

~~74.362/BT~~
~~PCT/US00/23817~~

KÖZZÉTÉTELI PÉLDÁNY

KIVONAT

Eljárás és berendezés elektronikus tranzakciók lebonyolítására

A találmány tárgya eljárás tranzakció lebonyolításához, amely eljárás során a szerver-nél fogadjuk a felhasználótól érkező tranzakció kérést, lekérdezést bocsátunk ki a felhasználónak, a felhasználó lekérdezés alapján adott válaszát fogadjuk, a felhasználó azonosításához feldolgozzuk a választ, megbízólevelet állítunk össze a tranzakcióhoz, amely megbízólevélnek legalább egy kulcsa van, a megbízólevél legalább egy részét a felhasználó rendelkezésére bocsátjuk, második kérést fogadunk a felhasználótól, amely második kérés tartalmazza a megbízólevél egy részét, és a megbízólevél egy részét a kulccsal érvényesítjük a tranzakciós szolgáltatás eléréséhez.

A találmány tárgya számítógépen implementált eljárás hálózati szerver hálózati kliens ellen indított támadás alapjaként történő használatától való védelméhez.

A találmány tárgya tranzakciós rendszer, mely lehetővé teszi az adathálózaton működő felhasználói számítógép által igényelt pénzügyi tranzakciót.

A találmány tárgya digitális pénztárca kliens elektronikus tranzakciók böngésző programmal egyesített digitális hálózaton keresztüli biztosításához, amely digitális pénztárca kliens rendelkezik pénztárca alkalmazással és csatlakozó egységgel az olvasó eszközhöz.

A találmány tárgya pénztárca szerver digitális hálózaton keresztül történő tranzakció biztosításához, amely pénztárca szerver rendelkezik digitális hálózathoz kapcsolódó csatlakozó egységgel és adatbázissal kapcsolatban álló pénztárca szerver alkalmazással.

A találmány tárgya számítógépen implementált eljárás online vásárlás biztosításához, amely eljárás az alábbi lépéseket tartalmazza: azonosítunk a biztonsági szerverrel, fogadjuk a megbízólevelet a biztonsági szervertől, azonosítjuk a kereskedői címet, ahonnan a vásárlást le kell bonyolítani, biztosítjuk a megbízólevelet a pénztárca szerver részére a felhasználó pénztárca szervernél történő azonosításához, a pénztárca szervernél történő sikeres azonosítás után a kereskedő címe és a pénztárca szerver közötti kommunikációt átirányítjuk úgy, hogy a pénztárca szerver a kereskedői címnek vásárlási információt biztosítson a felhasználóról, és fogadjuk a vásárlás eredményének visszajelzését.

A találmány tárgya számítógépen implementált eljárás szolgáltatás elérésének biztosításához, amely eljárás az alábbi lépéseket tartalmazza: fogadjuk a bejelentkezési igényt a felhasználótól, ellenőrizzük, hogy a felhasználó rendelkezik-e tokennel, sikeres azonosítás esetén megbízólevelet biztosítunk a felhasználó részére, fogadjuk a tranzakció igényt a felhasználótól, amely tranzakció igény rendelkezik a megbízólevél legalább egy részével, és feldolgozzuk a megbízólevél legalább egy részét a szolgáltatás elérésének biztosításához.

Jellemző ábra: 1A. ábra

P0202471
1756

KÖZZÉTÉTELI PÉLDÁNY

A_1

elválasztott számsorozat formátumnak (például "0000 0000 0000 0000") felelnek meg. Az első öt-hét számjegy a feldolgozási folyamatok számára és a kibocsátó bank, kártyatípus, stb. azonosítására van fenntartva. Az utolsó számjegy a tizenhat számjegyű szám ellenőrző összegeként szolgál. A közbenső nyolc-tíz számjegy a vásárló egyedi azonosításához szükséges. A kereskedő ezután feldolgozza a fizetői kártyaszámot, például a kártya kibocsátója általi közvetlen azonosítása alapján, majd befejezi a tranzakciót. Az SSL szabvány leírása elolvasható például az 1996. november 18-án kelt "The SSL Protocol Version 3.0"-ban, mely a <http://home.netscape.com/eng/ssl3/draft302.txt> címen online elérhető, és amelynek tartalmára a későbbiekben hivatkozni is fogunk.

Habár az Interneten tranzakciók milliói zajlanak naponta, a hagyományos SSL tranzakciók gyakran szembetűnő hátránnyal rendelkeznek. Annak ellenére, hogy az SSL jellemzően biztonságos pont-pont (end-to-end) kapcsolatot biztosít, amely megakadályozza, hogy rosszindulatú harmadik személyek lehallgassák (például "kiszimatolják") vagy más úton megszerezzék a vásárló fizető kártyájának számát, a protokoll semmilyen módon nem biztosít ellenőrzést arra vonatkozóan, hogy a fizetőkártya maga érvényes-e, illetve, hogy a kártyaszámot használó személy jogosan teszi-e azt. Az internetes tranzakcióknál sűrűn előforduló csalások miatt a legtöbb fizetőkártya kibocsátó "kártya nincs jelen" tranzakciónak tekinti a hálózati tranzakciókat, és így magasabb kezelési költséget számol fel. Másképpen fogalmazva, a "kártya nincs jelen" tranzakciók magasabb rizikófaktorai miatt a legtöbb kártya kibocsátó magasabb költséget számít fel a kereskedőnek, ha az a kártyát elektronikus úton fogadja el, mintha a kártya a kereskedőnél a maga fizikai valóságában kerülne bemutatásra.

A fizetőkártyák számának nem biztonságos hálózaton keresztüli továbbításával járó biztonsági hibák elkerülésére sokan "intelligens kártyák" használatát ajánlják. Az intelligens kártyák tipikusan integrált áramköri chipet tartalmaznak, amelynek van mikroprocesszora és memóriája a kártyán való közvetlen adattároláshoz. Az adat megfelelhet például egy kriptográfiai kulcsnak, vagy elektronikus pénztárcának, amely a fizetőeszköz elektronikus értékét tartja nyilván. Sok intelligens kártya sémát ajánlottak már korábban e téren, de ezekre tipikusan jellemző az a hátrány, hogy nem szabványosak. Más szavakkal, a kereskedőknek jellemzően új, speciális szoftvert kell beszerez-



niük Web-áruházaihoz az intelligens kártyás tranzakciók elfogadásához. Mi több, a kártyákhoz tartozó kriptográfiai információ kiosztásának és karbantartásának adminisztrációs költsége a mai napig rendkívül magas.

A biztonságos elektronikus tranzakció (Secure Electronic Transaction, SET) szabvány a célból jött létre, hogy különböző kriptográfiai módszerek segítségével biztonságosabbá tegye az internetes tranzakciókat. Bár a SET valóban biztonságosabb SSL-en keresztüli tranzakciókat biztosít, a tranzakciók lebonyolításához szükséges különböző nyilvános és titkos kulcsok adminisztrálása korlátozta a SET széles körű elterjedését. A SET speciális szoftvert is igényel azoknál a kereskedőknél, akik a SET tranzakciókat is támogatnák.

Létező digitális pénztárca technológia, mint például a GlobeSet Inc. (1250 Capital of Texas Highway South, 1.épület, 300. szám, Austin, TX 78746) által nyújtott digitális pénztárca technológia, olyan eszközt biztosít a vásárló részére, amellyel tranzakciós kártya termékeket (például hitel-, fizető-, vagy bankkártyákat, számlaszámokat, és hasonlókat) használhatnak termékek és szolgáltatások online kifizetésére. Általánosságban a digitális pénztárcák olyan eszközök, amelyek az elektronikus kereskedelemben vagy más hálózati interakció elősegítéséhez személyes információt (név, cím, fizetőkártya szám, hitelkártya szám, stb.) tárolnak. A személyes információ tárolható az általános szerveren gépen vagy a kliensen (számítógép vagy intelligens kártya), illetve az általános szerver és a kliens gép kombinációján. A digitális pénztárca általános szervere egy webszerverből és egy olyan adatbázis szerverből áll, amely nyilvántartja a vásárló személyes és hitelkártya információit, vásárlási szokásait és az online kereskedők profilját.

A digitális pénztárca ideális esetben olyan funkciókat szolgáltat, mint például az egyszerű bejelentkezés/egy jelszó, automatikus rendelési űrlapkitöltés, egy vagy két kattintással való vásárlás, honlapok személyes arculatának kialakítása, online rendelés és szállítás státusz követés, tételes elektronikus nyugták, és testreszabott ajánlatok és akciók a költségek sémák és döntések alapján. Az egy kattintással való vásárlás egyidőben aktiválja a pénztárcát és visszaigazolja a vásárlást. Két kattintás esetén az első kattintás aktiválja a pénztárcát és a második kattintás visszaigazolja a vásárlást.



Használat közben a pénztárca könyvjelzőjére kattint a vásárló, amely egy SSL viszonyt hoz létre a pénztárca szerverrel. A böngésző kiegészítő programja végrehajtódik és a vásárló az azonosításhoz megad egy azonosítót/jelszót vagy intelligens kártyát, így hozzáfér a pénztárca adatokhoz. Online kereskedőnél történő vásárlásnál a megfelelő pénztárca adat a pénztárca szerverből kerül a kereskedő webszerveréhez.

A fentiek miatt kívánatos egy új elektronikus tranzakció lebonyolító rendszer. Egy ilyen rendszer nagyobb biztonságot kellene, hogy nyújtson anélkül, hogy az kereskedők és vásárlók felé további költséget jelentene. Továbbá, egy ilyen új rendszernek különböző internetes pénztárcákkal és különböző szállítók szolgáltatásaival is együtt kellene működnie.

A találmány demonstratív jellegű kivitelezéseiben a felhasználó intelligens tokenel, például intelligens kártyával rendelkezik, amely elektronikus tranzakciók lebonyolítására használható. Az intelligens token tartalmaz egy digitális okmányt és megfelelően hitelesítődik a felhasználó részéről történő tranzakciót vagy annak egy részét lebonyolító hálózaton levő szerver által. A felhasználó egy vásárló, aki vásárlási tranzakciót bonyolít le, és a szerver egy pénztárca szerver, amely a biztonsági szerverrel együttműködve nagyobb megbízhatóságot biztosít.

Az elektronikus tranzakciókat, például vásárlási tranzakciókat, a következő módon bonyolítjuk le: fogadjuk a felhasználótól érkező tranzakció igényt a szervernél, lekérdezést bocsátunk ki a felhasználó felé, a felhasználó lekérdezés alapján történő választát fogadjuk, a választ feldolgozzuk a tranzakciós okmány ellenőrzéséhez, megbízólevelet állítunk össze, amely az elektronikus tranzakcióhoz tartalmaz legalább egy kulcsot, a megbízólevés legalább egy részét a felhasználónak elküldjük, fogadjuk a második felhasználói igényt, amely tartalmazza a megbízólevél egy részét, és a meghatalmazás egy részét kulccsal hitelesítjük a tranzakciós szolgáltatás elérés biztosításához.

Továbbá, a jelen találmány a következő módon támadás elleni védelemmel lát el egy hálózati szerver: korlátozzuk a hálózati szerverhez való hozzáférést a hálózati szerver egy részére legalább egy kiválasztott protokollra vonatkozóan, és a hálózati szerver egy

résében a kiválasztott protokollnak megfelelő speciális karaktereket figyeljük. A speciális karakterek eltávolíthatók vagy helyettesíthetők jóindulatú karakterekkel a célból, hogy csökkenjen a kiválasztott protokoll által felvetett biztonsági veszélyforrás. Ideális esetben a karakterek naplózhatók is a biztonsági napló vezetéséhez. A biztonsági napló felülvizsgálható annak eldöntéséhez, hogy bizonyos karakterek veszélyesek-e vagy nem. Adott esetben az igény visszautasítható.

A jelen találmány tartalmaz továbbá egy tranzakciós eszközt, például digitális pénztárcát vásárlási tranzakciók végrehajtásához, amely pénztárcának van aktivátora és eszközsora. Ideális esetben az eszközsor lehetővé teszi a felhasználó számára az aktivátor kis méretű letöltését, továbbá az eszközsor egy vagy több operációs rendszer vezérlést, például egy rendszer tálca ikont használ. A tranzakciós eszköz tartalmaz űrlap kitöltő összetevőt és automatikus emlékező összetevőt is a űrlapok automatikus, a felhasználó által korábban megadott adatok alapján történő kitöltéséhez.

A jelen találmány fent leírt és egyéb tulajdonságai, és felmutatott előnyei a következő, demonstratív jellegű kivitelezésekben szemmel láthatóakká válnak az ezután következő ábrák segítségével, ahol a hasonló hivatkozási jelek mindvégig azonos vagy hasonló részek azonos nézetére utalnak, és amelyben:

Az 1A-1C. ábrák egy példa jellegű tranzakciós rendszer különböző megvalósításainak blokkdiagramjai.

A 2. ábra egy példa jellegű vásárlói rendszer blokkdiagramja.

A 3. ábra egy példa jellegű biztonsági rendszer blokkdiagramja.

A 4. ábra egy példa jellegű pénztárca szerver blokkdiagramja.

Az 5-8. ábrák a jelen találmánynak megfelelően kialakított digitális pénztárca egy megvalósításának példa jellegű képernyő képe.

A 9. ábra a példa jellegű aktivátor alkalmazás példa folyamatának folyamatábrája.

A 10. ábra egy példa bejelentkezési üzenetsorozat szekvencia diagramja.

A 11. ábra egy példa vásárlási üzenetsorozat szekvencia diagramja.

A 12A. ábra egy, sok szkript nyelv (scripting language) használata esetén felmerülő potenciális biztonsági problémát illusztráló üzenetsorozat.



A 12B. ábra a pontos kommunikációs folyamat üzenetsorozat szekvencia diagramja, a 12A. ábrán mutatott biztonsági probléma nélkül.

A 13. ábra a nem kívánatos végrehajtható kód csökkentésére vagy kiküszöbölésére szolgáló folyamat példa jellegű folyamatábrája.

A jelen találmányt a következőkben funkcionális blokk részek és különféle feldolgozó lépések tekintetében ismertetjük. Belátható, hogy ezek a funkcionális blokkok akármekkora számú és bármilyen, a kijelölt funkció végrehajtására beállított hardver és/vagy szoftver összetevőkkel megvalósíthatók. Például a jelen találmány alkalmazhat különféle integrált áramkör (Integrated Circuit, IC) összetevőket, többek között memória elemeket, feldolgozó elemeket, logikai elemeket, keresőtáblákat, és más hasonlókat, melyek a legkülönbözőbb funkciókat valósíthatják meg egy vagy több mikroprocesszor vagy más vezérlő eszköz irányítása alatt. Hasonlóképpen, a jelen találmány szoftver elemei implementálhatók bármilyen programozási vagy kommunikáció vezérlő nyelven, például C, C++, Java, COBOL, assembler, PERL, vagy hasonló nyelveken, a különböző algoritmusokat bármilyen kombinációjú adatszerkezetekkel, objektumokkal, folyamatokkal, rutinokkal, vagy más programozási elemekkel implementálva. Továbbá fontos megjegyezni, hogy a jelen találmány az adatátvitelhez, jelzéshez, adatfeldolgozáshoz, hálózati vezérléshez és hasonlókhöz akármennyi hagyományos technikát alkalmazhat. Mi több, a találmány alkalmazható arra is, hogy észrevegye vagy megelőzze a kommunikáció vezérlő nyelvek, például JavaScript, VBScript vagy hasonló nyelvek használatából eredő biztonsági problémákat.

Belátható, hogy a találmány és annak legjobb oldalát az alábbiakban bemutatott és leírt különböző szemléltető implementációi csak illusztratív jellegűek, és semmilyen úton nem szándékozunk a találmány alkalmazhatósági körét korlátozni. Sőt, a rövideg kedvéért a hagyományos adathálózati működést, alkalmazásfejlesztést és a rendszerek (és rendszerek működésében résztvevő, különálló összetevők részeinek) más funkcionális szempontjait az alábbiakban nem ismertetjük részletesen. Azonkívül a különböző rajzok közötti összekötő vonal az ismertetésben csupán a különböző elemek közötti, példa jellegű funkcionális kapcsolatot és/vagy fizikai összeköttetést szándékozik jelenteni. Megjegyzendő, hogy az elektronikus tranzakciós rendszer gyakorlati megvalósításában



előfordulhatnak alternatív vagy kiegészítő funkcionális kapcsolatok vagy fizikai összeköttetések is.

A demonstratív megvalósítások ismertetésének egyszerűsítése végett, a találmányt gyakran az Interneten futó elektronikus kereskedelmi rendszerhez hozzátartozónak tekintjük. Látható azonban, hogy a jelen találmány sok más alkalmazása is megfogalmazható lenne. Például a rendszer alkalmazható lenne egy számítógépes rendszer felhasználóinak azonosítására, beléptető rendszer aktiválására, vagy más hasonló célra. Hasonlóképpen, a találmány bármilyen típusú személyi számítógépen, hálózati számítógépen, munkaállomáson, miniszámítógépen, nagyszámítógépen (mainframe), vagy más hasonló, olyan rendszeren is alkalmazható lenne, amelyen a Windows, Windows NT, Windows2000, Windows98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX vagy egyéb alkalmazási környezet valamelyik verziója fut. Azonkívül, habár a találmány az alábbiakban internet protokoll feletti átvitel protokoll (Transmission Control Protocol over Internet Protocol) segítségével kerül implementálásra, látható, hogy a találmány IPX (Internet Packet eXchange), Appletalk, IPv6 (Internet Protocol version 6), NetBios, OSI (Open System Interconnection), továbbá számos létező vagy jövőbeli protokoll alapján is implementálható.

Továbbá a vásárló és a kereskedő különböző személyeket, entitásokat vagy üzleteket, míg a bank más típusú kártyakibocsátó intézményeket, például hitelkártya cégeket, hűségkártya kibocsátókat vagy a pénzüzetekkel kapcsolatban álló harmadik fél kártyakibocsátókat is reprezentálhatja. A fizető hálózat tartalmazza a már meglévő magán-hálózatokat, amelyek jelenleg helyet adnak a hitelkártyás, bankkártyás és más típusú pénzügyi/bank típusú kártyás tranzakcióknak. A fizető hálózat zárt hálózat, mely a lehallgatás ellen biztonságosnak tekinthető, mint például az American Express(R), vagy a VisaNet(R) hálózata, illetve a Veriphone(R).

Továbbá, a tranzakcióban más résztvevők, például megállapodás közvetítő intézmények (intermediary settlement institution) is szerepet vállalhatnak, de ezek a résztvevők az ábrán nincsenek feltüntetve. Minden egyes résztvevő számítógépes rendszerrel rendelkezik a tranzakció megvalósításához. A vásárlónak személyi számítógépe, a keres-



kedőnek számítógépe/szervere van, míg a bank nagyszámítógéppel rendelkezik, bár bármelyik számítógép lehet mini-számítógép, számítógép szerver, számítógépek hálózata, laptop, notebook, kézisámítógép, és más hasonló is.

