

# Consorzio Triveneto S.p.A.

## Payment Gateway

Protocolli di Sicurezza  
SSL – 3-D Secure - SecureCode

Release 1.2

### TABELLA RELEASES DOCUMENTO

Data	Versione	Autore	Descrizione
01/04/2004	1.0	PM	Prima release
14/07/2006	1.1	PM	Aggiunto Capitolo 6 con descrizione HPP
26/10/2006	1.2	CG	<ul style="list-style-type: none"><li>• Modificato Capitolo 3 con aggiunta dell'incapacità dell'Issuer di autenticare il CardHolder tra i motivi di mancata Liability.</li><li>• Modificato Capitolo 4 per estensione Liability Shift MasterCard SecureCode da europeo a globale e con aggiunta dell'incapacità dell'Issuer di autenticare il CardHolder tra i motivi di mancata Liability.</li><li>• Modificato Capitolo 5 "Matrice di garanzia" per estensione Liability Shift MasterCard SecureCode da europeo a globale.</li></ul>

## SOMMARIO

<b>CAPITOLO 1 - LA SICUREZZA NELL' E-COMMERCE</b>	<b>4</b>
CONCETTI PRINCIPALI	4
LIABILITY SHIFT	5
<b>CAPITOLO 2 - MODALITÀ SSL</b>	<b>7</b>
DESCRIZIONE	7
<b>CAPITOLO 3 - 3-D SECURE</b>	<b>8</b>
DESCRIZIONE	8
PERCORSO DI UNA TRANSAZIONE 3-D SECURE	9
UTILIZZO DEL MARCHIO VERIFIED BY VISA	10
TRANSAZIONE 3-D SECURE IN AMBIENTE DI TEST	12
<b>CAPITOLO 4 - SECURECODE</b>	<b>13</b>
DESCRIZIONE	13
UTILIZZO DEL MARCHIO SECURECODE	14
<b>CAPITOLO 5 - MATRICE DI GARANZIA</b>	<b>16</b>
NOTIFICATION MESSAGE	16
BACK OFFICE	17
<b>CAPITOLO 6 - HOSTED PAYMENT PAGE</b>	<b>18</b>
<b>CAPITOLO 7 - TRANSAZIONI DI ESEMPIO</b>	<b>19</b>
<i>Transazione SSL</i> .....	20
<i>Transazione 3-D Secure</i> .....	23
<i>Transazione SecureCode</i> .....	24

# Capitolo 1 - La Sicurezza nell' E-Commerce

---

## Concetti principali

Internet e i nuovi dispositivi di accesso alla rete hanno creato un'indubbia convenienza per gli acquisti elettronici a distanza, sia per gli acquirenti che per i venditori. Il volume di affari generato dall'E-Commerce continua a crescere, ma di pari passo cresce anche la preoccupazione riguardante l'uso fraudolento delle carte di credito per gli acquisti.

Per fronteggiare questo pericolo, i circuiti carte di credito, sfruttando l'evoluzione continua della tecnologia, hanno implementato protocolli di sicurezza via via più raffinati. Queste iniziative sono volte ad aumentare le transazioni E-Commerce, infondendo maggiore fiducia negli acquirenti e incrementando la qualità del servizio fornito dai Merchants.

La sicurezza sulle transazioni che si svolgono tra due soggetti a distanza, come nel caso dell'E-Commerce, riguarda 3 aspetti:

- **RISERVATEZZA:** i dati sensibili, viaggiando in rete, devono essere cifrati per non permettere a terzi di entrarne illegalmente in possesso
- **INTEGRITA':** i dati scambiati tra le parti non devono essere modificati durante il percorso tra la sorgente e la destinazione
- **AUTENTICAZIONE:** è necessario controllare che la controparte sia effettivamente chi afferma di essere: il Merchant verifica che chi acquista sia il legittimo proprietario della carta di credito, il CardHolder verifica l'identità del Merchant

Nel seguito vengono descritti in dettaglio i protocolli di sicurezza gestiti e la loro rispondenza ai 3 requisiti sopra citati.

E' fondamentale sottolineare che la gestione di tutti i protocolli di pagamento supportati dal Merchant avviene automaticamente da parte della pagina di pagamento presentata dal Consorzio Triveneto S.p.A. al Cardholder (detta "HPP"). Inoltre, se in futuro dovessero verificarsi delle evoluzioni di tali protocolli o l'introduzione di nuovi, il Consorzio Triveneto S.p.A. apporterà le implementazioni direttamente sulla HPP, evitando così al Merchant qualsiasi modifica al proprio sito.

