

Università degli Studi di Perugia

Corso di Laurea Magistrale in Informatica

Millicent

Corso di Sicurezza Informatica - prof. Stefano Bistarelli

Seminario di

Caterina Lombardi – Marco Mencacci – Paolo Mengoni

Indice generale

Pagamenti e micropagamenti.....	3
Il protocollo Millicent.....	3
Come funziona.....	4
Chi è coinvolto.....	4
Vantaggi di Millicent.....	5
Sicurezza.....	5
Gli scrip.....	5
Produzione e validazione degli scrip.....	6
Possibili implementazioni del protocollo.....	7
Scrip in the clear:	8
Private and secure:.....	8
Secure without encryption:	9
Brokers	10
Modello "Scrip warehouse"	11
Modello "licensed scrip production"	12
Modello Multiple brokers	13
Interazioni tra Customer, Broker, e Vendor.....	13
Breve storia dei micropagamenti.....	17
Punti chiave per il successo.....	17
Online gaming.....	18
iTunes.....	18
Facebook credits.....	18
Flattr.....	18
Bibliografia.....	19

Pagamenti e micropagamenti

Tradizionalmente nel commercio il valore delle transazioni è stato regolato dal valore delle monete che le persone si possono scambiare.

La moneta più piccola che attualmente ci possiamo scambiare è quella da un centesimo di euro: per acquistare oggetti o servizi che hanno valore inferiore a questo la strategia che solitamente si applica è quella dell'aggregazione. Questa prevede il raggruppamento di beni o servizi fino al raggiungimento del valore minimo che è pagabile dal cliente.

Nel commercio online non è sempre possibile applicare questa strategia per esigenze di velocità delle transazioni.

I protocolli di pagamento adatti a pagamenti di maggiore entità solitamente hanno costi per transazione troppo alti, una pesante gestione degli account o coinvolgono troppi attori per essere impiegati in scambi di così bassa entità.

Si deve quindi ricercare un nuovo protocollo che si possa adattare alle microtransazioni che sia veloce, abbia un basso costo per transazione, sia altamente scalabile e coinvolga il minor numero di attori possibile.

Il protocollo Millicent

Il protocollo Millicent è stato sviluppato nei laboratori di ricerca della DEC con l'obiettivo di colmare la mancanza di strategie adatte ai pagamenti di basso valore su internet.

Questo protocollo supporta transazioni sicure utilizzando algoritmi di crittografia simmetrica molto veloci essendo il loro costo computazionale estremamente ridotto.

La valuta utilizzata sono degli **scrip** che possono essere validati direttamente nei server del venditore riducendo sia i costi di comunicazione che il numero di soggetti coinvolti nelle transazioni.

Come funziona

Millicent si basa sullo scambio di scrip che sono una rappresentazione del rapporto che si è stabilito fra venditore e acquirente.

Il nome scrip viene dalla tradizione statunitense di emettere questo tipo di buoni (o fogliettini) fin dalla fine dell'800 da parte sia di istituzioni pubbliche che di aziende private. Normalmente questo tipo di buoni erano utilizzati per l'acquisto di beni e servizi presso un unico venditore.

In ogni momento il venditore ha un certo numero di scrip emessi che rappresentano il numero di account aperti con i clienti. Il valore di questo buono è anche il bilancio dell'account che viene scalato dopo ogni acquisto.

Chi è coinvolto

Il protocollo Millicent prevede il coinvolgimento di tre soggetti strettamente legati fra di loro ma che hanno diversi livelli di affidabilità.

Il **Broker** è la figura chiave dell'intero processo di vendita degli scrip. Fa da intermediario fra cliente e venditore. Le transazioni in valuta reale avvengono solamente con lui: cliente e venditore si scambieranno soltanto degli scrip. Acquista vendor scrip dal venditore, con varie modalità, e li rivende al cliente.

È la figura che ha il maggiore livello di affidabilità fra tutte quelle interessate dall'intero processo, solitamente è un'istituzione finanziaria.

Il **venditore** emette degli scrip che il broker provvederà a vendere al cliente. Accetta gli scrip dai clienti e restituisce loro il resto, sempre sotto forma di scrip, quando il valore del buono non viene esaurito dalla transazione.

Il **cliente** acquista scrip dal broker usando valuta reale per poterli poi spendere presso il venditore. È la figura con l'affidabilità minore dell'intero processo.

Vantaggi di Millicent

Tra i vantaggi che si possono ottenere dall'adozione del protocollo Millicent per i micropagamenti possiamo sicuramente inserire il contenimento dei costi sia computazionali che di comunicazione.

I costi computazionali possono essere suddivisi fra quelli necessari alla crittografia dei messaggi, alla verifica degli scrip e alla gestione degli account.

La crittografia viene gestita tramite algoritmi a chiave simmetrica dato il basso valore degli scrip.

Il processo di validazione degli scrip avviene presso il venditore, senza coinvolgere gli altri attori nel processo.

La gestione degli account è suddivisa fra i tre attori. Il venditore mantiene i dati degli scrip che ha venduto ai broker e degli scrip che sono stati utilizzati dai clienti. Il broker gestisce sia lo storico delle transazioni in valuta reale che i dati degli utenti. Il cliente mantiene il bilancio dell'account all'interno dello scrip.

