

P 0400462

KÖZZÉTÉTELI
PÉLDÁNY

2014.03

AI

ELJÁRÁS DIGITÁLIS BÉRMENTESÍTÉSI JELEK ÉRVÉNYESSÉGÉNEK
ELLENŐRZÉSÉRE

K i v o n a t

A találmány eljárás postai küldeményre felvitt digitális bérmentesítési jel hitelességének ellenőrzésére, amelynek során a bérmentesítési jelben levő kriptográfiai információkat visszafejtjük, és a bérmentesítési jel hitelességének ellenőrzésére használjuk fel. Egy ellenőrzőegységgel részellenőrzések lefolyását vezéreljük, ahol egy első részellenőrzés folyamán beolvasunk egy, a digitális bérmentesítési jelben levő mátrixkódot, az ellenőrzőegységgel vezéreljük a mátrixkód tartalmának felbontását, a részellenőrzéseket ellenőrzési lépésekként hajtjuk végre, több ellenőrzéskérés, valamint ezekkel párhuzamosan az ellenőrzési lépések egy részének egyidejű végrehajtására alkalmas ellenőrzőegységet alkalmazunk, az ellenőrzési lépésekkel feltárjuk a jogosulatlanul előállított bérmentesítési jeleket, az ellenőrzés eredményét digitális üzenetként közöljük, és ezzel egy küldeményt kizárunk a postai küldemények normál feldolgozásának menetéből. (2. ábra)



ELJÁRÁS DIGITÁLIS BÉRMENTESÍTÉSI JELEK ÉRVÉNYESSÉGÉNEK
ELLENŐRZÉSÉRE

A találmány tárgya eljárás digitális bérmentesítési jelek érvényességének ellenőrzésére.

Ismeretes, hogy postai küldeményeket digitális bérmentesítési jelekkel látnak el.

A postai küldemények feladói számára a bérmentesítési jelek előállítását például a Német Posta (Deutsche Post AG) egy olyan bérmentesítési rendszerrel könnyíti meg, amelynél a bérmentesítési jeleket egy ügyfélrendszerben állítják elő, és egy tetszőleges interfészen át egy nyomtatóra adják ki.

Az esetleges visszaélések elkerülése érdekében a digitális bérmentesítési jelek kriptográfiai információkat tartalmaznak, például a bérmentesítési jel előállítását vezérlő ügyfélrendszer azonosítására.

Célunk a találmánnyal olyan eljárás létrehozása, amellyel a bérmentesítési jelek hitelességét gyorsan és megbízhatóan ellenőrizni lehet. Fontos, hogy az eljárás alkalmazható legyen levelek és egyéb küldemények vagy szállítmányok tömeges kezelésére.

A találmány szerint a kitűzött feladatot olyan eljárással oldjuk meg, amelynek során a bérmentesítési jelben levő kriptográfiai információkat visszafejtjük, és a bérmentesítési jel hitelességének ellenőrzésére használjuk fel. Egy ellenőrzőegységgel részellenőrzések lefolyá-

sát vezéreljük, ahol egy első részellenőrzés folyamán beolvasunk egy, a digitális bérmentesítési jelben levő mátrixkódot, az ellenőrzőegységgel vezéreljük a mátrixkód tartalmának felbontását, a részellenőrzéseket ellenőrzési lépéseként hajtjuk végre, több ellenőrzéskérés, valamint ezekkel párhuzamosan az ellenőrzési lépések egy részének egyidejű végrehajtására alkalmas ellenőrzőegységet alkalmazunk, az ellenőrzési lépésekkel feltárjuk a jogosulatlanul előállított bérmentesítési jeleket, az ellenőrzés eredményét digitális üzenetként közöljük, és ezzel egy küldeményt kizárunk a postai küldemények normál feldolgozásának menetéből.

Különösen előnyös, ha a részellenőrzések egyikének folyamán fejtjük vissza a bérmentesítési jelben levő kriptográfiai információkat. Célszerűen a részellenőrzések egyikének folyamán összehasonlítjuk a bérmentesítési jel előállításának dátumát az aktuális dátummal.

Előnyösen az olvasóegység és az ellenőrzőegység között szinkron protokoll segítségével információkat cserélünk, és ehhez RPC-alapú protokollt alkalmazunk.

Az olvasóegység és az ellenőrzőegység egymás közötti kommunikációjához előnyösen aszinkron protokollt alkalmazunk; az olvasóegységről adattáviratot küldünk az ellenőrzőegységre, amely adattávirat a bérmentesítési jel tartalmát foglalja magában, és felszólítást tartalmaz egy kriptográfiai ellenőrző rutin megindítására.

Szintén előnyös, ha egy kriptointerfészen át terhelosztást végzünk több ellenőrző eszköz között; a bérmen-

tesítési jel tartalmát mezőkre osztjuk fel; és a bérmentesítési jel előállítását vezérlő ügyfélrendszer azonosítószámát (bérmentesítési azonosítót) a bérmentesítési jelből határozzuk meg.

Célszerű továbbá, ha az ügyfélrendszer egyes azonosító adatait (bérmentesítési azonosító) tiltólista-adatállományba helyezzük, és az ehhez a bérmentesítési azonosítóhoz tartozó küldeményeket kizárjuk a postai küldemények normál feldolgozásának menetéből.

Előnyösen egy címzettnek a bérmentesítési jelben titkosítva megadott címét összehasonlítjuk a postai küldemény továbbításához megadott címmel.

Előnyös az is, ha változtatjuk az eljárás ellenőrzési paramétereit; célszerűen az eljárási paraméterek változtatását csak egy rendszeradminisztrátor személyes digitális kulcsának (magánkulcs) bevitele után hajtjuk végre.

A találmányt a továbbiakban kiviteli példák és rajzok alapján részletesen ismertetjük. A rajzokon az

1. ábra: egy díjbiztosítási rendszer felépítésének elvi vázlata, a

2. ábra: a díjbiztosítási rendszer egy különösen előnyös kiviteli alakja (kéziolvasóval és díjbiztosítási PC-vel), a

3. ábra: a bérmentesítési jelek előállításának és ellenőrzésének elvi vázlata, a

4. ábra: a kriptorendszer alkotórészeinek áttekintése, az

5. ábra: az ellenőrzési eljárás egy előnyös kiviteli alakja, a

6. ábra: az ellenőrzési eljárás egy további különösen előnyös kiviteli alakja a részellenőrzésekkel, és a

7. ábra: egy központi bérmentesítési hely és az egyes kriptográfiai ellenőrzőegységek (kriptoserverek) közötti kulcselosztás egy előnyös megvalósítási módja.

Az alábbiakban a találmányt egy PC-bérmentesítő (PC-F) rendszer példáján írjuk le. A díjazást biztosító eljárási lépések függetlenek a bérmentesítési jeleket előállító rendszertől.

Az ábrázolt, az egyes ellenőrzési helyeken, elsősorban a levélfeldolgozó központokban végzett decentralizált ellenőrzés különösen előnyös, bár központi ellenőrzés ugyanígy lehetséges.

A találmány egy első kiviteli alakjánál a bérmentesítési jelek hitelességét előnyösen szűrőpróbaszerűen, vonalkódolvasókkal ellenőrizzük.

Egy erre a célra alkalmas példakénti ellenőrzőrendszer mutat az 1. ábra.

Az 1. ábrán látható, hogy a kriptorendszer milyen részrendszerekkel áll kapcsolatban. Ezeket az alábbiakban röviden leírjuk.

Olvasók

Az olvasók a PC-bérmentesítés bérmentesítési jelének beolvasására szolgálnak. A bérmentesítési jelek adatmát-

rix (Data Matrix) alakú kétdimenziós kódok, ECC200 hibajavító kód alkalmazásával. Az olvasó típusának megfelelően az adatokat rádión vagy kábelén visszük át; a rádiós olvasók többsoros kijelzővel és érintőképernyővel, továbbá billentyűzettel rendelkeznek. Az olvasók és a díjbiztosítási-PC-bérmentesítési rendszer többi része közötti interfészt az olvasóvezérlő és az ellenőrzőegység képezi. Míg az olvasóvezérlő mátrixkódok sorozatát kezeli, amelyek a kéziolvasóról érkeznek az ellenőrzéshez, és lényegében a kapcsolatot jelentik az olvasókkal, az olvasóvezérlő a rendszer további részével csak az ellenőrzőegységen át van kapcsolatban.

Olvasóvezérlő/ellenőrzőegység

Az olvasóvezérlők, ill. az ellenőrzőegységek interfészt alkotnak az olvasók és a kétdimenziós vonalkódokat ellenőrző további rendszerek között. Az említett egységek a kétdimenziós vonalkód optikailag érzékelt, átalakított és hibajavított tartalmát kapják meg, és megindítják az ellenőrzést, rádiós olvasó esetén gondoskodnak a beolvasási és ellenőrzési eredmény kiadásáról, továbbá interfészként szolgálnak az esetleg szükséges utólagos manuális feldolgozás és ellenőrzés, valamint a többi rendszer között.

Kriptorendszer

A kriptorendszer végzi a kétdimenziós vonalkód tartalmi és kriptográfiai ellenőrzését, valamint a biztonsá-

sággal kapcsolatos adatok és algoritmusok védett tárolását. Az egyes alkotórészeket később még részletesen leírjuk.

Bérmentesítési hely (Postage Point)

A bérmentesítési hely a központi rendszer a PC-bérmentesítésen belül. Ez egy interfész az ügyfélrendszerek felé. A bérmentesítés előtt az ügyfelek innen tölthetik le az előírt díjakat. A bérmentesítési helyen generálják az eljárás biztonságossá tételéhez szükséges kulcsokat. Ezenkívül a bérmentesítési hely interfészként szolgál az elszámolási rendszerek felé. Az előnyös kiviteli alaknál a PC-bérmentesítéshez a következők állnak a díjbiztosítási rendszer rendelkezésére:

- kétdimenziós vonalkódban a küldeményre vonatkozó információk
- szimmetrikus kulcsok
- törzsadatok, mint pl. díjsszabás, számlaegyenleg

Díjbiztosítási központ

Az előnyösen kialakított díjbiztosítási központi rendszerben a küldeménnyel kapcsolatos információkat gyűjtjük, és más rendszerek rendelkezésére bocsátjuk. Az itt készülő jelentések alapján tiltólista-adatállományokat állítunk fel. Ezenkívül a díjbiztosítási központi rendszer a bérmentesítési helyről megkapja az aktuális kulcsadatokat, és ezeket továbbítja az egyes kriptoszerverekre.

Adatszolgáltatók

A kétdimenziós vonalkódok tartalmi ellenőrzéséhez egy sor törzsadat szükséges, például tiltólista-adatállományok, minimális díjak, érvényességi idők a termékkel kapcsolatban, valamint díjbiztosítási figyelmeztető és továbbfeldolgozási kódok. Ezek az adatok különböző rendszerekben (BDE, VIBRIS, helyi díjbiztosítási rendszer) rendelkezésre állnak.

Díjbiztosítási alkalmazás

A díjbiztosítási (Esi) alkalmazás lehetőséget ad az AGB-ellenőrnek, aki a kizárt PC-bérmentesítési küldemények utólagos feldolgozásával foglalkozik, hogy a bérmentesítést részletesen ellenőrizze olyan körülmények között, ahol a vizsgálati eredmények megjelenítését nem korlátozzák az olvasó behatárolt kijelzési lehetőségei. Ezenkívül a vizsgáló itt további adatokhoz is hozzáférhet, például a bérmentesítési díj érvényességi idejéhez az aktuális küldeménnyel kapcsolatban, valamint az összeghez és az igénybe vett bérmentesítésekhez.

