

MilliCent Protocol

Caterina Lombardi

Marco Mencacci

Paolo Mengoni

Pagamenti

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

Con l'introduzione di internet ci si è trovati di fronte alla necessità di effettuare dei **micro-pagamenti** il cui di valore inferiore a quello della moneta più piccola (attualmente 1 cent/€).



100 chiodi valgono 1 cent/€. E se ne volessi solo uno?

I classici metodi di pagamento risultano inadeguati poiché non è accettabile sostenere né meccanismi di sicurezza complessi né ritardi nelle transazioni.

Protocolli per micro-pagamenti

Si deve quindi ricercare un protocollo che:

- sia veloce
- abbia un basso costo per transazione
- sia adatto a pagamenti di piccolissimo valore
- sia altamente scalabile
- coinvolga un numero limitato di attori

Protocolli per macro-pagamenti

- Basati su account – hanno alti costi per transazione
- Aggregazione – pesante gestione degli account da parte del venditore
- Moneta elettronica – coinvolge troppi attori, ha una bassa velocità di transazione e quindi è poco scalabile

MilliCent

Il protocollo **MilliCent** è stato sviluppato da DEC per le transazioni internet di basso valore

- supporta transazioni sicure e di basso valore
- utilizza algoritmi di crittografia simmetrica dal basso costo computazionale
- utilizza degli scrip come valuta elettronica
- permette la validazione di questa valuta direttamente nei server del venditore
- elaborazione dati offline: non aggiunge costi di comunicazione ai processi

Come funziona

MilliCent si basa sullo scambio di **scrip** (fogliettini) che sono una rappresentazione del rapporto che si è stabilito fra venditore e acquirente.



Scrip

In ogni momento il venditore ha un certo numero di scrip emessi che rappresentano gli account aperti con i clienti.

Il bilancio dell'account è dato dal valore dello scrip. Il valore iniziale viene progressivamente scalato a ogni acquisto.

Chi è coinvolto

Cliente - acquista scrip dal broker per poi poterli spendere presso il venditore

Venditore - emette scrip che vende al broker

Broker - figura chiave dell'intero processo di vendita degli scrip. Fa da intermediario fra il cliente e il venditore

Ogni soggetto ha diversi livelli di affidabilità.

Vantaggi

Costi di comunicazione contenuti – la verifica degli scrip avviene direttamente presso il venditore

Costi crittografici contenuti – non è necessaria una crittografia avanzata dato l'esiguo valore degli scrip

Gestione degli account semplificata

- Il venditore mantiene i dati degli account dei broker a cui ha venduto gli scrip
- il broker mantiene i dati degli account degli utenti e gestisce l'accredito in valuta reale
- il cliente mantiene il bilancio dell'account all'interno dello scrip

Possono essere evitate commissioni prepagando gli scrip (sia al venditore che al broker)

Sicurezza

Autenticazione

- I segreti (di scrip e cliente) utilizzati per la firma non sono mai inviati in chiaro

Integrità

- Gli scrip firmati rendono inattuabile la modifica

Confidenzialità

- Non viene gestita in quanto le transazioni sono di valore così esiguo da non richiedere policy apposite

Scrip /1

Proprietà

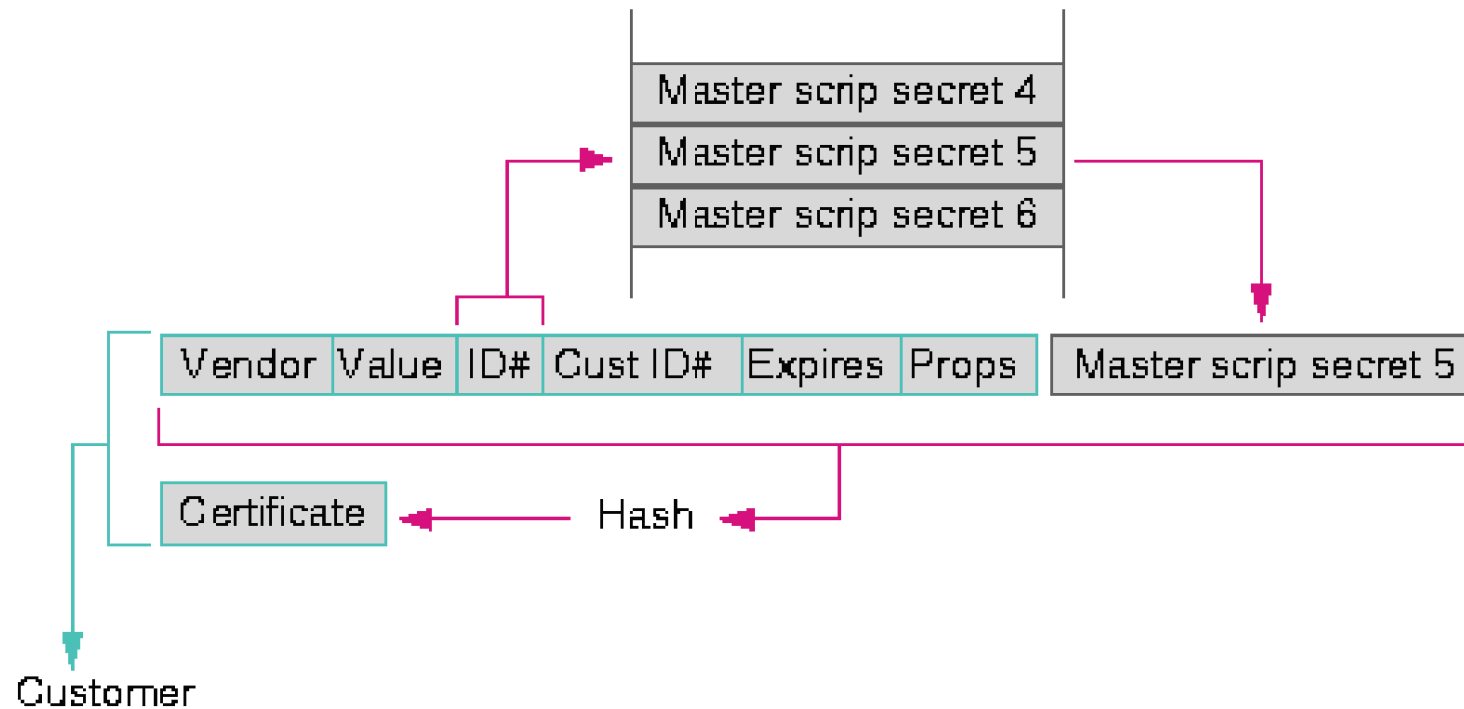
- il venditore presso il quale è spendibile è identificato nello scrip stesso
- il suo valore è predeterminato
- ha un numero seriale che ne determina il singolo utilizzo
- è spendibile solo dal proprietario
- ha una validità prefissata
- è personalizzabile tramite proprietà