Az 1A. ábrát tekintve, a 100 tranzakciós rendszer a megfelelő módon tartalmaz a legalább egy 110 felhasználói számítógépet, 120 tranzakció ellenőrző számítógépet, 130 biztonsági szervert, és opcionális 140 tranzakciós eszköz szervert. Az alább ismertetett megvalósításokban a 100 tranzakciós rendszert elektronikus kereskedelemben használják vásárlási tranzakciók lebonyolítására. Részletesebben, a 110 felhasználói számítógép a vásárló vagy fogyasztó számítógépe, a 120 tranzakció ellenőrző számítógép a kereskedő számítógépe és a 140 tranzakciós eszköz szerver a digitális pénztárca szerver. Látható, hogy habár az alább ismertetett tranzakciós rendszer elektronikus kereskedelmi rendszer, a jelen találmány ugyanígy alkalmazható számos más elektronikus tranzakciós rendszer esetén is.

A különböző számítógép rendszerek és szerverek alkalmas módon a 102 adathálózaton keresztül vannak összekötve, amely bármilyen adathálózat lehet, például az Internet vagy más nyilvános adathálózat. Más megfelelő 102 adathálózat lehet például a nyilvános kapcsolt telefonhálózat (Public Switched Telephone Network, PSTN), vállalati vagy egyetemi belső hálózat (intranet), és más hasonló. A különböző megvalósításokban, mint például amilyen az 1B. ábrán látható, a 120 kereskedői számítógép a 102 adathálózattól elkülönített, 152 adatkapcsolaton keresztül elektronikusan összeköttetésben áll a 130 biztonsági szerverrel. Hasonlóképpen a különféle megvalósítások tartalmazzák a 102 adathálózattól elkülönített 150 kapcsolatot a 140 pénztárca szerver és a 130 biztonsági szerver közötti összeköttetés biztosításához. A 150 és 152 kapcsolatoknak megfelelő adatkapcsolatok lehetnek például telefonos kapcsolatok, integrált szolgáltatást nyújtó digitális hálózati (Integrated Services Digital Network, ISDN) kapcsolatok, dedikált nagysebességű bérelt vonalak (T1) vagy más adatkapcsolatok, vezeték nélküli kapcsolatok, és más hasonló. Látható, hogy a 150 és 152 kapcsolatok azonos kapcsolatok is lehetnek, illetve mindkét kapcsolat a találmány megvalósításaitól teljesen eltérő is lehet.



A különféle megvalósítások, mint például az 1C. ábrán látható megvalósítás, tartalmazhatnak 160 alkalmazás szervert is. A különféle megvalósításokban az (ábrán nem látható) adatbázisok és/vagy a (képen nem feltüntetett) profil szerverek összeköthetők a 160 alkalmazás szerverrel és/vagy a 140 pénztárca szerverrel. A 160 alkalmazás szerver a terhelés kiegyensúlyozására használható. A terhelés megosztása a 140 pénztárca szerver és a 160 alkalmazás szerver között növelheti a hatékonyságot és/vagy a biztonságot. Például a 160 alkalmazás szerver felvállalhatja a 140 pénztárca szerver néhány olyan funkciójának teljesítését, mint például az adatbázis elérés. Mivel a 160 alkalmazás szerver nincs összekötve a 102 adathálózattal, a biztonság növelhető azzal, ha az adatbázis elérés a 160 alkalmazás szerver felelőssége, nem a 140 pénztárca szerveré.

Míg az 1A-1C. ábrák különféle megvalósításokat illusztrálnak, belátható, hogy más megvalósítások is elképzelhetők. Például egy megvalósítás tartalmazhatja a 150, de nem a 152 kapcsolatot, vagy fordítva. Továbbá az összetevők (például a 110 vásárló, a 120 kereskedő, a 130 biztonsági szerver, a 140 pénztárca szerver, és a 160 alkalmazás szerver) az alábbiakban leírásra kerülő funkciók elérése érdekében lehetnek mind külön számítógépek vagy alkothatják hasonló céllal működő számítógépek hálózatát. Az egyes összetevőkhöz rendelt funkciók eloszthatók egy vagy több különálló számítógép között a meghatározott funkciók teljesítéséhez. Például a 140 pénztárca szerver adott esetben lehet webszerverek, alkalmazás szerverek, adatbázis szerverek, és más típusú szerverek egy csoportja is.

Egy tranzakció lebonyolításához a 110 vásárló a megfelelő módon a 102 adathálózaton keresztül létrehozza a kapcsolatot a 120 kereskedővel. Mikor a vásárlás során fizetésre kerül sor, a 110 vásárló hozzáférést kezdeményez a 140 pénztárca szerverhez. A 110 vásárlót ezután átirányítják a 130 biztonsági szerverhez, annak igazolására, hogy az intelligens kártya a vásárló tulajdonában van-e. Az intelligens kártya tartalmazhat digitális okmányt, amely egyértelműen azonosítja a kártyát úgy, hogy az alább leírt módon létre lehessen hozni egy, a tranzakcióhoz kapcsolódó megbízólevelet. A különféle megvalósításokban a digitális megbízólevél egy részét a 110 vásárlóhoz küldik vissza, másik részét a biztonságos 150 kapcsolaton keresztül a 140 pénztárca szerverhez to-



vábbítják. A 110 vásárló ezután ezt a digitális megbízólevelet használhatja a 140 pénztárca szervernél történő azonosításhoz, majd a pénztárca szerver a vásárló számára kiszolgálóként működhet az elektronikus tranzakció befejezéséhez. A 140 pénztárca szerver például tartalmazhat olyan funkciót is, mellyel kitölthetők a 120 kereskedő számítógépével fémjelzett űrlapok. Mikor a 120 kereskedő a 110 vásárlótól vagy a 140 pénztárca szervertől biztonságos vásárlói eszköz azonosítót kap, a 152 kapcsolaton keresztül a szokásos fizetőkártya azonosítási módjának megfelelően megtörténhet a kártya azonosítása. Ahogyan az a fentiekben kifejtettük, a kommunikációt különböző protokollokkal, például SSL vagy látszólagos magánhálózat (Virtual Private Network, VPN) protokollal, vagy más hasonlóval is végre lehet hajtani. Mivel az intelligens kártya olyan azonosító információt tartalmaz, amely a kártyára vonatkozóan egyedi és amely a hálózat számára elektronikus úton ismertté tehető, az intelligens kártyával lebonyolított vásárlási tranzakció biztonságosabb, mint a szokásos fizető kártyával vagy hitelkártyával történő fizetés. A biztonságos tranzakció, amely a kártya kibocsátója szempontjából "kártya jelen" tranzakcióként dolgozható fel, alacsonyabb kezelési költséggel is honorálható. Továbbá, ha a tranzakció "kártya jelen" tranzakció, a csalás kockázata átadható a kereskedőtől a kártya kibocsátója felé.

A 2. ábrára áttérve, a példa jellegű 110 vásárlói számítógép (hivatkozásban kliens, vásárló, vagy felhasználói számítógép is előfordul) bármilyen számítógép rendszer lehet, amely a 102 adathálózaton keresztül képes elindítani egy elektronikus vásárlási tranzakciót. A különféle megvalósításokban a 110 vásárlói számítógép egy személyi számítógép, amely olyan 212 operációs rendszert futtat, mint például a Microsoft Corporation (Redmond, Washington) Windows operációs rendszerének bármelyik verziója, vagy az Apple Corporation (Cupertino, California) MacOS rendszerének valamelyik verziója.

A 110 vásárlói számítógép megfelelő módon tartalmaz hardvert és/vagy szoftvert a 202 intelligens kártya és a 216 web böngésző között a 212 operációs rendszeren keresztüli kapcsolódási pont létrehozásához. A 216 web böngésző akármilyen, a 110 vásárlói számítógéppel kompatibilis program lehet, amely a a 102 adathálózaton keresztül kommunikál, például a Netscape Corporation (Mountain View, California) Netscape



Communicator programja, a Microsoft Corporation (Redmond, Washington) Internet Explorere, vagy az America Online Corporation (Dulles, Virginia) AOL böngészője. A különböző megvalósításokban a 110 vásárlói számítógép tartalmaz 214 pénztárca kliens, amely bármilyen, a 140 pénztárca szerverrel történő kommunikációhoz beállított program lehet. Ilyen 214 pénztárca kliens például a Microsoft Wallet vagy a Globeset Corporation (Austin, Texas) Globeset Wallet nevű programja, azonban más pénztárca programok is használhatók.

A 214 pénztárca kliens és a 216 web böngésző a 202 intelligens kártyával úgy működik együtt, hogy a 212 operációs rendszeren keresztül adatot küld a 204 kártya olvasónak. A 204 kártya olvasó bármilyen olvasó eszköz lehet, amely képes információt továbbítani a 214 pénztárca kliens és a 202 intelligens kártya között. A különféle megvalósításokban a 204 kártya olvasó ISO-7816 kompatibilis olvasó, mint például a Gempius Corporation (Redwood City, California) GCR410 olvasója, vagy más megfelelő olvasó eszköz.

A 202 intelligens kártya bármilyen kártya lehet, amely képes elektronikus tranzakciók lebonyolítására, például bármilyen kártya, amely kompatibilis a következő ISO szabványokkal, melyeket az alábbiakban az egészükre történő hivatkozási alapként használni fogunk:

ISO/IEC 7816-1:1998 Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 1. rész: Fizikai jellemzők;

ISO/IEC 7816-2:1999 Informatika - Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 2. rész: Érintkezők méretezése és elhelyezése;

ISO/IEC 7816-3:1997 Informatika - Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 3. rész: Elektronikus jelek és átviteli protokollok;

ISO/IEC 7816-4:1995 Informatika - Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 4. rész: Átkapcsoláshoz szükséges iparközi utasítások;

ISO/IEC 7816-5:1994 Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 5. rész: Számozási rendszer és regisztrációs eljárás alkalmazási azonosítókhoz;

ISO/IEC 7816-6:1996 Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 6. rész: Iparközi adatelemek; és

ISO/IEC 7816-7:1999 Azonosító kártyák - Integrált áramköri kártyák érintkezőkkel - 7. rész: Iparközi utasítások strukturált kártyalekérdező nyelv (Structured Card Query Language, SCQL) használatához.

Egy, az ISO 7816 specifikációinak megfelelő 202 intelligens kártya többek között lehet például az Infineon Corporation (München, Németország) SLE66 típusú chipje. Az SLE66 chip tartalmaz memóriát (például 16k memóriát, habár több vagy kevesebb is megfelelő lehet) és egy Multos operációs rendszeren (például Multos v.4 rendszeren) futó processzort. A különböző megvalósításokban a 202 intelligens kártya tartalmaz továbbá egy kisalkalmazást (applet) a digitális okmányok feldolgozására és tárolására vagy más kriptográfiai funkció ellátására. A kriptográfia alapjainak megismeréséhez ajánljuk Bruce Schneier "Applied Cryptography: Protocols, Algorithms, And Source Code in C" című cikkét, melyet John Wiley és Fiai adtak ki (1996, második kiadás), és amelyet az alábbiakban hivatkozási alapként használunk. A 202 intelligens kártyán tárolható például egy X.509 Java kisalkalmazás a rajta tárolt X.509 digitális okmány feldolgozásához. Míg az alábbi megvalósítások intelligens kártyát használnak, látható, hogy a találmány más megvalósításaiban más intelligens token, például globális mobilkommunikációs rendszerű (Global System for Mobile Communication, GSM) mobiltelefon is helyettesítheti az intelligens kártyát.

A 3. ábrán a 130 biztonsági szerver megfelelő módon tartalmaz csatlakozó egységet (interface) a 102 adathálózat felé, 304 biztonsági motort, és a 310 adatbázissal kommunikáló 306 azonosítás szervert. A 302 hálózati csatlakozó egység bármilyen program, például web szerver lehet, amely lehetővé teszi a 102 adathálózaton való kommunikációt. Különféle megvalósításokban a 302 hálózati csatlakozó egység a Netscape Corporation (Mountain View, California) Netscape Enterprise Server programjára épül. A 302 hálózati csatlakozó egység a 102 adathálózaton elektronikus üzeneteket fogad és átirányítja azokat a 304 biztonsági motornak vagy a 306 azonosítás szervernek, mikor hogy célszerűbb.

A 304 biztonsági motor és a 306 azonosítási szerver elkülöníthető a 308 tűzfallal. A 308 tűzfal bármilyen hardver vagy szoftver vezérlő (például router hozzáférés vezérlő)



lehet, amely képes az adatfolyam korlátozására egy belső és egy külső hálózat között (az ábrán a tűzfal nem látható). Különféle megvalósításokban a 304 biztonsági motor a tűzfalon kívül van a 130 biztonsági szerver és a 110 vásárlói vagy 140 pénztárca szerver közötti adatforgalom adminisztrálásához. A 306 azonosítás szerver értékes és bizalmas információt, például a 310 adatbázist tart fent, amely tartalmazhat a különböző 202 intelligens kártyák X.509 digitális okmányai közötti, a 100 rendszerre vonatkozó kereszthivatkozást, emiatt célszerűen ajánlott belső hálózaton tartani a nagyobb biztonság érdekében. Látható, hogy a 304 biztonsági motor és a 306 azonosítás szerver funkcióinak halmaza tetszőlegesen, sokféleképpen kombinálható vagy szétválasztható anélkül, hogy a jelen találmány lényegétől eltérnénk.

A 4. ábrára történő hivatkozással, a példa 140 pénztárca szerver tartalmaz 402 hálózati csatlakozó egységet, 404 opcionális kisalkalmazás szervert, és 406 pénztárca alkalmazást. A 402 hálózati csatlakozó egység akármilyen program lehet, amely lehetővé teszi a 102 adathálózaton való kommunikációt, lehet például webszerver is. A különböző megvalósításokban a 402 hálózati csatlakozó egység a Netscape Corporation (Mountain View, California) Netscape Enterprise Server programján alapul. A 404 opcionális kisalkalmazás szerver elosztott programoknak, például Java programoknak vagy ActiveX vezérléseknek nyújt háttér szolgáltatást. Egy példa a kisalkalmazás szerverre a Sun Microsystems (Mountain View, California) Java Applet Server programja. A 404 kisalkalmazás szerver és a 402 hálózati csatlakozó egység támogatást nyújtanak a 406 pénztárca alkalmazás funkciói számára, amely pénztárca alkalmazás kezelheti a bejelentkezési funkciót, lekérdezheti a 408 pénztárca adatbázisból a pénztárca adatait, és/vagy adminisztrálhatja az alább ismertetett tranzakciókat. A találmány különböző megvalósításaiban a 140 pénztárca szerver tartalmazhatja a GlobeSet Corporation (Austin, Texas) SERVERWALLET (ismertebb nevén NETWALLET) programját.

A találmány bizonyos megvalósításai tartalmazhatnak aktivátor alkalmazást, amely a megfelelő módon segíti a vásárlókat a pénztárcával történő vásárlás során. Az aktivátor alkalmazás mutathat például állapot információt, vagy szükség esetén automatikusan elindítja a 214 pénztárca klienst (2. ábra). Továbbá, az aktivátor a pénztárca által támogatott oldalak gyorsítótárban (cache) történő karbantartását is végezheti.



Az aktivátor alkalmazás programja hagyományos számítógépes alkalmazásoknál megszokott módon implementálható. A különböző megvalósításokban az aktivátor alkalmazás az információt tálcás elrendezésű ikonokként, "lebegő bittérképes képeként (floating bitmap)", vagy bármely más megfelelő módon mutathatja. A grafikus megjelenítés (például ikonok) az állapot információt is jelezheti, mint például "támogatott oldal böngészése", "támogatott pénztár oldal böngészése", "támogatott fizetési oldal böngészése", "nincs nyitott böngésző ablak", "böngészés nem támogatott oldalon", és/vagy hasonló.

A lebegő bittérképes kép bármilyen grafikus fájlként vagy formátumban, például grafika csere formátumban (Graphics Interchange Format, GIF) implementálható. Más megvalósítások grafikus, audio-, vizuális, audiovizuális, multimédia, animált vagy más formátumban jelenítik meg az információt. Továbbá a GIF fájlok helyettesíthetők LZW (Lempel-Ziv-Welsh) fájlokkal, TIFF (Tagged Image File Format) fájlokkal, animált GIF fájlokkal, JPEG (Joint Photography Experts Group) fájlokkal, MPEG (Motion Pictures Experts Group) fájlokkal, vagy bármely más grafikus, audio, vagy multimédia formátumú fájlokkal.

Ideális esetben a jelen találmány kibővül egy ablakkal rendelkező tranzakciós eszköz biztosításával, amely olyan vezérlő eszközöket tartalmaz, melyekkel a felhasználó még könnyebben használhatja a tranzakciós eszközt. A tranzakciós eszköz különféle elektronikus tranzakciókhoz használható. Alkalmazható például vásárlási tranzakciókhoz, pénzügyi tanácsadás típusú tranzakciókhoz, biztosítási tranzakciókhoz, vásárló és vásárló közötti tranzakciókhoz (ilyen lehet például a barter tranzakció, ajánlatokhoz és jutalmakhoz kapcsolódó tranzakciók, stb.) is. Az itt részletesen ismertetett tranzakciós eszköz elektronikus vásárlási tranzakciókhoz használt digitális pénztárca. A digitális pénztárca kibővül egy ablak biztosításával, amely olyan vezérlő eszközöket tartalmaz, mellyel a felhasználó még könnyebben használhatja a pénztárcát. Ideális esetben a jelen találmány tartalmazza a digitális pénztárca funkció elérésének kliens oldali implementációját és a szerver oldali eszközsort, amely a felhasználó számára lehetővé teszi az aktivátor kis méretű letöltését és az operációs rendszer felhasználói interfész vezérlő elemeinek, például a Microsoft Windows egy tálca ikonjának használatát.