A kétdimenziós vonalkódok automatikus olvasása

A kétdimenziós vonalkódok automatikus olvasása az SSA-n belül történik. Ehhez a képinformációkat az AFM-2D-kódolvasóra továbbítjuk. Ott megtörténik a kép átalakítása az adatmátrixkód tartalmává. A kétdimenziós vonalkód tartalma ezután a kriptorendszerre kerül az ellenőrzés-

hez, a visszakapott eredményt kiértékeljük és az optikai érzékelőrendszerre (IMM) továbbítjuk a küldemény kódolásához. Egy így kibővített ellenőrzési eljárás alkotórészei a 2. ábrán láthatóak.

AFM-2D-kódolvasó

Olvasókészülékneként (ALM/ILVM) van egy AFM-2D-kódolvasó, amely egy optikai érzékelőrendszeren (IMM) át megkapja a küldemények képadatait, és díjbiztosítási célból elvégzi azok további feldolgozását. Az előnyös díjbiztosítási PC-bérmentesítés keretében ez egy felismert kétdimenziós kód esetében azt jelenti, hogy a képadatokból meghatározzuk a kétdimenziós adatmátrixkódot, és az ECC200 hibajavító eljárás segítségével egy olyan bájtlanccá alakítjuk át, amely a kétdimenziós vonalkód tartalmát ábrázolja.

Ezt a bájtlanccot ellenőrzésre az ellenőrzőegységre adjuk. Az ellenőrzés eredményét ezután az optikai érzékelőrendszer interfészén át továbbítjuk, és kódolásra használjuk fel.

Kriptorendszer AFM-2D-kódolvasókhoz

A kriptokártyák tulajdonságainak megfelelően például másodpercenként kb. 27 ellenőrzéssel lehet számolni. Mivel az olvasók sebessége másodpercenként kb. tíz leolvasott küldemény, nem ésszerű mindegyik AFM-2D-kódolvasót egy kriptorendszerrel kombinálni. Ezenkívül abból sem lehet kiindulni, hogy a PC-bérmentesítési küldemények

mindegyik gépet egyidejűleg száz százalékgig terhelik. Ezért célszerűnek látszik a kriptorendszerek elválasztása, és több PC-F-olvasó üzemeltetése egy kriptorendszerrel. A megoldást előnyösen úgy kell megválasztani, hogy minden levélkezelő és elosztó központban több kriptorendszert lehessen létesíteni. Ez például a nagy forgalmú, több leolvasóval működő központokban fontos, amelyekben először egy második kriptorendszert lehet üzembe helyezni. A későbbiekben a szerverek száma az igényeknek megfelelően növelhető.

Az egyszerűség kedvéért a rendszert előnyösen úgy építjük fel, hogy az egyes olvasókat állandó jelleggel hozzárendeljük egy kriptorendszerhez, és esetleg még egy olyan elrendezéssel egészítjük ki, amely hiba esetén megkísérel áttérni egy másik kriptorendszerre.

A kriptorendszer és az AFM-2D-kódolvasó elválasztása azzal az előnnyel is jár, hogy mind a gépi leolvasás, mind a kéziolvasóval végzett ellenőrzés ugyanazzal a kriptorendszerrel végrehajtható, és ezért ugyanazt a funkciót nem kell duplán megvalósítani, ami további lényeges előnyökkel jár a találmány alkalmazásánál.

A 3. ábrán azok az előnyös eljárási lépések láthatóak, amelyekkel egy postai küldemény - egy központi bérmentesítési helyről kapott díjtétellel történő terhelés után - digitális bérmentesítési jellel látható el, és a bérmentesítési jel előállítható egy helyi PC segítségével; ezután a postai küldemény beszállítható, és a küldeményre felvitt bérmentesítési jel ellenőrizhető.

A kulcselosztástól függetlenül az eljárás úgy folyik le, hogy egy ügyfél először egy bérmentesítési összeget visz be a PC-jébe. A lekérdezés megjelölésére egy véletlen számot generálunk. A bérmentesítési helyen egy újabb bérmentesítési összeget állítunk elő az ügyfél számára, és a továbbított véletlen számból további információkat állítunk elő az ügyfélrendszer azonosításához (a továbbiakban bérmentesítési azonosítónak nevezzük), és a bérmentesítési összeghez előállítjuk az ún. kriptosztringet, amelyet a bérmentesítési helyen rendelkezésre álló titkos szimmetrikus kulccsal titkosítunk.

Ezt a kriptosztringet és a megfelelő bérmentesítési összeget ezután átvisszük az ügyfél PC-jére, és ott a véletlen számmal együtt elhelyezzük az illetéktelen hozzáféréstől védett, biztonságos rekeszben.

Ha ezután az ügyfél a kapott bérmentesítési összeggel egy postai küldeményt bérmentesít, akkor a kétdimenziós vonalkód számára fontos küldeményi adatokat - többek között a kriptosztringet, a bérmentesítés dátumát és összegét - kibővítjük a véletlen számmal, és a bérmentesítési azonosítót nem titkosított formában gyűjtjük, továbbá egy hash-értéket állítunk elő, amely egyértelműen jellemzi a tartalmat.

Mivel a véletlen szám titkosított formában a kriptosztringben, valamint nem titkosított formában a hash-értékben jelen van, a küldemény adatai nem változtathatók meg, ill. önkényesen nem generálhatók, és vissza lehet következtetni az előállítóra.

A küldemény szempontjából fontos adatokat ezután egy kétdimenziós vonalkóddá alakítjuk át, amit bérmentesítési jelként az ügyfél a nyomtatójával a küldeményre nyomtat. Ezt követően a kész küldemény bevihető a postai forgalomba.

A díjazásbiztosítás egy különösen előnyös kiviteli alakjánál a kétdimenziós vonalkódot a levélkezelő központban egy AFM-2D-kódolvasóval, ill. egy kéziolvasóval olvassuk le, majd ellenőrizzük. Az eljárás ezzel kapcsolatos lépéseit 5-8 számokkal jelöltük. A kétdimenziós vonalkód helyességének ellenőrzéséhez az AFM-2D-kódolvasó a küldemény összes adatát átadja a kriptorendszernek. Az visszafejt egy, a küldemény adataiban levő kriptográfiai információt, elsősorban a kriptosztring információját, amelyből meghatározza a hash-érték előállításánál használt véletlen számot.

Ezután egy hash-értéket (message digest-nek is nevezik) határozunk meg a küldemény adataihoz, beleértve a visszafejtett véletlen számot, és ellenőrizzük, hogy az eredmény azonos-e a kétdimenziós vonalkódban levő hash-értékkel.

A kriptográfiai érvényesítésen kívül további tartalmi ellenőrzéseket (7b folyamat) is végzünk, amelyek például kizárják egy kétdimenziós vonalkód kétszeres használatát, illetve megvizsgálják, hogy az ügyfél korábbi csalási kísérlet miatt nem került-e tiltólistára.

Az ellenőrzés eredményét a PC-F-olvasóra továbbítjuk, amely az eredményt az optikai érzékelőrendszerre

(IMM) adja a vonalkód kódolásához. Ezután a vonalkódot felvisszük a levélre, ill. a küldeményeket kizárjuk, ha negatív az ellenőrzés eredménye.

Kriptorendszer-architektúra:

Alkotórészek áttekintése

A 4. ábra áttekintő képet ad a kriptorendszer részegységeiről, ahol a felirattal ellátott nyilak be- és kimeneti adatáramokat jelölnek külső rendszerekhez. Mivel az előnyös díjbiztosítási központi rendszeren át történik a bérmentesítési hely kulcsainak elosztása a helyi díjbiztosítási rendszerek kriptorendszerére, és ezeket az adatokat átmenetileg tárolni kell, ott szintén szükség van egy kriptorendszer-komponensre, amelynél azonban az ellenőrzőegységet általában nem használjuk.

A kriptorendszer részegységeit a továbbiakban részletesen leírjuk.

Ellenőrzőegység

Az ellenőrzőegység képezi az interfészt a kétdimenziós vonalkód teljes tartalmának ellenőrzéséhez. A kétdimenziós vonalkód ellenőrzése tartalmi és kriptográfiai ellenőrzésből áll. Erre a célra a kétdimenziós vonalkódok olvasókkal beolvasott tartalmát az olvasóvezérlőn át az ellenőrzőegységre kell továbbítani.

Mivel a vezetékes olvasó vezérlője és az ellenőrzőegység különböző számítógéprendszerekhez tartoznak, kö-

zöttük TCP/IP alapú kommunikációt folytatunk, és előnyösen egy arra épülő protokollt is alkalmazunk. A kriptorendszer keretében itt szóba jöhet az üzemi adatgyűjtésnél (BDE) használt táviratkezelő vagy az optikai adatgyűjtő rendszer keretében használt protokoll, például a Corba/IIOP.

Az ellenőrzőegység indítja az egyes vizsgálórutinkat, amelyek az ellenőrzések eredményeit visszaküldik az ellenőrzőegységnek.

Mivel egyidejűleg több AGB-ellenőr működik különböző olvasókkal, az ellenőrzőegységet párhuzamos kapcsolatokra alkalmasan célszerű kialakítani. Ez azt jelenti, hogy egyidejűleg több vizsgálatkérést képes teljesíteni, és a megfelelő választ a megfelelő olvasóra irányítani. Ezenkívül alkalmasnak kell lennie arra, hogy egyidejűleg több vizsgálatkérést, valamint az ellenőrzési lépések egy részét, például a hash-érték és a minimális díj vizsgálatát is párhuzamosan végrehajtsa.

Egy kapcsolat kezdetén közöljük a vezérlést végző ellenőrzőegységgel, hogy milyen típusú olvasóval kommunikál; az ellenőrzőegységnek lehetősége van arra, hogy callback-eljárásokkal segítségével kimeneti és manuális utóvizsgálati folyamatokat vezéreljen. Az üzemmód és az olvasó típusa szerint az eredményeket vagy a rádiós olvasóra, vagy a díjbiztosító rendszerre adja ki, valamint manuális vizsgálati eredményeket regisztrál.

Kriptokártya

Külön probléma annak a kulcsnak a megőrzése, amelylyel a kriptosztringet egy kétdimenziós vonalkóddá kell titkosítani, majd az ellenőrzéshez ismét visszafejteni. Ez a kulcs zárja ki a kétdimenziós vonalkód hamisítását, és ezért meg kell akadályozni a kulcs kifürkészését. Ezért különleges biztonsági intézkedéseket kell hozni, hogy ez a kulcs nyílt szöveggként sohasem jelenjen meg a merevlemezen, a memóriában vagy az átvitelnél, és erős kriptográfiai eljárásokkal kell biztosítani.

A tisztán szoftver alapú megoldások ezen a téren nem elég megbízhatóak, mivel egy kulcs a rendszer valamelyik helyén nyílt szöveggként jelenik meg, vagy a kulcs egy hibakeresővel nyílt szöveggként a tárból kiolvasható. Ez a veszély különösen azért fenyeget, mert a rendszerek távolról kezelhetők, illetve a javításokat esetleg házon kívül végzik.

Ezenkívül a kriptográfiai eljárások erősen leterhelik a rendszer processzorát, amely nincs optimalizálva az ilyen műveletek végrehajtására.

Ezért célszerű egy olyan kriptoprocesszor-kártyát alkalmazni, amelynek a következő jellemzői vannak:

- speciális kriptoprocesszor a kriptográfiai eljárások gyorsítására
- zárt black-box-rendszer a hozzáférés megakadályozására a biztonsági szempontból kritikus adatokhoz és eljárásokhoz.

