Szakdolgozat

Készítette:
Bökönyi Sándor

Debrecen
2010

Debreceni Egyetem

Informatikai Kar

A SET- alapú fizetési mód

Témavezető:
Dr. Huszti Andrea
Egyetemi adjunktus

Készítette:
Bökönyi Sándor
Gazdaságinformatikus (Bsc)

Debrecen
2010

Tartalomjegyzék

Bevezetés

A technológiák és azon belül a számítástechnika fejlődése a személyi számítógépek gyártási költségeinek csökkenését vonta maga után. Ennek köszönhetően, az árak csökkenésével egyre több háztartásban jelent meg, nem csak mint munkaeszköz, hanem mint szórakoztató elektronika. Az emberek megbarátkoztak a számítógéppel, életük szerves részét alkotja annak használata. Az internet terjedésével az üzletemberek annak üzleti lehetőségeit is felfedezték és haszonszerzés céljából is elkezdődött a felhasználása. Megjelentek a különböző elektronikus üzleti modellek. Az e-business elnevezés az internetes kommunikációtól, az adat átvitelen, az elektronikus beszerzésen, a pénzügyi tranzakciókon, az aukciókon, a távfelügyeleten és a kontrollon keresztül egy sor olyan tevékenységet jelöl, amely digitalizált kommunikáció segítségével megy végbe. Az e-business tehát nem csupán az elektronikus úton történő vételt és eladást, hanem a vevők részére nyújtott szolgáltatást és az üzleti partnerekkel történő együttműködést is jelenti. Ezért az üzleti partnerek közötti olyan tranzakcióként, vagy kommunikációként fogható fel, amelyben az információcsere nem fizikai, hanem elektronikus úton megy végbe. Az e-business része az elektronikus kereskedelem.

Az elektronikus kereskedelem (e-commerce) hat síkon jelentkezik. Megjelenik a cégek egymás közötti üzletkötései során (Business-to-Business), a vállalkozások és a fogyasztók között (Business-to-Consumer), illetve ide sorolják még a cégek és a közigazgatás (Businessto-Administration), a fogyasztók egymás közötti (Consumer-to-Consumer), a közigazgatás és a fogyasztó között létrejövő (Consumer-to-Administration) és a közigazgatási szervek egymás között létrejövő (Administration-to-Administration) kapcsolatait is.[4] De esetleg ide tartozhat még a vállalat és az alkalmazottak közötti online kapcsolat is (Business-to-Employee). [3]

A vásárlás csakúgy, mint egy átlagos boltban a fizetéssel zárul. Erre a célra ma már több elektronikus forma is rendelkezésre áll.

1996-ban a VISA és a Mastercard bemutatta közös fejlesztésű elektronikus hitelkártya tranzakciókkal kapcsolatos technológiáját. Ez lecserélte az addig versenyző szabványokat. 1997-ben a együttműködve megalkották a SET nevű protokollt.

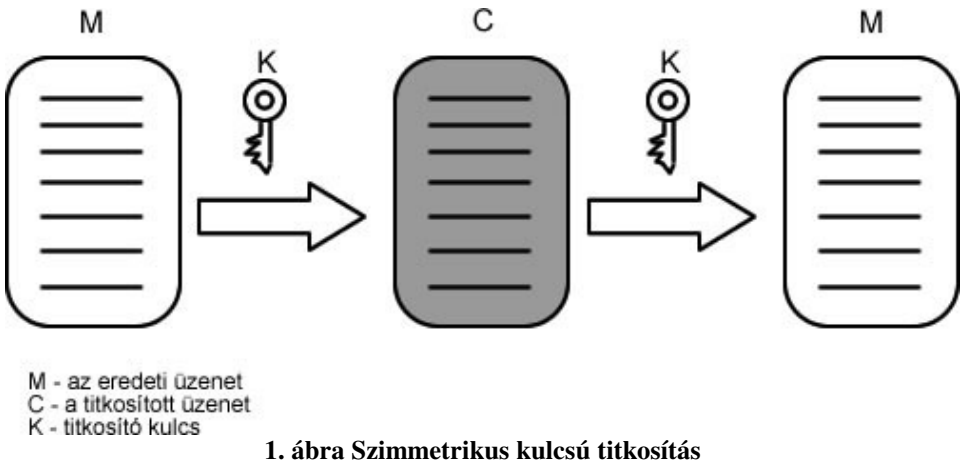
Ebben a rendszerben a fizetési adatok nem kerültek sem a kereskedő sem más személyek tudtára, a fizetési lebonyolítása egy online fizetési kapu segítségével zajlik. [2]

Annak ellenére, hogy mai napig ezt a szabályrendszert tartják az eddig használt legbiztonságosabbnak, mégsem terjedt el.. Miért nem? Az embereknek nem fontos adatainak biztonsága? Vagy technológiai fejlettség nem engedi? Vagy az árával van a probléma? Mi az, ami helyette megfelel? Ezekre a kérdésekre keresem a választ dolgozatom hátralévő részében.

1. Általános tudnivalók az alkalmazott titkosítási technikákról

1.1. Szimmetrikus kulcsú (titkos-kulcsú) kriptográfia

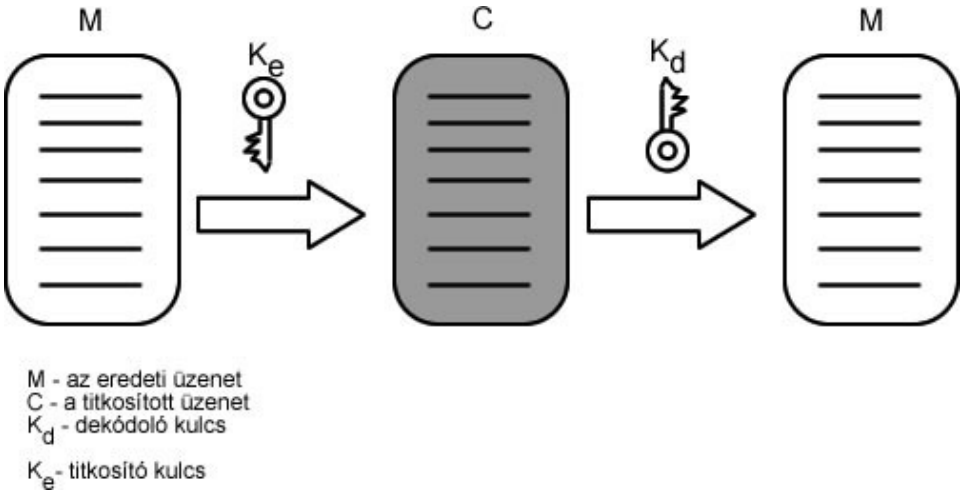
Ebben az esetben a dokumentum titkosítására és a titkosított dokumentum visszafejtésére használt kulcs megegyezik vagy a kódolóból a dekódoló kulcs könnyen meghatározható. A módszer legfőbb előnye a gyorsaság, ám a titkos kulcs cseréjéről a feleknek gondoskodniuk kell. Gyorsasága miatt nagyobb méretű dokumentumok titkosítására is alkalmas. A szimmetrikus kulcsú kriptográfiát alkalmazó rendszerek közül kiemelendő a DES, TripleDES és az AES. [1]



1. ábra Szimmetrikus kulcsú titkosítás

1.2. Aszimmetrikus kulcsú (nyilvános-kulcsú) kriptográfia

A módszer lényege, hogy a titkosító és a visszafejtéshez használt kulcs nem egyezik meg ill. a kódolóból a dekódoló csak „nehezen” meghatározható. Magas műveleti igénye miatt lassú, így főleg kisebb dokumentumok titkosítására alkalmazzák. Nagy előnye viszont, hogy kódoló kulcs nyilvános, így a titkosító kulcs cseréjéről nem kell gondoskodni a feleknek. A dekódoló kulcs viszont titkos így a titkosított üzenetek visszafejtésére kizárólag a titkos kulcs ismeretével rendelkező fél képes. Az aszimmetrikus kulcsú kriptográfiát alkalmazó rendszerek közül kiemelendő az RSA.



2. ábra Aszimmetrikus kulcsú titkosítás

1.3. Digitális boríték

Ahhoz, hogy kommunikációnkat gyorsan tudjuk titkosítani, szimmetrikus kulcsú kriptorendszerre van szükségünk. Ebben az esetben viszont gondoskodni kell a kulcscseréről. Aszimmetrikus esetben igaz, hogy nem szükséges kulcscsere, viszont a folyamat nagy számítási igénye miatt meglehetősen lassú. A digitális boríték technológia a két kriptográfiai módszer ötvözete. A generált szimmetrikus kulcsot a címzett nyilvános kulcsával aszimmetrikus módon titkosítva elérhetővé teszi a küldő a fogadó számára, lehetővé téve a titkos kulcsú titkosítás alkalmazását.[1]

A módszer alkalmazásának lépései:

1. A küldő titkos kulcsot *(k)* generál, amivel titkosítja a dokumentumot *(M)*, a titkosított dokumentum jelölése: $\{M\}_k$
2. A titkos kulcsot a fogadó nyilvános kulcsával (K_B) titkosítja a titkosított kulcs jelölése: $\{k\}_{K_B}$
3. A titkosított dokumentumot és a titkosított kódoló kulcsot a küldő elküldi a fogadónak
4. A fogadó dekódoló kulcsával meghatározza a titkos kulcsot és visszafejti a kapott titkosított dokumentumot

Jelölése: $[M]_{K_B} = \{k\}_{K_B} | \{M\}_k$

1.4. Digitális aláírás

A digitális aláírást egyrészt a küldő azonosítására, másrészt a dokumentum sértetlenségének ellenőrzésére alkalmaznak. A digitális aláírás alapját az aszimmetrikus titkosítás adja. A titkos kulcsot használjuk aláírásra, míg a nyilvános kulcsot az ellenőrzésre. [1]

Az aláírás folyamata a következő:

1. Az aláírandó dokumentumról *(M)* a küldő lenyomatot *(h(M))* készít egy nyilvános *h()* hash függvény alkalmazásával
2. A lenyomatot az aláíró titkos kulccsal $(K_i^{(sig)})$ aláírja
3. Az aláírt dokumentumot és az eredetit elküldi a fogadónak

Az ellenőrzés folyamata:

1. A fogadó a kapott üzenetről lenyomatot készít
2. A nyilvános kulccsal az aláírt üzenetet ellenőrzi, megkapva ezzel a küldő által készített lenyomatot
3. Az általa készített lenyomatot és a kapott lenyomatot összehasonlítja
4. Ha megegyeznek, akkor a küldő azonosítása megtörtént, továbbá meggyőződtünk arról is, hogy az átküldött üzenet sem sérült

Jelölése: $\mathrm{sig}_{K_i^{(sig)}}(M) = M \mid \{h(M)\}_{K_i^{(sig)}}$

1.5. Kettős digitális aláírás

A következőkben tárgyalt fizetési rendszer egyik jellegzetességének mondhatjuk ezt a technológiát. Egyszerre lát el azonosító, ellenőrző és titkosító feladatot.