## Liability Shift

La caratteristica più importante, a livello economico, per l'adozione dei protocolli sicuri da parte dei Merchants è sicuramente la Liability Shift, letteralmente lo spostamento delle responsabilità.

Questo meccanismo, già adottato in passato col protocollo SET, mette al riparo un Merchant da un possibile ripudio (o "chargeback") della transazione da parte del Cardholder. Nell'E-Commerce tradizionale infatti, non essendovi alcuna prova (ad es. la firma sullo scontrino) dell'identità del Cardholder durante l'acquisto, il Merchant è esposto alla possibilità di ripudio della transazione, caso che si verifica se il Cardholder non accetta una transazione addebitata sul conto della propria carta. Questo causa un addebito sul conto del Merchant per l'importo della transazione precedentemente accreditata.

Il livello e le caratteristiche della liability shift variano da protocollo a protocollo, in base ai regolamenti imposti dai circuiti carte di credito e dalle banche partecipanti.

Nel seguito esporremo per ogni protocollo descritto le caratteristiche della liability shift, sulla base delle norme vigenti. Tali regole devono comunque essere ritenute subordinate al contenuto del contratto sottoscritto con la propria banca.

## Notification Message

Al termine di ogni transazione il Payment Gateway invia un messaggio contenente l'esito della transazione (detto "NotificationMessage") al server del Merchant. All'interno del messaggio sono presenti 3 campi che informano il Merchant sul tipo di carta usato, il protocollo seguito e la protezione contro un eventuale chargeback (vedi cap. 5).

In base alle informazioni ricevute il Merchant può procedere come ritiene più opportuno: provvede all'evasione dell'ordine, oppure richiede ulteriori informazioni al CardHolder per verificarne l'identità, oppure ancora non dà luogo alla spedizione in quanto ritenuta troppo a rischio.

## Capitolo 2 - Modalità SSL

---

### Descrizione

Il protocollo SSL è la modalità base di ogni sistema di pagamento e-commerce sicuro oggi sul mercato.

Tale protocollo prevede che i dati della carta di credito inseriti dall'utente viaggino cifrati dal suo computer fino al Payment Gateway, in modo che nessuno sia in grado di intercettare e riutilizzare queste informazioni.

Per creare questo canale cifrato, il Consorzio Triveneto S.p.A. si avvale di un certificato SSL3 a 128 bit rilasciato da Verisign, la massima entità di certificazione a livello mondiale. La presenza del certificato permette all'utente di verificare in ogni momento, semplicemente cliccando sul simbolo del lucchetto in basso a destra, che la pagina di pagamento HPP sia effettivamente presentata dal Consorzio Triveneto S.p.A..

Inoltre, il Payment Gateway prevede che il messaggio di inizializzazione del pagamento avvenga direttamente tra il Merchant e il Payment Gateway, senza usare il browser del CardHolder come intermediario. Pertanto, i dati inviati dal Merchant (tra cui l'importo della transazione) non possono essere modificati dal Cardholder in alcun modo.

Riassumendo, il protocollo SSL implementato dal Payment Gateway soddisfa i seguenti requisiti di sicurezza:

- **RISERVATEZZA**: i dati della carta di credito, digitati direttamente sulla form del Payment Gateway, viaggiano cifrati
- **INTEGRITA'**: il CardHolder non può modificare i dati in transito
- **AUTENTICITA'**: viene garantita l'autenticità del server dei pagamenti, sul quale il CardHolder inserisce i dati della carta

Il protocollo SSL difetta nell'autenticazione del CardHolder. Per questo motivo, il Merchant non è protetto da chargeback sulle transazioni SSL.  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **7**.

## Capitolo 3 - 3-D Secure

---

### Descrizione

3-D Secure, conosciuto commercialmente col nome “Verified by Visa” o “VbV”, è un protocollo sicuro sviluppato da Visa per le transazioni di e-commerce effettuate con carte Visa su siti di Merchant convenzionati.

Il mezzo utilizzato da 3-D Secure per ridurre le frodi e rendere così sicuro l’e-commerce è l’autenticazione del Cardholder durante la transazione.

L’autenticazione è quel processo che permette alla banca, che ha emesso una carta di credito, di verificare che chi stà effettuando l’acquisto con la carta è il legittimo proprietario della stessa.

3-D Secure aggiunge delle ulteriori fasi per il completamento della transazione, come viene spiegato nel seguito, ma non vi è necessità di installare alcun software sul device del Cardholder, mentre dal lato Merchant è la HPP del Consorzio Triveneto S.p.A. che gestisce l’intero processo.