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

- è firmato digitalmente per renderlo resistente alle contraffazioni
- prodotto e validato efficientemente tramite funzioni hash

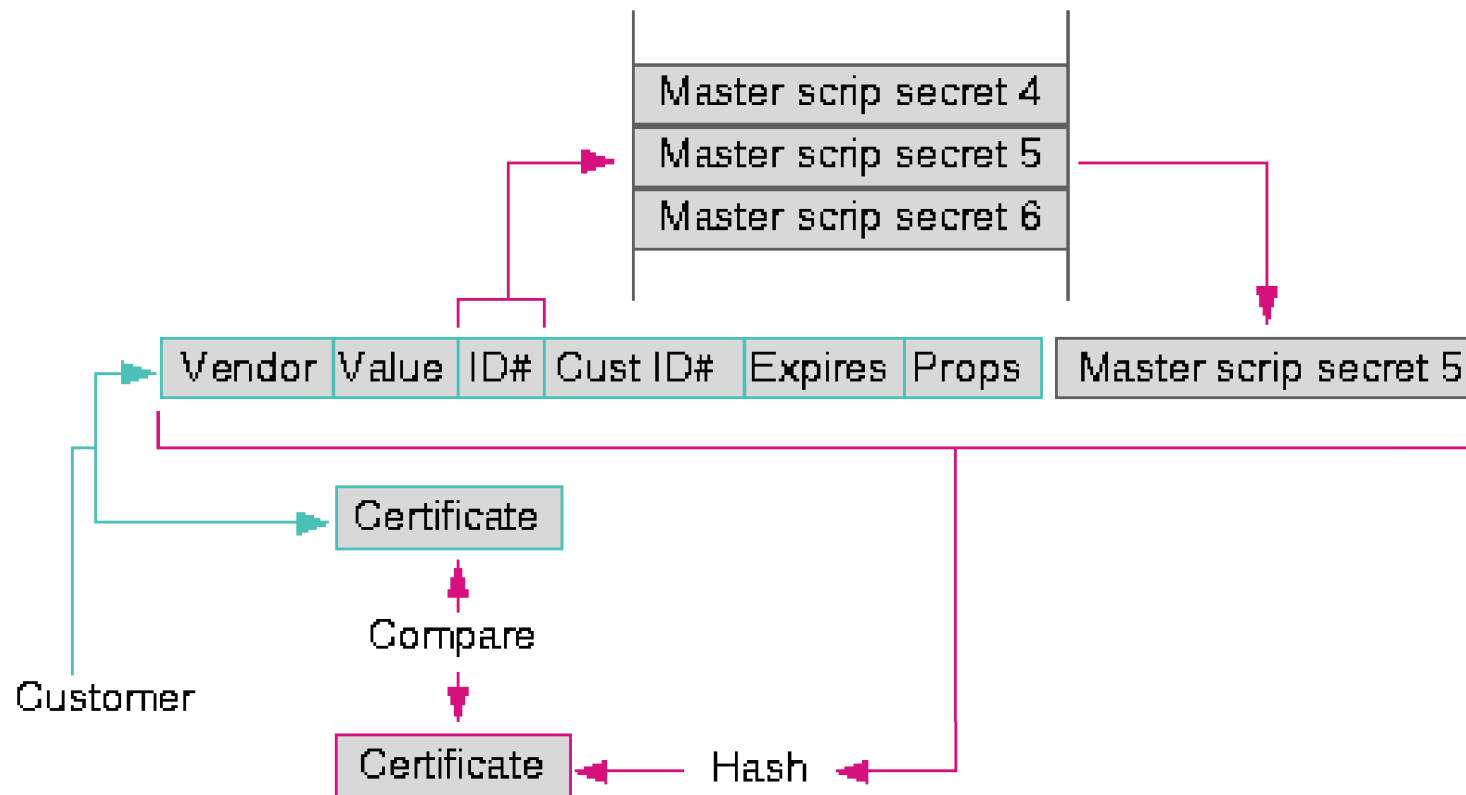
Scrip /2

Creazione dello scrip



Scrip /3

Validazione dello scrip



Broker 1/2

- Mantiene i conti di clienti e venditori
- Effettua tutte le transazioni in denaro reale
- Ottiene vendor scrip dai commercianti
- Vende broker scrip ai clienti
- Cambia in moneta reale gli scrip spesi dai clienti

Broker 2/2

Ottiene i vendor scrip con 3 modalità diverse:

1. Scrip warehouse
2. Licensed scrip production
3. Multiple brokers

Scrip warehouse 1/2

- acquista in blocchi i vendor scrip dai commercianti
- rivende un vendor scrip alla volta ai clienti
- non esiste nessuna relazione particolare tra broker e vendor

Scrip warehouse 2/2

VANTAGGI/SVANTAGGI

- Non presuppone nessuna relazione particolare tra vendor e broker
- Il broker deve avere un'idea chiara delle possibili richieste del cliente
- Il vendor deve effettuare vendite in blocchi
- Il vendor deve applicare uno sconto sulle grandi quantità
- Il broker ricava un profitto rivendendo gli scrip singolarmente

Licensed scrip production 1/2

- Un commerciante dà una “licenza” ad un broker
- Il commerciante può verificare in qualsiasi momento chi ha emesso gli scrip
- Alla scadenza della “licenza” broker e commerciante decidono se sottoscriverne un'altra
- Un commerciante può dare la “licenza” a più broker

Licensed scrip production 2/2

VANTAGGI /SVANTAGGI

- E' più efficiente per il vendor e il broker
- La trasmissione dei dati è meno pesante
- Il commerciante ha un onere della computazione inferiore
- Il broker non deve tenere in deposito grandi blocchi di scrip
- Per il broker è più semplice garantire le proprietà specifiche di uso codificate in ciascun di scrip generato.

