

UNIVERSITÀ DEGLI STUDI DI PERUGIA  
Facoltà di Scienze Matematiche, Fisiche e Naturali

---

Corso di Laurea in INFORMATICA



Sicurezza Informatica

**Il Protocollo iKP**

*Pietro Montanari & Cosimo Basile*

---

Anno Accademico 2011–2012

# Indice

<b>Introduzione</b>	<b>1</b>
<b>1 Impostazioni di base</b>	<b>3</b>
<b>2 Protocollo</b>	<b>7</b>
2.1 1KP . . . . .	8
2.2 2KP . . . . .	9
2.3 3KP . . . . .	10
2.4 Chiavi pubbliche e certificazioni . . . . .	11
2.5 2KP vs 3KP . . . . .	12
<b>Bibliografia</b>	<b>13</b>

# Introduzione

Il protocollo iKP (Internet Keyed Payment Protocol), sviluppato dalla IBM, è un prototipo di sistema di pagamento su Internet basato su carta di credito. È stato la base dello standard SEPP di Mastercard, poi abbandonato in favore del nuovo standard SET, in cooperazione con VISA. iKP può facilmente essere usato per implementare un sistema di assegni elettronici.

Il protocollo iKP era stato originariamente pensato come contributo alla standardizzazione piuttosto che come una tecnologia di proprietà IBM. iKP è stato progettato per:

- Ottenere un alto livello di integrità per tutte le parti coinvolte, tenendo conto delle differenze di rischio e di esigenze tra una parte e l'altra.
- Fornire riservatezza nelle transazioni economiche.
- Lavorare con il minimo impatto sui sistemi finanziari esistenti.

Pur fornendo quanto necessario per pagamenti sicuri, iKP:

- Non consente alcuna trattativa su modalità di pagamento, prezzo ecc.: contiene una semplice procedura di contratto (offerta/ordine).
- Non fornisce la non tracciabilità dei pagamenti (ma protegge dal venditore i dati del compratore).

- Non fornisce mezzi per una distribuzione sicura di informazioni: fornisce ricevute di pagamento ma non le protegge.

# Capitolo 1

## Impostazioni di base

Come in tutti i sistemi di pagamento elettronico le parti interessate alle transazioni economiche sono: compratore, venditore, acquirente, fornitore. Tuttavia, nel sistema iKP, le parti direttamente coinvolte sono tre: il compratore, il venditore ed il gateway dell'acquirente, come indicato in Figura 1.1.

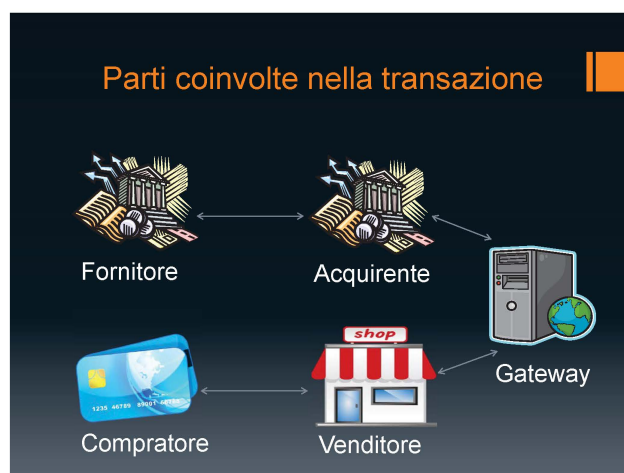


Figura 1.1: Le parti coinvolte nel sistema iKP

Il sistema di pagamento è gestito da un'organizzazione tipo Mastercard, VISA. Tali enti hanno relazioni fisse di affari con certe banche che agiscono da fornitore di carta di credito per il compratore e da acquirente dei pagamenti per il venditore. Ogni fornitore ha un BIN (Bank Identification Number), che riceve al momento in cui stipula il contratto con l'organizzazione che gestisce il sistema, e che è in rilievo su ogni carta di credito fornita, come parte del numero di carta di credito. Il BIN identifica inoltre l'organizzazione che gestisce il sistema. È molto importante notare la presenza del gateway (dell'acquirente): tale entità funziona da interfaccia tra il mondo elettronico e l'infrastruttura per pagamenti già esistente. Il gateway autorizzerà le transazioni usando proprio tale infrastruttura: la rete commerciale di compensazione/autorizzazione per carte di credito.