Il meccanismo di autenticazione si aggiunge alla presenza del protocollo SSL, comunque presente, per cui i requisiti di sicurezza soddisfatti sono:

- **RISERVATEZZA:** i dati della carta di credito, digitati direttamente sulla form del Payment Gateway, viaggiano cifrati
- **INTEGRITA’:** il CardHolder non può modificare i dati in transito
- **AUTENTICAZIONE MERCHANT:** l’identità viene verificata su un server centrale Visa che viene contattato ad ogni transazione, e sul quale il Merchant è stato censito in fase di attivazione del servizio
- **AUTENTICAZIONE CARDHOLDER:** l’identità viene accertata mediante inserimento della password associata alla carta di credito

L’autenticazione del CardHolder ha un impatto fondamentale sulla liability shift. Le regole Visa infatti impongono quanto segue:



- Su ogni transazione avvenuta con esito positivo utilizzando una carta Visa qualunque, il Merchant è garantito contro richieste di chargeback con motivi di “transazione non valida” o “transazione fraudolenta”.  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **5, 6, 06**.
- Se si verificano inconvenienti tecnici durante la fase di autenticazione del CardHolder (mancata connessione verso il server VISA) o incapacità di autenticare la carta da parte della banca emittente la carta, il Merchant NON è garantito contro le richieste di chargeback.  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **7**.

## Percorso di una transazione 3-D Secure

Una transazione 3-D Secure introduce alcuni nuovi steps necessari all'autenticazione del Cardholder. Queste fasi si inseriscono tra lo step 11 e lo step 12 del percorso transazionale dettagliato nel Capitolo 2 del manuale tecnico. Nello specifico:

11. Dopo essere stato rediretto sulla HPP, il Cardholder digita i dati della propria carta di credito.
  - I. La HPP verifica il numero carta. Se viene utilizzata una carta Visa, la HPP interroga il server centrale Visa per sapere se il Cardholder si è registrato al servizio 3-D Secure. In caso positivo il server Visa ritorna alla HPP l'URL del server della banca che ha emesso la carta
  - II. Se il Cardholder non si è registrato al servizio la transazione prosegue al passo 12, altrimenti la HPP redirige il Cardholder verso il server della sua banca
  - III. La banca presenta al Cardholder una pagina in cui sono presenti i dati del Merchant, della transazione, della banca stessa, e il logo “Verified by Visa” che permettono al Cardholder di riconoscere l'acquisto sicuro in corso. E' presente anche un campo nel quale il Cardholder è tenuto a digitare la password associata alla carta di credito
  - IV. Il Cardholder inserisce la password. Se errata, il server permette altri 2 tentativi. Poi il browser viene rediretto nuovamente sulla HPP

- V. La HPP controlla l'esito del processo di autenticazione del Cardholder sul sito della banca. Se positivo la transazione prosegue al passo 12, se negativo la transazione si blocca e il Payment Gateway invia un NotificationMessage con il campo Error valorizzato a "GV90004"
12. Il Payment Gateway riceve i dati necessari, li associa con i dati del Merchant e della transazione ed invia al Sistema Autorizzativo la richiesta
13. Tutti i passi successivi rimangono invariati....

## Utilizzo del marchio Verified by Visa

Visa raccomanda a tutti i Merchants che sono convenzionati al servizio 3-D Secure di esporre il marchio "Verified by Visa" sul proprio sito. Così facendo, il messaggio proposto dal servizio viene rinforzato e aumenta la fiducia dei visitatori che sono più propensi ad effettuare acquisti.

Il marchio dovrebbe essere esposto (1 sola volta per pagina) sulla Home Page del sito, sulla pagina dove sono esposte le indicazioni riguardo i criteri di sicurezza adottati, e sulla pagina di checkout dell'ordine di acquisto.

Il marchio da visualizzare consiste di un marchio "Verified by Visa" unito ad un link "learn more" che apre una finestra Visa con le informazioni riguardanti 3-D Secure. Il marchio complessivo deve essere sempre riportato seguendo le indicazioni seguenti:

- Non alterare le proporzioni originali o la disposizione degli elementi, e non includere il marchio in una cornice. Inoltre, mantenere ove possibile la versione full-color:



- Riservare una certa quantità di spazio libero attorno al marchio. Il marchio dovrebbe essere chiaramente separato da altri marchi eventualmente presenti, da elementi grafici, testo o elementi di background:



- La grandezza del marchio può variare da un minimo di 60 pixels ad un massimo di 155 pixels.
- Visa fornisce 3 versioni colorate in modo diverso per venire incontro ai vari stili definiti sui siti dei merchants:



On a white, light, or neutral background, the Verified by Visa logotype appears in Visa Blue and the cursor appears in Visa Gold. The "learn more" link appears in Visa Blue.