Sicurezza

Per quanto riguarda i goal di sicurezza da raggiungere tramite questo protocollo questi sono rapportati al valore delle transazioni che saranno coinvolte nel processo.

Infatti la confidenzialità delle comunicazioni non viene protetta in Millicent. L'esiguo valore delle transazioni non richiede delle policy apposite. D'altro canto l'autenticazione viene garantita dall'invio in modo criptato dei segreti di scrip e cliente e l'integrità degli scrip è tutelata dalla loro firma.

Gli scrip

L'elemento che è alla base del protocollo Millicent è lo scrip. All'interno di questo oggetto vengono mantenute le informazioni necessarie agli attori coinvolti nelle transazioni.

Vendor	Value	ID#	Cust ID#	Expires	Props
--------	-------	-----	----------	---------	-------

Figura 1: struttura dello scrip

Lo scrip è strutturato per mantenere delle informazioni obbligatorie ed alcune opzionali.

Fra quelle obbligatorie troviamo i dati del venditore presso il quale è spendibile e il suo valore. Lo scrip viene identificato da un numero seriale, ha una data di scadenza entro la quale deve essere utilizzato ed è spendibile solo dal legittimo proprietario, il cui identificativo viene salvato all'interno della struttura.

Vi è poi una sezione libera e personalizzabile a piacimento dal venditore e dal broker nella quale possono essere registrate informazioni aggiuntive.

Produzione e validazione degli scrip

La fase di produzione degli scrip viene svolta dal venditore o dal broker a seconda del modello produttivo che si è scelto di implementare (questione che affronteremo in seguito).

Tramite l'identificativo unico viene generato, con un algoritmo noto solo all'emittente, un master scrip secret che viene memorizzato in un registro.

Questo viene poi concatenato allo scrip e utilizzato per generare un certificato tramite funzioni hash (SHA-1 o MD5).

Lo scrip e il certificato così ottenuto verranno inviati al cliente.

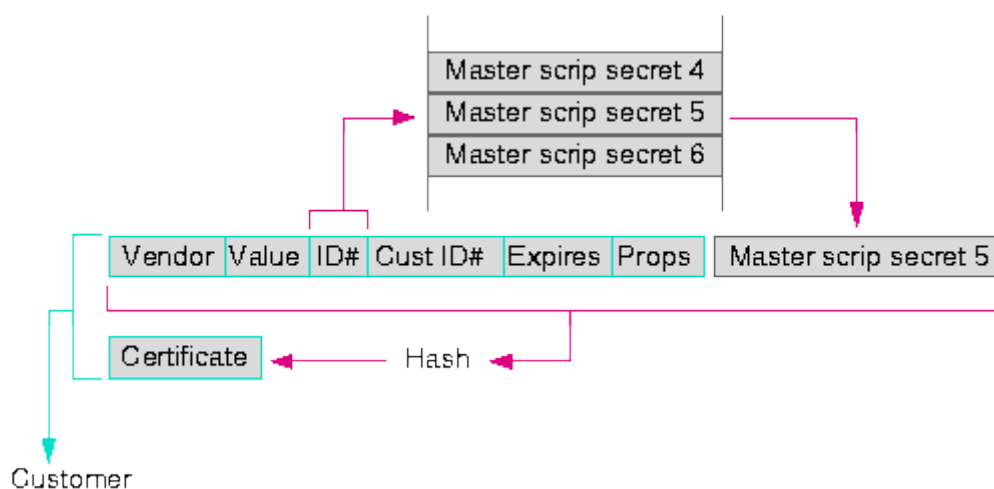


Figura 2: produzione dello scrip

Il cliente che vuole utilizzare lo scrip presso il venditore deve inviare a questi sia lo scrip che il certificato.

Il venditore che li riceve prenderà lo scrip e genererà, tramite l'algoritmo segreto, il master scrip secret. Confronterà questo con quelli che sono nel suo elenco di scrip già spesi per evitare che venga utilizzato due volte, ed infine procederà a concatenare il master scrip secret con lo scrip per produrre il nuovo certificato.

Questo nuovo certificato viene quindi confrontato dal venditore con quello che il cliente gli ha inviato per verificarne l'integrità.