Jelölése: $\mathrm{dsig}_{K_i^{(sig)}}(M_1, M_2) = M_1 \mid h(M_2) \mid \{h(h(M_1) \mid h(M_2))\}_{K_i^{(sig)}}$

Az aláírás folyamata:

1. A küldő a két dokumentumról (M_1,M_2) lenyomatot készít
2. A két lenyomatot összefűzi és az eredményről szintén lenyomatot ($h(h(M_1) \mid h(M_2))$) készít egy nyilvános *h()* hash függvény alkalmazásával

3. Az így kapott adathalmazt $K_i^{(sig)}$ aláíró kulcsával aláírja
4. Az üzenethez hozzáfűzésre kerül még az eredeti M_1 üzenet és az M_2 lenyomata ($h(M_2)$) is

Az ellenőrzés folyamata:

1. A fogadó az M_1 dokumentumról lenyomatot készít és összefűzi a kapott M_2 üzenet lenyomatával
2. Az eredményül kapott adatokról lenyomatot készít
3. A küldő nyilvános kulcsával ellenőrzi az aláírást úgy, hogy összehasonlítja az aláírás által tartalmazott és a kapott lenyomatokat
4. Ha megegyeznek, akkor egyrészt a küldő azonosítása megtörtént, másrészt az üzenet sértetlensége is bizonyításra került

Használata akkor javasolt, mikor egy dokumentumot két címzettnek kell elküldeni, viszont nem mindkét címzett láthatja azt teljes terjedelmében. Az aláírással csak az egész dokumentum egyik felét küldjük el eredeti formában, a fennmaradónak kizárólag a lenyomatát kapja meg a címzett. Az esetlegesen felmerülő viták kezelése érdekében kapja meg a másik fél a rá nem tartozó részek lenyomatát. Ha valamelyik fél hamisítani próbálná a dokumentumot, akkor másik fél, aki megkapta a rá vonatkozó részt, ellenőrizni tudja, hogy az eredeti dokumentumot mutatják-e be neki. Ezt az alkalmazott hash függvény teszi lehetővé. A hash függvények egyirányú tulajdonságából adódóan a lenyomatból nehéz meghatározni az eredeti dokumentumot. Ez garantálja az aláírás biztonságát. [1]

2. Az elektronikus fizetési rendszerek

Az internetes fizetési rendszerek legfőbb kérdése biztonság. A biztonságot itt az jelenti, hogy a fizetési rendszer résztvevőinek nem kell attól félniük, hogy pénzt veszítenek vagy valaki számukra bizalmas információhoz jut. Ezért a rendszerek tervezőinek mindhárom oldal (vásárló, kereskedő, bank) biztonsági elvárásait is figyelembe kell venni, és törekedni kell olyan kialakítására, hogy a felek biztonsága egyáltalán ne függjön a másik két fél viselkedésétől. A fő biztonsági szempontok a következők:

- Azonosítás/Authorizáció: ez azt jelenti, hogy a bank ügyfele pénzének költését, csak a tulajdonos megfelelő felhatalmazása esetén engedi. Ehhez szükséges a folyamat során egy felhatalmazás, amely biztosítja, hogy a jóváhagyás a törvényes tulajdonostól érkezett. Megbízhatóan kell ezért az ügyfelet azonosítani, melyre számos módszer létezik napjainkban: személyes telefonos jóváhagyás, jelszó, vagy PIN kód alapú, biometriai azonosítás vagy akár a digitális aláírás.
- Adatok titkossága és hitelessége: a tranzakcióban nem érintett felek számára a tranzakciós adatokat el kell rejteni. Ennek érdekében kriptográfiai algoritmusokat alkalmaznak. Biztosítani kell a folyamat során elküldött üzenetek hitelességét és sértetlenségét is. A fogadónak meg kell tudni állapítani, hogy a kapott üzenetet ténylegesen a megjelölt küldő küldte-e, ill. hogy nem sérült-e az üzenet. Erre ellenőrzőösszeg-képző és digitális aláírás technikák állnak rendelkezésre.
- Rendelkezésre állás és megbízhatóság: a rendszer folyamatos elérhetősége alapkövetelmény. Ez nem mindig teljes mértékben lehetséges, mivel az internetes infrastruktúra, amire épülnek, egy több hálózatból létrejött kommunikációs csatorna, melynek meghibásodása vagy túltelítettsége esetén a rendszer elérhetősége nem biztosított. Online rendszerek esetén ilyen esetben teljes elérhetetlenség lép fel, amely minden tranzakciót meghiúsít. Ennek elkerülése érdekében tartalékrendszer kiépítése ajánlott. A fizetési folyamat végrehajtása során vagy minden tranzakciónak végre kell hajtódni vagy egyiknek sem. A gyakorlatban azonban ez nem mindig így van. Előfordulhat, hogy egy folyamat megszakadhat egy külső ok miatt. A megszakadt műveletek nem szabad, hogy kárt okozzanak egyik résztvevő számára sem. A félbeszakadt tranzakciók kezeléséről gondoskodni kell.

- Személyes adatok védelme és anonimitás: biztosítani kell a résztvevőket arról, hogy a tranzakció során személyes vagy rendelési információi kizárólag az arra illetékes félhez kerülhessen. Anonimitást biztosító rendszerekben még a vásárló neve is ismeretlen marad a kereskedő előtt. [2]

2.1. Elektronikus fizetési rendszerek (EPS) csoportosítása

Egy online tranzakciónak három szereplője van: a vásárló, a kereskedő és a bank. A bank lehet valódi bank, hitelkártya társaság, vagy bármely olyan társaság, mely hitelesíteni tudja a vásárlást fedezeti szempontból

A fizetési rendszerek osztályozása történhet az alábbi szempontok alapján [1]:

- kredit vagy debit
- online vagy offline
- azonosított vagy anonim
- kártyát vagy elektronikus pénzt használó vagy mikrofizetés

2.1.1. Kredit vagy debit

A debit (betéti) rendszer működése az átlagos banki csekkszámlához hasonló. Ahhoz, hogy pénzt költhessünk, szükségünk van a számlánkon lévő megfelelő fedezet biztosítására. Ilyen amikor bankjegy kiadó automatából pénzt veszünk fel mágnescsíkos, PIN kódos bankkártyával, csoportos beszedés automatikusan kiegyenlítettjük a számláinkat vagy egyszerűen egy üzletben készpénz helyett ezen módon fizetünk. A pénzintézetek többsége lehetőséget nyújt betéti számlánk elektronikus kezelésére is, ahol akár otthonról átutalásokat, vásárlásokat is intézhetünk. A kredit (hitel) kártyákkal is elvégezhetőek ezek a műveletek, viszont a fedezet forrásában jelentős különbség van. A hitelkártya használatának esetében a fedezet nem feltétlen áll a vásárló rendelkezésére a vásárlás időpontjában. Tulajdonosa egy előre meghatározott hitelkerettel rendelkezik, melynek keretein belül költekezhet. A debit számlára épülő kártyát viszont - alapértelmezetten - kizárólag a betéti számlán rendelkezésre álló számlán összeg erejéig alkalmazhatja. Online fizetés ezzel a kártyatípussal viszont sokkal egyszerűbb, mivel a csak a kártya érvényessége és a fedezetül szolgáló hitelkeret kerül ellenőrzésre,

2.1.2. Online vagy offline

Offline vásárlás során a tranzakció a két fél a vásárló és a kereskedő között jön létre, harmadik fél beiktatása nélkül. A vásárló továbbítja a megfelelő pénzt a kereskedőnek, aki maga győződik meg annak hitelességéről. Legegyszerűbb példa erre hétköznapi a vásárlás során történő készpénzes fizetés.

Online vásárlás során a két fél mellé egy harmadik a bank is megjelenik. Legfőbb szerepe a vásárlás során keletkezett kötelezettség kiegyenlítésének jóváhagyása. Online esetben a vásárló készít egy üzenetet, amely tartalmazhatja a vásárlás információit, a kereskedő és a vásárló nevét és bankszámlaszámát, a pénzösszeget, a vásárlás időpontját és az üzenetre a vásárló által adott digitális aláírást. A felsorolt elemek nagy része, főként a digitális aláírás opcionális, rendszerenként változó, mint az is hogy melyik félnek és hogy mennyi üzenet kerül elküldésre. A kereskedő a bank pozitív visszajelzését követően elfogadja a vásárlást és teljesíti a rá vonatkozó kötelezettségeket, tájékoztatva az ügyfelét is.

2.1.3. Azonosított vagy anonim

Azonosított esetben a felhasználó vásárlásai teljesen nyomon követhetőek. Anonim rendszerekben viszont a vásárló adatai titokban maradnak, így itt nem követhetőek a tranzakciók. Az azonosított és anonim rendszerek tovább kategorizálhatóak kommunikációjuk online illetve offline jelleg szerint:

- Azonosított online elektronikus fizetési rendszereknél mind a kereskedő, mind a bank azonosítja a vásárlót. A kereskedő a fizetés során kapcsolatba lép a bankkal, várva visszaigazolását. Ilyen debit és kredit kártyás rendszerek találhatóak a legtöbb ma üzemelő webáruházban.
- Anonim online fizetési rendszer esetén a vásárló ismeretlen marad a kereskedő számára. A kereskedő csak a vásárló gépe által aktuálisan használt IP címét látja. A kereskedő a banktól kéri a visszaigazolást itt is. A bank számára viszont a vásárló be van azonosítva, így az tudja itt is követni a tranzakciókat.
- Azonosított offline rendszer estén a kereskedő és a bank is beazonosítja a vásárlót. A banki kiszolgáló jelen estben viszont online nem elérhető vagy elérése kényelmetlen. Tipikus példa az elektronikus chipkártyák használatával történő fizetés. A kártya tárolja az elektronikus pénzt és gondoskodik annak fizikai és algoritmikus védelméről.

- Anonim offline rendszer esetén a vásárlót sem a kereskedő, sem a bank nem azonosítja. A kereskedő kizárólag a vásárló gépének IP címét látja.

2.1.4. Kártyát vagy elektronikus pénzt használó vagy mikrofizetés

Kártyát használó fizetési rendszerről beszélhetünk abban az esetben, mikor a fizetés során hitelkártyánkat vagy betéti kártyánkat használjuk. Az elektronikus fizetési rendszerek közötti nagy népszerűségét leginkább a kártyák nagyfokú elterjedtségének köszönheti. A kártya tulajdonosának legtöbbször nincs más dolga, csak a terheléshez szükséges adatok továbbítása az arra jogosult félnek és már is elvégezte a rá vonatkozó kötelezettséget. Az adatok továbbítása történhet telefonon, webes felületen (SSL alapú rendszer) vagy egy arra alkalmas kliens program (SET) segítségével. Az utóbbi két eset alkalmazásának biztonságára a fejlesztők óriási hangsúlyt fordítnak, melyekről dolgozatomban a továbbiakban még szó esik.