Az aktivátor tárgy kód, amely a felhasználó számítógépén fut és a pénztárca szerverhez való hozzáféréshez szükséges rutinokat tartalmazza. Az aktivátor létrehozhat eseményeket és eljárási logikát tartalmaz, amely a felhasználói és a rendszer műveletekre vagy eseményekre történő válaszadáshoz szükséges, pénztárca szerverrel való kommunikációt teszi lehetővé. Ideális esetben az aktivátor egyszerű grafikus elemet, például egy ikont mutat, ami a Microsoft Windows megvalósításban Windows tálcá ikonként jelenik meg, és ami lehetővé teszi a felhasználó számára, hogy beindítsa a pénztárca eszközsor megjelenítését. A különféle megvalósításokban a pénztárca eszközsor tulajdonképpen speciális böngésző ablak, mely hozzáfér a pénztárca szerverhez. Az aktivátor a pénztárca szerverrel kommunikál, hogy automatizálja az aktivátor tárgy kódjának egyszerű letöltéssel való frissítését. Ideális esetben az aktivátor letöltés előtt a felhasználói jóváhagyás is szükséges a folyamat elindulása előtt. A különböző megvalósításokban az aktivátor más alkalmazásokkal kommunikál, például akciós ajánlatokkal vagy jutalmakkal, mint a pénztárca,

A rendszer minden egyes oldalán biztosítja a fontosabb opciók tartalmát, mégpedig dinamikus és szövegfüggő információt, amely a felhasználó által megtekintett oldalra nézve egyedi. Ezt úgy lehet elérni, hogy az aktivátor figyeli az egységes erőforrás-meghatározókat (Uniform Resource Locator, URL) és esetleg rákucskolódik az oldalakra, hogy a felhasználó értesüljön a lehetséges előnyökről. Például az aktivátor ellenőrizheti, hogy a felhasználó egy kereskedő oldalát nézi, és megfelelő ajánlatokat (például bizonyos termékek akciós árait, stb.) jelenítheti meg a felhasználónak. Az aktivátor továbbá figyelheti a felhasználó rendszerének szoftver verzióit, és tájékoztatja a felhasználót a lehetséges szoftver frissítési lehetőségekről. Egy demonstratív jellegű megvalósításban a rendszer valamilyen hálózaton, például nagy kiterjedésű hálózaton (Wide Area Network, WAN), helyi hálózaton (Local Area Network, LAN), vagy az interneten, illetve valamilyen személyi számítógépen, vezeték nélküli elektronikus eszközön vagy más hasonló eszközön van implementálva. A rendszer operációs rendszeren, például Microsoft Windows, Mac OS, Linux, Windows CE, Palm OS, és más operációs rendszereken kerülhet implementálásra.

Az aktivátor, amely ideális esetben a kliens oldalon van implementálva, lehetővé teszi a 110 felhasználó számára, hogy állandó vagy szakaszos kommunikációt folytasson a 140 digitális pénztárca kibocsátóval, például az American Express-szel, anélkül, hogy tolakodó ablakok foglalnák el a helyet a képernyőn. Ahogyan azt a fentiekben ismertettük, ez lehetővé teszi a pénztárca kibocsátó számára, hogy figyelje és a megfelelő időben megjelenítse a felhasználó érdeklődési körébe esetleg beletartozó termékeket. Az ablakban megjelenített, testreszabható vezérlők megengedik a felhasználónak, hogy gyorsan navigáljon a kívánt web oldalak között és hogy azonnal előhozza a kívánt funkciónak megfelelő oldalt, például a digitális bevásárlókosárban levő termékek virtuális pénztárnál történő kifizetését. Ideális esetben a kliens eszközsor a felhasználó böngésző ablakához kapcsolódó különálló ablak lehet, amely mégis olyan pozíciót foglal el, amely hatékonyan teszi a a felhasználó böngésző ablakának részévé. Azonban, mikor a felhasználó az eszközsor vezérlőire kattint, az ablak az eredeti állapotában marad, vagyis az ablak a böngésző ablakot a kívánt URL címnek megfelelő oldalra irányítja és bizonyos műveleteket hajt végre (például használja a digitális pénztárcát). Például a tálcá ikonok közül a digitális pénztárca ikon kiválasztásával az 5. ábrán látható módon az 502 digitális pénztárca eszközsor jelenik meg az 500 böngésző ablakhoz kapcsolódó külön ablakban. Egy másik megvalósításban a kliens eszközsor a létező pénztárca ablakot keretezi a fent leírt módon, a már létező pénztárca által nyújtott ablak területének kiterjesztéseként további vezérlőket biztosítva. Egy másik lehetséges megvalósításban a felhasználó böngésző ablakának területe ketté van osztva egy olyan terület létrehozásához, amely a fent leírt pénztárcának és más vezérlőknek ad helyet.

A rendszer ideális esetben a felhasználó számára nem csak a kedvenc URL címek látogatását teszi kényelmes módon teszi lehetővé, hanem olyan funkciók elérését is biztosítja, amelyek amúgy sok (és a kereskedők folyamatos frissítése miatt állandóan változó) lépésen keresztül lennének csak elérhetők. A rendszer használata továbbá ideális esetben egyszerű, mivel nemcsak hogy könnyen használhatók a pénztárca és e-kereskedelmi oldalak, hanem könnyen meg is lehet találni a pénztárcát és a kliens eszközsort. Mikor a felhasználónak sok különböző ablaka áll nyitva, a pénztárca ablakot megtalálni bonyolult és bosszantó lehet, főleg mivel normális navigálás és az oldalakkal történő kölcsönhatások során a különböző böngésző ablakok elfoglalják a grafikus

felhasználói interfész (Graphical User Interface, GUI) középpontját. Így a tálca ikon és a szerveroldali funkciók együttes használata nagyobb felhasználói élményt biztosít. Egy ajánlott megvalósításban a jelen rendszer minden ismert böngészővel (mint például a Netscape Navigator) együttműködik.

Míg a korábbi hasonló rendszerek (például a MyAmericanExpress.com oldal) csak testreszabható portált biztosítanak, amely megengedi a felhasználó számára, hogy meglátogassa az oldalt és az onnan kiinduló linkeken elinduljon, a jelen találmány egy példa jellegű megvalósítása megfelelő módon vezérlőkkel rendelkező ablakot nyújt, amely a felhasználó képernyőjén marad míg az Interneten navigálnak. Továbbá a kliens eszközsor a felhasználó számára olyan műveletek automatizálását is lehetővé teszi, amelyek egy harmadik fél e-kereskedelmi oldalain kerülnek végrehajtásra. Mi több, míg a korábbi rendszerek külön böngésző ablakot használhatnak a pénztárca vezérlők biztosításához, a jelen találmány a szokásos böngésző ablakot használja, amely fel van osztva a pénztárca által elfoglalt hely biztosításához. Például egy ajánlott megvalósításban a digitális pénztárca ikon elérhető a tálca ikonok között (az ábrán nem látszik). A digitális pénztárca ikon előhívásakor a 6. ábrán látható módon az 502 digitális pénztárca eszközsor jelenik meg. A digitális pénztárca eszközsor nem tola-kodó, mégis tartalmazza mindazon vezérlőket, melyekkel a felhasználó hozzáférhet a digitális pénztárcához. Ideális esetben az 502 digitális pénztárca eszközsor az 500 böngésző ablakhoz kapcsolódik.

A 6. ábrán látható módon, ha a felhasználó az 502 digitális pénztárca eszközsor vásárlási katalógus gombját választja, az eszközsor 602 vásárlási katalógus oldallá változik. A felhasználó a 602 vásárlási katalógusban megjelenő 604 kereskedői listából kiválaszthat egy kereskedőt. A 604 kereskedői listából való kereskedő kiválasztása után a digitális pénztárca a kiválasztott 702 kereskedői oldalra irányítja a felhasználót, ahogyan az a 7. ábrán is látható. Ideális esetben, mikor a pénztárca a 702 kereskedő oldalra viszi a felhasználót, az 502 digitális pénztárca eszközsor visszaváltozik eredeti méretére.



Mikor a felhasználó vásárlást eszközöl a kereskedőnél, például termékek virtuális kosárba való helyezésével és a virtuális pénztárhoz való továbblépésével, a jelen találmány digitális pénztárcája által részben végrehajtódik a fizetési funkció. A 8. ábrán látható módon, mikor a felhasználó a 702 kereskedői oldalon jelzi a fizetési szándékát, a digitális pénztárca 802 virtuális pénztár interfésze jelenik meg. Például a 802 virtuális pénztár interfész a böngésző egyik oldalán jelenik meg, míg a 702 kereskedői oldal továbbra is látszik a böngésző ablak másik oldalán. A felhasználó által a virtuális pénztárnál normális esetben kitöltendő információ (például név, cím, e-mail cím, hitelkártya információ) nagy része már ismert a digitális pénztárca számára, így azok a digitális pénztárca 802 virtuális pénztár ablaknál automatikusan kitöltésre is kerülnek. Az ajánlott megvalósításban a felhasználó módosíthatja az előre kitöltött információt.

Ideális esetben a jelen rendszer tartalmaz eljárásokat és berendezést is a internetes oldalakon levő, megbízható HTML űrlapok számának növeléséhez. A végeredmény az, hogy a felhasználók meghatározhatják azon információt, melyet általános esetben a kereskedői oldalak tudomására szeretnének hozni, függetlenül a tényleges megjelenéstől, címkézéstől, és a különböző e-kereskedelmi internetes oldalak viselkedésétől. Ideális esetben a jelen találmány tartalmaz "automatikusan emlékező" összetevőt, amely a felhasználó számára megjegyzi a beírt adatokat, és "űrlapkitöltő" összetevőt, amely a néhány különböző modellnek megfelelő kereskedői oldal és felhasználói típus kombinációjából származó folyamatok hatékony összességét tartalmazza.

A jelen találmány begyűjti a felhasználótól az információt, biztonságosan és megbízhatóan tárolja azokat egy szerveren, és a felhasználó irányítása alatt azokat a megfelelő űrlap mezőkbe illeszti. A rendszer felügyeli a felhasználói információ a felhasználó figyelmét felkeltő kereskedői oldalak különböző HTML űrlap mezőire történő leképezését. Ez az információ ezután azon felhasználók esetében, akik a kereskedői oldallal kapcsolatba kívánnak lépni, meghatározhatja, hogyan legyenek kitöltve (vagy előre kitöltve) a HTML űrlapok.

Ami az "automatikusan emlékező" tulajdonságot illeti, korábbi kivitelezésű digitális pénztárcák implementálhatták az emlékező funkciót, de azt a felhasználónak kellett



kezdeményeznie. A jelen "automatikusan emlékező" tulajdonsággal a digitális pénztárca felhasználónak nem kell egy gombra kattintania ahhoz, hogy a rendszer emlékezzen az éppen kitöltött űrlapra, mivel a jelen rendszer emlékszik azokra a mezőkre, amelyeket a felhasználó a kereskedői ablakban kitöltött és elküldött. Mikor az űrlapot a felhasználó elküldte (például az "Elküld" vagy a "Vásárol" gomb megnyomásával), az online pénztárca azzal válaszol, hogy meghatározza, hogy a űrlap elküldését eredményező gombnyomás figyelemre érdemes kereskedői ablakból származik-e vagy nem. Ha igen, a pénztárca a megfelelő módon megjegyzi az adatot, ha nem, a pénztárca figyelmen kívül hagyhatja a űrlap elküldésének eseményét és folytathatja normál működését.

A digitális pénztárca vezérlők tartalmazhatnak egy "Megjegyez" feliratú gombot, vagy támogathatnak egy olyan automatikus emlékező tulajdonságot, mely állandóan aktív. Általánosságban a pénztárca által automatikusan kitöltött mezőktől eltérő mezőkbe beírt adat megjegyezhető. Ebben a szöveggörnyezetben az emlékezés azt jelenti, hogy amikor a felhasználó egy adott mezőbe adatot ír be, az értéket a rendszer eltárolja. A pénztárca összetevő érzékeli az ily módon beírt mező értékeket, és azokat biztonságos módszerrel az Interneten keresztül egy szerverhez továbbítja. Mikor a felhasználó újra meglátogatja az adott kereskedői oldalt, a pénztárca úgy tölti ki az űrlapot, hogy ahhoz a pénztárca rendszer mezőiből előkeresett általános információ mellett a korábban megjegyzett speciális adatokat is felhasználja. A űrlap feldolgozásakor (automatikus kitöltések) a pénztárca a mezőértékeket a szerverből biztonságosan hívja elő.

Egy kicsit részletesebben, az Internet Explorer böngészőt tekintve, a találmány a megfelelő módon implementál egy ActiveX vezérlőt, amely hozzacsatolja magát egy internetes oldalhoz, például az American Express Online Wallet oldalhoz. Az ajánlott megvalósításban az ActiveX vezérlő tartalmaz olyan eljárást, amely megjegyzi az összes Internet Explorer böngésző eseményeit, hogy az American Express Online Wallet ezekre az eseményekre szükség esetén válaszolhasson egy, az American Express Online Wallet oldalon belül betöltött JavaScript függvénnyel, így a rendszer számára lehetővé téve, hogy az Internet Exploreren belül megszerezze a teljesen letöltött dokumentumot. Ez megengedi, hogy a rendszer elkapjon egy "Dokumentum Kitöltve" ese-



ményt, amelyet az Internet Explorer böngésző dobott, és amely meghatározza, hogy mikor fejeződött be a dokumentum betöltése. Mikor ezt az eseményt sikerült elkapni, az ActiveX vezérlő értesíti az American Express Online Wallet oldalát egy JavaScript függvény American Express Online Wallet oldalán belül történő betöltésével. Ez a függvény megfelel ennek az eseménynek azzal, hogy a megfelelő módon kommunikál az ActiveX vezérlővel, hogy az kapja el a "Nyomtatvány Elküldése" eseményeket minden Internet Explorer böngészőn megjelenő minden űrlapnál.

Mikor a felhasználó kitölt egy űrlapot egy internetes oldalon és rákattint az adott oldalhoz tartozó "Elküld" gombra (azaz bármilyen vezérlőre, például gombra, amely elküldi az űrlapot), az American Express Online Wallet a saját oldalán, az ActiveX vezérlő általi JavaScript függvény hívás miatt értesül az eseményről. Az American Express Online Wallet ezután a megfelelő módon az URL cím ellenőrzésével eldönti, hogy az a dokumentum, amely az "Elküld" eseményt dobta, figyelemre érdemes-e vagy sem. Ha az eseményt kezelni kell, az American Express Online Wallet oldalnak az ActiveX vezérlőn belül egy megfelelő függvényt kell meghívnia, amely megszerzi azt a dokumentum objektum modellt (Document object Model, DOM), amely az eseményt dobta. A DOM ezután továbbítható és az űrlap értékei eltárolhatók, hogy el lehessen küldeni őket (tárolásra) a szervernek. Az ajánlott megvalósításban az ActiveX vezérlő el kell, hogy határolódjon a böngésző eseményeinek elkapásától és "Elküld" eseményeket kell előállítania, hogy a futás közbeni hibák minimálisra csökkenthetők legyenek.

A Netscape böngészőjét tekintve, az események Netscape böngészőben történő implementációja miatt, a rendszer az eseményt a JavaScript programon belül kapja el. Ha a rendszer sikeresen szerzi meg az "Általános Böngésző Írás" ("Universal Browser Write") privilégiumot (azaz a felhasználó engedélyezi), a rendszer sikeresen meghívhat egy függvényt, amely megengedi, hogy egy külső ablak kapja el egy másik ablak eseményeit. A rendszer ezután a dokumentum objektum modellt annak az ablaknak minden kerete felé továbbíthatja. Mikor így tesz, a rendszer értesíti az ablak minden űrlapját, hogy egy "Elküld" eseményt kíván elkapni. Így, mikor a felhasználó kitölt egy űrlapot abban az ablakban, amelyet a rendszer észrevett, majd rákattint az adott oldalhoz tartozó "Elküld" gombra (azaz bármilyen vezérlőre, például gombra, amely elküldi

az űrlapot), az online pénztárca értesül a műveletről és a megfelelő módon válaszol arra. A szakterületen jártasak értékelni fogják, hogy a jelen találmány bármilyen megfelelő tranzakciós rendszerben implementálható, beleértve (de nem csak erre korlátozva) bármilyen megfelelő digitális pénztárca rendszert is.

Ami az űrlap kitöltő funkciót illeti, a digitális pénztárca, például az American Express Online Wallet, a felhasználókat segítő, az űrlapok kitöltéséhez űrlap kitöltő lehetőséget nyújt. Korábbi megvalósítású rendszerek, mint például a GlobeSet Inc. által biztosított rendszer, általában böngészést segítő objektumot (Browser Helper Object, BHO) használnak. A BHO megközelítés gyakran hátrányokkal jár, például az Internet Explorer 5.0 böngészőnek van olyan hibája, hogy csak a regisztrációs adatbázisban (registry) elsőként megadott BHO-t tölti be. Ez bármilyen alkalmazás számára probléma lehet, mivel nem lehet biztos abban, hogy az ő BHO-ja betöltődött-e vagy sem. Mi több, a BHO az Internet Explorer minden példányához betöltődik, így akár több BHO példány is futhat egyszerre, memóriát lefoglalva és a az összes böngésző ablakban történő navigálást lelassítva, ahelyett, hogy csak a figyelemre érdemes ablakkal foglalkozna.

A jelen találmány ajánlott esetben helyettesíti a BHO megoldást az "automatikusan emlékező" tulajdonság megoldásánál már megismert ActiveX vezérlő alkalmazásával. Az ActiveX vezérlő Online Wallet internetes oldalhoz történő csatolásával a rendszer a megfelelő módon megszerzi a például a Shell Windows API-t alkalmazó bármelyik Internet Explorer ablakába betöltött dokumentum objektum modelljét. Mikor a felhasználó rákattint az Online Wallet oldalán levő "Űrlap Kitöltés" gombra, a pénztárca azzal válaszolhat, hogy az ActiveX vezérlőn keresztül először megszerzi a dokumentum objektum modellt. Ezután a pénztárca elmentheti a űrlapot alkotó mezők neveit, és elküldheti őket a szerveren levő heurisztikus motornak. A szerver azzal válaszol erre a kérésre, hogy visszaküldi azokat az értékeket, melyek ezeknek a mezőknek a kitöltéséhez szükségesek. A mezők kitölthetők a korábban már megszerzett dokumentum objektum modell alapján. Így a jelen találmány csökkenti azt a problémát, hogy az internetes oldalakon található űrlapokat ismétlődő adatokkal kell kitölteni.

Azon felül, hogy ez a vásárlóktól kisebb igénybevételt kíván, növeli a beírt adatok pontosságát is.

Speciálisabban, a jelen találmány architektúrája kombinálja az egyes honlapok szervertől oldali modelljét (például mezők, oldalak, linkek, stb.), a felhasználó szervertől oldali modelljét (például testreszabott profil), a honlap felhasználó által létrehozott modelljét (például makró rögzítés, kijelölés, húzz és ejts [drag and drop] típusú mozgatható), a honlap rendszer által manuálisan létrehozott modelljét (például a felhasználó által létrehozott modellek kiterjesztésére és jóváhagyására), és a honlap heurisztikusan létrehozott modelljét (például a mezők szemantikus információinak egymásra hatása, műveletek, stb.). A jelen rendszer néhány különböző modell típust hoz létre és tárol. Az első az adott honlapot jellemzi, például hogyan fizetünk a virtuális pénztárnál, hogyan rakunk bele valamit a virtuális bevásárlókosárba, hogyan keresünk meg egy bizonyos terméktípust, hogyan adunk meg fontossági sorrendeket (például utazás), stb. A második modell a felhasználót jellemzi, például mit csinálhat és milyen profil attribútumokkal rendelkezik. E két modell kombinálásával a jelen rendszer speciális folyamatokat hoz létre, amelyek nagy rugalmasságot és hatékonyságot nyújtanak. A rendszer a felhasználói hatáskör modelljétől a honlap modelljéig mindent meghatároz, ahol a honlap modellek bármilyen ismert eljárással elkészíthetők. Így a honlap modelljét létrehozhatja a felhasználó, a kiszolgáló, a tranzakciós kártya cég (kibocsátó), vagy akár a honlap karbantartója is. Az ajánlott megvalósításban a honlap modellek megjelenítéséhez használható elektronikus kereskedelem modellező nyelv (Electronic Commerce Modeling Language, ECML), illetve kiterjeszthető jelölésrendszerű nyelv (eXtensible Markup Language, XML). A különböző megvalósításokban a honlap modellek más rendszerekkel is cserélhetők.