Multiple brokers 1/2

Intera transazione :

- Il cliente contatta il suo broker per dei vendor scrip.
- Il broker del cliente prova a stabilire un account con il commerciante.
- Il commerciante comunica al broker del cliente il nome del suo broker.
- Il broker del cliente acquista dei broker scrip dal broker del commerciante.
- Il broker del cliente invia gli scrip del broker del commerciante al cliente.
- Il cliente acquista i vendor scrip dal broker del commerciante.
- Il cliente utilizza i vendor scrip con il commerciante.

Multiple brokers 2/2

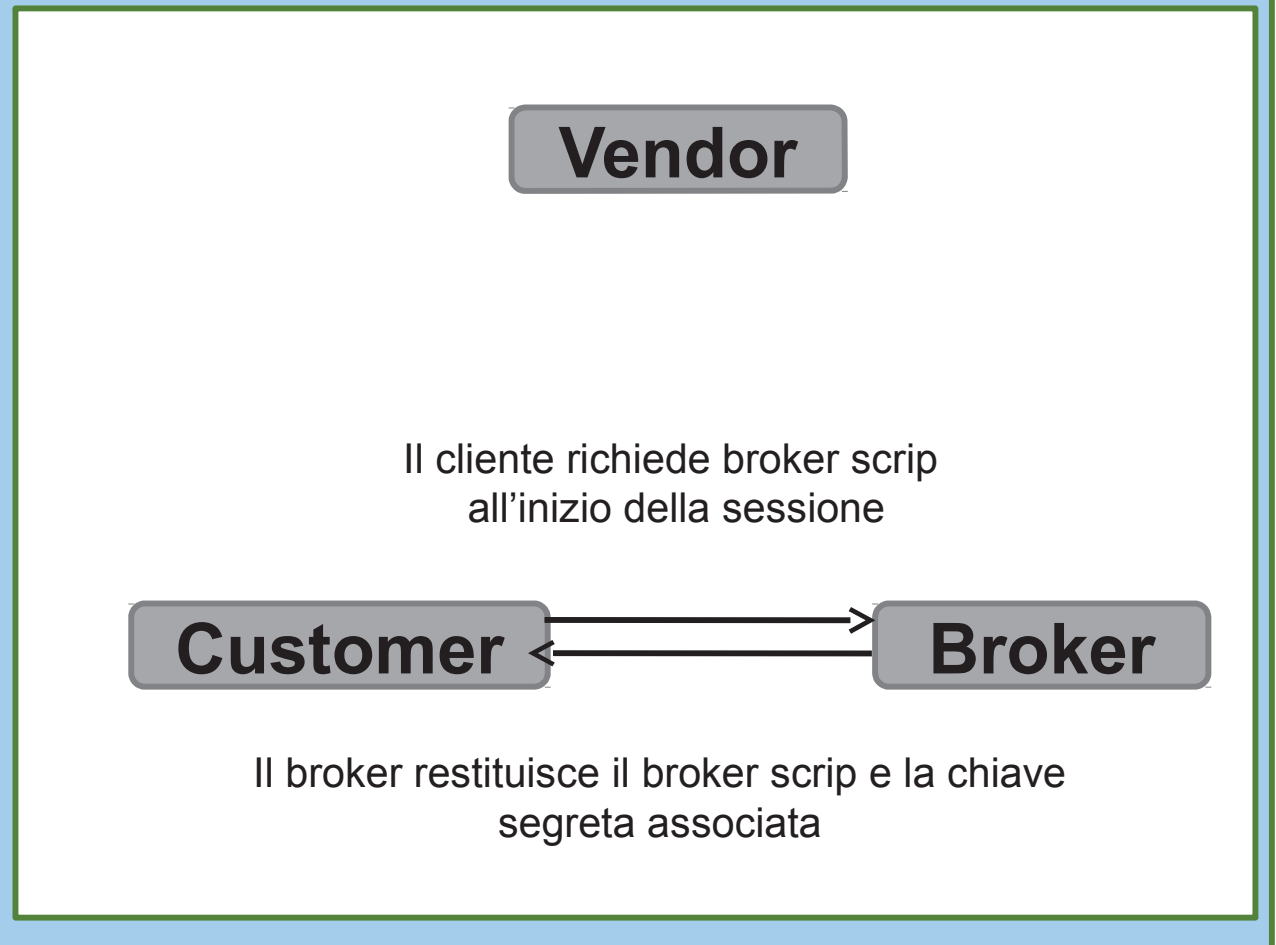
VANTAGGI/SVANTAGGI

- La transazione risulta più macchinosa
- Il cliente attraverso il suo broker può acquistare da qualsiasi vendor
- Un commerciante può vendere a più clienti pur avendo rapporti con un solo broker
- Un broker può generare broker scrip di un altro broker

