Consorzio Triveneto S.p.A.

Payment Gateway

Specifiche di Interfacciamento Merchant

Release 1.4.1

TABELLA RELEASES DOCUMENTO

Data	Versione	Autore	Descrizione
09/01/2003	0.1	PM	Prima bozza
14/01/2003	1.0	PM	Prima release
15/01/2003	1.0.1	PM	Limitato i demo disponibili alla sola vers. ASP
13/02/2003	1.0.2	PM	Revisione BAPV
18/04/2003	1.0.3	PM	• Variazione descrizione plug-in • Cenno gestione e-mail di notifica dal Merchant
03/07/2003	1.1	PM	Introdotte specifiche di interfacciamento Merchant senza utilizzo di plug-in
23/07/2003	1.1.1	PM	• Corretti i riferimenti al ResponseURL a pg. 13 • Corretto il riferimento alla pagina Receipt.asp a pg.22 • Corretto il paragrafo “Richiesta Notification Message” a pg. 16 con il dettaglio dei campi in caso di errore
04/08/2003	1.1.2	AL	Precisazione relativa al Merchant Notification URL (“responseURL”) nel messaggio di richiesta PaymentInit a pag. 15
01/09/2003	1.1.3	PM	Correzione del formato della stringa di risposta al NotificationMessage: “REDIRECT=”, pg. 17
03/09/2003	1.1.4	PM	Correzione dei campi presenti nel NotificationMessage a pg. 16 e 17
02/10/2003	1.2.0	PM	• Requisiti javascript browser Cardholder, pg 7 • Multilingua esteso a 5 lingue per la visualizzazione della HPP, pg 15 • Il Demo ASP include il collegamento senza utilizzo del plug-in (pure-buy.asp), pg 22 • Incluso il riferimento al manuale specifico per la personalizzazione della HPP, pg 24 • Maggiori informazioni per l’installazione del demo ASP, Appendice B • Il software viene fornito via e-mail dal Consorzio, dato che il BackOffice non è

			disponibile in ambiente di test, pg 19
20/10/2003	1.2.1	PM	• Introdotta la possibilità di effettuare storni multipli su singola transazione, con totale storni non superiore al tot. contabilizzato. Variazioni a pg. 14, 38, 39, 40
03/11/2003	1.2.2	PM	Aggiunto un paragrafo nel cap. 3 per dettagliare l'utilizzo dell'ErrorURL, pg 19
12/02/2004	1.2.3	PM	• Aggiornata la lista dei codici di errore in Appendice C • Aggiunta l'Appendice D con l'elenco delle CA accettate • Aggiornati i seguenti paragrafi nel cap. 3: – "Risposta NotificationMessage" – "Error URL" – "e24PaymentPipe - Descrizione"
29/03/2004	1.3.0	PM	• Modificato il paragrafo "Richiesta NotificationMessage" nel cap. 3, in cui si specificano a) i 3 nuovi campi inseriti nel NotificationMessage: Card Type, Payment Instrument, Liability e b) si consiglia di considerare il primo NotificationMessage ricevuto. • Eliminati i Capitoli 5 e 6. Sono stati inseriti nel nuovo documento "Protocolli di sicurezza"
10/01/2008	1.4.0	PM	Revisione generale documento. Elementi nuovi: • Cap. 2 Inserito l'invio dell'e-mail di notifica dell'esito nel flusso di elaborazione di una transazione • Cap. 3 - Aggiunta specifica per UDF3 per preimpostare il campo "Indirizzo E-Mail" sulla pagina di pagamento - Aggiunta specifica per UDF5 che

			permette di impostare un timeout sulla pagina di pagamento, superato il quale il viene bloccata l'elaborazione della transazione • Cap. 4 - Aggiunti casi di test raccomandati
02/07/2008	1.4.1	PM	• Cap. 3 - Aggiunta specifica per UDF1 per ricevere nel Notification Message il codice hash, con algoritmo SHA-1, della carta usata durante il pagamento.

SOMMARIO

Capitolo 1 - Introduzione

Payment Gateway

Il servizio di Commercio Elettronico offerto dal Consorzio Triveneto S.p.A. si pone lo scopo di intermediare i flussi finanziari provenienti dalle transazioni di Commercio Elettronico, convogliando tali pagamenti sugli esistenti sistemi di autorizzazione e contabilizzazione.

Il Consorzio Triveneto S.p.A. fornisce ai Merchants, che già dispongono di un proprio sito in Internet, una piattaforma unica per la gestione completa delle transazioni E-Commerce con carta di credito:

- Online: gestisce in modalità sicura di tutte le fasi della transazione economica.
- Offline: crea e fornisce al Merchant un account per l'accesso via web all'interfaccia amministrativa, nella quale è possibile verificare lo stato delle transazioni, generare i report di operatività e procedere alle operazioni contabili necessarie.

Hosted Payment Page (HPP)

Durante la fase di pagamento di una transazione E-Commerce con carta di credito, il Merchant redireziona il browser del Cliente (in seguito "Cardholder") sul sito del Consorzio Triveneto S.p.A. per l'inserimento dei dati della carta di credito. In questo modo il Merchant raggiunge molti obiettivi significativi:

- Non viene a conoscenza dei dati della carta di credito del Cardholder, eliminando quindi l'onere di dover implementare tutti i requisiti di sicurezza, fisici e logici, richiesti dalla gestione e memorizzazione di questo tipo di dati.
- Delega al Consorzio Triveneto S.p.A. la gestione dei protocolli E-Commerce che intende supportare e per i quali ha ottenuto, dalla propria banca, il convenzionamento (vedere il documento allegato *"Protocolli di sicurezza*" per maggiori informazioni).

- Può personalizzare le pagine presentate dal Consorzio Triveneto S.p.A. al Cardholder, in modo da non intaccare il livello della shopping experience di quest'ultimo creando una redirezione trasparente, mantenendo quindi il look & feel del sito del Merchant.

La pagina di pagamento presentata dal Consorzio Triveneto S.p.A. al Cardholder è chiamata Hosted Payment Page (HPP). Essa gestisce tutti i protocolli di pagamento (detti anche Strumenti di Pagamento) supportati dal Merchant. Per maggiori informazioni consultare il documento allegato *"Protocolli di sicurezza*".

Inoltre, se in futuro dovessero verificarsi delle evoluzioni di tali protocolli o l'introduzione di nuovi, il Consorzio Triveneto S.p.A. potrà implementare la HPP, evitando al Merchant qualsiasi modifica al proprio sito.

Capitolo 2 - Fasi di una transazione

Introduzione

Questo capitolo intende descrivere tutti i passi di una transazione E-Commerce utilizzando la piattaforma Payment Gateway e l'interfaccia web HPP del Consorzio Triveneto S.p.A., dapprima focalizzando sulle azioni effettuate da ognuno dei soggetti coinvolti e poi integrandole in un flusso omogeneo e continuo di fasi successive.

Il punto di vista del Cliente

Il cliente, o Cardholder, effettua un acquisto sul sito del Merchant:

- Sceglie i prodotti
- Inserisce i propri dati anagrafici per permettere la spedizione della merce, e clicca sul pulsante "Acquista"
- Viene redirezionato sulla HPP.
  N.B. **E' necessario che il browser abbia le impostazioni javascript attive per un corretto funzionamento della HPP**
- Sceglie lo strumento di pagamento tra quelli supportati dal Merchant, inserisce i dati della propria carta di credito e clicca sul pulsante "Paga"
- Viene redirezionato su una pagina specifica del sito del Merchant la quale visualizza l'esito del pagamento
- Eventualmente riceve, se attivata l'impostazione da parte del Merchant, un messaggio e-mail di notifica dell'avvenuto pagamento, da utilizzare come scontrino virtuale

Il punto di vista del Merchant

Il Merchant riceve un ordine di acquisto dal Cardholder:

- Invia un messaggio di inizializzazione al pagamento (PaymentInit) al Payment Gateway

- Riceve in risposta un codice univoco di pagamento (PaymentID) e l'URL della HPP
- Redireziona il Cardholder all'URL della HPP allegando l'informazione PaymentID
- Riceve dal Payment Gateway la notifica dell'esito della transazione
- Risponde con l'URL al quale desidera che il Cardholder venga rediretto per la presentazione dell'esito della transazione
- Presenta l'esito al Cardholder
- Eventualmente riceve, se attiva l'impostazione, un messaggio e-mail di notifica dell'avvenuto pagamento, da utilizzare come scontrino virtuale