Például a felhasználó gyakorlatiasan meglátogathatja a különböző légitársaságok és utazási irodák honlapjait, hogy repülőjegyet vásároljon. Minden honlapnak tipikusan különböző ablakokban levő mezői vannak a nagyjából hasonló információ begyűjtéséhez. Azonban minden egyes honlap különböző HTML űrlapot használ, melyek különböző URL címeken találhatók, és amelyek az idő múlásával még változhatnak is. Habár a különböző oldalakon begyűjtendő információ természete nagyon hasonló, jelen-

leg nincs olyan elfogadott mechanizmus, amellyel a mezők kitöltése a felhasználó utazási preferenciái (például ültetés, étkezés, időpontok, hűségpontok, stb.) alapján automatizálható lenne. Az egyes honlapok rendelkezhetnek az egyedi felhasználói profil kialakításának lehetőségével, ahol a profil tartalmazza ezen információ nagy részét. Azonban a jelenlegi gyakorlat szerint a felhasználónak ekkor is minden egyes honlaponál, a többitől függetlenül létre kellene hoznia a felhasználói profilját.

A jelen találmány heurisztika alapú mezőfelismerést tartalmaz. Ebben a megközelítésben a mező címkéket a térbeli közelségük alapján azonosítjuk, így azok figyelemre érdemes mezőket alkothatnak. A mező címkék és az űrlapok HTML attribútumainak (megemlítendő a HTML "bevitel", "kiválaszt", és "művelet" elemek attribútumai) kombinációját alkalmazzuk a kívánt mezők felismerését segítő katalógust tartalmazó heurisztikus motor bemeneteként.

Egy másik megvalósításban a jelen találmány a felhasználó közvetítése általi mezőfelismerést tartalmaz. Ebben a megközelítésben a felhasználó szándékosan rögzíti a bemenetet a "Megjegyez" gomb vagy más, olyan vezérlő megnyomásával, amely a szerver számára megengedi a felhasználó által végrehajtott műveletsorozattal kapcsolatos információ rögzítését. Mikor a felhasználó ezt teszi, tulajdonképpen "visszajátszhatja" a műveleteket (a más szoftver rendszerekben alkalmazott makró rögzítéshez hasonló módon). Ily módon a felhasználó műveletei ráadhatók a heurisztikus motor bemenetére és továbbíthatók közvetlenül a motor folyamatai által használt mező feltérképező táblához is.

Egy ajánlott megvalósításban a fenti két megközelítés némi manuális vezérlést is igényelhet a teljes folyamat térképek és űrlapok mezőtérképeinek létrehozásához, melyek pontosan lefestik a jelen találmányt lehetővé tevő navigálási mezőkitöltési opciókat. Szükség esetén emberi elemzők dolgozhatnak a felhasználó által vezérelt mezőfelismerés módszeréhez hasonló módon, habár ők a navigációjukról és mezőkitöltési folyamataikról messze több információt fognak biztosítani, mint amennyit a tipikus felhasználó adna. Mindegyik esetben a folyamattérkép (vagy részletes honlap térkép) létrehozásához gyűjtjük össze az információt, amelyek lefestik a különböző tevékenységek



során előforduló műveletek sorozatát (űrlap kitöltés, hipertext átviteli protokoll [HyperText Transfer Protocol, HTTP] küldés, HTTP fogadás, stb.). A folyamattérképben levő minden egyes internetes oldalhoz létrejön egy mezőtérkép, amely az automatikus űrlap elküldésre használható mezők neveit pontosan definiálja. Szükség lehet állapot-térképekre is a felhasználók a honlap látogatása során változó állapotának követéséhez (az állapot, például, hogy be van-e jelentkezve vagy nincs, a honlapon végzett műveletek eredményét módosíthatja).

Egy ajánlott megvalósításban a folyamat, mellyel a felhasználó a rendszerre hat, lehet teljesen automatizált (ebben az esetben a felhasználó csupán jelzi az adott művelet végrehajtásának igényét), vagy lehet felhasználó által közvetített (ekkor a találmány a felhasználó számára előre kitöltheti a űrlapot, így lehetővé téve a felhasználónak, hogy pontosítson, módosítson vagy kitöltsön egy olyan mezőt, mely további adatbevitelt igényel). A fent ismertetett termékek és szolgáltatások mellett a folyamat formáját és a mezőtérképeket lehetővé tevő technológia átemelhető új termékek és szolgáltatások területére is, például megoldható, hogy a cégek automatizálják a honlapjuk látogatóinak űrlap-adatainak kitöltését. Például, ha egy cég a vásárlói számára (a fenti eszközök bármelyikével) összeállítja a folyamat-, és mezőtérképeket, a cég ezt az információt, a szolgáltatásokat, és a termékeket tovább is adhatja kívülálló vásárlók részére. Azon honlapok - amelyekért ezek a térképek léteznek - is használhatják a jelen találmányt, így a honlapok előnyre tesznek szert azzal, hogy hasonló szolgáltatást szállítanak a saját vásárlóik felé, akik amúgy nem élveznék a rendszer előnyeit. A háttér-folyamatok maguk is olyan rendszerre támaszkodnak, amely megszerzi ezt az információt és átformálja, például XML és ECML formátumúvá. Ezek a szabványos megjelenítési formák az utóbbi két termékhez/szolgáltatáshoz tartozó információcsere alapjait képeznek.

A 9. ábrára áttérve, a 900 folyamat, amelyet egy példa jellegű aktivátor program valósít meg, a megfelelő módon tartalmazza az alkalmazás elindítását (902 lépés), az URL cím figyelését, mikor a felhasználó böngészik vagy online vásárol (904 lépés), így meghatározva, hogy a felhasználó támogatott oldalon böngészik-e (906 lépés), a támogatott oldal típusának meghatározását (908 és 912 lépés), és a megfelelő válaszadást,



rendre a 910 és 914 feldolgozási lépésekben. Más jellemzők (például kuponok, speciális ajánlatok, figyelés, biztonság, és hasonló) a 916 lépésben implementálhatók.

A 902 alkalmazás indítása lépés az aktivátor alkalmazás alkalmas módon történő megnyitását és az alkalmazás megfelelő módon történő elindítását foglalja magában. Az aktivátor alkalmazás elindulását kiválthatja a rendszer elindulása, a hálózatra (például Internetre vagy LAN-ra) való csatlakozás, vagy a böngésző elindítása (például a Microsoft Corporation [Redmond, Washington] Internet Explorer böngészőjének, vagy a Netscape Corporation [Mountain View, California] Netscape Communicator böngészőjének elindítása). Különbő megvalósításokban az aktivátor alkalmazás értesítheti a 140 pénztárca szervert (1. ábra), a 406 pénztárca alkalmazást (4. ábra), vagy más szervert a 102 adathálózaton. Az aktivátor alkalmazás alkalmas módon kapcsolatban lép a távoli szerverrel olyan információ megszerzéséhez, mint például a pénztárca által támogatott internetes oldalak, körzetnevek, vagy URL címek. Ez az információ megszerzhető időzítéses alapon (például naponta, hetente, vagy az ügynök alkalmazás minden indításakor), illetve a szerver vagy aktivátor alkalmazás által kezdeményezett lekérdezésekkor. A különböző megvalósításokban az aktivátor alkalmazás a támogatott URL címeket gyorsítótárban, háttértárolón, vagy a kliens számítógép memóriájában tárolja.

Mikor a felhasználó az Internetet vagy más 102 adathálózatot böngészi, az aktivátor alkalmazás a megfelelő módon figyeli a felhasználó hálózati elhelyezkedését. A felhasználó böngészésének figyelésére egy eljárás lehet a felhasználó böngészőjében használt URL címek figyelése. Az ilyen megvalósításoknál az aktivátor alkalmazás megszerzi a felhasználó böngészőjéből (vagy alkalmas módon a rendszer hálózati interfészéből) a jelenleg használt URL címet, és összehasonlítja (906 lépés) azt a 902 alkalmazás indítás lépésben a távoli szervertől megszerzett támogatott URL címek listájával. Ezek az összehasonlítások a 9. ábrán a logikailag különválasztott 906, 908, 912, és 916 lépéseknél látható, habár ezek a lépések akármilyen módon összevonhatók és különválaszthatók anélkül, hogy a találmány lényegétől eltávolodnánk. Például, bár a 9. ábra több végrehajtott összehasonlítást is mutat, bizonyos megvalósításokban ele-

gendő lehet a jelenlegi URL cím és a támogatott URL címek listájának egyszeri összehasonlítása is.

Ha a jelenlegi URL cím megfelel egy támogatott URL címnek, az aktivátor alkalmazás a megfelelő módon reagál. Például, ha a jelenlegi cím támogatott virtuális pénztár oldal ('igen' válasz a 908 lépésben), az aktivátor alkalmazás végrehajt egy kassza folyamatot (910 lépés). A kassza folyamat tartalmazhatja a felhasználó értesítését arról, hogy a kassza oldal egy felpattanó üzenet formájában, a tálcá ikonok között, vagy a beúszó ablakban egy bizonyos ikon formájában lesz látható. Ha a 214 pénztárca kliens alkalmazás még nincs elindítva, az aktivátor alkalmazás megjeleníthet egy dialógusablakot vagy más módon jelezheti a felhasználónak, hogy az internetes oldalt a 214 pénztárca alkalmazás támogatja. A jelzés biztosíthat gombot vagy más mechanizmust is, mellyel a felhasználó elindíthatja a 214 pénztárca alkalmazást.

Ha a jelen URL egy támogatott fizetés oldalnak felel meg ('igen' válasz a 912 lépésben), az aktivátor alkalmazás fizetési utasításokat adhat a pénztárca alkalmazásnak, vagy átadhatja a vezérlést a pénztárca alkalmazásnak (914 lépés). Az aktivátor alkalmazás, a pénztárca alkalmazás, a böngésző, és hasonlóok közötti üzenetváltás történhet Open Desktop és objektum csatolás és beágyazódás (Object Linking and Embedding, OLE) üzenetekkel, objektum rutinhívásokkal, rendszerhívásokkal (Operating System call, OS call), vagy hasonló módon.

Különbő megvalósításokban a fent ismertetett funkciókat a most leírásra kerülő sütik (cookies) használatával érik el. A sütik az érvényes felhasználói kontextus észlelésére szolgálnak. Ha érvényes felhasználói kontextust fedez fel, az aktivátor vagy elindít egy szerver alkalmazást, vagy elindít egy szerver eszközsort, amely lehetővé teszi a felhasználónak, hogy más alkalmazásokat indítson el. Például a felhasználó böngészőjének lehet néhány sütije, melyek azt jelzik, hogy a felhasználó tud személyes fizetéssel vagy speciális kártya termékkel vásárolni. Az aktivátor elindíthat egy eszközsort, amely felajánlja a felhasználónak a fizetési eszköz kiválasztását (például személyes fizetés vagy fizetés a felhasználó digitális pénztárcájában levő kártyával). Látható azonban, hogy az elérhető alkalmazások köre nem zárul be a vásárlási tranzakcióval. Kü-



lőnböző megvalósításokban a kontextus információt mind a szerveren, mind a böngészőhöz kapcsolódó sütikben tároljuk. Például a sütik funkcionálhatnak kulcsként is, amellyel a szerveren lévő kontextus információ lehívható.

Más funkciók is beépíthetők az aktivátor alkalmazásba. Például biztonsági mechanizmusok (mint a korábban ismertetettek és az ezután leírásra kerülők), vásárlót figyelő funkciók, kuponok, speciális ajánlatok, és más hasonlóak is implementálhatók. Kuponok és speciális ajánlatok esetén az aktivátor észreveheti, hogy a jelenlegi URL cím megfelel egy bizonyos terméknek vagy internetes oldalnak. Mikor a felhasználó "szörföl", vagy böngészik egy bizonyos támogatott URL címen, az aktivátor észreveszi az azonosságot és (dialógus ablakon, böngészőn, vagy más hasonlón keresztül) felajánl a felhasználónak egy speciális ajánlatot, például, hogy egy bizonyos terméket megvásárolhat vagy hogy speciális árengedménnyel vásárolhat. Belátható, hogy más funkcionalitások is beépíthetők az aktivátor alkalmazásba anélkül, hogy a jelen alkalmazás hatáskörétől eltérnének.

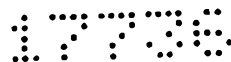
A találmány különböző megvalósításaiban a 214 pénztárca kliens (2. ábra) fel van töltve az adott felhasználóra/vásárlóra jellemző információval. Az 1. ábrának megfelelően a felhasználó a 102 adathálózaton keresztül egy webszerverrel, például a 140 pénztárca szerverrel való kapcsolatfelvétellel igényelhet digitális pénztárcát. A felhasználó a pénztárca igényléséhez kitölt egy jelentkezési űrlapot (mely generálható például szabványos átjáró interfész [Common Gateway Interface, CGI] szkriptekkel). A 140 pénztárca szerver a megfelelő módon demográfiai, számla-, és más információt (például cím, szállítási cím, név, hitelkártyaszám, és más hasonló) fogad a 306 azonosítás szervertől (3. ábra) vagy a magánhálózat egy másik szerverétől. Ez az információ használható a 214 pénztárca kliens (2. ábra) beállításához, amely az egyes felhasználókra nézve egyedi. A 214 pénztárca kliens beállításának egy eljárása az, hogy a 214 pénztárca klienshez kapcsolódó konfigurációs fájlt hozunk létre, amelyet a 214 pénztárca kliens olvas a fent leírt pénztárca információ megszerzéséhez.

Ideális esetben a regisztrációs információ tartalmaz kártya olvasó információt is, amely tartalmazza, hogy a kártya olvasó csatlakozóegység (port) soros vagy univerzális soros



busz (Universal Serial Bus, USB) típusú-e. Ha a pénztárca igénylést jóváhagyják, le szállíthatják vagy más úton rendelkezésre bocsáthatják a kártyaolvasót, és adnak hozzá egy speciális kódot (például kriptografikus kulcsot, jelszót, vagy másfajta elektronikus vagy nyomtatott kódot). A felhasználó ezután bejelentkezik az online pénztárca szolgáltatáshoz a 140 pénztárca szerverrel való kapcsolatfelvétellel, magát a kártyával és/vagy a speciális kóddal azonosítva a szervernél. A speciális kód megadása után a felhasználó a pénztárca szoftver egy speciálisan beállított példányát kapja meg, amely a megfelelő módon feltelepíthető a 110 vásárló számítógépére. A pénztárca előre-kitöltő eljárás bármilyen hitelkártyával vagy fizető kártyával használható a pénztárca program speciális kóddal való beállításának köszönhetően. Az adott felhasználó beállítási információja a felhasználónak kiadott kódhoz kapcsolódik, és a felhasználó később azonosítás céljából megadhatja a speciális kódját a 140 pénztárca szervernek, hogy így az ő adatai alapján előre beállított pénztárca programot megszerezze.

Elsősorban az 1. és a 10. ábrákra hivatkozva, a 110 vásárló a megfelelő módon a 202 intelligens kártya használatával jelentkezik be a 140 pénztárca szerverhez és indít el egy tranzakciót. A 140 pénztárca szerverhez való bejelentkezéshez a 110 vásárlónak először a 216 böngészőn keresztül a 130 biztonsági szerverhez kell kapcsolódnia. A felhasználó a bejelentkezési oldal eléréséhez könyvjelző, internetes parancsikon (shortcut), hipervivatkozás (hyperlink), vagy más megfelelő eszköz segítségével kiválaszt egy bizonyos URL címet. A 130 biztonsági szerver ekkor a 320 hálózati csatlakozó egységen keresztül kiadhat egy bejelentkezési oldalt. A különböző megvalósításokban a bejelentkezési oldal részeként adott egy űrlap és egy "Elküld" gomb a felhasználó/jelszó típusú bejelentkezéshez, továbbá egy link az intelligens kártya bejelentkezéshez. A felhasználó kiválasztja az intelligens kártya bejelentkezést és a 216 böngésző a megfelelő módon válaszol az 1002 kérés üzenet továbbításával (10. ábra). A 130 biztonsági szerver fogadja az 1002 kérés üzenetet és a megfelelő módon elindítja az intelligens kártya bejelentkezési folyamatot. A különféle megvalósításokban a 130 biztonsági szerver az 1002 kérés üzenetre adott válaszként a 304 biztonsági motornak vagy a 306 azonosítás szerver segítségével megformáz egy kriptográfiai lekérdezést. Az 1004 kriptográfiai lekérdezés bármilyen lekérdező üzenet lehet, amely megelőzi a visszajátszásos támadásokat (például korábban elküldött azonosítás csomagok újrakül-



désével létrehozott félrevezető üzeneteket), úgy, hogy véletlen adatokon alapszik és olyan tervezésű, hogy az intelligens kártyán tárolt X.509 alkalmazástól választ idéz elő. A lekérdezés ezután a megfelelő módon a 102 adathálózaton keresztül 1004 kriptográfiai lekérdezésként a 110 felhasználó rendelkezésére áll.

Az 1004 kriptográfiai lekérdezés fogadásakor a 216 böngésző a megfelelő módon átadja az 1004 lekérdezést a 214 pénztárca kliensnek, hogy az a 202 intelligens kártyával dolgozza fel. Ha a 214 pénztárca kliens az adott pillanatban nem fut, a 216 böngésző automatikusan elindíthatja azt. A 214 pénztárca kliens ekkor a megfelelő módon előkészíti az aláírás választ. Például a 214 pénztárca kliens kibonthatja a szerver lekérdezés információt, megformálhat egy új kliens lekérdezést (például egy második kriptográfiai lekérdezést a 202 intelligens kártyának), összeállíthatja a két lekérdezést egy kettős lekérdezésbe, és kiszámíthat a kettős lekérdezés számára egy hash kódot a későbbi használatra, például egyes típusú nyilvános kulcsú kriptográfiai rendszerű kriptográfiai (Public-Key Cryptography System 1, PKCS1) blokk formájában. A hash bármilyen algoritmussal, például hármas vagy négyes típusú üzenet kivonatolás (Message Digest version 3-4, MD3, MD4) algoritmussal számítható, és a megfelelő módon azt biztosítja, hogy a kettős lekérdezés blokkban az adat teljes és pontos. A PKCS1 nyilvános kulcsú titkosítási szabvány, amely meghatározza az RSA (Rivest, Shamir, Adleman) nyilvános kulcsú kriptográfiai rendszerek titkosítási és jelzési adatait. A PKCS szabvány teljeskörű leírása megtalálható a PKCS #1: RSA Kriptográfiai Specifikációk 2. verzió, 1998. szeptemberi kiadásában, (amely a <http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-1.html> címen online elérhető), és amelyet annak egészére történő hivatkozási alapként használni fogunk.

