Eljárás, berendezés, biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára, továbbá eljárás és rendszer digitális adatok készülék és biztonsági modul közötti biztonságos kommunikációjára

Kivonat

Eljárás digitális adatok készülékek közötti biztonságos kommunikációjára, amelynek során egyrészt egy készüléktől egy készülék azonosítót közlünk egy független biztonsági modullal, és a közölt azonosító azonosságától függően készülék érvényesség ellenőrzést végzünk; másrészt egy készüléktől kapott azonosítót legalább egy tárolt azonosítóval összehasonlítunk, minden egyes tárolt azonosítót egy-egy érvényes készülékhez hozzárendelünk, és ha a kapott azonosító a tárolt azonosítók legalább egyikével azonos, a készülékek érvényességét jóváhagyjuk; harmadrészt egy biztonsági modult hozunk létre, a biztonsági modulban egy véletlen eseménykulcsot állítunk elő, és a véletlen eseménykulcs felhasználásával a készülékek között továbbított adatokat kódoljuk.

Eljárás digitális adatok egy készülék és egy biztonsági modul közötti biztonságos kommunikációjára, amelynek során a biztonsági modulhoz egy véletlenszámot és a készülék azonosítóját a biztonsági modul egy nyilvános kulcsával kódolva elküldjük, majd a biztonsági modullal a véletlenszámot és a készülék azonosítót a biztonsági modul egy privát kulcsával dekódoljuk, a készüléket a készülék azonosító felhasználásával érvényesítjük, és a készülék érvényessége esetén a véletlenszám használatával a biztonsági modul és a készülék között továbbított adatokat kódoljuk és dekódoljuk.

Berendezés digitális adatok készülékek közötti biztonságos kommunikációjára, amely egyrészt egy készülék azonosítót vevő eszközt, valamint a vett azonosító azonosságától függően készülék érvényesítést végrehajtó eszközt tartalmazó biztonsági modullal van ellátva; másrészt legalább egy azonosítót eltároló eszköze van, amelyben minden egyes eltárolt azonosító egy-egy érvényes készülékkel van társítva, továbbá egy készülék azonosítóját legalább egy eltárolt azonosítóval összehasonlító eszközt, valamint a készülék azonosítójának legalább egy eltárolt azonosítóval való azonossága esetén a készüléket érvényesítő eszközt tartalmaz; harmadrészt készülékeket, valamint egy véletlen eseménykulcsot előállító eszközt, valamint a véletlen kulcsot a készülékekhez továbbító eszközzel rendelkező biztonsági modult tartalmaz, ahol minden egyes készülék a készülékek között továbbított adatok véletlen kulcs felhasználásával történő kódolására alkalmasan van kiképezve.

Biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára,

amely egyrészt egy készülék azonosítójának vételére és a vett azonosító azonosságától függően készülék érvényesítés elvégzésére alkalmasan van kiképezve; másrészt legalább egy, egy-egy érvényes készülékkel társított azonosító eltárolására, egy készülék azonosítójának legalább egy eltárolt azonosítóval történő összehasonlítására, és a készüléket a készülék azonosítójának legalább egy azonosítóval való azonossága esetén érvényesítésére alkalmas módon van kialakítva; harmadrészt egy véletlenszám és a biztonsági modul nyilvános kulcsával kódolt készülék azonosító vételére, a véletlenszám és a készülék azonosító biztonsági modul privát kulcsának felhasználásával történő dekódolására, a készüléknek a készülék azonosító használatával történő érvényesítésére, és érvényes készülék esetén a véletlenszámnak a biztonsági modul és a készülék között továbbított adatok kódolásához és dekódolásához történő felhasználására alkalmasan van kialakítva; negyedrészt a készülékek között továbbított adatok kódolására egy véletlen kulcsot előállító, valamint a véletlen kulcsot a készülékekhez továbbító módon van kiképezve.

Rendszer adatok biztonságos kommunikációjára egy készülék és egy biztonsági modul között, amelynek egy véletlenszámot, valamint a készüléknek a biztonsági modul nyilvános kulcsával kódolt azonosítóját a biztonsági modulhoz elküldő készüléke van, továbbá a biztonsági modulnak a véletlenszámot és a készülék azonosítót a biztonsági modul privát kulcsának felhasználásával dekódoló eszköze van, valamint a készüléket a készülék azonosító felhasználásával érvényesítő készüléke van, valamint a véletlenszámot a biztonsági modul és a készülék között továbbított adatok kódolásához és dekódolásához felhasználó eszköze van.

(5. ábra)

Eljárás, berendezés, biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára, továbbá eljárás és rendszer digitális adatok készülék és biztonsági modul közötti biztonságos kommunikációjára

A találmány tárgya több különböző eljárás, berendezés, biztonsági modul digitális adatok biztonságos kommunikációjára, készülékek között, továbbá eljárás valamint rendszer digitális adatok biztonságos kommunikációjára egy készülék és egy biztonsági modul között, továbbá egy biztonsági modul.

A digitális technológia bevezetése az audiovizuális területen jelentős előnyöket hozott a fogyasztó számára az analóg technológiákhoz képest, főként ami a hang- és képrögzítés minőségét és a hordozó tartósságát illeti. A kompakt lemezek - CD-k - gyakorlatilag felváltották a hagyományos hanglemezeket, és hasonló irányzat várható az általában a multimédia és a házi szórakoztató piacokra szánt új digitális termékek, főként a digitális videolemezek (Digital Versatile Disk, DVD) bevezetésétől is.

A digitálisan rögzített adatokkal kapcsolatban felmerül egy speciális, éppen a könnyű reprodukálhatóságból és ezáltal a kalózkodás lehetőségéből adódó probléma. Egyetlen digitális felvételről tetszőleges számú tökéletes másolat készíthető, a hang- illetve képminőség bárminemű romlása nélkül. Ez komoly problémát jelent, különösen az olyan írható digitális termékek megjelenésével, mint a minidiszk vagy a DAT, és lelassítja az új médiatermékek piaci bevezetését, mivel a szórakoztató cégek vonakodnak engedélyezni a szerzői jogvédelmet élvező alkotások felhasználását mindaddig, amíg ez a probléma fennáll.

Jelenleg a szerzői jogvédelmet élvező munkák engedély nélküli reprodukálása ellen kizárólag csak jogi megoldás létezik: Európában és másutt is több ország is hozott már kalózkodás elleni törvényeket annak megakadályozására, hogy egyre több kalóz film, CD stb. kerüljön be a piacára. A megelőzés szempontjából azonban a jogi megoldás nyilván semmiképp sem tekinthető optimálisnak.

Az audiovizuális termékek másolásának megakadályozására javasolt eddigi technológiai megoldások egészen egyszerűek voltak, mint például az, amely azon az elgondoláson alapult, hogy valamiféle, az olvasó és a hordozó médium közötti digitális „kézfogást" alkalmazzanak a felvétel eredetének azonosítására. Az ilyen védelem azonban csak a legalacsonyabb szintű másolási tevékenység ellen hatásos, hiszen a kézfogásjelet nem védi semmi, könnyen elolvasható és reprodukálható, és ezáltal az engedélyezetlen másolat látszólag en-

gedélyezett és olvasható másolattá alakítható át.

Ismertek az adatvédett számítógéplemez-adatokhoz való hozzáférés szabályozására szolgáló, programozható csipkártyán tárolt titkos kulccsal működő számítógépes rendszerek, pl. az US 5 191 611 számú szabadalmi leírásból. Az ilyen rendszereknek az a hátrányuk, hogy az olvasónak jelentős feldolgozó- és memóriakapacitással kell rendelkeznie ahhoz, hogy a rögzített kódolt adatcsoportokat dekódolja és tárolja. Az ilyen rendszerek számítógépes adatvédelmi alkalmazása óhatatlanul sok kényelmetlenséget okoz, és még kevésbé alkalmasak az audiovizuális területen történő alkalmazásra, hiszen ott az olvasóeszközök tipikusan lényegesen kisebb adatfeldolgozó- és tárolókapacitással rendelkeznek, mint a számítógép, ugyanakkor fenn kell tartani az adatok valós idejű áramlását.

A találmánnyal célunk az ismert korábbi technikák, módszerek hátrányainak a kiküszöbölése és hatásos technológiai megoldás biztosítása a digitálisan rögzített szerzői jog által védett munkák engedély nélküli másolásának megakadályozására, különösen az audiovizuális alkotások vonatkozásában.

A kitűzött feladatot elsősorban egy eljárással oldottuk meg digitális készülékek közötti adatok biztonságos kommunikációjára, amelynek során a találmány értelmében egy készüléktől egy független biztonsági modulhoz egy készülék azonosítót közlünk, és a közölt azonosító azonosságától függően készülék érvényesség ellenőrzést végzünk.

Egy ilyen eljárás során egy független biztonsági modult használunk fel arra, hogy például egy digitális audiovizuális rendszerben egy készülék érvényességét, érvényességét megállapítsuk. Például egy olyan rendszerben amelyben adatokat kell egy DVD lejátszó készülékből egy digitális felvevő készülékbe továbbítanunk, a rendszer felhasználója rendelkezhet egy olyan megfelelő programozható csipkártyával, amelynek segítségével a digitális felvevő készüléket és/vagy a DVD lejátszó készüléket érvényesíteni tudja, mielőtt bármilyen adattovábbításra kerül sor. Így az egyes készülékek érvényesítéséhez egy biztonsági modul alkalmazásával egy különleges biztonsági szintet tudunk a rendszerben biztosítani.

Valójában egy független biztonsági modul alkalmazása egy rendkívüli mértékben személyre szabott digitális audiovizuális rendszerhez vezethet. Például a biztonsági modul lehetővé teheti, hogy az adatokat csak abban az esetben lehessen egy DVD lejátszó készülékből egy digitális televízióba táplálni, ha mind a DVD lejátszó készüléket, mind a digitális televíziót a biztonsági modul érvényesnek minősíti, biztosítva ezzel, hogy a digitális adatokat kizárólag a felhasználó digitális televízióján lehessen megnézni.

Az egymással láncba kapcsolt készülékek érvényesítéséhez egy biztonsági modul használata azzal az előnnyel jár, hogy a készülék érvényesítés függetlenné válhat az egyes készülékek közötti kapcsolattól. Így ha a kommunikációs kapcsolatot egy harmadik személy megcsapolja, a készülékek azonosítóit nem tudja megszerezni, mivel azok nem kerülnek továbbításra a készülékek között, hanem mindig az egyes készülék és a biztonsági modul közötti kommunikációban játszanak szerepet.

Az ilyen biztonsági modulok bármely megfelelő formában megvalósíthatók, a modulok fizikai méretétől és jellemzőitől függően. Például a biztonsági modul egy különálló, például eltávolítható, egy foglalatba helyezhető modulként is kialakítható, ha a készülék el van látva ilyen foglalattal, vagy akár egy különálló, a készülékhez kapcsolt modulként is megvalósítható. Egyes esetekben egy bankkártya méretű, ahhoz hasonló programozható csipkártyát használhatunk (akár a biztonsági modul részeként), de más formátumok, például PCMCIA típusú kártyák is éppilyen jól használhatók. Ezáltal a biztonsági modul könnyen cserélhető annak érdekében, hogy a biztonsági modul által adott jogosultságokat felfrissítsük, például hogy bizonyos készülékek érvényességét megvonjuk olyan esetekben, amikor a rendszer üzemeltetője tudomást szerez ezeknek a készülékeknek a jogosulatlan másolásáról és használatáról.

A készülék azonosító bármilyen megfelelő formátumú lehet, például a készülékkel társított nyilvános kulcsként is megvalósítható.

A javasolt eljárás egy előnyös foganatosítási módja értelmében a biztonsági modullal végzett készülék érvényesség ellenőrzés során a közölt azonosítót legalább egy tárolt azonosítóval összehasonlítjuk. Ezeket az eltárolt azonosítókat a biztonsági modul memóriájában tárolhatjuk. Az azonosítókat tárolhatjuk például egy lista formájában, és a kapott azonosítót a készülék érvényesítése céljából a listában szereplő azonosítóval hasonlítjuk össze. Ezzel gyors és hatékony készülék érvényesítést tudunk megvalósítani.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében minden egyes tárolt azonosítót egy érvényes készülékkel vagy egy érvénytelen készülékkel társítunk. Ilyen esetben a közölt azonosítót érvénytelen készülékekkel társított tárolt azonosítókkal hasonlítjuk össze. Az is előnyös az utóbbi esetekben, ha a közölt azonosítót érvényes készülékekkel társított tárolt azonosítókkal hasonlítjuk össze. az azonosító vételét követően a biztonsági modullal összehasonlíthatjuk a kapott azonosítót, tehát mind az érvénytelen készülékekkel társított és eltárolt azonosítókkal, mind pedig az érvényes készülékekkel tár-

sított és eltárolt azonosítókkal.

Ily módon a biztonsági modulban legalább egy olyan "visszavonási listát" hozhatunk létre, amelynek az a célja, hogy segítségével fekete listára tudjuk tenni azokat a készülékeket, amelyek nem működhetnek együtt a rendszer többi elemeivel, valamint egy olyan "jogosultsági listát", amelynek segítségével az adatátvitelt kizárólag már előzőleg regisztrált készülékek között engedjük megvalósulni. A harmadik személyek részéről szándékosan publikált készülék azonosítókat, amelyeket például az Interneten tesznek közzé, így fel tudjuk tenni a visszavonási listára, amikor a biztonsági modult időszakosan frissítjük, annak érdekében, hogy megakadályozzuk az adatforgalmat ezekhez a készülékekhez vagy ezektől a készülékektől. Egy jogosultsági lista alkalmazásával ugyancsak meg tudjuk akadályozni, hogy a szándékosan és rosszindulatúan, például az Interneten közzétett készülék azonosítók használhatók legyenek, hiszen ezek az azonosítók sehol sem minősülnek érvényesnek, kizárólag például egy otthoni hálózatban.

A jogosultsági lista ezért lényegesen rövidebb és kisebb, mint a visszavonási lista, amivel memória kapacitást takarítunk meg, és kevésbé gyakran kell frissítenünk.

A kitűzött feladatot így másodsorban egy eljárással oldottuk meg digitális készülékek közötti adatok biztonságos kommunikációjára, amelynek során egy készüléktől kapott azonosítót legalább egy tárolt azonosítóval összehasonlítunk, minden egyes tárolt azonosítót egy-egy érvényes készülékhez hozzárendelünk, és ha a kapott azonosító a tárolt azonosítók legalább egyikével azonos, a készülékek érvényességét jóváhagyjuk.

A javasolt eljárás egy előnyös foganatosítási módja értelmében a legalább egy tárolt azonosítót egy független biztonsági modulban tároljuk.

Ugyancsak előnyös a találmány értelmében, ha a kapott azonosítót egy indikátor értékétől függően hasonlítjuk össze az érvényes készülékekkel társított tárolt azonosítókkal. Ezt az indikátort a biztonsági modulban tárolhatjuk, vagy pedig a készülékkel juttathatjuk el a biztonsági modulhoz.

Például a biztonsági modullal össze tudjuk hasonlítani a kapott azonosítót az érvénytelen készülékekkel társított eltárolt azonosítókkal, ha ennek az indikátornak egy első meghatározott értéke van, illetve a kapott azonosítót az érvényes készülékekkel társított eltárolt azonosítókkal hasonlítjuk össze, ha az indikátornak az elsőtől eltérő második meghatározott értéke van.

Ezt az indikátor értéket a felhasználó mindenkori jogosultságainak megfelelően állíthatjuk be. Például az indikátor egy első értéket vehet fel mondjuk egy üzletben, ahol számos különböző készüléket használnak, és ilyen esetben az indikátor olyan értékű, hogy a kapott azonosítót kizárólag az érvénytelen készülékekkel társított eltárolt azonosítókkal hasonlítsuk össze. Ezzel ellentétben az indikátor a már említett második értékű lehet például egy otthoni felhasználó esetén, aki csak kevés készüléket használ, és ilyen esetben az indikátor értéke azt eredményezi, hogy a kapott azonosítót kizárólag az érvényes készülékekkel társított eltárolt azonosítókkal hasonlítsuk össze.

Egy lehetséges megvalósítás szerint a biztonsági modullal a kapott azonosítót az érvénytelen készülékekkel társított eltárolt azonosítókkal hasonlítjuk össze, ha az indikátor értéke "0", illetve a kapott azonosítót mind az érvénytelen készülékekkel társított eltárolt azonosítókkal, mind pedig az érvényes készülékekkel társított eltárolt azonosítókkal összehasonlítjuk, ha az indikátor értéke "1".