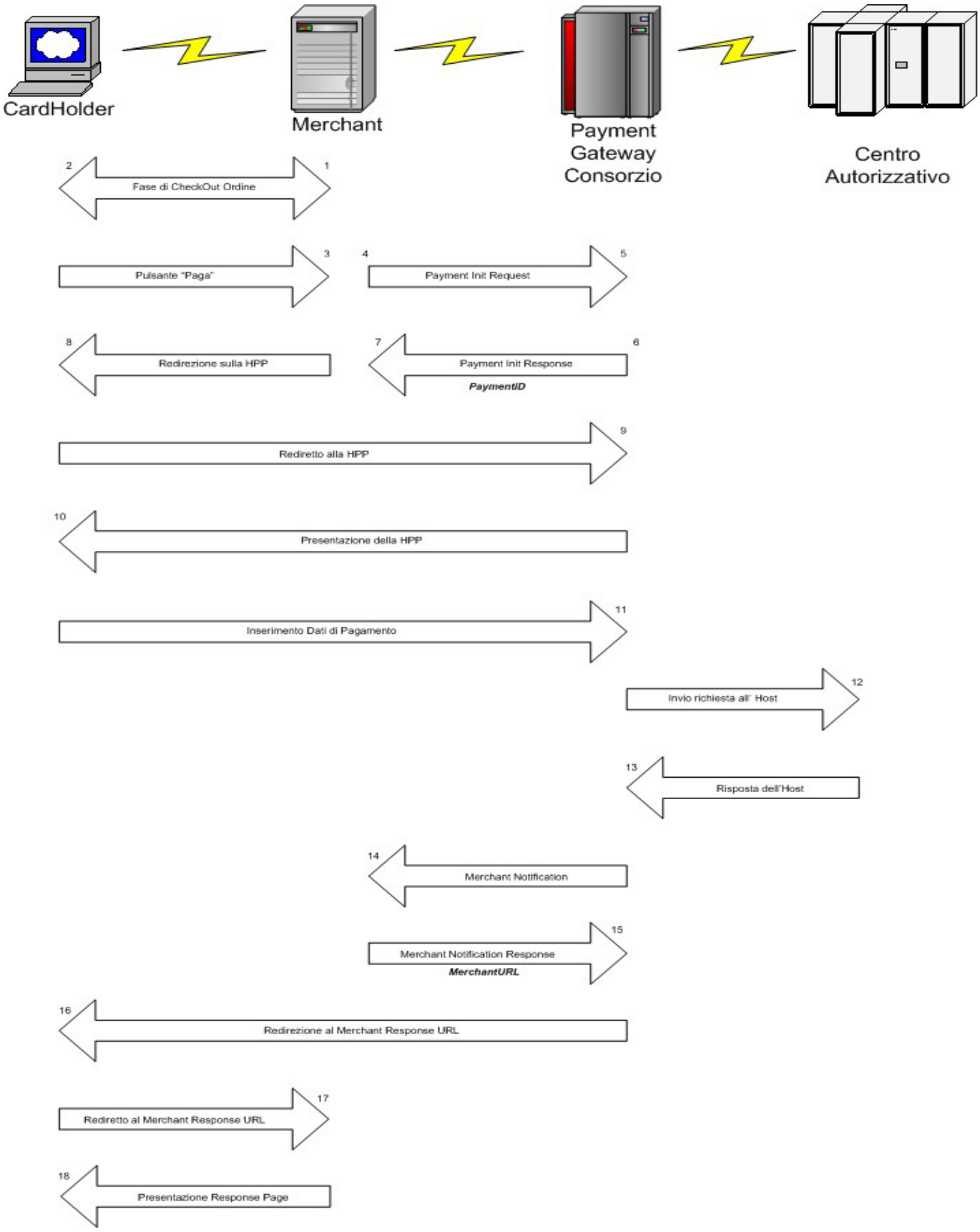
Il punto di vista del Payment Gateway

Il sistema del Consorzio Triveneto S.p.A. riceve un messaggio di inizializzazione (PaymentInit) dal Merchant.

- Risponde con l'URL della HPP e un codice identificativo della transazione (PaymentID)
- Presenta la HPP al Cardholder, personalizzata dal Merchant e contenente tutti gli strumenti di pagamento supportati dal Merchant stesso
- Riceve i dati della carta di credito del Cardholder
- Elabora la transazione inviando la richiesta ai sistemi autorizzativi delle compagnie carte di credito e ottenendo la relativa risposta
- Invia al Merchant un messaggio di notifica dell'esito
- Riceve in ritorno l'URL a cui redirezionare il Cardholder
- Redireziona il Cardholder all'URL ricevuto
- Eventualmente (se attivata l'impostazione da parte del Merchant) invia un messaggio e-mail di notifica dell'avvenuto pagamento al Cardholder e/o al Merchant, da utilizzare come scontrino virtuale

Schema del flusso di informazioni

Integrando tutte le attività precedentemente descritte, ne deriva il seguente schema delle azioni/comunicazioni che avvengono durante una transazione tra i soggetti partecipanti:


CardHolder
Merchant
Payment Gateway Consorzio
Centro Autorizzativo
1
2
Fase di CheckOut Ordine
3
Pulsante "Paga"
4
5
Payment Init Request
6
7
Payment Init Response
PaymentID
8
Redirezione sulla HPP
9
Rediretto alla HPP
10
Presentazione della HPP
11
Inserimento Dati di Pagamento
12
Invio richiesta all' Host
13
Risposta dell'Host
14
Merchant Notification
15
Merchant Notification Response
MerchantURL
16
Redirezione al Merchant Response URL
17
Rediretto al Merchant Response URL
18
Presentazione Response Page

Descrizione degli steps

La tabella seguente analizza in dettaglio il flusso completo delle attività presenti in una transazione.

Browser Cardholder	**Sito Web Merchant**	**Payment Gateway Consorzio**	**Centro Autorizzativo**
1. Completamento del Carrello.	2. Prepara e ritorna la pagina di Check Out.		
3. Compila i campi necessari e preme il pulsante “Compra”.	4. Prepara la richiesta HTTP PaymentInit con tutti i dati della transazione.		
	5. Invia la richiesta via POST al Consorzio	6. Dopo la verifica di validità della richiesta ricevuta, salva i dati della transazione, vi associa un PaymentID, ritorna al Merchant l’URL cui redirezionare il browser del Cardholder e il PaymentID da utilizzare nella redirezione.	
		7. Ritorna URL + PaymentID al Merchant	
	8. Salva il PaymentID con gli altri dati della transazione, poi ritorna al browser una pagina di redirezione verso l’URL Consorzio con associato il PaymentID della transazione.		

9. Richiama automaticamente l'URL Consorzio. Nessuna azione richiesta al Cardholder.		10. Dopo la verifica del PaymentID ricevuto, prepara la pagina di pagamento con gli strumenti supportati dal Merchant e la ritorna al browser.	
11. Sceglie lo strumento di pagamento tra quelli supportati, inserisce i dati necessari, e preme il pulsante "Paga".		12. Riceve i dati, li associa con i dati del Merchant e della transazione ed invia al Sistema Autorizzativo la richiesta.	13. Riceve e processa la richiesta, e ritorna l'esito al Payment Gateway.
		14. Invia un messaggio POST al Merchant comunicando l'esito della transazione. Se attivata l'impostazione, invia un'e-mail di notifica dell'esito al Cardholder e/o al Merchant.	
	15. Riceve il messaggio e aggiorna lo stato della transazione con l'esito ricevuto. Poi ritorna l'URL cui redirezionare il browser per la presentazione della pagina di risposta.	16. Redireziona il browser verso l'URL indicato dal Merchant al punto precedente.	
17. Richiama automaticamente l'URL del Merchant. Nessuna azione richiesta al Cardholder.	18. Riceve la richiesta e ritorna la pagina finale, con i dettagli della transazione e l'esito del pagamento.		
19. Riceve e visualizza la pagina di risposta del Merchant.			

Capitolo 3 - Integrazione del Merchant

Introduzione

La piattaforma Payment Gateway del Consorzio Triveneto S.p.A. prevede la presenza di alcune comunicazioni dirette col server del Merchant per portare a termine le transazioni. Questo scambio di messaggi può essere implementato in due modi, tramite l'installazione di un apposito plug-in oppure creando una propria interfaccia di comunicazione:

- Il plug-in si chiama **e24PaymentPipe**: è di facile integrazione ed è compatibile con tutti i siti sviluppati in Java, C/C++, ColdFusion, ActiveX/COM, VB, e ASP.
- Seguendo le specifiche fornite nel seguito è possibile creare una propria interfaccia di comunicazione, necessaria nel caso in cui il plug-in non sia compatibile con la propria piattaforma oppure il sito sia pubblicato tramite un Provider esterno in hosting condiviso.

Percorso di una transazione con indicazione dei messaggi utilizzati

Fasi on-line

- Il Cardholder completa il carrello, fornisce i dati per la spedizione della merce e clicca sul pulsante "Compra"
- Il Merchant invia al Payment Gateway il messaggio **PaymentInit** contenente tutti i dati relativi all'acquisto
- Il Merchant riceve in risposta l'URL della HPP e il codice PaymentID che identifica la transazione
- Il Merchant redireziona il browser del Cardholder sull'URL della HPP passando il PaymentID come parametro

- Una volta che il pagamento è avvenuto, il Payment Gateway invia il messaggio di notifica dell'esito, **NotificationMessage**, ad un URL che il Merchant ha appositamente preparato (ResponseURL). Questo URL viene comunicato al Payment Gateway nel messaggio PaymentInit
- Il Merchant risponde al messaggio **NotificationMessage** con l'URL al quale deve essere rediretto il browser del Cardholder
- Il Payment Gateway redireziona il browser all'URL appena ricevuto
- Il Merchant presenta l'esito della transazione al Cardholder

Fasi off-line

Successivamente il Merchant procederà all'evasione dell'ordine. Possono rendersi necessarie varie operazioni contabili dall'accredito in conto (se la transazione non prevedeva l'accredito automatico) al rimborso del Cardholder in caso di restituzione della merce e così via. Per effettuare queste operazioni si può procedere in 2 modi:

- Collegandosi al sito del Consorzio e utilizzando le funzioni ivi presenti
- Inviando direttamente la richiesta al Payment Gateway col messaggio **Payment**. Andranno inseriti tutti i parametri della transazione originaria e valorizzato il codice azione opportuno

In Appendice A viene riportato l'elenco delle operazioni contabili disponibili e la corretta sequenza permessa.

Dettaglio dei messaggi tra il Merchant e il Payment Gateway

Abbiamo quindi visto che i messaggi server-to-server tra Sito Merchant e Payment Gateway sono di 3 tipi e consistenti ognuno in una coppia richiesta-risposta:

- **PaymentInit**: Messaggio di inizializzazione della transazione inviato dal Merchant al Payment Gateway, il quale risponde comunicando l'URL della HPP e il PaymentID
- **NotificationMessage**: Messaggio di comunicazione dell'esito della transazione che il Payment Gateway invia al Merchant, il quale risponde con l'URL al quale redirezionare il browser del Cardholder

- **Payment**: Messaggio che il Merchant può usare per inviare al Payment Gateway richieste di operazioni contabili su transazioni precedentemente effettuate. Il Payment Gateway risponde con l'esito dell'operazione.

I messaggi **PaymentInit** e **Payment** sono generati dal Merchant, quindi per la loro implementazione è necessario utilizzare il plug-in e24PaymentPipe oppure creare una propria interfaccia seguendo le specifiche fornite nel seguito.