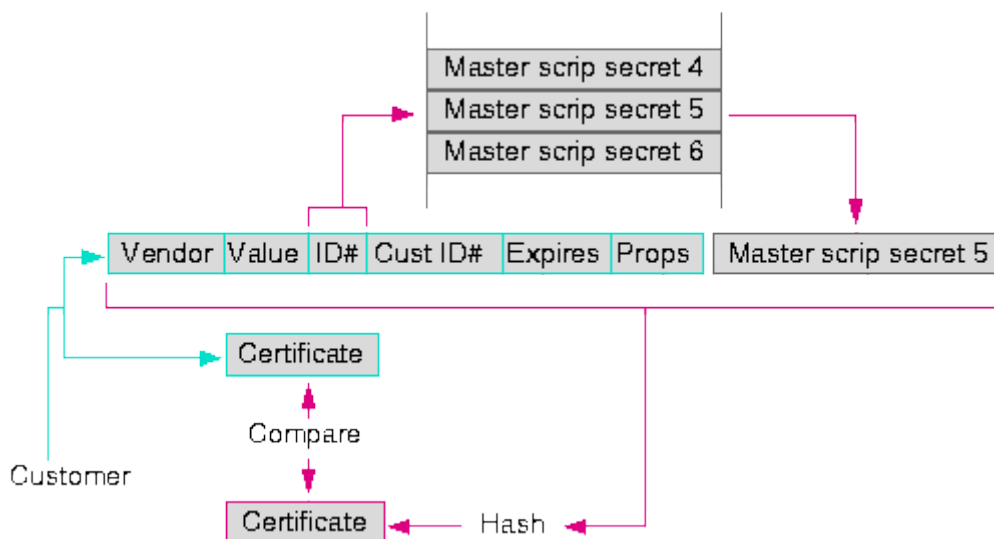


Figura 3: validazione dello scrip

Concluse positivamente queste fasi, lo scrip viene accettato dal venditore.

Possibili implementazioni del protocollo

Millicent nasce per microtransazioni, quindi i goal di sicurezza vanno interpretati in tal senso. Non è necessario avere gli stessi livelli di sicurezza delle transazioni finanziarie o di elevati scambi di denaro. Nel caso del Millicent i valori coinvolti sono esigui e la frequenza delle transazioni elevata, è inutile pertanto appesantire la comunicazione e la gestione delle transazioni.

Parlando di micropagamenti infatti lo scenario è: transazioni di basso valore ma molto frequenti. Va, quindi, preferito il protocollo che garantisce maggior velocità e minor costo computazionale per elaborare le richieste e le risposte.

Per capire il giusto compromesso, partiamo a descrivere le possibili implementazioni del protocollo.

Scrip in the clear:

È il modo più semplice possibile di interpretare il Millicent. Tutta la comunicazione avviene in chiaro. Il cliente spedisce al vendor la richiesta e lo scrip in chiaro (ovvero non criptato o protetto in alcun modo).

Il vendor processa la richiesta e risponde con un nuovo scrip (sempre in chiaro) come resto.

Questa implementazione del protocollo non offre alcuna sicurezza. Qualsiasi soggetto in ascolto sul canale potrebbe intercettare lo scrip di ritorno ed usarlo come suo. Quando il possessore si ripresenta al vendor, questo rifiuterà la richiesta perché nel suo sistema avrà registrato già come speso quel particolare scrip.

In questo primo caso è massimizzata la leggerezza delle comunicazioni ma senza un minimo di sicurezza è praticamente inutilizzabile.

Il punto chiave della sicurezza in Millicent è la generazione della chiave segreta per l'utente (customer_secret). La chiave è generata dal broker a partire dall'ID cliente e viene spedita tramite canale sicuro al cliente al momento della prima registrazione presso il broker. Algoritmo e modalità di generazione della chiave sono noti sia al broker che al vendor ma non al cliente.

Questa chiave diventa a tutti gli effetti un segreto e può essere utilizzato per la cifratura delle comunicazioni.

Private and secure:

In questa versione del protocollo, si utilizza il customer_secret come segreto condiviso per la generazione di un canale di comunicazione sicuro tramite uno dei protocolli di cifratura a chiave simmetrica.

Il venditore condivide con il broker l'algoritmo di generazione delle chiavi e può risalire alla chiave segreta del cliente (a partire dal campo ID cliente del messaggio) per decifrare la richiesta.

Lo scrip di ritorno può essere rispedito in chiaro mentre la risposta e la nuova chiave cliente vengono cifrati con con la chiave del messaggio.

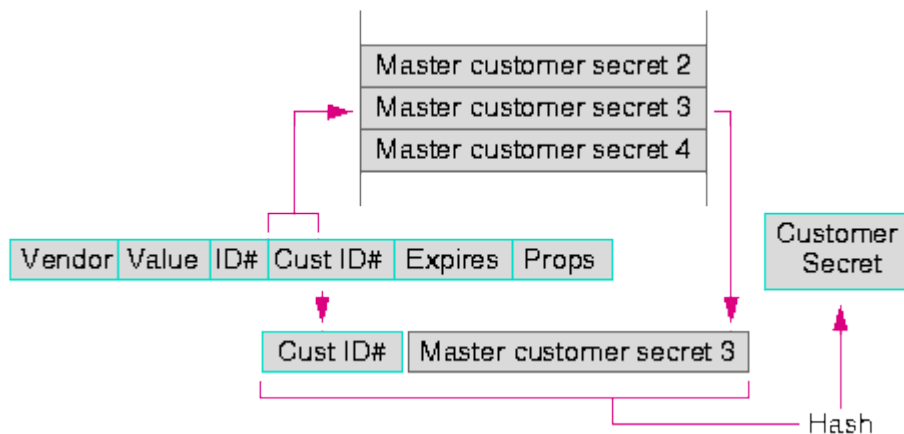


Figura 4 a : criptazione dello scrip

In questa implementazione del protocollo, sia la richiesta che la risposta sono tenute completamente private; un intercettatore non può risalire al contenuto dei messaggi in quanto non possiede il customer_secret. Il costo computazionale per costruire il canale sicuro e la necessità di codificare i messaggi è tuttavia penalizzante rispetto all'obiettivo di contenere costi e overheads (informazioni aggiuntive alla comunicazione).

Secure without encryption:

Questa implementazione del protocollo utilizza il customer_secret non per cifrare l'intera comunicazione ma per firmare gli scrip.