A javasolt eljárás egy előnyös foganatosítási módja értelmében a készülék és a biztonsági modul között a készülék érvényesítéséhez bizonyítványokat továbbítunk.

Egy bizonyítvány rendszer használata egy készülék, illetőleg a készülékek érvényességének megállapítására biztonságos azonosító átvitelt eredményezhet a készülék és a biztonsági modul közt. Így például a találmány értelmében előnyösen a készülék azonosítóját kódolt bizonyítványban továbbítjuk a biztonsági modulhoz, és így el tudjuk kerülni a készülék azonosítók "tiszta", kódolatlan formában történő továbbításával együtt járó problémákat.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében a bizonyítványt az elküldött bizonyítvány hitelessége ellenőrzésének a lehetővé tételéhez aláírjuk. Ezen belül a bizonyítványt egy privát kulcs használatával kódoljuk. Így ha a biztonsági modullal azt állapítjuk meg, hogy a bizonyítványban lévő adatok és a bizonyítvány aláírása nem illeszkedik egymáshoz, a bizonyítványt elutasíthatjuk.

Ugyancsak előnyös a találmány szerinti eljárás olyan foganatosítási módja, amelynek során a biztonsági modulhoz egy rendszer privát kulccsal kódolt bizonyítványban a privát kulccsal ekvivalens kulcsot továbbítunk, és egy rendszer nyilvános kulcsot mind a biztonsági modulban, mind a készülékben eltárolunk.

Előnyös továbbá a javaslat értelmében, ha a kódolt bizonyítványt a készülékkel egy bizton-

sági modul nyilvános kulcs használatával tovább kódoljuk, és a biztonsági modulhoz továbbítjuk. Előnyös módon a kódolt bizonyítványt a biztonsági modullal dekódoljuk, úgy, hogy először egy biztonsági modul privát kulcsot használunk, másodszor pedig az ekvivalens kulcsot használjuk, lehetővé téve a készülék azonosítójának kivonását a dekódolt bizonyítványból.

A biztonsági modul nyilvános kulcsát a biztonsági modullal egy bizonyítványban is továbbíthatjuk egy készülékhez. A biztonsági modul nyilvános kulcsát is magában foglaló bizonyítványt egy privát kulcs használatával kódolhatjuk, például a biztonsági modul gyártójának privát kulcsát használhatjuk fel erre a célra. Ezt a bizonyítványt alá is írhatjuk, a privát kulcs használatával, hogy lehetővé tegyük a közölt bizonyítvány hitelességének az ellenőrzését. A privát kulcs ekvivalensének számító kulcsot a rendszer privát kulcsával kódolt bizonyítványban küldhetjük el a készüléknek, ilyen esetben a rendszer nyilvános kulcsát mind a biztonsági modulban, mind a készülékben eltároljuk.

A javasolt eljárás egy további előnyös foganatosítási módja értelmében a készülék azonosítót tartalmazó bizonyítványt a készülékkel még a kódolás előtt véletlenszám-generálásnak vetjük alá, és a véletlenszám-generálást a bizonyítvány dekódolását követően a biztonsági modullal visszájára fordítjuk. Ezzel jelentősen meg tudjuk növelni az egy készüléktől a biztonsági modulhoz továbbított készülék azonosító továbbításának a biztonságát.,

Egy készülék érvényességének a megállapításán túlmenően a biztonsági modullal információt is továbbíthatunk egy készülékhez, például azért, hogy lehetővé tegyük a készülék számára, hogy egy másik készüléktől kapott digitális adatot dolgozzon fel. Ennek értelmében előnyös, ha a készülék és a biztonsági modul között egy biztonságos kommunikációs csatornát hozunk létre.

Ennek értelmében a javasolt eljárás egy további előnyös foganatosítási módja szerint a készülékkel egy véletlenszámot állítunk elő, és a véletlenszámot és a készülék azonosítóját tartalmazó kódolt bizonyítványt a készülékkel kódoljuk egy biztonsági modul nyilvános kulcs használatával, majd a biztonsági modulhoz továbbítjuk. Előnyösen a kódolt véletlenszámot és a kódolt bizonyítványt a biztonsági modullal dekódoljuk, úgy, hogy először egy biztonsági modul privát kulcsot használunk a véletlenszám kinyerésére, másodszor pedig a nyilvános kulcsot használjuk a készülék azonosítójának a biztonsági modullal történő kinyerésére.

Ugyancsak előnyös találmányunk értelmében, ha a kinyert véletlenszámot a biztonsági modulban tároljuk, úgy, hogy a biztonsági modultól a készülékhez irányuló kommunikációt a biztonsági modulban és a készülékben a véletlenszámmal kódolni és dekódolni tudjuk, ezáltal biztonságos kommunikációs kapcsolatot hozunk létre a készülék és a biztonsági modul között.

A kitűzött feladatot harmadsorban egy eljárással oldottuk meg digitális adatok egy készülék és egy biztonsági modul közötti biztonságos továbbítására, amelynek során újszerű módon a biztonsági modulhoz egy véletlenszámot és a készülék azonosítóját a biztonsági modul egy nyilvános kulcsával kódolva elküldjük, majd a biztonsági modullal a véletlenszámot és a készülék azonosítót a biztonsági modul egy privát kulcsával dekódoljuk, a készüléket a készülék azonosító felhasználásával érvényesítjük, és a készülék érvényessége esetén a véletlenszám használatával a biztonsági modul és a készülék között továbbított adatokat kódoljuk és dekódoljuk.

A javasolt eljárás egy előnyös foganatosítási módja értelmében a készülék azonosítóját a készülékkel előállított bizonyítványba építjük be, és a bizonyítványt a biztonsági modul nyilvános kulcsával kódoljuk.

Ugyancsak előnyös a találmány szerinti eljárás olyan foganatosítási módja, amelynek során a véletlenszámot a készülékkel még a kódolást megelőzően generáljuk, és a véletlenszám-generálást a biztonsági modullal a véletlenszám dekódolását követően visszafordítjuk.

Egy alternatív megoldásként előnyösen a véletlenszámot és a készülék azonosítóját tartalmazó bizonyítványt a készülékkel még a kódolást megelőzően generáljuk, majd a véletlenszám-generálást a biztonsági modullal a véletlenszám és a bizonyítvány dekódolását követően visszafordítjuk.

Annak érdekében, hogy a készülék és a biztonsági modul közötti kommunikációs kapcsolat biztonságát megnöveljük, előnyös, ha a biztonsági modullal a készülékhez egy a biztonsági modulban előállított és a véletlenszám használatával kódolt véletlen eseménykulcsot továbbítunk, és a készülékkel a kapott eseménykulcsot a véletlenszám felhasználásával dekódoljuk, majd az így kapott eseménykulcsot használjuk a biztonsági modulhoz küldött adatok kódolására.

Egy készülék érvényességének a megállapításán túl, a készülék és a biztonsági modul közötti biztonságos adatkommunikáció céljából a biztonsági modult alkalmassá tehetjük arra,

hogy a készülék által fogadott adatokhoz hozzáférési jogosultságokat rendeljen.

Például egy javasolt előnyös módon a készülékkel a biztonsági modulhoz az adatok bitsordekódolásához szükséges ellenőrző szót tartalmazó kódolt jogosultság vezérlő üzenetet továbbítunk, és a készülékkel a kódolt jogosultság vezérlő üzenetet az eseménykulcs használatával tovább kódoljuk. Így tehát az egy készülék és egy biztonsági modul között továbbított jogosultság vezérlő üzeneteket kétszeresen is kódoljuk, ahol a kódoló kulcsok egyikét a biztonsági modullal hozzuk létre, így az egyedi kulcsnak számít mind a készülék, mind a biztonsági modul vonatkozásában. Ezzel jelentős lépést érhetünk el a jogosultság vezérlő üzenetek illegális másolásának és terjesztésének a megakadályozása terén.

Előnyös a találmány értelmében, ha a biztonsági modullal a kódolt jogosultság vezérlő üzenetet dekódoljuk, abból az ellenőrző szót kinyerjük, és az ellenőrző szót az eseménykulcs (SK) használatával kódolva a készülékhez továbbítjuk.

Ezzel egy készülék számára, például egy digitális televízió számára lehetővé tesszük, hogy bitsordekódolja a lejátszótól, például egy DVD lejátszó készüléktől kapott bitsorkódolt adatokat. Ezen túlmenően az ellenőrző szót mindig kódolt formában juttathatjuk el a készülékhez, ahol a kódolást a készülék érvényességének megállapítását követően a készülékhez korábban eljuttatott kulccsal hajtjuk végre. Ezért az ellenőrző szavak kódolására és dekódolására szolgáló járulékos nyilvános kulcsokat és privát kulcsokat, vagy a készüléknek a biztonsági modul felé történő hitelesítésére (vagy fordítva) nincs többé szükség.

Egy alternatív foganatosítási mód értelmében a készülékkel a biztonsági modulhoz egy kódolt kiterjesztett jogosultság vezérlő üzenetet továbbítunk, amely az adatokhoz való hozzáférési jogosultságokat tartalmazza, és a készülékkel a kódolt kiterjesztett jogosultság vezérlő üzenetet az eseménykulcs felhasználásával tovább kódoljuk. Ez utóbbi esetben a találmány szerinti előnyös eljárás értelmében a biztonsági modullal a kódolt kiterjesztett jogosultság vezérlő üzenet dekódoljuk, az abban található hozzáférési jogosultságokat módosítjuk, a módosított kiterjesztett jogosultság vezérlő üzenetet kódoljuk, majd ezt az kódolt módosított kiterjesztett jogosultság vezérlő üzenetet az eseménykulcs felhasználásával tovább kódoljuk és a készülékhez továbbítjuk.

Így a biztonsági modullal egy kiterjesztett jogosultság vezérlő üzenettel tudjuk módosítani a készülék által igényelt hozzáférési jogosultságokat. Például ha a készülék egy digitális felvevő készülék, akkor ezek a hozzáférési jogosultságok tartalmazhatják a tárolt adatok bármely további ismételt rögzítésének, felvételének a megakadályozását, avagy azt a szá-

mot, ahányszor a rögzített adatokat a felhasználó lejátszhatja, a rögzített adatok lejátszásának lejárati idejét és így tovább.

A készülékek sokkal hatékonyabb működésének a biztosítása érdekében a készülékek között egy biztonságos vagy kódolt kommunikációs kapcsolatot kell létrehoznunk. A készülékek közötti ilyen biztonságos kommunikációs kapcsolat révén például a készülékek között szabadon továbbítható felvétel készítéséhez vagy lejátszásához szükséges információt továbbíthatunk. Sajnálatos módon a DVD lejátszó készülékek gyártói és a digitális felvevő készülékek gyártói közötti összhang hiányában számos probléma jöhet létre a kódoló kulcsok ilyen célú létrehozása és terjesztése vonatkozásában.

Például egy DVD lejátszó készülék gyártója nem bízik meg annyira a digitális felvevő készülék gyártójának biztonsági rendszerében, hogy a gyártót ellássa például egy olyan titkos szimmetrikus algoritmus kulccsal, amelyre a digitális felevőnek szüksége lenne annak a kapott digitális adatnak a dekódolásához, amelyet a DVD lejátszó készülékben lévő ekvivalens kulcs használatával kódoltak.

Ezen túlmenően az egyes tevékenységek szétválasztása miatt nem célszerű olyan helyzetet kialakítani, amelyben a digitális felvevő készüléket egy terjesztő rendszer üzemeltetőjének kell elküldeni, hogy az a felvevőt a megfelelő kulcsokkal egyedivé tegye. Ezért olyan megoldásra célszerű törekedni, amely a lehető legnagyobb függetlenséget biztosítja a lejátszó és a felvevő működtetésével kapcsolatosan.

Az ilyen jellegű problémák megoldása érdekében a találmány szerinti eljárás egy további előnyös foganatosítási módja szerint, az adatokat egy első készülék és egy második készülék között továbbítjuk, és az egyes készülékeknek a biztonsági modullal végzett érvényesítése során a biztonsági modullal az első készülékhez a biztonsági modulban előállított és az első által előállított véletlenszám használatával kódolt véletlen eseménykulcsot küldünk, majd az első készülékkel a kapott véletlen eseménykulcsot az általa előállított véletlenszám használatával dekódoljuk, és a biztonsági modullal a második készülékhez a második készülék által előállított véletlenszám felhasználásával kódolt véletlen eseménykulcsot elküldjük, és a második készülékkel a kapott véletlen eseménykulcsot az általa előállított véletlenszám felhasználásával dekódoljuk, majd az így kapott véletlen eseménykulcsot ezt követően a biztonsági modul és a készülékek között továbbított adatok, valamint az egyes készülékek között továbbított adatok kódolására használjuk.

A kitűzött feladatot negyedsorban egy eljárással oldottuk meg digitális adatok készülékek

közötti biztonságos kommunikációjára, amelynek során egy biztonsági modult hozunk létre, a biztonsági modulban egy véletlen eseménykulcsot állítunk elő, és a véletlen eseménykulcs felhasználásával a készülékek között továbbított adatokat kódoljuk.

Ennek az eljárásnak a révén az egyes készülékek közötti kommunikáció biztonságossá tételét szolgáló kódoló kulcs előállítását a biztonsági modullal hajtjuk végre, annak a készülékekkel folytatott kommunikációja során, így tehát a kulcs-generálást a készülékektől függetlenül tudjuk végrehajtani.

Egy ilyen eljárás egy biztonságos, rugalmas és könnyen továbbfejleszthető készülék interfésztől független rendszert biztosít, amellyel digitális adatokat biztonságosan tudunk az egyes készülékek között továbbítani. a rendszer az eseménykulcs előállítására szolgáló programozható csipkártyán alapulhat, így olcsón kiképezhető, és gyors cselekvési lehetőséget biztosít a jogosulatlan kalózkodásokkal szemben a programozható csipkártyák könnyű felfrissítése vagy cseréje révén, különösen mivel a biztonsági jellemzők aktuális szinten tartásáért egy erre kijelölt programozható csipkártya gyártó vagy szolgáltató a felelős, nem pedig az egyes készülékek gyártói.

A javasolt eljárás egy előnyös foganatosítási módja értelmében a biztonsági modullal minden egyes készülékhez elküldjük a készülék által előállított véletlenszám felhasználásával kódolt véletlen eseménykulcsot, és a készülékkel a véletlen eseménykulcsot a véletlenszám felhasználásával dekódoljuk.

Előnyös a találmány értelmében, ha minden egyes készülékkel elküldjük a biztonsági modulhoz a biztonsági modul nyilvános kulcsának használatával kódolt, a készülékhez tartozó véletlenszámot.

Ugyancsak előnyös, ha a kódolt véletlenszámot a biztonsági modullal dekódoljuk, a biztonsági modul privát kulcsának a felhasználásával, a véletlenszám kinyerésére. Egy további előnyös foganatosítási mód értelmében minden egyes véletlenszámot az egyes készülékekkel állítunk elő még a kódolást megelőzően, és a véletlenszám-generálást a biztonsági modullal visszafordítjuk a véletlenszám dekódolását követően. Ugyancsak előnyös a javaslat értelmében, ha biztonsági modullal minden egye készüléket érvényesítünk, mielőtt a véletlen eseménykulcsot továbbítanánk az egyes készülékekhez. Egy ilyen érvényesség megállapításának a lehetővé tétele érdekében minden egyes készülékkel egy a készülékhez tartozó azonosítót továbbítunk a biztonsági modulhoz, a készülék biztonsági modullal történő érvényesítéséhez.

Előnyösen a kulcsot időszakosan a biztonsági modullal módosítjuk. Ezt a kulcsot például akár óránként frissíthetjük, vagy például a készülékek között továbbításra került előre meghatározott adatcsomag számot követően. Ez további biztonságot jelent az adatkommunikáció számára. Alternatív megoldásként a kulcsot véletlenszerűen változtathatjuk a biztonsági modullal, például a készülék bekapcsolásakor, lemez behelyezésekor, a készüléknek a felhasználó általi kapcsolgatásakor, a biztonsági modullal létrehozott kapcsolat során, és így tovább.

A javasolt eljárás egy további előnyös foganatosítási módja értemében egy otthoni hálózati rendszerben készülékekként egy első és egy második, egymás között egy kommunikációs kapcsolaton keresztül adatok továbbítására alkalmas fogyasztói elektronikai készüléket alkalmazunk. A két készülék közötti kommunikációs kapcsolat bármilyen formában létrehozható, például rádiós, telefon vagy infravörös kapcsolat révén. Azonban a kommunikációs kapcsolatot előnyösen az első és a második készülék közötti busz kapcsolattal, például IEEE 1394 típusú busz kapcsolattal valósíthatjuk meg.