Il messaggio **NotificationMessage** è generato dal Payment Gateway, quindi il Merchant deve predisporre una pagina dinamica in grado di ricevere i parametri presenti nel messaggio e ritornare al Payment Gateway l'URL di redirezione finale per il browser del Cardholder.

Messaggio PaymentInit

Questo messaggio viene creato dal Merchant e inviato all'URL del Payment Gateway per dare il via ad una transazione. Esso utilizza i seguenti elementi:

Nome Campo	Obbligatorio	Lungh. max	Descrizione
id	S	8	Codice identificativo del Merchant, assegnato in fase di attivazione del servizio
password	S	8	Password assegnata al Merchant in fase di attivazione del servizio
action	S	1	Tipo di transazione: 1=**Purchase** 4=**Authorization**
amt	S	10	Importo dell'operazione (formato NNNNN.NN).
currencycode	S	3	Codice ISO valuta Fisso a "978" (Euro).
langid	S	3	Codice per impostare la lingua con cui verrà visualizzata la HPP al Cardholder. La HPP supporta le seguenti lingue: "ITA" = italiano "USA" = inglese "FRA" = francese

			"DEU" = Tedesco "ESP" = spagnolo "SLO" = sloveno
responseURL	S	256	URL che verrà utilizzato dal Payment Gateway per comunicare al Merchant l'esito della transazione tramite il **NotificationMessage**. L'URL specificato: • non può puntare a porte diverse dalla 80 e 443 • non può contenere parametri di nessun tipo • se punta a siti protetti da un certificato SSL, il certificato deve essere emesso da una delle Certification Authority elencate in Appendice D. In caso contrario il Merchant dovrà fornire al Consorzio Triveneto il/i certificato/i della/e Certification Authority che garantiscono l'autenticità del certificato del Merchant.
errorURL	S	256	URL che verrà utilizzato dal Payment Gateway per presentare al Cardholder una pagina di errore, in caso dovessero verificarsi degli inconvenienti nella comunicazione del NotificationMessage.
trackid	S	256	Codice identificativo della transazione impostato dal Merchant. Di solito è il codice identificativo dell'ordine di acquisto presso il sito del Merchant. E' consigliabile che questo codice sia univoco per ogni transazione.
udf1	N	256	Campo a discrezione del Merchant per informazioni che desidera inserire e che verranno restituite inalterate nel NotificationMessage. **Valorizzazione speciale:** se impostato con "**SHA1**" permette di ricevere nel campo UDF1 del Notification Message il codice hash, calcolato con algoritmo SHA-1, della carta di credito usata dall'acquirente per il pagamento.
udf2	N	256	Campo a discrezione del Merchant per informazioni che desidera inserire e che verranno restituite inalterate nel NotificationMessage.

udf3	N	256	Campo a discrezione del Merchant per informazioni che desidera inserire e che verranno restituite inalterate nel NotificationMessage. **Valorizzazione speciale**: se inizia con "**EMAILADDR:**" la parte seguente del campo viene interpretata come l'indirizzo e-mail del Cardholder. Se il Merchant ha impostato (tramite back office) l'invio dell'e-mail con l'esito del pagamento al Cardholder, la pagina di pagamento conterrà un campo "Indirizzo e-mail" che il Cardholder potrà valorizzare per ricevere l'e-mail. Il campo può essere pre-valorizzato con l'indirizzo ricevuto nel campo UDF3 (che può riportare, ad esempio, l'indirizzo usato dal Cardholder per la registrazione sul sito del Merchant).
udf4	N	256	Campo a discrezione del Merchant per informazioni che desidera inserire e che verranno restituite inalterate nel NotificationMessage.
udf5	N	256	Campo a discrezione del Merchant per informazioni che desidera inserire e che verranno restituite inalterate nel NotificationMessage. **Valorizzazione speciale:** se inizia con "**HPP_TIMEOUT=**"<**XX**> imposta un timeout di <**XX**> minuti sulla HPP. Se il Cardholder rimane sulla pagina oltre questo periodo, il Payment Gateway non elaborerà la transazione, inviando lo specifico codice di errore CT0001.

La risposta che il Payment Gateway ritorna al Merchant dopo aver ricevuto il messaggio PaymentInit e averne verificato la validità (ID e Password del Merchant) contiene i seguenti campi:

Nome Campo	Lungh. max	Descrizione
PaymentID	20	Codice univoco identificativo dell'ordine. Il Merchant deve inserirlo nella redirezione del Cardholder, in modo da permettere al Payment Gateway di verificare la validità dell'utente che sta accedendo al sistema di pagamento
PaymentURL	256	URL della HPP a cui il Merchant deve redirezionare il Cardholder per procedere al pagamento

Messaggio NotificationMessage

Il Payment Gateway invia questo messaggio per comunicare al Merchant l'esito della transazione.

Il Merchant predispone una pagina dinamica in grado di ricevere questo messaggio e ne comunica l'URL al Payment Gateway nel messaggio PaymentInit (campo responseURL).

Il Payment Gateway usa il metodo POST per l'invio del messaggio.

I campi presenti nel messaggio sono diversi a seconda che la transazione sia stata elaborata o che invece si sia verificato un problema tecnico.

NOTA:

E' possibile, anche se molto improbabile, che per una stessa transazione vengano ricevuti più NotificationMessage, nel caso in cui il Cardholder riesca a tornare per errore sulla pagina di pagamento usando il tasto BACK del browser. Il Payment Gateway rifiuta l'ulteriore tentativo di pagamento sullo stesso PaymentID ed invia il NotificationMessage al Merchant segnalando il fatto.

Si raccomanda, quindi, di considerare solo il primo NotificationMessage per l'aggiornamento dello stato della transazione sul proprio database, per evitare di sovra-scrivere l'esito dell'unica transazione elaborata con un tentativo di elaborazione anomalo successivo.

Caso: transazione elaborata

In questo caso il NotificationMessage consiste dei seguenti campi:

Nome Campo	Lungh. max	Descrizione
paymentid	20	Codice univoco identificativo dell'ordine
tranid	20	Codice univoco identificativo della transazione assegnato dal Payment Gateway
result	20	Esito dell'operazione: "**APPROVED**" = Autorizzata "**NOT APPROVED**" = Non Autorizzata "**CAPTURED**" = Accreditata "**NOT CAPTURED**" = Non Accreditata "**DENIED BY RISK**" = Negata per superamento limiti imposti dalla banca "**HOST TIMEOUT**" = Non elaborata per mancato collegamento con l'host
auth	9	Codice di Autorizzazione rilasciato dalla compagnia carte di credito in caso di transazione autorizzata
postdate	4	Data della transazione (formato mmgg)
trackid	256	Codice identificativo della transazione associato dal Merchant
ref	20	Codice della transazione rilasciato dalla banca che convenziona il Merchant
udf1 – udf5	256	Campi valorizzati nel PaymentInit a discrezione del Merchant e che il Payment Gateway ritorna inalterati
cardtype	10	Il tipo di carta utilizzata per l'acquisto: "VISA" = Visa "MC" = Mastercard "AMEX" = American Express "DINERS" = Diners Club "JCB" = JCB
payinst	10	Indica il protocollo di sicurezza utilizzato per l'acquisto.

		Per i dettagli sulle valorizzazioni e relativi significati, si rimanda al documento allegato *"Protocolli di sicurezza*".
liability	1	Può assumere i seguenti valori: "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. Vedere il documento allegato *"Protocolli di sicurezza*" per maggiori informazioni.

Caso: Transazione non elaborata, a causa di errori tecnici

In questo caso il NotificationMessage consiste dei seguenti campi:

Nome Campo	Lungh. max	Descrizione
paymentid	20	Codice univoco identificativo dell'ordine
Error	10	Codice dell'errore riscontrato
ErrorText	256	Descrizione dell'errore riscontrato

In risposta, il Merchant comunicherà l'URL a cui vuole che il Cardholder venga rediretto per la presentazione della pagina di risposta. La stringa di testo da ritornare al Payment Gateway, che deve costituire l'unico output della pagina dinamica predisposta dal Merchant, deve avere la seguente struttura:

"REDIRECT=" + URL da utilizzare per la redirezione del browser

esempio: REDIRECT=http://www.miosito.com/result.asp?paymentID=123456

Se per cause tecniche il browser non dovesse raggiungere l'URL di visualizzazione dell'esito, si verrebbe a creare una situazione di disallineamento in cui il Merchant conosce l'esito della transazione mentre il Cardholder no. Il Cardholder potrebbe credere che la transazione non sia andata a buon fine e procedere con un nuovo pagamento.

Per allineare comunque il Cardholder, il Merchant può configurare (utilizzando le funzioni presenti sul sito di Back Office) l'invio dell'e-mail di notifica dell'esito della transazione verso il Cardholder.

In alternativa, si consiglia di verificare sempre che il browser visualizzi la pagina di esito. Se ciò non avvenisse, si potrebbe decidere di procedere in uno dei seguenti modi:

- contattare direttamente il Cardholder, magari inviandogli un messaggio e-mail nel quale gli si comunica l'esito della transazione
- oppure effettuare lo storno/annullo automatico on-line della transazione (vedi "Messaggio Payment")

ErrorURL

Se per qualunque motivo lo scambio di messaggi NotificationMessage (Richiesta PG + Risposta Merchant) non va a buon fine, il Payment Gateway redireziona il browser del Cardholder sull'ErrorURL. La situazione che si crea è la seguente:

- La transazione potrebbe essere andata a buon fine
- Il Merchant non ha ricevuto la notifica e quindi non è allineato
- Il Cardholder viene rediretto sull'ErrorURL, che chiaramente presenta un'informazione statica in quanto il Merchant non conosce l'esito. Egli vede una risposta negativa e potrebbe essere indotto a riprovare l'acquisto

E' quindi importante che il Merchant prepari l'ErrorURL in modo tale da ricavare informazioni utili per poter investigare l'accaduto e informare successivamente il Cardholder sull'esito dell'acquisto.

Si consiglia, quindi, d'inserire un parametro identificativo in coda all'URL, ad esempio il TrackID, già noto al Merchant in fase di inizializzazione del pagamento.