Azoknál a kártyáknál, amelyek ezeket a jellemzőket teljesítik, autark rendszerekről van szó, amelyek a kivi-

telnek megfelelően a PCI- vagy az ISA-buszon keresztül vannak összekötve a számítógéppel, és egy meghajtón át kommunikálnak a számítógép szoftverrendszereivel.

A telepes áramforrással ellátott főtár mellett a kártyákon flash-ROM is van, amelyben egy egyéni alkalmazási kód tárolható. A külső rendszerekből nem lehet közvetlenül hozzáférni a kártyák főtárához, ami nagyon nagy biztonságot nyújt, mivel a biztonsági kulcsadatok és kriptográfiai eljárások csak a biztosított meghajtón át érhetők el.

Ezenkívül a kártyák saját érzékelőkkel figyelik, hogy vannak-e manipulációs kísérletek (a kártyák kialakítása szerint például hőmérsékleti csúcsok, sugárzás, a védőburkolat nyitása, feszültségcsúcsok).

Ha ilyen manipulációs kísérlet fordul elő, a telepes áramforrással ellátott főtár tartalmát azonnal töröljük, és azonnal kikapcsoljuk a kártyát.

A kriptoserver számára a bérmentesítési azonosító visszafejtéséhez, a hash-érték vizsgálatához, valamint a kulcsadatok importálásához szükséges funkciókat közvetlenül a kártyára kellene tölteni, mivel ezek a rutinok biztonsági szempontból nagyon fontosak.

Ezenkívül az összes kriptográfiai kulcsot, valamint a hitelesítés végrehajtásához szükséges tanúsítványok konfigurációit szintén a kártya telepes áramforrással ellátott tárában kellene biztosítani. Ha a kártya nem rendelkezik elegendő tárhellyel, akkor a kártyán általában egy mesterkulcsot tárolnak, amellyel a fent említett

adatokat titkosítják, majd elhelyezik a rendszer merevlemezén. Ez azonban azzal jár, hogy ezeknek az információknak a felhasználása előtt az adatokat először vissza kell fejteni.

Az alábbi táblázat áttekinti a különböző gyártók szóba jöhető kártyamodelljeit, és egyidejűleg megnevezi ezek tanúsítványait.

Az előnyös díjbiztosító rendszerben PC-bérmentesítéshez használható kriptokártyák:

Gyártó	Típusjelzés	Tanúsítvány
IBM	4758-023	FIPS PUB 140-1 Level 3 és ZKA-eCash
IBM	4758-002	FIPS PUB 140-1 Level 4 és ZKA-eCash (2000/07); CCEAL 5 (tanúsítás folyamatban)
Utimaco	Kriptoszerver	ITSEC-E2 és ZKA-eCash
Utimaco	Kriptoszerver 2000 (2001. 1. negyedév)	FIPS PUB 140-1 Level 3, ITSEC-E3 és ZKA-eCash (folyamatban)
Racal/Zaxus	WebSentry PCI	FIPS PUB 140-1 Level 4

A kártyával szemben támasztott követelmények teljesítése mellett a BSI által végzett kívánt tanúsítás miatt nagyon fontos, hogy mely modellek rendelkeznek már tanúsítvánnyal, és melyeknél van még folyamatban a tanúsítás.

A termékek számára kiállított tanúsítványok a különböző tanúsítóhelyek által alkalmazott három fokozatba sorolhatók be.

Az ITSEC az Európai Bizottság által nyilvánosságra hozott kritériumok szerint a biztonsági tulajdonságok alapján minősíti az IT-termékeket és IT-rendszereket. A megbízhatóságot E0-E6 fokozatok szerint értékelik, ahol az E0 fokozat nem megfelelő biztonságot, az E6 fokozat pedig a legnagyobb biztonságot jelenti. Továbbfejlesztés és a hasonló nemzetközi szabványokkal történt egyeztetés eredménye a CC (Common Criteria), amelynek szabványosítása az ISO-nál (ISO 15408) jelenleg folyamatban van. Ez a szabályrendszer alkalmazható a rendszer biztonságának értékelésére.

A fenti táblázatban felsorolt termékek egyike sem rendelkezik még CC szerinti tanúsítvánnyal. Az IBM 4758-002 sz. modell azonban jelenleg ebben a tanúsítási fázisban van.

Az FIPS PUB 140-1 szabvány az amerikai kormányzat által kiadott kritériumrendszert tartalmazza a kereskedelmi forgalomba hozható kriptográfiai eszközök megítéléséhez. Ez a kritériumrendszer nagyon erősen a hardvertulajdonságokra irányul. Az értékelés négy fokozatban történik, ahol az első szint a legalacsonyabb, a negyedik szint pedig a legmagasabb biztonságot jelenti.

A fent említett értékelési szabvány mellett létezik egy további kritériumrendszer, amelyet a Zentraler Kreditausschuss (ZKA) ad ki, és amely az elektronikus pénz területén alkalmazott IT-rendszerekre és IT-termékekre vonatkozik.

A kártyák már említett tulajdonságai és a megadott tanúsítványok mellett még egy sor további előny van, amelyeket az alábbiakban röviden felsorolunk:

- Saját (alálírt) szoftver kidolgozása és kártyára töltése lehetséges
- Integrált véletlenszám-generátor (FIPS PUB 140-1 tanúsított)
- DES, triple-DES és SHA-1 hardveroldalon megvalósítva
- RSA-kulcs előállítás és magán/nyilvános kulcs - feldolgozás 2048 bites kulcsméretig
- Kulcsmenedzsment - funkciók
- Tanúsítványmenedzsment - funkciók
- Részben több kriptokártya párhuzamos használata lehetséges egy rendszerben

Kriptointerfész

A kriptokártya-alkalmazás keretében biztonsági szempontból fontos funkciókat közvetlenül a kártyán tároljuk, és ezért ezek kívülről csak a kártyameghajtón át érhetők el. A meghajtó és a vezérlőegység közötti interfészként szolgál a kriptointerfész, amely a vizsgálórutinok iránti kéréseket meghajtónként a kártyára továbbítja.

Mivel egy számítógépen belül több kártya használható, a kriptointerfész feladata az is, hogy az egyes vizsgálatkérések teherelosztását elvégezze. Ez a funkció különösen akkor célszerű, ha még egy vagy egyes levélke-

zelő központokban több AFM-2D kódolvasó használja a kriptorendszer vizsgálórutinjait.

Egy további feladat a kommunikáció lebonyolítása a kulcsadatok elosztása céljából. A második fokozatban esetleg csak egy kezdetleges mechanizmus létezik, amely a biztonság kedvéért titkosított kulcsokat egy aláírt adatállományon belül átviszi. A kriptointerfésszel szemben követelmény, hogy olyan segédprogramot bocsásson rendelkezésre, amely lehetővé teszi egy ilyen adatállomány importját.

A kriptorendszer funkciói

Az ellenőrzés lefolyása az ellenőrzőegységben

A kétdimenziós vonalkód ellenőrzéséhez az ellenőrzőegység interfészként egy központi ellenőrzési funkciót bocsát az olvasó-, ill. olvasórendszerek rendelkezésére. Ez az ellenőrzési funkció koordinálja az egyes részvizsgálatok lefolyását.

Az egyes részvizsgálati rutinokból átadott kódokat a díjbiztosítási eseményhez egy előre megadott táblázat segítségével - amelyet előnyösen központilag kezelünk és viszünk át a kriptorendszerre - alakítjuk át a megfelelő díjbiztosítási kóddá. Ezen a táblázaton belül prioritásokat határozunk meg, amelyek szabályozzák a díjbiztosítási kódok kiosztását, ha több díjbiztosítási esemény fordul elő.

Ezt a díjbiztosítási kódot ezután egy leíró szöveggel együtt az ellenőrzés eredményeként visszaküldjük. A kriptorendszeren kívüli további feldolgozórendszernek megfelelően ezt az eredményt kiadjuk a rádiós olvasóra vagy a díjbiztosítási alkalmazáson belül, ill. az automatikus ellenőrzésnél egy TIT2-kóddá alakítjuk át, és ezt nyomtatjuk a küldeményre.

Mivel a kézi olvasórendszerek és az automatikus olvasórendszerek közötti folyamatok különbözőek, a mindegyik alkalmazási esethez más funkciót implementálunk.

Aszerint, hogy melyik kommunikációs mechanizmust alkalmazzuk az olvasórendszer és az ellenőrzőegység között, különbözik a hívás és az eredmények visszaadása. Egy szinkron RPC alapú protokoll, pl. Corba/IIOP, alkalmazása esetén az ellenőrzési módszert közvetlenül hívjuk, és az ellenőrzési eredményeket az ellenőrzés lezárása után átadjuk. A kliens, tehát az olvasóvezérlő, ill. az olvasórendszer ebben az esetben a végrehajtásra és az ellenőrzési eredmények visszaadására vár. Az utóbbinál ezért a kliensen több végrehajtási szál fut, azaz több párhuzamos ellenőrzés hajtható végre.

Aszinkron mechanizmusnál a TGM segítségével az olvasóvezérlő, ill. az olvasórendszer az ellenőrzési módszert nem közvetlenül hívja, hanem egy táviratot küldünk a kriptorendszerre, amely a vizsgálatkérést, a kétdimenziós vonalkód tartalmát és további információkat tartalmaz, például az aktuális rendezőprogramot. Ennek a táviratnak a kriptorendszerbe történő bevitelekor hívjuk az ellenőr-

zési funkciót, azt végrehajtjuk, és az olvasási és ellenőrzési eredményeket ismét egy új táviratként visszaküldjük. Ennek az eljárásnak az az előnye, hogy az igénylő rendszerben nem blokkolódik a folyamat, amíg rendelkezésre áll az eredmény.

Ellenőrzés kézi olvasórendszerekkel:

A kézi olvasórendszerek vizsgálórutinja bemeneti értékeként a kapcsolatazonosítót, valamint a kétdimenziós vonalkód tartalmát igényli. További paraméterként még a rendezőprogram azonosítója szükséges. Ez utóbbi paraméter szolgál a minimális díj meghatározására.

Az 5. ábra áttekintést ad az ellenőrzőegységen belüli ellenőrzés lefolyásáról abban az esetben, amikor az ellenőrzés indítása egy kéziolvasóról történik. Ekkor egy rádiós olvasóról végzett ellenőrzésből és ezt követően a címzés és a kétdimenziós vonalkód tartalmának összehasonlításából indulunk ki. Vezetékes olvasónál az ábrázolás hasonló módon történik a díjbiztosító rendszeren, ill. a díjbiztosítási alkalmazáson.

Az előnyösen rádiós olvasóval, olvasóvezérlővel és ellenőrzőegységgel végzett ellenőrzést szemléltető vázlat látható az 5. ábrán.

Az ellenőrzőegység vezérli az ábrázolt különösen előnyös kiviteli alaknál a részellenőrzések lefolyását, ahol az első részellenőrzés egy digitális bérmentesítési jelben levő mátrixkód beolvasását tartalmazza. A beolvasott mátrixkódot egy rádiós olvasó egy olvasóvezérlőre

viszi át. Ezután következik az olvasóvezérlő tartományában a mátrixkód ellenőrzése, valamint az átvitel az ellenőrzőegységre. Az ellenőrzőegység vezérli a kódtartalom felbontását. Az olvasás eredményét ezután a beviteli egységre - jelen esetben egy rádiós olvasóra - adjuk. Ezáltal azt tapasztalja például az olvasóegység használója, hogy le lehet olvasni a bérmentesítési jelet, és meg lehet ismerni a mátrixban elhelyezett információkat. Ezután az ellenőrzőegység visszafejt egy a mátrixkódban levő kriptosztringet. Ehhez célszerű először a bérmentesítési jel előállításához valószínűleg használt kulcs változatát vizsgálni. Ezután ellenőrizzük a kriptosztringben levő hash-értéket.