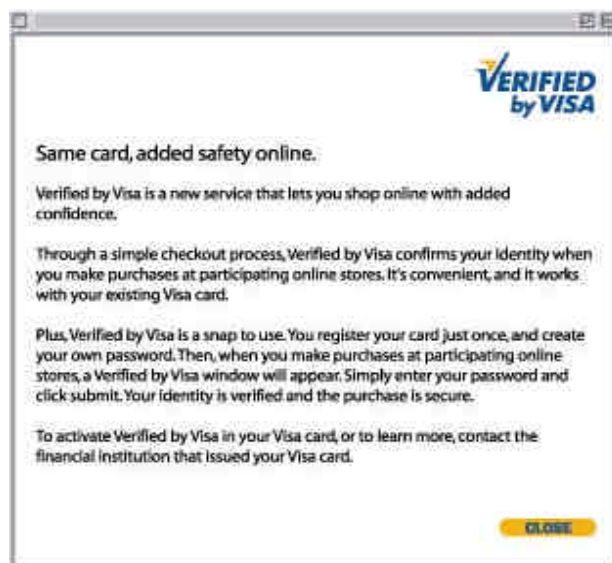


On a dark background, the Verified by Visa logotype appears in white and the cursor appears in Visa Gold. The "learn more" link appears in white.



On a gold background, the Verified by Visa logotype appears in white and the cursor appears in Visa Blue. The "learn more" link appears in white.

- Il marchio è in realtà un link cliccabile, come indicato dal testo "learn more". Ogni uso del marchio deve fare uso del link verso "Visa Service Description Page", una pagina creata e ospitata dal Merchant che deve avere il layout e il testo seguente:



# Transazione 3-D Secure in ambiente di test

Per effettuare una transazione 3-D Secure in ambiente di test, utilizzare gli stessi parametri di interfacciamento al Payment Gateway descritti nel Capitolo 4. Una volta giunti sulla HPP, utilizzare la seguente carta di credito:

- Numero Carta: 4015505250179218
- Data Scadenza: 12/<aaaa> (<aaaa> va sostituito con l'anno corrente)

Quando la pagina del server della banca viene caricata, autenticarsi usando la seguente password:

ctv2002

## Capitolo 4 - SecureCode

---

### Descrizione

Anche MasterCard ha aderito all'utilizzo del protocollo 3-D Secure per gli acquisti sicuri in Internet. Il nome del prodotto nella versione MasterCard è "SecureCode" e copre le transazioni e-commerce effettuate con carte MasterCard su siti di Merchant convenzionati.

Dal punto di vista tecnico, quindi, una transazione SecureCode si svolge con modalità identiche a quelle 3-D Secure, e i requisiti di sicurezza soddisfatti sono gli stessi del caso precedente:

- **RISERVATEZZA**: i dati della carta di credito, digitati direttamente sulla form del Payment Gateway, viaggiano cifrati
- **INTEGRITA'**: il CardHolder non può modificare i dati in transito
- **AUTENTICAZIONE MERCHANT** l'identità viene verificata su un server centrale Visa che viene contattato ad ogni transazione, e sul quale il Merchant è stato censito in fase di attivazione del servizio
- **AUTENTICAZIONE CARDHOLDER**: l'identità viene accertata mediante inserimento della password associata alla carta di credito

Le regole di MasterCard impongono quanto segue:

- Su ogni transazione autorizzata utilizzando una carta MasterCard con autenticazione positiva del CardHolder, il Merchant è garantito contro richieste di chargeback per motivi di "transazione non valida" o "transazione fraudolenta".  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **2**.

- Su ogni transazione avvenuta con esito positivo utilizzando una carta MasterCard qualunque, il Merchant è garantito contro richieste di chargeback con motivi di “transazione non valida” o “transazione fraudolenta”.  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **1**.
- Se si verificano inconvenienti tecnici durante la fase di autenticazione del CardHolder (mancata connessione verso il server MasterCard) o incapacità di autenticare la carta da parte della banca emittente la carta, il Merchant **NON** è garantito contro le richieste di chargeback.  
>> La transazione appare nel sito di Back Office con il campo **ECI** (Electronic Commerce Indicator) valorizzato a **7**.

## Utilizzo del marchio SecureCode

MasterCard impone ai Merchant partecipanti al servizio di esporre il marchio SecureCode all'interno del proprio sito. Il marchio viene fornito da MasterCard stessa in diverse forme; il Merchant può utilizzare pertanto una o più versioni tra quelle fornite, ma mai marchi non ufficiali MasterCard.

Il marchio contiene vari colori e può essere visualizzato sopra uno sfondo qualunque purchè venga garantito un contrasto sufficiente a mantenerne la corretta leggibilità.. Lo sfondo di colore bianco uniforme è da preferire.

