Crittografia avanzata
Lezione del 21 Marzo 2011

RC4

- Nato nel 1987, ha una storia interessante
- ARC4 pubblicato su cypherpunks nel 1994
- Stream cypher, un PRGA produce un keystream che è messo in XOR con il testo
- Problema: dato che il keystream è generato, necessariamente è ciclico, quindi non è un cifrario di Veron e la chiave è riutilizzata
  - Soluzione: assicurarsi che il ciclo sia sufficientemente lungo per l'uso che ne viene fatto

Bit flipping

- $T \oplus T = 0$, $T \oplus 0 = T$
- Dato che $C = T \oplus K$
- Se conosco T e voglio sostituire T' a T nello stream mi basta fare

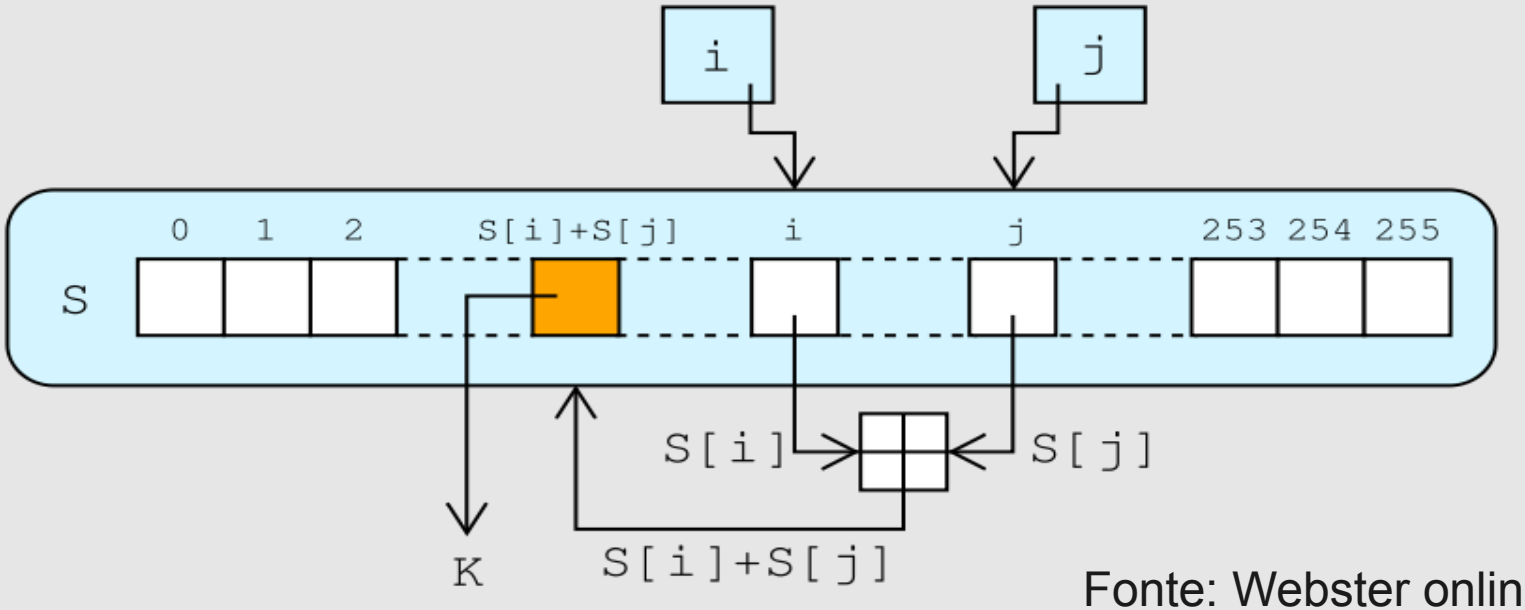
$$M = T \oplus T'$$

$$C' = C \oplus M$$

$$C' = T \oplus K \oplus T \oplus T' = K \oplus T'$$

- Vale per tutti i cifrari di questo tipo, quindi il messaggio deve essere protetto es. con HMAC

RC4 – PRGA keystream



Fonte: Webster online

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

Inizializzazione dello stato

- Lo stato interno è inizializzato utilizzando la chiave mediante il Key Scheduling Algorithm