Az első készülék a második készülékhez bitsorkódolt audio és/vagy vizuális adatokat, valamint az adatok bitsordekódolásához szükséges ellenőrző szót tartalmazó kódolt jogosultság vezérlő üzenetet küldhet, ahol az adatok és a kódolt jogosultság vezérlő üzenet a kulcs felhasználásával az első készülékben kerül kódolásra.

A második készülék az adatokat és a kódolt jogosultság vezérlő üzenetet a kulcs felhasználásával dekódolhatja, a kódolt jogosultság vezérlő üzenetet elkülöníti az adatoktól, és a kódolt jogosultság vezérlő üzenetet a kulcs felhasználásával újra kódolva a biztonsági modulhoz továbbíthatja. A biztonsági modul ezt a kódolt jogosultság vezérlő üzenetet dekódolja, az abban lévő ellenőrző szót kinyeri, és a kulccsal kódolt ellenőrző szót továbbítja a második készülékhez. Ennél a megvalósításnál az első készülék egy DVD lejátszó készülék, a második készülék pedig egy digitális televízió lehet.

Ezen túlmenően a biztonsági modullal a jogosultság vezérlő üzenetet is módosíthatjuk, és a második készülékhez a kulcs felhasználásával kódolt módosított jogosultság vezérlő üzenetet küldhetjük el. Ilyen esetben az első készülék egy DVD lejátszó készülék, a második készülék pedig egy digitális felvevő készülék lehet.

A kitűzött feladatot ötödsorban egy berendezéssel oldottuk meg digitális adatok készülékek közötti biztonságos kommunikációjára, amely a találmány értelmében egy készülék azonosítót vevő eszközt, valamint a vett azonosító azonosságától függően készülék érvényesítést

végrehajtó eszközt tartalmazó biztonsági modullal van ellátva.

A kitűzött feladatot hatodsorban digitális adatok készülékek közötti biztonságos kommunikációjára szolgáló biztonsági modullal oldottuk meg, amely javaslatunk értelmében egy készülék azonosítójának vételére és a vett azonosító azonosságától függően készülék érvényesítés elvégzésére alkalmasan van kiképezve.

A kitűzött feladatot hetedsorban digitális adatok készülékek közötti biztonságos kommunikációjára szolgáló berendezéssel oldottuk meg, amely a találmány értelmében legalább egy azonosítót eltároló eszköze van, amelyben minden egyes eltárolt azonosító egy-egy érvényes készülékkel van társítva, továbbá egy készülék azonosítóját legalább egy eltárolt azonosítóval összehasonlító eszközt, valamint a készülék azonosítójának legalább egy eltárolt azonosítóval való azonossága esetén a készüléket érvényesítő eszközt tartalmaz.

A kitűzött feladatot nyolcadsorban digitális adatok készülékek közötti biztonságos kommunikációjára szolgáló biztonsági modullal oldottuk meg, amely javaslatunk értelmében legalább egy, egy-egy érvényes készülékkel társított azonosító eltárolására, egy készülék azonosítójának legalább egy eltárolt azonosítóval történő összehasonlítására, és a készüléket a készülék azonosítójának legalább egy azonosítóval való azonossága esetén érvényesítésére alkalmas módon van kialakítva.

A kitűzött feladatot kilencedsorban adatok egy készülék és egy biztonsági modul közötti biztonságos kommunikációjára szolgáló rendszerrel oldottuk meg, amelynek a találmány értelmében egy véletlenszámot, valamint a készüléknek a biztonsági modul nyilvános kulcsával kódolt azonosítóját a biztonsági modulhoz elküldő eszköze van, továbbá a biztonsági modulnak a véletlenszámot és a készülék azonosítót a biztonsági modul privát kulcsának felhasználásával dekódoló eszköze van, valamint a készüléket a készülék azonosító felhasználásával érvényesítő eszköze van, valamint a véletlenszámot a biztonsági modul és a készülék között továbbított adatok kódolásához és dekódolásához felhasználó eszköze van.

A kitűzött feladatot tizedsorban egy olyan biztonsági modullal oldottuk meg, amely a találmány értelmében egy véletlenszám és a biztonsági modul nyilvános kulcsával kódolt készülék azonosító vételére, a véletlenszám és a készülék azonosító biztonsági modul privát kulcsának felhasználásával történő dekódolására, a készüléknek a készülék azonosító használatával történő érvényesítésére, és érvényes készülék esetén a véletlenszámnak a biztonsági modul és a készülék között továbbított adatok kódolásához és dekódolásához történő felhasználására alkalmasan van kialakítva.

A kitűzött feladatot tizenegyedrészben digitális adatok készülékek közti biztonságos kommunikációjára szolgáló berendezéssel oldottuk meg, amely újszerű módon készülékeket, valamint egy véletlen eseménykulcsot előállító eszközt, valamint a véletlen kulcsot a készülékekhez továbbító eszközzel rendelkező biztonsági modult tartalmaz, ahol minden egyes készülék a készülékek között továbbított adatok véletlen kulcs felhasználásával történő kódolására alkalmasan van kiképezve.

A kitűzött feladatot tizenkettedrészben digitális adatok készülékek közötti biztonságos kommunikációjára szolgáló biztonsági modullal oldottuk meg, amely újszerű módon a készülékek között továbbított adatok kódolására egy véletlen kulcsot előállító, valamint a véletlen kulcsot a készülékekhez továbbító módon van kiképezve.

Jóllehet a találmány ismertetése során egy első készülékről és egy második készülékről beszélünk, szakember számára nyilvánvaló, hogy az ismertetett elvek alapján akár láncszerű kommunikációs kapcsolatot is létre tudunk hozni több ilyen készülék között.

A találmány során a privát és nyilvános kulcsok előállítására használt megfelelő algoritmusok lehetnek például az RSA, vagy Diffie-Hellman féle algoritmus és az alkalmas szimmetrikus kulcs algoritmusok magukban foglalhatják például az ismert DEES típusú algoritmust. Amíg a szövegkörnyezetből más nem olvasható ki, vagy külön nem jelezzük, nem teszünk megkülönböztetést a szimmetrikus algoritmusokhoz tartozó és az aszimmetrikus algoritmusokhoz tartozó kulcsok között sem.

A "bitsorkódolt", "kódolt", "ellenőrző szó", "kulcs", "kódoló kulcs" kifejezéseket csupán a használt fogalmak egyszerűsítése érdekében vezettük be és használtuk, és használjuk leírásunkban. Nyilvánvaló azonban, hogy a "bitsorkódolt adatok" és a "kódolt adatok" között, vagy például az "ellenőrző szó" és a "kódoló kulcs" kifejezések között alapvető különbséget nem lehet tenni.

Hasonlóképpen, az "ekvivalens" kulcs, tulajdonképpen egy másolat kulcs kifejezés alatt is olyan kulcsot értünk, amellyel egy első kulccsal kódolt adatokat tudunk dekódolni, és fordítva.

Ezen túlmenően a "kódolt" és "aláírt", valamint a "dekódolt" és "hitelesített" "érvényesített" kifejezéseket váltakozva használjuk a leírás különböző részeiben, azonban ezen kifejezések tényleges tartalma között semmilyen lényeges megkülönböztetést nem teszünk, hasonlóképpen nincs érdemi különbség a "kódolt adat" és "aláírt adat", vagy a "dekódolt

adat" és "hitelesített adat" között.

Hasonlóképpen az "ekvivalens kulcs" kifejezés egy olyan kulcsot jelent, amelyet egy első kulccsal kódolt adatok dekódolására használhatunk, vagy fordítva.

Az eljárással kapcsolatosan bemutatott találmányi ismérvek egyaránt hasznosan megvalósíthatók a berendezések vonatkozásában is, és fordítva.

A találmányt az alábbiakban a csatolt rajz segítségével ismertetjük részletesebben, amelyen a javasolt eljárás, illetve az azt megvalósító berendezés és rendszer példakénti kiviteli alakját vázoltuk. A rajzon az

1. ábra egy digitális audiovizuális rendszer főbb egységeit és azok kapcsolatát mutatja, a

2. ábrán egy digitális audiovizuális rendszerben bizonyítványok szétosztásának vázlata látható, a

3. ábra egy készülék és egy biztonsági modul kapcsolatát mutatja, a

4. ábrán egy biztonsági modul és két készülék kapcsolata látható, az

5. ábra egy készüléknek a biztonsági modul általi érvényesség ellenőrzésével, valamint azt követően a készülék és a biztonsági modul közötti biztonságos kommunikáció megvalósításával kapcsolatos lépéseket tartalmazza, a

6. ábrán egy készülék és egy biztonsági modul közötti biztonságos kommunikációs csatorna létrehozásával kapcsolatos lépéseket vázoltuk, a

7. ábrán adatok bitsordekódolását mutatjuk egy készülék segítségével, a

8. ábrán két készülék közötti biztonságos kommunikáció megvalósítására vonatkozó lépéseket rajzoltuk fel, a

9. ábra két készülék között biztonságos kommunikációs kapcsolaton keresztüli adatátvitel vázlata, a

10. ábra egy DVD lejátszó készülék és egy digitális televízió közötti biztonságos kommunikációs kapcsolat felépítésével, majd azt követően a DVD lejátszó készüléktől a digitális televízióval kapott adatok bitsordekódolásához elvégzett műveletekkel kapcsolatos lépéseket mutatja, és a

11. ábrán egy DVD lejátszó készülék és egy digitális felvevő készülék közötti bizton-

ságos kommunikációs kapcsolat felépítésével, majd azt követően a DVD lejátszó készüléktől a digitális felvevő készülékkel fogadott adatok bitsordekódolásához elvégzett műveletekkel kapcsolatos lépések láthatók.

Rátérve a találmánynak az ábrák segítségével történő részletesebb ismertetésére, az 1. ábrán 10 digitális audiovizuális rendszer főbb elemeit, valamint azok egymáshoz való viszonyát és egymáshoz történő kapcsolódását tüntettük fel fő tömbvázlat szinten. A 10 digitális audiovizuális rendszer digitális adatok felvételére és lejátszására szolgál, és jóllehet leírásunkban egy 12 DVD lejátszó készülék audiovizuális adatainak a lejátszásáról beszélünk, szakember számára nyilvánvaló, hogy ez az audiovizuális adat, vagy digitális információ más jellegű is lehet, például kizárólag audio információ lejátszása is szóba jöhet, amelyet azt követően DAT magnetofonon vagy Minidisc felvevőn rögzíthetünk, vagy akár egy számítógép merev lemezén rögzítésre kerülő szoftver kommunikációja is elképzelhető.

A 10 digitális audiovizuális rendszer jellemző esetben valamilyen módon korábban eltárolt digitális audiovizuális adatok lejátszására szolgáló 12 DVD lejátszó készüléket tartalmaz, ahol az adatok egy lemezen kerülnek rögzítésre, bár digitális magnetofon esetében az adatok ugyancsak ismert és szokásos módon szalagon, mint mágneses adathordozón vannak rögzítve. A 12 DVD lejátszó készülék 14 digitális kijelzőhöz kapcsolódik, amely a 12 DVD lejátszó készülék által lejátszott adatok megjelenítésére szolgál. Ez a 14 digitális kijelző előnyösen digitális televízióként van kiképezve. A 12 DVD lejátszó készülék és a 14 digitális kijelző közötti 16 kommunikációs kapcsolat számos módon megvalósítható, például lehet vezeték nélküli rádiós kapcsolat, telefonkapcsolat vagy infravörös kapcsolat, azonban előnyösen a 12 DVD lejátszó készülék és a 14 digitális kijelző buszon, például IEEE 1394 típusú buszon keresztül áll egymással kapcsolatban.

A 10 digitális audiovizuális rendszer ezen kívül 18 digitális felvevő készüléket is magában foglal, például DVHS vagy DVD felvevőt, amely például egy IEEE 1394 típusú 20 buszon keresztül kommunikációs kapcsolatban áll a 12 DVD lejátszó készülékkel. A 18 digitális felvevő készülék az ábrán nem látható digitális tároló közeget is tartalmaz, amelyre a kapott információt rögzítjük. A 18 digitális felvevő készülék 22 közvetlen kapcsolatban áll a 14 digitális kijelzővel, azonban a digitális audiovizuális adatokat a 12 DVD lejátszó készüléktől a 18 digitális felvevő készüléken keresztül is elküldhetjük a 14 digitális kijelzőre, ahelyett, hogy a már korábban említett 16 kommunikációs kapcsolatot használnánk erre a célra.

Ugyan a 10 digitális audiovizuális rendszer részét képező 12 DVD lejátszó készüléket, 14 digitális kijelzőt és 18 digitális felvevő készüléket külön-külön egységként tüntettük fel az ábrán, nyilvánvaló, hogy ezeket a készülékeket vagy egységeket akár részben, akár mind együtt integrálhatjuk, például egy kombinált lejátszó és televízió berendezés formájában.

Annak érdekében, hogy a 10 digitális audiovizuális rendszer egyes készülékei között biztonságos adatkommunikációt hozhassunk létre, például hogy megakadályozzuk a digitálisan rögzített adatok jogosulatlan másolását és terjesztését, egy érvényességet ellenőrző rendszert használunk, amellyel a 10 digitális audiovizuális rendszer egy vagy több készülékét ellenőrizzük, még a készülékek közötti bármely adatkommunikációt megelőzően.

Egy általunk előnyösnek tartott készülék érvényesség ellenőrző rendszer egy készülék és egy biztonsági modul között hitelességi bizonyítványok közvetítésén, továbbításán alapul. Erre mutatunk példát a 2. ábrán, ahol minden egyes készüléket és biztonsági modult egy egyedi bizonyítvánnyal láttunk el a érvényesség ellenőrzéséhez.

Egy bizonyítvány szétosztó rendszer első fokozatában egy 50 hitelesítő hatóság kódolt bizonyítványokat küld 52 fogyasztói elektronika gyártókhoz és 54 biztonsági szolgáltatókhoz.

Az 50 hitelesítő hatóság minden egyes 52 fogyasztói elektronika gyártó részére egy-egy kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítványt küld. Ez az 56 bizonyítvány többek között egy CEman_Kpub gyártó nyilvános kulcsot tartalmaz, és egy rendszer vagy hitelesítő hatósági CA_Kpri privát kulccsal van kódolva. Annak érdekében, hogy az 56 bizonyítvány tartalmát az 52 fogyasztói elektronika gyártó dekódolhassa, az 50 hitelesítő hatóság az 52 fogyasztói elektronika gyártó részére megküldi a CA_Kpub nyilvános kulcsot. Megjegyezzük, jóllehet ismert, hogy a CA_Kpri privát kulcs egyedi, és kizárólag az 50 hitelesítő hatóság birtokában található fel.

Hasonlóképpen, az 50 hitelesítő hatóság minden egyes 54 biztonsági szolgáltató részére megküld egy-egy kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítványt. Ez az 58 bizonyítvány többek között egy 54 biztonsági szolgáltatóhoz tartozó SP_Kpub nyilvános kulcsot tartalmaz, és az 50 hitelesítő hatóság CA_Kpri privát kulcsával van kódolva. Annak érdekében, hogy az 58 bizonyítvány tartalmát az 54 biztonsági szolgáltató dekódolhassa, az 50 hitelesítő hatóság az 54 biztonsági szolgáltató számára megadja saját CA_Kpub nyilvános kulcsát.

A bemutatott bizonyítvány szétosztó rendszer második fokozatában minden egyes 52 fo-

gyasztói elektronika gyártó és 54 biztonsági szolgáltató egy-egy bizonyítványt rendel hozzá minden egyes saját termékéhez.

Így például minden egye 52 fogyasztói elektronika gyártó minden egyes 60 fogyasztói elektronikai készülékéhez egy-egy kódot $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt rendel. Ez a 62 bizonyítvány többek között egy egyedi Device_Kpub készülék nyilvános kulcsot tartalmaz, az illető készülék tulajdonságának (felvevő, lejátszó és így tovább) jelzésével együtt. A 62 bizonyítvány a CEman_Kpub nyilvános kulccsal ekvivalens kulccsal van kódolva. Annak érdekében, hogy a 62 bizonyítvány tartalmát dekódolhassuk, az 52 fogyasztói elektronika gyártó a 60 fogyasztói elektronikai készülékben eltárolja a CA_Kpub nyilvános kulcsot, valamint az 52 fogyasztói elektronika gyártó kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítványát. Így a 60 fogyasztói elektronikai készülék Device_Kpub nyilvános kulcsa az illető készülék egyedi azonosítójául szolgálhat.