Il protocollo sfrutta le solite primitive crittografiche. Per l'autenticazione di un messaggio iKP usa:

- Firma digitale;
- Codifica dei segreti con protocollo a chiave pubblica di tipo plaintext-aware;

La codifica di tipo plaintext-aware è un modo di operare che assicura l'integrità dei messaggi, ed è sicuro sotto ragionevoli ipotesi. Al contrario della firma digitale, tale metodo non consente la risoluzione di contestazioni. Per la riservatezza, iKP sfrutta due meccanismi:

- I dati segreti che devono essere verificati dal destinatario ma che non necessitano di essere trasmessi, sono nascosti sfruttando funzioni salted hash (per esempio un numero  $N$  può essere nascosto nella funzione  $h(N,x)$ , dove  $x$  è un valore random noto a mittente e destinatario).

- Codifica a chiave pubblica di tipo plaintext-aware.

iKP limita la codifica a quei dati che l'acquirente deve ricevere dal compratore per avviare il pagamento (per esempio il numero di carta di credito) e a quei dati che consentono l'autentica del compratore (come PIN o valori random usati nelle funzioni hash). Tali tipi di restrizioni non riducono il grado di sicurezza di iKP. Infatti, dal momento che tutte le parti possono firmare, e visto che i dati usati per identificare il compratore non sono utilizzabili per pagamenti senza la firma digitale del compratore stesso, non esisterebbe la necessità di alcuna codifica. Il motivo per cui iKP utilizza la codifica anche se il compratore sfrutta la firma elettronica dipende dal fatto che in Internet i dati di una carta di credito possono essere usati come in transazioni commerciali ordinarie. Il compratore non è responsabile per tali transazioni; tuttavia, transazioni contraffatte sono fonte di problemi sia per il compratore che per il mercante che le ha accettate.

Esistono tre varianti del protocollo iKP, identificate dal valore dell'indice  $i$  presente nel nome.

- In 1KP solo l'acquirente può firmare i messaggi (cioè solo l'acquirente possiede una coppia di chiavi pubblica e privata).
- In 2KP anche il venditore può firmare (esistono due proprietari di coppie di chiavi).
- In 3KP anche il compratore può firmare (esistono tre proprietari di coppie di chiavi).

Tutti i protocolli iKP possono essere implementati sia via software che via hardware. In 1KP e 2KP il cliente non necessita di un dispositivo di paga-

mento personalizzato: per completare un pagamento bastano il numero di carta di credito e il PIN (se presente). Comunque, per garantire maggiore sicurezza, è raccomandabile l'utilizzo di dispositivi anti-frode che proteggano il PIN e, nel caso 3KP, la chiave segreta del cliente.

È importante sottolineare ancora che lo scopo dei protocolli iKP è quello di abilitare ai pagamenti. iKP non si preoccupa di gestire come l'ordine venga inoltrato; iKP assume che l'ordine, incluso il prezzo, sia già stato concordato fra compratore e venditore. Inoltre, iKP non consente alcuna codifica dei dati relativi all'ordine. Si suppone che tale tipo di protezione sia fornita da altri protocolli esistenti, come SHTTP e SSL . Il prototipo iKP supporta solo i protocolli 2KP e 3KP; questo perché 1KP, pur essendo un protocollo molto semplice, non permette la risoluzione di contestazioni tra compratore e venditore.

# Capitolo 2

## Protocollo

Lo scenario è lo stesso per ognuno dei tre protocolli iKP. Durante la discussione del protocollo useremo la seguente notazione:

**B** : Cliente che effettua il pagamento;

**S** : Commerciante che riceve il pagamento;

**A** : Acquirente che agisce come un intermediario tra il mondo elettronico e le infrastrutture di pagamento già esistenti, ed autorizza le transazioni usando tali infrastrutture;

**H** : una funzione hash one-way;

**E<sub>i</sub>** : cifratura usando la chiave pubblica del partecipante *i*;

**S<sub>i</sub>** : firma usando la chiave privata del partecipante *i*;

**Cert<sub>i</sub>** : certificato della chiave pubblica del partecipante *i*;

**Offer** : descrizione dell'offerta, somma da pagare, valuta, data, identificatore del commerciante, indirizzo del destinatario;

**Order** : descrizione dell'ordine, valuta, data, identificatore, indirizzo del destinatario;

**Slip** : somma da pagare, valuta, data, identificatore del commerciante, numero di carta di credito, data di scadenza, PIN, H (Order);

**Auth** : approvazione/rifiuto, H (somma da pagare, valuta, data, identificatore del commerciante) , H (Order);

## 2.1 1KP

1KP è il protocollo di base. In 1KP, solo l'acquirente ha una chiave pubblica. Le transazioni del protocollo sono le seguenti:

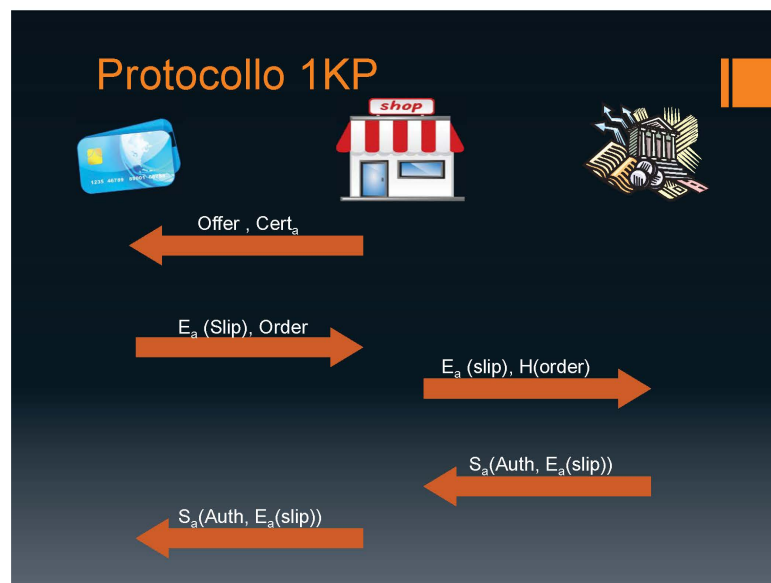


Figura 2.1: Il protocollo 1KP

Ci sono alcune cose interessanti da notare in questo protocollo: l'acquirente vede solo il valore della funzione hash calcolata sull'ordine di acquisto, e non la descrizione della merce, garantendo la privacy del cliente. Sia il cliente che l'acquirente non hanno nessuna sicurezza sull'identità del commerciante. Il cliente è identificato solo dal suo numero di carta di credito e dal PIN. Si noti che 1KP può essere implementato molto facilmente, dal momento che solo l'acquirente possiede una chiave pubblica. 1Kp è un protocollo semplice ed efficiente, ed il suo principale scopo è di ottenere un sistema di pagamento elettronico sicuro, con piccole modifiche sulle strutture già esistenti. Le sue principali debolezze sono:

- il cliente autentica se stesso all'acquirente solamente usando il numero di carta di credito ed il pin;
- il commerciante non autentica se stesso al cliente o all'acquirente: né il commerciante né il cliente forniscono ricevute inconfutabili della transizione.

## **2.2 2KP**

Questo protocollo risolve il problema che riguarda l'identità del commerciante, assumendo che anche il commerciante abbia una chiave pubblica. Questa modifica fa sì che il commerciante debba inviare il suo certificato sia al cliente che all'acquirente. Il protocollo è il seguente:

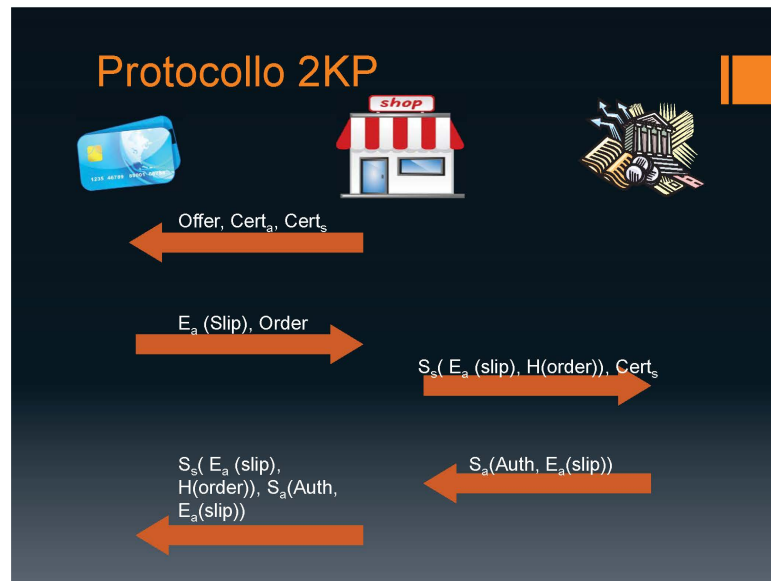


Figura 2.2: Il protocollo 2KP

E' preferibile che il commerciante firmi il messaggio 1, in questo modo il cliente sarebbe sicuro della validità dell'offerta. Si noti anche che, invece di ripetere il messaggio 3 nel messaggio 5, il commerciante potrebbe firmare il messaggio 5 ma questo aggiungerebbe il tempo della firma al costo del protocollo.