Ezután következik az előírányzott minimális díj ellenőrzése.

Ezenkívül ellenőrizzük a bérmentesítési jel előállítását vezérlő ügyfélrendszer azonosítószámát (bérmentesítési azonosító).

Ezt követően az azonosítószámot összehasonlítjuk egy tiltólistával.

Ezekkel az ellenőrzési lépésekkel, ebben a különösen egyszerű és célszerű formában lehetővé válik a jogosulatlanul előállított bérmentesítési jelek egyszerű módon történő felismerése.

Az ellenőrzés eredményét digitális üzenetként továbbítjuk, ahol a digitális üzenet például az eredeti rádiós olvasóra vihető át. Ezáltal például a rádiós olvasó használója a küldeményt kizárhatja a továbbítandó küldemények

közül. Az eljárás itt leírt változatának automatikus végrehajtásakor természetesen ugyanígy lehetséges a küldemény kizárása a postai küldemények normál feldolgozási láncolatából.

Előnyösen az ellenőrzés eredményét az ellenőrzőegység jegyzőkönyvezi.

Válaszértékként a díjbiztosítási esethez tartozó kódot és a hozzá tartozó szöveges jelentést, valamint a kétdimenziós vonalkód objektumot kell visszaküldeni.

Ellenőrzés AFM-2D kódolvasónál

Az AFM-2D kódolvasó ellenőrzőrutinjának beviteli paramétereiként szintén a kapcsolataazonosító, valamint a kétdimenziós vonalkód tartalma és az éppen aktív rendező-program egyértelmű ismertetőjele alkalmazható.

A 6. ábrán az ellenőrzés lefolyása tekinthető át az ellenőrzőegységben abban az esetben, amikor ezt egy olvasórendszer működésbe hozta.

Az ábrán a folyamat magyarázatához az optikai beviteli rendszert (IMM-rendszert), valamint az AFM-2D kódolvasót is feltüntettük, az ellenőrzés teljesebb szemléltetése érdekében. A kriptorendszernek megfelelő rész mindenestre a kétdimenziós kód és a visszaküldés közötti funkciókra, valamint az eredmény jegyzőkönyvezésére korlátozódik.

A táviratmenedzser-interfész esetében az ellenőrzőegységen több kiszolgálótaskot indítunk, amelyek az ellenőrzést kérő táviratra várnak, és a távirat tartalmá-

val hívják az ellenőrzőrutint. Megvárjuk az ellenőrzés eredményét, és azt egy táviratba foglaljuk, és visszaküldjük a kliensnek.

A 6. ábrán az ellenőrzőegység által végzett részellenőrzések vezérlésének egy további előnyös kiviteli alakja látható. Ennél a további előnyös kiviteli alaknál a bérmentesítési jeleket egy automatikus optikai beviteli rendszerrel (Prima/IMM) visszük be. Az adatok az optikai ellenőrzőegységről egy olvasó- és beviteli egységre (AFM-2D kódolvasó) kerülnek.

A digitális bérmentesítési jelek érvényességének ellenőrzésére szolgáló eljárás 6. ábrán látható kiviteli alakjánál a digitális bérmentesítési jeleket előnyösen még erősebben automatizált módon olvassuk be, például a postai küldemény egy olyan helyének optikai érzékelésével, ahol előnyösen egy bérmentesítési jel van elhelyezve. Az ellenőrzés további lépései lényegében az 5. ábrával kapcsolatban leírtaknak megfelelően történnek.

Az ellenőrző rutin válaszáértéke egyrészt a díjbiztosítási kódból és egy hozzátartozó jelentésből, valamint az átalakított és a bérmentesítési azonosítóval kibővített tartalomból áll. Ezekből a válaszáértékekből egy táviratot állítunk elő, és átvisszük az igénylő olvasórendszerre.

Tartalmi ellenőrzések

A kétdimenziós vonalkód tartalmának felbontása és átalakítása

Bemenet: letapogatott kétdimenziós vonalkód

Leírás:

Ebben a funkcióban a kétdimenziós vonalkód 80 bájt-ból álló tartalmát felosztjuk és egy strukturált objektummá alakítjuk át, amit a továbbiakban kétdimenziós vonalkód objektumnak nevezünk, hogy jobb ábrázolási lehetőséget, valamint hatékonyabb utólagos feldolgozást érjünk el. Az egyes mezőket és átalakításokat az alábbi táblázatban írjuk le:

A bináris számok decimális számokká alakításánál arra kell ügyelni, hogy egy bájtsorozat bal oldali bájtja a legmagasabb értékű bájt. Ha az átalakítás típuskötközés vagy hiányzó adatok miatt nem történik meg, "PC-F vonalkód nem olvasható" díjbiztosítási esetjelentést generálunk és küldünk vissza az ellenőrzőegységnek. Ebben az esetben nincs értelme a további tartalmi, ill. kriptográfiai ellenőrzésnek.

Mező	Típus	Átalakítás	Leírás
Postavállalat	ASCII (3 bájt)		Átalakítás nem szükséges
Bérmentesítés jellege	Bináris (1 bájt)	Kis egész szám	
Változat jele	Bináris (1 bájt)	Kis egész szám)	Az eljárás változatszama
Kulcs száma	Bináris (1 bájt)	Kis egész szám	Kulcstípus

Kriptosztring	Bináris (32 bájt)		A bájtsorozat változatlan átvétele, visszafejtés után a bérmentesítési azonosító kihasítása
Bérmentesítési azonosító		Szöveg (16 karakter)	A kriptosztring visszafejtése után kitöltve
Küldemény folyószáma	Bináris (3 bájt)	Egész szám	Csak pozitív számok
Termékkulcs	Bináris (2 bájt)	Egész szám	Pozitív számok, utalás a hozzá tartozó referencia-táblázatra
Díj	Bináris (2 bájt)	Lebeg	Átalakítás százszal oszt- ható pozitív decimális számmá, euróban megadva
Bérmentesítés dátuma	Bináris (3 bájt)	Dátum	Pozitív decimális számmá történt átalakítás után a dátum átalakítása év/hónap/nap (YYYYMMDD) formára
Címzett postai irányítószáma (PLZ)	Bináris (3 bájt)	Két érték, egyik az ország, másik a PLZ-kódhoz	Pozitív decimális számmá történt átalakítás után az első két jegy az országkódot, a többi öt jegy a postai irányítószámot adja meg
Utca/postafiók	ASCII (6 bájt)	Rövidített utcajel vagy postafiók	Ha az első két jegy szám, akkor egy irányítószám van kódolva, különben az utca és házszám első és utolsó három helye
Maradék bérmentesítési díj	Bináris (3 bájt)	Lebeg + pénznem (szöveg, 32 karakter)	Pozitív decimális számmá történt átalakítás után az első jegy a pénznemet adja meg (1=euró), a következő négy jegy a

			szám egész részét, és a maradék két jegy a törtrészt
Hash-érték	Bináris (20 bájt)		Változatlanul átvett bájtsorozat a bérmentesítés kriptográfiai érvényesítésére

Válaszérték: kétdimenziós vonalkód objektum

00 figyelmeztető kód, ha az átalakítás OK,
egyébként "PC-F vonalkód nem olvasható"
díjbiztosítási figyelmeztetés

Változatszám ellenőrzése

Bemenet: aktuális kétdimenziós vonalkód objektum

Leírás:

Az első három mezőből megismerhető a kétdimenziós vonalkód változata. Innen az is látható, hogy a bérmentesítési jel egyáltalán a Német Posta kétdimenziós vonalkódja, vagy egy másik szolgáltatóé. A mezők tartalmát az érvényes értékeknek az alkalmazásban előre konfigurált listájával kell összevetni. Ha nincs egyezés, a "PC-F verzió" díjbiztosítási figyelmeztetést küldjük vissza. Ebben az esetben további tartalmi és kriptográfiai ellenőrzésnek nincs értelme, az eljárást be kell fejezni.

Válaszérték: 00 figyelmeztető kód, ha a változat
ellenőrzése OK,

különben "PC-F verzió" díjbiztosítási
figyelmeztetés

Bérmentesítési azonosító ellenőrzése

Bemenet: kétdimenziós vonalkód objektum visszafejtett
bérmentesítési azonosítóval

Leírás:

A kétdimenziós vonalkódban levő bérmentesítési azonosítót egy ellenőrzőszámossal (CRC 16 ciklikus redundanciaellenőrzés) biztosítjuk, amit ezen a helyen ellenőrzünk. Ha ez az ellenőrzés hibát mutat ki, eredményként "PC-F hamisítási gyanú (bérmentesítési azonosító)" díjbiztosítási figyelmeztetést küldünk vissza. A bérmentesítési azonosító ellenőrzéséhez előzetesen vissza kell fejteni a kriptosztringet.

Válaszérték: "00" kód, ha az ellenőrzés OK,
különben "PC-F hamisítási gyanú
(bérmentesítési azonosító)" figyelmeztető
kód

Időtűllépés ellenőrzése

Bemenet: kétdimenziós vonalkód objektum

Leírás:

Ez a funkció egy PC-bérmentesített küldemény bérmentesítése és a levélkezelő központban történő feldolgozása

közötti időtartam automatikus ellenőrzésére szolgál. A két időpont között csak adott számú nap telhet el. A napok száma a termékhez és ennek továbbítási idejéhez igazodik, amihez még egy nap várakozási idő járul.

Az időtartam-konfigurációt előnyösen egy termékérvényességi idő táblázatban tároljuk, és egy gondozómaszk keretében központilag gondozzuk. A táblázatban rögzítjük a PC-bérmentesítésnél lehetséges minden egyes termék-kulcshoz (a kétdimenziós vonalkód mezője) tartozó napok számát, amelyek a bérmentesítés és a levélkezelő központban történő feldolgozás között eltelhetnek. Egy egyszerűsített eljárásban csak egy időtartamot adunk meg előre, amely a szabványos küldeményekre vonatkozik, és amelyet konstansként tartalmaz a rendszer.

Az ellenőrzéshez a feldolgozásnál az aktuális vizsgálati időpont és a kétdimenziós vonalkódban elhelyezett időpont között eltelt napok számát képezzük; ha például a két dátum 08. 02. és 08. 01, az eltelt napok száma 1. Ha az így meghatározott napok száma nagyobb a termék számára előre megadott értéknél, akkor a "PC-F dátum (bérmentesítés)" díjbiztosítási figyelmeztetéshez hozzárendelt kódot küldjük vissza az ellenőrzőegységnek, egyébként pedig a sikeres ellenőrzést igazoló kódot. Ha egy egyszerűsített eljárásban mindig a szabványos küldeményekre megadott értékkel végezzük az összehasonlítást, az ellenőrzési eredmény kiadása után lehetőséget kell biztosítani az eredmény korrigálására például az olvasó

egy gombjának manuális működtetésével, ha az aktuális terméknel hosszabb a megengedett továbbítási idő.

Az időtúllépés további ellenőrzése a bérmentesítési azonosító tartalmára vonatkozik. Az előre megadott és letöltött bérmentesítési összegnek és azonosítónak adott érvényességi ideje van, amelynek folyamán a küldeményeket bérmentesíteni kell. A bérmentesítési azonosító tartalmazza azt az időpontot, ameddig a bérmentesítési díj érvényes. Ha a bérmentesítés időpontja meghatározott számú nappal túllépi az érvényesség idejét, akkor a "PC-F dátum (bérmentesítési díj)" díjbiztosítási figyelmeztetéshez tartozó kódot küldjük vissza.