Hasonlóképpen, minden egyes 54 biztonsági szolgáltató minden egye 64 biztonsági modulhoz egy-egy kódolt $Cert_{SP}$(SM_Kpub) 66 bizonyítványt rendel hozzá. Ezek a 64 biztonsági modulok bármilyen alakban megvalósíthatók, fizikai méretük és jellemzőjük függvényében. Például a 64 biztonsági modul egy 60 fogyasztói elektronikai készülékben kialakított foglalatba eltávolíthatóan behelyezhető modulként képezhető ki, vagy akár a 60 fogyasztói elektronikai készülékhez csatlakoztatható különálló egységként gyártható. Egyes esetekben egy bankkártyához hasonló kialakítású programozható csipkártyát is használhatunk, de egyéb alakú készülékek, például PCMCIA típusú kártyák is egyaránt jól használhatók.

A 64 biztonsági modulhoz társított kódolt 66 bizonyítvány többek között egy egyedi SM_Kpub nyilvános kulcsot tartalmaz. A 66 bizonyítvány az SP_Kpub nyilvános kulccsal ekvivalens kulccsal van kódolva. Annak érdekében, hogy a 66 bizonyítvány tartalmát dekódolhassuk, az 54 biztonsági szolgáltató a 64 biztonsági modulban eltárolja az 50 hitelesítő hatóság CA_Kpub nyilvános kulcsát, valamint az 54 biztonsági szolgáltató kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítványát. Így a 64 biztonsági modul SM_Kpub nyilvános kulcsa a 64 biztonsági modul azonosítójául szolgálhat.

A fent említett 56, 58, 62, 66 bizonyítványok bármelyikét aláírással láthatjuk el, hogy az 56, 58, 62, 66 bizonyítványok tartalmát azok dekódolását követően ellenőrizni tudjuk. Az 56, 58, 62, 66 bizonyítványok tartalmát azok kódolásához használt kulcs segítségével írhatjuk alá.

A 10 digitális audiovizuális rendszer egyes készülékei érvényességének az ellenőrzését az egyes készülékek és az egyes 64 biztonsági modulok között az 56, 58, 62, 66 bizonyítványok cseréje révén valósíthatjuk meg. Mint a 3. ábrán vázoltuk, egy első lehetséges kiviteli alaknál a 64 biztonsági modul 70 kommunikációs kapcsolaton keresztül áll a 60 fogyasztói elektronikai készülékkel kapcsolatban, ami csupán annak az egy 60 fogyasztói elektronikai készüléknek az ellenőrzését teszi lehetővé a 64 biztonsági modul számára. Azonban a 4. ábrán látható vázlat szerint a 64 biztonsági modult két vagy több 60a, 60b készülékhez is csatlakoztathatjuk egy-egy 70a, 70b kommunikációs kapcsolaton keresztül.

Egy 60 fogyasztói elektronikai készülék 64 biztonsági modullal történő ellenőrzésére az 5. ábrán bemutatott folyamatábra segítségével adunk példát.

A érvényesség ellenőrzési műveletet bármikor megindíthatjuk, például a 60 fogyasztói elektronikai készülék bekapcsolását követően, valamilyen adathordozó, például lemez behelyezésekor, a 60 fogyasztói elektronikai készüléknek a felhasználó általi vezérlésekor, a 64 biztonsági modullal létrehozott kapcsolat létrejöttekor, és így tovább.

A érvényesség ellenőrzési műveletet a 64 biztonsági modul kezdeményezi. Mint az 5. ábrán látható, 100 lépésben a 64 biztonsági modullal a 60 fogyasztói elektronikai készülék részére ismertetjük az 54 biztonsági szolgáltató kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítványát. 102 lépésben a 60 fogyasztói elektronikai készülékkel dekódoljuk a kapott kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítvány tartalmát az 50 hitelesítő hatóság CA_Kpub nyilvános kulcsának az alkalmazásával, hogy az 58 bizonyítványból megkaphassuk az 54 biztonsági szolgáltató SP_Kpub nyilvános kulcsát.

A kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítvány 60 fogyasztói elektronikai készülékhez történő továbbítását követően a 64 biztonsági modul saját egyedi kódolt $Cert_{SP}$(SM_Kpub) 66 bizonyítványát is átküldi a 60 fogyasztói elektronikai készüléknek. 106 lépésben a 60 fogyasztói elektronikai készülék dekódolja a kódolt $Cert_{SP}$(SM_Kpub) 66 bizonyítvány tartalmát, amelyet a 60 fogyasztói elektronikai készülék a kódolt $Cert_{CA}$(SP_Kpub) 58 bizonyítványból megkapott 54 biztonsági szolgáltató SP_Kpub nyilvános kulcsának alkalmazásával kap meg, annak érdekében, hogy a 64 biztonsági modul SM_Kpub nyilvános kulcsát meg lehessen kapni a 66 bizonyítványból.

108 lépésben a 60 fogyasztói elektronikai készülék a 64 biztonsági modulhoz elküldi az 52 fogyasztói elektronika gyártó kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítványát. 110 lépésben a 64 biztonsági modul ezt a kapott kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítványt az

50 hitelesítő hatóság CA_Kpub nyilvános kulcsának felhasználásával dekódolja, hogy megkapja az 56 bizonyítványból az 52 fogyasztói elektronika gyártó CEman_Kpub nyilvános kulcsát.

A kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítvány 64 biztonsági modulhoz történő eljuttatását követően 112 lépésben a 60 fogyasztói elektronikai készülékkel X véletlenszámot állítunk elő. Ez a X véletlenszám nem játszik szerepet a 60 fogyasztói elektronikai készülék 64 biztonsági modullal történő ellenőrzése során. Ehelyett az X véletlenszámot a 60 fogyasztói elektronikai készülék és a 64 biztonsági modul között egy biztonságos hitelesített csatorna létrehozására használjuk, amelynek folyamatát az alábbiakban részletesebben is leírjuk.

114 lépésben a 60 fogyasztói elektronikai készülék az X véletlenszám és a 60 fogyasztói elektronikai készülékben tárolt kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítvány bitjeit összekeveri, hogy ezzel az X véletlenszámot és a kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt bitsorkódolja. A bitsorkódolt X véletlenszámot és a kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt ezt követően a korábban a 64 biztonsági modul által a 104 lépésben a 60 fogyasztói elektronikai készülékhez továbbított 64 biztonsági modul SM_Kpub nyilvános kulcs alkalmazásával kódolja, majd ezt a kódolt és bitsorkódolt X véletlenszámot és kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt 118 lépésben elküldi a 64 biztonsági modulhoz.

120 lépésben a 64 biztonsági modul dekódolja a kódolt és bitsorkódolt X véletlenszámot és kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt, amelyhez az SM_Kpub nyilvános kulccsal ekvivalens SM_Kpriv privát kulcsot használ. A kevert X véletlenszámot és a kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt 122 lépésben bitsordekódoljuk.

Az X véletlenszám és a kódolt SM_Kpub nyilvános kulcs bitjeinek összekeverésére szolgáló algoritmust a 64 biztonsági modulban tárolhatjuk el, hogy ezzel lehetővé tegyük a bitek összekeverésének megfordítását, vagyis a bitek helyreállítását. Egy alternatív javaslat értelmében a 64 biztonsági modul a 60 fogyasztói elektronikai készülékhez egy másik Z véletlenszámot küldhet, a kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítvány vételét követően. A Z véletlenszámot a 60 fogyasztói elektronikai készülék bit szinten összekeveri, a 64 biztonsági modul SM_Kpub nyilvános kulcsának használatával kódolja, majd előnyösen ugyanabban az időben továbbítja a 64 biztonsági modulhoz, mint amikor az összekevert bitű X véletlenszámot és a kódolt $Cert_{CEman}$(Device_Kpub) 62 bizonyítványt is elküldi. A

64 biztonsági modul a kódolt és bit szinten kevert Z véletlenszámot dekódolja, és összehasonlítja a benne eltárolt, bitkeverés nélküli véletlenszámmal. annak érdekében, hogy meghatározza, hogy a 60 fogyasztói elektronikai készülék hogyan keverte meg a Z véletlenszám bitjeit. A 64 biztonsági modul ennek a próbának az eredményét arra használja fel, hogy megfordítsa az X véletlenszámmal és a kódolt $Cert_{CA}$(CEman_Kpub) 56 bizonyítványon elvégzett bitkeverést.

E rövid kitérő magyarázat után visszatérve az 5. ábrára látható, hogy 124 lépésben a 64 biztonsági modullal az X véletlenszámot megkapjuk és eltároljuk. 126 lépésben a 64 biztonsági modul az 52 fogyasztói elektronika gyártó már korábban a 60 fogyasztói elektronikai készülék közvetítésével a 64 biztonsági modulhoz eljuttatott CEman_Kpub nyilvános kulcsának a felhasználásával, annak érdekében, hogy a 60 fogyasztói elektronikai készülék Device_Kpub nyilvános kulcsát ki tudjuk vonni a 62 bizonyítványból.

A 60 fogyasztói elektronikai készülék érvényességének ellenőrzését a 64 biztonsági modul a 128 lépésben végzi el, a 60 fogyasztói elektronikai készülék Device_Kpub nyilvános kulcsának a felhasználásával. Ennek során a 64 biztonsági modul a kapott Device_Kpub készülék nyilvános kulcsot összehasonlítja egy, benne korábban eltárolt készülék nyilvános kulcs listával. A készülék nyilvános kulcs listát az 50 hitelesítő hatóság állíthatja elő, és például az 54 biztonsági szolgáltató a 64 biztonsági modul memóriájában, például valamilyen nem felejtő tárában rögzítheti.

A 64 biztonsági modul kétféle listát támogat. Egy úgynevezett "visszavonási lista" az érvénytelen készülékekhez tartozó készülék nyilvános kulcsokat tartalmazza, és a nem megfelelő vagy nem jóváhagyott készülékek fekete listára tételére használjuk. Egy "hitelesítési lista" az érvényes, jóváhagyott készülékekhez tartozó készülék nyilvános kulcsokat tartalmazza, és arra használjuk, hogy az adatátvitelt két korábban regisztrált készülék között engedélyezzük csak.

A harmadik személyek által szándékosan, például az Interneten nyilvánosságra hozott készülék azonosítókat az 50 hitelesítő hatóság a 64 biztonsági modul időszakos frissítése során a visszavonási listára teheti annak érdekében, hogy meggátolja az adatátvitelt ezekhez a készülékekhez vagy ezektől a készülékektől, vagy ezek utánzataitól. A hitelesítési lista alkalmazásával hasonlóképpen meg tudjuk gátolni például az Interneten szándékosan megjelenített készülékazonosítók működését, mivel ezek az azonosítók például egy házi hálózat kivételével sehol máshol nem lesznek érvényesek.

A kódolt készülék bizonyítványba vagy a kódolt 64 biztonsági modul bizonyítványba ágyazott indikátor (flag) határozza meg a listát, amelyek a kapott készülék nyilvános kulcsot összehasonlítjuk. Például a 64 biztonsági modul a kapott készülék nyilvános kulcsot összehasonlíthatja az érvénytelen készülékekhez tartozó, tárolt nyilvános kulcsokkal, ha ennek az indikátornak az értéke "0" és a kapott készülék nyilvános kulcsot mind az érvénytelen készülékekhez tartozó eltárolt nyilvános kulcsokkal, mind pedig az érvényes készülékekhez tartozó tárolt nyilvános kulcsokkal összehasonlíthatja, ha az indikátor értéke "1".

Ha a 60 fogyasztói elektronikai készülék érvénytelen készüléknek minősül, akkor a 64 biztonsági modul a 60 fogyasztói elektronikai készülékkel folytatott kommunikációt megszakítja. Ha a 4. ábrán látható módon a 64 biztonsági modul más 60 fogyasztói elektronikai készülékekkel is kommunikációt folytat, akkor a kommunikációt ilyen esetben azokkal a 60 fogyasztói elektronikai készülékekkel is megszakítja.

Ha a 60 fogyasztói elektronikai készülék érvényes készüléknek minősül, akkor a 64 biztonsági modul a 60 fogyasztói elektronikai készülék és a 64 biztonsági modul között létrehoz egy biztonságos hitelesített csatornát a kommunikáció céljára. A 6. ábrán egy 60 fogyasztói elektronikai készülék és egy 64 biztonsági modul közötti, kommunikáció céljára szolgáló biztonságos hitelesített csatorna létrehozásának folyamatát vázoltuk.

200 lépésben a 64 biztonsági modul egy SK véletlen eseménykulcsot hoz létre. Ezt az SK véletlen eseménykulcsot 202 lépésben a 64 biztonsági modul a 60 fogyasztói elektronikai készülék által részére megküldött X véletlenszám felhasználásával TDES módon kódolja. 204 lépésben ezt a kódolt $TDES_X(SK)$ eseménykulcsot azután továbbítjuk a 60 fogyasztói elektronikai készülékhez.

206 lépésben a 60 fogyasztói elektronikai készülék a kapott kódolt $TDES_X(SK)$ eseménykulcsot az X véletlenszám felhasználásával dekódolja, és az SK eseménykulcsot 208 lépésben eltárolja memóriájában. Ezt követően az SK eseménykulcsot használja fel a 60 fogyasztói elektronikai készülék és a 64 biztonsági modul között közvetített adatok kódolásához.

A 60 fogyasztói elektronikai készülék érvényességének megállapítását követően a 64 biztonsági modul kulcs szétosztást végez, annak érdekében, hogy létrehozzon egy biztonságos kommunikációs csatornát a 60 fogyasztói elektronikai készülék és a 64 biztonsági modul közt. Az SK eseménykulcs frissítését szintén bármikor kezdeményezhetjük, például a 60

fogyasztói elektronikai készülék bekapcsolásakor, lemez behelyezésekor, a 60 fogyasztói elektronikai készüléknek a felhasználó általi működtetésekor, a 64 biztonsági modullal történő kapcsolat felvételekor és így tovább.

Az 1. ábrán feltüntetett 12 DVD lejátszó készülék általában bitsorkódolt adatokat továbbít a 14 digitális kijelzőhöz és a 18 digitális felvevő készülékhez. Az említett 60 fogyasztói elektronikai készülékek által fogadott adatok bitsordekódolását a 7. ábra segítségével mutatjuk be.

Egy DVD lemez általában kódolt, jogosultság vezérlő üzeneteket tárol, a bitsorkódolt audio és/vagy vizuális adatokkal együtt. Egy ilyen jogosultság vezérlő üzenet ezekre a bitsorkódolt és/vagy vizuális adatokra vonatkozó üzenet, amely egy ellenőrző szót (ez teszi lehetővé az adatok bitsordekódolását), valamint az adatokhoz való hozzáférés feltételeit tartalmazza. A hozzáférési feltételeket és az ellenőrző szót a 12 DVD lejátszó készülék adja át például a 16 kommunikációs kapcsolaton keresztül a 14 digitális kijelzőnek.

A 12 DVD lejátszó készülékhez tartozó lemezen tárolt adatok általában számos vagy több különböző összetevőt tartalmaznak, például egy televízió programnak van egy videó összetevője, egy audio összetevője, egy alcím összetevője, és így tovább. Ezen összetevők mindegyike külön-külön van bitsorkódolva és kódolva. Az adatok minden egyes bitsorkódolt összetevőjéhez egy-egy önálló jogosultság vezérlő üzenet szükséges, de alternatív lehetőségként egyetlen jogosultság vezérlő üzenet érvényes lehet egy adott szolgáltatás összes bitsorkódolt összetevőjére is.

Az ellenőrző szó általában néhány másodpercenként módosul, így a jogosultság vezérlő üzeneteket időszakonként be kell illesztenünk az adatáramba, hogy lehetővé tegyük az ellenőrző szó ismétlődő bitsordekódolását. Redundancia céljából minden egyes jogosultság vezérlő üzenet általában két vezérlő szót tartalmaz, nevezetesen a jelenlegi ellenőrző szót és a rákövetkező ellenőrző szót.

Ha a 14 digitális kijelző megkapja a 12 DVD lejátszó készüléktől a bitsorkódolt adatokat és a kódolt jogosultság vezérlő üzenetet, úgy a bitsorkódolt adatokból kivonja a jogosultság vezérlő üzenetet, és azt átadja a bitsordekódoló áramkörnek, hogy az dekódolja a jogosultság vezérlő üzenetet, majd a dekódolt jogosultság vezérlő üzenetből kapja meg az ellenőrző szót.