Interazione broker, vendor e customer

Passo 1

Viene eseguito una sola volta nel corso dell'intera sessione



Interazione broker, vendor e customer

Passo 2

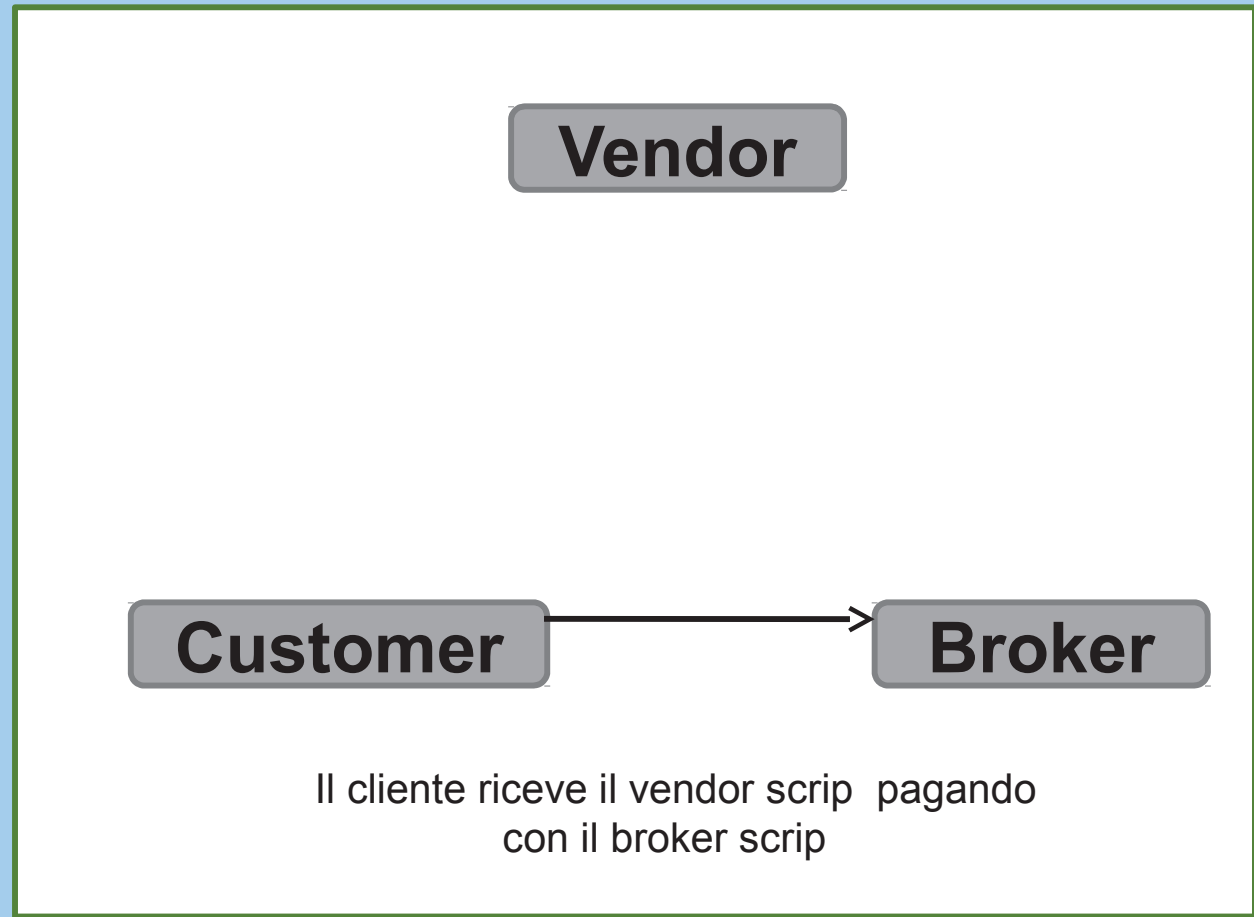
Si rende necessario ogni volta che il cliente non ha lo scrip relativo ad un determinato commerciante

Vendor

Customer

Broker

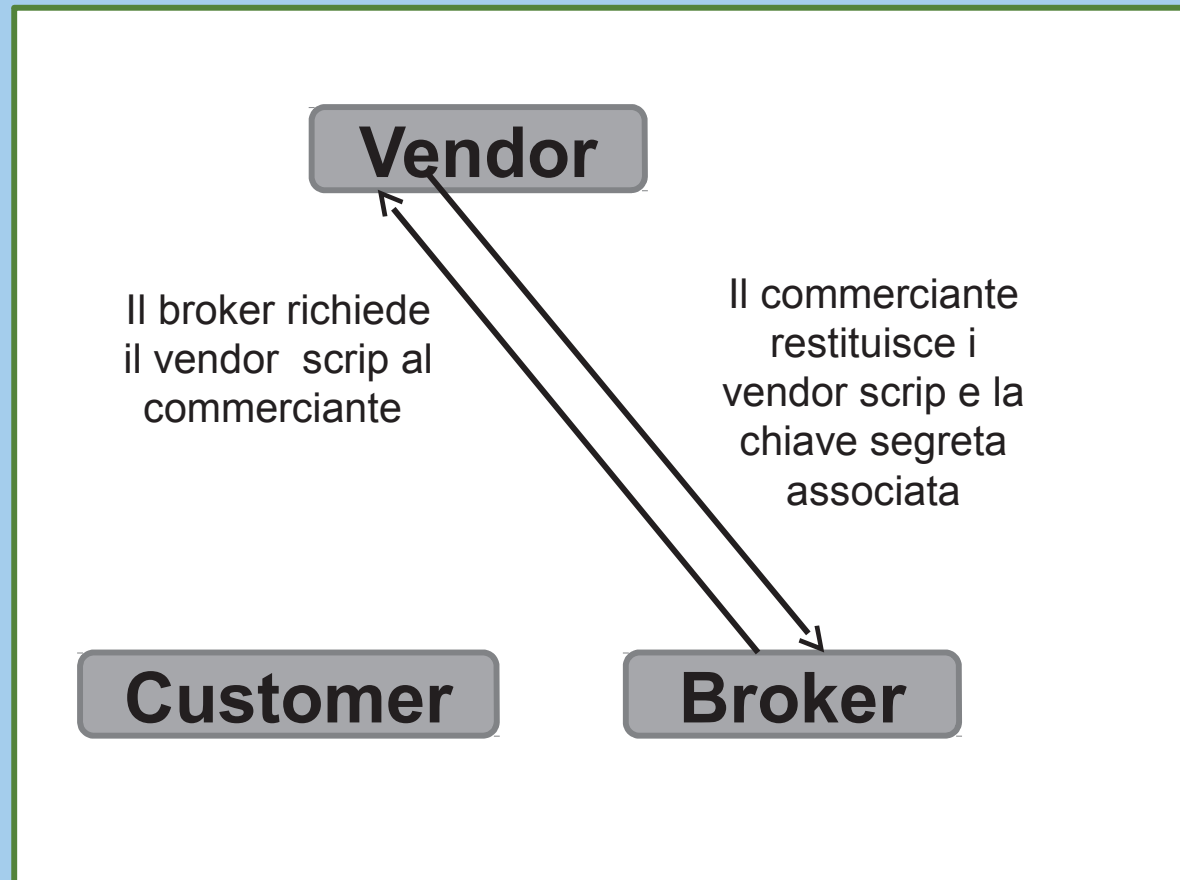
Il cliente riceve il vendor scrip pagando con il broker scrip