Válaszérték: "00", ha az ellenőrzés OK,

egyébként "PC-F dátum (bérmentesítési díj)"

vagy "PC-F dátum (bérmentesítés)"

díjbiztosítási figyelmeztető kód.

Díjellenőrzés

Bemenet: kétdimenziós vonalkód objektum; aktuális

rendezőprogram-azonosító

Leírás:

Ezen a funkción belül ellenőrizzük a kétdimenziós vonalkódban levő díjat egy minimális díjhoz viszonyítva, amely a hozzátartozó rendezőprogram küldeményeihez van definiálva. A díjak euróban vannak megadva.

A rendezőprogram és a minimális díjak közötti hozzárendelések egy automatikus interfészen át történnek.

Egy egyszerűsített eljárás hasonlóan alkalmazható, mint az időtúllépés ellenőrzésénél. Itt az alkalmazáshoz tartozó konfigurációs adatállomány egy állandó minimális díjat határoz meg, amely az összes küldeményre érvényes. Ezért a rendezőprogram átadása nem szükséges.

Az ezt követő ellenőrzésnél összehasonlítjuk, hogy a kétdimenziós vonalkódban rögzített minimális díj alatta van-e az említett értéknek. Ha igen, a "PC-F díjhiány" díjbiztosítási kódot küldjük vissza, egyébként a sikeres ellenőrzést jelentő kódot.

Válaszérték: "00" kód, ha az ellenőrzés OK,
egyébként "PC-F díjhiány" díjbiztosítási
figyelmeztető kód.

Tiltólista egyeztetése

Bemenet: kétdimenziós vonalkód objektum visszafejtett
bérmentesítési azonosítóval

Leírás:

Ezen a funkción belül azt ellenőrizzük, hogy a kétdimenziós vonalkódhoz tartozó bérmentesítési azonosítót tartalmazza-e egy tiltólista-adatállomány. A tiltólisták arra szolgálnak, hogy ki lehessen zárni azokat az ügyfeleket, akik visszaéléssel próbálkoztak, vagy akiknek a számítógépét ellopták.

A tiltólistákat tartalmazó adatállományokat a bérmentesítési adatbank projekt központilag kezeli. Az ide csatlakozó interfész keretében határozható meg az az eljárás, amellyel az adatcsere lebonyolítható a szétszór-tan elhelyezkedő levélkezelő rendszerek felé.

Ha a gondozási alkalmazás, ill. az adatcsere esetleg még nem létezik, egy átmeneti mechanizmust kell létrehozni. Ezeknek az adatoknak a gondozása átmenetileg történhet egy Excel-lapon, amelyből egy CSV-adatállományt generálunk. Ezt az adatállományt elektronikus postával elküldjük az AGB-ellenőrnek, és innen egy importmechanizmuson keresztül beolvassuk a rendszerekbe. Később megtörténik az átvitel az előnyös díjbiztosítási-IT-finomkon koncepcióban definiált úton.

Egy bérmentesítési azonosító egyetlen előírást határoz meg, amelyet egy ügyfél a rendszerből (a bérmentesítési helyről) lehív. Ezeket az előírásokat az ügyfélrendszer egy ún. biztonsági rekeszben tárolja. Itt egy olyan hardverkomponensről van szó, amely intelligens kártyaként van kialakítva, és olvasórendszerrel, ill. hardverkulccsal van ellátva. A biztonsági rekeszben biztonságosan őrizzük az előírt díjakat, és az ügyfél onnan lehívhatja az egyes bérmentesítési díjakat anélkül, hogy online kapcsolatban lenne a bérmentesítési hellyel.

Mindegyik biztonsági rekeszt egy egyértelmű azonosító jellemzi. Ezt a biztonságirekesz-azonosítót bevisszük a tiltólista-adatállományba, ha a hozzátartozó küldeményeket visszaélés gyanúja miatt ki kell zárni. A

biztonságirekesz-azonosító több mezőből áll. Az egyértelmű kulcs mellett a biztonságirekesz-azonosítóban további mezők is vannak, például az érvényességi idő és az ellenőrzőszámok számára. A biztonsági rekesz egyértelmű azonosításához a biztonságirekesz-azonosító első három mezője a fontos. Ezek a bérmentesítési azonosító első három mezőjében is megtalálhatóak, aminek következtében elvégezhető a biztonsági rekesz és az előírás közötti hozzárendelés. A mezőket az alábbi táblázatban írjuk le:

Bájt szám	Hossz	Jelentés	Adattartalom	Megjegyzés
b1	1	Ajánlattevő ismertetőjele	00 01 FF	Használaton kívül Tesztajánló: postavállalat A postavállalat bérmentesítési pontja
b2	1	Engedélyezett modellszám	XX	Mindegyik gyártónak 01-től (első benyújtott modell) emelkedően mindegyik újonnan engedélyezett modellhez
b3, b4, b5	3	A modell sorozatszáma	XX XX XX	Mindegyik gyártó mindegyik engedélyezett modelljéhez 00 00 00-tól emelkedően FF FF FF-ig

Ha az éppen ellenőrzött bérmentesítés bérmentesítési azonosítójának első három mezője azonos a tiltólista-adatállományban levő biztonságirekesz-azonosító első három mezőjével, akkor a tiltólista-adatállományban az ügyfélhez hozzárendelt díjbiztosítási esetnek megfelelő választ küldjük vissza, egyébként az ellenőrzés sikerét jelentő kódot.

Válaszérték: "00" kód, ha az ellenőrzés OK,
különben az ügyfélhez, ill. a biztonsági
rekeszhez a tiltólista-adatállományban
hozzárendelt figyelmeztető kód.

A kétdimenziós vonalkód tartalmának összehasonlítása a
küldemény nyílt szövegével

Bemenet: kétdimenziós vonalkód objektum

Leírás:

Annak megakadályozására, hogy kétdimenziós vonalkódok másolatait elő lehessen állítani, összehasonlítjuk a kétdimenziós vonalkódban kódolt küldeményadatokat a levélen nyílt szövegben feltüntetett adatokkal. Ez az összehasonlítás a rádiós olvasóknál közvetlenül lehetséges, mivel ott megfelelő ábrázolási és beviteli lehetőségek vannak. A vezetékes kézi olvasóknál az ellenőrzést a PC-n (díjbiztosítási rendszer) kell végrehajtani.

A folyamat úgy néz ki, hogy az ellenőrzőegység az automatikus ellenőrzések megtörténte után a rádiós olva-

són, ill. a díjbiztosítási PC-n kezdeményezi a kétdimenziós vonalkód adatainak kiadását. Ehhez egy visszahívó eljárás áll rendelkezésére, amelyet az elején hozzárendelünk egy kapcsolathoz.

Ennek a hívása történik az aktuális kétdimenziós vonalkód objektummal. Ezután az olvasóvezérlő, ill. díjbiztosítási PC felelős a kétdimenziós vonalkód tartalmának ábrázolásáért, és küld vissza a visszahívó eljárás válaszáértékeként (az ellenőr által végzett feldolgozás után) egy "00"-t, ill. egy hozzá tartozó hibakódot.

Sikeres kiértékelés után az ennek megfelelő kódot, egyébként pedig a "PC-F nyílt szöveg" díjbiztosítási figyelmeztető kódot küldjük vissza.

Automatikus ellenőrzésnél ez a vizsgálat nem szükséges. Ebben az esetben az ellenőrzés előnyösen a központi kiértékelések keretében offline akár forgalomösszehasonlítással, akár a rendeltetési hely postai irányítószámának és a kétdimenziós vonalkódban rögzített postai irányítószámnak az összehasonlításával elvégezhető.

Válaszárték: "00" kód, ha az ellenőrzés OK,
egyébként "PC-F nyílt szöveg" díjbiztosítási
figyelmeztető kód

Kriptográfiai ellenőrzések

A kriptográfiai ellenőrzés két részből áll:

a) a kriptosztring visszafejtéséből és

b) a hash-érték összehasonlításából.

Mindkét eljárást a kriptokártya védett tartományában kell végrehajtani, mivel egy ügyfél a feldolgozáskor keletkező információ kikémlelésével a bérmentesítéshez érvényes hash-értékeket tudna előállítani.

Kriptosztring visszafejtése

Bemenet: kétdimenziós vonalkód objektum

Leírás:

Ez a funkció bemeneti paraméterként a leolvasás eredményének felbontott kétdimenziós vonalkód objektumát kapja meg. A bérmentesítés dátuma és a kulcsszám alapján kikeressük az ebben az időpontban érvényes szimmetrikus kulcsot, és az átadott objektum kriptosztringjét ennek a kulcsnak a segítségével a triple-DES CBC eljárással visszazafejtjük. Hogy milyen kezdeti értéket kell adni az inicializáló vektornak, ill. hogy belső vagy külső CBC-vel és milyen blokkhosszal dolgozunk, azt a díjbiztosítási rendszerhez kapcsolódó interfész keretében döntjük el.

Ha a kétdimenziós vonalkódban levő kulcs nincs meg a kriptorendszerben, akkor a "PC-F hamisítási gyanú (kulcs)" díjbiztosítási figyelmeztetést küldjük vissza azzal a hibajelentéssel, hogy a kulcsot a kulcsszámmal nem találtuk meg.

A művelet eredménye a visszafejtett bérmentesítési azonosítóból, valamint a visszafejtett véletlen számból áll. A visszafejtett bérmentesítési azonosítót a kétdi-

menziós vonalkód objektum egy megfelelő mezőjében helyezzük el. A véletlen számot biztonsági okokból nem szabad ismertté tenni, mert az ügyfél ennek az információnak a birtokában érvényes hash-értékeket állíthatna elő, és ezekkel kétdimenziós vonalkódokat hamisíthatna.

A visszafejtést követően kezdeményezzük a hash-érték számítását, és visszaküldjük a válaszerőteket.

Hash-érték számítása

Bemenet: kétdimenziós vonalkód objektum

a kriptosztringből visszafejtett véletlen szám
(a visszafejtett véletlen szám a kártyán kívül
nem lehet ismert)

Leírás:

A hash-érték számításának funkciója a kétdimenziós vonalkód objektumban levő eredeti leolvasási eredményből meghatározza az első 60 bájtot. Ehhez kapcsolódik a visszafejtett bérmentesítési azonosító, valamint az átadott visszafejtett véletlen szám. Ebből az SHA 1 eljárással egy hash-értéket számítunk ki, és összehasonlítjuk a kétdimenziós vonalkódnak a kétdimenziós vonalkód objektumban levő hash-értékével. Ha mind a 20 bájt egyezik, a kriptográfiai ellenőrzés sikeres, és egy ennek megfelelő válaszerőteket küldünk vissza.

Ha nincs egyezés, egy "PC-F hamisítási gyanú (hash-érték)" díjbiztosítási figyelmeztetést küldünk vissza az ellenőrzőegységre.

Válaszértékként a kiszámított hash-értéket is átvisz-
szük, hogy ezt az ellenőrzés eredményével együtt ki le-
hessen adni.

Válaszérték: kiszámított hash-érték

"00" kód, ha az ellenőrzés OK, különben
"PC-F hamisítási gyanú (hash-érték)" vagy
"PC-F hamisítási gyanú (kulcs)"
díjbiztosítási figyelmeztető kód.

Eredmény kiadása

Ellenőrzési és olvasási eredmény ábrázolása

Leírás:

Egy visszahívási eljárás segítségével az ellenőrző-
egységnek lehetősége van arra, hogy vezérelje az eredmény
kiadását az aktuális ellenőrzéshez tartozó kimeneti esz-
közre. Ehhez átadja a visszahívási eljárásnak a kétdimen-
ziós vonalkód objektumot és a meghatározott díjbiztosítá-
si figyelmeztető kódot. Válaszértékként az AGB-ellenőr
által kiválasztott utólagos feldolgozási eljárás kódja
szolgáltatatható.