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

Problemi

- Bit flipping
- RC4 non descrive come includere un IV, il cui uso è quindi lasciato al protocollo; questo è uno dei punti deboli di WEP (vedremo)
- Correlazioni, bias: il keystream lascia “trasparire” informazioni sulla chiave
  - Dato che gli stream cypher sono usati spesso per cifrare comunicazioni, in cui un gran numero di bit è noto/fisso, questo è un grosso problema

Secure Electronic Transaction

Un protocollo per il commercio elettronico

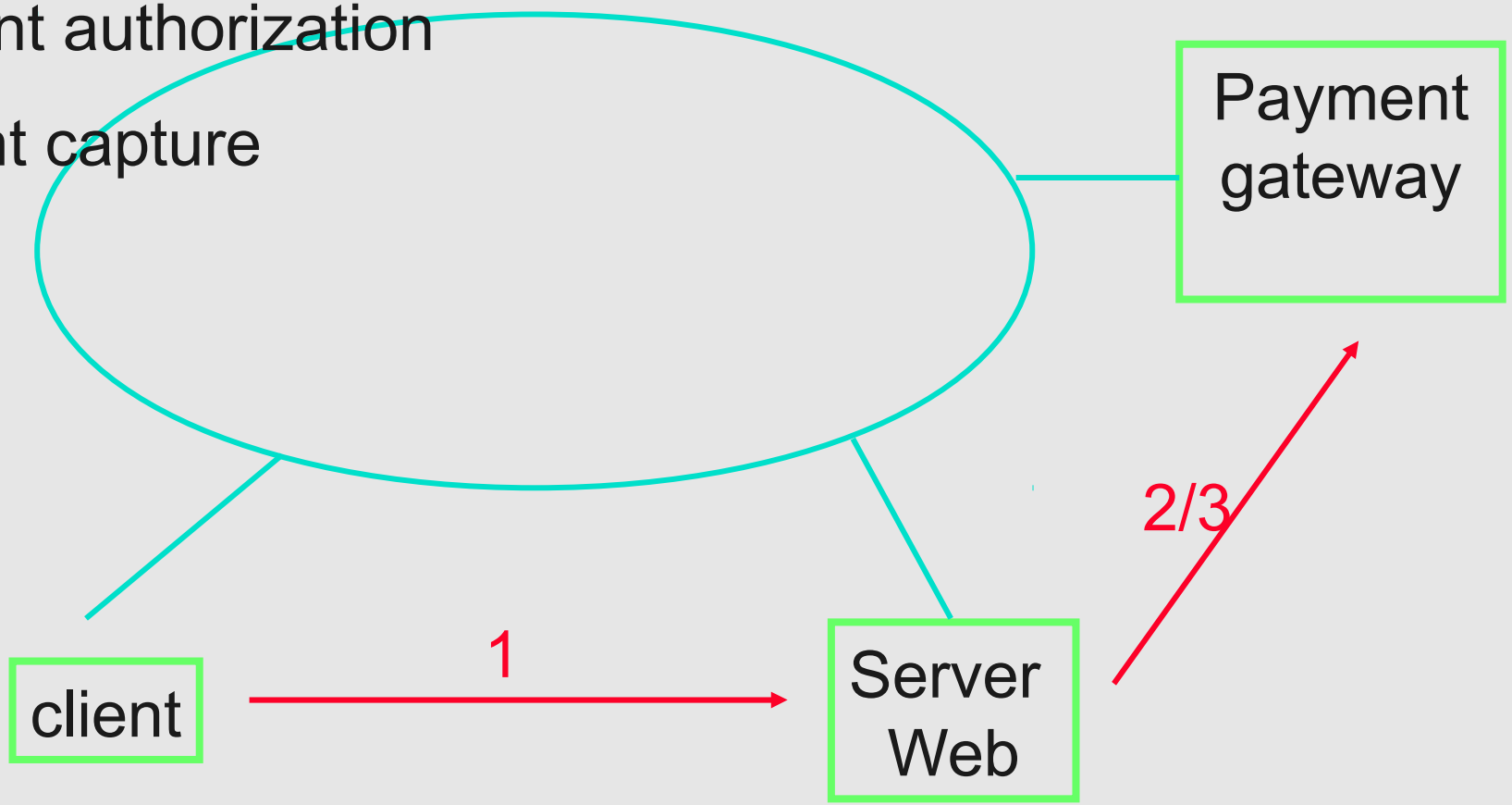
- SET cerca di riprodurre i meccanismi delle carte di credito:
  - merchant accreditati
  - verifica degli utenti
  - autenticazione della transazione, sia per il server che per il client, e non della connessione
  - Riservatezza dei dati non necessari alla transazione (es. identità del “cardholder”)

