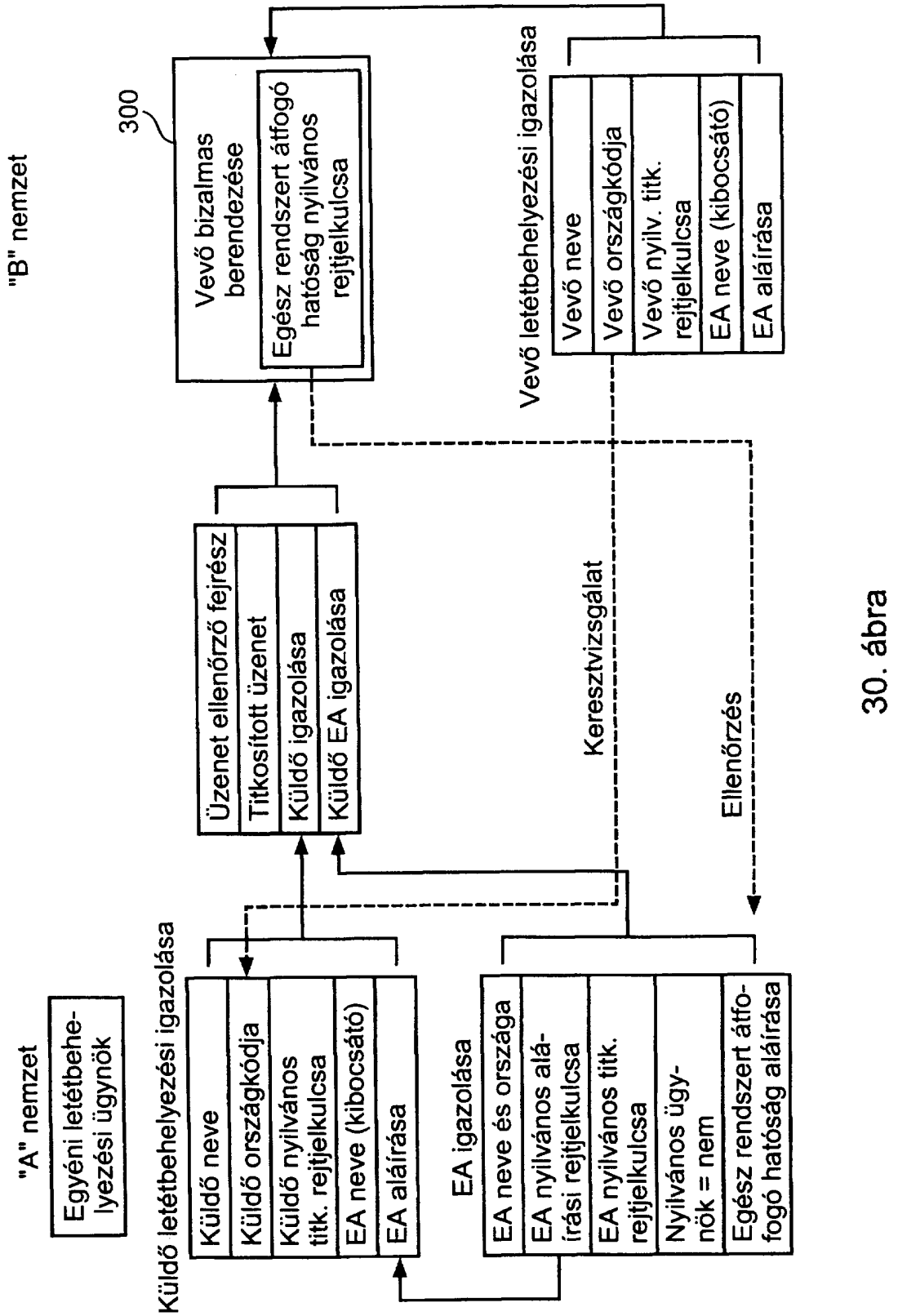
27. ábra


280
Bizalmas berendezés
281
1. tulajdonos nyilvános rejtjelkulcsa
Mfgr nyilvános rejtjelkulcsa
ismétlés
ellenőrzés
282
Tulajdon - átruházási utasítás
Berendezés típusa
Berendezés száma
2. tulajdonos nyilvános rejtjelkulcsa
- 1. tulajdonos aláírása
284
283

28. ábra


"A" nemzet
"B" nemzet
1. felhasználó letétbe-helyezési igazolása
291
1. felhasználó neve
1. felh. országkódja
1. felh. nyilvános titk. rejtjelkulcsa
EA1 neve (kibocsátó)
EA1 aláírása
297
EA1 igazolás
292
EA1 neve és országa
EA1 nyilvános alá-rási rejtjelkulcsa
EA1 nyilvános titk. rejtjelkulcsa
Nyilvános ügynök = nem
Egész rendszert átfogó hatóság aláírása
298
290
Küldő bizalmas berendezés
Egész rendszert átfogó hatóság nyilvános rejtjelkulcsa
2. felhasználó letétbe-helyezési igazolása
293
2. felhasználó neve
2. felh. országkódja
295
2. felh. nyilvános titk. rejtjelkulcsa
EA2 neve (kibocsátó)
EA2 aláírása
EA2 igazolás
294
EA2 neve és országa
296
EA2 nyilvános alá-rási rejtjelkulcsa
EA2 nyilvános titk. rejtjelkulcsa
Nyilvános ügynök = igen
299
Egész rendszert átfogó hatóság aláírása

29. ábra



30. ábra

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna osztályvezető
Windor Bt., Budapest