A PKCS1 blokk a 204 kártya olvasón keresztül a 202 intelligens kártyához kerül feldolgozásra (1006 lépés a 10. ábrán). A különféle megvalósításokban a 204 kártya olvasó a 110 felhasználói számítógéppel működik együtt, hogy a felhasználótól valamilyen személyes azonosítót, például személy azonosító számot (Personal Identification Number, PIN) vagy más egyedi azonosítót kérjen be a kártyához való hozzáféréshez. Más változatokban a PIN vagy más személyi azonosító tárolható máshol is a rendszeren, például a 204 olvasón vagy a 110 felhasználói számítógépen. A felhasználó a



megfelelő módon megadja a személy azonosítót a 202 intelligens kártya feloldásához, amely a 214 pénztárca klientsztől fogadja a kettős lekérdezés blokkot és digitálisan alá is írja azt. Különböző megvalósításokban a 202 intelligens kártya tartalmaz egy titkos kulcsot, amellyel a hitelesítő aláírás számítható. Az aláírt blokk ezután a megfelelő módon visszakérül a 214 pénztárca klienshez. Különféle megvalósításokban a 202 intelligens kártya bizonyítványt is biztosít (például X.509 bizonyítványt), amely megfelel a digitális aláírás számításához felhasznált titkos kulcsnak.

Az aláírás és bizonyítvány 202 intelligens kártyától való fogadása után a 214 pénztárca kliens alkalmas módon létrehoz egy megfelelő, 130 biztonsági szervernek címzett 1008 válasz üzenetet. Habár az 1008 válasz üzenet bármilyen formátumú lehet, különféle megvalósítások PKCS7 formátumban adják meg azt. A PKCS7 formátumot az 1993. november 1-én javított kiadású PKCS #7: Kriptográfiai Üzenet Szintaxis Szabvány. RSA Laboratóriumok Feljegyzés, 1.5 verziója definiálja, mely elérhető online az <ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-7.doc> címen, és amelyet annak egészére történő hivatkozási alapként használni fogunk.

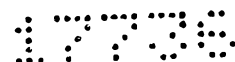
Az 1008 válasz fogadása után a 130 biztonsági szerver a megfelelő módon feldolgozza az üzenetet (1010 lépés a 10. ábrán). Különféle megvalósításokban az 1008 válasz üzenet továbbítódik a 306 azonosítás szerverhez, amely hitelesíti a 202 intelligens kártya által kiadott bizonyítványt és aláírást. A bizonyítvány sikeres ellenőrzése és az aláírás hitelesítése után, különböző megvalósításokban létrehozható egy biztonsági token, mely visszaküldhető a 110 felhasználó számítógépének vagy a 202 intelligens kártyának.

Ily módon a biztonsági token későbbi bemutatása a felhasználó számára eszközt biztosít ahhoz, hogy létrehozzon egy azonosítást és biztonságosan kapcsolatba lépjen a pénztárca szerverrel. Különféle megvalósításokban a 306 azonosítás szerver is létrehozhat egy másik biztonsági tokent, amely a felhasználót azonosítja. Különféle megvalósításokban ez a token több részből állhat, melyek együtt meghatározhatnak egy megfelelő bizonyítványt, intelligens kártyát, vagy más adatot, feltehetően a 310 adatbázisban tárolt adatok segítségével. Különféle megvalósításokban a második biztonsági

token és/vagy annak részei az 1012 újraküldött üzenettel továbbíthatók a 110 felhasználónak. Különböző megvalósításokban a kiegészítő biztonsági token továbbítható a felhasználó felé vagy karbantartható a 306 azonosítás szerveren.

Az 1012 újraküldött üzenet fogadásakor a 110 felhasználó alkalmas módon kapcsolatba lép a 140 pénztárca szerverrel hogy kérje a kapcsolatfelvételt. Különböző megvalósításokban az 1014 "Kapcsolatfelvétel" üzenet alkalmas módon tartalmazza a biztonsági tokent és esetleg a kiegészítő biztonsági token egészét vagy részét az 1012 újraküldött üzenet részeként. A 140 pénztárca szerver a 110 felhasználó azonosításához a biztonsági tokenek egészének vagy részének valamilyen kombinációjával lekérdezi a 130 biztonsági szervert. Az 1016 lekérdezés és az 1018 válasz hitelesítés alkalmas módon a 150 hálózaton keresztül továbbítódik, amely néhány megvalósításban a 102 adathálózattól külön van fenntartva a 100 rendszer biztonságának fokozásához. Egy lehetséges megvalósítás a 102 hálózatot alkalmazza, ami, néhány megvalósításnál virtuális magánhálózat, SSL protokoll, megosztott titkok, és/vagy más kriptográfiai eszköz alkalmazásával nagyobb biztonságot jelent. Ha az 1018 válasz hitelesítések rendszerben vannak, a 140 pénztárca szerver előhossa a 110 felhasználóhoz kapcsolódó attribútumokat a 408 pénztárca adatbázisból és az 1020 üzeneten keresztül értesíti a 110 felhasználót a sikeres bejelentkezésről. Látható, hogy más bejelentkezési eljárás is lehetséges. Belátható továbbá, hogy bármilyen titkosítási séma, üzenetformátum, stb. is implementálható az 1000 bejelentkezési folyamatot illetően.

A 11. ábrára, egy példa jellegű, vásárlási tranzakció 1100 azonosítás folyamatára áttérve, a folyamat azzal kezdődik, hogy a 110 felhasználó egy olyan eseményre (például vásárlásra), amely azonosítást igényel, a 140 pénztárca szerverrel elhelyez egy 1102 kérést. A 140 pénztárca szerver alkalmas módon felismeri az eseményt és a lekérdezés üzenet megformálására elküld egy 1104 kérés üzenetet a 130 biztonsági szervernek például a 150 kommunikációs csatornán keresztül. A 306 azonosítás szerver (vagy a 130 biztonsági szerver más alkalmas része) ezután megformázza az 1106 lekérdezés üzenetet (mely tartalmazhat véletlen adatot), és továbbítja az 1106 lekérdezés üzenetet a 140 pénztárca szerverhez például a 150 kapcsolaton keresztül. A 140 pénztárca szerver fogadja az 1106 lekérdezés üzenetet és 1108 aláírás igénylő üzenetként továbbítja a



lekérdezés adatot a 216 böngészőnek. A 216 böngésző szükséges esetben elindítja a 214 pénztárca kliensét és továbbítja az 1108 aláírás igénylő üzenetet. A fent leírtak alapján a 214 pénztárca kliens megformál egy aláírás igénylő blokkot, például egy PKCS1 blokkot, amely tartalmazza a szerver lekérdezést, a kliens lekérdezést, és a hash kódot. Az eredményül kapott aláírás igénylő blokk a 204 kártya olvasón keresztül továbbításra kerül a 202 intelligens kártyához. A 202 intelligens kártya alkalmas módon aláírja a blokkot és a megfelelő módon biztosítja a saját X.509 bizonyítványának másolatát.

Az aláírt blokk ezután visszaküldhető a 214 pénztárca klienshez, amely alkalmas módon egy megfelelő 1110 aláírás válasz üzenetet (például PKCS1 üzenetet) formál és elküldi azt a 140 pénztárca szervernek. A 140 pénztárca szerver ezután előállít egy 1112 érvényesség ellenőrzés üzenetet, amely az 1110 aláírás válasz üzenetből származó adatokat és a bejelentkezési folyamat (mint például a 10. ábra példa jellegű bejelentkezési folyamata) során a 110 felhasználóhoz társított biztonsági tokent tartalmazza. Lehetséges megvalósításokban a biztonsági token az 1110 aláírás válaszban érkezik a 110 felhasználótól. Az 1112 érvényesség ellenőrző üzenet a 150 kapcsolaton keresztül kerül a 130 biztonsági szerverhez. A 130 biztonsági szerver az érvényesség ellenőrző üzenetet ezután alkalmas módon a 306 azonosítás szerverhez irányítja, amely ellenőrizheti az aláírást és előhozhatja a megfelelő biztonsági tokent a 310 adatbázisból (1114 lépés a 11. ábrán). A biztonsági token és/vagy az adatbázisból előhozott opcionális azonosító kód ezután összehasonlításra kerül a 140 pénztárca szervertől kapott biztonsági tokennel vagy azonosítóval. Ha a két objektum (például a két biztonsági token vagy a két azonosító) egyezik, megállapítható, hogy a jelenleg használt kártya ugyanaz a kártya, mint amelyet a 110 felhasználó bejelentkezéskor használt. A 130 biztonsági szerver egy megfelelő 1116 elfogadó vagy elutasító üzenetet küld a 140 pénztárca szervernek, és a tranzakció engedélyezésre kerül.

Különböző megvalósításokban a 140 pénztárca szerver a 110 felhasználó szempontjából proxy szerverként üzemel. Például a 140 pénztárca szerver a 110 felhasználó részéről kitölthet szállítási címet, kártyaszámot, és más hasonló adatokat kérő vásárlási urlapokat. A 120 kereskedő ezután ellenőrizheti a vételi tranzakciót, úgy, mintha az szoká-

sos fizető kártyás tranzakció volna, hagyományos hardverek és szoftverek használatával. Szemmel látható azonban, hogy az itt leírt rendszerek által biztosított nagyobb biztonság nagyobb megbízhatóságot tesz lehetővé a vásárló kilétét illetően, így alacsonyabb tranzakciós kezelési költséget indokol.

A találmány különböző megvalósításai a biztonsági rések elleni további védelmet foglalják magukba. Mivel a sok, 130 biztonsági szerverbe vagy a 140 pénztárca szerverbe zsúfolt szerveroldali funkció különböző kommunikációleíró nyelvvel (például a Sun Microsystems [Mountain View, California] által definiált JavaScripttel, vagy a Microsoft Corporation [Redmond, Washington] által definitált VBScripttel megírt összetevőt tartalmazhat, a 102 hálózathoz kapcsolódó szerverek különböző funkciókat biztosítanak több 110 felhasználónak, egyúttal továbbítják is ezen nyelven implementált szkripteket (vagy kódokat) a felhasználónak. A kódot a 110 felhasználó számítógépe értelmezi, fordítja, vagy másképpen lefuttatja. JavaScript leíró nyelvet alkalmazó megvalósításokban például a szkripteket a 110 felhasználó számítógépén futó böngésző program (például Internet Explorer, Netscape Communicator, vagy hasonló) értelmezi és futtatja. Más megvalósítások más nem-PC böngészőket tartalmaznak, például vezeték nélküli alkalmazás protokoll (Wireless Application Protocol, WAP) alapú telefonok, amelyek támogatják a vezeték nélküli jelölési nyelv (Wireless Markup Language, WML) alapú szkripteket. A különböző szkript nyelvek tartalmazhatnak utasításokat, objektumokat vagy más adat mechanizmusokat például a felhasználó me-revlemezén levő fájlok eléréséhez, vagy a felhasználó számítógépén történő más adatmanipulációhoz. Annak megelőzésére, hogy ellenőrizetlen források futtatható kódot továbbítsanak a felhasználónak, a szkript nyelvek tartalmazhatnak olyan mechanizmust, mely a felhasználó számára lehetővé teszi, hogy csak megbízható forrásból származó szkriptet fogadjon el. Például a fent leírt, elektronikus tranzakciót lebonyolító felhasználó megengedheti, hogy a pénztárca szervertől érkező kódokat elfogadja, de megakadályozhatja, hogy más forrásból származó más szkriptek lefussanak a gépén.

Sok szkript leíró nyelv komoly biztonsági problémáját ábrázolja a 12A. ábra. Egy rossz szándékú "cracker" létrehozhat egy 1204 weboldalt, amely úgy van megtervezve, hogy egy 1206 legitim webszerver felhasználói ellen rosszindulatú támadást hajtson végre.

Az 1204 cracker oldal (az ábrán "bűnözői honlap"-ként feltüntetve) például a felhasználónak egy kódrészletet, például szkriptet továbbíthat. Az 1204 bűnözői honlap utasíthatja a felhasználó 216 böngészőjét, hogy az az 1206 legitim szervertől egy adott URL címet kérjen. A hivatkozott URL cím szándékosan cselt alkalmaz úgy, hogy az 1206 legitim szerver hibaüzenetet vagy más választ ad a felhasználó 216 böngészőjének. Különféle megvalósításokban az 1206 legitim szerver válasza automatikusan tartalmazhatja a felhasználó 216 böngészője által kiadott kérés egy részletét vagy változatát. Ha ez a válasz JavaScript, VBscript, vagy más, az 1204 bűnözői honlap általi rosszindulatú támadás eredményeképpen létrehozott kódot tartalmaz, a kód a felhasználó számítógépén végrehajtható lesz. Ez a példa a "crackerek" által alkalmazható technikák közül csak egy, mellyel az 1206 legitim webszerver arra kényszeríthető, hogy rosszindulatú utasításokat adjon a felhasználó 216 böngészőjének. Mivel a különböző kódolási és szkript nyelvekkel a felhasználó számítógépének fájlrendszer leíró regisztrációs adatbázisához, vagy máshoz is hozzáférhetnek, látható, hogy az ilyen kódok ellenőrizetlen végrehajtása semmiképpen sem kívánatos. Mindazonáltal a 12A. ábrán látható technika lehetővé teszi szkript vagy más kód az 1204 bűnözői honlapról a felhasználó számítógépére történő továbbítását. Mivel a felhasználó számítógépe azt hiszi, hogy a szkript megbízható forrástól (például a pénztárca szervertől) származik, végre is hajthatja a rosszindulatú kódot, így alapot adva egy esetleges károkozásnak, ellenőrizetlen fájlterjesztésnek, fájlmegsemmisítésnek, vagy más hasonlóknak. A 12B. ábra a megfelelő kommunikációs folyamatot illusztrálja (szemben a 12A. ábra bűnözői támadásával szemben).

E jelentős probléma megelőzése céljából a találmány különféle megvalósításai tartalmaznak megoldásokat a nemkívánatos végrehajtható kódok csökkentésére vagy megszüntetésére. A 13. ábrára hivatkozva, a szkript alapú támadás valószínűségét csökkentő 1300 folyamatnak alkalmas módon részei a lépések, melyek során a szerver nagyobb hatáskörű részeit korlátozzuk (1302 lépés), a szerver ezen részein belül töröljük a veszélyes karaktereket (1304 lépés), szükség esetén kódolunk bizonyos karaktereket (1306 lépés), és esetleg naplózuk az adatokat, melyeket az internetes oldal lényeges részéről a felhasználó felé továbbítunk (1308 lépés).



Az 1302 lépést tekintve, egy internetes oldal tipikusan különféle, egyedi URL címmel rendelkező lapokat tartalmaz. A honlap felhasználói nagyobb bizalmat tanúsíthatnak bizonyos szerverek esetében (például pénzügyi intézmények vagy kereskedők szervereinek). Azzal, hogy ezt a bizalmat a honlapnak csak egy részére korlátozzuk (például a megbízhatónak tekintett honlapnak megfelelő URL címek korlátozott részhalmazára), a honlap fennmaradó részére a megbízhatósági szintet alkalmas módon csökkentjük és a biztonság ezzel nő. A bizalom például úgy korlátozható a honlap bizonyos részeire, hogy a böngészőt úgy állítjuk be, hogy a honlapnak csak egy részét tekintse megbízhatónak. A felhasználó böngészője beállítható például manuálisan vagy egy, a pénztárca által biztosított konfigurációs szkripttel. Mikor az internetes oldalnak csak bizonyos lapjait (például egy részét) tekintjük megbízhatónak, minden, más oldalra mutató hivatkozást tartalmazó szkript vagy nem hajtódik végre, vagy nem magasabb megbízhatósági szinten hajtódik végre.

Azon túl (vagy a helyett), hogy a kliens beállítható úgy, hogy a szervernek csak bizonyos részeit tekintse megbízhatónak, a szerver is beállítható a kliens-szerver együttműködés biztonságának növeléséhez. Például a szerver nagy részén a magasabb bizalmi szintű szkript futtatást le lehet tiltani. Mi több, figyelhető vagy módosítható az internetes oldal megbízhatónak tekintett részének rendelkezésére bocsátott adat is, még mielőtt visszaküldené a felhasználónak (1304 és 1306 lépés). A legtöbb szkript nyelv bizonyos karaktereket ír elő a formázási parancsokhoz. Például a JavaScript nyelvben a szkript utasításokat nyitó és csukó zárójelekben ("<" és ">") kódolják. Ennélfogva a nyitó és csukó zárójelek kitörölhetők minden olyan szövegben, amely az internetes oldal megbízható részéről kerül visszaadásra. Ha az internetes oldal megbízhatónak tekintett részéről elérhető honlap nyitó és csukó zárójeleket alkalmazó rosszindulatú JavaScript programot tartalmaznak, a szkript utasítások nem fognak a felhasználó számítógépén lefutni, hiszen a szkript utasítások a zárójelek kitörlése után nem az előírt formátumúak lesznek. Egy másik lehetséges megoldás, hogy bizonyos "veszélyes" karakterek (mint például a zárójelek a JavaScript-ben) más formátumúak lesznek, például "& jelölésűek", vagyis egy "&" jellel kezdődnek és azt követi a nekik megfelelő amerikai szabványos kód információcseréhez szükséges (American Standard Code for Information Interchange, ASCII) érték, vagy úgy, hogy a "veszélyes" karakter bizton-

ságos karakterre, például "szóköz" karakterre cserélődik (1306 lépés). Látható, hogy a találmány különböző megvalósításaiban az adott nyelvre, szkript környezetre, vagy más alkalmazható módszerre jellemző bármilyen karakter megsemmisíthető vagy kódolható lenne.

A különféle megvalósításokban az opcionális 1308 lépés a megfelelő módon tartalmazza az internetes oldal különböző részei által rendelkezésre bocsátott információ alapján vezetett napló karbantartását. Naplózható minden olyan tartalom, amelyből karakterek lettek eltávolítva, vagy amelyekben a karaktereket kódoltuk, így a napló visszanezhető, hogy egy adott honlapot hálózati kliens tartalmazására használják-e. Például minden, a honlap által elküldött tartalom, minden, a honlap megbízhatónak tekintett részéből elküldött tartalom, minden szkripteket/programokat tartalmazó tartalom, minden, a megbízható részen kívülről, vagy a honlap más részéről elküldött tartalom naplózható egy vagy több fájlba. Ezek a fájlok alkalmas módon kereshetők vagy más módon megvizsgálhatók annak eldöntésére, hogy volt-e próbálkozás a szerver felhasználójának irányába történő ellenőrizetlen tartalomküldés.