Messaggio Payment

Tramite un semplice scambio di messaggi server-to-server il Merchant può effettuare in modo automatizzato operazioni contabili da remoto. I campi da inserire nel messaggio di richiesta sono:

Nome Campo	Obbligatorio	Lungh. max	Descrizione
paymentid	S	20	Codice univoco identificativo dell'ordine originario creato dal Payment Gateway e comunicato al Merchant nel PaymentInit
tranid	S	20	Codice univoco identificativo della transazione originaria, creato dal Payment Gateway e comunicato al Merchant nel NotificationMessage
id	S	8	Codice identificativo del Merchant, assegnato in fase di attivazione del servizio
password	S	8	Password assegnata al Merchant in fase di attivazione del servizio
action	S	1	Tipo di operazione richiesta: 2 = **Credit** 3 = **Reversal** 5 = **Capture** 9 = **Void** Si rimanda all'Appendice A per le operazioni permesse e relativi ambiti di applicazione
amt	S	9	Importo dell'operazione in formato NNNNN.NN. Si rimanda all'Appendice A per gli importi permessi sui vari tipi di operazione
trackid	S	256	Codice identificativo dell'ordine associato dal Merchant. Solitamente è il codice identificativo dell'ordine

			di acquisto presso il sito del Merchant. E' consigliabile che questo codice sia univoco per ogni transazione
currencycode	S	3	Codice ISO valuta. Fisso a "978" (Euro)
udf1 – udf5	N	256	Campi valorizzati a discrezione del Merchant e che il Payment Gateway ritorna inalterati

La risposta che il Payment Gateway ritorna al Merchant, dopo aver verificato la validità (ID e Password del Merchant) della richiesta ed elaborato l'operazione, contiene i seguenti campi:

Nome Campo	**Lungh. max**	**Descrizione**
Result	20	Esito dell'operazione: "**CAPTURED**" = Accreditata (se Action=5) "**CAPTURED**" = Riaccreditata (se Action=2) "**NOT CAPTURED**" = Non Accreditata/Riaccreditata "**VOIDED**" = Annullata (Action=9) "**REVERSED**" = Stornata (Action =3) "**DENIED BY RISK**" = Negata per superamento limiti imposti dalla banca "**HOST TIMEOUT**" = Non elaborata per mancato collegamento con l'host
Auth	9	Codice di Autorizzazione rilasciato dalla compagnia, relativo alla transazione originaria
Ref	20	Codice di Riferimento banca per l'operazione
Avr	1	Fisso a "NA"
postdate	4	Data dell'operazione (formato mmgg)
tranid	20	Codice univoco identificativo dell'operazione assegnato dal Payment Gateway
trackid	256	Codice identificativo della operazione associato dal Merchant

udf1 – udf5	256	Campi valorizzati a discrezione del Merchant e che il Payment Gateway ritorna inalterati

e24PaymentPipe - Descrizione

Il Consorzio Triveneto S.p.A. fornisce ai merchants un pacchetto software che comprende il plug-in e24PaymentPipe nelle versioni disponibili, che coprono una vasta gamma di piattaforme utilizzate per le applicazioni Internet, tra cui:

- Java
- ASP
- ActiveX/COM
- ColdFusion

Il software viene fornito dal Consorzio, assieme a questo manuale, all'interno dell'e-mail di attivazione in ambiente di test inviata al Merchant. La release più recente, sia del manuale che del software, è comunque sempre disponibile per il download collegandosi al Back Office del Consorzio, aprendo poi il menu "Sviluppatori" e selezionando la voce "Downloads". L'accesso al Back Office viene fornito solo in ambiente di produzione.

Riportiamo qui di seguito le caratteristiche principali delle diverse versioni di e24PaymentPipe.

ActiveX/COM

L'oggetto ActiveX/COM e24PaymentPipe.dll fornito è provvisto di un insieme di metodi e proprietà per effettuare transazioni in tempo reale in Internet in modo sicuro. L'oggetto può essere utilizzato in applicazioni desktop, CGI, web server API, ASP e altre.

L'elenco completo delle proprietà supportate dal componente è presente nella documentazione presente nella cartella "docs\dll" dello zip.

Occorre tener presente che le proprietà con accesso in sola lettura acquistano significato solo dopo che una transazione è stata portata a termine con successo.

Nella cartella "docs\vb-example"dello zip è riportato anche un semplice esempio di utilizzo del componente all'interno di un programma Visual Basic.

Active Server Pages

Lo stesso oggetto visto al punto precedente può essere utilizzato, con un'altra interfaccia, in ambiente ASP tenendo presente che, poiché i progetti ASP non supportano la comunicazione ed elaborazione asincrona, il componente e24PaymentPipe non ritornerà messaggi di stato.

Nella cartella "docs\asp-example" dello zip è riportato un semplice esempio di creazione e utilizzo del componente da uno script in ambiente ASP.

ColdFusion

Lo stesso oggetto può ancora essere utilizzato con i progetti creati con tecnologia ColdFusion.

Nella cartella "docs\coldfusion" dello zip è presente un documento con le indicazioni per referenziare il componente dall'interno di script ColdFusion, comprensivo di un semplice esempio.

Java

La classe Java e24PaymentPipe può essere usata in una grande varietà di ambienti di sviluppo per realizzare applicazioni che vanno dal desktop al web e che sono platform independent. L'oggetto e24PaymentPipe è un componente che ogni sviluppatore può utilizzare per abilitare alle transazioni e-commerce il proprio sito web.

Il plug-in viene reso disponibile sia come insieme di classi stand-alone (cartella "java" all'interno dello zip) sia come package jar (cartella "java-package" all'interno dello zip). La classe "e24PaymentPipeTester contiene un metodo main e può essere utilizzata per lanciare manualmente, impostando opportunamente i parametri, il plug-in.

Nella cartella "docs\java" dello zip si trova la documentazione in cui vengono descritte le classi e dettagliati tutti i campi e i metodi gestiti dal plug-in.

Specifiche di interfacciamento diretto

Nel caso in cui non si disponga di una piattaforma adatta all'utilizzo del plug-in e24PaymentPipe o si desideri creare una propria interfaccia, vengono elencate qui di seguito tutte le informazioni relative al protocollo di comunicazione, al formato di trasmissione e ricezione dei messaggi, delle loro variabili e dei messaggi di errore.

Il plug-in e24PaymentPipe è stato sviluppato su queste specifiche, e fornisce un'interfaccia di alto livello già pronta per l'utilizzo.

Specifiche del protocollo di comunicazione

- **Protocollo**:
  http in ambiente di test
  https in produzione

- **Target (action):**
  in ambiente di test
  http://test4.constriv.com/cg301/servlet/PaymentInitHTTPServlet
  per il messaggio PaymentInit

  http://test4.constriv.com/cg301/servlet/PaymentTranHTTPServlet
  per il messaggio Payment

  in ambiente di produzione
  https://www.constriv.com/cg/servlet/PaymentInitHTTPServlet
  per il messaggio PaymentInit

  https://www.constriv.com/cg/servlet/PaymentTranHTTPServlet
  per il messaggio Payment

- **Porta**:
  80 in ambiente di test
  443 in produzione

- **Method**: POST

- **Content-Type**: "application/www-form-urlencoded" o "application/x-www-form-urlencoded"

- **Formato Transmissione Dati**:Url Encoded

- **Formato Ricezione Dati**:Singola stringa di testo formata dai valori dei campi, separati da ":"

- **Encryption Level**:
  nessuno in ambiente di test
  SSL3 in produzione

Formato Trasmissione Dati

Tutti i dati devono essere postati in formato URL encoded, composto da coppie nome-valore.

Messaggio PaymentInit
id=TranPortalID&password=password&action=action&langid=language&currencycode=978&amt=amount&responseURL=www.merchant.com/response&errorURL=www.merchant.com/error &trackid=unique tracking id&udf1=User Defined Field 1&udf2=User Defined Field 2&udf3=User Defined Field 3&udf4=User Defined Field 4&udf5=User Defined Field 5

Messaggio Payment:
id=TranPortalID&password=password&action=action&currencycode=978&amt=amount&paymentid=paymentID&transid=transID&trackid=trackID&udf1=User Defined Field 1&udf2=User Defined Field 2&udf3=User Defined Field 3&udf4=User Defined Field 4&udf5=User Defined Field 5

Formato Ricezione Dati

La risposta del Payment Gateway ha sempre il formato di una stringa di testo in cui sono presenti i valori delle variabili (non i nomi) in un'ordine prestabilito; è compito del Merchant recuperare i dati dalla stringa:

PaymentInit Response:
PaymentId:PaymentURL

Payment Response:
Result:Auth:Ref:AVR:Date:TransId:TrackId:UDF1:UDF2:UDF3:UDF4:UDF5

Messaggi di risposta in condizioni di errore

Se un errore si verifica durante l'elaborazione di un messaggio inviato al Payment Gateway (**PaymentInit** o **Payment**), il messaggio di risposta che il Payment Gateway invia ha la forma di una stringa di testo particolare. La stringa inizia con l'identificatore:

"!ERROR!"

al quale segue il codice d'errore e la descrizione dello stesso. E' perciò fondamentale per prima cosa, quando si riceve una risposta, verificare che la stringa contenga o meno l'identificatore, per capire se si è verificato un errore.

In Appendice C è riportata la lista dei codici di errore di Payment Gateway.

Demo

Nel Plugin302.zip è stato incluso un semplice sito e-Commerce di esempio, chiamato "Colors of Success", che implementa le funzioni base del meccanismo di interfacciamento al servizio Payment Gateway. Questo negozio demo è disponibile in 3 tecnologie differenti:

- ASP – realizzato sia in modalità interfacciamento diretto sia agganciandosi al plug-in e24PaymentPipe versione .dll
- PHP – realizzato in modalità interfacciamento diretto, dato che non è disponibile un plug-in per php
- JSP – realizzato agganciandosi al plug-in e24PaymentPipe versione classe java.