### 2.3 3KP

In 3kp anche il cliente ha una chiave pubblica. Il protocollo è modificato per fare in modo che il cliente mandi il suo certificato al commerciante (che viene poi mandato all'acquirente) e che firmi il messaggio 2. il protocollo è il seguente:

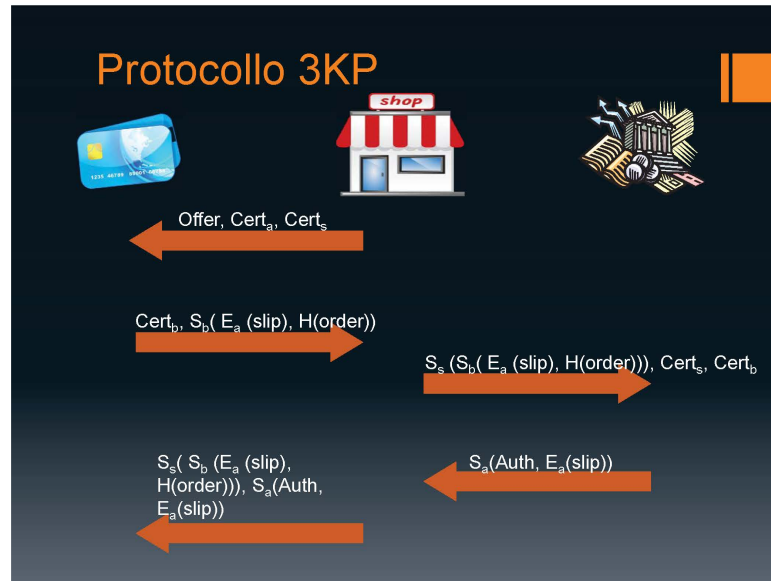


Figura 2.3: Il protocollo 3KP

Si noti che poiché ogni partecipante possiede una chiave pubblica deve essere implementato uno schema per la distribuzione dei certificati.

## 2.4 Chiavi pubbliche e certificazioni

Dal momento che tutti i protocolli iKP sono basati su crittografia a chiave pubblica, si rende necessario un meccanismo per autenticare tali chiavi pubbliche. Si assume l'esistenza di un'Autorità di Certificazione, AC, con la propria chiave segreta,  $CS_{AC}$ . La rispettiva chiave pubblica,  $CP_{AC}$ , è distribuita a tutte le altre parti. L'autorità di certificazione autenticerà la chiave pubblica della parte X firmando la coppia  $(X, CP_X)$ , cioè l'identità di X e la sua chiave pubblica. Tale firma è calcolata sfruttando la  $CS_{AC}$ . È

da notare che la  $CP_{AC}$  deve essere distribuita in modo sicuro alle altre parti; tipicamente questo si ottiene con comunicazioni fuori banda.

In tutti i protocolli iKP, dunque, l'acquirente A ha la propria chiave segreta,  $CS_A$ , che abilita alla firma e alla decodifica. La corrispondente chiave pubblica,  $CP_A$ , (che abilita alla verifica della firma e la codifica) è posseduta da ogni venditore accreditato, insieme al corrispondente certificato rilasciato dall'autorità di certificazione.

## 2.5 2KP vs 3KP

Le differenze tra 2KP e 3KP sono evidenti:

- In 3KP il compratore è responsabile solo per gli ordini di pagamento da lui firmati.
- In 2KP con passphrase segreta nello slip (2KP<sup>+</sup>), l'acquirente può facilmente falsificare ordini di pagamento, e non esiste alcun modo di provarlo. Esiste sicurezza verso esterni, anche per passphrase relativamente corte (come PIN, per esempio), dal momento che non sono possibili attacchi tipo del dizionario.
- In 2KP senza segreto (2KP<sup>-</sup>) chiunque conosca i dati del pagamento può effettuare pagamenti falsi.

# Bibliografia

- [1] Analisi dettagliata dei protocolli: iKP,  
<http://telemat.die.unifi.it/book/Security/ikp.htm>, ultima visita  
04-05-2012.
- [2] Capitolo settimo: i sistemi di pagamento online,  
<http://galileo.cincom.unical.it/centro/Newmedia/gesitec/market/cap7/cap7.html>,  
ultima visita 04-05-2012.
- [3] Sicurezza nei sistemi di pagamento online, Cristina Magro, Università  
degli Studi di Catania, 2007/2008.