A bitsordekódoló áramkör akár egy különálló, eltávolítható 40 feltételes hozzáférési mo-

dulként is megvalósítható, amely igen gyakran PCMCIA kártya alakjában kerül megvalósításra, és a befogadó 60 fogyasztói elektronikai készülék egy erre a célra kialakított foglalatába helyezhető. Egy alternatív megoldásként a 40 feltételes hozzáférési modul és a 14 digitális kijelző bármely megfelelő 42 kommunikációs kapcsolaton keresztül, például soros vagy párhuzamos interfészen keresztül is kapcsolatban állhat egymással.

A 40 feltételes hozzáférési modul ezen túlmenően például egy programozható csipkártya felvételére, befogadására alkalmas kártyaolvasót is tartalmazhat. Ilyen rendszereknél a programozható csipkártya határozza meg, hogy a végfelhasználó jogosult-e a hozzáférés vezérlő üzenet dekódolására, és ezen keresztül a programokhoz történő hozzáférésre. Ha a végfelhasználó rendelkezik ezekkel a jogosultságokkal, akkor a jogosultság vezérlő üzeneteket a programozható csipkártyán lévő 41 processzor dekódolja, és kivonja belőle az ellenőrző szót. A 40 feltételes hozzáférési modul 41 processzora ezt követően bitsordekódolja a bitsorkódolt adatokat, hogy a fogadó 60 fogyasztói elektronikai készüléket például dekomprimálás majd azt követő megjelenítés céljából tiszta, kódolatlan adatárammal lássa el. Alternatív megoldásként az adatok bitsordekódolását a 14 digitális kijelzőn belül is végrehajthatjuk, amelyhez a 40 feltételes hozzáférési modultól a 14 digitális kijelzőhöz közvetített ellenőrző szó információt használjuk fel.

Olyan esetben, amikor a bitsorkódolt adatokat a 12 DVD lejátszó készülékből továbbítjuk a 18 digitális felvevő készülékbe azt követő megnézés céljából, a DVD lemez gyártója korlátozhatja a tárolt adatokhoz történő hozzáférést. Például a lemez gyártója meggátolhatja a lemezre rögzítette adatok további másolását. Ilyen körülmények között a hozzáférési jogosultságokat, vagy kiterjesztett vezérlést kezelő információt egy kiterjesztett jogosultság vezérlő üzenetben helyezzük el, amely a lemez gyártója által meghatározott hozzáférési jogosultságokat tartalmazza. Egy ilyen kiterjesztett jogosultság vezérlő üzenet vétele esetén a 40 feltételes hozzáférési modul 41 processzora dekódolja a kiterjesztett jogosultság vezérlő üzenetet, azt módosítja, például úgy, hogy megtiltja a felvett adatok bármilyen jellegű másolását, újrakódolja a jogosultság vezérlő üzenetet, majd ezt a módosított és újrakódolt jogosultság vezérlő üzenetet visszajuttatja a 18 digitális felvevő készülékbe.

Egy ilyen típusú rendszerben az érzékeny és bizalmas adatok (ellenőrző szavak, módosított kiterjesztett jogosultság vezérlő üzenetek, vagy bitsordekódolt adatok) szabadon áramlanak a 40 feltételes hozzáférési modul és a 14 digitális kijelző vagy 18 digitális felvevő készülék között, és ennél az interfésznél éppen ezért biztonsági problémák léphetnek fel. az ilyen

jellegű gondok elkerülésére még az adatok kommunikációját megelőzően, például a 14 digitális kijelzőtől egy jogosultság vezérlő üzenetnek egy programozható csipkártyához történő elküldését megelőzően létrehozunk az 5. és 6. ábra segítségével bemutatott 42 biztonságos hitelesített csatornát a 14 digitális kijelző és a 40 feltételes hozzáférési modul között. Annak érdekében, hogy a 14 digitális kijelző és a 40 feltételes hozzáférési modul között létrehozhassunk egy 42 biztonságos hitelesített csatornát, a 40 feltételes hozzáférési modulnak például a programozható csipkártyában tárolnia és tartalmaznia kell a készülék nyilvános kulcsokat tartalmazó listát, azért, hogy hitelesíteni tudja a 14 digitális kijelzőt.

Mint a 4. ábrán látható, a 64 biztonsági modul két vagy több 60a, 60b fogyasztói elektronikai készülékhez is kapcsolódhat egy-egy 70a, 70b kommunikációs kapcsolaton keresztül. Ezen 60a, 60b fogyasztói elektronikai készülékek érvényességének az ellenőrzésére vonatkozóan mindegyiket az 5. ábra kapcsán ismertetett módon ellenőrizhetjük, és ennek eredményeképpen a 64 biztonsági modul a 60a, 60b fogyasztói elektronikai készülékek között létrehozhat egy biztonságos kommunikációs csatornát. A 8. ábrán két ilyen 60a, 60b fogyasztói elektronikai készülék között egy biztonságos kommunikáció létrehozásának jellemző lépéseit tüntettük fel.

Egy 60a, valamint egy 60b fogyasztói elektronikai készülék közötti biztonságos kommunikációt azt követően hajtunk végre, hogy a 60a, 60b fogyasztói elektronikai készülékeket a 64 biztonsági modul segítségével ellenőriztük. A 8. ábrán látható módon 300 lépésben 64 biztonsági modullal egy SK véletlen eseménykulcsot állítunk elő. 302 lépésben ezt az előállított SK véletlen eseménykulcsot kódoljuk a 64 biztonsági modullal, amelyhez a 60a fogyasztói elektronikai készülék érvényességének ellenőrzése közben az azáltal a 64 biztonsági modulhoz továbbított X véletlenszámot használjuk fel. A kódolást előnyösen valamilyen szimmetrikus algoritmus, például Triple DES (TDES) algoritmus segítségével hajtjuk végre.

A kódolt $TDES_X(SK)$ eseménykulcsot 304 lépésben juttatjuk el a 60a fogyasztói elektronikai készülékhez.

306 lépésben a 60a fogyasztói elektronikai készülék ezt a kapott kódolt $TDES_X(SK)$ eseménykulcsot az X véletlenszám felhasználásával dekódolja, és az SK eseménykulcsot eltárolja a memóriájában.

308 lépésben a 64 biztonsági modul az SK eseménykulcsot a 64 biztonsági modulhoz a 60b fogyasztói elektronikai készülék által annak hitelesítése során eljuttatott Y

véletlenszám felhasználásával TDES módon is kódolja. Az így kódolt $TDES_YSK$ eseménykulcsot 310 lépésben elküldi a 60c fogyasztói elektronikai készülékhez. 312 lépésben a 60b fogyasztói elektronikai készülék dekódolja a kódolt $TDES_X(SK)$ eseménykulcsot az Y véletlenszám felhasználásával, és az így kapott SK eseménykulcsot eltárolja memóriájában.

Így tehát az SK eseménykulcsot egy-egy biztonságos hiteles csatornán keresztül eljuttattuk mindegyik 60a, 60b fogyasztói elektronikai készülékhez. Ezt követően az SK eseménykulcsot például a 60a fogyasztói elektronikai készülék használhatja fel arra, hogy a 60b fogyasztói elektronikai készülékhez 75 kommunikációs kapcsolaton keresztül továbbított adatokat kódolja vele.

A 9. ábrán látható, hogy 400 lépésben a 60a fogyasztói elektronikai készülék a kódolt $TDES_{SK}(D)$ adatokat az SK eseménykulcs felhasználásával kódolja. Az erre a célra felhasznált kódoló algoritmus valamilyen szimmetrikus algoritmus, például a Triple DES (TDES) algoritmus vagy hasonló.

A kódolt C 402 lépésben a 75 kommunikációs kapcsolaton keresztül juttatjuk el a 60b fogyasztói elektronikai készülékhez. 404 lépésben a 60b fogyasztói elektronikai készülék dekódolja a kódolt $TDES_{SK}(D)$ adatokat az SK eseménykulcs felhasználásával, hogy megkapja, vagyis visszaállítsa a D adatokat.

Mint korábban már említettük, semelyik többi készülék vagy készülék nem állít elő újabb eseménykulcsot, az eseménykulcsokat kizárólag a 64 biztonsági modul állítja elő. Ezért a fent vázolt eljárás igen egyszerű, mégis biztonságos eljárás arra, hogy az egyes 60 fogyasztói elektronikai készülékek között biztonságos kommunikációt létesítsünk, hiszen az egyik 60 fogyasztói elektronikai készülék által továbbított adatokat csak egy olyan másik 60 fogyasztói elektronikai készülék tudja dekódolni, amely egy ilyen biztonságos hitelesített csatornát hozott létre ugyanazzal a 64 biztonsági modullal, mint a kibocsátó 60 fogyasztói elektronikai készülék.

A 7. ábra ismertetése kapcsán már említettük, hogy az egyes 60 fogyasztói elektronikai készülékek érvényességének megállapításán, valamint egy biztonságos hitelesített csatorna létrehozásán túl a 64 biztonsági modul ellenőrző szavakat, hozzáférési jogosultságokat és/vagy bitsorkódolt adatokat továbbíthat egy 60 fogyasztói elektronikai készülékhez. A 10. és 11. ábrán olyan példákat vázoltunk, amelyekben egy 64 biztonsági modullal biztonságos kommunikációs kapcsolatot létesítünk két 60 fogyasztói elektronikai készülék kö-

zött, majd azt követően a bitsorkódolt adatokkal társított adatokat továbbítunk a 60 fogyasztói elektronikai készülékhez.

A 10. ábrán látható első példában az egy 12 DVD lejátszó készülék és egy 14 digitális kijelzőként használt televízió között egy biztonságos kommunikációs kapcsolat létesítésével, valamint az azt követő műveletekkel társított lépésekkel bitsordekódolni tudjuk a 14 digitális kijelzővel a 12 DVD lejátszó készüléktől kapott bitsorkódolt adatokat.

500 lépésben a 64 biztonsági modullal megállapítjuk a 12 DVD lejátszó készülék, valamint a 14 digitális kijelző érvényességét és jogosultságát, amelyhez az 5. ábra kapcsán leírt lépéseket használjuk fel. Ha a két említett 60 fogyasztói elektronikai készülék valódinak és érvényesnek minősül, akkor a 64 biztonsági modullal biztonságos hitelesített csatornákat hozunk létre a 12 DVD lejátszó készülékhez és a 14 digitális kijelzőhöz, a 6. ábra kapcsán bemutatott lépéseket felhasználva. A biztonságos hitelesített csatornák létrehozásának az eredményeképpen mindegyik 60 fogyasztói elektronikai készülékben és a 64 biztonsági modulban eltárolunk egy SK eseménykulcsot.

502 lépésben a vezérlő rendszerrel bitsorkódolt adatokat, valamint hagyományosan kódolt jogosultság vezérlő üzeneteket tartalmazó adatok, amelyek az adatok bitsordekódolásához szükséges ellenőrző szavakat is magukban foglalják, a 12 DVD lejátszó készülékkel kódoljuk, amihez az SK eseménykulcsot használjuk fel, majd a 16 kommunikációs kapcsolaton keresztül a digitális televízióként megvalósított 14 digitális kijelzőhöz továbbítjuk.

504 lépésben a 14 digitális kijelzővel vesszük a kódolt adatokat és az SK eseménykulcs felhasználásával dekódoljuk. A bitsorkódolt adatokat ezt követően olyan 90 demultiplexerbe vezetjük, amely 506 lépésben a vezérlő rendszer által bitsorkódolt adatokat különválasztja a kódolt jogosultság vezérlő üzenetektől. A kódolt jogosultság vezérlő üzeneteket a biztonságos hitelesített csatornán keresztül a 14 digitális kijelzővel 508 lépésben juttatjuk el a 64 biztonsági modulhoz. Annak érdekében, hogy az adatokat a 64 biztonsági modulhoz a biztonságos hitelesített csatornán keresztül továbbíthassuk, a kódolt jogosultság vezérlő üzeneteket a 14 digitális kijelzővel még tovább kódoljuk, amihez a 64 biztonsági modul által előállított SK eseménykulcsot használjuk fel.

Mint a 10. ábrán látható, a 64 biztonsági modult képzeletben egy 666 szabványos formátumú biztonsági részre, valamint egy 68 saját formátumú biztonsági részre oszthatjuk fel. A kétszeresen kódolt jogosultság vezérlő üzeneteket 510 lépésben a 666 szabványos formátumú biztonsági résszel vesszük, és az SK eseménykulcs felhasználásával egyszer de-

kódoljuk. 512 lépésben a saját formátumban kódolt jogosultság vezérlő üzeneteket a 64 biztonsági modul 68 saját formátumú biztonsági részéhez továbbítjuk, amellyel 514 lépésben a kódolt jogosultság vezérlő üzeneteket dekódoljuk és érvényességüket megvizsgáljuk, amihez a tulajdonosnak a jogosultság vezérlő üzenetek kódolásához használt kulcsával ekvivalens kulcsot használunk, és ezt követően, amennyiben jogosultságunk van rá, feldolgozzuk jogosultság vezérlő üzenetet, hogy abból megkapjuk az ellenőrző szavakat vagy a vezérlő rendszer által bitsorkódolt kulcsokat.

516 lépésben ezeket a vezérlő rendszer által bitsorkódolt és megkapott kulcsokat a 666 formátumú biztonsági részbe tesszük át, amellyel a vezérlő rendszer által bitsorkódolt kódokat kódoljuk, az SK eseménykulcs felhasználásával, és az így kódolt kulcsokat a biztonságos hitelesített csatornán keresztül továbbítjuk a 14 digitális kijelzőhöz. Az azáltal vett kódolt vezérlőrendszer által bitsorkódolt kulcsokat a 14 digitális kijelzőben dekódoljuk az 518 lépésben, amihez az SK eseménykulcsot használjuk fel, majd ezt követően 92 bitsordekódolóhoz továbbítjuk, amellyel a vezérlőrendszer által bitsorkódolt adatokat bitsordekódoljuk. 520 lépésben a bitsordekódolt adatokat megjelenítés céljából 94 kijelzőhöz továbbítjuk.

A fentiekből kitűnik, hogy az ellenőrző szavakat az SK eseménykulcs felhasználásával mindig kódoljuk, mielőtt továbbítanánk bármely 60 fogyasztói elektronikai készülék és a 64 biztonsági modul között.

A fenti példában az ellenőrzőszavak a jogosultság vezérlő üzenetekben vannak beépítve. Ezek a jogosultság vezérlő üzenetek azonban a kiterjesztett vezérlési kezelő információval, vagy hozzáférési jogosultságokkal együtt egy kiterjesztett jogosultság vezérlő üzenetben is elhelyezhetők, amelyet például a 68 saját formátumú biztonsági résszel dolgozunk fel például annak érdekében, hogy megállapítsuk, hogy a felhasználó jogosultsága az adatok megismerésére már lejárt.

A 11. ábra a második példát mutatja, ahol a bemutatott lépések egybiztonságos kommunikációs kapcsolat felépítésére vonatkoznak egy 12 DVD lejátszó készülék és egy 18 digitális felvevő készülék között, míg az azt követő lépéseket a 18 digitális felvevő készülék által a 12 DVD lejátszó készüléktől kapott adatok bitsordekódolása céljából hajtjuk végre.

600 lépésben a 64 biztonsági modullal megvizsgáljuk a 12 DVD lejátszó készülék és a 18 digitális felvevő készülék érvényességét, amelyhez az 5. ábra kapcsán ismertetett lépéseket használjuk. Ha a 12 DVD lejátszó készüléket és a 18 digitális felvevő készüléket érvényes-

nek minősítjük, a 64 biztonsági modullal biztonságos hitelesített csatornákat hozunk létre a 12 DVD lejátszó készülékhez és a 18 digitális felvevő készülékhez, a 6. ábra ismertetés e során jelzett lépések segítségével. A biztonságos hitelesített csatornák létrehozásának az eredményeképpen mindegyik 60 fogyasztói elektronikai készülékben, valamint a 64 biztonsági modulban eltárolunk egy-egy SK eseménykulcsot.

602 lépésben a vezérlő rendszer által bitsorkódolt adatokat és saját formátumban kódolt, az adatok és a kiterjesztett vezérlési kezelő információ bitsordekódolására szolgáló ellenőrző szavakat tartalmazó kiterjesztett jogosultság vezérlő üzeneteket magában foglaló adatokat a 12 DVD lejátszó készülék kódolja az SK eseménykulcs felhasználásával, és 20 buszon keresztül a 18 digitális felevőhöz továbbítja.