MasterCard consiglia di visualizzare il marchio SecureCode in tutte le pagine del sito in cui si faccia riferimento alle opzioni di pagamento. Inoltre, il marchio deve essere posto ad una certa distanza dai marchi delle carte di credito accettate. In alcun modo il marchio SecureCode potrà sostituire o essere affiancato al marchio MasterCard.

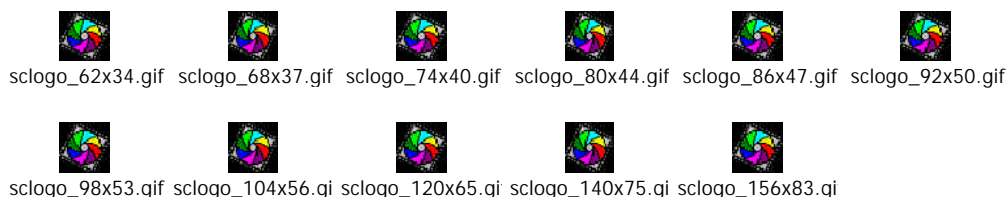
Nessun elemento grafico (testo, linee, loghi, forme, immagini, sfondi troppo pesanti) deve essere posto nelle vicinanze del marchio, per impedire che il messaggio comunicato venga trascurato. Come regola generale, dovrebbe essere mantenuta una distanza di sicurezza attorno al marchio pari alla lunghezza della lettera “M” di “MasterCard” presente nel marchio stesso.

Infine, se il marchio viene esposto in una pagina che contiene anche i marchi delle carte di credito accettate, esso deve essere posto ad una distanza minima da loro di almeno 4 volte la larghezza del marchio stesso (vedi immagine).



Se il Merchant fa riferimento nel proprio sito, o in documentazione correlata, al servizio SecureCode, esso deve sempre essere referenziato come “MasterCard SecureCode”, ovvero mantenendo sempre unite le parole MasterCard e SecureCode. Inoltre devono essere mantenute le lettere maiuscole e minuscole come riportato. Infine, alla prima ricorrenza è necessario evidenziare il copyright, nel seguente modo: “MasterCard® SecureCode™”.

Qui di seguito alleghiamo il marchio SecureCode nelle versioni disponibili.



## Capitolo 5 - Matrice di garanzia

---

### Notification Message

Il Payment Gateway invia un messaggio on-line al server del Merchant al termine di ogni transazione, per comunicargliene l'esito. All'interno di questo messaggio, chiamato NotificationMessage, sono presenti 3 campi che permettono di conoscere il tipo di carta e il protocollo usati, e l'eventuale garanzia contro il chargeback per la transazione appena conclusasi. I campi sono chiamati Brand ("cardtype"), Payment Instrument ("payinst"), e Liability Shift ("liability").

#### ***Brand ("cardtype")***

I tipi di carta possibili sono:

- "VISA" = Visa
- "MC" = Mastercard
- "AMEX" = American Express
- "DINERS" = Diners Club
- "JCB" = JCB

#### ***Payment Instrument ("payinst")***

I protocolli possibili sono:

- "VPAS" = Transazione effettuata seguendo il protocollo "Verified by VISA" o "SecureCode" in cui il CardHolder dispone di una carta (rispettivamente Visa o MasterCard) registrata al servizio
- "CC" = Transazione effettuata con protocollo di sicurezza SSL, oppure con 3-D Secure o SecureCode in cui il CardHolder non dispone di una carta (rispettivamente Visa o MasterCard) registrata al servizio



## Liability Shift (“liability”)

Il valore ha il significato seguente:

- “Y” = Il Merchant è garantito: un eventuale chargeback sulla transazione non darà luogo ad un addebito sul conto del Merchant
- “N” = Il Merchant NON è garantito: potrebbe subire un addebito in conto in caso di richiesta di chargeback per i motivi citati

## Back Office

Sul sito di Back Office, nei dettagli dell’Ordine, compare lo stesso campo liability già presente nel NotificationMessage.

Inoltre, nel dettaglio della Transazione compaiono i campi Brand, Payment Instrument, ed ECI. Sulla base di questi campi la matrice sottostante permette di risalire al valore del campo liability.