Al momento dell'acquisto il customer spedisce la richiesta, lo scrip e una firma della richiesta al vendor. La firma non è altro che l'hash di [scrip+request+customer_secret].

Quando il vendor riceve la richiesta, ricava il customer secret dallo scrip, rigenera la firma e la confronta con quella arrivata. Se qualcuno ha modificato in qualche modo lo scrip o la richiesta, la firma non coinciderà. Se tutto corrisponde, il vendor processa la richiesta e ritorna un nuovo scrip

come resto. Il nuovo scrip emesso avrà lo stesso customer ID di quello originale, quindi solo il possessore, a conoscenza del customer secret potrà firmarlo e utilizzarlo di nuovo.

Non c'è alcun bisogno di cifrare la risposta, un intercettatore non potrà mai spendere gli scrip letti, in quanto non sarà in grado di rifirmarli (non conoscendo il customer secret).

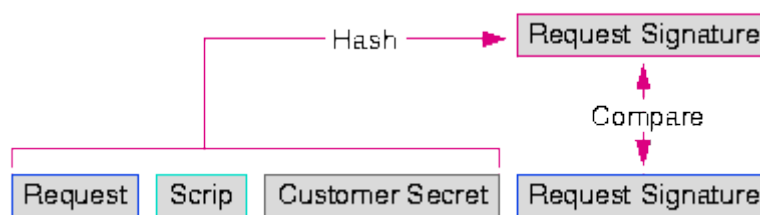


Figura 4 b : criptazione dello scrip

In questo caso sono rispettati tutti e due i goal del Millicent. Utilizzando soltanto una funzione hash, si realizza un protocollo leggero e ragionevolmente sicuro.

Brokers

I brokers fanno da intermediari tra cliente e commerciante effettuando tutte le transazioni in denaro reale.

Il commerciante e l'intermediario (broker) hanno rapporti di lavoro a lungo termine.

Ogni commerciante produce la propria valuta elettronica chiamata "Scrip", caratterizzata dal "piccolissimo taglio" e firmata digitalmente per impedire contraffazioni.

Il broker acquista dal commerciante i vendor scrip e sulla base di essi emette dei broker scrip.

Per effettuare una transazione, il consumatore contatta il Broker Server e apre un conto con il broker, mediante un pagamento sicuro ad esempio con carta di credito, per acquistare i broker scrip.

Una volta fatto ciò, l'utente può comprare presso qualsiasi commerciante aderente al circuito Millicent versando in contropartita i vendor scrip ottenuti utilizzando i broker scrip.

A questo punto il venditore che si trova in possesso degli Scrip può, nel momento in cui abbia accumulato un valore consistente di "crediti", cambiare gli scrip ed ottenere dal broker "moneta normale" sul proprio conto bancario, tramite canali sicuri.

Il broker ottiene i vendor scrip utilizzando vari metodi: pay in advancer, consignment sale, licensed production. In tutti i modelli, il broker può aggiungere un piccolo profitto su ogni scrip, perché acquista dal commerciante in blocco con un piccolo sconto e rivende singolarmente gli scrip al cliente.

Esamineremo tre modi attraverso cui il broker ottiene i vendor scrip:

Il modello "Scrip warehouse" che presuppone una relazione causale tra il broker e il commerciante.

Il modello "licensed scrip producer" che presuppone un rapporto duraturo e di sostanziale fiducia tra il mediatore e il venditore.

Il modello "multiple broker" che presuppone un relazione tra broker, ma non richiede alcun rapporto tra commerciante e broker.

Modello "Scrip warehouse"

In questo caso l'intermediario funge da scrip warehouse, acquista in grandi quantità gli scrip da un commerciante e li conserva e ne vende uno alla volta ai clienti (Figura 5b-5d).

Questo modello non presuppone alcuna relazione speciale tra il commerciante e il broker.

Funziona meglio quando i broker hanno un'idea chiara dei vendor scrip che i clienti potrebbero volere.

Il broker, infatti, utilizza il protocollo Millicent per acquistare in blocco, i vendor scrip che ritiene possano essere richiesti dai clienti.

Vendere scrip in blocchi di grandi dimensioni è più conveniente per il commerciante in quanto la comunicazione e i costi di transazione finanziaria sono meglio ammortizzati.

In genere il commerciante offre uno sconto sulla quantità per incoraggiare i broker ad acquistare grandi blocchi di scrip.

Il broker ottiene un profitto quando rivende singolarmente gli scrip ai clienti a prezzo pieno.

Il broker si assume la responsabilità di garantire al cliente le proprietà codificate negli scrip dal commerciante.

Modello "licensed scrip production"

Se i clienti di un broker comprano molti scrip di uno specifico venditore, può essere desiderabile per quest'ultimo dare al broker una "licenza" per produrre i suoi vendor scrip.

Ciò significa che il broker genera scrip che il venditore è grado di convalidare e confermare.

Il venditore vende al broker il diritto di generare scrip utilizzando un `master_scrip_secret`, una serie di ID #, un `master_customer_secret` e una serie di identificatori dei clienti.

Il venditore può convalidare la licenza di produzione degli scrip perché gli è noto il `master_scrip_secret`, il numero seriale ID dello scrip, il `master_customer_secret` e l'identificatore del cliente.