Il negozio, in ciascuna delle versioni sviluppate, comprende le seguenti pagine:

- "Index": una prima pagina che rappresenta la scelta di un prodotto a catalogo e l'impostazione della quantità desiderata
- "Details": la pagina di checkout, nella quale l'utente controlla gli articoli presenti nel carrello e i prezzi, fornisce i propri dati necessari per l'evasione dell'ordine e clicca sul pulsante "Paga" per accedere all'area protetta dove inserire i dati di pagamento
- "**Buy**": (solo versioni ASP e JSP) attivato dal pulsante "Paga", richiama il plug-in fornendogli i dati dell'ordine. Il plug-in prepara ed invia al Payment Gateway il messaggio PaymentInit. Il Payment Gateway restituisce i dati per la redirezione e il browser viene quindi redirezionato sulla pagina HPP del Consorzio sulla quale inserire i dati della carta di credito.
- "**Pure-Buy**": (solo versioni ASP e PHP) in alternativa alla pagina precedente, questa pagina effettua le stesse azioni senza bisogno di installare il plug-in sul proprio server. Per utilizzarla, modificare Details.asp per puntare a questa pagina (nella action del form).
- "Receipt": dopo che la transazione è stata elaborata il Payment Gateway manda il NotificationMessage al Notify URL, infine il Payment Gateway redireziona il browser all'URL ritornato da questa pagina.
- "Result": l'URL finale del Merchant che visualizza l'esito al browser.
- "Error": in caso di errore nell'invio del NotificationMessage, il browser viene redirezionato su questa pagina.

Per l'installazione delle demo si rimanda all'Appendice B.

Capitolo 4 - Ambiente di Test

Il Consorzio Triveneto S.p.A. mette a disposizione un ambiente di test dove il Merchant può effettuare liberamente transazioni per predisporre correttamente l'interfacciamento verso il Payment Gateway, in vista del passaggio in produzione.

L'ambiente di test è sempre disponibile, anche se non può esserne garantita la disponibilità H24, a causa d'interventi di manutenzione correttiva o evolutiva che potrebbero renderlo inutilizzabile, senza preavviso.

Variabili da impostare per la creazione del messaggio PaymentInit

Se si utilizza il plug-in, per la connessione al Payment Gateway di test usare i valori seguenti:

- address: test4.constriv.com
- context: /cg301
- port: 80
- SSL: False (usato solo per plug-in versione .dll)

Se invece si utilizza l'interfacciamento diretto l'indirizzo completo per creare la connessione è il seguente:

- http://test4.constriv.com/cg301/servlet/PaymentInitHTTPServlet

L'ambiente di test è attivo anche in modalità SSL, utilizzando per la cifratura del canale un certificato auto-generato.

Se si utilizza il plug-in, per la connessione usare i valori seguenti:

- port: 443
- SSL: True (usato solo per plug-in versione .dll)

Se invece si utilizza l'interfacciamento diretto l'indirizzo completo per creare la connessione è il seguente:

- https://test4.constriv.com/cg301/servlet/PaymentInitHTTPServlet

Tenere presente che il certificato dell'ambiente di test è auto-generato: per evitare errori nella connessione, in alcuni sistemi è necessario inserire il nostro certificato di CA, utilizzato per l'emissione del certificato SSL, tra le CA ritenute attendibili sul proprio server.

Il certificato è fornito, in formato PEM, nell'Appendice E.

Le variabili da impostare in modo fisso sono le seguenti:

- id: comunicato tramite e-mail assieme a questo documento
- password: comunicato tramite e-mail assieme a questo documento

Gli altri parametri possono essere definibili liberamente.

Casi di test raccomandati

Il Consorzio Triveneto raccomanda di effettuare almeno i seguenti test, che rappresentano le casistiche reali più frequenti, prima di inviare al Supporto Clienti la conferma di fine test e richiedere quindi il passaggio in produzione.

Test n°1 – Transazione con esito positivo

Una volta giunti alla HPP del Consorzio, utilizzare la seguente carta

Numero	**Scadenza**	**CVV2**
4539990000000012	qualsiasi data futura	qualsiasi numero di 3 o 4 cifre

Verificare che:

- il NotificationMessage sia stato ricevuto correttamente con tutti i campi previsti (PaymentID, TransID, TrackID, postdate, resultcode, auth, udf1, udf2, udf3, udf4, udf5, cardtype, payinst, liability)
- la transazione abbia esito positivo (resultcode="APPROVED" se si è usato Action=4, "CAPTURED" se si è usato Action=1)
- Il browser sia stato re-direzionato correttamente all'indirizzo fornito in risposta al NotificationMessage precedente

Test n°2 – Transazione con esito negativo

Una volta giunti alla HPP del Consorzio, utilizzare la seguente carta

Numero	**Scadenza**	**CVV2**
4539990000000020	qualsiasi data futura	qualsiasi numero di 3 o 4 cifre

Verificare che:

- Il NotificationMessage sia stato ricevuto correttamente con tutti i campi previsti (PaymentID, TransID, TrackID, postdate, resultcode, auth, udf1, udf2, udf3, udf4, udf5, cardtype, payinst, liability)

- la transazione abbia esito negativo (resultcode="NOT APPROVED" se si è usato Action=4, "NOT CAPTURED" se si è usato Action=1)

- Il browser sia stato re-direzionato correttamente all'indirizzo fornito in risposta al NotificationMessage precedente

Test n°3 – Transazione 3-D Secure con esito positivo

Una volta giunti alla HPP del Consorzio, utilizzare la seguente carta:

Numero	**Scadenza**	**CVV2**	**Password**
4015505250179218	qualsiasi data futura	qualsiasi numero di 3 o 4 cifre	ctv2002

Verificare che:

- Il NotificationMessage sia stato ricevuto correttamente con tutti i campi previsti (PaymentID, TransID, TrackID, postdate, resultcode, auth, udf1, udf2, udf3, udf4, udf5, cardtype, payinst, liability)

- la transazione abbia esito positivo (resultcode="APPROVED" se si è usato Action=4, "CAPTURED" se si è usato Action=1)

- lo strumento di pagamento utilizzato sia "VPAS" (campo "payinst")

- Il browser sia stato re-direzionato correttamente all'indirizzo fornito in risposta al NotificationMessage precedente

Test n°4 – Transazione non elaborata per dati non corretti

Una volta giunti alla HPP del Consorzio, utilizzare la seguente carta:

Numero	**Scadenza**	**CVV2**
4999000055550000	qualsiasi data futura	qualsiasi numero di 3 o 4 cifre

Verificare che:

- Il NotificationMessage sia stato ricevuto correttamente con tutti i campi previsti (PaymentID, Error, ErrorText)

- Il campo “Error” abbia valore “GW00853” e che il campo “ErrorText” contenga la descrizione dell’errore “GW00853-Numero Carta non valido.”

- Il browser sia stato re-direzionato correttamente all’indirizzo fornito in risposta al NotificationMessage precedente

Test n°5 (opzionale) – Operazioni Contabili

Nel caso si desideri testare l’effettuazione di operazioni contabili post-transazionali (messaggio “Payment”) da remoto senza utilizzo del back office, tenere presenti le seguenti impostazioni.

Connessione: se si utilizza il plug-in non vi sono modifiche ai parametri, mentre con l’interfacciamento diretto l’indirizzo cui puntare è il seguente:

- http://test4.constriv.com/cg301/servlet/PaymentTranHTTPServlet

Altri parametri:

- TrackID: lo stesso TrackID utilizzato per la transazione originaria
- TransID: il TransID fornito dal Payment Gateway per la transazione originaria
- PaymentID: il PaymentID fornito dal Payment Gateway per la transazione originaria

N.B. **Verificare in Appendice A le operazioni contabili consentite in base al tipo di transazione.**

Capitolo 5 - Personalizzazione della HPP

Come accennato in precedenza, la Hosted Payment Page presentata dal Payment Gateway al Cardholder può essere personalizzata dal Merchant. Il Merchant può impostare sulla HPP uno stile grafico simile al proprio sito dando al Cardholder l'impressione di rimanere sul sito iniziale e rendendo quindi la redirezione trasparente.

Assieme al presente manuale viene fornito anche il documento "Specifiche Personalizzazione HPP", al quale si rimanda per produrre la personalizzazione in modo corretto, attenendosi alle direttive imposte dalla propria banca. Nel caso in cui non si intenda fornire una propria personalizzazione, verrà utilizzata quella standard predisposta dalla banca stessa.

Appendice A - Gestione contabile delle transazioni

In una transazione con carta di credito su Internet, il movimento di denaro dall'acquirente (Cardholder) verso il venditore (Merchant) può avvenire nel momento stesso della transazione o in un momento successivo.

Il sistema Payment Gateway fornito dal Consorzio Triveneto S.p.A. permette al Merchant di stabilire a livello di singola transazione quale dovrà essere il sistema di contabilizzazione da seguire.

Il sistema Payment Gateway permette altresì di effettuare tutta una serie di operazioni successive alla transazione, come l'annullo o il rimborso dell'importo al Cardholder. Ogni operazione descritta può essere effettuata in due modi distinti, a seconda delle esigenze e della propria struttura:

- Modalità automatizzata: l'operazione si concretizza da remoto con un messaggio server-to-server (messaggio "Payment") dal sistema del Merchant al Payment Gateway. Si può utilizzare indifferentemente allo scopo il Plugin e24PaymentPipe o l'interfacciamento diretto.
- Modalità Manuale: l'operazione si concretizza collegandosi al sito di Back Office fornito dal Payment Gateway al Merchant, selezionando la transazione di interesse e richiedendo l'operazione.

Contabilizzazione Immediata

Questa modalità viene attivata se nel messaggio PaymentInit il Merchant imposta il parametro **Action=1**. La transazione prende in questo caso il nome di "Purchase".

Se la transazione ha esito positivo il Merchant viene accreditato con data contabile pari alla data della transazione.