Az emberek az elektronikus kereskedelem terjedése ellenére még mindig a készpénz használatát részesítik a legnagyobb előnyben. A fejlesztőket ez motiválta egy a készpénz használatát alapul vevő megoldás megalkotásában. A rendszer lényegében egy elektronikus pénztárca, amelyben e-pénz van. Az elektronikus pénz, csakúgy mint kézzelfogható társa, rendelkezik címlettel és sorozatszámmal. A rendszer a fizetőjenek teljes anonimitást biztosít, a sorozatszám alapján nem visszakereshető, hogy azt ki költötte el. Egy adott sorozatszámú e-pénzt viszont csak egyszer szabad elkölteni. A rendszer legnagyobb hátránya viszont ennek a feltételnek a megoldása. Az alkotók erre több megoldást fejlesztettek. Ilyen rendszer például a DigiCash, vagy a CAFE. [7]

Sok esetben előfordult a vásárlások során, hogy a fizetett összeg alacsonyabb volt mint maga a tranzakciós költség. Ennek kiküszöbölésére fejlesztettek ki úgynevezett mikrofizetési protokollokat. Ezek a rendszerek biztonságuk mellett anonimitást is biztosítanak használójuknak. Alapul szolgáló forrásuk viszont többféle lehet. Lehet betéti vagy hitel számlán alapuló, internet szolgáltató által kezelt számla alapú és telefontársaság által kezelt számla alapú. Ilyen rendszerek: PayPal, WiSP, X-pay, PayWord [7]

3. A SET

1997-ban mutatta be a VISA és a Mastercard saját közös fejlesztésű elektronikus fizetési rendszerét, a SET-et. A szó a Secure Electronic Transactions kifejezésből ered, amely biztonságos elektronikus tranzakciókat jelent.[7] A nevében is már jelen van a biztonság szó, amelynek fizetési rendszerekre vonatkozó mezőnyében még mindig az első helyen áll hosszú évek óta. A protokoll fejlesztőinek ez volt a legfontosabb szempont. Valószínű ez volt köszönhető annak, hogy megjelenését követően hamar az elektronikus fizetések lebonyolításának szabványává vált. A biztonság megteremtése viszont nagyon sok erőforrást igényelt. A SET magas rendszer követelményekkel rendelkezik a jelentős számításigényű műveletek végrehajtásának szükségessége végett.
A SET egy hitelkártyát használó, online fizetési rendszer, melyben a tranzakciók minden résztvevője azonosításra kerül.

3.1. Üzleti elvárások

Mivel a tranzakciók többsége az interneten keresztül zajlik az üzleti élet résztvevői legfőbbképp saját adataik védelme érdekében magas elvárásokat támasztottak a protokollal szemben. Ezt azonnal megértjük, ha belegondolunk, hogy több milliós hitelkerettel rendelkező kártyák adatainak kezelését is ezzel oldhatják meg. Ilyen információk illetéktelen kezekbe jutása óriási károkat okozhat a felhasználóknak, ill. megrengetheti a többi felhasználó rendszerbe vetett bizalmát.

A SET hét fő üzleti elvárásnak is eleget tesz:

1. Biztosítja, hogy kizárólag az arra jogosult résztvevők férjenek hozzá a fizetési és a rendelési információkhoz, annak ellenére, hogy együtt kerülnek továbbításra.
2. Biztosítja a továbbított információk sértetlenségét
3. Azonosítást biztosít, amely által ellenőrzésre kerül, hogy a hitelkártyát törvényes tulajdonosa használja-e
4. A kereskedő azonosítását is lehetővé teszi, ill. annak biztosítását, hogy a kereskedő kapcsolatban áll egy a hitelkártyák elfogadására alkalmas pénzintézettel
5. A legmagasabb szintű biztonsági technológiák használatát garantálja védve ezzel az elektronikus kereskedelem résztvevőnek adatait

6. Létrehoz egy protokollt, amely nem függ az adatátvitel biztonsági megoldásaitól, de nem is korlátozza azokat
7. Biztosítja az együttműködést a szoftverkészítők és a hálózati szolgáltatók között.

A leírt elvárások magas szintű biztosítása tette a SET rendszert a mai ismert legbiztonságosabb fizetési rendszerré.

3.2. Specifikációk

3.2.1. Az információk titkosságának biztosítása

Azért, hogy megkönnyítsék és serkentsék a hitelkártyák használatát az elektronikus kereskedelemben, biztosítani kell a vásárlót, hogy a fizetési információihoz kizárólag az arra jogosult fél fér hozzá. Biztonságossá kell tenni a fizetési információk hálózaton keresztüli adatátvitelét, annak érdekében, hogy elkerüljék a lehetséges lehallgatást, mellyel illetéktelen személy férne hozzá bizalmas adatokhoz.

Internetes vásárlás esetén a webes felületen kell megadni a hitelkártya adatait, mely a vásárló és a kereskedő között a nyílt hálózaton keresztül kerül továbbításra egyre növekvő biztonsági feltételekkel, mivel az itt átküldött információk szolgálnak alapul hamis kártyák készítésére és a hitelkártya jogtalan terhelésére.

Amíg lehetőség van a kártyainformációk megszerzésére, addig a fejlesztők egyik legfontosabb feladatuknak látják a biztonság megteremtését. Ebből a szemléletből is látszik, hogy léteznek olyan személyek, akik mások adatainak ellopására magas szinten képzettek, és akár képesek a hálózati eszközökre olyan szűrőket telepíteni, melyekkel lehallgathatják a számítógépek közötti kommunikációt, vagy éppen adatbázisok feltörésével az adatokat tömegesen ellopni. Mindezek következtében a tranzakciós adatok nem biztonságos átviteli módot jelentős negatív benyomást eredményez a potenciális kártyahasználókban.

A SET által használt titkosítási módszer viszont biztosítja az elvárt biztonsági szintet és adatok bizalmas kezelését.

3.2.2. Az információk sértetlenségének biztosítása

A rendszernek garantálnia kell, hogy a küldő és a fogadó közötti adatátvitel során az információk nem változhatnak meg. A vásárlási információk - amely a rendelési, személyes és a fizetési adatokat tartalmazza - továbbítódnak a vásárlótól a kereskedő felé. Amennyiben bármely összetevő megváltozik az adatátvitel során, akkor az átutalás hibásan hajtódik végre. Azért, hogy kiküszöböljük ennek a hibának vagy éppen a módosítás érdekében végzett támadásnak a lehetőségét a rendszernek biztosítania kell olyan eszközök halmazát, melyek lehetővé teszik, hogy a kapott rendelési és fizetési információk megegyezzenek az elküldött üzenettel. A SET digitális aláírásokat használ az üzenetek sértetlenségének biztosítására és ellenőrzésére egyaránt.

3.2.3. A vásárló személyének azonosítása

A kereskedőnek szüksége van egy módszerre, amellyel ellenőrizheti, hogy a megadott számú és érvényességű hitelkártyát a törvényes tulajdonosa használja-e. Egy olyan technológia szükséges, amely egyértelműen összekötheti a vásárlót az általa használt kártyával csökkentve ezzel a csalások előfordulását és a vásárlás folyamatának összköltségét is. A SET ennek biztosítására is digitális aláírást használ.

3.2.4. A kereskedő azonosítása

A vásárlót is biztosítani kell arról, hogy a kereskedő kapcsolatban áll egy pénzintézettel, biztosítva a hitelkártyák elfogadását. A vásárlónak is szüksége van a kereskedő azonosítására, mivel ő az, akivel lényegében az egész folyamatot lebonyolítja. A bizalom felépítéséhez így mindenféleképpen azonosítás szükséges. A SET hasonlóan itt is digitális aláírást használ az azonosításra.

3.2.5. Együttműködés

A rendszer alkalmazható kell legyen minden egyes szoftver és hardver platformon és szigorúan tilos bármelyiket előnyben részesíteni egy másikkal szemben. Bármely vásárló által használt szoftver képes kell legyen a kereskedő által használt szoftverrel, amennyiben az is megfelel az előírt szabványnak. A SET sajátos protokollokat és üzenetformátumot használ a kompatibilitás biztosítása érdekében.

4. SET, Áttekintés

Két fő része van protokollnak:

- Regisztráció
- Tranzakciók végrehajtása

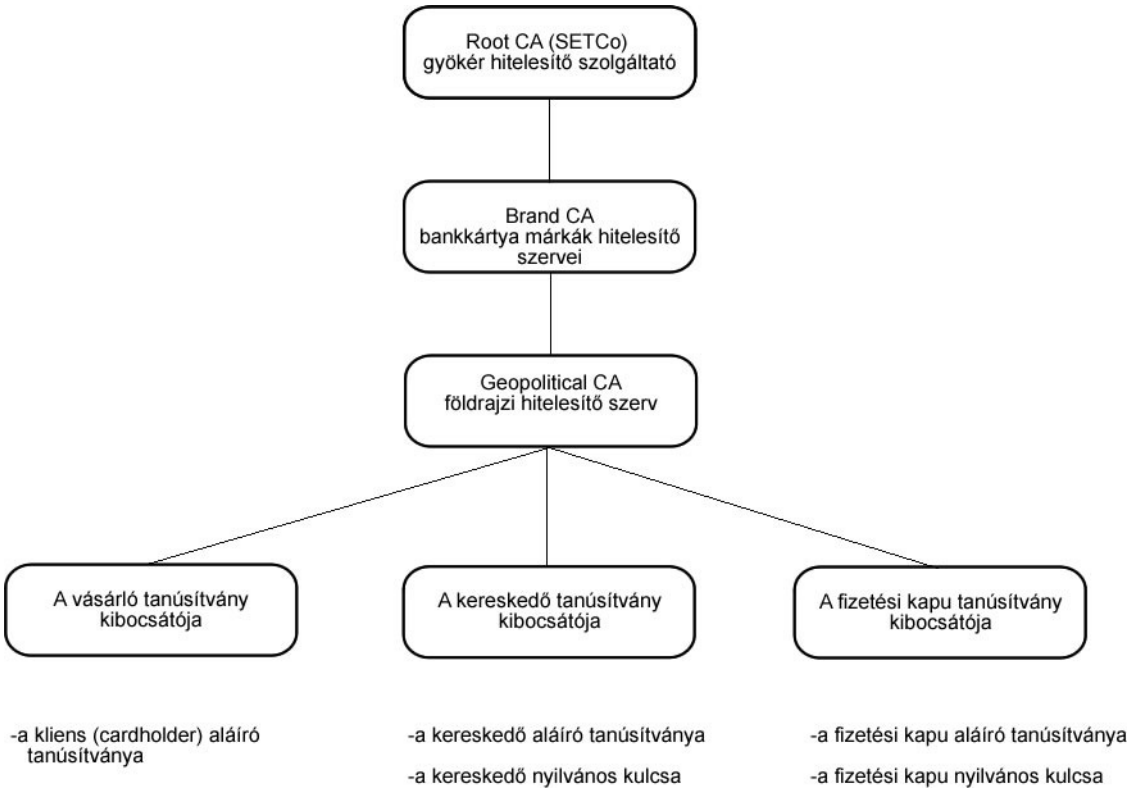
4.1. Regisztráció

A banki tranzakciók biztonsága és sértetlensége a nyilvános kulcsú tanúsítványok használatán alapul.

A SET három féle résztvevőt különböztet meg egy tranzakció során:

- Az eladó (Merchant - M)
- A vásárló (C – Cardholder)
- És a használt fizetési átjáró (Payment Gateway - PG)

A protokoll definiál egy hierarchikus megközelítést a három résztvevő közötti nyilvános kulcs szétosztás között. A SET saját, globális nyilvános kulcsú infrastruktúrára támaszkodik, melynek hierarchikus felépítését az 1. ábra szemlélteti. A csúcson a gyökér hitelesítő szolgáltató található, mely a SET esetén a SETCo (Secure Electronic Transaction Limited Liability Company). A SETCo biztosítja a különböző bankkártya kibocsátóknak és bankoknak a tanúsítványokat, melyeket azok a földrajzilag elosztanak. Az ügyfelek a területileg illetékes intézményeken keresztül igényelhetik a SET alkalmazásához szükséges aláírásokat és a titkosító/dekódoló kulcspárt. [7]



3. ábra A tanúsítvány kibocsátók hierarchiája

4.1.1. A vásárló regisztrációja

A vásárlónak regisztrálnia kell magát a területileg illetékes elektronikus tanúsítvány kibocsátó szervezetnél. Ahhoz, hogy a SET alkalmazásával üzenetet küldjön a tanúsítvány kibocsátó szervezetnek, ismernie kell a kibocsátó kulcscseréhez használt nyilvános kulcsát, melyet annak tanúsítványa tartalmaz.