Entità coinvolte

- Compratore: cardholder
- Venditore: merchant
- Issuer: chi emette la carta di credito (“banca” del compratore)
- Acquirer: entità che gestisce i pagamenti (“banca”) del venditore
- Payment Gateway: server con cui il venditore interagisce

Le fasi

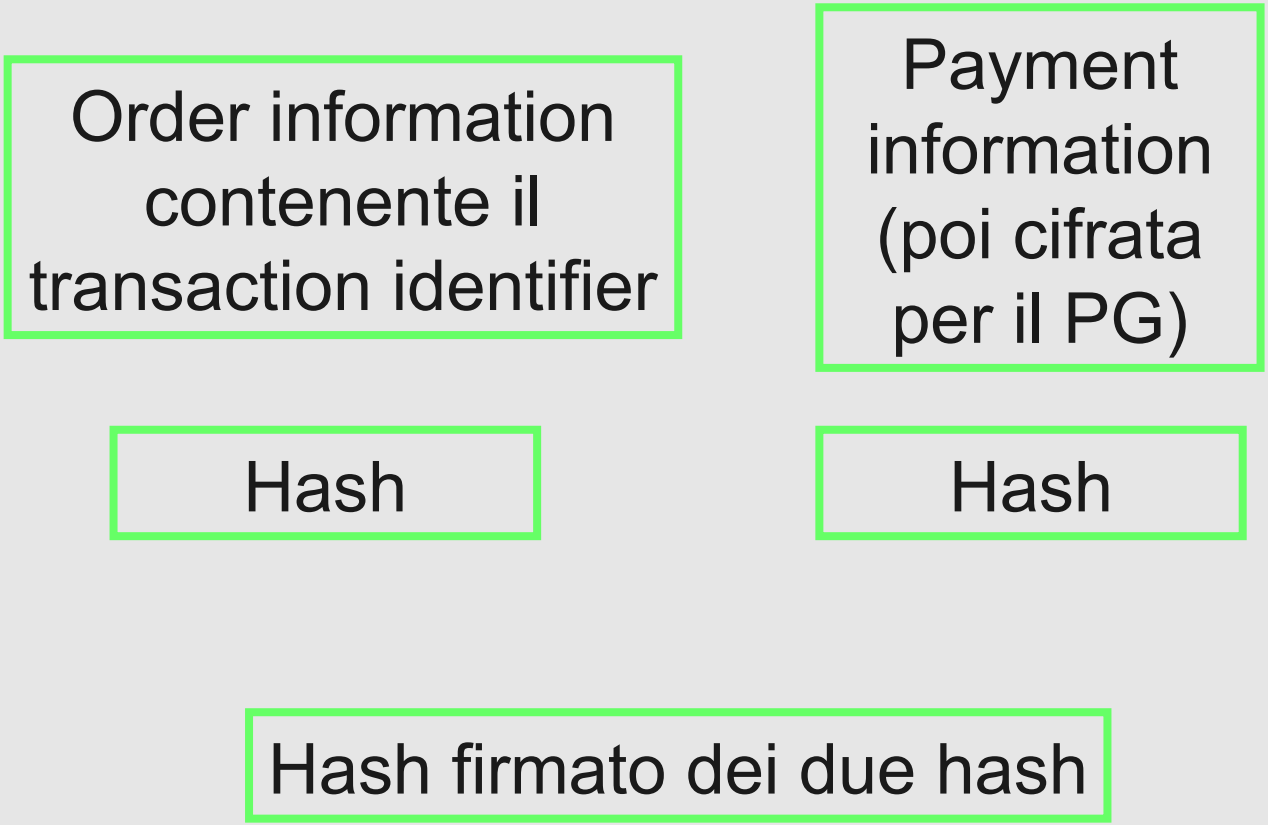
1. Purchase request
2. Payment authorization
3 Payment capture