A kódolt adatokat 604 lépésben vesszük a 18 digitális felevővel, és az SK eseménykulcs felhasználásával dekódoljuk. A bitsorkódolt adatokat 90 demultiplexerhez továbbítjuk, amellyel 606 lépésben a vezérlő rendszer által bitsorkódolt adatokat külön választjuk a kódolt kiterjesztett jogosultság vezérlő üzenetektől. A kódolt kiterjesztett jogosultság vezérlő üzeneteket a biztonságos hitelesített csatornán keresztül a 18 digitális felvevő készülékkel 608 lépésben a 64 biztonsági modulhoz továbbítjuk. Annak érdekében, hogy a 64 biztonsági modulhoz adatot tudjunk küldeni a biztonságos hitelesített csatornán keresztül, a kódolt, kiterjesztett jogosultság vezérlő üzeneteket a 18 digitális felevőben tovább kódoljuk, a 64 biztonsági modul által előállított SK eseménykulcs felhasználásával.

Mint a 11. ábrán látható, a 64 biztonsági modult képzeletben itt is egy 666 szabványos formátumú biztonsági részre és egy 68 saját formátumú biztonsági részre oszthatjuk fel. A kétszeresen kódolt kiterjesztett jogosultság vezérlő üzeneteket 610 lépésben a 666 szabványos formátumú biztonsági résszel vesszük, és az SK eseménykulcs felhasználásával egyszer dekódoljuk. 512 lépésben a saját formátumban kódolt kiterjesztett jogosultság vezérlő üzeneteket a 64 biztonsági modul 68 saját formátumú biztonsági részéhez továbbítjuk, amellyel 614 lépésben a kódolt kiterjesztett jogosultság vezérlő üzeneteket dekódoljuk és érvényességüket ellenőrizzük, amihez a felhasználónak a kiterjesztett jogosultság vezérlő üzenetek kódolásához használt kulcsával ekvivalens kulcsot használunk, majd amennyiben jogosultak vagyunk, feldolgozzuk a kiterjesztett jogosultság vezérlő üzeneteket, hogy felfrissítsük a kiterjesztett vezérlés kezelő információt, például azért, hogy korlátozzuk azt a számot, ahányszor a felhasználó újrajátszhatja az adatokat, hogy ezzel az adat további újrafelvételét meggátoljuk, és így tovább.

616 lépésben a módosított kiterjesztet jogosultság vezérlő üzeneteket egy saját formátumú PA algoritmus használatával, valamint a 64 biztonsági modul 68 saját formátumú biztonsági részében tárolt 96 felhasználói kulccsal kódoljuk. Ez további biztonságot ad a 18 digitális felvevő készülékkel rögzítet adatok számára, hiszen a vezérlő rendszer által bitsorkódolt adatok bitsordekódolásához szükséges ellenőrző szavakat kizárólag akkor lehet a módosított kiterjesztett jogosultság vezérlő üzenetekből megszerezni, ha a felhasználó hozzáfér ehhez a 96 felhasználói kulcshoz. Így a rögzített adatok lejátszását és megtekintését a 64 biztonsági modul mindenkori birtokosa részére tudjuk korlátozni.

618 lépésben a kódolt kiterjesztett jogosultság vezérlő üzeneteket a 64 biztonsági modul 666 szabványos formátumú biztonsági részéhez továbbítjuk, amellyel a kódolt kiterjesztett jogosultság vezérlő üzeneteket tovább kódoljuk, az SK eseménykulcs felhasználásával, és az így kódolt kiterjesztett jogosultság vezérlő üzeneteket a biztonságos hitelesített csatornán keresztül a 18 digitális felvevő készülékhez juttatjuk el. A 18 digitális felvevő készülék a kapott kódolt kiterjesztett jogosultság vezérlő üzeneteket az SK eseménykulcs felhasználásával 620 lépésben egyszer dekódolja, majd ezt követően valamilyen 98 adathordozóhoz, például DAT szalaghoz továbbítjuk, amelyen a vezérlő rendszer által bitsorkódolt adatokat és a kódolt kiterjesztett jogosultság vezérlő üzeneteket el tudjuk tárolni.

A fentiek alapján nyilvánvaló, hogy találmányunkat kizárólag általunk előnyösnek tartott példákkal mutattuk be, így az egyes megoldási részletek megváltoztatása vagy módosítása a találmány oltalmi körén belül esik.

Például, míg a fenti példák az egyes 60 fogyasztói elektronikai készülékek közötti 16 70 42 75 kommunikációs kapcsolatokat egy IEEE 1394 típusú digitális interfész használatával megvalósított kapcsolatként írják le, egyirányú kapcsolatokat, például 8-VSB és 16-VSB típusú kapcsolatokat is használhatunk.

Nem feltétlenül szükséges, hogy egy 60 fogyasztói elektronikai készülék az 56, 58, 62, 66 bizonyítványokat közvetlenül egy 64 biztonsági modulhoz továbbítsa. Például olyan esetben, amikor egy első 60 készülék nem képes adatokat fogadni egy 64 biztonsági modultól, ez az első készülék bizonyítványait egy kétirányú kommunikáció során, amelyet a 64 biztonsági modullal folytat le az első 60 fogyasztói elektronikai készülék érvényességének a megállapítása érdekében, egy második 60 fogyasztói elektronikai készülékhez vigyük át.

A leírt példákban csupán egyetlen 64 biztonsági modult alkalmazunk. Egy hálózaton belül, amely több, egymással különböző interfészeken keresztül kapcsolatban álló 60 fogyasztói

elektronikai készülékekből áll, különböző 64 biztonsági modulok lehetségesek.

A leírásban, és (ahol fennáll) az igénypontokban és a rajzokban megismerhető minden egyes jellemző önállóan, de egymással megfelelően kombinálva is felhasználható.

Szabadalmi igénypontok

1. Eljárás digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy egy készüléktől egy készülék azonosítót közlünk egy független biztonsági modullal (64), és a közölt azonosító azonosságától függően készülék érvényesség ellenőrzést végzünk.

2. az 1. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modullal (64) végzett készülék érvényesség ellenőrzés során a közölt azonosítót legalább egy tárolt azonosítóval összehasonlítjuk.

3. A 2. igénypont szerinti eljárás, ***azzal jellemezve***, hogy minden egyes tárolt azonosítót egy érvényes készülékkel vagy egy érvénytelen készülékkel társítunk.

4. A 3. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a közölt azonosítót érvénytelen készülékekkel társított tárolt azonosítókkal hasonlítjuk össze.

5. A 3. vagy 4. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a közölt azonosítót érvényes készülékekkel társított tárolt azonosítókkal hasonlítjuk össze.

6. Eljárás digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy egy készüléktől kapott azonosítót legalább egy tárolt azonosítóval összehasonlítunk, minden egyes tárolt azonosítót egy-egy érvényes készülékhez hozzárendelünk, és ha a kapott azonosító a tárolt azonosítók legalább egyikével azonos, a készülékek érvényességét jóváhagyjuk.

7. A 6. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a legalább egy tárolt azonosítót egy független biztonsági modulban (64) tároljuk.

8. Az 5. vagy 7. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kapott azonosítót egy indikátor értékétől függően hasonlítjuk össze az érvényes készülékekkel társított tárolt

azonosítókkal.

9. Az 1-6., 8. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy a készülék és a biztonsági modul (64) között a készülék érvényesítéséhez bizonyítványokat továbbítunk.

10. A 9. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a készülék azonosítóját kódolt bizonyítványban továbbítjuk a biztonsági modulhoz (64).

11. A 10. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a bizonyítványt az elküldött bizonyítvány hitelessége ellenőrzésének a lehetővé tételéhez aláírjuk.

12. A 10. vagy 11. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a bizonyítványt egy privát kulcs használatával kódoljuk.

13. A 12. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modulhoz (64) egy rendszer privát kulccsal kódolt bizonyítványban a privát kulccsal ekvivalens kulcsot továbbítunk, és egy rendszer nyilvános kulcsot mind a biztonsági modulban (64), mind a készülékben eltárolunk.

14. A 12. vagy 13. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kódolt bizonyítványt a készülékkel egy biztonsági modul (64) nyilvános kulcs használatával tovább kódoljuk, és a biztonsági modulhoz (64) továbbítjuk.

15. A 14. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kódolt bizonyítványt a biztonsági modullal (64) dekódoljuk, úgy, hogy először egy biztonsági modul (64) privát kulcsot használunk, másodszor pedig az ekvivalens kulcsot használjuk, lehetővé téve a készülék azonosítójának kivonását a dekódolt bizonyítványból.

16. A 15. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a készülék azonosítót tartalmazó bizonyítványt a készülékkel még a kódolás előtt véletlenszám-generálásnak vetjük alá, és a véletlenszám-generálást a bizonyítvány dekódolását követően a biztonsági modullal (64) visszájára fordítjuk.

17. A 12. vagy 13. igénypontok szerinti eljárás, ***azzal jellemezve***, hogy a készülékkel egy véletlenszámot (X) állítunk elő, és a véletlenszámot (X) és a készülék azonosítóját tartalmazó kódolt bizonyítványt a készülékkel kódoljuk egy biztonsági modul (64) nyilvános kulcs használatával, majd a biztonsági modulhoz (64) továbbítjuk.

18. A 17. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kódolt véletlenszámot (X) és a kódolt bizonyítványt a biztonsági modullal (64) dekódoljuk, úgy, hogy először egy biz-

tonsági modul (64) privát kulcsot használunk a véletlenszám (X) kinyerésére, másodszor pedig a nyilvános kulcsot használjuk a készülék azonosítójának a biztonsági modullal (64) történő kinyerésére.

19. A 18. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kinyert véletlenszámot (X) a biztonsági modulban (64) tároljuk, úgy, hogy a biztonsági modultól (64) a készülékhez irányuló kommunikációt a biztonsági modulban (64) és a készülékben a véletlenszámmal (X) kódolni és dekódolni tudjuk

20. Eljárás digitális adatok egy készülék és egy biztonsági modul közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy a biztonsági modulhoz (64) egy véletlenszámot és a készülék azonosítóját a biztonsági modul (64) egy nyilvános kulcsával kódolva elküldjük, majd a biztonsági modullal (64) a véletlenszámot és a készülék azonosítót a biztonsági modul (64) egy privát kulcsával dekódoljuk, a készüléket a készülék azonosító felhasználásával érvényesítjük, és a készülék érvényessége esetén a véletlenszám használatával a biztonsági modul (64) és a készülék között továbbított adatokat kódoljuk és dekódoljuk.

21. A 20. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a készülék azonosítóját a készülékkel előállított bizonyítványba építjük be, és a bizonyítványt a biztonsági modul (64) nyilvános kulcsával kódoljuk.

22. A 20. vagy 21. igénypont szerinti eljárás, *azzal jellemezve*, hogy a véletlenszámot a készülékkel még a kódolást megelőzően generáljuk, és a véletlenszám-generálást a biztonsági modullal (64) a véletlenszám dekódolását követően visszafordítjuk.

23. A 17-19., 21. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy a véletlenszámot és a készülék azonosítóját tartalmazó bizonyítványt a készülékkel még a kódolást megelőzően generáljuk, majd a véletlenszám-generálást a biztonsági modullal (64) a véletlenszám és a bizonyítvány dekódolását követően visszafordítjuk.

24. A 19-23. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modullal (64) a készülékhez egy a biztonsági modulban (64) előállított és a véletlenszám (X) használatával kódolt véletlen eseménykulcsot (SK) továbbítunk, és a készülékkel a kapott eseménykulcsot (SK) a véletlenszám (X) felhasználásával dekódoljuk, majd az így kapott eseménykulcsot használjuk a biztonsági modulhoz (64) küldött adatok kódolására.

25. A 24. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a készülékkel a biztonsági mo-

dulhoz (64) az adatok bitsordekódolásához szükséges ellenőrző szót tartalmazó kódolt jogosultság vezérlő üzenetet továbbítunk, és a készülékkel a kódolt jogosultság vezérlő üzenetet az eseménykulcs (SK) használatával tovább kódoljuk.

26. A 25. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modullal (64) a kódolt jogosultság vezérlő üzenetet dekódoljuk, abból az ellenőrző szót kinyerjük, és az ellenőrző szót az eseménykulcs (SK) használatával kódolva a készülékhez továbbítjuk.

27. A 24. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a készülékkel a biztonsági modulhoz (64) egy kódolt kiterjesztett jogosultság vezérlő üzenetet továbbítunk, amely az adatokhoz való hozzáférési jogosultságokat tartalmazza, és a készülékkel a kódolt kiterjesztett jogosultság vezérlő üzenetet az eseménykulcs felhasználásával tovább kódoljuk.

28. A 27. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modullal (64) a kódolt kiterjesztett jogosultság vezérlő üzenet dekódoljuk, az abban található hozzáférési jogosultságokat módosítjuk, a módosított kiterjesztett jogosultság vezérlő üzenetet kódoljuk, majd ezt az kódolt módosított kiterjesztett jogosultság vezérlő üzenetet az eseménykulcs (SK) felhasználásával tovább kódoljuk és a készülékhez továbbítjuk.

29. A 19-28. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy az adatokat egy első készülék és egy második készülék között továbbítjuk, és az egyes készülékeknek a biztonsági modullal (64) végzett érvényesítése során a biztonsági modullal (64) az első készülékhez a biztonsági modulban (64) előállított és az első által előállított véletlenszám (X) használatával kódolt véletlen eseménykulcsot (SK) küldünk, majd az első készülékkel a kapott véletlen eseménykulcsot (SK) az általa előállított véletlenszám (X) használatával dekódoljuk, és a biztonsági modullal (64) a második készülékhez a második készülék által előállított véletlenszám (Y) felhasználásával kódolt véletlen eseménykulcsot (SK) elküldjük, és a második készülékkel a kapott véletlen eseménykulcsot (SK) az általa előállított véletlenszám (Y) felhasználásával dekódoljuk, majd az így kapott véletlen eseménykulcsot (SK) ezt követően a biztonsági modul (64) és a készülékek között továbbított adatok, valamint az egyes készülékek között továbbított adatok kódolására használjuk.

30. Eljárás digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy egy biztonsági modult (64) hozunk létre, a biztonsági modulban (64) egy véletlen eseménykulcsot (SK) állítunk elő, és a véletlen eseménykulcs (SK) felhasználásával a készülékek között továbbított adatokat kódoljuk.

31. A 30. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a biztonsági modullal (64) minden egyes készülékhez elküldjük a készülék által előállított véletlenszám (X) felhasználásával kódolt véletlen eseménykulcsot (SK), és a készülékkel a véletlen eseménykulcsot (SK) a véletlenszám (X) felhasználásával dekódoljuk.

32. A 31. igénypont szerinti eljárás, ***azzal jellemezve***, hogy minden egyes készülékkel elküldjük a biztonsági modulhoz (64) a biztonsági modul (64) nyilvános kulcsának használatával kódolt, a készülékhez tartozó véletlenszámot.

33. A 32. igénypont szerinti eljárás, ***azzal jellemezve***, hogy a kódolt véletlenszámot (X) a biztonsági modullal (64) dekódoljuk, a biztonsági modul (64) privát kulcsának a felhasználásával, a véletlenszám (X) kinyerésére.

34. A 33. igénypont szerinti eljárás, ***azzal jellemezve***, hogy minden egyes véletlenszámot (X) az egyes készülékekkel állítunk elő még a kódolást megelőzően, és a véletlenszámgenerálást a biztonsági modullal (64) visszafordítjuk a véletlenszám (X) dekódolását követően.

35. A 30-34. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy biztonsági modullal (64) minden egye készüléket érvényesítünk, mielőtt a véletlen eseménykulcsot (SK) továbbítanánk az egyes készülékekhez.

36. A 35. igénypont szerinti eljárás, ***azzal jellemezve***, hogy minden egyes készülékkel egy a készülékhez tartozó azonosítót továbbítunk a biztonsági modulhoz (64), a készülék biztonsági modullal (64) történő érvényesítéséhez.

37. A 28-36. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy az eseménykulcsot (SK) a biztonsági modullal (64) időszakosan változtatjuk.

38. A 29-37. igénypontok bármelyike szerinti eljárás, ***azzal jellemezve***, hogy egy otthoni hálózati rendszerben készülékekként egy első és egy második, egymás között egy kommunikációs kapcsolaton keresztül adatok továbbítására alkalmas fogyasztói elektronikai készüléket alkalmazunk.