A visszahívási eljárást a kivitelhez szintén a kap-
csolat elején, az ellenőrzőegységen történő jelentkezés-
kor jelöljük ki.

Az eredmény jegyzőkönyvezése

Bemenet: kétdimenziós vonalkód objektum, az ellenőrzési
eredmény kódja

Leírás:

Az eredmény jegyzőkönyvezése egy egyszerűsített eljárás keretében egy adatállományban azon a rendszeren történik, amelyen az ellenőrzőegység fut. Általában az eredményeket, ill. jelentéseket közvetlenül a BDE-re visszük át, és az előnyös díjbiztosítási BDE-interfészen át beírjuk az előnyös helyi díjbiztosítási rendszer adatbankjába.

Előnyösen tároljuk a bérmentesítési azonosítót, a folyószámot, a bérmentesítési dátumot, a díjat, a termékulcsot, a postai irányítószámot, a díjbiztosítási eredménykódot, a jelentés szövegét, az ellenőrzés időtartamát, az ellenőrzés időpontját, az olvasó azonosítóját, az olvasó üzemmódját, a regisztrálás módját, valamint a további feldolgozás módját. Az összes értéket, egymástól pontosvesszővel elválasztva, küldeményenként egy rekordban adjuk ki; a további kiértékelés például Excel-ben történhet.

Ha a rendszer "első érzékelés" üzemmódban van, akkor az érzékelési mód oszlopban "e"-t, egyébként az utólagos érzékelésre "n"-t kell megadni.

Törzsadatok előkészítése

Leírás:

A tartalmi ellenőrzéshez egy sor törzsadat szükséges:

- PC-F tiltólisták
- Rendezőprogramok és minimális díjak
- Általános minimális díj
- PC-F termékkulcsok
- Maximális feladási idő PC-F termékkulcsonként
- Általános maximális feladási idő
- Díjbiztosítási esetek, prioritások és hozzárendelés a további kezelésre vonatkozó utasításokhoz
- További kezelésre vonatkozó utasítások

A törzsadatok egy átmeneti időben, a PC-F tiltólisták, valamint a bérmentesítési hely kriptográfiai kulcsainak kivételével, előre fixen konfigurálhatók.

Ha szükséges, az adatok egy részéhez egyszerű feldolgozási és elosztási alkalmazások implementálhatók. A kezelés egy Excel-lapon történhet, amelyből egy CSV-adatállomány generálható. Ezt az adatállományt elektronikus postával elküldjük az AGB-ellenőrnek, és onnan egy megfelelő mechanizmuson át beolvassuk a rendszerbe.

Általában az adatokat az előnyös díjbiztosítási-IT-finomkonceptióval kapcsolatban leírt eljárásnak megfelelően osztjuk el, ill. tesszük lehetővé a hozzáférést ezekhez az adatokhoz.

A hozzá tartozó adatstruktúrákat az előnyös díjazás-biztosítás finomkonceptiójához tartozó adatmodellben írjuk le.

A kulcsadatok elosztása

A szimmetrikus kulcsokat, amelyek a bérmentesítési helyen a kétdimenziós vonalkódok tartalmának biztosítására szolgálnak, és amelyekre a kriptorendszernek szüksége van az ellenőrzéshez, biztonsági okokból szabályos időközökben kicseréljük. Az összes levélkezelő központban történő alkalmazáshoz a kulcsokat automatikusan és biztonságosan kell átvinni a bérmentesítési helyről a kriptorendszerekhez.

A cserét az előnyös díjbiztosítási szerveren át kell lebonyolítani, hogy a bérmentesítési helyen ne kelljen konfigurálni, hogy mely helyi díjbiztosítási rendszerek, és mely kriptorendszerek léteznek ehhez.

A kulcscsere különösen előnyös eljárási lépései láthatók a 7. ábrán. Az előnyös kulcscsere egy központi bérmentesítési hely, egy központi kriptoserver és több helyi kriptoserver között történik.

Mivel a szimmetrikus kulcsoknak nagy jelentőségük van a kétdimenziós vonalkód hamisítással szembeni védelme szempontjából, a cserét erős titkosítással és a kommunikációs partner egyértelmű azonosításával kell biztosítani.

Konfiguráció

A kriptohardver alapkonfigurációja/kulcsmenedzsmentje

A kriptokártya alapkonfigurálásához különböző intézkedések szükségesek. Ezeket egy biztonsági adminisztrátornak kell végrehajtani. Nagy vonalakban a következő tevékenységekről van szó:

- Szoftver-API-k installálása a kártyán
- A titkos kulcs generálása, ill. installálása az adminisztrációs alkalmazások és a közreműködő szoftverek biztosításához

A választott kártyatípusnak és -gyártónak megfelelően eközben különböző intézkedések szükségesek.

A kriptokártya alapkonfigurálása az előnyös díjbiztosítási rendszerhez tartozó alkalmazásnak megfelelően a következő lépésekből áll:

- A szimmetrikus kulcsok - például RSA-kulcspár - biztonságos titkosítása és átvitele a kártyára, és egyidejűleg tanúsítvány előállítás a nyilvános kulcshoz, és a kulcsok kiadása
- A bérmentesítési hely tanúsítványának fix előzetes konfigurálása annak biztosítékaként, hogy az importálandó kulcsot a bérmentesítési hely állította ki.

A kriptorendszer-alkalmazás alapkonfigurálása

Mindegyik olvasót, mindegyik felhasználót és mindegyik kriptokártyát a kriptorendszerben egy egyértelmű azonosítóval kell ellátni. Végül mindegyik AFM-2D-kódolvasót is egy egyértelmű azonosítóval kell azonosítani.

Bejelentkezés/kijelentkezés

Az ellenőrzőegységgel létesített kapcsolat kezdetén be kell jelentkezni. Ez a bejelentkezés paraméterként tartalmazza az olvasó azonosítóját, a felhasználó azonosítóját, valamint a visszahívási eljárásokat a manuális ellenőrzéshez, ill. az olvasási és ellenőrzési eredmények kiadásához.

Válaszértékként egy kapcsolatazonosítót küldünk vissza, amelyet a kapcsolat folyamán az ellenőrzési hívásoknál át kell adni. Az ellenőrzőegység a kapcsolatazonosítóhoz egy kapcsolatkörnyezetet tárol, amely az átadási paramétereket tartalmazza.

Ha a felhasználó a kapcsolat folyamán változtat az üzemmódon, az előre meghatározott terméken, ill. a futás-idő alatt konfigurálható további beállításokon, akkor ezeket a változtatásokat végrehajtjuk a kapcsolatkörnyezeten belül hozzárendelt változóknak.

Kijelentkezéskor töröljük a kapcsolatkörnyezetet. Az ezzel a kapcsolatazonosítóval érkező további ellenőrzési felhívásokat elutasítjuk.

A felhasználók és jelszavak kezelését az előnyös díjazásbiztosításhoz kidolgozott általános felhasználókezelési koncepcióban definiáljuk, amely a díjbiztosítási IT finomkoncepciójának alkotórésze.

Az olvasórendszereknek az ellenőrzési megkeresések végrehajtása előtt regisztráltatni kell magukat az ellenőrzőegységnél. Paraméterként az olvasórendszer azonosítóját, valamint egy jelszót kell megadni. Sikeres bejelent-

kezés esetén válaszáértékként szintén egy kapcsolatazonosítót küldünk vissza, amelyet a következő ellenőrzési megkereséseknél meg kell adni.

Az olvasórendszer leállításánál ezzel a kapcsolat-azonosítóval kell kijelentkezni.

Egyebek

Speciális felhasználói szerepek

A biztonsági koncepció keretében két speciális felhasználói szerep van, amelyeket két különböző személynek kell betölteni.

Biztonsági adminisztrátor

A biztonsági adminisztrátor szerepe a következő feladatokat foglalja magában:

- Utasítás-adatállományok felállítása a kriptokártya adminisztrálásához
- Ezeknek az utasítás-adatállományoknak az aláírása
- A kriptokártyák inicializálása és kezelése
- A felhasznált szoftver és a hozzá tartozó konfiguráció ellenőrzése

A biztonsági adminisztrátor a titkos kulccsal azonosítja magát a kártya adminisztrálásához. A kulcs pl. hajlékonylemezen vagy intelligens kártyán tárolható, amit a biztonsági adminisztrátor szigorúan elzárva tart.

Csak ezzel a kulccsal aláírt adminisztrációs utasítások hajthatók végre a kriptokártyán. Mivel ez a mecha-

nizmus védi az utasítássorozatot és a hozzá tartozó paramétereket, ezeknek az utasításoknak a végrehajtása a helyszíni rendszeradminisztrátorokra is átruházható. Ehhez a biztonsági adminisztrátor rendelkezésre bocsátja az utasításokat, és megfelelő eljárási útmutatást ír.

Egy további feladat a kriptokártyák kezelése, ahol minden kártyához rögzíteni kell a sorszámot, annak a rendszernek a konfigurációját és rendszerszámát, amelyben installáljuk a kártyákat, valamint a rendszer helyét. A tartalék kriptokártyáknál azt is rögzíteni kell, hogy azok kinek a birtokában vannak.

Feladata az is, hogy a biztonsági QS-menedzserrel együtt kontrollálja a szoftverforrásokat és a hozzá tartozó szoftverkonfigurációt, és ezt átadja az installáláshoz.

Ezenkívül ellenőrzi a kártyán és a kriptoserveren installálandó vagy már installált szoftvert, valamint átadja és aláírja a kártyaszoftvert.

A kártyaszoftvert különösen abból a szempontból kell ellenőrizni, hogy valamelyik helyen a titkos kulcsok egyike a meghajtóinterfészen át kiadható-e, ill. hogy ott előfordultak-e manipulációs kísérletek, például állandó, előre meghatározott kulcsok tárolása, vagy nem biztonságos titkosítási eljárások alkalmazása. Ezenkívül a kártyaszoftverhez a kriptoservernek a vele kapcsolatban álló alkalmazási szoftverét is ellenőrizni kell.

A hitelesítés egy titkos kulccsal ugyanúgy történik, mint a rendszeradminisztrátornál. Itt azonban a szoftver-aláírássra szolgáló titkos kulcsról van szó.

További biztonságot jelent az, hogy a szoftver installálásához nem csak a szoftvert kell aláírni, hanem a hozzá tartozó installálási utasításokat is. Mivel erre két különböző személy illetékes (QS-menedzser és biztonsági adminisztrátor), és azért, mert a hozzá tartozó kulcsokat két különböző helyen őrzik, fokozódik a biztonság.

A szoftver elosztását a biztonsági QS-menedzser a biztonsági adminisztrátorral összhangban végzi.

A találmánynak ez a különösen előnyös kiviteli alakja tehát két különböző hitelesítőkulcsot alkalmaz, ami jelentősen növeli az adatbiztonságot.