Il protocollo (1)

- La richiesta dell'acquirente contiene informazioni di pagamento cifrate con la chiave del Payment Gateway, che quindi non è visibile al venditore
- La richiesta è composta da due parti:
  - order information, concordata con il merchant
  - payment information
- La richiesta è composta con uno schema che SET chiama "dual signature"

Dual Signature



Il protocollo (2)

- Quando riceve la richiesta, il merchant verifica il certificato dell'acquirente e la dual signature per l'integrità del messaggio; se tutto va bene conferma l'ordine al compratore
- Genera poi una richiesta di autorizzazione per il Payment Gateway

Il protocollo (3)

- Il payment gateway verifica la richiesta, estrae la Payment Information e chiede l'autorizzazione all'issuer. Se tutto va bene risponde al merchant con un ok ed eventualmente un "capture token"
- A questo punto il venditore può inviare la merce

Il protocollo (4)

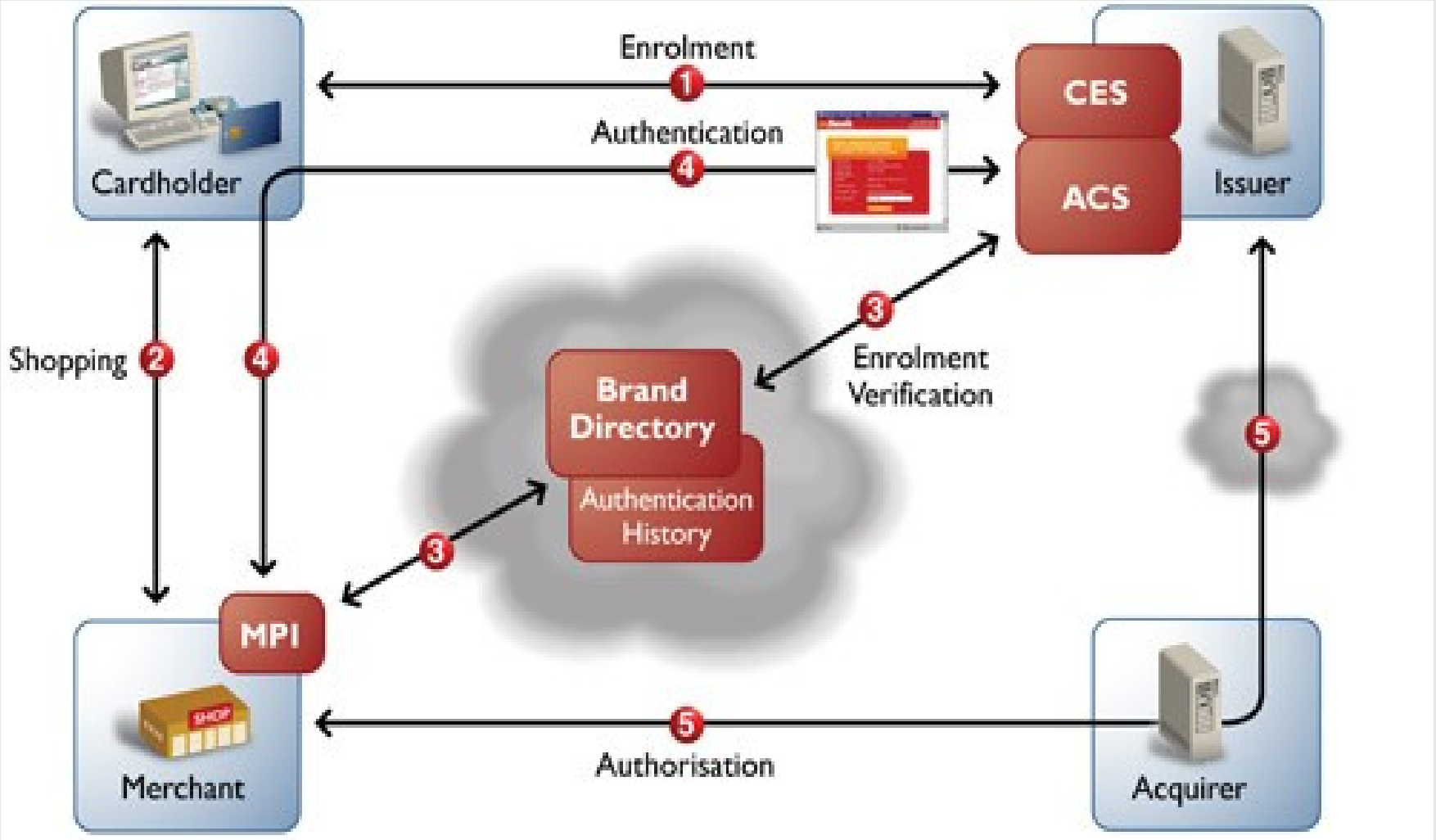
- Per ottentere il pagamento, il merchant invia una “capture request” ed eventualmente il capture token al Payment Gateway, che invia una “Clearing Request” all’issuer. Se tutto va bene il merchant riceve un OK.