39. Berendezés digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy egy készülék azonosítót vevő eszközt, valamint a vett azonosító azonosságától függően készülék érvényesítést végrehajtó eszközt tartalmazó biztonsági modullal (64) van ellátva.

40. Biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy egy készülék azonosítójának vételére és a vett azonosító azonosságától függően készülék érvényesítés elvégzésére alkalmasan van kiképezve.

41. Berendezés digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy legalább egy azonosítót eltároló eszköze van, amelyben minden egyes eltárolt azonosító egy-egy érvényes készülékkel van társítva, továbbá egy készülék azonosítóját legalább egy eltárolt azonosítóval összehasonlító eszközt, valamint a készülék azonosítójának legalább egy eltárolt azonosítóval való azonossága esetén a készüléket érvényesítő eszközt tartalmaz.

42. Biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy legalább egy, egy-egy érvényes készülékkel társított azonosító eltárolására, egy készülék azonosítójának legalább egy eltárolt azonosítóval történő összehasonlítására, és a készüléket a készülék azonosítójának legalább egy azonosítóval való azonossága esetén érvényesítésére alkalmas módon van kialakítva.

43. Rendszer adatok biztonságos kommunikációjára egy készülék és egy biztonsági modul között, ***azzal jellemezve***, hogy egy véletlenszámot, valamint a készüléknek a biztonsági modul (64) nyilvános kulcsával kódolt azonosítóját a biztonsági modulhoz (64) elküldő készüléke van, továbbá a biztonsági modulnak (64) a véletlenszámot és a készülék azonosítót a biztonsági modul (64) privát kulcsának felhasználásával dekódoló eszköze van, valamint a készüléket a készülék azonosító felhasználásával érvényesítő készüléke van, valamint a véletlenszámot a biztonsági modul (64) és a készülék között továbbított adatok kódolásához és dekódolásához felhasználó eszköze van.

44. Biztonsági modul, ***azzal jellemezve***, hogy egy véletlenszám és a biztonsági modul (64) nyilvános kulcsával kódolt készülék azonosító vételére, a véletlenszám és a készülék azonosító biztonsági modul privát kulcsának felhasználásával történő dekódolására, a készüléknek a készülék azonosító használatával történő érvényesítésére, és érvényes készülék esetén a véletlenszámnak a biztonsági modul (64) és a készülék között továbbított adatok kódolásához és dekódolásához történő felhasználására alkalmasan van kialakítva.

45. Berendezés digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy készülékeket, valamint egy véletlen eseménykulcsot előállító eszközt, valamint a véletlen kulcsot a készülékekhez továbbító eszközzel rendelkező biztonsági modult (64) tartalmaz, ahol minden egyes készülék a készülékek között továbbított adatok

véletlen kulcs felhasználásával történő kódolására alkalmasan van kiképezve.

46. Biztonsági modul digitális adatok készülékek közötti biztonságos kommunikációjára, ***azzal jellemezve***, hogy a készülékek között továbbított adatok kódolására egy véletlen kulcsot (SK) előállító, valamint a véletlen kulcsot (SK) a készülékekhez továbbító módon van kiképezve.

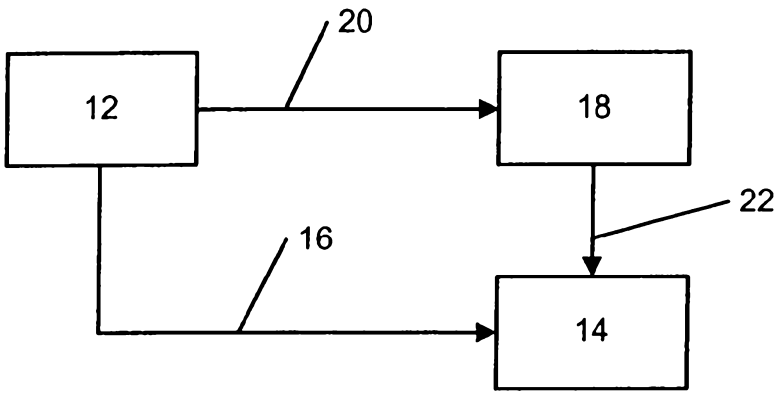
Budapest, Malom

A meghatalmazott:

DANUBIA

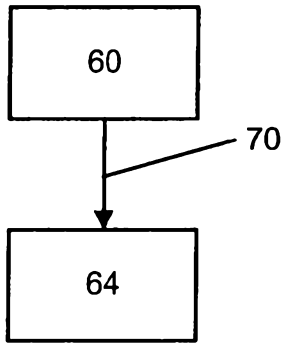
Szabadalmi és Védjegy Iroda Kft.