Il Broker produce lo scrip e raccoglie il denaro dai clienti, i commercianti registrano il valore totale degli scrip provenienti da un determinato broker. Quando tutti gli scrip prodotti a seguito di un contratto sono finiti, broker e commerciante possono decidere. Il broker presumibilmente riceve un'altra commessa per la produzione di scrip.

Una licenza copre una specifica serie (il range di identificatori è univoco - ID#'s) di scrip per un dato periodo di tempo, e il codice segreto condiviso tra il broker e il commerciante può essere applicato solo a quegli ID.

Il commerciante può dare un licenza a diversi broker inviando a ciascuno una differente serie di ID e diversi codici segreti. Naturalmente, un commerciante può produrre propri scrip usando propri ID e propri codici segreti.

La licensed scrip production è più efficiente sia per il commerciante che per il broker rispetto al modello scrip warehouse.

La trasmissione è più leggera perché la licenza è più piccola da trasmettere dei blocchi di scrip.

Il commerciante ha dei costi di computazione inferiori visto che non deve generare da solo gli scrip.

Il broker non deve memorizzare i dati di grandi blocchi di scrip visto che può generare gli scrip su richiesta.

Inoltre è più semplice per il broker garantire le proprietà specifiche di uso codificate in ciascun pezzo di scrip generato.

Modello Multiple brokers

In un ambiente dove ci sono molti broker, un cliente di un broker può voler effettuare un acquisto da un commerciante associato con un altro broker.

Se il commerciante vuole avere un account solo con il proprio vendor, il cliente dovrebbe cambiare broker per acquistare i vendor scrip, mentre ciò non accade nel modello multiple brokers.

L'intera transazione sarà così:

1. Il cliente contatta il suo broker per dei vendor scrip.
2. Il broker del cliente prova a stabilire un account con il commerciante.
3. Il commerciante comunica al broker del cliente il nome del suo broker.
4. Il broker del cliente acquista dei broker scrip dal broker del commerciante.
5. Il broker del cliente invia gli scrip del broker del commerciante al cliente.
6. Il cliente acquista i vendor scrip dal broker del commerciante.
7. Il cliente utilizza i vendor scrip con il commerciante.

L'idea di base della licensed scrip production può essere intesa come un broker che può generare broken scrip per un altro broker.

Interazioni tra Customer, Broker, e Vendor

Il seguente diagramma (figure 5 a-e) presenta gli step per una sessione completa Millicent (incluso l'acquisto del broker dal commerciante).

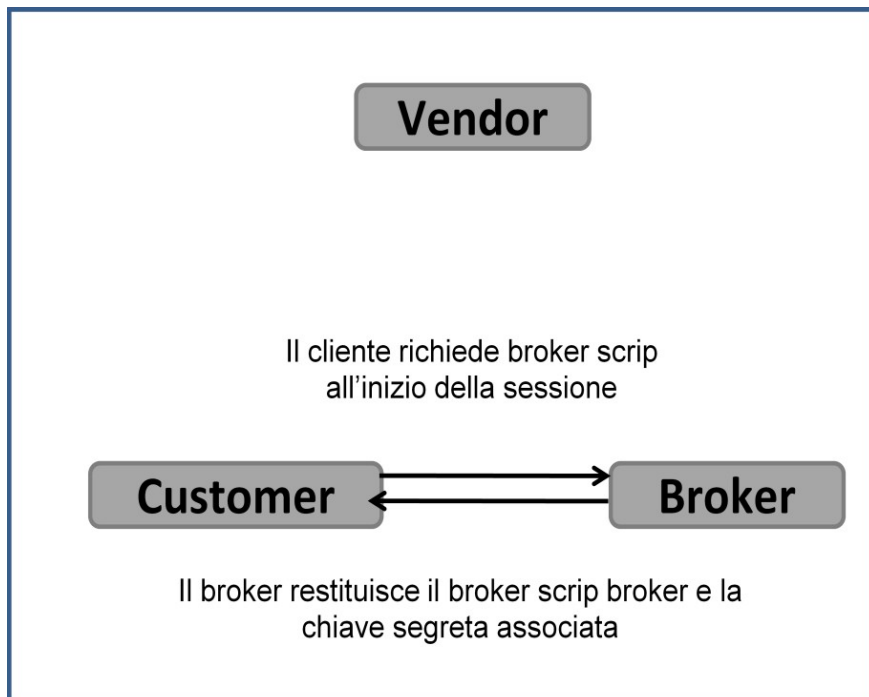


Figura 5a: Il cliente stabilisce una connessione sicura con il broker per avere dei broker scrip.

Questo step iniziale avviene una sola volta per sessione.