Svantaggi e vantaggi di SET

- Riproduce i meccanismi delle carte di credito, quindi anche:
  - la distinzione fra purchaser e merchant
  - il controllo e i costi degli Issuer
- Offre garanzie a compratori e venditori (il rischio è coperto dall'issuer)
- Protegge l'acquirente da un uso improprio dei suoi dati
- Ha i limiti delle carte di credito

3-D Secure

Lo schema generale



Fonte: clear2pay

Welcome to Citibank Payment Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address https://www.citibank.co.in/servlets/TransReq Go

Links Prayer Customize Links Free Hotmail Google BlogPing Yahoo! deadpresident Google Groups Google Go Bookmarks Settings

citibank

- Learn more about online payments.
  View Demo.
- Have questions?
  Click here.

VeriSign Secure Site Click to verify

Online security tips

MasterCard SecureCode

HDFC BANK

Enter your password

Please enter your MasterCard® SecureCode™ in the field below to confirm your identity for this purchase. This information is not shared with the merchant.

Merchant Name: BHARTI CELLULAR LTD

Date: Nov 13, 2008

Total Charge: 1515.81

Card Number: XXXX XXXX XXXX 1221

Personal Message: CHETAN

Name: Chetan

Password:

(forgot password? Click Here)

Submit Cancel

This page will automatically timeout after 90 seconds.