Szükség van továbbá a vásárló pénzintézeténél kitöltött regisztrációs lap másolatára. Ahhoz, hogy a hitelesítő szerv biztosítsa, a regisztrációs űrlapot, a vásárló szoftverének azonosítania kell a vásárló számlavezető pénzintézetét.

A regisztrációs folyamat a következő:

1. A vásárló szoftvere kérvényezi (C INIT REQ) a kibocsátó szervezet kulcscseréhez alkalmazott tanúsítványának másolatát.
2. Az üzenet megérkezését követően a tanúsítvány kibocsátó választ generál (C INIT RES), melyet digitálisan aláír saját titkos aláíró kulcsával és elküld a kért tanúsítvánnyal együtt a vásárló felé.
3. (i) A vásárló szoftvere a kapott tanúsítványt és annak forrásait is ellenőrzi egészen a gyökér tanúsítvány kibocsátóig, majd a tanúsítvány tárolásra kerül

a további folyamatok végrehajtásához. Ellenőrzi továbbá a kibocsátó aláíró tanúsítványát is.

(ii) Ezt követően a vásárló bankszámlaszámát digitális borítékba helyezi. A digitális borítékot és a regisztrációs űrlap felőli kérelmét (REG FORM REQ) összefűzve elküldi a kibocsátó felé.

4. A kibocsátó dekódolja a szimmetrikus kulcsot, megkapva ezzel a bankszámlaszámot, amely alapján ellenőrzi a számlavezető pénzintézetet, és a kérést. A kérelemnek eleget téve létrehoz egy űrlapot, aláírja azt saját kulcsával és elküldi a vásárló szoftverének.
5. A vásárló ellenőrzi a kapott üzeneten található aláírást. A program ekkor legenerálja a digitális aláírásához szükséges titkos és az ellenőrzéshez szükséges nyilvános kulcsát. A szoftver elkészít egy újabb üzenetet, amely tartalmazza a tanúsítvány kérelmét (CERT REQ), a saját aláírás ellenző kulcsát és egy frissen generált szimmetrikus kulcsot. Az üzenetet digitálisan aláírja. Az így kapott üzenetet egy újabb szimmetrikus kulccsal titkosítja, melyet ezt követően kibocsátó kulcsával titkosít, digitális borítékba helyezve ezzel az üzenetet. Az üzenet elküldésre kerül a kibocsátó felé.
6. A kapott üzenetet visszafejtésre kerül, amíg minden információt meg nem tud a kibocsátó, majd ellenőrzi a benne található számlainformációkat és az aláírást. Ha sikeres az ellenőrzés, a kibocsátó elkészíti a vásárló tanúsítványát és generál egy választ (CERT RES) és digitálisan aláírja. Az aláírt választ ezt követően az előző üzenetben titkosítva kapott szimmetrikus kulccsal titkosítja és elküldi a vásárlónak.
7. Az vásárló kliens szoftvere dekódolja az üzenetet és ellenőrzi a digitális aláírást. A kapott tanúsítványt ($\mathrm{Cert}(\mathrm{K}_{\mathrm{C}}^{(\mathrm{sig})})$) eltárolja további felhasználásra. [10]

4.1.2. A kereskedő regisztrációja

A kereskedő regisztrációjának folyamata nagyrészt megegyezik a vásárló regisztrációs folyamatával. Alapvető különbség a kulcsok számában van. A kereskedő rendelkezik az aláíró kulcs páron kívül egy titkosító/dekódoló kulcs párral is, melyek igénylése szintén a regisztrációs folyamat során történik. A kapott tanúsítványok jelölése: $\mathrm{Cert}(\mathrm{K}_{\mathrm{M}}^{(\mathrm{sig})})$ aláíró , és $\mathrm{Cert}(\mathrm{K}_{\mathrm{M}}^{(\mathrm{enc})})$ titkosításhoz használt tanúsítvány [10]

4.2. Tranzakciók végrehajtása

Három fő szakasza van:

1. Vásárlási kérelem
2. Fizetési felhatalmazás kérelme
3. Fizetés végrehajtása

A három fő szakaszban a következő műveletek kapnak helyet [10]:

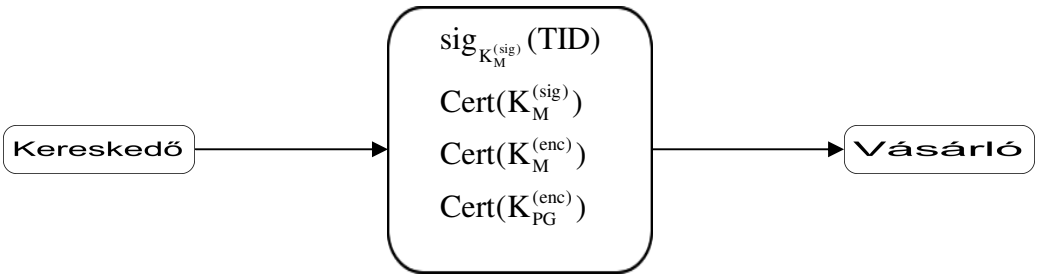
4.2.1. Vásárlási kérelem

1. **A kérelem kezdeményezése (Initiate Request – P INIT REQ)**

   A folyamat elején vásárló kiválasztja a megvételre szánt termékeket. A kártyatulajdonos számítógépén futó szoftvercsomag elküldi a kérését, melyben kéri a kereskedőt a saját és a fizetési kapu tanúsítványának elküldésére.

2. **Kereskedő visszajelzése (Initiate Response)**

   A kereskedő a kérés érkezését követően hozzárendel egy egyedi műveleti azonosítót (TID) és ezt ellátja saját aláírásával, továbbá három tanúsítványt csatol: a kereskedő aláírás-ellenőrző kulcsának tanúsítványát, a kereskedő titkosító tanúsítványát és a fizetési kapu titkosító tanúsítványát.



3. **Kliens vásárlási kérelme (Purchase Request)**

   (i) Ebben fázisban ellenőrzésre kerülnek a tanúsítványok és a tranzakciós azonosítóhoz tartozó aláírás. Ezt követően elkészít két dokumentumot: először a rendelési információkról (OI - **O**rder **I**nformation) a kereskedő számára majd egy a fizetési információkról (PI - **P**ayment **I**nformation) szólót a fizetési rendszer számára. A fizetési információk a vásárló személyes adatait

tartalmazzák, mint hitelkártyaszám, az érvényességi idő és az ellenőrző kód, így ezek a kereskedő előtt titkosak maradnak. Mindkét üzenet tartalmazza az eladó rendszere által meghatározott műveleti azonosítót (TID), annak érdekében, hogy a két rész között a kapcsolat fennmaradjon. Ezt követően két dokumentumon kettős digitális aláírást alkalmaz.

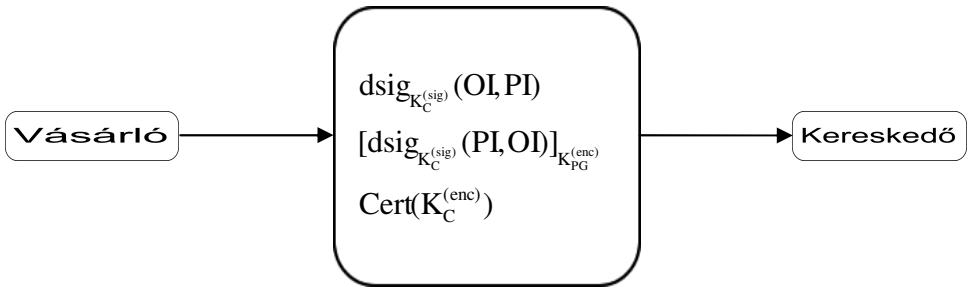
$$\mathrm{dsig}_{K_C^{(sig)}}(OI, PI)$$

Az előzőekben leírt definíció alapján az aláírt változat mellett a kereskedő megkapja a rendelési információk eredeti változatát és a fizetési információk lenyomatát is. Erre azért van szükség, mert a két dokumentum együttesen tartalmazza a vásárlás részletes leírását, viszont egyes részeket tikosítani kell az arra nem jogosult fél elől, de az ellenőrzéshez szüksége van rá.

(ii) A következő lépésben a fizetési információk titkosítása következik. A vásárló elkészíti a PI és OI dokumentumok kettős aláírt változatát, viszont itt az aláírás mellé a PI eredeti változata kerül. Mivel az üzenet továbbításában a kereskedő közvetítő szerepet játszik és a vásárló el akarja az adatait titkolni, így az üzenet rész egy digitális borítékba helyezi.

$$[\mathrm{dsig}_{K_C^{(sig)}}(PI, OI)]_{K_{PG}^{(enc)}}$$

(iii) A kereskedőnek elküldésre kerül a két üzenet lenyomata digitálisan aláírva, az eredeti rendelési információkról szóló dokumentum, a fizetési információk lenyomata, a fent leírt módon titkosított fizetési információkról szóló dokumentum és a vásárló aláírásának ellenőrzéséhez szükséges tanúsítvány.



Amennyiben vita merülne fel a vásárló és az eladó között az eredeti rendelési információk lenyomata elérhető a fizetési kapu számára is így ellenőrizhető melyik fél követelése jogos.

4. **Kereskedői válasz (Purchase Response)**

   Az üzenet megérkezése után ellenőrzésre kerül a vásárló tanúsítványa és a kettős aláírás az üzenet sértetlenségének biztosítása végett. Mindezeket követően az eladó generál egy választ majd azt digitálisan aláírva visszaküldi a vásárlónak.

5. **Vásárlói visszajelzés**

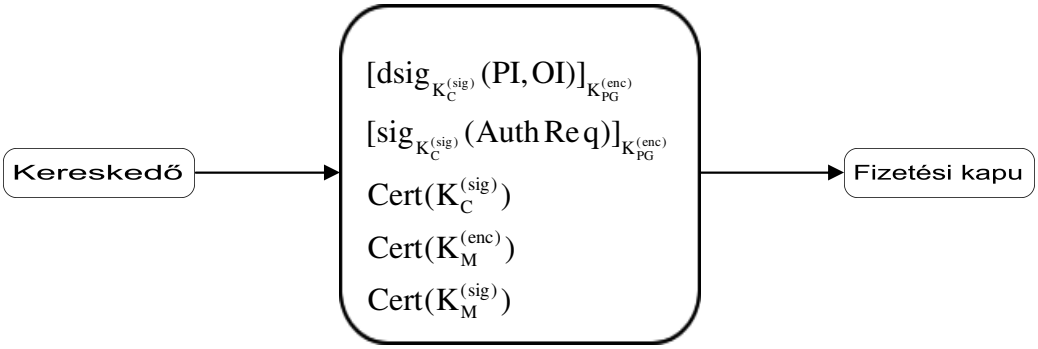
   Ellenőrzi a kereskedő nyilvános kulcsával az üzenetet és tárolja azt a gyorsabb jövőbeni kommunikáció érdekében.

4.2.2. Fizetési felhatalmazás

Ez a rész a fizetési rendszer és a kereskedő között zajlik. Az eladó célja a fizetés felhatalmazásának megszerzése.