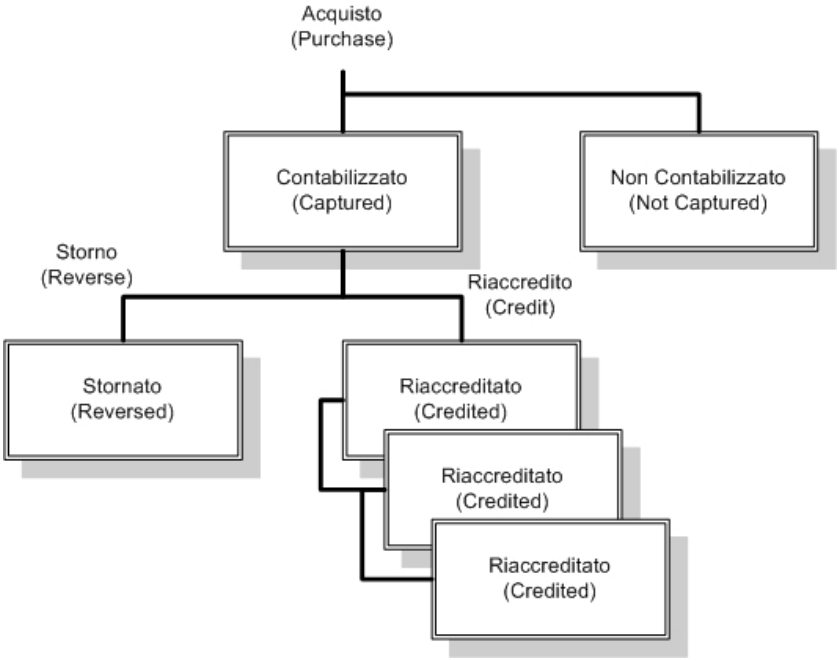
La modalità immediata dovrebbe essere adottata esclusivamente nel caso di vendita di servizi di cui l'acquirente comincia ad usufruire immediatamente.

Successivamente alla transazione originaria, in caso di reso della merce o altri fattori, è possibile:

- Stornare ("**Reversal**") la transazione: l'intero importo viene rimborsato al Cardholder e il Merchant viene addebitato per lo stesso importo. Se l'operazione avviene nella stessa giornata dell'acquisto è possibile (a discrezione dell'ente emittente della carta) ripristinare la disponibilità di spesa mensile della carta. L'operazione di Reversal si ottiene impostando il paramentro **Action=3**.

- Riaccreditare ("**Credit**") totalmente o parzialmente la transazione: e' possibile effettuare più riaccrediti successivi su una stessa transazione; ma l'importo totale dei riaccrediti non può comunque superare l'importo contabilizzato. L'operazione di Credit si ottiene impostando il parametro **Action=2**.

Lo schema temporale completo comprendente tutte le azioni possibili è il seguente:



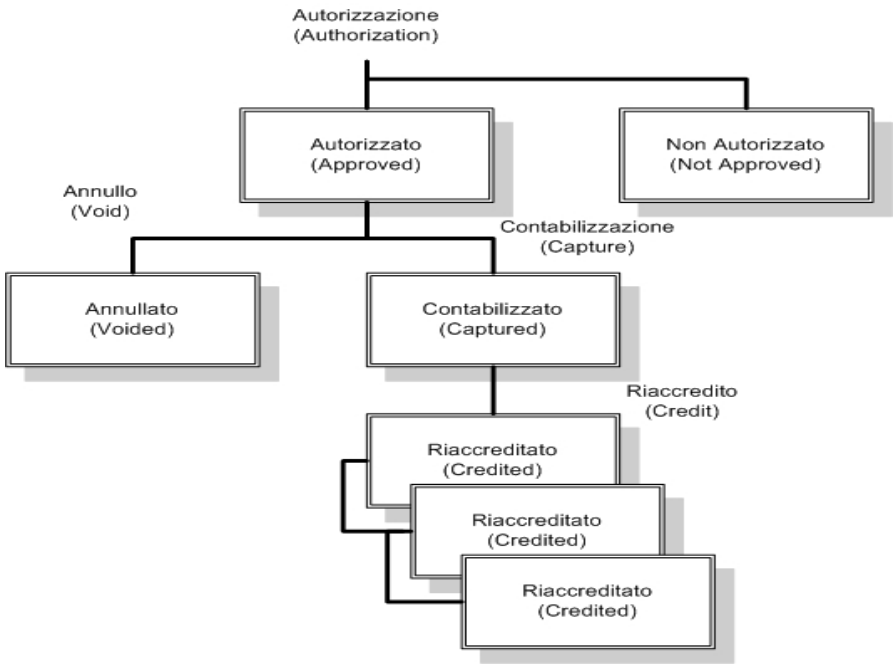
Contabilizzazione differita

Questa modalità viene attivata se nel messaggio PaymentInit il Merchant imposta il parametro **Action=4**. La transazione prende in questo caso il nome di "Authorization".

Se la transazione ha esito positivo il plafond della carta di credito del Cardholder viene bloccato per l'importo della transazione.

- Con la modalità differita il Merchant deve richiedere espressamente l'accredito (detto "**Capture**") della transazione, che di solito avviene al momento dell'evasione dell'ordine. Pertanto l'importo da accreditare può essere impostato sulla base della merce effettivamente inviata (comunque non superiore all'importo inizialmente bloccato). L'operazione di Capture si ottiene impostando il paramentro **Action=5**.
- Se si verificano dei problemi il Merchant, anziché richiedere l'accredito, può annullare (detto "**Void**") la transazione. Se la richiesta è effettuata nella stessa giornata della transazione iniziale, il plafond della carta di credito utilizzata può (a discrezione dell'ente emittente) essere ripristinato immediatamente). L'operazione di Void si ottiene impostando il parametro **Action=9**.
- In un momento successivo all' accredito l'acquirente potrebbe restituire tutte o parte delle merci acquistate al Merchant. In questo caso il Merchant procede al riaccredito (detto "**Credit**"), totale o parziale, dell'importo precedentemente accreditato. E' possibile effettuare più riaccrediti su una stessa transazione; ma l'importo totale dei riaccrediti non può comunque superare l'importo accreditato. L'operazione di Credit si ottiene impostando il parametro **Action=2**.

Lo schema temporale completo comprendente tutte le azioni possibili è il seguente:



Appendice B - Installazione del Demo

Versione asp

Registrazione dll

- Estrarre i files forniti nel package Plugin302.zip in una nuova directory, ad es. “c:\e24plugin”
- Aprire una finestra DOS e andare alla directory “c:\e24plugin\DLL\Release”
- Digitare il seguente comando: “regsvr32 e24PaymentPipe.dll”
- Dovrebbe comparire una finestrella che segnala il successo dell’operazione. Cliccare allora su “OK” per chiuder la finestra.
- Se la finestra segnala un errore, chiuderla. Tornare poi alla finestra DOS, puntare alla directory “ c:\e24plugin\DLL\Debug”, e ritentare il comando: “regsvr32 e24PaymentPipe.dll”

Installazione sito demo

- Installare Microsoft IIS, se non presente.
- Copiare i files forniti nella cartella c:\e24plugin\demo-asp in una nuova directory, “c:\inetpub\wwwroot\demo”
- Tramite la Console di IIS creare un nuovo sito “MerchantDemo”:
  - Nella finestra “Properties->Home Directory” impostare nel Local Path il percorso della directory “demo”
  - In Execute Permissions impostare “Scripts only”
- Riavviare IIS
- Aprire un browser e puntare all’URL: http://localhost:port/demo/index.asp (dove port è la porta TCP configurata per IIS)

Versione jsp

- Copiare il file “demo-jsp.war” presente nella cartella c:\e24plugin\demo-jsp sotto la cartella “webapps” (o equivalente cartella base in cui inserire le web application) del proprio application server.
- Riavviare l’application server
- Aprire un browser e puntare all’URL: http://localhost:port/demo-jsp/index.jsp (dove port è la porta TCP configurata per l’application server)

Versione php

- Copiare i files forniti nella cartella c:\e24plugin\demo-php sotto la cartella configurata per le applicazioni php.
- Creare un website “demo-php” sul web server utilizzato in collegamento con il motore php.
- Riavviare il web server utilizzato in collegamento con php.
- Aprire un browser e puntare all’URL: http://localhost:port/demo-php/index.php (dove port è la porta TCP configurata sul web server per il sito demo-php)

Appendice C - Lista dei Codici di Errore

GW00100-Institution ID required.
GW00101-Brand ID required.
GW00102-Brand Description required.
GW00103-BIN range overlaps an existing brand.
GW00104-Start BIN required.
GW00105-BIN length too long.
GW00106-Start and end BIN lengths differ.
GW00107-End BIN not greater then Start BIN.
GW00108-Invalid Brand ID.
GW00109-Invalid Description.
GW00110-Invalid Payment Instrument List.
GW00111-Invalid Start Bin.
GW00112-Invalid End Bin.
GW00113-Terminal exists for this Brand.
GW00114-Card Check Digit Flag Invalid.
GW00115-Card Expiration Flag Invalid.
GW00116-Card Verification Code Flag Invalid.
GW00117-Card Address Verification Flag Invalid.
GW00150-Missing required data.
GW00151-Invalid Action type
GW00152-Invalid Transaction Amount.
GW00153-Invalid Transaction ID.
GW00154-Invalid Terminal ID.
GW00155-Invalid Batch Track ID.
GW00156-Batch track ID not unique.
GW00157-Invalid Payment Instrument.
GW00158-Card Number Not Numeric.
GW00159-Card Number Missing.
GW00160-Invalid Brand.
GW00161-Invalid Card/Member Name data.
GW00162-Invalid User Defined data.
GW00163-Invalid Address data.
GW00164-Invalid Zip Code data.
GW00165-Invalid Track ID data.
GW00166-Invalid Card Number data.
GW00167-Invalid Currency Code data.
GW00168-Institution ID mismatch.
GW00169-Merchant ID mismatch.
GW00170-Terminal ID mismatch.
GW00171-Payment Instrument mismatch.
GW00172-Card Verification Code Mismatch.
GW00173-Currency Code mismatch.
GW00174-Card Number mismatch.
GW00175-Invalid Result Code.
GW00176-Failed Previous Captures check.
GW00177-Failed Capture Greater Than Auth check.
GW00178-Failed Void Greater Than Original Amount check.
GW00179-Failed Previous Voids check.
GW00180-Failed Previous Credits check.
GW00181-Failed Credit Greater Than Debit check.
GW00182-Failed to Load Merchant Record for Validation.
GW00183-Card Verification Digit Required.
GW00184-Failed to Load Terminal Record for Validation.
GW00185-Invalid Authentication Token.
GW00186-Invalid Transaction Identifier (XID).
GW00187-Invalid Electronic Commerce Indicator.
GW00188-Missing Electronic Commerce Indicator.
GW00189-Missing Authentication Token.
GW00190-Missing Transaction Identifier (XID).
GW00191-Void After Capture Not Allowed.
GW00192-Transaction denied due to previous transactions check failure.
GW00193-Credit denied due to previous Void check failure.
GW00194-Capture denied due to previous Void check failure.
GW00195-Void Purchase denied due to previous Credit check failure.
GW00196-Void Auth denied due to previous Capture check failure.
GW00200-Address verification failed.
GW00201-Transaction not found.
GW00202-Hack attempt detected.
GW00203-Invalid access: Must use POST method.
GW00204-Invalid Original Transaction ID.
GW00205-Invalid Subsequent Transaction.
GW00250-Transaction denied: Negative Card
GW00251-Maximum transaction count exceeded.
GW00252-Maximun transaction volume exceeded.
GW00253-Maximum credit volume exceeded.