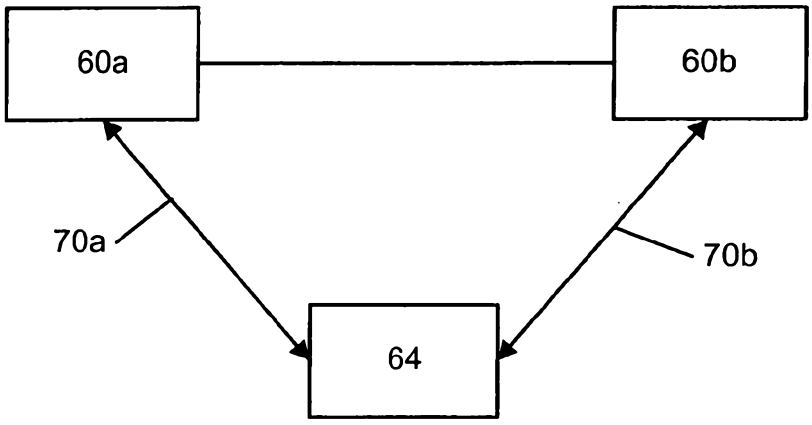
Dr. Antalffy-Zsíros András



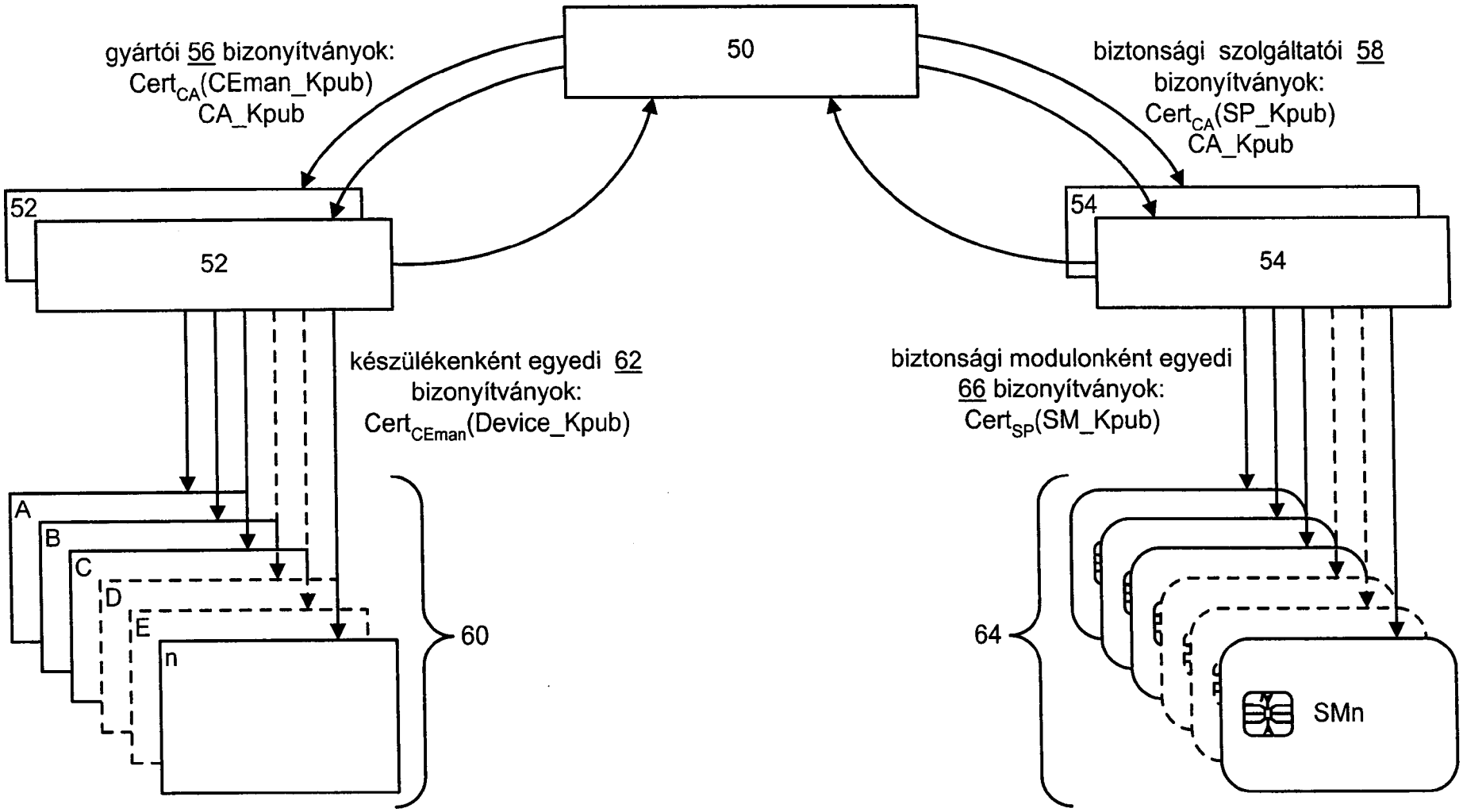
1. ÁBRA

3. ÁBRA



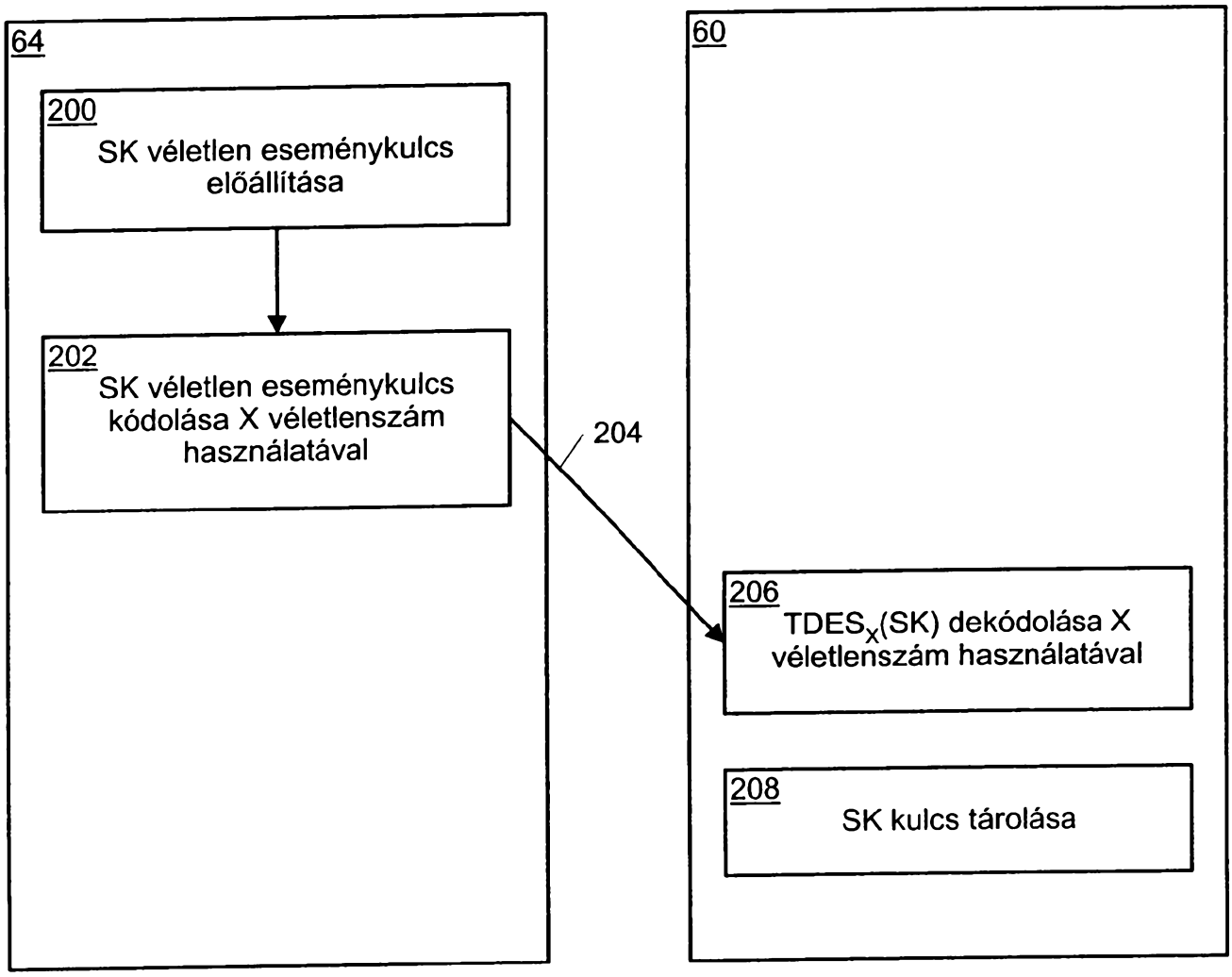


4. ÁBRA

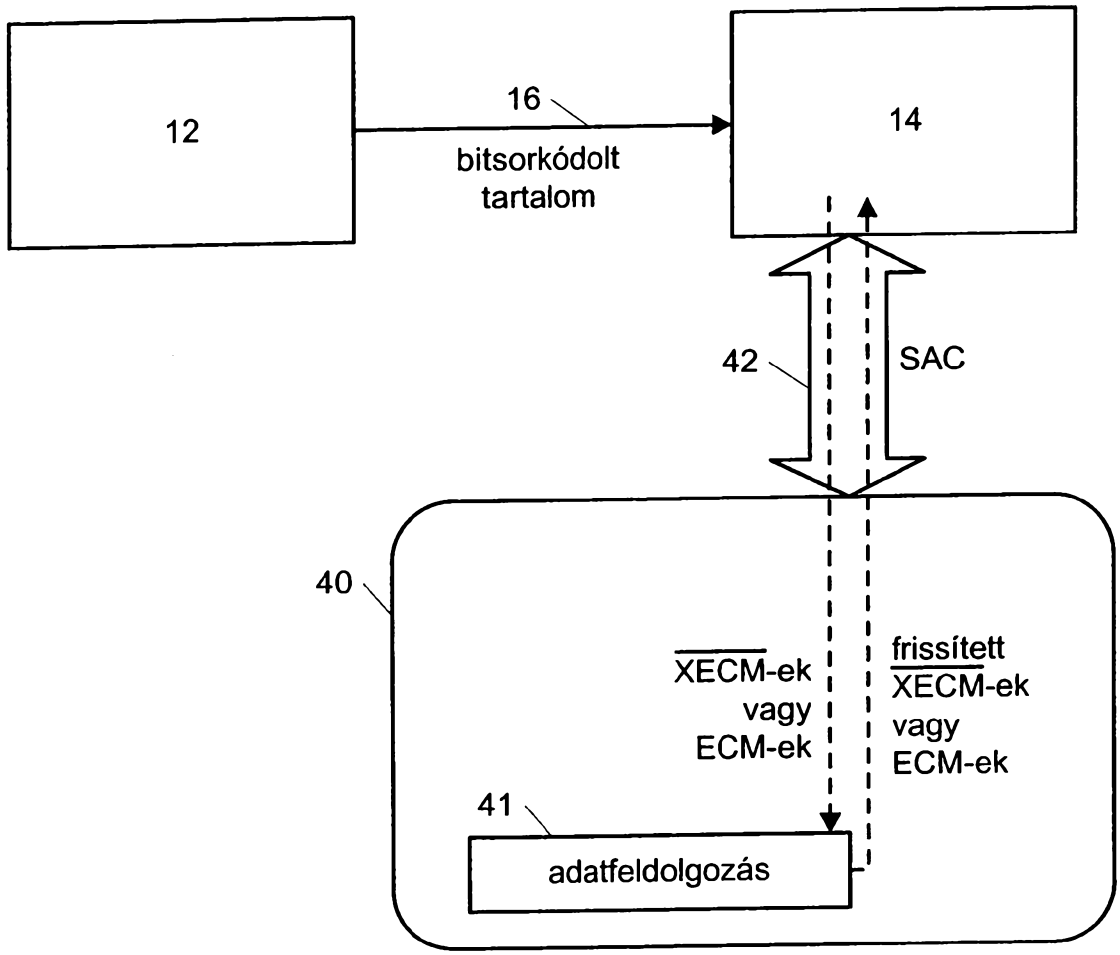


2. ÁBRA

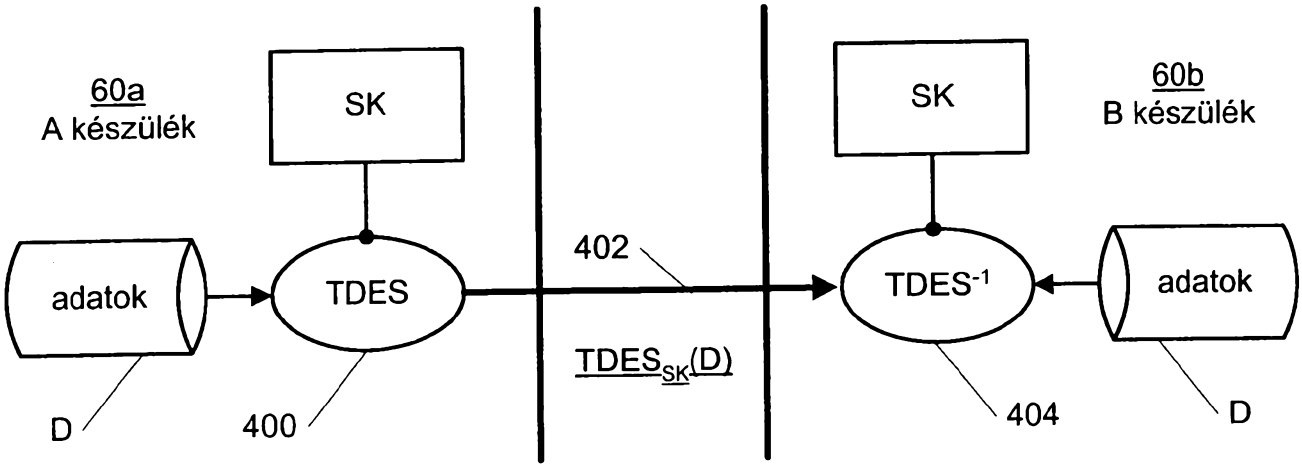
6. ÁBRA


64
200
SK véletlen eseménykulcs előállítása
202
SK véletlen eseménykulcs kódolása X véletlenszám használatával
204
60
206
TDES$_X$(SK) dekódolása X véletlenszám használatával
208
SK kulcs tárolása

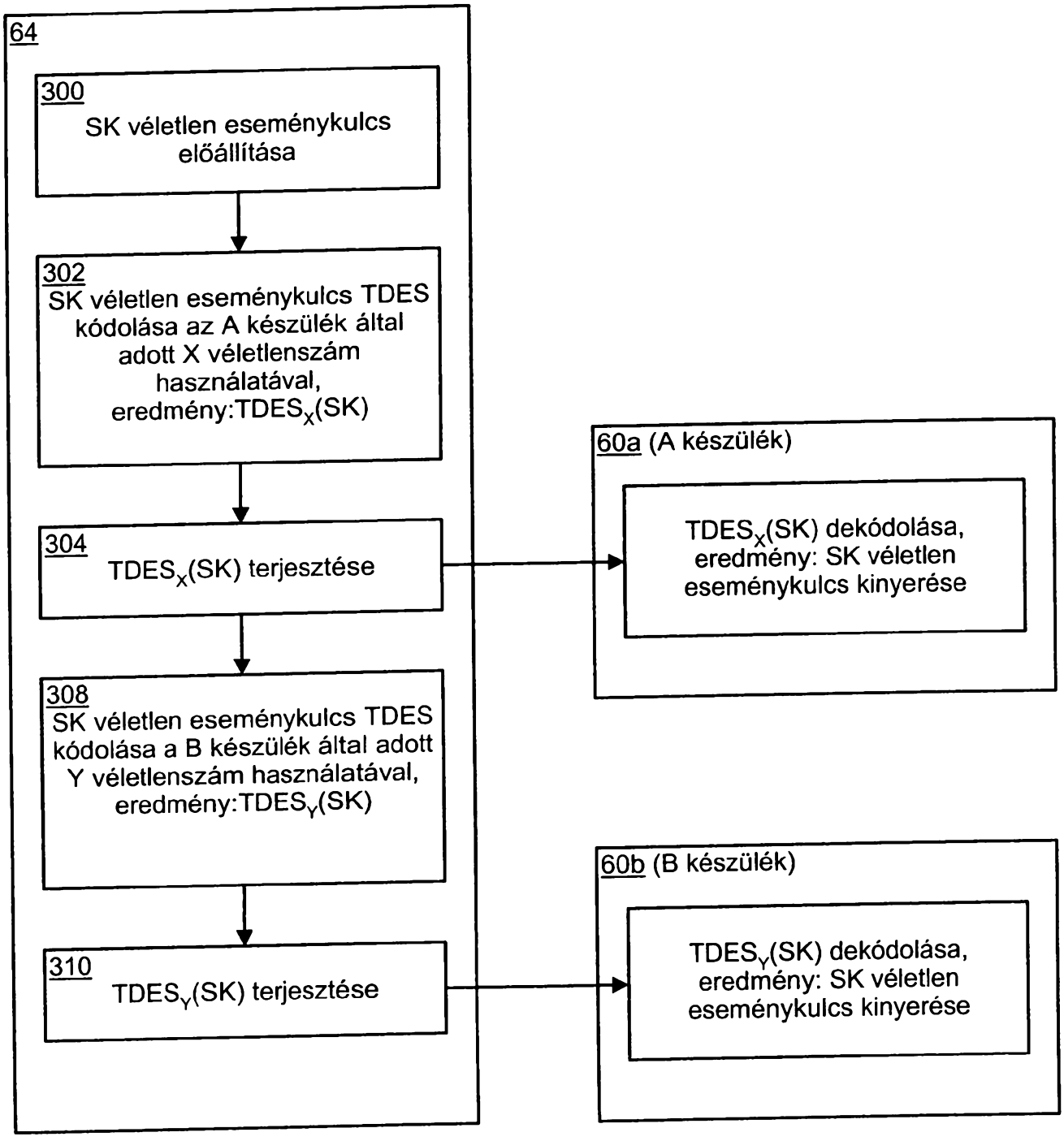
7. ÁBRA

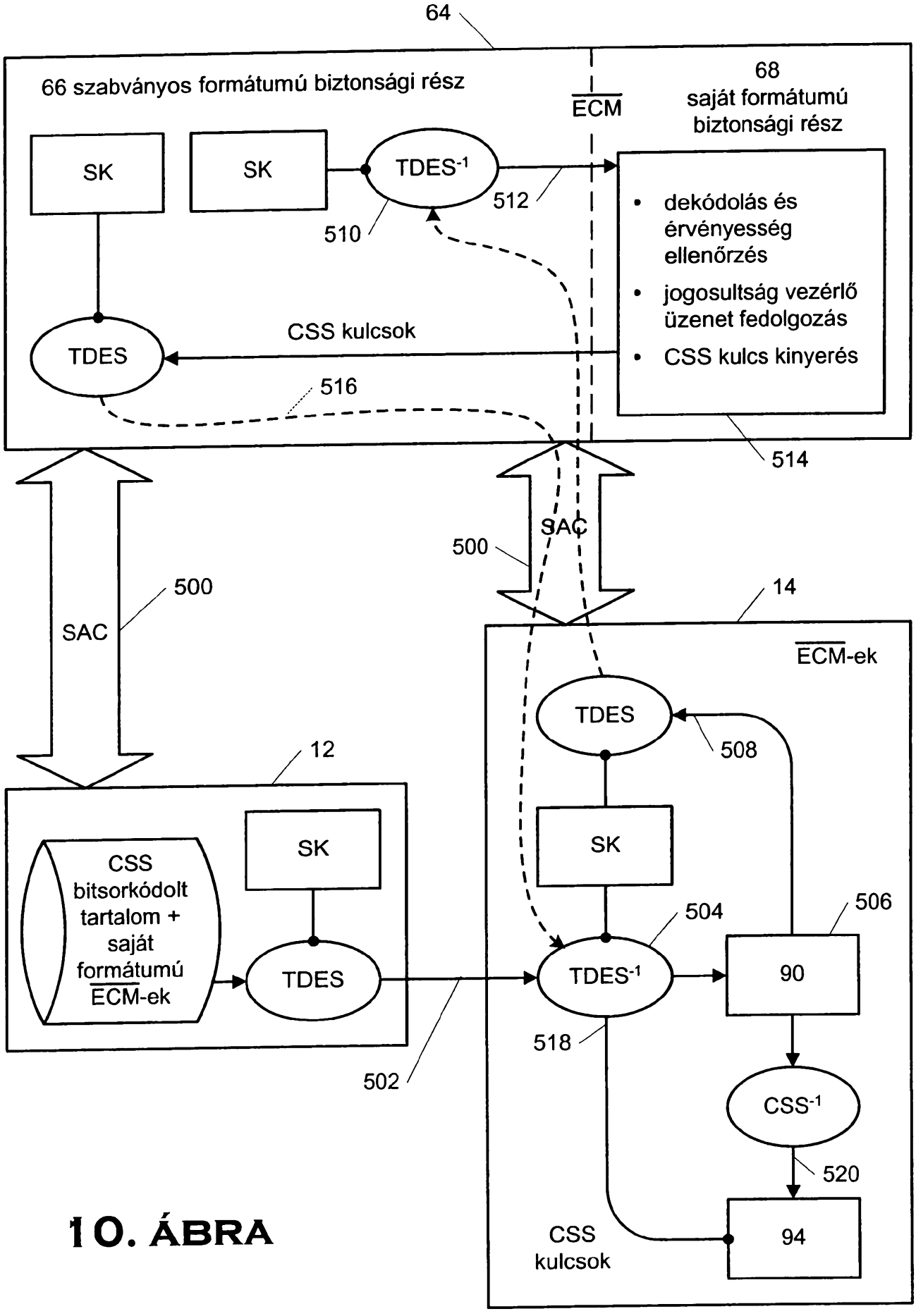

12
16
bitsorkódolt tartalom
14
42
SAC
40
XECM-ek vagy ECM-ek
frissített XECM-ek vagy ECM-ek
41
adatfeldolgozás

9. ÁBRA

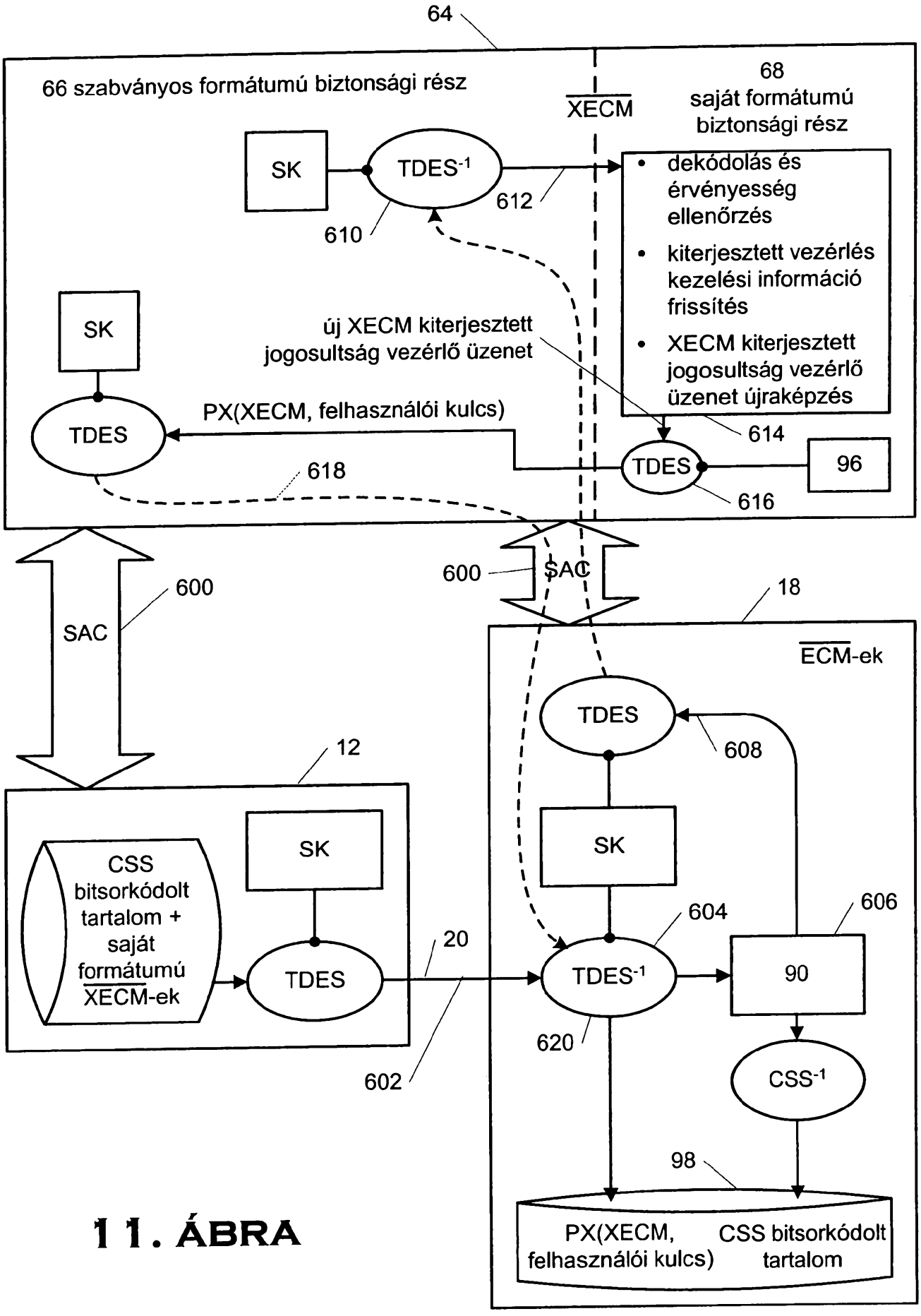

60a
A készülék
SK
SK
60b
B készülék
adatok
TDES
402
TDES-1
adatok
TDESSK(D)
D
400
404
D

8. ÁBRA


64
300
SK véletlen eseménykulcs előállítása
302
SK véletlen eseménykulcs TDES kódolása az A készülék által adott X véletlenszám használatával, eredmény:TDES$_X$(SK)
304
TDES$_X$(SK) terjesztése
308
SK véletlen eseménykulcs TDES kódolása a B készülék által adott Y véletlenszám használatával, eredmény:TDES$_Y$(SK)
310
TDES$_Y$(SK) terjesztése
60a (A készülék)
TDES$_X$(SK) dekódolása, eredmény: SK véletlen eseménykulcs kinyerése
60b (B készülék)
TDES$_Y$(SK) dekódolása, eredmény: SK véletlen eseménykulcs kinyerése


64
66 szabványos formátumú biztonsági rész
ECM
68
saját formátumú
biztonsági rész
SK
SK
TDES-1
512
510
• dekódolás és érvényesség ellenőrzés
• jogosultság vezérlő üzenet fedolgozás
• CSS kulcs kinyerés
TDES
CSS kulcsok
516
514
SAC
500
500
SAC
14
ECM-ek
TDES
508
12
SK
CSS bitsorkódolt tartalom + saját formátumú ECM-ek
TDES
SK
504
506
TDES-1
90
518
502
CSS-1
520
CSS kulcsok
94

10. ÁBRA


64
66 szabványos formátumú biztonsági rész
XECM
68
saját formátumú biztonsági rész
SK
TDES-1
612
610
• dekódolás és érvényesség ellenőrzés
• kiterjesztett vezérlés kezelési információ frissítés
• XECM kiterjesztett jogosultság vezérlő üzenet újraképzés
SK
új XECM kiterjesztett jogosultság vezérlő üzenet
PX(XECM, felhasználói kulcs)
TDES
614
TDES
96
618
616
600
SAC
600
SAC
18
ECM-ek
TDES
608
12
SK
CSS bitsorkódolt tartalom + saját formátumú XECM-ek
SK
604
606
20
TDES
TDES-1
90
620
CSS-1
602
98
PX(XECM, felhasználói kulcs)
CSS bitsorkódolt tartalom

11. ÁBRA