		ECI					
		1	2	5	6	06	7
BRAND	VISA	-	-	Y	Y	Y	N
	MC	Y	Y	-	-	-	N
	DINERS	-	-	-	-	-	N
	AMEX	-	-	-	-	-	N
	JCB	-	-	-	-	-	N

## Capitolo 6 - Hosted Payment Page

Esaminiamo brevemente in questo capitolo le informazioni visualizzate o richieste al Cardholder sulla pagina di pagamento visualizzata dal Payment Gateway:

The screenshot shows a web browser window titled "Portal Payment - Microsoft Internet Explorer". The address bar shows "Indirizzo: ...". The page content includes the title "Colors of Success" in a large, stylized font. Below the title, there are two sections of information:

**Informazioni per l'acquisto**

Merchant	CTV Test Merchant
Sito Web	<a href="http://www.ctv.test">http://www.ctv.test</a>
Importo	Eur 1,00
Numero ordine	999999

**Informazioni per il pagamento**

Carte Accettate:

Carta di Credito n°:

CVV2/CVC2:  [info](#)

Data Scadenza:  -

At the bottom of the page, there are logos for "Consorzio Triveneto", "VERIFIED by VISA learn more", "MasterCard SecureCode", and another "Consorzio Triveneto" logo.

### **Informazioni visualizzate:**

**Merchant:** Insegna del punto vendita, comunicato alla banca durante la fase di convenzionamento

**Sito Web:** URL del proprio sito, comunicato alla banca durante la fase di convenzionamento

**Importo:** importo dell'acquisto, comunicato dal Merchant nel messaggio di inizializzazione (PaymentInit)

**Numero Ordine:** Codice dell'ordine comunicato dal Merchant nel messaggio di inizializzazione (PaymentInit) nel campo TrackID.

**Carte Accettate:** Vengono visualizzati i marchi delle carte di credito accettate dal Merchant.

### ***Informazioni richieste:***

**Numero Carta:** è il numero della carta di credito da utilizzare per l'acquisto, e può essere di lunghezza compresa tra 13 e 19 cifre. Solitamente, la lunghezza è di 16 cifre per carte VISA e MasterCard, di 15 cifre per carte American Express e di 14 cifre per carte Diners.

**Data Scadenza:** Mese e Anno di scadenza della carta, così come presente sul fronte della stessa. La carta è valida fino all'ultimo giorno del mese indicato.

**CVV2/CVC2:** Questo Codice, di 3 Cifre, che **Visa** e **Diners** chiamano **CVV2** mentre **MasterCard** lo identifica con **CVC2**, è posizionato sul **retro** della Carta di Credito dopo il numero che identifica la carta stessa.

**American Express** chiama questo codice **4DBC** ed è composto da 4 Cifre posizionate nella parte **frontale** della Carta di Credito sopra al numero della carta stessa.

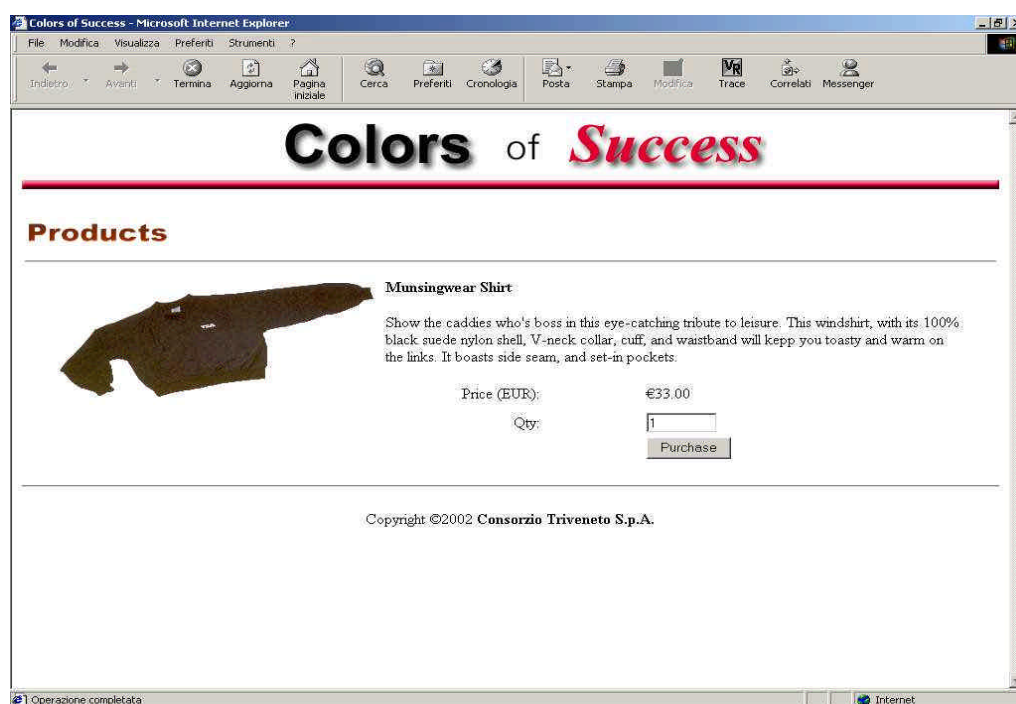
L'inserimento del dato è **obbligatorio**, tranne che per le carte JCB.