6. **A kereskedő felhatalmazás kérelme (Authorization Request)**

   Mivel a kereskedő számára nem érhetőek el a vásárló fizetési információi, így ellenőrizni sem tudja annak fizetőképességét. A felülvizsgálat elvégzésére a fizetési kaput kell megkérnie. Először készít egy digitálisan aláírt kérvényt (AuthReq), mely tartalmazza a művelet azonosítóját (TID), a teljesítendő végösszeget és a rendelés egyéb részleteit. A kérvényt digitális borítékba teszi és továbbítja a saját és a vásárló kliens programjának tanúsítványaival. Az üzenet tehát formálisan a következő:



Látható, hogy a maga által generált üzenetekhez és tanúsítványokhoz hozzáfűzve tovább küldésre kerül az előzőleg a vásárlótól kapott fizetési és rendelési információkról szóló digitálisan aláírt üzenet is. A kettős aláírás biztosítja a vásárló számára, hogy a fizetési kapu a dekódolást követően is kizárólag a fizetési információkhoz jusson hozzá, mivel a rendelési információknak csak a lenyomata került elküldésre. Az üzenet küldőjének azonosítása és a lenyomatok ellenőrzéséből az üzenet sértetlenségének vizsgálata itt is az előzőekhez hasonlóan lehetséges.

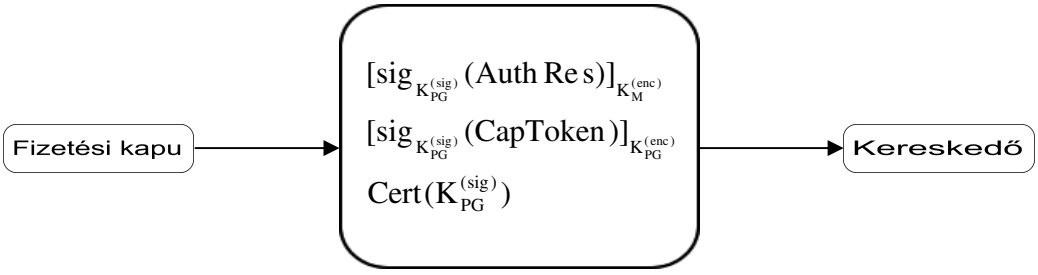
7. **Engedélyezés (Authorization Response)**

(i) A rendszer a kapott üzenetet dekódolja, és ellenőrzi a kereskedő adatait. A kapott információ és kulcs alapján dekódolásra kerül a fizetési információ. Továbbá ellenőrzi, hogy a műveleti (TID) azonosító egyezik-e a fizetési információk és a AuthReq üzenetben. Ha megegyeznek akkor a rendszer elfogadja a kereskedő engedélyezés-kérését.

(ii) A következő lépésként a vásárló számlavezető bankjának egy fizetési információkat tartalmazó üzenetet küld egy privát hálózaton belül. Ha a kérés jogos és teljesíthető a rendszer „engedélyezve” választ generál (AuthRes), melyet digitálisan aláír. Az üzenetet digitális borítékba helyezi.

$$[\mathrm{sig}_{K_{PG}^{(sig)}}(\mathrm{Auth\,Res})]_{K_{M}^{(enc)}}$$

Az üzenet továbbá tartalmazhat egy (CapToken) lehívási zsetont, melyet a fizetési kapu generál, és amit a kereskedő felhasználhat az átutalás későbbi elindítására. A zsetont elküldés előtt a kapu aláírja és saját nyilvános kulcsával titkosított digitális borítékba helyezi, így kizárólag ő férhet hozzá. Lényegében magának küldi egy a kereskedő által megtestesített késleltető csatornán. A teljes üzenet tehát a következő:



8. **Kereskedői reakció**

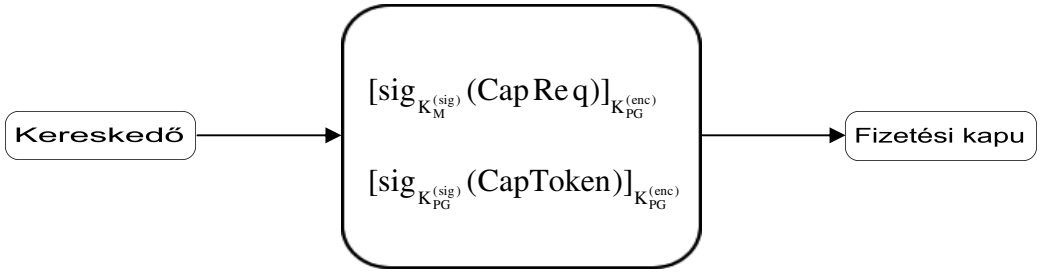
   Az üzenet megérkezésével értesül a kérés jóváhagyásáról és digitálisan aláírt nyugtázó üzenetet küld a vásárlónak, majd teljesíti a tranzakció során vállalt kötelezettségeit és elküldi a rendelt árut a vásárlónak. A vásárló ellenőrzi a kereskedő aláírását és eltárolja azt.

4.2.3. Fizetés végrehajtása

9. **Kereskedő fizetési igénye (Capture Request)**

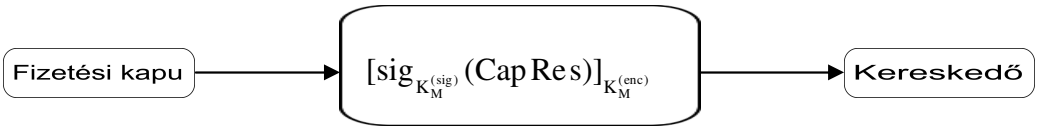
   Ebben a szakaszban kéri a kereskedő a rendszert az összeg átutalására. Generál egy digitálisan aláírt kérést (CapReq), amely tartalmazza a végösszeget, a műveleti azonosítót és egyéb információit. Az üzenetet digitális borítékba kerül.

   Elküldésre kerül még a hozzáfűzve az eddigiekhez az előzőekben kapott CapToken üzenet titkosított változata is.



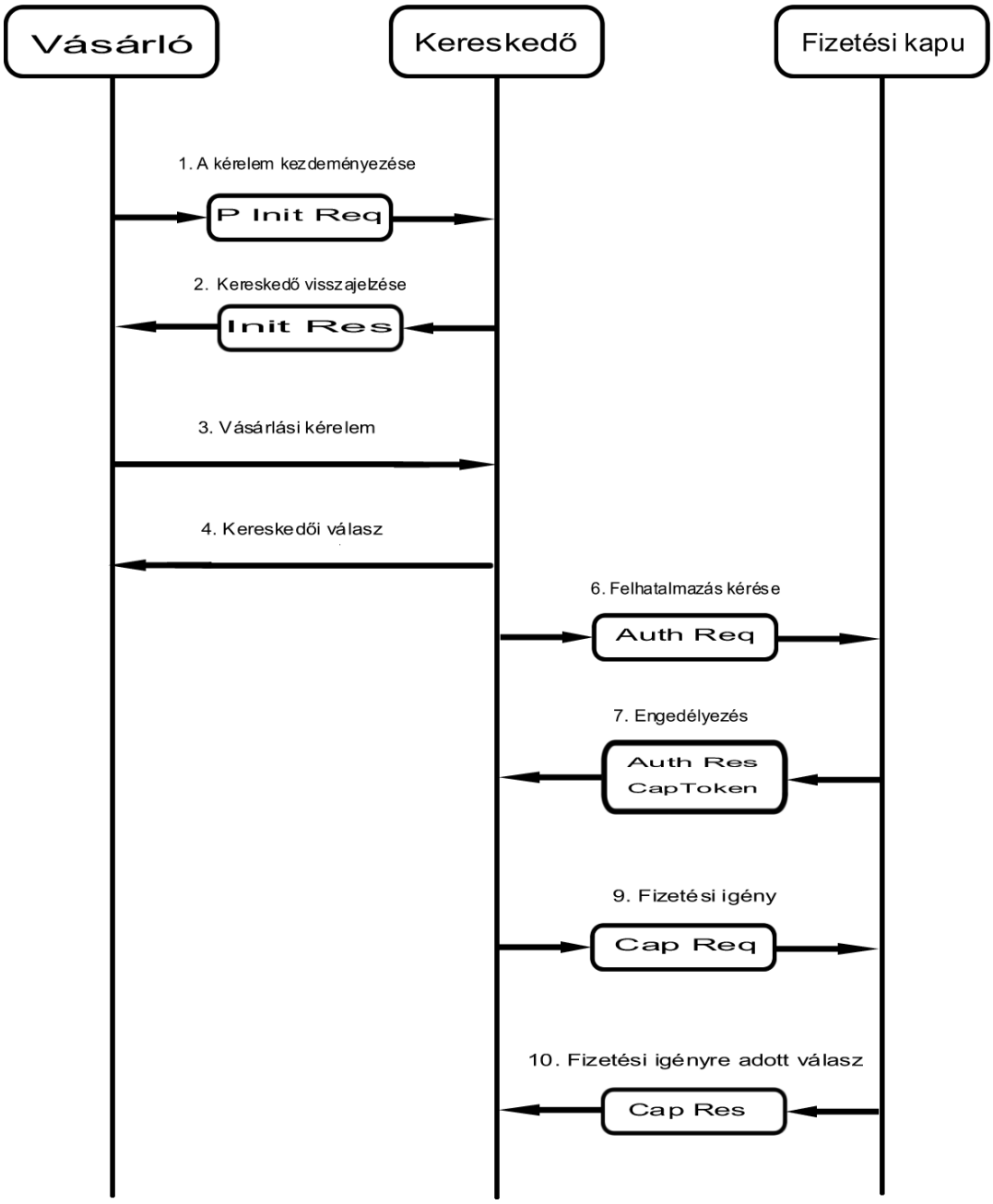
10. **A fizetési igényre adott válasz (Capture Response)**

    A kérés (CapReq) megérkezését követően a rendszer dekódolja az új kulcsot, kibontja a digitális borítékot és ellenőrzi a kereskedő tanúsítványát. Ha az ellenőrzés sikeresen zárult, akkor a fizetési rendszer kezdeményezi az átutalást a vásárló bankjánál, viszont ez már a pénzintézetek privát hálózatán történik. A kezdeményezést követően tanúsítványa segítségével generál egy nyugtát (CapRes), melyet a kereskedő nyilvános kulcsával védett digitális borítékba helyez és elküld a kereskedőnek.



11. **Kereskedői reakció**

A kereskedő kibontja a borítékot, megkapva a kulcsot dekódolja az üzenetet, ellenőrzi a fizetési kapu azonosítóit. Ezt az üzenetet (CapRes) a fizetési rendszer automatikusan tárolja, az esetleges későbbi viták rendezése érdekében. [7]



4. ábra A fizetés folyamata

5. A SET teljesítménye

A SET protokoll leírásából adódóan, nyilvánvaló. hogy a biztonsági eljárásokat magas szinten alkalmazza, köszönhetően a nyilvános kulcsú titkosításnak, a digitális aláírásnak és az üzenetek többszörös ellenőrzésének. A rendszerbe vetett bizalom a nyilvános kulcs infrastruktúra fejlesztésein alapul. Ahol ez nem elérhető ott a SET-nek sincs lehetősége a felhasználók körében elterjedni.

Az 1.0-ás verzióban RSA algoritmussal biztosítják a titkosítást napjainkban minimum 768 bites kulccsal, de az 1024 bites ajánlott. A nyilvános kulcsú műveletek (aláírás/ellenőrzés, titkosítás/dekódolás) alapos számítási igénye és a nagyméretű tanúsítványok átvitele széles sávot igényel, így azt mobil eszközökön, intelligens kártyákon alkalmazni a jelenleg elterjedt technológiai fejlettség mellett sem lehet.