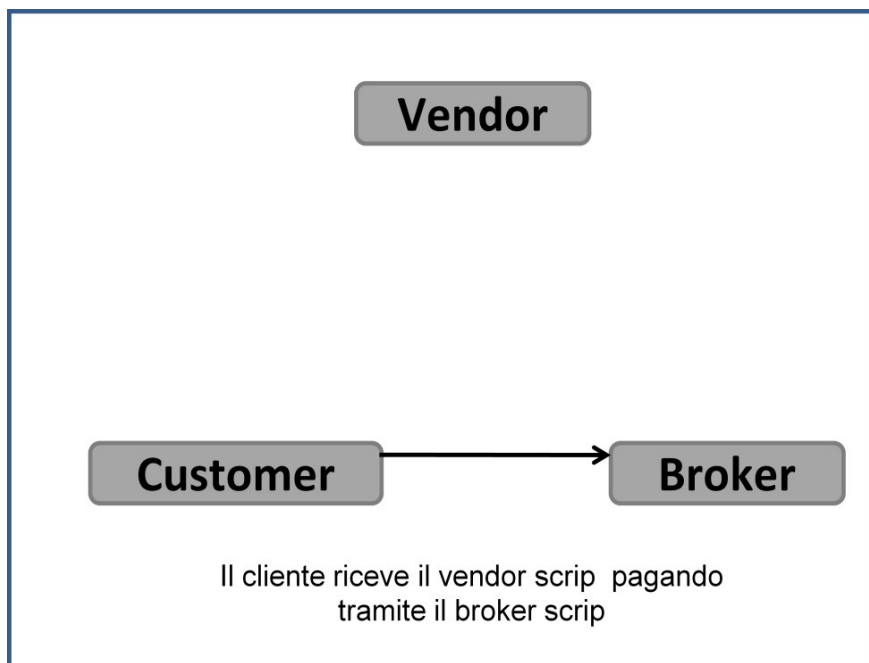


Figura 5b: Il cliente senza vendor scrip, ne chiede al broker usando il suo broker scrip. Questo step avviene ogni volta che il cliente deve acquistare da un venditore e non ha scrip specifici di quel venditore.

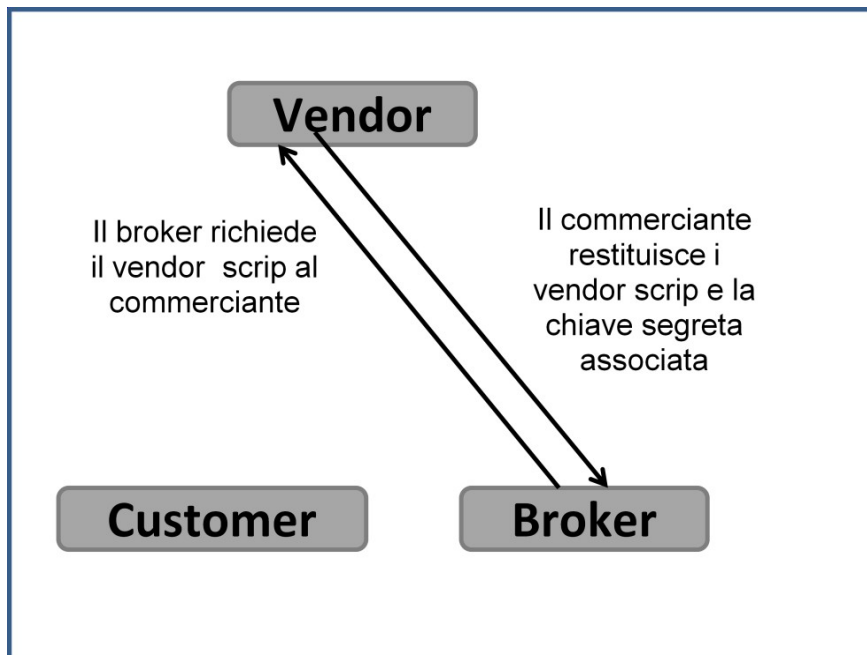


Figura 5c: Se il broker non ha già scrip di quel venditore, egli deve comprarli dal venditore stesso. Questo passaggio avviene soltanto se il broker no ha già in deposito scrip di un vendor. Non è necessario per licensed scrip production.

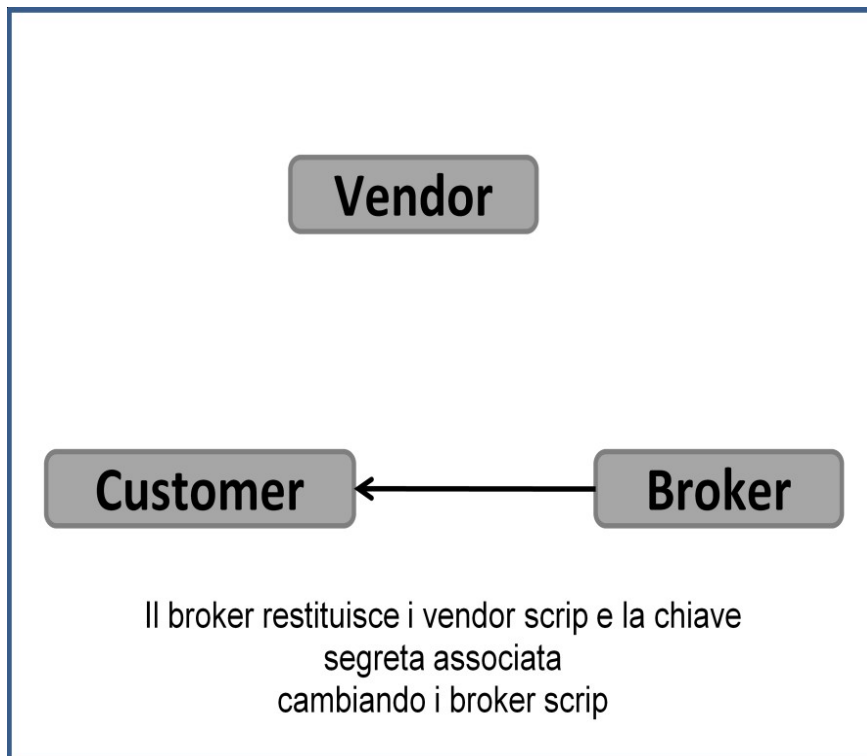


Figura 5d: Il broker rimanda il vendor scrip ed il resto (in broker scrip) al cliente.