Interazione broker, vendor e customer

Passo 3

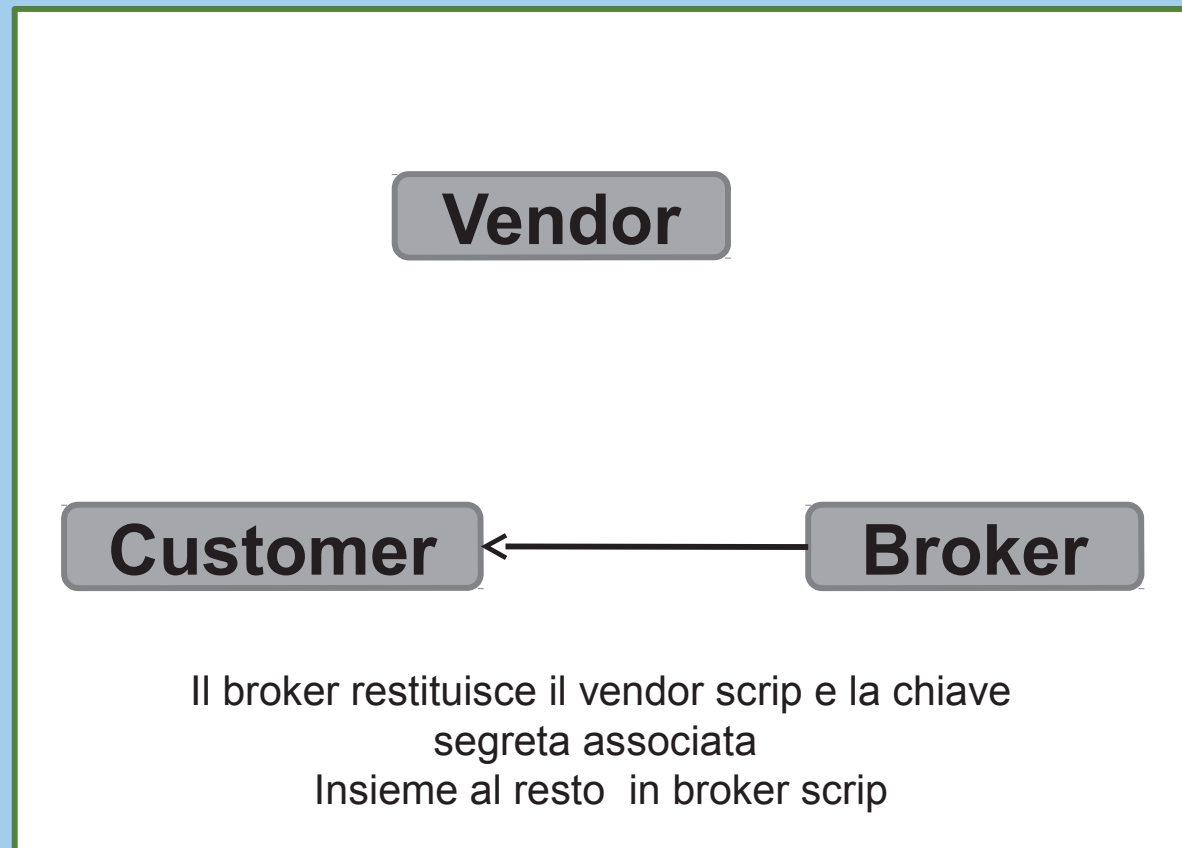
Si ha solo se il broker deve contattare un determinato commerciante per acquistare i vendor scrip



Interazione broker, vendor e customer

Passo 4

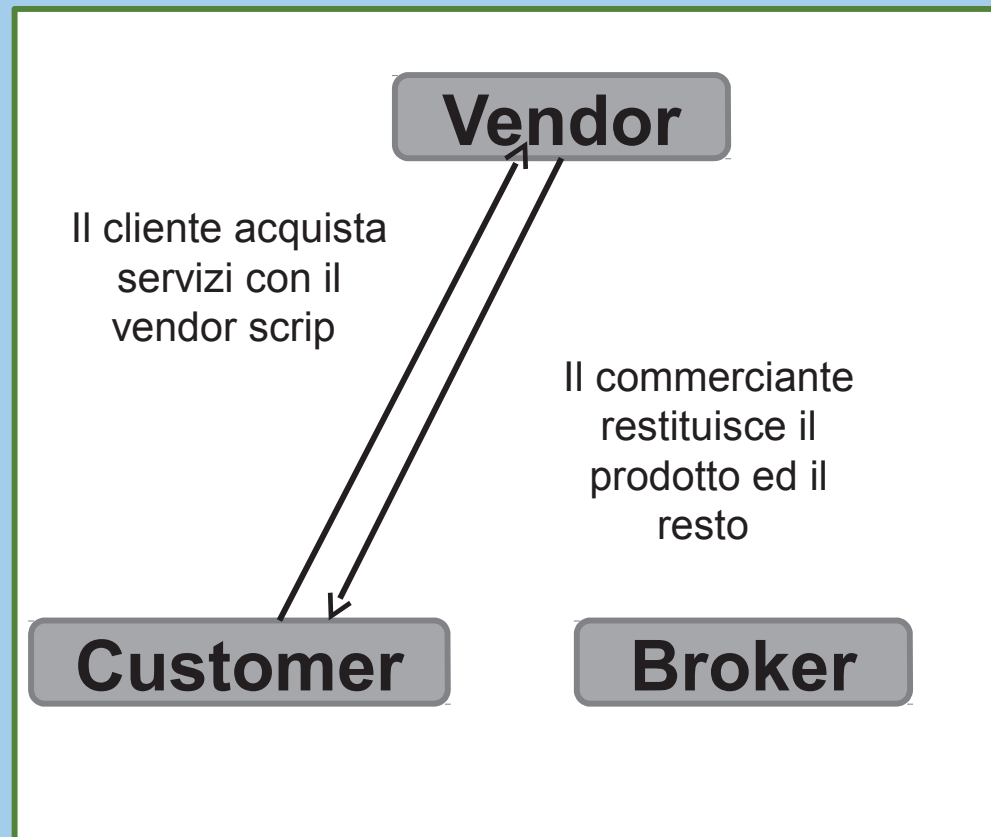
Si ha quando il broker restituisce lo scrip al cliente che lo ha chiesto precedentemente