	Aláíró	**Kulcscsere**	**Tanúsítvány aláíró**
Vásárló	1024		
Kereskedő	1024	1024	
Fizetési kapu	1024	1024	1024

1. Táblázat Ajánlott kulcsméret

Amennyiben a kártyatulajdonos személyi számítógépet használ, a töltési jelentéktelen. Másrészt, ha a felhasználó nem kapcsolódik számítógéphez, a kriptográfiai funkciók tárolva lehetnek akár egy smart kártyán is. Ahhoz, hogy egy smart kártyán RSA algoritmus fusson, erre alkalmas processzort tartalmazzon, mely az árát is jelentősen megnöveli. Ez a rendszer is hozzájárul a kézi eszközök használatának terjedéséhez az elektronikus kereskedelemben. Hátrányuk viszont az alacsony sávszélesség és az alacsonyabb teljesítményű processzor, melyek a SET futtatását lassabbá teszik.

A GartnerConsulting Group által készített széleskörű tanulmány szerint a kereskedők hisznek a napi 10. 000 db tranzakcióban, de a fizetési kapuk kb. fél millió átutalásra számítanak. Ebben az esetben a nyilvános kulcsú szoftverek teljesítménye viszont kevés az rendszer ellátásához. Kérdésessé vált a nyilvános kulcsú titkosítás használata. Egy tanulmányban az elliptikus görbék kriptográfiai használatainak előnyeit is felvetették a számítási igény és a sávszélesség tekintetében.[2]

6. A jelenleg elterjedt online fizetési rendszerek és a SET

6.1. Online hitelkártyás fizetés

A napjainkban használt online hitelkártyás fizetési rendszer is háromszereplős (vásárló, kereskedő, bank (fizetési kapu) a SET-hez hasonlóan. A módszer biztonságát itt viszont nem a többszörös digitális aláírások, hanem a használt VeriSign tanúsítvánnyal ellátott SSL(Secure Socket Layer) protokoll biztosítja. A jelenlegi biztonsági elvárásoknak a 128 bites titkosító kulcsú csatorna tökéletesen megfelel. Itt az adatokat közvetlen az arra jogosult oldalon adhatjuk meg. Adat közvetítő szerepet egyik résztvevő sem játszik, ellentétben a SET-tel, ahol a fizetési adatokat a kereskedő továbbítja a bank felé. Meg kell jegyeznem azonban, hogy a fizetési adatok közvetlen a bank felé továbbítása a Magyarországon használt hitelkártyás fizetési rendszerek sajátossága. Külföldi oldalakon sok esetben észrevehető, hogy hitelkártya adatainkat a kereskedőnek vagyunk kénytelenek közvetlenül megadni.

Ahhoz, hogy az elektronikus hitelkártyás fizetési szolgáltatás létrejöjjön a bank és az áruház, a kettőjük között létrehozandó titkosított kapcsolat érdekében szimmetrikus kulcscserét kell végrehajtson.

A vásárlás folyamata:

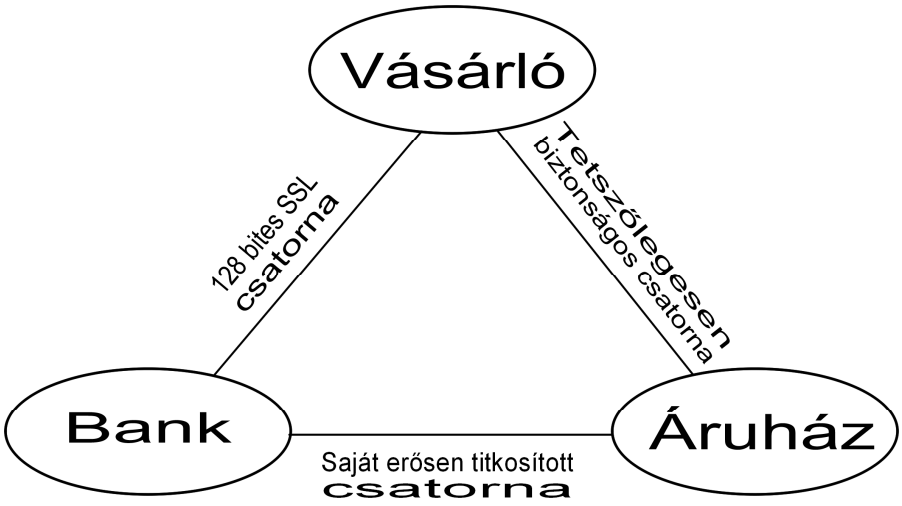
1. Természetesen a vásárlás folyamata itt is a megvételre szánt termék(ek) kiválasztásával kezdődik, melyben a vásárlás jóváhagyását követően kiválasztásra kerül a fizetési mód. Jelen esetben kizárólag az online hitelkártyás módot tárgyaljuk.
2. Az igény beérkezését követően a webáruház ellátja a vásárlás adatait és tranzakciót egy egyedi azonosítóval, amely ettől a ponttól a folyamat végéig követi a lépéseket. Az azonosítót ezt követően a regisztrált vásárló felhasználó nevével és a vásárlás ellenértékével együtt elküldi a bank felé. Amennyiben az oldal nem igényel regisztrációt vásárlóitól, akkor fizetéskor egy fiktív felhasználói nevet küld a bank felé.
3. A pénzintézet regisztrálja és ellenőrzi a kérést majd az eredményről értesíti a kereskedőt. Ekkor még csak a tranzakciókérés regisztrációja történik, a vásárló még nincs jelen.
4. Ha a bank a tranzakciókérés sikertelenségét jelzi, a vásárló az áruháztól értesítést kap és a vásárlásnak vége szakad, de a természetesen van lehetőség a próbálkozás

megismétlésére, esetlegesen az áruház automatikusan újrakéri a regisztrációt. Ha bank sikeres regisztrációt jelez vissza, akkor az áruház a vásárlót transzparens módon a tranzakció-azonosítóval ellátva a bankhoz küldi. Itt felváltja az áruház-bank és áruház-vásárló kapcsolatot a vásárló-bank kapcsolat.

5. A bank az URL-ben kapott tranzakciós azonosító alapján lekérdezi adatbázisából a 3. lépésben letárolt adatokat.
    a. A banki felület tartalmazza az átutalandó összeg, a webáruház neve és egyéb kiegészítő információk, továbbá tartalmaz egy űrlapot, melynek kitöltésével a vásárló megadhatja hitelkártya adatait. Ez az utolsó pont, ahol még kérheti a vásárlás megszakítását.
    b. A kitöltést követően elküldi a bank felé, amely ha az űrlapon engedélyezésre került elkezdi a tranzakció végrehajtását.
6. A bank elvégzi az authorizálást. Ez a lépés a vásárló és az áruház elől is el van rejtve, egy önálló kommunikációs csatornán zajlik.
7. Amennyiben a vásárló a tranzakció megszakítását kérte, akkor a bank bejegyzi a megszakítást és nem authorizál.
8. Következő lépésként a bank visszaküldi a vásárlót az áruház oldalára csatolva hozzá a tranzakciós azonosítót. Az áruház ez alapján lekéri adatbázisából a vásárlás adatait és ellenőrzi azokat.
9. Az áruház újra felveszi a kapcsolatot a bankkal és kérvényezi az authorizáció eredménynek közlését.
10. A bank közli az eredményt az áruházzal és lezárja a folyamatot.
11. Az áruház továbbítja az eredményt a vásárlónak és szintén lezárja a folyamatot. A vásárló újra vásárolhat vagy elhagyhatja a webáruházat.
12. Amennyiben az áruház nem fogadja a 10. pontban közölt eredményt, akkor a bank visszavonja a vásárló számláján lévő terhelést

A bank-vásárló kapcsolat a folyamat teljes ideje alatt erős 128 bites SSL csatornán történik, melyért a bank a felelős. A bank által alkalmazott 128 bites VerySign tanúsítvány képes egy megfelelően erős titkosított kommunikációs csatorna létrahozására és fenntartására. A vásárló kártyájának adatai így semmiféleképpen sem kerülnek illetéktelenek kezébe. Az áruház-bank kapcsolatban ezzel szemben saját titkosító eljárás felhasználásával közölnek a felek adatokat

egymásnak nyílt csatornán. Ennek a megoldásához áruházi oldalon is fejlesztések szükségesek.



5. ábra Csatornatípusok

Gondoskodni kell továbbá a banki titkosító program más rendszerekre való átültetésének lehetőségéről is.

Az esetleges nézeteltérések elkerülése érdekében a bank minden tranzakciós lépést naplóz és rendszeresen archivál. [5]

6.2. „Megbízható harmadik fél" módszert alkalmazó online fizetési rendszerek

Az online kereskedelmi rendszerek megjelenését megelőzően is léteztek „megbízható harmadik felet" alkalmazó ügyletek. Gondoljunk csak a közjegyző által hitelesített egyezményekre, vagy ügyvéd által ellenjegyzett nagyobb értékű eladásainkra. Az online világban is a kereskedelem terjedésével szükségessé vált ez a végrehajtási eljárás alkalmazása, mely jelentős előnyökkel rendelkezik a többi fizetési protokollal (pl. SET) szemben.

- Nem kell semmilyen alkalmazást telepíteni a fizetés lebonyolításának elvégzése érdekében, mégis a felek az eredményről a megfelelő védelem mellett kapnak értesítést legtöbb esetben a megadott e-mail címükre.

- A SET használatához, ahogy azt előzőleg leírtam szükségünk van regisztrációra, ahol a vásárló személyazonosságát és nyilvános kulcsát is ellenőrzik. Jelen esetben viszont nincs szükség semmilyen fizetési rendszernél történő regisztrációra (habár egyes szolgáltatók mint például a CyberCash és a Paypal igényelnek egy ennél sokkal egyszerűbb regisztrációt). Ezzel biztosítva a vásárlók megnövelt rugalmasságot és kényelmet.
- A protokollt úgy tervezték, mint egy HTTP-típusú kérdés-válasz protokollt. Ez a megközelítés sokkal egyszerűbbé tette az implementálást. Például nincs szükség minden pontban üzenetet küldeni a két félnek és várni míg összehangolódnak a felek. Ehelyett egy a protokoll használatának minden lépéséhez tartozik egy elküldendő üzenet és egy a kapott üzenetre küldendő, visszaigazoló válasz üzenet.
- A protokoll egy másik erőssége, hogy lehetőség van bármely pontból visszaállítani a megfelelő állapotokat esetleges sikertelenség esetén. Ezáltal biztosítja mind a vásárlót mind a kereskedőt a kommunikáció vagy a rendszer meghibásodásának lehetőségével szemben.
- A protokollt bármely mai létező fizetési eszközzel (hitelkártya, bankszámla) használhatjuk, ezzel biztosítva elérhetőséget a felhasználók széles körének.
- Mivel a művelet természetéből kifolyólag viták léphetnek fel, a rendszer biztosít a felek számára bizonyítékot az állításuk igazolására, mivel a teljes művelet lezárása [2]

A vásárlás folyamata:

1. A vásárló elküldi rendelését a kereskedőnek, illetve a továbbítja fizetéshez szükséges információkat (bank-, vagy hitelkártya adatok)
2. A kereskedő az üzenet megérkezését követően elküldi azt a „megbízható harmadik félnek”, amelynek központi egysége feldolgozza, majd a vásárló számláját vezető bank felé továbbítja
3. A bank visszaküldi a fizetési jóváhagyás eredményét a központi feldolgozó egységének, amely továbbküldi a „megbízható harmadik félnek”
4. A harmadik fél elküldi az eredményt a kereskedőnek
5. A kereskedő a választól függően eldönti, hogy elfogadja vagy elutasítja a vásárlást

7. A SET és az SSL alapú fizetési rendszer összehasonlítása

7.1. Azonosítás

7.1.1. Vásárló azonosítása

A SET esetében a vásárló azonosítása egy több lépcsős folyamat. A felhasználónak regisztrálnia kell a rendszer saját nyilvántartásába. A regisztráció során ellenőrzésre kerül a felhasználó személyazonossága, a hitelkártyájának adatai, mint például érvényesség és kibocsátó pénzintézet továbbá ellenőrzik, hogy a bemutatott kártya a regisztrációt kezdeményező személyhez tartozik-e. A sikeres regisztrációt követően a felhasználó kap egy digitális aláírást tartalmazó tanúsítványt, mellyel a SET használata közbeni azonosítására szolgál. Az azonosítás első része itt le is zárult. Látható, hogy ebben az esetben a fizetési rendszert alkalmazni kívánó személyeknek alapos ellenőrzési folyamatokon kell átesni kizárólag azért, hogy használhassák a rendszert.