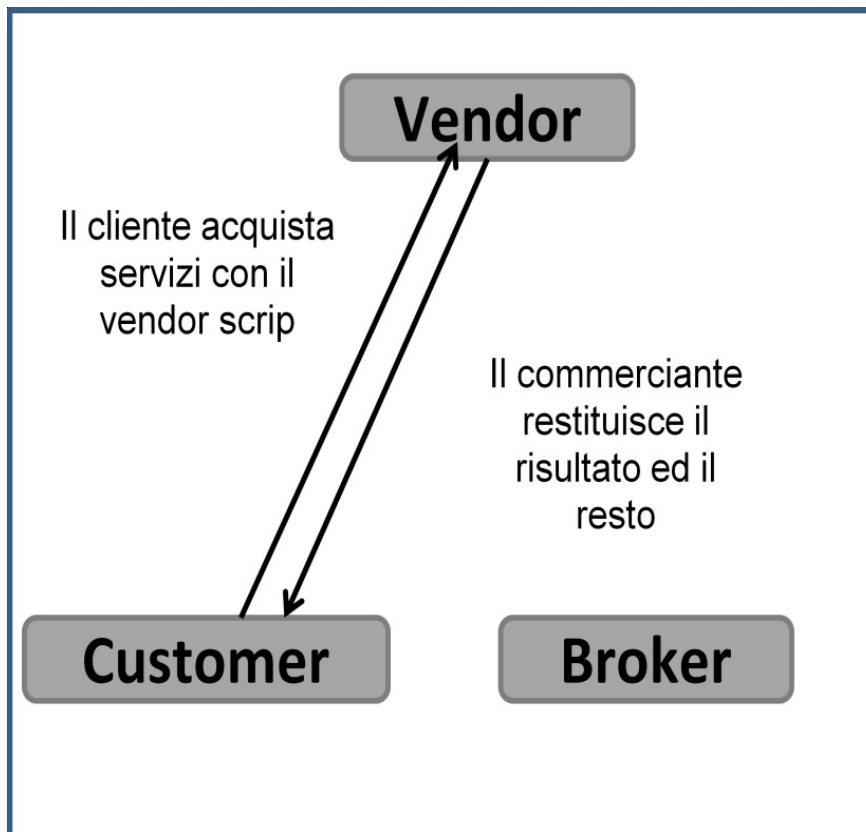


Figure 5e: Il cliente usa il vendor scrip per effettuare un un acquisto del relativo venditore. Il venditore rimanda il resto (in vendor scrip) al cliente.

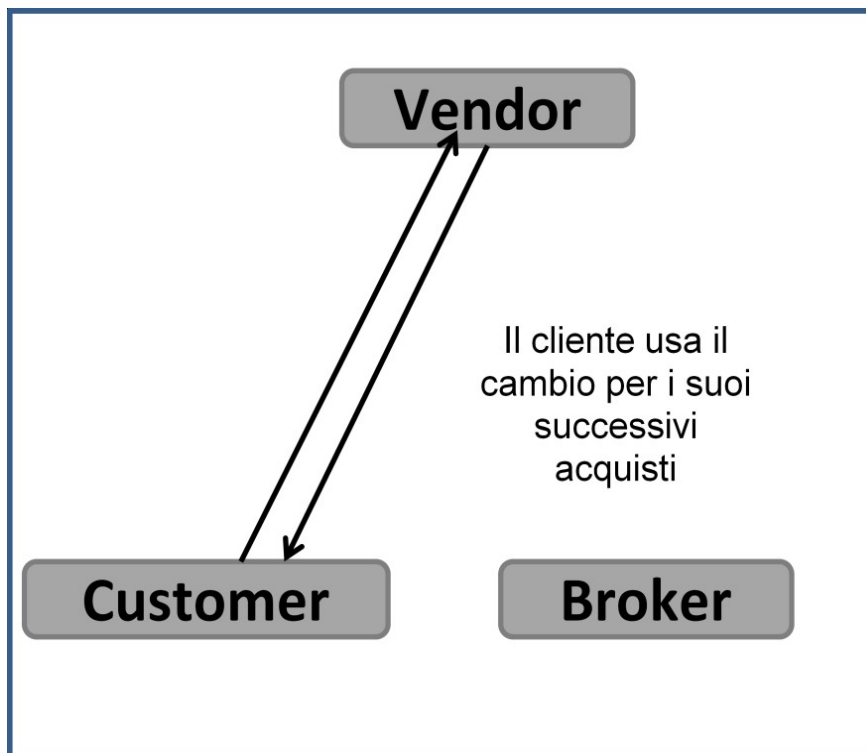


Figura 5f: Il cliente continua a usare il resto per effettuare altri acquisti

Breve storia dei micropagamenti

Millicent è stato uno dei primi protocolli proposti per la gestione delle microtransazioni (o micro pagamenti) alla fine degli anni '90, insieme a IBM Micro Payments, iPIN e NetBill. Anche se oggi non è utilizzato, molte delle intuizioni del modello sono state inserite in future implementazioni o modelli concettuali per la gestione dei micro pagamenti.