GW00254-Maximum card debit volume exceeded.
GW00255-Maximum card credit volume exceeded.
GW00256-Maximum card transaction count exceeded.
GW00257-Maximum transaction amount exceeded.
GW00258-Transaction denied: Negative BIN
GW00259-Transaction denied: Declined Card
GW00260-Transaction denied: Credits exceed Captures
GW00261-Transaction denied: Captures exceed Authorizations
GW00300-Institution ID required.
GW00301-Risk Profile ID required.
GW00302-Currency code required.
GW00303-Risk Profile in use.
GW00304-Invalid Risk Profile ID.
GW00305-Invalid Currency Code.
GW00306-Invalid Risk Profile setting.
GW00307-Invalid Max floor limit/$ amount.
GW00308-Invalid Max floor limit transaction count.
GW00309-Invalid Max daily processing amount.
GW00310-Invalid Max credit processing amount.
GW00311-Invalid Max 24hr debit amount.
GW00312-Invalid Max 24hr credit amount.
GW00313-Invalid Max transaction count daily.
GW00350-Merchant has terminals.
GW00351-Merchant ID required.
GW00352-Institution ID required.
GW00353-Invalid Login.
GW00354-Invalid Login.
GW00355-New password mismatch.
GW00356-New password same as old.
GW00357-Console password required.
GW00358-Invalid Login.
GW00359-ISO Country code is invalid.
GW00360-Website address in invalid.
GW00361-Console Password Confirmation required.
GW00362-Console Password Confirmation invalid.
GW00363-Password Confirmation mismatch.
GW00364-Name is invalid.
GW00365-Institution ID is invalid.
GW00366-Merchant ID is invalid.
GW00367-Category Code is invalid.
GW00368-Address is invalid.
GW00369-City is invalid.
GW00370-State is invalid.
GW00371-Country is invalid.
GW00372-Web Site is invalid.
GW00373-Zip Code is invalid.
GW00374-Phone is invalid.
GW00375-FAX is invalid.
GW00376-Email is invalid.
GW00377-Contact is invalid.
GW00378-Currency Code is invalid.
GW00379-View Tran Detail is invalid.
GW00380-Merchant ID not numeric.
GW00381-Merchant Password data invalid.
GW00382-Merchant Category Description invalid.
GW00383-Merchant Password Confirmation invalid.
GW00384-Merchant New Password invalid.
GW00385-Merchant New Password is required.
GW00386-Merchant New Confirm Password is required.
GW00387-Merchant User Password is expired.
GW00388-Merchant User Name is required.
GW00389-Merchant User Password Confirmation is required.
GW00390-Password and confirmation password do not match.
GW00391-Merchant User password length is too short.
GW00392-Merchant User Status is required.
GW00393-Merchant User Status is invalid.
GW00394-Merchant User Password is required.
GW00395-Merchant Password and confirmation password do not match
GW00396-Merchant User new password same as old.
GW00397-Merchant User inactive.
GW00398-Merchant User Password length too long.
GW00399-Merchant User ID is invalid.
GW00400-Merchant User Password is invalid.
GW00401-Merchant New Password is invalid.
GW00402-Merchant User Name is invalid.
GW00403-Merchant Password Expire Code is invalid.
GW00404-Merchant Password Expires Date is invalid.
GW00405-Merchant exists with this Merchant Category.
GW00407-Category code must be numeric.
GW00408-Category code must be four digits.
GW00409-Merchant Parent ID is invalid.
GW00410-Merchant Super Merchant Flag is invalid.
GW00411-Generate Resource File is invalid.
GW00412-Deletion of current merchant user is invalid.
GW00420-Currency Code data in not available.
GW00421-Currency Code minor digits is invalid.
GW00422-Error Packing Message to Host.
GW00450-Institution ID required.
GW00451-Merchant ID required.
GW00452-Terminal ID required.

GW00453-TranPortal ID required.
GW00454-TranPortal password required.
GW00455-TranPortal ID not unique.
GW00456-Invalid TranPortal ID.
GW00457-Action not supported.
GW00458-Invalid Transaction Attempt.
GW00459-Terminal not active.
GW00460-TranPortal ID required.
GW00461-Invalid Transaction amount.
GW00462-Invalid Tranportal Password.
GW00463-Invalid Terminal Institution ID.
GW00464-Invalid Terminal Merchant ID.
GW00465-Invalid Terminal Terminal ID.
GW00466-Invalid Terminal Description.
GW00467-Invalid Terminal External Connection ID.
GW00468-Invalid Terminal Risk Profile.
GW00469-Invalid Terminal Currency Code List.
GW00470-Invalid Terminal Action Code List.
GW00471-Invalid Terminal Payment Instrument List.
GW00472-Invalid Terminal Brand List.
GW00473-Invalid Terminal Option Code List.
GW00474-Invalid Terminal Risk Flag.
GW00475-Invalid Terminal Address Verification List.
GW00476-Invalid Terminal Tranportal ID.
GW00477-Invalid Terminal Status.
GW00478-Invalid Terminal Card Acceptor ID.
GW00479-Invalid Terminal Card Acceptor Terminal ID.
GW00480-Invalid Terminal Acquirer Institution.
GW00481-Invalid Terminal Base24 Terminal Data.
GW00482-Invalid Terminal Retailer ID.
GW00483-Invalid Terminal Retailer Group ID.
GW00484-Invalid Terminal Retailer Region ID.
GW00485-Invalid Terminal Cutover Hour.
GW00486-Invalid Terminal Cutover Minute.
GW00487-Invalid Terminal Account Brand List.
GW00488-Error with Transaction Origin.
GW00600-Card number required.
GW00601-Card BIN required.
GW00602-Invalid BIN length.
GW00603-Institution ID required.
GW00604-Merchant ID required.
GW00605-Terminal ID required.
GW00606-Card number required.
GW00607-Invalid Card Number.
GW00608-Invalid Currency Code.
GW00609-Invalid Decline Reason.
GW00610-Invalid Card Number.
GW00611-Invalid Negative Reason.
GW00612-Invalid Card Bin.
GW00613-Invalid Negative Reason.
GW00700-No processes available.
GW00701-Batch not processed.
GW00702-Batch could not be started.
GW00703-Institution ID required.
GW00704-Batch ID not numeric.
GW00705-Batch ID required.
GW00706-Invalid Batch Response File Name
GW00750-Error hashing card number.
GW00850-Missing required data.
GW00851-Invalid Action Type.
GW00852-Invalid Card Number.
GW00853-Invalid Card Number.
GW00854-Invalid Expiration Date.
GW00856-Invalid Card Verification Code.
GW00857-Invalid Electronic Commerce Indicator.
GW00858-Missing required data - CVV
GW00859-Missing required data - Expiry Year
GW00860-Missing required data - Expiry Month
GW00861-Missing required data - Cardholder Name
GW00862-Missing required data - Card Address
GW00863-Missing required data - Card Postal Code
GW00870-Missing required data.
GW00871-Invalid Action Type.
GW00872-Invalid Card Number.
GW00873-Invalid Card Number.
GW00874-Invalid Expiration Date.
GW00876-Invalid Card Verification Code.
GW00877-Invalid Electronic Commerce Indicator.
GW00878-Missing required data - CVV
GW00879-Missing required data - Expiry Year
GW00880-Missing required data - Expiry Month
GW00881-Missing required data - Cardholder Name
GW00882-Missing required data - Card Address
GW00883-Missing required data - Card Postal Code
GW00884-Missing required data - PIN
GW00925-Authorization Color Invalid.
GW00926-Authorization Range Invalid.
GW00927-Authorization Unit of Measurement Invalid.
GW00950-Batch Upload Directory Required.
GW00951-Batch Download Directory Required.
GW00952-Batch Archive Directory Required.
GW00953-Access Log Retention Days Required.