A fizetési folyamatban a vásárló első azonosítását a kereskedő végzi a rendelési és fizetési adatokról szóló dokumentumokon található kettős aláírás ellenőrzésével. A kereskedőn túl a fizetési kapu is azonosítja az ügyfelet a folyamat hatodik lépésében. Ekkor kapja meg, a kereskedő által továbbított fizetési információkat a vásárló által digitálisan aláírva.

A SET esetében a vásárló minden esetben digitális aláírása alapján kerül azonosításra, tehát a készítéséhez használt kulcsméret határozza meg az azonosítás biztonságát. A SET esetében az aláírásokhoz SHA-1 lenyomatkészítő függvényt és 1024 bit nagyságú RSA kulcsokat használnak.

Az SSL-alapú online fizetési rendszer estében a vásárló kereskedő általi azonosítása opcionális, kizárólag azonosított rendszerekben történik. [5] Ebben az esetben regisztrációhoz kötött a vásárlás. A regisztrált vásárló azonosítása felhasználói neve és hozzátartozó jelszava alapján történik. Az azonosítás biztonsága a jelszó erősségén múlik. Gyenge jelszó kiválasztása esetén könnyen feltörhetővé válik felhasználói fiók. A vásárlót a kereskedő irányítja fizetési igényének kielégítése céljából egy banki felületre. Itt kerül a vásárló és a bank először kapcsolatba. A vásárló azonosítása az által birtokolt kártya információk alapján történik. Ezek a kártyaszám, az érvényességi idő és a hátoldalán található kártyakibocsátótól függő CVC2 vagy CVV2 kódot. Amennyiben az adatok egyértelműen meghatároznak egy

adott hitelkártyát, akkor annak tulajdonosa is azonosításra került. Az azonosításra használt adatok védelméről azonban annak tulajdonosa gondoskodik, a fizetési rendszer felügyelete nem terjed ki erre. Ezzel szemben a SET esetén a regisztráció során is meg kell adni, majd azt követően a vásárlásoknál alkalmazott kliens program kezeli.
Az SET rendszerben a vásárlót mindkét másik fél azonosítja a ma használt legbiztonságosabb technika, a digitális aláírás alapján. Ezzel szemben az SSL- alapú rendszer esetében az azonosítás biztonsági színvonala lényegesen alacsonyabb. Amennyiben valaki tudomására jutnak egy hitelkártya használatához szükséges adatok, akkor az azzal visszaélve kedvére használhatja, vásárolhat azzal, károkat okozva törvényes tulajdonosának.

7.1.2. Kereskedő azonosítása

A SET esetében az azonosítás első lépcsőfoka megegyezik a vásárlónál leírtakéval. A regisztráció során aláíró tanúsítványt kap. A fizetési folyamat során a kereskedő a vásárló által kerül először azonosításra, már a harmadik lépésben. A kereskedő fizetési kapu általi azonosítása később, a hatodik lépésében kerül sor, mindkét esetben digitális aláírás alkalmazásával. A kereskedő azonosítása több szempontból is nagyon fontos. Egyrészt a vásárló olyan a hitelkártyájával kapcsolatos információkat közöl vele (ha titkosítva is), mellyel később a fizetési igényét benyújthatja a pénzintézetnek. Másrészt a banknak is ismernie kell, kinek a fizetési igényét teljesíti, milyen számlán jelenjen meg a vásárló számlájának terheléséből adódó jóváírás.
Az SSL- alapú rendszernél az áruház és a bank között állandó hálózati kapcsolat van. A bank a kereskedőt rendszeren belüli azonosítója (PID) alapján ismeri fel. Ez egy hét karakterből álló azonosító. Azonosítja továbbá az áruházat is a szolgáltatás létrejöttét megelőző kulcscserében szereplő közös titkos kulcs ismerete. [5]
A leírtak alapján itt is egyértelműen látszik, hogy a SET azonosítása lényegesen alaposabb.

7.2.3 A fizetési kapu/bank azonosítása

A SET esetében a fizetési kapuval kizárólag a kereskedő kerül kapcsolatba, közvetítő szerepet játszva a fizetési adatok továbbításában. Az azonosítása a fizetési folyamat hetedik lépésében történik a megszokott digitális aláírás technikát alkalmazva.
Az SSL- alapú rendszernél a bankkal a kereskedő és a vásárló is kapcsolatba kerül. A vásárló és a bankot SSL tanúsítványa által azonosítja. A tanúsítvány segítségével generált digitális

ellenőrzésével történik az aláírás. Ez az első és egyébként egyetlen olyan azonosítási technika, amely hasonló a SET-ben alkalmazottakéhoz. A bank és a kereskedő között saját titkosított csatorna van fenntartva. A titkosításhoz alkalmazott szimmetrikus kulcs egyértelműen meghatározza a bankot, mivel azt a két fél, a kereskedő és a bank ismerheti csak.

Mindezeket összevetve a SET a digitális technika használatának köszönhetően a biztonságos azonosítás elvárását mai is teljesíti. A biztonság érdekében viszont feláldozásra került a hatékonyság. Az SSL- alapú rendszerben történő azonosítás biztonsága lényegesen elmarad a SET-hez képest, viszont sokkal hatékonyabb és alacsonyabb költségekkel rendelkezik.

7.2. Az üzenet sérthetetlenségének biztosítása

A SET fejlesztői a digitális aláírás használatával egyszerre két problémát is megoldottak. Az azonosításon túl alkalmas az üzenetek sértetlenségének megőrzésére is. Pontosabban lehetővé teszi annak vizsgálatát, hogy a megkapott dokumentumok megegyezik az aláírt üzenetben szereplőkkel. A ma használt lenyomatkészítő készítő függvények és az aláírásokhoz használt titkosító eljárás az a mai elvárásoknak teljes mértékben eleget tesznek.

Az SSL- alapú rendszer az üzenetek sértetlenségének vizsgálatához MAC (Message Authentication Code) értéket alkalmaz.[1] Ez egy kriptográfiai ellenőrző összeg, amit a küldő az elküldés előtt kiszámol, titkosít és az üzenethez csatol. A digitális aláírással ellentétben itt a titkosításra szimmetrikus kulcsot használnak, melynek cseréjéről az üzenetküldést megelőzően a küldőnek és a címzettnek gondoskodni kell. A fogadó az ellenőrzéshez dekódolja az üzenetet, a küldővel azonos módon kiszámolja ezt az ellenőrző értéket. Amennyiben megegyezik az elküldött értékkel, akkor az üzenet sértetlensége bizonyítottá válik. Ellenkező esetben az üzenet a továbbítás során megsérülhetett, vagy nem a továbbított üzenetről készült az ellenőrző érték. Az adatintegritás biztosítása mellett azonosító szerepet is ellát, mivel a titkosításra használt szimmetrikus kulcsot kizárólag a kommunikációban résztvevő két fél ismerheti.

Ebből a szempontból közel azonos értéket kaphatnának, de az SSL- alapú rendszer talán itt hatékonyabbnak bizonyulhat. Egyrészt a MAC alacsonyabb számítási igényéből adódó gyorsasága miatt, másrészt ez semmilyen tanúsítványt nem igényel tehát bárki számára elérhető. Az aláírás előnyeként meg kell említenünk, hogy az akár harmadik fél számára is képes az üzenet sértetlenségének ellenőrzését biztosítani. Az aláírás ellenőrzéséhez használt kulcs ugyanis nyilvános ellentétben a MAC által használt szimmetrikus kulcséval. Itt is újra látszik, hogy a biztonság érdekében alkalmazott erőforrások leginkább hiánya okozhatta, hogy ez a rendszer mégsem terjedt el a várt módon.

7.3. Titkosság megőrzése

A vásárlási folyamat során a felhasználó olyan információkat közölhet magáról, melyeket a fogadó feleknek titokban kell tartaniuk. Ilyenek lehetnek a fizetéssel kapcsolatos adatok vagy akár a vásárolni kívánt áru megnevezése. Ezeket a résztvevő feleknek bizalmasan kell kezelni. A rendszernek kezelnie kell, hogy a résztvevők kizárólag olyan információkhoz jussanak, amelyek az ő feladatuk ellátásának szükséges feltételei. Tehát a rendelési információkat ne lássa a bank, a fizetési információk pedig a kereskedő előtt maradjanak titokban.
A belső titkosság mellett biztosítani kell, hogy rendszeren kívüli személy ne férjen hozzá az adatokhoz. Az adatok illetéktelen személyekhez jutása visszaéléshez vezethet, mely a fizetési rendszer megbízhatóságát, és ez által a használatának népszerűségét jelentősen csökkentené.

7.3.1. A belső titkosság megőrzése

A SET-en belül a belső titkosság megőrzésének szükségességét a kereskedő információ közvetítő szerepe indokolja. A SET-en belül az adatok bizalmas továbbításáról a digitális boríték technológia felel. A dokumentumok titkosításához DES titkosítást alkalmaztak 56 bites kulcsmérettel. A SET készítésekor szimmetrikus titkosításra még ez volt a szabvány. Mára már viszont ez elavulttá vált. A szabvány és az általa használt kulcs mérete is megváltozott. Nincs azonban semmilyen megkötés a SET-ben, arra vonatkozóan, hogy milyen titkosítást alkalmazzon annak felhasználója. A rendszer szimmetrikus titkosításra használt modulja könnyen átváltható a manapság szabványként használt 128 bites kulcsmérettel rendelkező AES titkosításúra. A kulcs titkosítására a címzett nyilvános kulcsát használja a rendszer. Ezt az 1024 bit méretű kulcsot RSA titkosításra alkalmazzák. A kulcs méretéből adódó biztonsági szint alkalmassága megosztja a hozzáértők véleményét. Egyes szakértők szerint ma már egy 2048 bites kulcs alkalmazása lenne javallott.
Az SSL- alapú rendszerben ezt sokkal egyszerűbben oldották meg. Az adatokat a vásárló közvetlenül adja meg az arra jogosult félnek. A kereskedő nem kerül kapcsolatba a fizetési információkkal még titkosított formában sem, mivel annak megadása előtt a vásárlót átirányítja a 128 bites AES titkosítású fizetési felületre és ugyanígy a bank sem értesül a vásárlás tárgyát képző termék adatairól. [5] A két információ halmazt egy közös azonosító kapcsolja össze, annak érdekében, hogy a kerekedő össze tudja hangolni az egyes folyamatokat.