Szabadalmi igénypontok

1. Eljárás postai küldeményre felvitt digitális bérmentesítési jel hitelességének ellenőrzésére, amelynek során a bérmentesítési jelben levő kriptográfiai információkat visszafejtjük, és a bérmentesítési jel hitelességének ellenőrzésére használjuk fel,
azzal jellemezve, hogy egy ellenőrzőegységgel részellenőrzések lefolyását vezéreljük, ahol egy első részellenőrzés folyamán beolvasunk egy, a digitális bérmentesítési jelben levő mátrixkódot, az ellenőrzőegységgel vezéreljük a mátrixkód tartalmának felbontását, a részellenőrzéseket ellenőrzési lépésekként hajtjuk végre, több ellenőrzéskérés, valamint ezekkel párhuzamosan az ellenőrzési lépések egy részének egyidejű végrehajtására alkalmas ellenőrzőegységet alkalmazunk, az ellenőrzési lépésekkel feltárjuk a jogosulatlanul előállított bérmentesítési jeleket, az ellenőrzés eredményét digitális üzenetként közöljük, és ezzel egy küldeményt kizárunk a postai küldemények normál feldolgozásának menetéből.
2. Az 1. igénypont szerinti eljárás,
azzal jellemezve, hogy a részellenőrzések egyikének folyamán fejtjük vissza a bérmentesítési jelben levő kriptográfiai információkat.
3. Az 1. vagy 2. igénypont szerinti eljárás,

azzal jellemezve, hogy a részellenőrzések egyikének folyamán összehasonlítjuk a bérmentesítési jel előállításának dátumát az aktuális dátummal.

4. Az 1-3. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy az olvasóegység és az ellenőrzőegység között szinkron protokoll segítségével információkat cserélünk.

5. A 4. igénypont szerinti eljárás, azzal jellemezve, hogy RPC-alapú protokollt alkalmazunk.

6. Az 1-5. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy az olvasóegység és az ellenőrzőegység egymás közötti kommunikációjához aszinkron protokollt alkalmazunk.

7. A 6. igénypont szerinti eljárás, azzal jellemezve, hogy az olvasóegységről adattáviratot küldünk az ellenőrzőegységre.

8. A 7. igénypont szerinti eljárás, azzal jellemezve, hogy az adattávirat a bérmentesítési jel tartalmát foglalja magában.

9. Az 1-8. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy az adattávirat felszólítást tartalmaz egy kriptográfiai ellenőrző rutin megindítására.

10. Az 1-9. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy egy kriptointerfészen át teherelosztást végzünk több ellenőrző eszköz között.
11. Az 1-10. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy a bérmentesítési jel tartalmát mezőkre osztjuk fel.
12. Az 1-11. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy a bérmentesítési jel előállítását vezérlő ügyfélrendszer azonosítószámát (bérmentesítési azonosítót) a bérmentesítési jelből határozzuk meg.
13. Az 1-12. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy az ügyfélrendszer egyes azonosító adatait (bérmentesítési azonosító) tiltólista-adatállományba helyezzük, és az ehhez a bérmentesítési azonosítóhoz tartozó küldeményeket kizárjuk a postai küldemények normál feldolgozásának menetéből.
14. Az 1-13. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy egy címzettnek a bérmentesítési jelben titkosítva megadott címét összehasonlítjuk a postai küldemény továbbításához megadott címmel.
15. Az 1-14. igénypontok bármelyike szerinti eljárás,

azzal jellemezve, hogy változtatjuk az eljárás ellenőrzési paramétereit.

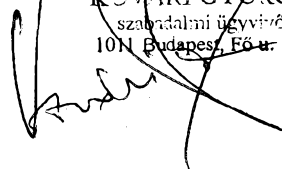
16. Az 15. igénypont szerinti eljárás, azzal jellemezve, hogy az eljárási paraméterek változtatását csak egy rendszeradminisztrátor személyes digitális kulcsának (magánkulcs) bevitele után hajtjuk végre.

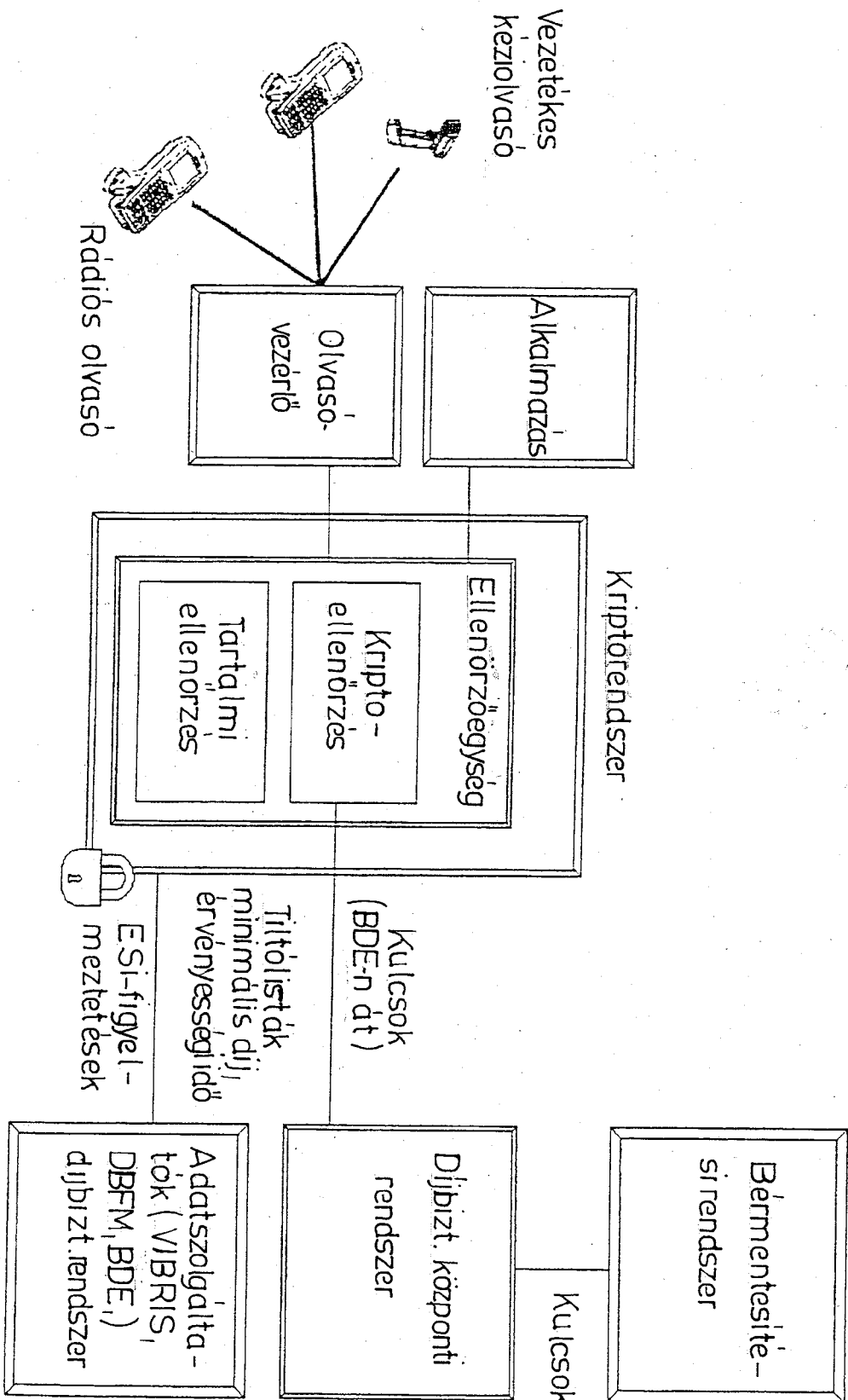
Frajz, F. a. Kovari



A meghatalmazott:

ADVOPATENT
SZABADALMI ÉS VEDJEGY IRODA
KOVARI GYORGY
szabadalmi ügyvivő
1011 Budapest, Fő u. 19.