Néhány esetben belső gépek is megtámadhatók egy "bűnözői honlap" által, olyan tartalom hálózati szervernek való elküldésével, amely szkriptet foglal magában arra, hogy a tartalom útját naplózza a nyomkövető (például napló-) fájlok segítségével. Feltéve, hogy a böngésző úgy van beállítva, hogy nagyobb bizalmat ad a szerveren levő fájloknak, különféle megvalósításokban, mikor a felhasználó a böngészővel visszanézi a web-, és más e-kereskedelmi szerverek nyomkövető fájljait, a hálózati kliensen, a nyomkövető fájlt küldő hálózati szerver szintjén (például magasabb bizalmi szinten) végrehajtható egy szkript. Ezen szkript végrehajtása támadást okozhat, amely sokkal később is bekövetkezhet, mint amikor a szkriptet a hálózati szerver megkapta. Ez a támadás megelőzhető ugyanazon módszerekkel és eljárásokkal, mint amelyeket fentebb definiáltunk honlapokon keresztüli szkript-küldések, például a fent leírt "bűnözői" támadások megelőzésére. Egy hálózati szerveren, például webszerveren vagy hálózati kliensen, például böngészőn működő szűrő, mint amilyen a 13. ábrán is látható, kiszűrheti a szkriptek vezérlő karaktereit és kódolhatja vagy eldobhatja ezeket a karaktereket, vagy akár az egész bejegyzést.

Az alábbiakban következő igénypontoknak megfelelő szerkezetek, anyagok, műveletek és elemek ekvivalensei szándékunk szerint tartalmazzanak minden szerkezetet, anyagot, vagy műveletet, amelyek a más igényelt elemekkel együtt a speciálisan igényelt funkciót végrehajtják. A találmány területe inkább az ismert igénypontok és törvényes megfelelőik, mint a fent ismertetett példák alapján határozható meg.

Szabadalmi igénypontok

1. Eljárás tranzakció lebonyolításához, amely eljárás során:
 - a. a szervernél fogadjuk a felhasználótól érkező tranzakció kérést,
 - b. lekérdezést bocsátunk ki a felhasználónak,
 - c. a felhasználó lekérdezés alapján adott válaszát fogadjuk,
 - d. a felhasználó azonosításához feldolgozzuk a választ,
 - e. megbízólevelet állítunk össze a tranzakcióhoz, amely megbízólevélnek legalább egy kulcsa van,
 - f. a megbízólevél legalább egy részét a felhasználó rendelkezésére bocsátjuk,
 - g. második kérést fogadunk a felhasználótól, amely második kérés tartalmazza a megbízólevél egy részét, és
 - h. a megbízólevél egy részét a kulccsal érvényesítjük a tranzakciós szolgáltatás eléréséhez.
2. Az 1. igénypont szerinti eljárás, azzal jellemezve, hogy a tranzakció elektronikus vásárlási tranzakció.
3. A 2. igénypont szerinti eljárás, azzal jellemezve, hogy az elektronikus vásárlási tranzakció digitális pénztárca használatával kerül lebonyolításra.
4. Az 1. igénypont szerinti eljárás, azzal jellemezve, hogy az eszköz intelligens kártya.
5. Számítógépen implementált eljárás hálózati szerver hálózati kliens ellen indított támadás alapjaként történő használatától való védelméhez, amely eljárás során:
 - a. a szervernél fogadjuk a hálózati kienstől érkező kapcsolat felépítésére irányuló kérést, és
 - b. megvizsgáljuk a protokollnak megfelelő speciális karakterek jelenlétét a hálózati szerver egy részén,
 - c. ellenőrizzük, hogy a hálózati szerver hálózati kliensnek adott minden válasza speciális karakterektől mentes, és
 - d. választ biztosítunk a hálózati szervertől a hálózati kliensnek.



6. Az 5. igénypont szerinti eljárás, mely tartalmazza továbbá a protokoll számára a hálózati szerverhez való hozzáférés a hálózati szerver egy részére való korlátozását.
7. Az 5. vagy 6. igénypont szerinti eljárás, mely tartalmazza továbbá a speciális karakterek jóindulatú karakterekkel történő helyettesítését, úgy, hogy a kiválasztott protokoll által felvetett biztonsági kockázat csökkenjen.
8. Az 5. vagy 6. igénypont szerinti eljárás, azzal jellemezve, hogy a protokoll tartalmaz JavaScriptet.
9. Az 5-8. igénypontok szerinti eljárás, mely tartalmazza továbbá a speciális karakterek naplózását biztonsági napló készítéséhez.
10. A 9. igénypont szerinti eljárás, mely tartalmazza továbbá a biztonsági napló vizsgáltságát annak eldöntéséhez, hogy a speciális karakterek ellenségesek-e.
11. Az 5-10. igénypontok szerinti eljárás, azzal jellemezve, hogy a hálózati szerver védelme az elektronikus tranzakció során megvalósul.
12. A 11. igénypont szerinti eljárás, azzal jellemezve, hogy az elektronikus tranzakció digitális pénztárca használatával kerül lebonyolításra.
13. Tranzakciós rendszer, mely lehetővé teszi az adathálózaton működő felhasználói számítógép által igényelt pénzügyi tranzakciót, amely rendszernek van:
 - a. tranzakció engedélyezője, és
 - b. biztonsági szervere, amely úgy van beállítva, hogy ellenőrizze, hogy az intelligens token a felhasználó tulajdonában van-e, és hogy digitális megbízólevelet biztosítson a felhasználónak, ha az ellenőrzés sikeres, azzal jellemezve, hogy a tranzakció engedélyező úgy van beállítva, hogy a felhasználói számítógép által igényelt tranzakciót legalább részben az adathálózaton keresztül biztosított digitális megbízólevél alapján engedélyezze.

14. A 13. igénypont szerinti tranzakciós rendszer, melynek van továbbá tranzakciós eszköz szervere.
15. A 13. igénypont szerinti tranzakciós rendszer, melynek van továbbá a digitális hálózaton keresztül a felhasználói számítógéppel kapcsolatban álló pénztárca szervere.
16. A 15. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a pénztárca szerver úgy van beállítva, hogy fogadja a felhasználói számítógéptől érkező tranzakció igényt, kapcsolatba lépjen a kereskedői számítógép rendszerrel, és a felhasználóról a kereskedői számítógép rendszernek információt szolgáltatson.
17. A 13. vagy 16. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a felhasználói számítógépnek van tranzakciós eszköze és olvasója, ahol az olvasó úgy van beállítva, hogy információt szállítson a tranzakciós eszköz és az intelligens token között.
18. A 17. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a tranzakciós eszköz pénztárca kliens.
19. A 13. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a token intelligens kártya.
20. A 13. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a biztonsági szerver és a tranzakció engedélyező számítógép közötti kapcsolat az adathálózattól elkülönített adatkapcsolaton keresztül jön létre.
21. A 17. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy a tranzakciós eszköz a biztonsági szerverrel az adathálózattól elkülönített adatkapcsolaton keresztül kommunikál.

22. A 13. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy az intelligens token rendelkezik digitális megbízólevéllel, amely egyértelműen azonosítja a tokenhez társított felhasználót.

23. A 22. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy az intelligens token használója személyi azonosítót használ a digitális megbízólevélhez való hozzáféréshez.

24. A 13. igénypont szerinti tranzakciós rendszer, azzal jellemezve, hogy az intelligens token egy kibocsátó által kerül kibocsátásra, és hogy a tranzakciós rendszer használatával lebonyolított tranzakció az intelligens token kibocsátója megítélése szempontjából "kártya jelen" tranzakciónak minősül.

25. Digitális pénztárca kliens elektronikus tranzakciók böngésző programmal egyesített digitális hálózaton keresztüli biztosításához, amely digitális pénztárca kliens rendelkezik:

a. pénztárca alkalmazással, amely arra van beállítva, hogy a felhasználói bemenetekre adott válaszként a digitális hálózaton keresztül viszonyt kezdeményezzen a pénztárca szerverrel, és

b. csatlakozó egységgel az olvasó eszközhöz, ahol az olvasó eszköz úgy van beállítva, hogy a felhasználó azonosságának ellenőrzése céljából tokent fogadjon el, és azzal jellemezve, hogy a pénztárca alkalmazás a token használatával működtethető a felhasználó pénztárca szerver felé történő azonosításához és az elektronikus tranzakciók végrehajtásához a pénztárca szerverrel digitális hálózaton keresztül való kapcsolatfelvételhez.

26. A 25. igénypont szerinti digitális pénztárca, mely rendelkezik továbbá aktivátorral a pénztárca szerverhez való hozzáféréshez, azzal jellemezve, hogy az aktivátor az elektronikus tranzakciók befejezéséhez információt cserél a pénztárca szerverrel.

27. A 25. vagy 26. igénypont szerinti digitális pénztárca, azzal jellemezve, hogy a pénztárca alkalmazás továbbá úgy van beállítva, hogy azonosítsa a felhasználót a

pénztárca szervernél legalább részben a digitális pénztárca kliens által a digitális hálózaton levő biztonsági szervertől kapott megbízólevél alapján.

28. A 26. igénypont szerinti digitális pénztárca, azzal jellemezve, hogy az aktivátornak van egy, a felhasználónak mutatott státusz jelzője, amely egy internetes oldal pénztárca szolgáltatásainak lehetőségének felel meg.

29. A 27. igénypont szerinti digitális pénztárca, azzal jellemezve, hogy a pénztárca alkalmazás továbbá úgy van beállítva, hogy a tokentől digitális aláírást szerezzen, továbbá a digitális aláírást a digitális hálózaton keresztül a pénztárca szerver részére biztosítsa.

30. Pénztárca szerver digitális hálózaton keresztül történő tranzakció biztosításához, amely pénztárca szerver rendelkezik:

- a. digitális hálózathoz kapcsolódó csatlakozó egységgel, és
 - b. adatbázissal kapcsolatban álló pénztárca szerver alkalmazással,
- azzal jellemezve, hogy a pénztárca szerver úgy van beállítva, hogy fogadja a pénztárca kienstől érkező tranzakcióra vonatkozó igényt, feldolgozza a pénztárca kienstől kapott megbízólevelet a pénztárca kliens felhasználójának azonosításához, a felhasználó azonosítása után az adatbázisból előhossa a felhasználói információt, és a felhasználói információ használatával a felhasználó részéről befejezze a tranzakciót.

31. A 30. igénypont szerinti pénztárca szerver, azzal jellemezve, hogy a megbízólevélnek van digitális aláírása.

32. A 31. igénypont szerinti pénztárca szerver, azzal jellemezve, hogy a megbízólevélnek van a felhasználó tulajdonában levő token által digitálisan aláírt véletlen kivonata.

33. A 32. igénypont szerinti pénztárca szerver, azzal jellemezve, hogy a kivonatot a biztonsági szerver bocsátja a pénztárca kliens rendelkezésére.

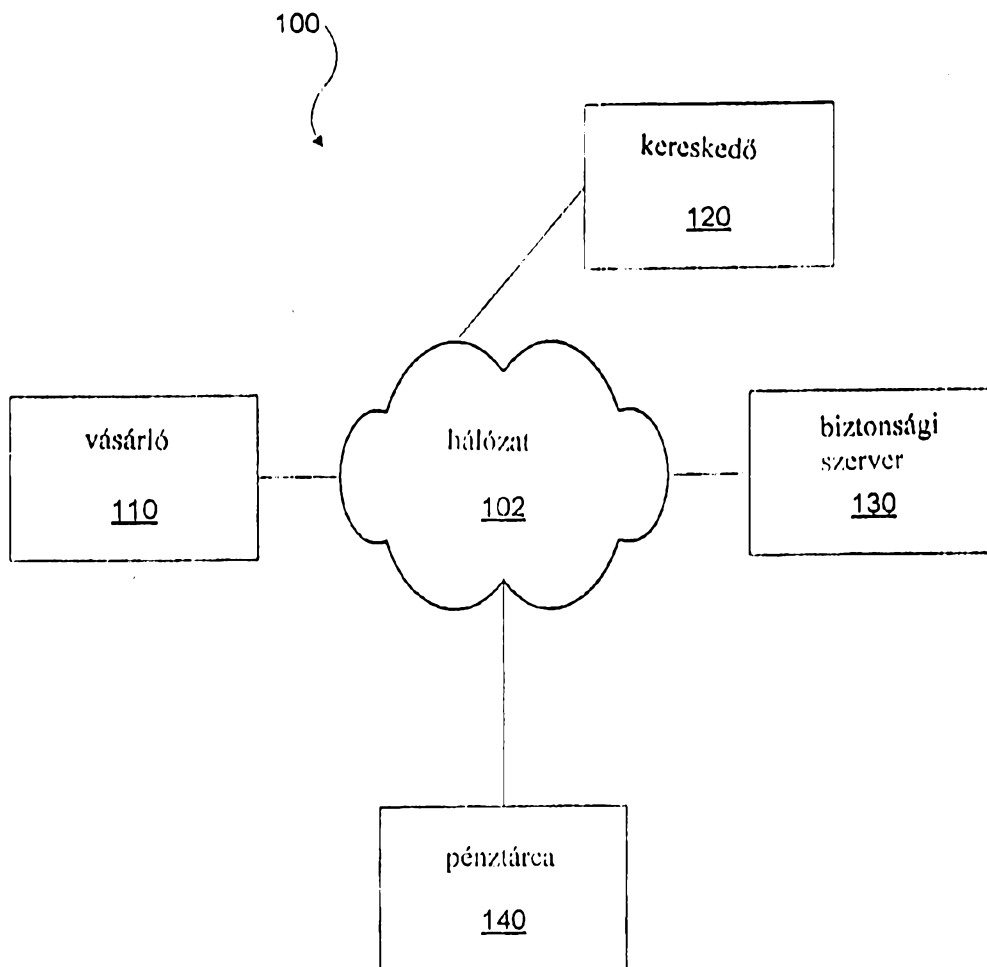
34. A 30. vagy 32. igénypont szerinti pénztárca szerver, azzal jellemezve, hogy a tranzakció felhasználó részéről történő befejezése tartalmazza a kereskedői űrlap felhasználói információval történő kitöltését.
35. Számítógépen implementált eljárás online vásárlás biztosításához, amely eljárás az alábbi lépéseket tartalmazza: azonosítunk a biztonsági szerverrel, fogadjuk a megbízólevelet a biztonsági szervertől, azonosítjuk a kereskedői címet, ahonnan a vásárlást le kell bonyolítani, biztosítjuk a megbízólevelet a pénztárca szerver részére a felhasználó pénztárca szervernél történő azonosításához, a pénztárca szervernél történő sikeres azonosítás után a kereskedő címe és a pénztárca szerver közötti kommunikációt átirányítjuk úgy, hogy a pénztárca szerver a kereskedői címnek vásárlási információt biztosítson a felhasználóról, és fogadjuk a vásárlás eredményének visszaigazolását.
36. A 35. igénypont szerinti eljárás, azzal jellemezve, hogy a megbízólevélnek van digitális aláírása.
37. A 36. igénypont szerinti eljárás, azzal jellemezve, hogy a megbízólevél rendelkezik biztonsági szervertől fogadott adattal.
38. Számítógépen implementált eljárás online vásárlás biztosításához, amely eljárás az alábbi lépéseket tartalmazza: a szervernél fogadjuk a felhasználtól érkező tranzakció kérést, amely kérés rendelkezik kereskedői címmel és megbízólevéllel, ellenőrizzük a megbízólevelet a felhasználó azonosításához, az ellenőrző lépésre adott válaszként előhívjuk a felhasználói információt az adatbázisból, kitöltjük az online űrlapot a kereskedői címnek megfelelően, és biztosítjuk a vásárlás eredményét a felhasználónak.
39. A 36. igénypont szerinti eljárás, azzal jellemezve, hogy a megbízólevélnek van digitális aláírása.

40. A 37. igénypont szerinti eljárás, azzal jellemezve, hogy a megbízólevélnek van biztonsági szervertől fogadott adata.
41. A 38. igénypont szerinti eljárás, azzal jellemezve, hogy a biztonsági szerver a szerverhez kapcsolódik.
42. A 37-39. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy a digitális aláírást intelligens kártya állítja elő.
43. Számítógépen implementált eljárás szolgáltatás elérésének biztosításához, amely eljárás az alábbi lépéseket tartalmazza: fogadjuk a bejelentkezési igényt a felhasználótól,
ellenőrizzük, hogy a felhasználó rendelkezik-e tokennel,
sikeres azonosítás esetén megbízólevelet biztosítunk a felhasználó részére,
fogadjuk a tranzakció igényt a felhasználótól, amely tranzakció igény rendelkezik a megbízólevél legalább egy részével, és
feldolgozzuk a megbízólevél legalább egy részét a szolgáltatás elérésének biztosításához.
44. A 43. igénypont szerinti eljárás, azzal jellemezve, hogy az ellenőrzés lépés tartalmaz lekérdezés-választ.
45. A 44. igénypont szerinti eljárás, azzal jellemezve, hogy a lekérdezés-válasz rendelkezik a token részére biztosított véletlen adattal.
46. A 45. igénypont szerinti eljárás, azzal jellemezve, hogy a lekérdezés-válasz rendelkezik továbbá a véletlen adat digitális aláírásával.
47. A 43-46. igénypontok bármelyike szerinti eljárás, azzal jellemezve, hogy a szolgáltatás pénzügyi tranzakció.