Interazione broker, vendor e customer

Passo 5

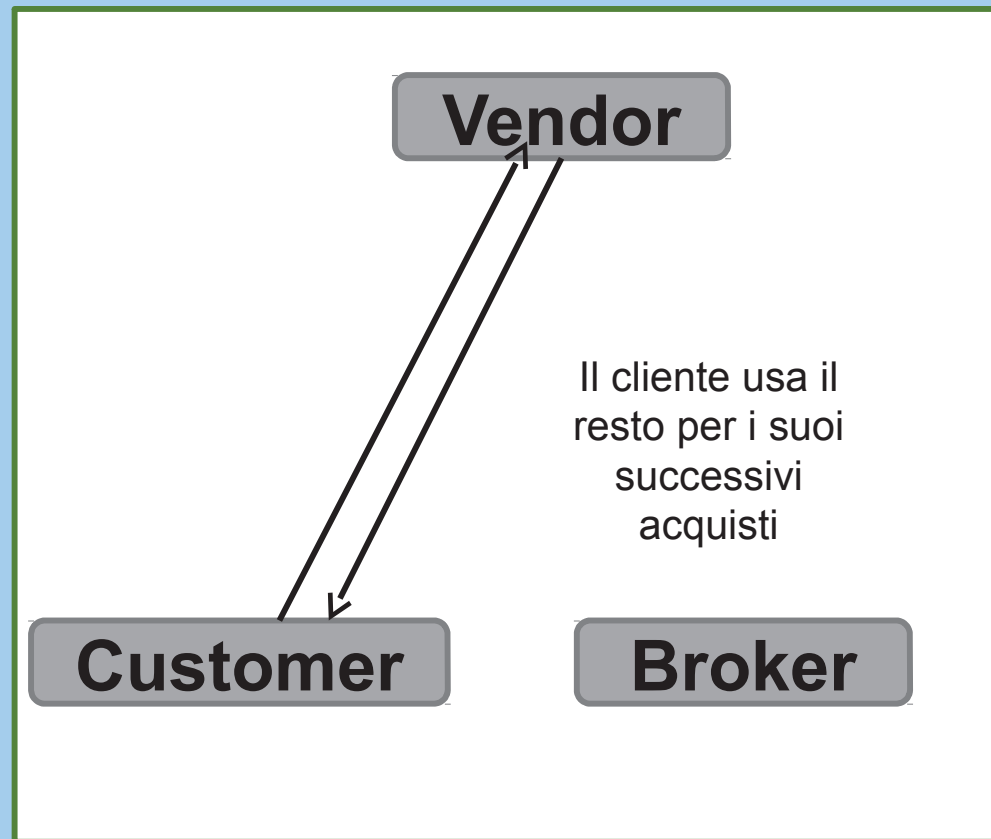
Il cliente usa lo scrip per acquistare



Interazione broker, vendor e customer

Passo 6

Mostra una tipica transazione Millicent: il cliente ha già lo scrip del commerciante e lo utilizza per fare acquisti



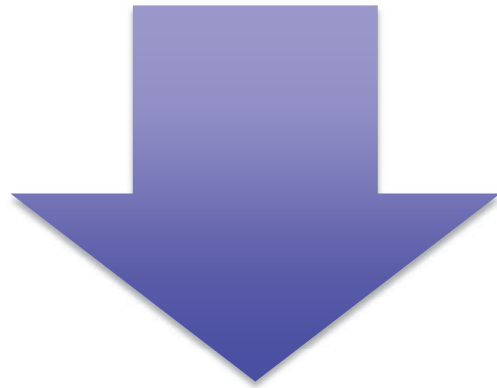
Millicent

INEXPENSIVE



YET SECURE

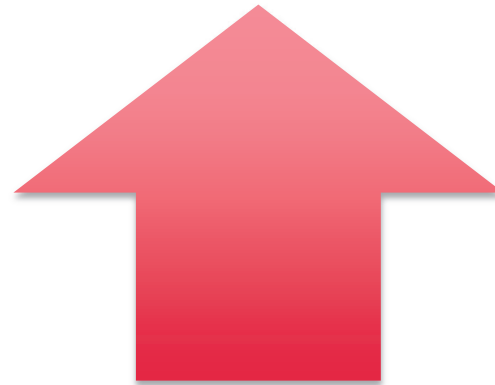
Goal



Inexpensive:
Ridurre costi
computazionali e
“peso” delle
comunicazioni



Secure:
Garantire che il
costo dell'attacco
sia maggiore del
beneficio



Implementazioni del protocollo

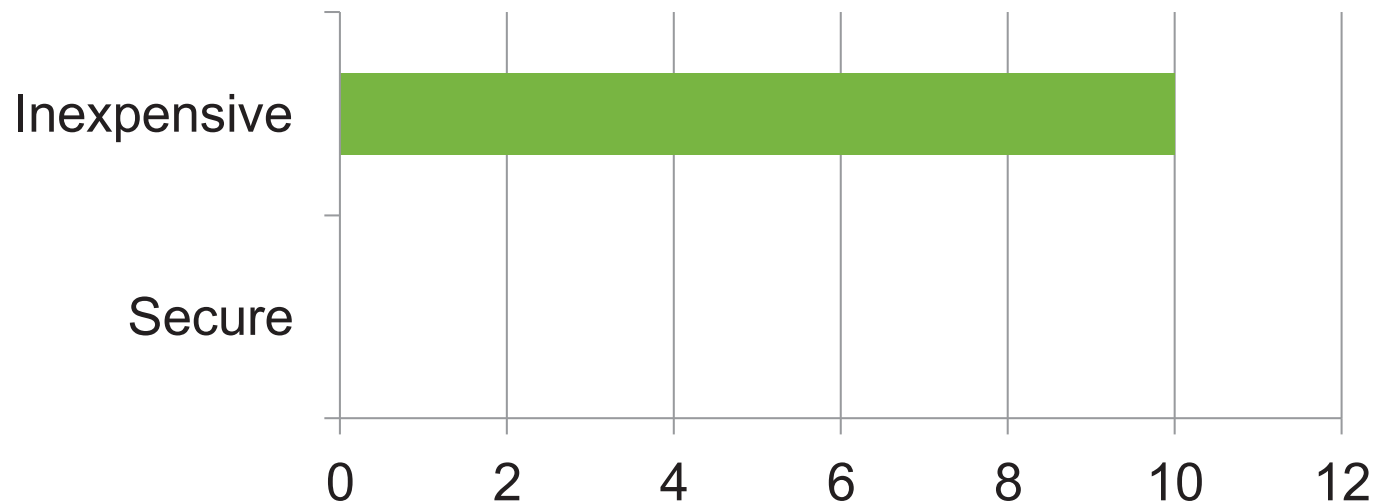
Esistono varie possibilità per garantire i goal del protocollo:

- Script in the clear
- Private and secure
- Secure without encryption

Scrip in the clear

- Il cliente spedisce al vendor la richiesta e lo scrip in chiaro
- Il vendor processa la richiesta e risponde con un nuovo scrip (sempre in chiaro) come resto

Rispetto degli obiettivi



Scrip in the clear

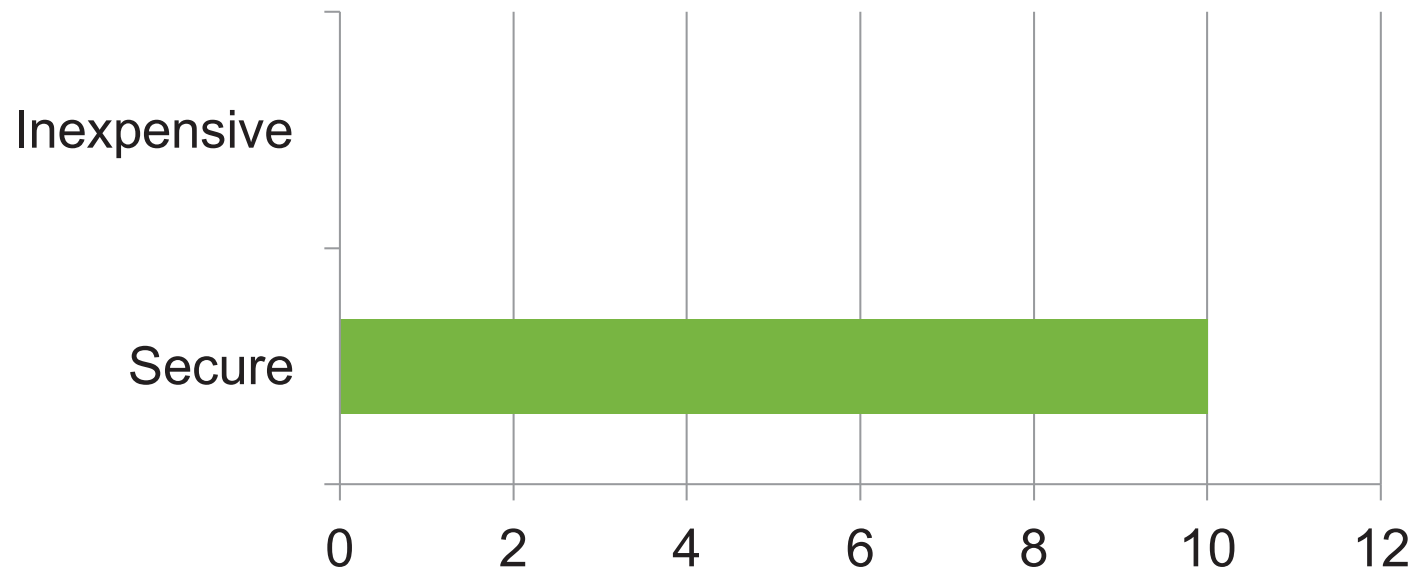
- Il cliente spedisce al vendor la richiesta e lo scrip in chiaro.
- Il vendor processa la richiesta e genera un nuovo scrip (sempre in chiaro) come resto.



Private and secure

- Si utilizza il **customer secret** come chiave condivisa per creare un canale di comunicazione sicuro
- Un qualsiasi soggetto in ascolto sul canale non riesce ad intercettare nulla perché tutto è cifrato