# Capitolo 7 - Transazioni di Esempio

## Transazione SSL

### Fase 1:

Il Cardholder seleziona un prodotto dal catalogo, stabilisce la quantità da acquistare e preme il pulsante “Purchase” per accedere alla fase di checkout dell’ordine di acquisto.



### Fase 2:

Il Cardholder controlla la composizione finale dell'ordine e il costo, fornisce i propri dati anagrafici per permettere al Merchant di spedire la merce, e clicca sul pulsante "Buy" per passare alla fase di pagamento con carta di credito.

**Colors of Success**

SKU	Description	Unit Price	Qty	Price
ACI-203	Munsingwear Shirt	33.00	1	33.00
Total Price:				33.00

**Shipping Details:**

Price: 33.00

Name: Mario Rossi

Address Line 1: Piazza 20 Aprile

Address Line 2: Località Ceola

Address Line 3: Macerno

City: Milano

State: MI

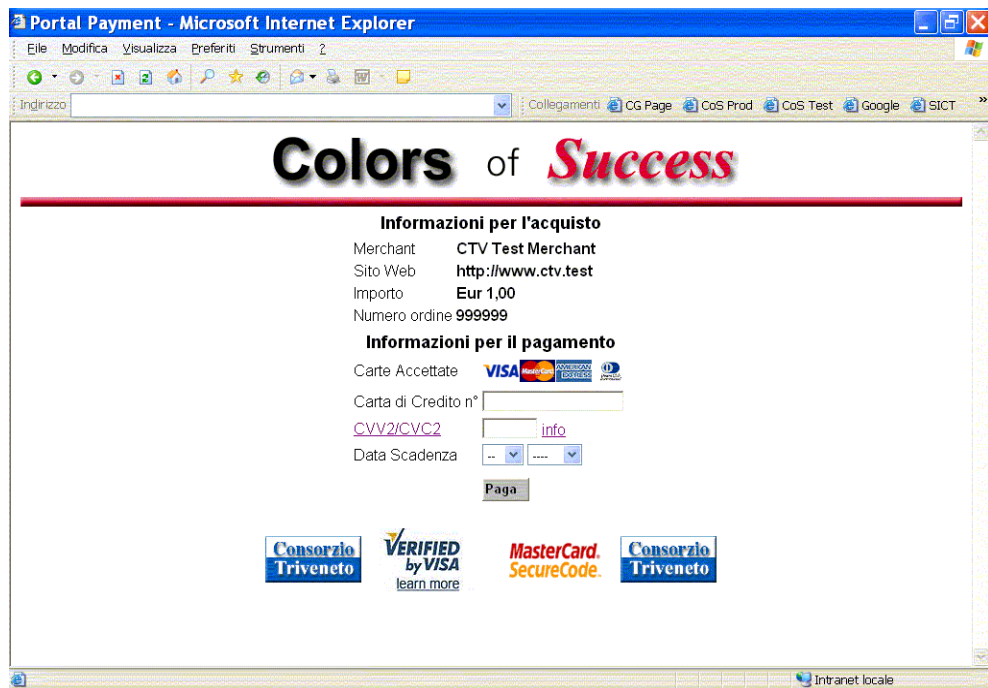
Country: Italy

Postal Code: 20100

Copyright ©2002 Consorzio Triveneto S.p.A.

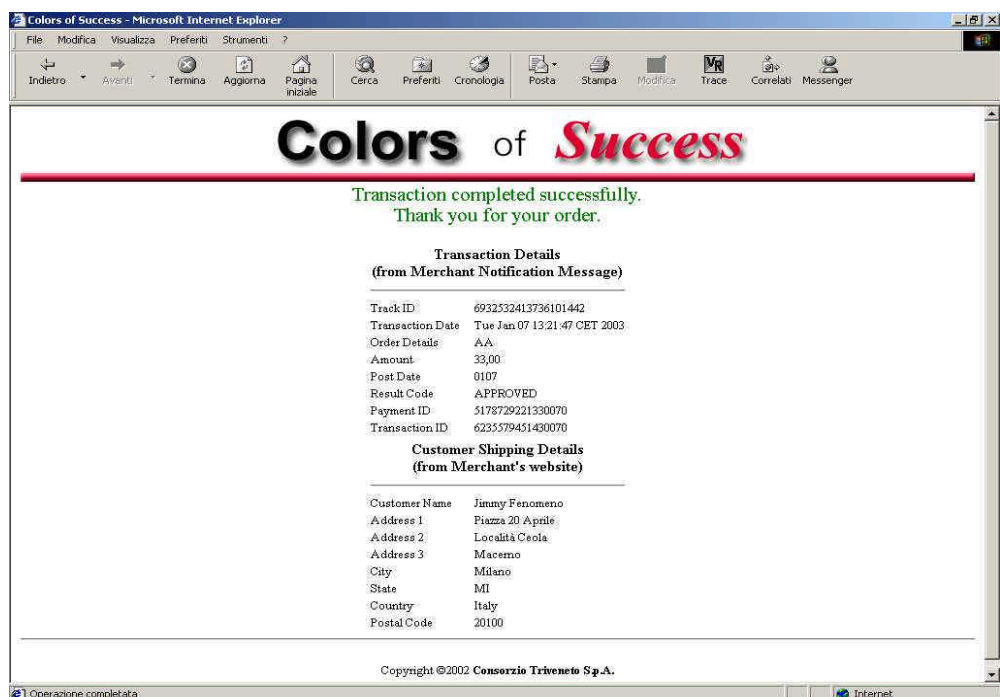
### Fase 3:

Il Merchant invia il messaggio PaymentInit al Payment Gateway. Il Gateway fornisce in risposta l'URL della HPP su cui redirezionare il browser. Il Merchant allora redirige il browser a tale URL, sul quale il Cardholder è chiamato ad inserire i dati della propria carta di credito e a cliccare sul pulsante "Continue" che avvia l'elaborazione della transazione.



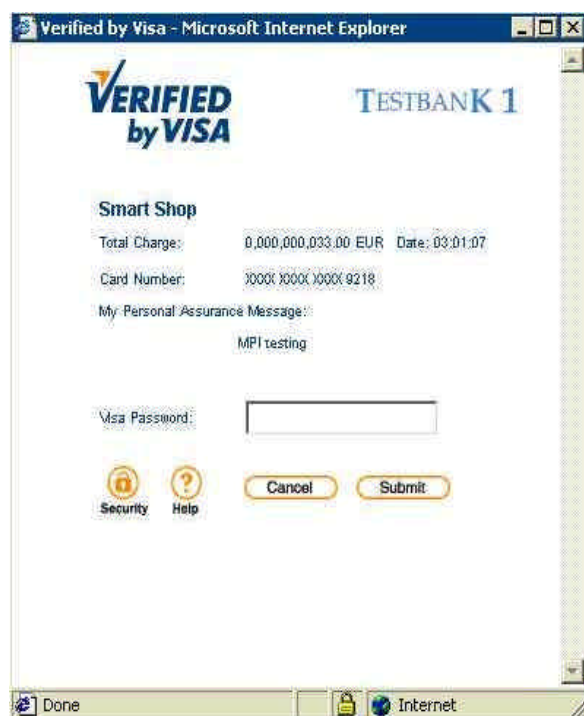
#### Fase 4:

Dopo l'elaborazione il P.G comunica al Merchant (NotificationMessage) l'esito della transazione; il Merchant risponde con l'URL cui redirezionare il browser del cliente. Il P.G redireziona quindi il browser a tale URL per la visualizzazione dell'esito.



## Transazione 3-D Secure

In una transazione 3-D Secure le prime 2 fasi sono uguali al caso precedente. Nella fase 3, se il Merchant supporta anche il pagamento sicuro con Visa 3-D Secure, la HPP presenterà il relativo logo “Verified by VISA”. Se il Cardholder possiede una carta Visa 3-D Secure, dopo la digitazione del numero della propria carta di credito viene aperto un collegamento verso il server della banca che ha rilasciato la carta Visa 3D Secure al Cardholder. Il Cardholder deve quindi digitare la password associata alla carta di credito, per dimostrare di essere il legittimo proprietario della carta di credito.



Se la password inserita è corretta, il sistema prosegue l'elaborazione come nel caso precedente e, dopo lo scambio di messaggi di notifica tra Payment Gateway e Merchant, il Merchant presenta al browser il risultato della transazione. Se la password non è corretta, il server della banca del Cardholder comunica la fallita autenticazione al Payment Gateway, il quale blocca il proseguimento della transazione e invia un messaggio di notifica al merchant con codice errore GV90004.

## Transazione SecureCode

La transazione segue lo stesso percorso dell'esempio precedente. Dopo l'inserimento di una carta MasterCard il sistema controlla se tale carta è registrata al servizio. In caso positivo, al CardHolder viene presentata una finestra da parte della propria banca sulla quale digitare la password associata alla carta.

Se la password inserita è corretta la transazione procede, altrimenti si blocca e il Payment Gateway comunica al merchant un esito negativo con codice d'errore GV00004.