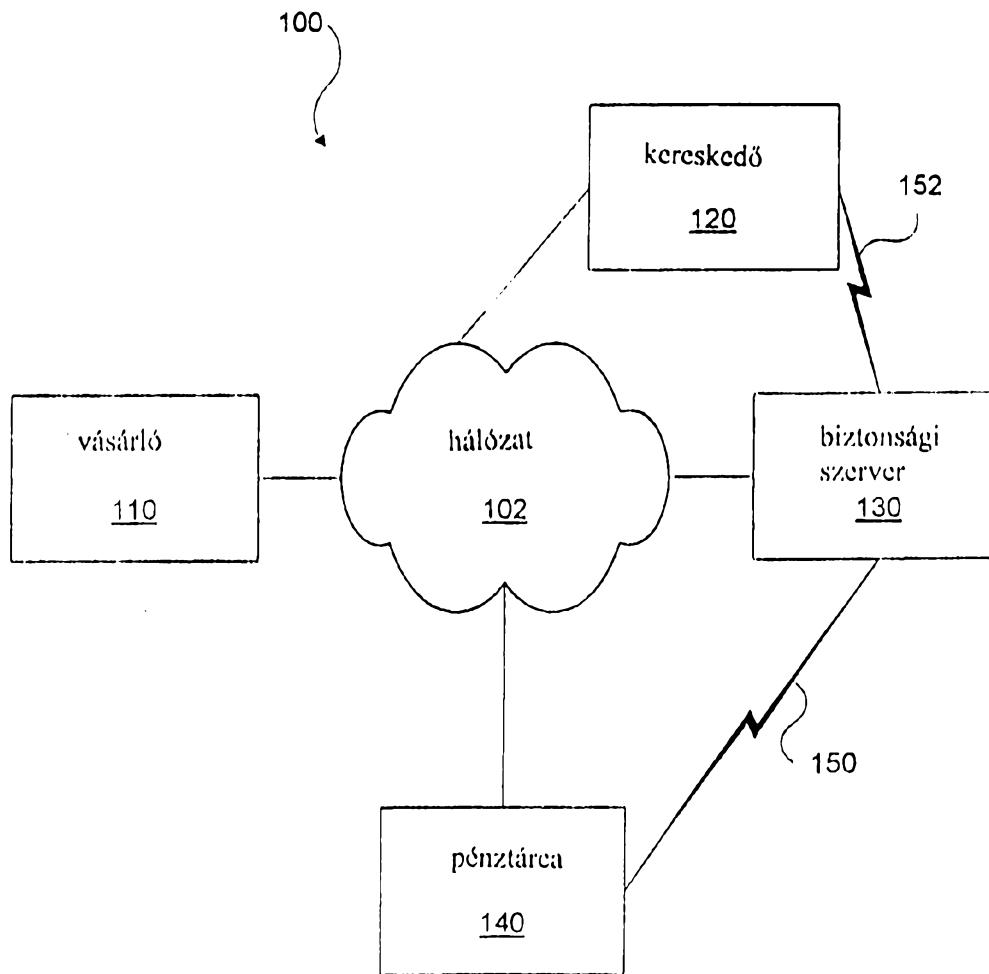
A meghatalmazott

13 rajt 16 lora

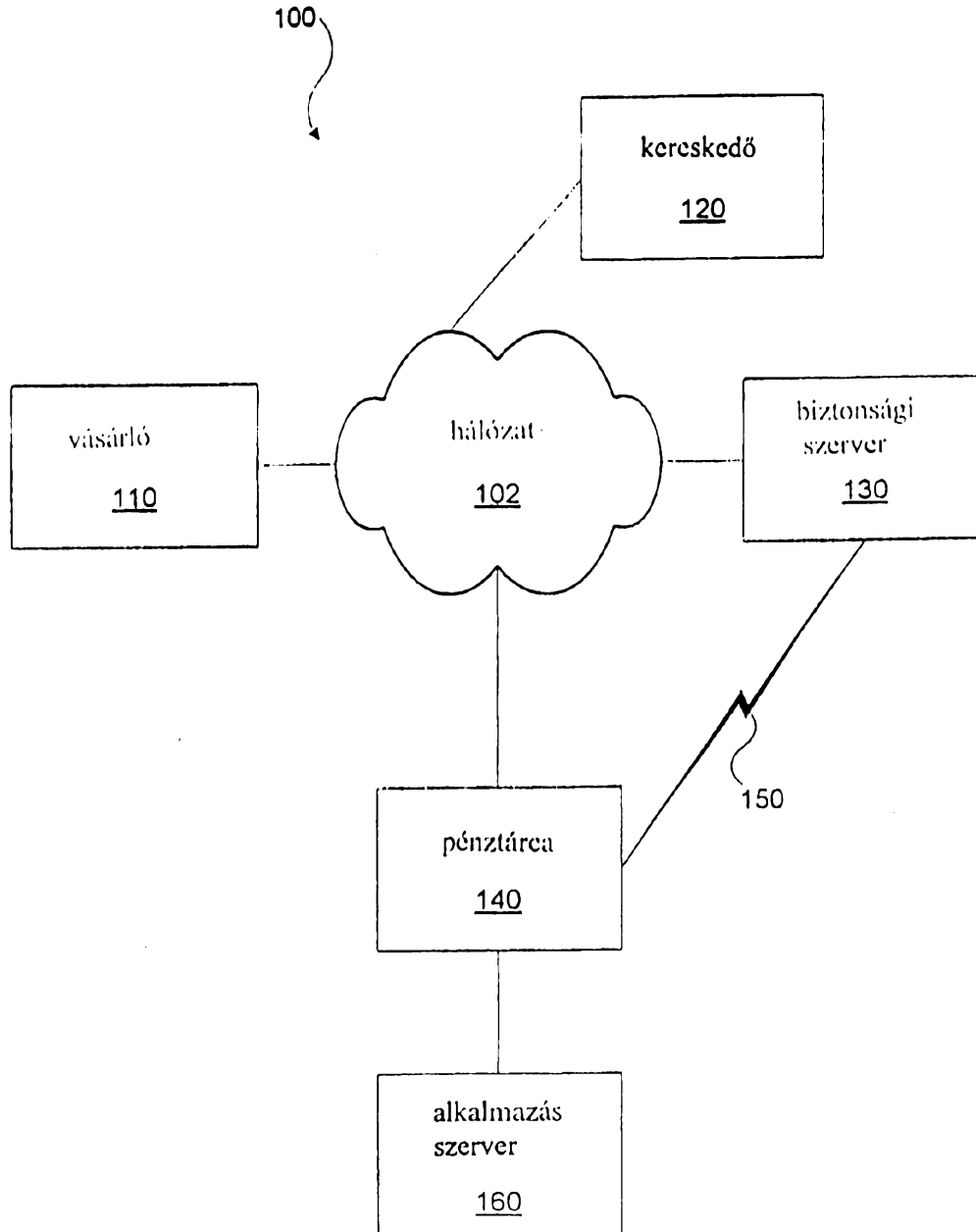
Dr. Bokor Tamás
szabadalmi ügyvivő
az S.B.G. & K. Szabadalmi Ügyvédi Iroda
tagja
H-1062 Budapest, Andrassy út 113.
Telefon: 461-1000 Fax: 461-1099
74.362/BT*44*2002.03.21.



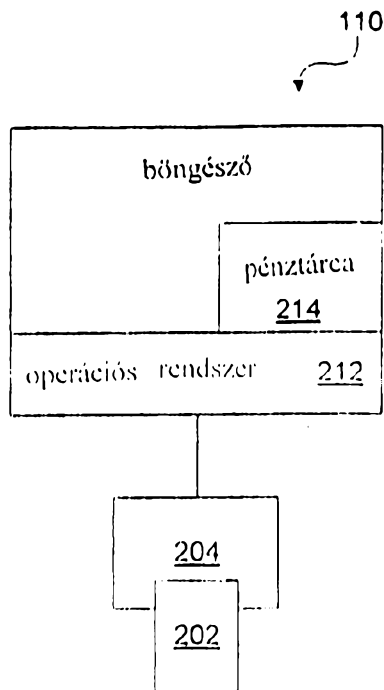
1A. ábra



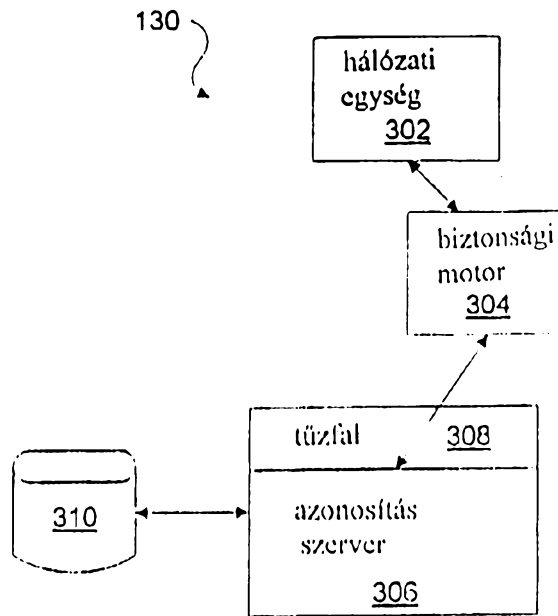
1B. ábra



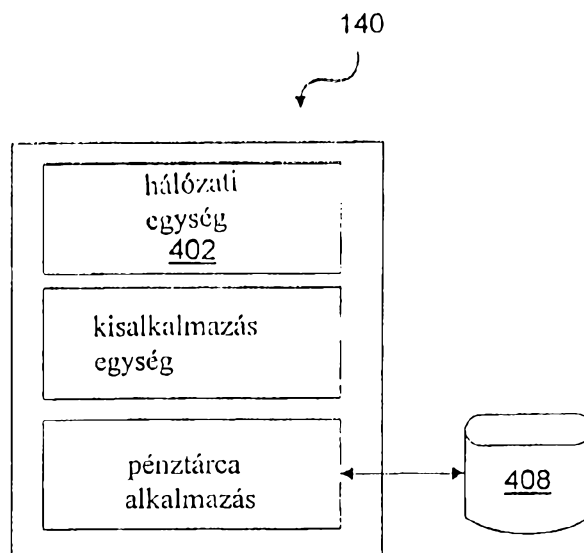
1C. ábra



2. ábra



3. ábra



4. ábra

500

Welcome to MSN.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Size Print Messenger

Address http://www.msn.com/

Links American Express InfoWeb Bug Depot Login Customize Links Deep Thoughts by Jack Handy Free Hotmail

msn.

SEPTEMBER 12
 It's the Information Age:
Hunt Less. Gather more.

Home	Hotmail	Search	Shopping	Money	People & Chat	Passport sign in
Red hot deals on Web TV Plus & MSN						
☐ Autos ☐ Back to School Gear ☐ Boredom Buster ☐ Business ☐ Careers ☐ City Guides ☐ Computers & Web ☐ Entertainment ☐ Games ☐ Health ☐ Home & Loans ☐ Knowledge Center ☐ Love & Relationships ☐ News ☐ Radio & Video ☐ Sports ☐ Travel ☐ Women	Air Tickets Auctions Buy Music	Buy Books Calendar Downloads	Fine Games Greeting Cards Home Pages	Misses Sport Quotes More...	 Go	
Today on MSN						
Soulmates: Romantic or Unrealistic? • Big Brother cast revolt • Eat-free books: a larcy? • Find your TV trove • Top 10 books: 40% off						
Do we want too much? On and off track • Sydney's fastest athletes • Spike Lee: a sourpuss • Fast-track NASCAR chat						
Interactive highlights • Live! Pop with U.L. Cool J • Vote for baseball's MVP • Test your firing I.Q. • Get breaking stock news New music from Limp Bizkit Korn producer A.T. The Drive-In download						
Welcome SHERYL LINDSAY - Microsoft Internet Explorer print... AMERICAN EXPRESS Online WalletSM HELP LOG OUT Use Online Wallet Shopping Directory						
CHANGE Content / Layout / Colors / Zip GET MORE Add scores.						
Worth a Click Local News and Weather						

Internet

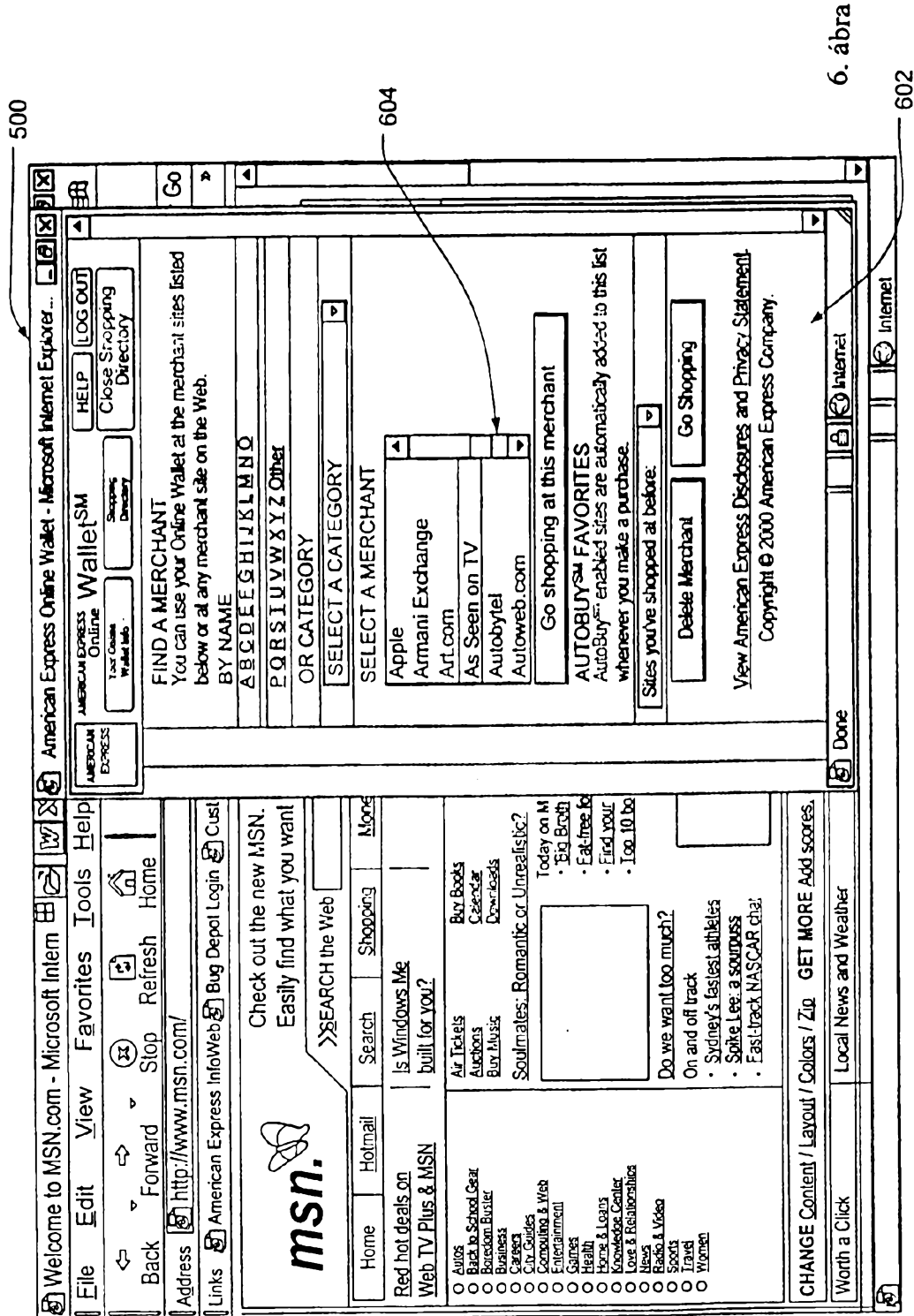
KÖZZÉTÉTELI PÉLDÁNY

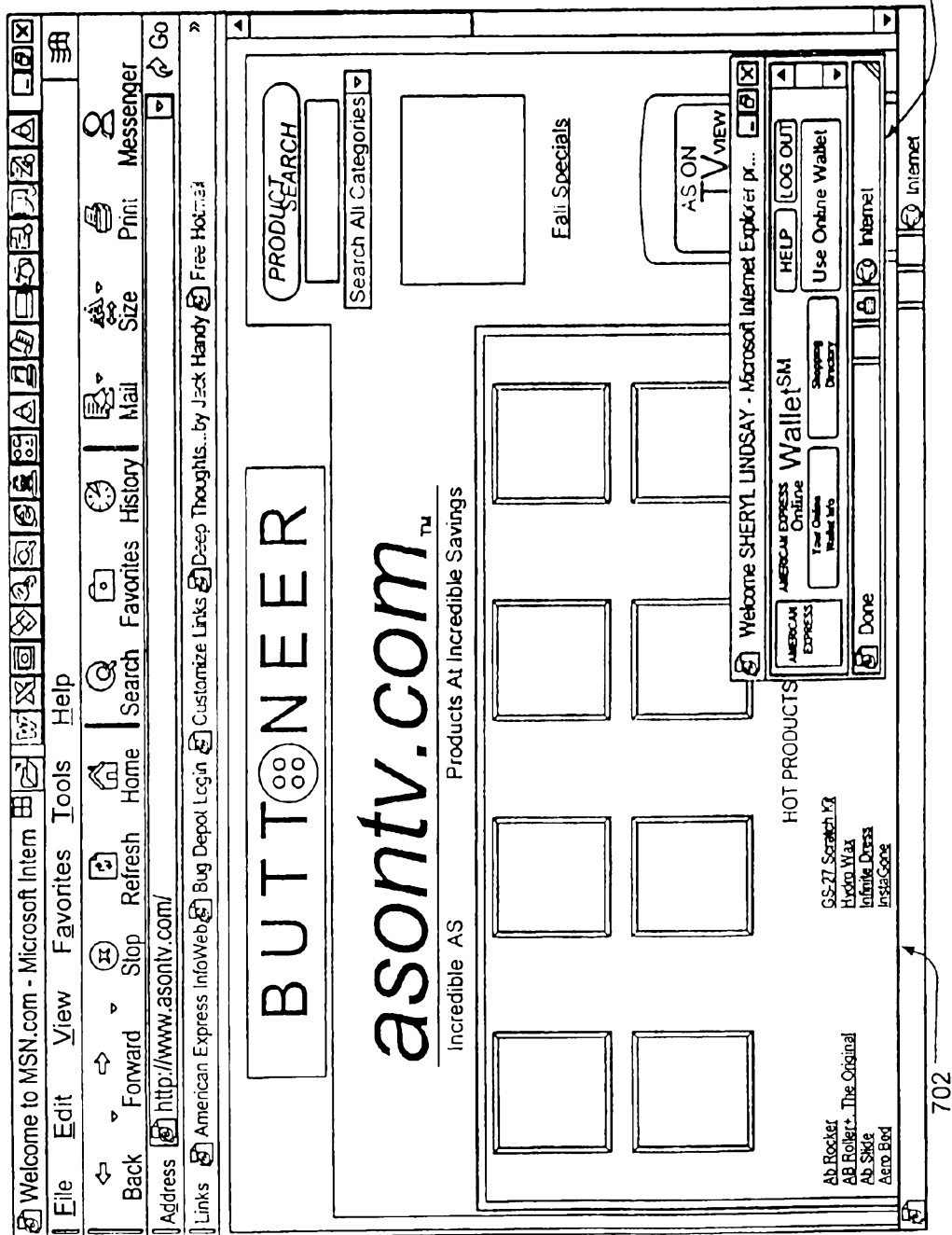
P 02 02 47 1

WO 01/16900

PCT/US00/23817

6 / 13





7. ábra

502

702

KÖZZÉTÉTELI PÉLDÁNY

P 02 02 47 1



WO 01/16900

PCT/US00/23817

8 / 13

As seen on TV - Order Form - Microsoft Internet Explorer... American Express Online Wallet - Microsoft Internet Explorer...

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home

Address <http://www.asontv.com/>

Links American Express InfoWeb Bug Depot Login Cust

Incredible AS ON

This is the "As Seen On TV" order form. Please click the "Preview Order" button to see the detailed options to select the free gift (with purchases over \$50).

We do not ship to PO Boxes.

You may also order by calling (800) ENTE 0702.