7.3.2. A külső titkosság megőrzése

A SET-et úgy tervezték, hogy az adatok biztonsága független legyen az adattovábbítási csatorna titkosításának szintjétől. Lényegében a belső titkosítás fenntartása közben biztosítja, hogy az információk rejtettek maradjanak külső, a folyamatban nem résztvevő személyektől.
Az SSL- alapú rendszer esetében az adatok külső titkosságának megőrzésére három kommunikációs vonalon is szükség van. A bank és a vásárló között, a kereskedő és a bank között és a vásárló és a kereskedő között. A bank és a vásárló közötti tikosításról az SSL protokoll gondoskodik. Alapját a jelenleg is a szimmetrikus titkosítás szabványául szolgáló 128 bites AES titkosítás szolgáltatja. Ez a szint jelenleg teljesen elfogadott. A bank és a kereskedő közötti privát hálózaton egyéni titkosítást alkalmaznak. Itt a titkosításra TripleDES módszert alkalmaznak leggyakrabban, de ettől természetesen eltérhetnek, ez nem szabvány. A TripleDES végrehajtása során lényegében három DES futása történik. Az első kulccsal a titkosítás, a másodikkal visszafejtés, a harmadikkal pedig ismét tikosítás történik. A kulcsok mérete mindhárom esetben 56 bit, így összességében a rendszer 168 bites kulcsot használ.[7]

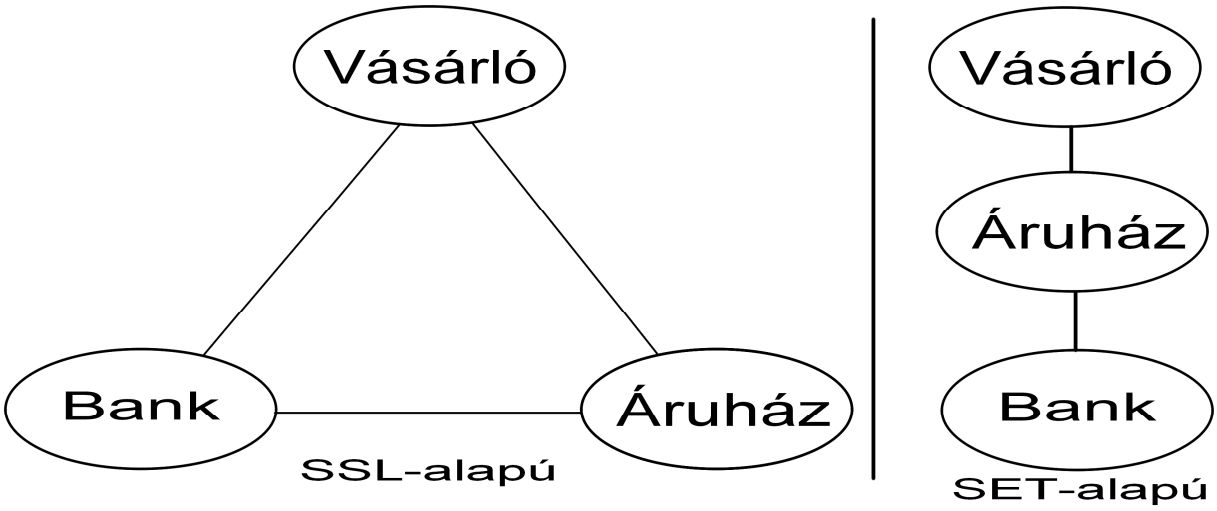
	AES	**TripleDes**
Lehetséges kulcsméret (bit)	128, 192, 256	112 vagy 168
Sebesség	Magas	Alacsony
Feltöréséhez szükséges idő (255 kulcs kipróbálására alkalmas számítógéppel)	149 trillió (10^{18}) év	4,6 milliárd év
Erőforrás szükséglet	Alacsony	Magas

2. Táblázat Az AES és a TripleDES összehasonlítása

A kereskedő és a vásárló közötti csatorna biztosítása opcionális. Ezen a kommunikációs vonalon is SSL-t használnak a megfelelő biztonsági szint eléréséhez. Ennek biztosítása a felhasználói név és a hozzá tartozó jelszó biztonságos továbbításához szükséges.

7. 4. Rendelkezésre állás, megbízhatóság

Rendelkezésre állásának feltételei ugyanazok mindkét rendszernél. Használatukhoz számítógépre és internet hozzáférésre van szükség. Alapvető feltétel továbbá a résztvevő felek hozzáférhetőségének biztosítása. A legfontosabb feltétele mindkét rendszernek a bank állandó elérhetősége. A fizetés lebonyolítása megoldhatatlanná válna a pénzintézet jelenléte nélkül.
A SET esetében viszont eggyel kevesebb szálon történik a kommunikáció, mivel itt a vásárló a fizetési kapuval nincs közvetlen kapcsolatban, melyet a 6. ábra is szemléltet.



6. ábra Az SSL-alapú és a SET-alapú rendszer kapcsolatainak jellege

Mindkét rendszer naplózza az egyes eseményeket. Ennek köszönhetően lehetőség van – a folyamat megszakadása esetén – bármely már befejezett lépéstől folytatni. A fizetést csak akkor tekinthetjük lezártnak, ha minden egyes lépés végrehajtásra kerül.
Továbbá alapvető feltétele mindkét rendszernek a bank állandó elérhetősége is. A fizetés lebonyolítása megoldhatatlanná válna a pénzintézet jelenléte nélkül.

7.6. Hatékonyság

A SET tervezésénél, ahogy már azt többször is leírtam a biztonsági szempontok voltak az elsődleges szempontok. Ennek biztosítása érdekében a rendelkezésre álló módszereket alkalmazták. Ennek azonban jelentős hátránya is van. Magas számítás igénnyel rendelkező műveletek végzésének nagy száma a rendszer sebességét és ezáltal hatékonyságát jelentősen csökkenti. Több ponton elhagyható lenne a többszörös titkosítás, amennyiben a vásárló és a fizetési kapu közvetlenül kommunikálhatna.

	SET	SSL-alapú
Digitális aláírás	8	0
Aszimmetrikus titkosítás	6	1-2
Szimmetrikus titkosítás	6	4
Tanúsítvány ellenőrzés	8	1-2
MAC ellenőrzés	0	1-2

3. Táblázat Műveleti igények

Nagy hátránya a SET-nek a kliens alkalmazás használatának szükségessége. Futtatása a magas műveleti igények mellett további terhelést jelent a résztvevő számítógépeknek.

Az SSL- alapú rendszer esetében, ahogyan azt a 3. táblázat is mutatja, minden műveletből kevesebb kerül végrehajtásra az SSL-re jellemző MAC érték számításán kívül. Kliens program alkalmazása nem szükséges, így az plusz terhelést nem jelent a felhasználó számítógépe számára. Ennek az oka, hogy kizárólag webes felületen lebonyolítandó fizetésekre tervezték.

.

8. Mire várhatunk a jövőben?

Jelenleg számos vállalat kínálja a SET szolgáltatást mint pl.: az IBM, Verisign, Cybertrust, Verifone, Sterling Commerce, Terisa, Netpay és a Globeset

A SET jelenleg több mint negyven országban elérhető szolgáltatás.

A 2.0-ás változathoz előterjesztették, hogy használja az aszimmetrikus kriptográfiai algoritmusokat és támogassa a hitelkártyák használatát engedve a személyazonosság ellenőrzését PIN kód segítségével, melyet titkosítva tartalmazna a fizetési üzenet. A smart kártyákat használó SET rendszert C-SET-nek (chip-secured) nevezik.

Összefoglalás

Az elektronikus üzleti modellek folyamatosan növekvő térnyerésével egyre nagyobb igénnyé vált a biztonságos elektronikus fizetés is. A fejlesztők elsődleges szempontnak a biztonságot tekintették. Ez a SET fejlesztőinél sem történt máshogy. A készítők az üzleti világ minden igényét figyelembe vették termékük létrehozásánál. A SET biztosítja, hogy kizárólag az arra jogosult személyek férjenek hozzá az információkhoz, melyeknek sértetlenségéről szintén a rendszer gondoskodik. A folyamatok résztvevőinek egyértelmű azonosítása is megoldásra került. Mindezeket teljesen platform független környezetben képes végrehajtani. A biztonsági szint az átviteli csatornától sem függ, önmaga hozza létre azt saját titkosító moduljaival. Mindezek használatához egy kliens alkalmazás telepítése és alkalmazása is szükséges. Ennek használata viszont már komolyabb felhasználói ismereteket igényelt.

A magas szintű biztonság ellenére a SET- nek, a hitelkártyás elektronikus fizetési rendszerek terén van egy igen erős konkurense, az SSL- alapú fizetési rendszerek. A biztonság és a teljesítmény a felhasználók teljes igényét kielégíti kevesebb erőforrás felhasználásával. A rendszer nagy előnye a SET- hez képest, hogy nem szükséges kliens program használata, így a fizetés lebonyolítása bárhol elvégezhető, nem csak kliens alkalmazással ellátott számítógépen.

A magas rendszerkövetelmény és a nyilvános kulcsú infrastruktúra alacsony elterjedtsége végett a SET nem teljesítette a várt sikereket.

A kriptográfiai módszerek azonban egyre jobban fejlődnek. A tudósaink egyre alacsonyabb mennyiségű erőforrás igénybevételével végrehajtható műveletek segítségével próbálják elérni és meghaladni a jelenleg rendelkezésre álló biztonsági szintet. Egyik ilyen terület az elliptikus görbék felhasználásával kifejlesztett kriptorendszer. Ennek eredményeképpen létrejöhetnek olyan eszközök, melyek jelenleg is használt tárgyainkba (pl.: mobiltelefon) beépülve tesznek elérhetővé olyan szolgáltatásokat, melyek eddig különálló eszközön vagy helyhez kötött személyi számítógépen volt csak elérhető.

Mindezek fejlődése vagy a rendszer egyes elemeinek módosítása vagy elhagyása eredményezhetné, a jelenlegi elvárások alapján a SET terjedését.

Ezúton szeretnék köszönetet mondani témavezetőmnek, Dr. Huszti Andreának szakdolgozatom elkészítésében nyújtott segítségéért és útmutató tanácsaiért.

Irodalomjegyzék

Könyvek, tanulmányok

[1] Buttyán Levente - Vajda István: Kriptográfia és alkalmazásai, Typotex kiadó 2004

[2] Weidong Kou: Payment Technologies for E-Commerce, Springer 2003

[3] Berecz Patrícia- Elektronikus kereskedelem a gyakorlatban 2004

[4] Mostafa Hashem Sherif: Protocols for Secure Electronic Commerce, CRC Press 2004

[5] CIB Bank Zrt.: Internetes kártyaelfogadás szolgáltatás technikai dokumentációja Verzió: 1.41

Internetes források

[6] Carl Eric Wolrath - Secure Electronic Transaction
http://www.wolrath.com/set.html
Letöltés dátuma:2010. 02.06

[7] Dr. Phillip M. Hallam- Baker: Electric Payment Scemes
http://www.w3.org/ECommerce/roadmap.html
Letöltés dátuma: 2010.04.25

[8] Feature: Goodbye DES, Hello AES
http://www.networkworld.com/research/2001/0730feat2.html
Letöltés dátuma: 2010.04.24.

[9] Gócza Zoltán: Mikrofizetési megoldások
http://www.mikrofizetes.info/mikrofizetes-megoldasok
Letöltés dátuma: 2010.04.15.

[10] SET Business Description - ccc.cs.lakeheadu.ca/set/set_bk1.pdf
Letöltés dátuma: 2009.12.05.

Ábrajegyzék

Táblázatjegyzék