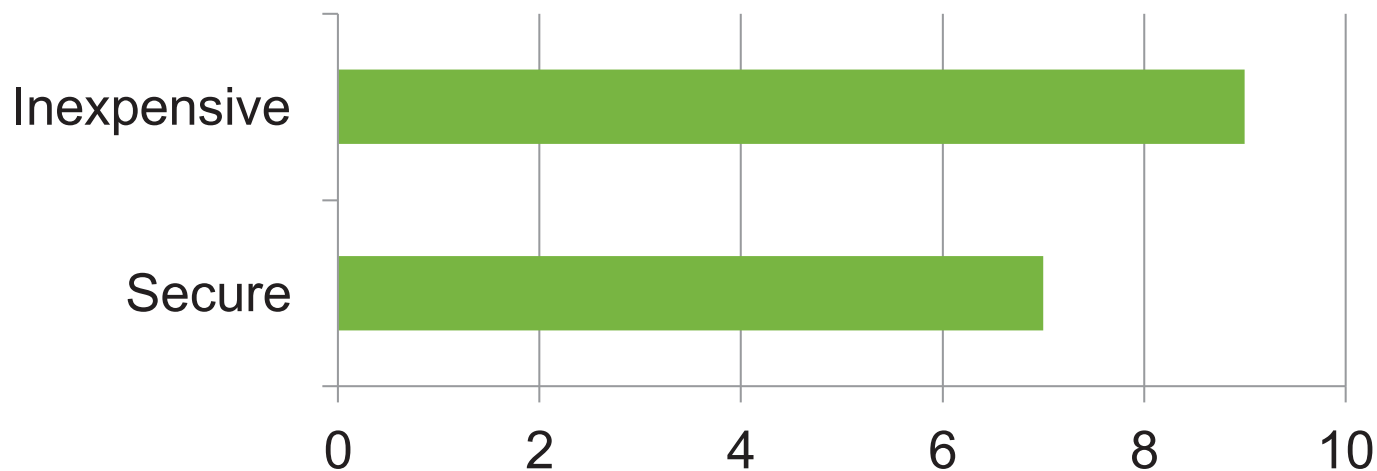
Rispetto degli obiettivi



Secure without encryption

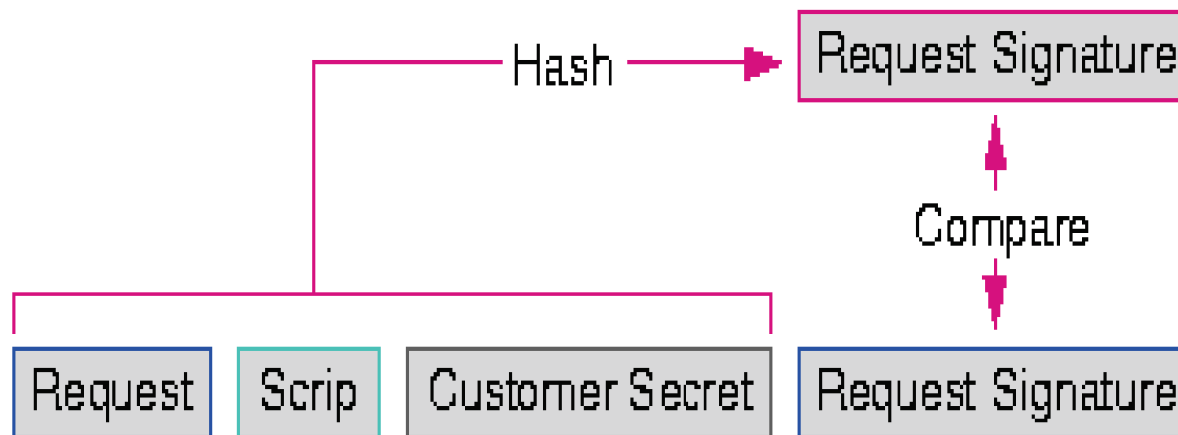
- Il customer secret viene utilizzato per firmare le richieste
- La firma è l'hash di [scrip+request+customer_secret]
- Quando il vendor riceve la richiesta, controlla la corrispondenza dell'hash con quello da lui calcolato
- Non c'è alcun bisogno di cifrare la risposta

Rispetto degli obiettivi



Secure without encryption

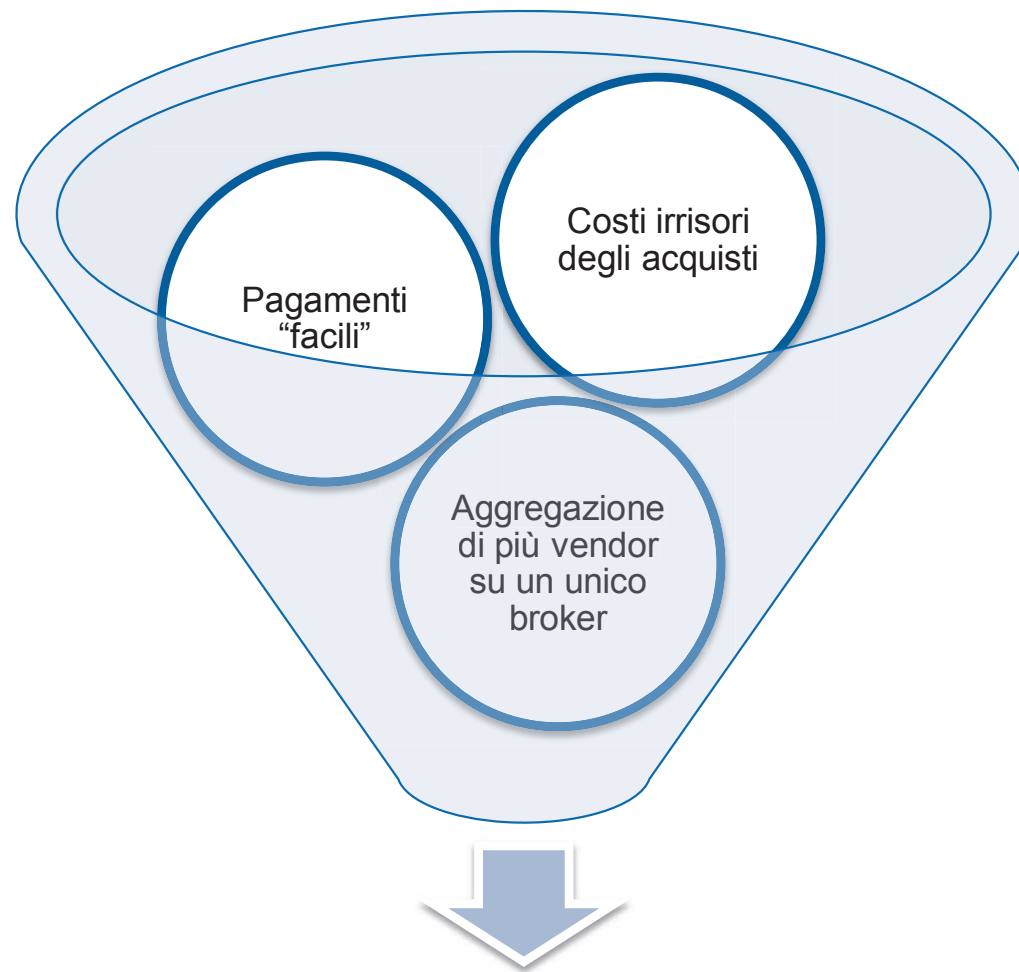
Utilizzando soltanto una funzione hash, si realizza un protocollo leggero e ragionevolmente sicuro.



L'eredità del Millicent

- Un protocollo per micropagamenti si differenzia da un protocollo per (macro)pagamenti perché:
 - Deve prevedere transazioni frequenti e contemporanee
 - Deve “facilitare” i pagamenti (non costringere gli utenti a digitare dati, pin, password ad ogni transazione)
 - Deve limitare al massimo i movimenti di denaro vero per evitare commissioni dagli istituti di credito

Sistemi di micropagamento punti chiave



Gli utenti spendono più

Micropagamenti.. Sono usati?

- Dopo un periodo di abbandono nei primi anni del millennio, il tema dei micropagamenti è tornato alla ribalta:
 - E' aumentata la fiducia degli utenti nello spendere in rete
 - Chi ha adottato i micropagamenti come modello di business sta guadagnando

Micropagamenti oggi

- Online gaming



- iTunes



- Facebook credits



- Flattr



Grazie!