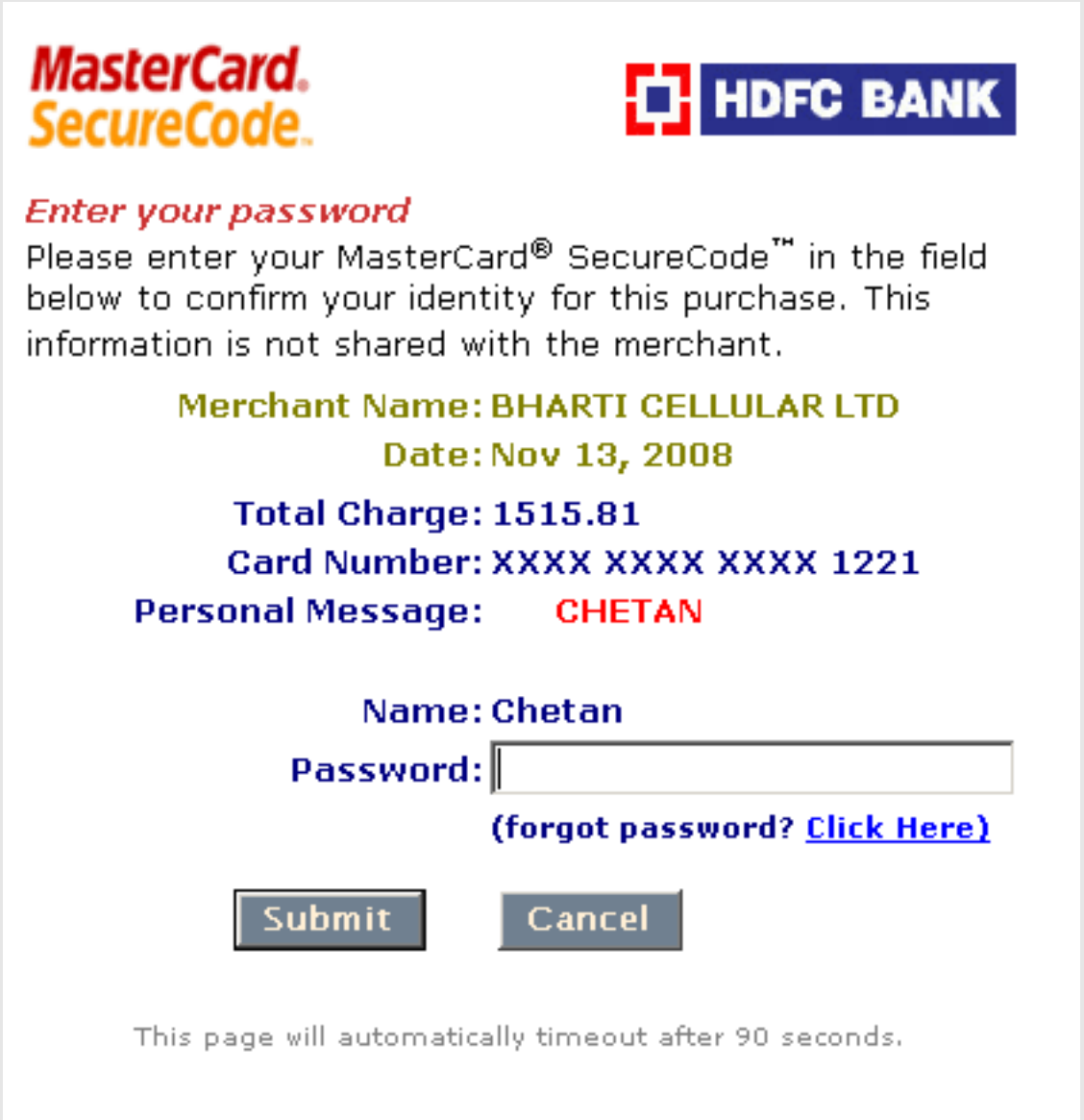
citibank

Citigroup Privacy Promise

Done Internet

Start vs.net ::Airtel::Mobile Services ... Welcome to Citibank ... 8:19 PM

Esempio di richiesta di securecode



Digicash

Digicash: il meccanismo di base

- Un utente deposita una somma presso una banca
- In cambio riceve un equivalente in “digibucks”
- I digibucks possono essere scambiati come banconote in modo anonimo
- In qualsiasi momento ne può essere chiesta la riconversione
- Nel 1998 acquisita da Ecash (partner D. Bank)

Vantaggi

- Non è richiesta una grossa percentuale per ogni transazione
- Il meccanismo permette un notevole anonimato dei pagamenti
- È possibile effetuare con facilità pagamenti da persona a persona e micropagamenti

Svantaggi

- È stata espressa una forte preoccupazione sul controllo dei flussi di capitali: il denaro rimarrebbe in deposito “in garanzia” come una volta era per l’oro
- Il meccanismo per garantire che i digibucks non possano essere duplicati è complesso

Pagamenti person-to-person

- SET non è un meccanismo di uso generale:
  - non tutti sono merchant
  - può servire ricevere pagamenti occasionali
  - le cifre possono essere troppo basse
- Soprattutto per le aste on-line, alcune società si offrono per ricevere i pagamenti via carta di credito, e trasferire i soldi al venditore con strumenti tradizionali

E-Purse (borsellino elettronico)

- Il concetto è quello delle tessere a scalare (es. tessere telefoniche)
- L'uso di smart card permette di ricaricare le tessere
- Generalmente non protette da PIN, sono adatte a cifre contenute
- Permettono pagamenti anonimi, esatti al "centesimo" e e micropagamenti
- Possono o meno bloccare le tessere "rubate"
- Standardizzazione in corso (es. CEPS)