1. Billing Information: (If you are paying with a credit card, your billing address must be the same as the address on your credit card.)

Name:

Address:

Apt./Suite#

AMERICAN EXPRESS Online Wallet

HELP LOGOUT

Your Online Wallet Info

Close Autobuy

Go

CHECK OUT: Step 1 of 3

Your Online Wallet is beginning the AutobuySM function, this will take you through a 3-step process.

Please make sure the information you've provided for As Seen on TV is correct. Then click "continue" to go to step 2.

Credit Card:

Shipping Address:

Billing Phone:

Billing Email:

Shipping Phone:

Additional Shipping Information: Domestic orders will be sent via UPS unless Next-Day Service is selected. Domestic orders for states or territories outside of the US continent are automatically sent via Next-Day Service.

I want Next-Day Service: ☐

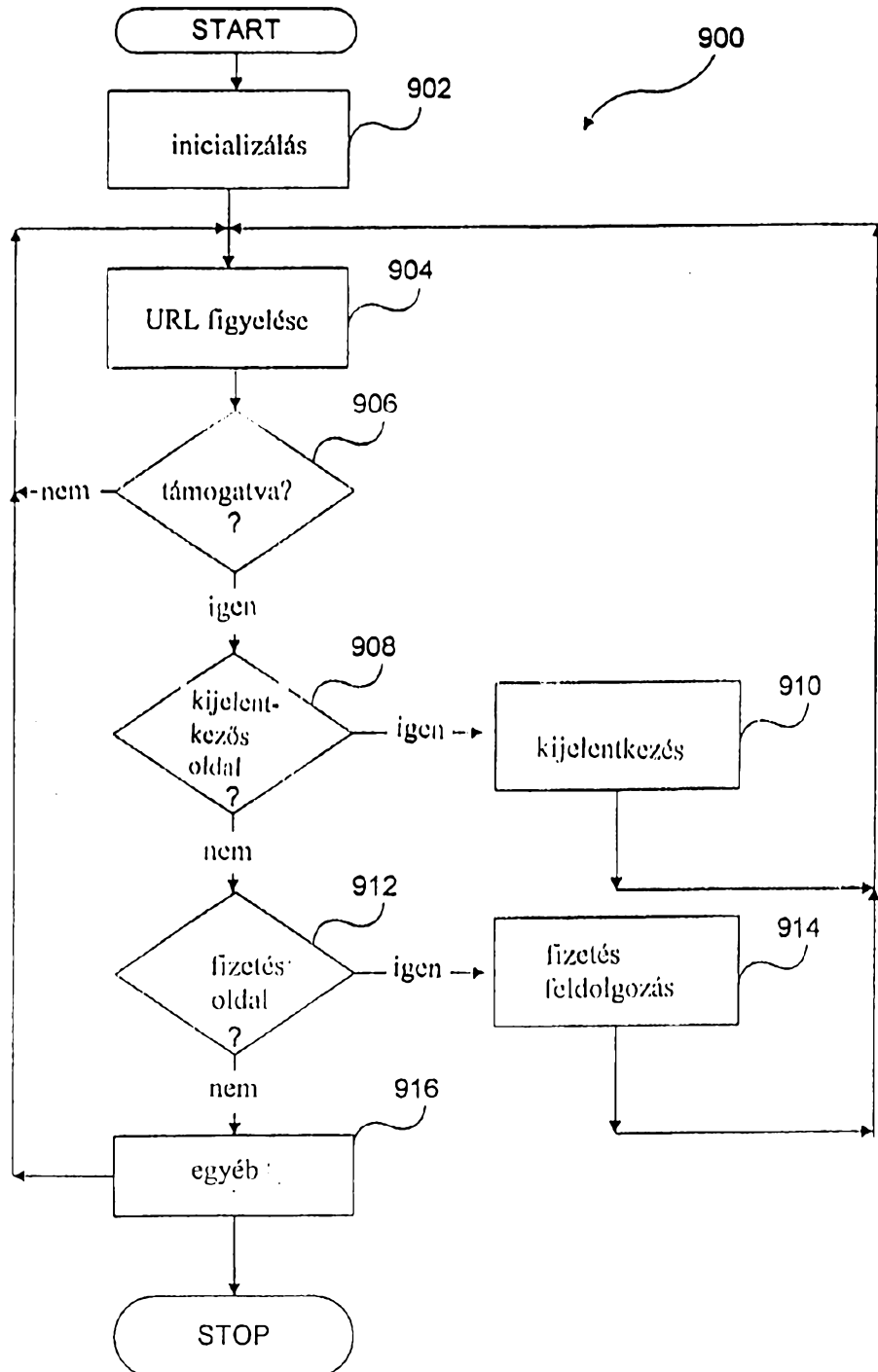
Done

Internet

8. ábra

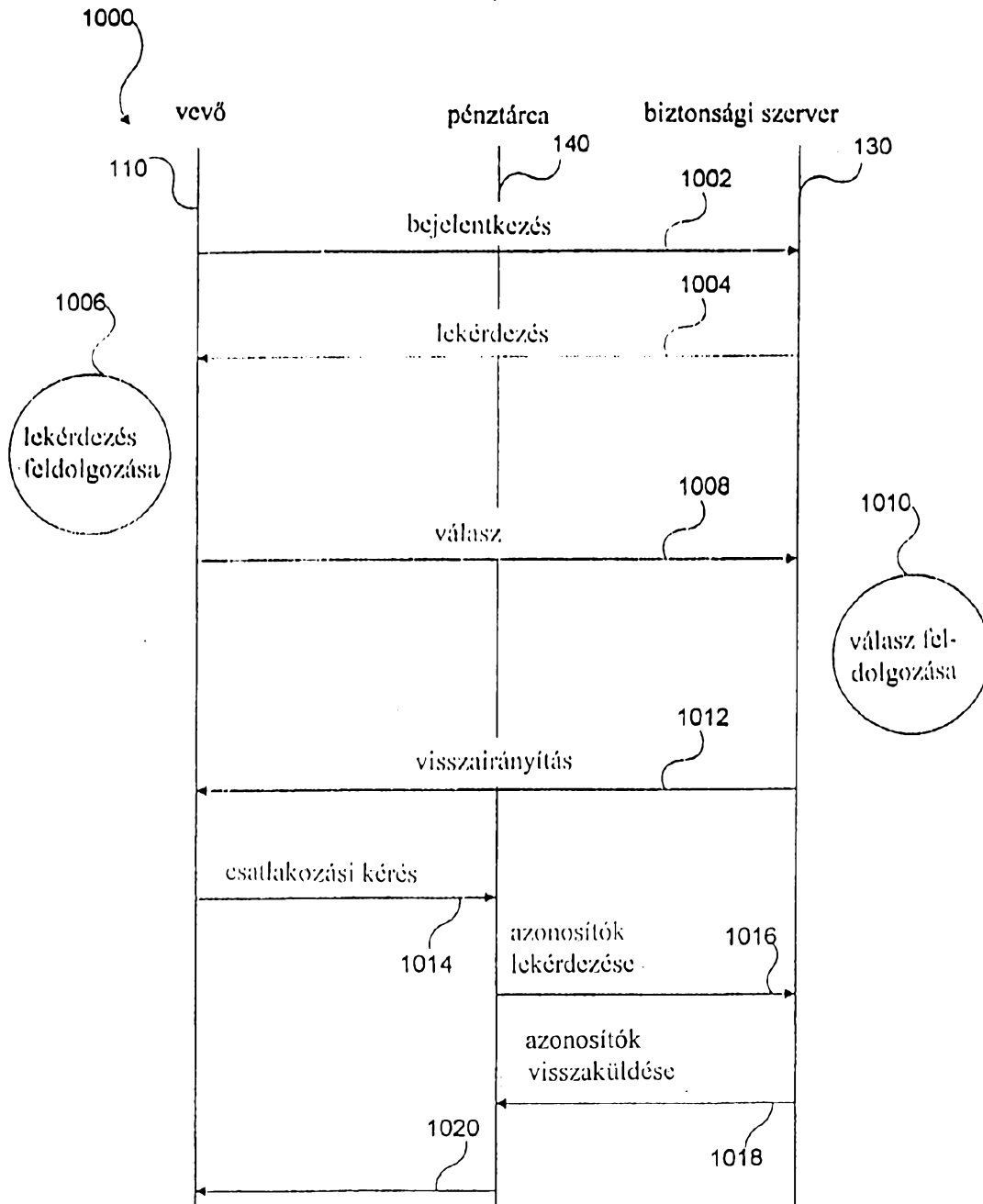
802

702

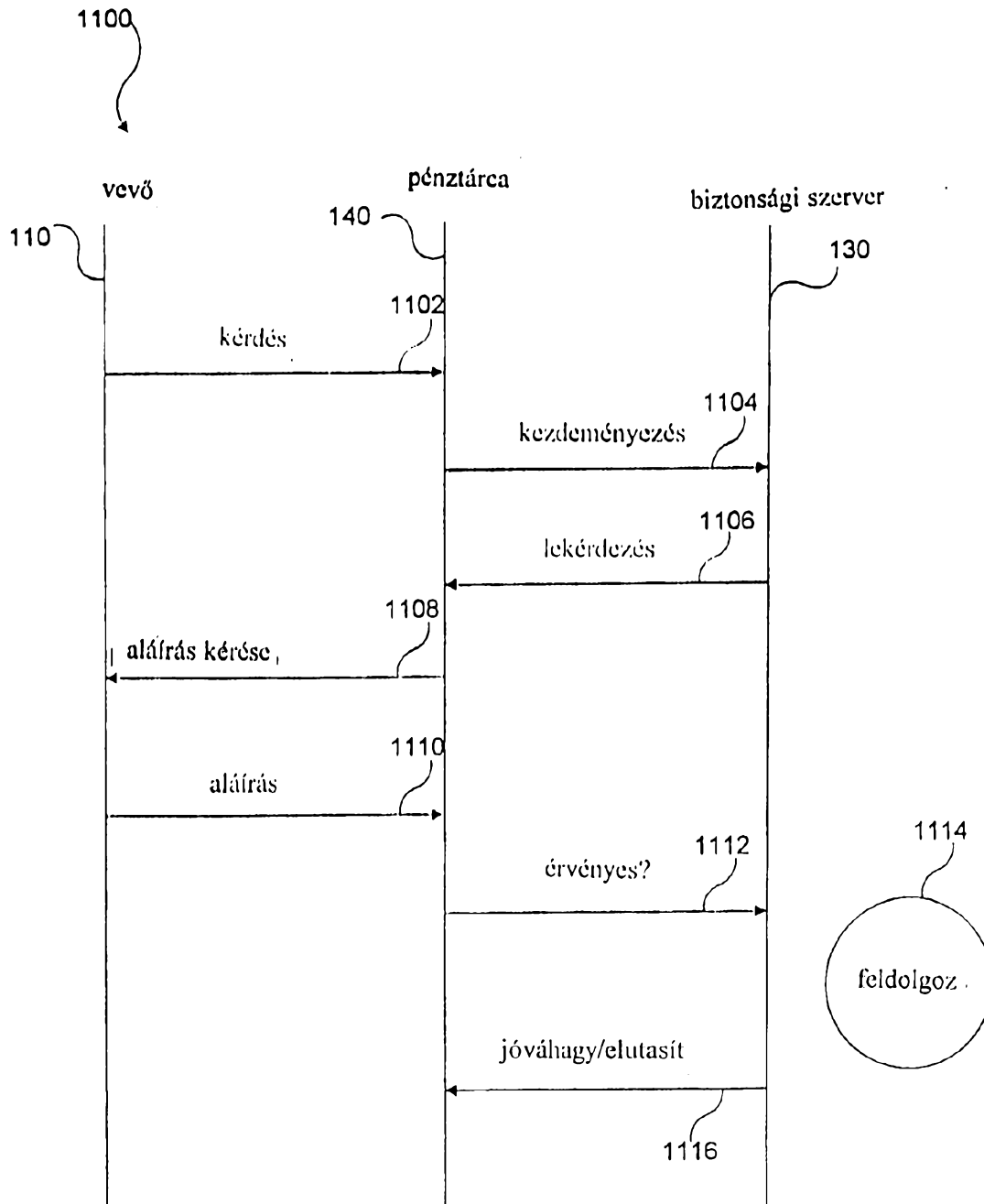


9. ábra

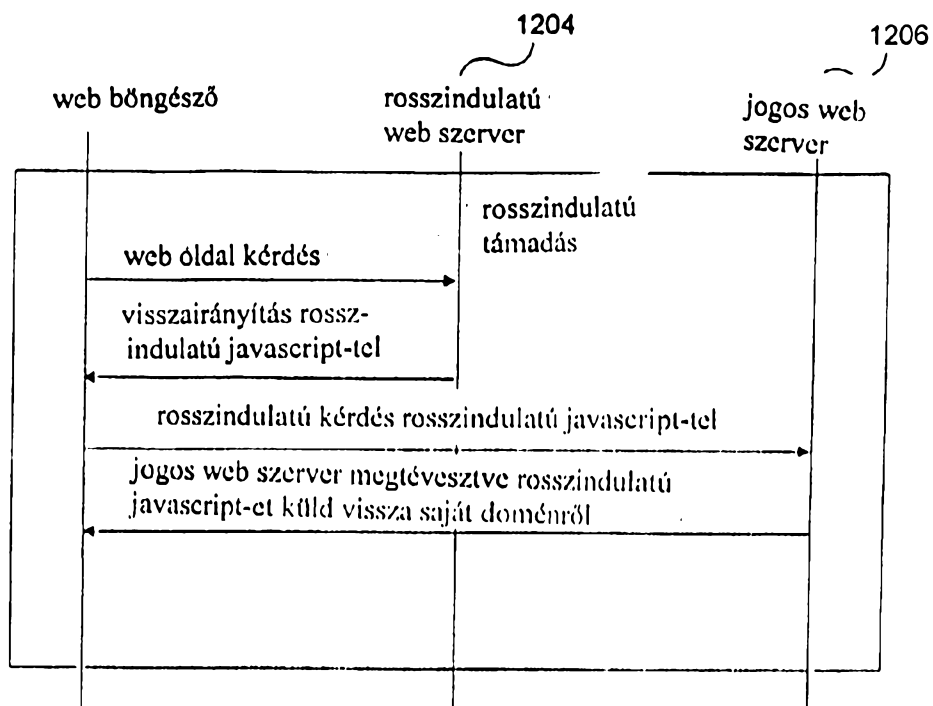
10 / 13



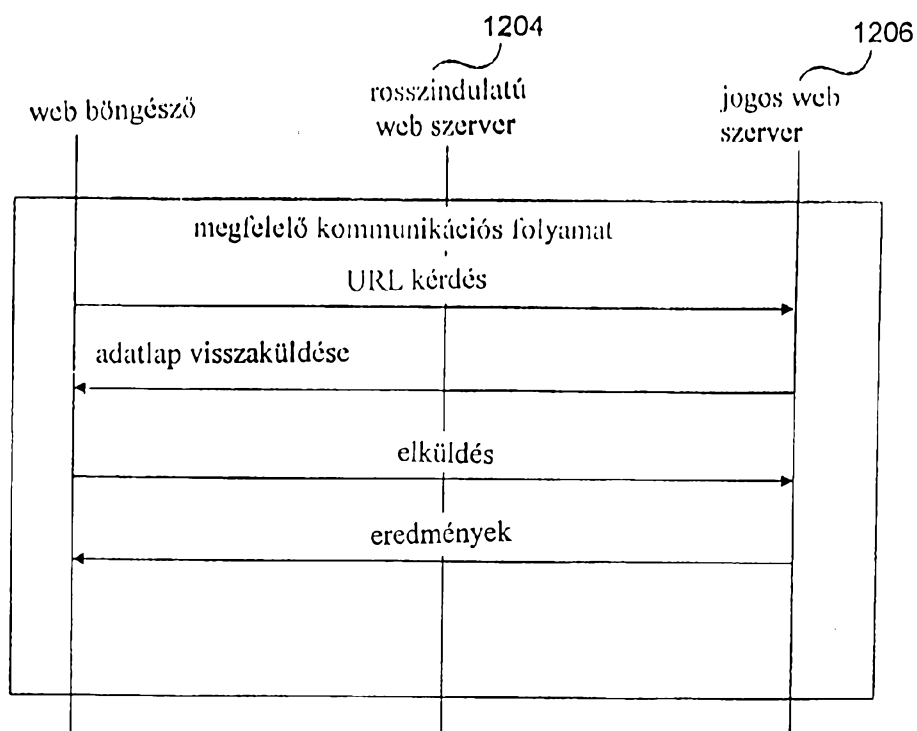
10. ábra



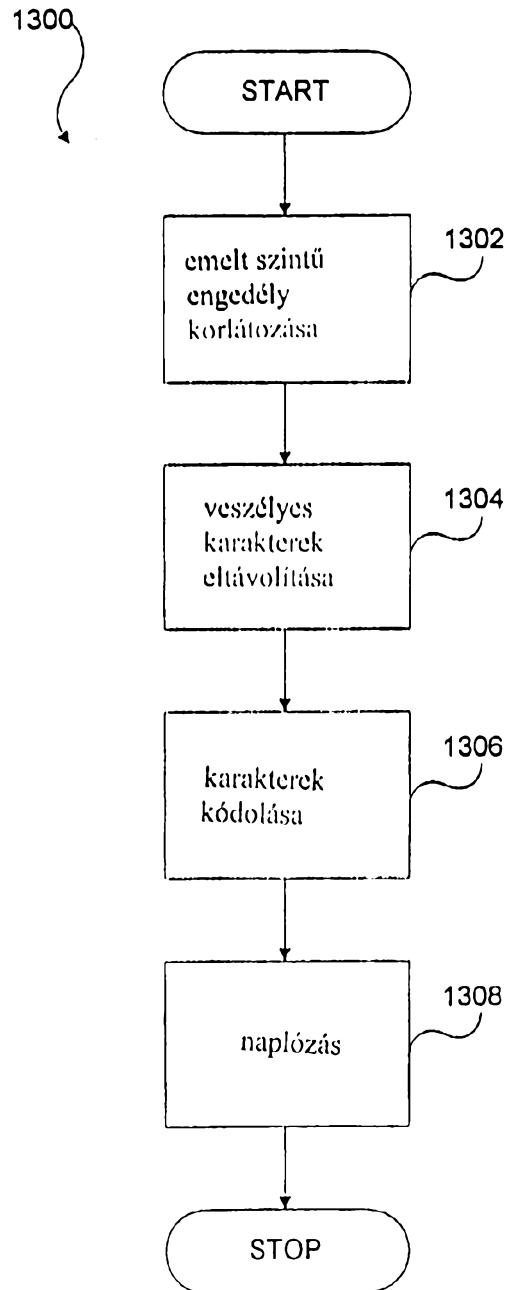
11. ábra



12A. ábra



12B. ábra

KÖZZÉTÉTELI
PÉLDÁNY

13. ábra