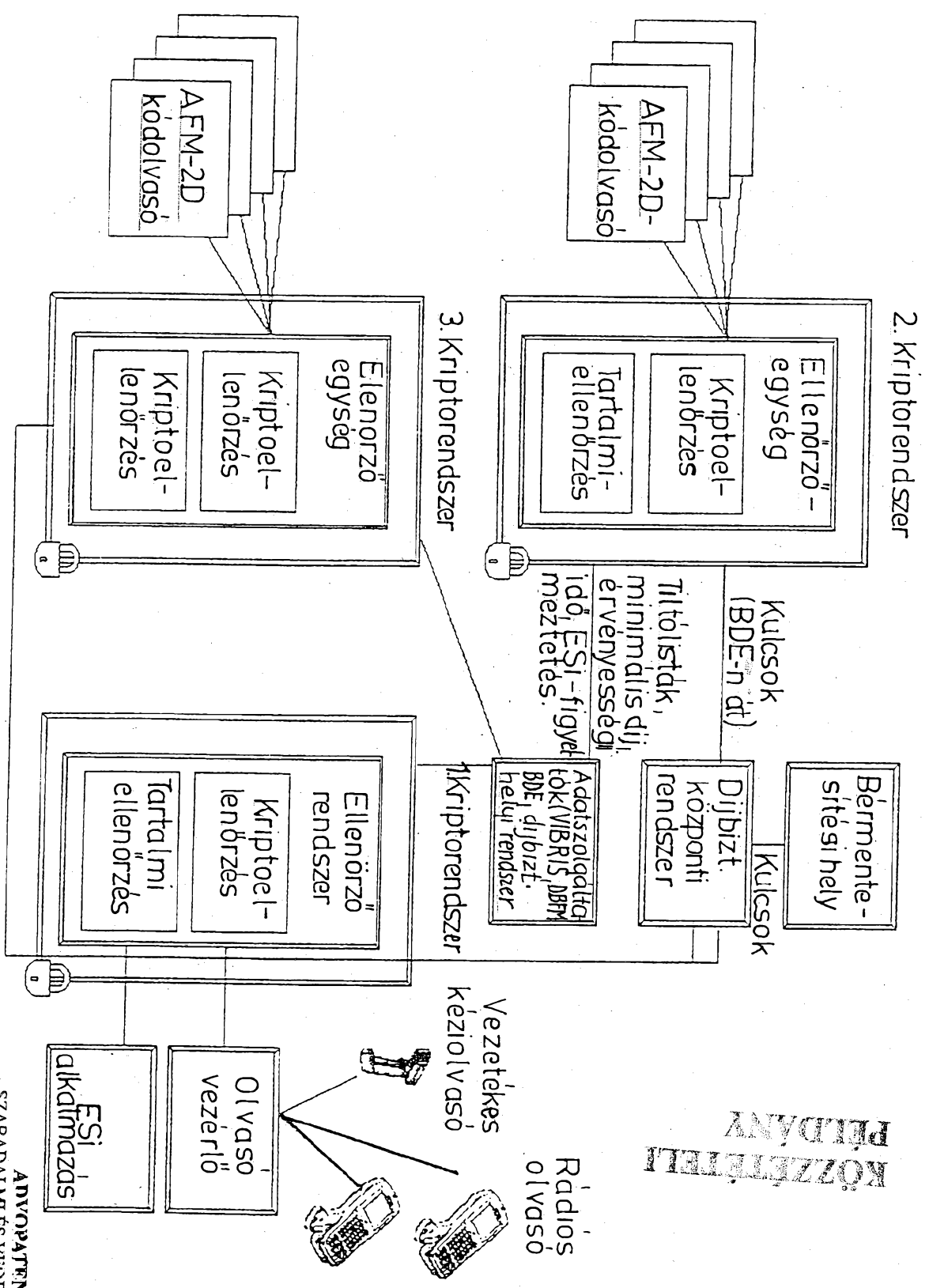


1. ábra

0400462

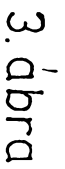
P 0400462

2. ábra



KÖZZÉTETEL
PÉLDÁNY

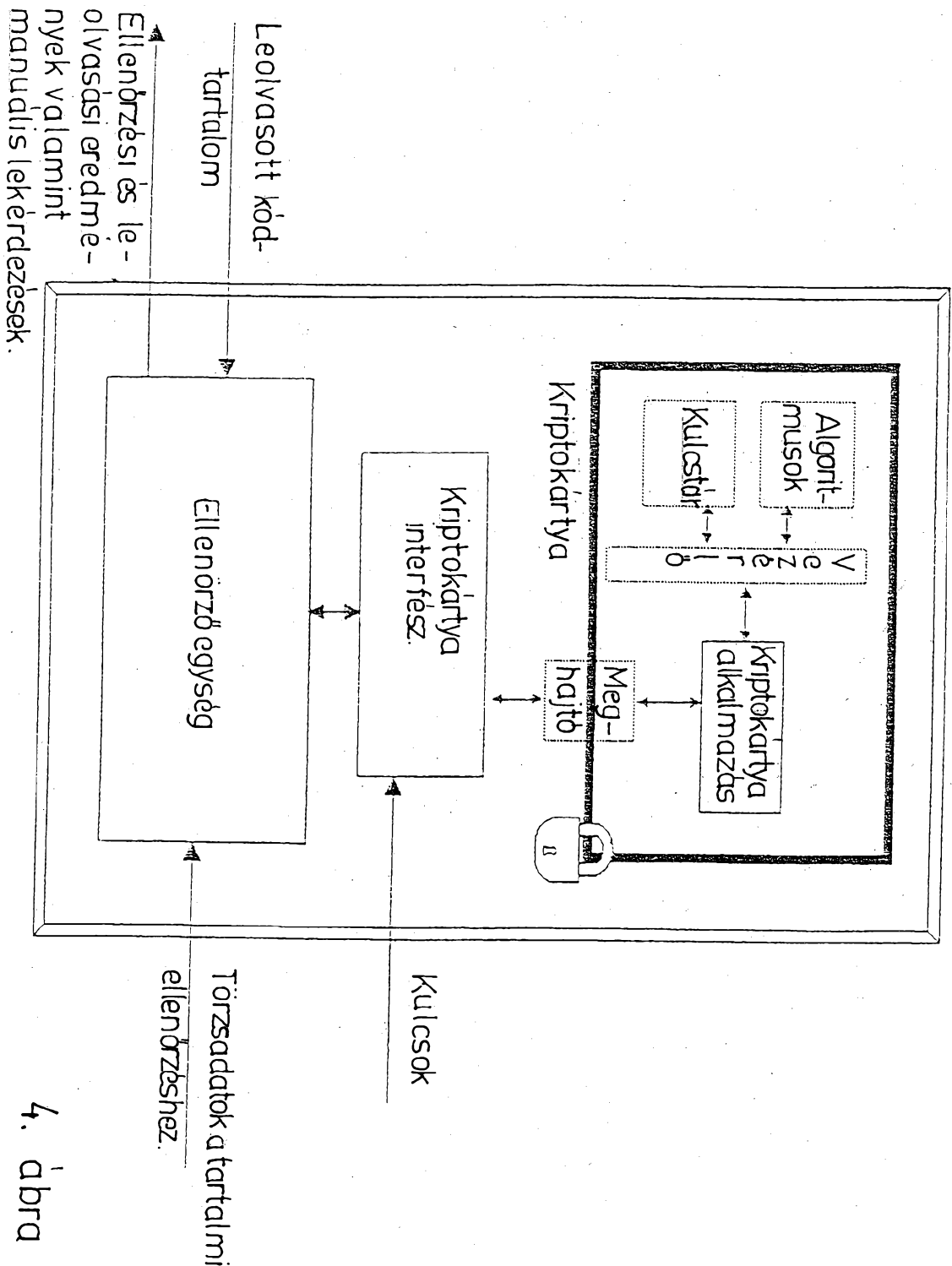
Dijbízti helyi rendszer Kriptoszerver



**ADVOKÁTI
SZABADALMI ÉS VÉDELGEY IRODA
KOVÁRI GYÖRGY**

szabadalmi ügyvédek
1011 Budapest, Fő u. 19.

NYCTED
TELETYPE



HOZZÁTARTALOM
BÉLDARAB

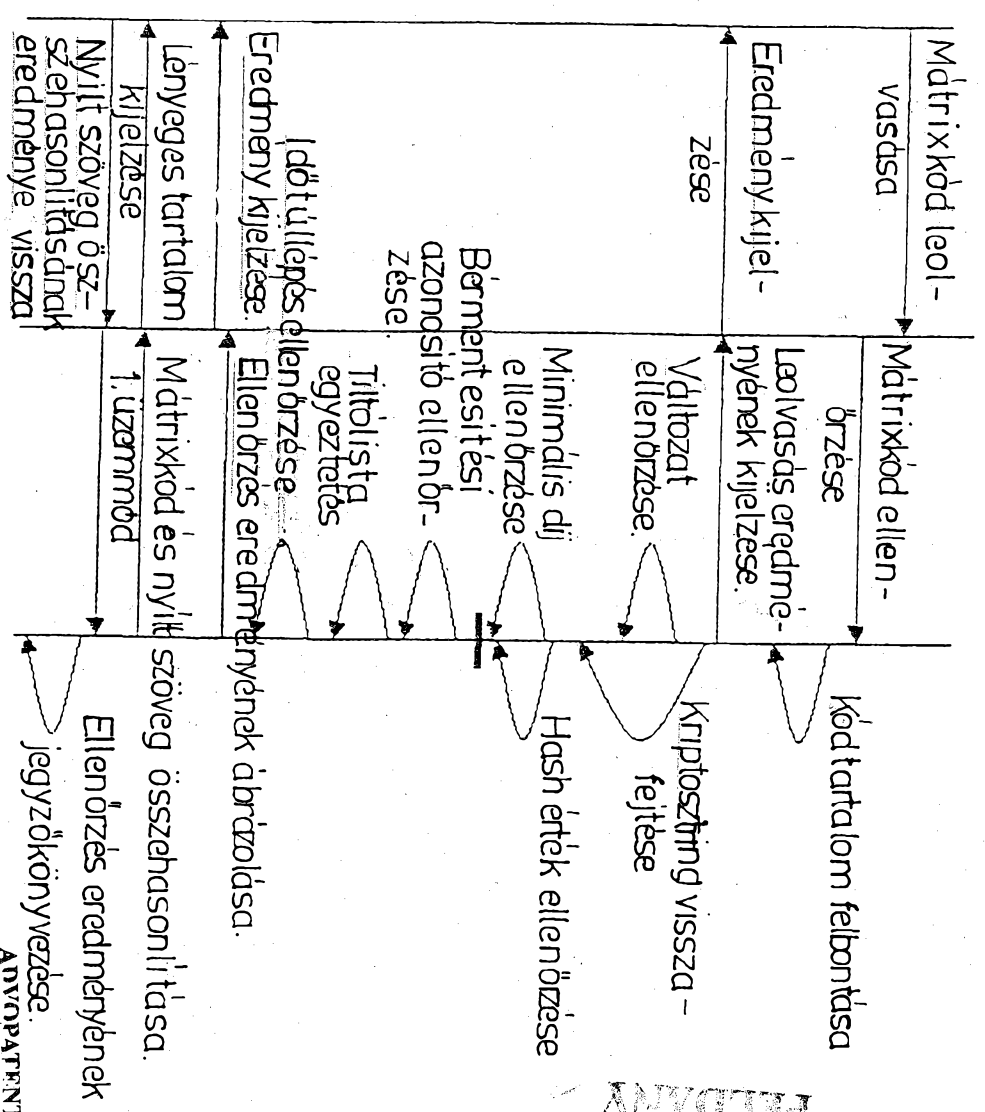
4. ábra

0400462

Rádiós olvasó Olvasóvezető

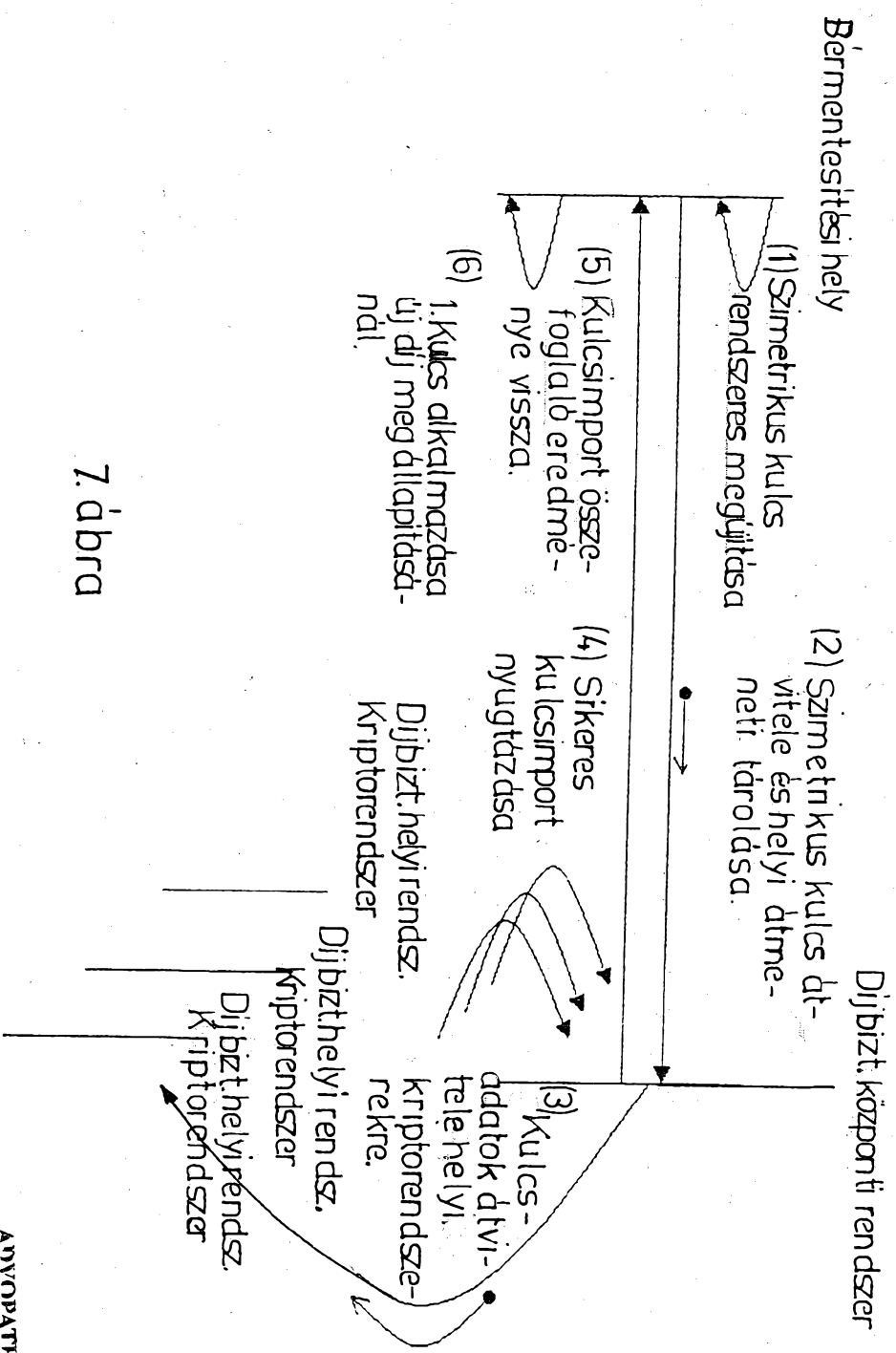
Mátrixkód beolvasása

5. ábra



KÖZZÉTÉTEL FELDARAB

ADVOKÁTIKAI SZABADALMI ÉS VÉDJEI IRODA
KOVÁRI
SZABADALMI ÉS VÉDJEI IRODA
1011 Budapest, Fő utca 10.
1011 Budapest, Fő utca 10.
1011 Budapest, Fő utca 10.



7. ábra

KÖZZÉTETEL
FELDARAB