Nei primi anni 2000 il modello dei micro pagamenti è stato quasi abbandonato, in favore di altri modelli di business. I guadagni dell'online advertising hanno permesso di mantenere molti siti solo con la pubblicità, mentre per i contenuti a pagamento (riviste scientifiche, giochi online, accesso ad aree riservate), ha funzionato bene il sistema ad abbonamenti (subscription systems).

Negli ultimi anni c'è stata un'inversione di tendenza e molte aziende hanno adattato il loro modello ai micro pagamenti. Dopo un decennio la tecnologia è maturata ed è cresciuta la fiducia della gente nello spendere online. Un modello misto tra pubblicità e micro-transazioni si sta rivelando vincente per molte società di servizi in rete. Per questo è tornato prepotentemente sotto l'occhio del marketing e delle divisioni di ricerca delle aziende il sistema dei micro pagamenti.

Punti chiave per il successo

Più il pagamento è piccolo e "facile", meno l'utente si fa problemi a spendere. Pagare un abbonamento mensile ad una rivista o ad un servizio online implica un utilizzo assiduo, cosa che nel mare magnum di possibilità che offre la rete è sempre più difficile.

Pagare meno di un euro, solo quando realmente serve, è un'ipotesi migliorativa. La carta di credito però non è la soluzione adatta; in primo luogo perché ogni transazione è soggetta a commissione, in secondo luogo (non meno importante), perché l'utente è costretto ad inserire i dati della propria carta di credito e questo porta nella maggior parte dei casi a desistere dall'acquisto.

Oltre all'economicità dei prezzi quindi il successo di un sistema di micro pagamenti è l'aggregazione. La possibilità di avere un unico punto in cui l'utente registra la propria carta di credito e una nutrita rete di "negozi virtuali" dove spendere senza doversi autenticare di nuovo. Qualcosa già schematizzato in Millicent, con la distinzione **customer – broker – vendor**.

Il mercato sta dando ragione alle aziende che per prime hanno intrapreso questa strada e molti nuovi progetti stanno nascendo in tal senso:

Online gaming

Nel settore dei giochi online (MMORPG) è stata per anni legge incontrastata la necessità per gli utenti di sottoscrivere un abbonamento mensile. Negli ultimi due anni moltissimi dei titoli anche più famosi hanno cambiato in favore delle microtransazioni. Gli utenti possono giocare gratis ma alcuni oggetti nel gioco sono acquistabili con soldi veri.

iTunes

Un esempio riuscito di microtransazioni è iTunes di Apple, in cui ogni giorno vengono scaricate 30 milioni di app. iTunes ha il grande merito di aver convinto molti utenti a “pagare” per scaricare la musica, rendendo “facili” e poco costosi gli acquisti.

Facebook credits

Da un anno il più conosciuto social network ha creato il suo sistema di moneta elettronica, spendibile all'interno del network per giochi, applicazioni o regali ad altri utenti. Anche qui il sistema è snello e amichevole. Con lo stesso account che si usa per accedere si possono ricaricare crediti dalla carta di credito. Facebook funge da broker verso gli sviluppatori di giochi e servizi presenti sulla piattaforma. Se voglio animali in Farmville o vestiti per i Sims, non interagisco direttamente con le software house ma con Facebook, che si occupa della transazione dei crediti dall'account dell'utente a quello dello sviluppatore del gioco (il quale sarà pagato con moneta vera ogni mese per il totale delle transazioni effettuate).

Flattr

Il network Flattr è l'ultima idea in fatto di micro pagamenti. E' una rete di piccole donazioni “sociali” per i produttori di contenuti su Internet, ideata da Peter Sunde, fondatore di Pirate Bay.

L'utente crea il proprio account, decide una somma mensile (pochi euro) e naviga normalmente nella rete. Alcuni siti espongono un bottone “Flattr this” (analogo al “Mi Piace” di Facebook o al “Tweet” di Tweeter). Ogni volta che l'utente clicca sul bottone, effettua una micro-donazione all'autore dei contenuti. Si crea così un sistema per cui gli utenti finanziano blogger, musicisti indipendenti e altri “lavoratori” della rete che hanno possibilità così di guadagnare oltre che dalla pubblicità anche direttamente dai loro estimatori.

Anche qui lo schema è composto da utenti, un broker (il circuito Flatrr) e molti “vendor” (anche se impropri), che accettano piccolissime donazioni dagli utenti.

Bibliografia

- S. GLASSMAN, M. MANASSE, M. ABADI, P. GAUTHIER, P. SOBALVARRO – *The Millicent Protocol for Inexpensive Electronic Commerce - World Wide Web Consortium Conference Paper* – <http://www.w3.org/Conferences/WWW4/Papers/246/> (12.4.2012)

- P.J.M. HAVINGA, G.J.M. SMIT, A. HELME – *Survey of electronic payment methods and systems* – University of Twente, Department of Computer Science