GW00954-Transaction Log Retention Days Required.
GW00955-Declined Card Retention Minutes Required.
GW00956-Declined Card Maximum Count Required.
GW00957-Access Log Retention Days Invalid.
GW00958-Transaction Log Retention Days Invalid.
GW00959-Declined Card Retention Minutes Invalid.
GW00960-Declined Card Maximum Count Invalid.
GW00961-Multiple Capture Flag Invalid.
GW00962-Multiple Capture Amount Flag Invalid.
GW00963-Multiple Void Flag Invalid.
GW00964-Compare Void Amount Flag Invalid.
GW00965-Multiple Credit Debit Flag Invalid.
GW00966-Compare Credit Debit Amount Flag Invalid.
GW00967-Batch Upload Directory Invalid.
GW00968-Batch Download Directory Invalid.
GW00969-Batch Archive Directory Invalid.
GW00970-Invalid Terminal Cutover Hour.
GW00971-Invalid Terminal Cutover Minute.
GW00972-Card Number Mask Required.
GW00973-Card Number Mask Invalid.
GW00990-Card Number Encryption Failure.
GW00995-TranPortal ID invalid.
GW00996-TranPortal Password invalid.
GW00997-Batch Action invalid.
GW00998-Batch Transaction ID invalid.
GW00999-Batch Filename invalid.
GW01060-Currency Code Required.
GW01061-Institution ID Required.
GW01062-Invalid Minor Digits Range.
GW01063-Currency Code Not Numeric.
GW01064-Currency Code Not Valid ISO Code.
GW01065-Invalid Minor Digits.
GW01066-Invalid Amount.
GW01067-Invalid Currency Code Data.
GW01068-Invalid Currency Description Data.
GW01069-Invalid Minor Digits Data.
GW01070-Invalid Currency Symbol Data.
GW01071-Terminal exists with this Currency Code.
GW01072-Merchant exists with this Currency Code.
GW01100-Option Invalid Attempt Lockout is invalid.
GW01101-Option Maximum Password Days is invalid.
GW01102-Option Minimum Password Length is invalid.
GW01103-Option Maximum Password Length is invalid.
GW01104-Option Min Password Length is greater than the Max length.
GW01180-Hex required.
GW01181-Invalid Key length.
GW01182-Key encryption failed.
GW01190-TranPortal Password required.
GW01191-TranPortal Password invalid.
GW01192-Password encryption failed.
GW01193-Terminal Alias invalid.
GW01194=Error Generating Merchant Resource.
GW01195=Terminal Alias required.
GW01220-Institution ID Required.
GW01221-Transaction ID Required.
GW01222-Transaction Amount Required.
GW01240-Transaction denied: Merchant not allowed to capture greater then authorized amount
GW01241-Transaction denied: Merchant trying to capture greater then authorized percentage over authorization

---

CM00001-External message timeout.
CM00002-External message system error.
CM00026-External connection ID required.
CM00027-External connection description required.
CM00028-External connection Protocol code required.
CM00029-External connection Formatter class name invalid.
CM00030-External connection Protocol not supported.
CM00050-Institution has Merchants.
CM00051-Institution ID required.
CM00052-Invalid Institution Data Encryption Key Name.
CM00053-Missing Institution Data Encryption Key.
CM00054-Institution Data Encryption Key does not exist.
CM00055-Missing Institution Data Encryption Key.
CM00056-Institution Data Encryption Key does not exist.
CM00057-Institution User Security Admin class error.
CM90000-Database error.
CM90001-Database configuration error.
CM90002-Data format error.
CM90003-No Records Found.
CM90004-Duplicate found error.
CM90005-TimeStamp Mismatch error.
CM90100-Message formatter class failure.

PY20000-Missing required data.
PY20001-Invalid Action Type.
PY20002-Invalid amount.
PY20003-Invalid Order Status.
PY20004-Non Numeric Card Number.

PY20005-Missing Card Number.
PY20006-Invalid Brand.
PY20007-Invalid Order Status.
PY20008-Invalid Currency Code.
PY20009-Transaction Not Found.
PY20010-Invalid Merchant URL.
PY20011-Invalid Merchant Error URL.
PY20012-Invalid Track ID.
PY20013-Invalid Language Code.
PY20014-Invalid User Defined Field
PY20015-Invalid Card Name.
PY20016-Invalid Card Address.
PY20017-Invalid Zip Code.
PY20018-Invalid Card Verification Code.
PY20019-Invalid Transaction ID.
PY20049-Transaction failed with a VbV PARes Error.
PY20050-Card Number Encryption Failure.
PY20060=PY20060-Card Number Decryption Failure.
PY20080=PY20080-Invalid Payment Page Style File.
PY20081=PY20081-Invalid Payment Page Header File.
PY20082=PY20082-Invalid Payment Page Footer File.
PY20083=PY20083-Invalid Payer Authentication Response Message.
PY20084=PY20084-Invalid Payment ID.
PY20085=PY20085-Invalid Payment Status.
PY20086=PY20086-Instrument Not Allowed.
PY20090=PY20090-Customer cancelled transaction.

-------- ERRORI Durante transazioni 3-D Secure ----------

GV00001-Unknown 3-D Secure version
GV00002-Cardholder not enrolled
GV00003-Not a 3-D Secure Card
GV00004-PARes status not successful
GV00005-Certificate chain validation failed
GV00006-Certificate chain validation error
GV00007-Signature validation failed
GV00008-Signature validation error
GV00009-Invalid root certificate
GV00010-Missing data type
GV00011-Invalid expiration date
GV00012-Invalid action type
GV00013-Invalid Payment ID

-----ERRORI di plug-in legati a transazioni 3-D Secure ----

GV00100-Invalid action type
GV00101-Missing data type
GV00102-Invalid Amount
GV00103-Invalid Brand
GV00104-Payment ID not numeric
GV00200-Invalid Merchant Acceptor (Length)
GV00201-Invalid Merchant Acceptor
GV00202-Invalid Merchant Acceptor Terminal (Length)
GV00203-Invalid Merchant Acceptor Terminal
GV00204-Invalid Merchant Password (Length)
GV00205-Invalid Merchant Password
GV00206-Invalid Merchant Certificate Alias (Length)
GV00207-Invalid Merchant Certificate Alias

CGW000074-Merchant ID Invalid
CGW000160-Terminal ID Invalid
CGW000161-Terminal ID Missing
CGW000185-Track ID Invalid
CGW000191-Batch ID Invalid
CGW000241-Batch Action Invalid
CGW000242-Track ID In Use
CGW000296-Batch ID Missing
CGW000297-Batch Status Missing
CGW000313-Merchant Exists for Category
CGW000359-Unable to Parse Input Record
CGW001000-Batch Track ID Invalid
CGW001001-Batch Received Time Invalid
CGW001002-Batch Input File Invalid
CGW001003-Batch Output File Invalid
CGW001004-Batch Status Invalid
CGW001005-Total Transaction Count Invalid
CGW001006-Processing Start Time Invalid
CGW001007-Processing Completion Time Invalid
CGW001008-Processed Transaction Count Invalid
CGW001012-Start Range Invalid
CGW001013-Start Range Missing
CGW001014-Processing Transaction Count Invalid
CGW001015-Suspend Command Invalid
CGW000367-Batch In Use

CT00001-Expired Session
CT00002-Session Timeout format error

Appendice D - Certification Authority Riconosciute

Il Payment Gateway attualmente può inviare messaggi con protocollo HTTPS verso i server dei merchants il cui certificato SSL è stato emesso da una delle seguenti Certification Authority:

ThawtePremium CA
Creation date: 9-gen-2006
Owner: CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc,
Issuer: CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc
Serial number: 1
Valid from Thu Aug 01 02:00:00 CEST 1996 until Fri Jan 01 00:59:59 CET 2021
Certificate fingerprints:
MD5: 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
SHA1: 62:7F:8D:78:27:65:63:99:D2:7D:7F:90:44:C9:FE:B3:F3:3E:FA:9A

****

Thawte CA
Creation date: 3-feb-2004
Owner: CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc
Issuer: CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc
Serial number: 1
Valid from Thu Aug 01 02:00:00 CEST 1996 until Fri Jan 01 00:59:59 CET 2021
Certificate fingerprints:
MD5: C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
SHA1: 23:E5:94:94:51:95:F2:41:48:03:B4:D5:64:D2:A3:A3:F5:D8:8B:8C

****

Infocamere 2
Creation date: 19-mag-2006
Owner: CN=InfoCamere Servizi di Certificazione 2, OU=Ente Certificatore del Sistema Camerale, O=InfoCamere SCpA, C=IT
Issuer: CN=InfoCamere Servizi di Certificazione 2, OU=Ente Certificatore del Sistema Camerale, O=InfoCamere SCpA, C=IT
Serial number: 1
Valid from Wed Mar 24 17:03:18 CET 2004 until Thu Mar 24 17:02:29 CET 2016
Certificate fingerprints:
MD5: E0:A3:9F:CB:B4:C7:0E:E7:F1:13:EB:AC:8A:C0:DE:17
SHA1: 7E:4C:1C:F8:FF:38:8D:9F:51:89:73:86:47:79:BD:F5:5C:ED:18:A6

****

Infocamere
Creation date: 3-feb-2004
Owner: CN=InfoCamere Servizi di Certificazione, OU=Ente Certificatore del Sistema Camerale, O=InfoCamere SCpA, C=IT
Issuer: CN=InfoCamere Servizi di Certificazione, OU=Ente Certificatore del Sistema Camerale, O=InfoCamere SCpA, C=IT
Serial number: 1c
Valid from Tue Jan 16 10:17:00 CET 2001 until Mon Jan 17 00:59:00 CET 2011
Certificate fingerprints:
MD5: 8C:0A:E8:00:D8:22:3C:38:DF:33:CC:B9:7B:7E:A0:A1
SHA1: DC:58:3E:76:06:46:BC:5C:CD:2B:8A:28:CF:7A:87:13:38:03:8B:C9

****

Equifax Global CA
Creation date: 5-ott-2006
Owner: CN=Equifax Secure Global eBusiness CA-1, O=Equifax Secure Inc., C=US
Issuer: CN=Equifax Secure Global eBusiness CA-1, O=Equifax Secure Inc., C=US
Serial number: 1
Valid from Mon Jun 21 06:00:00 CEST 1999 until Sun Jun 21 06:00:00 CEST 2020
Certificate fingerprints:
MD5: 8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC
SHA1: 7E:78:4A:10:1C:82:65:CC:2D:E1:F1:6D:47:B4:40:CA:D9:0A:19:45

****

Equifax CA
Creation date: 27-gen-2004
Owner: OU=Equifax Secure Certificate Authority, O=Equifax, C=US
Issuer: OU=Equifax Secure Certificate Authority, O=Equifax, C=US
Serial number: 35def4cf
Valid from Sat Aug 22 18:41:51 CEST 1998 until Wed Aug 22 18:41:51 CEST 2018
Certificate fingerprints:
MD5: 67:CB:9D:C0:13:24:8A:82:9B:B2:17:1E:D1:1B:EC:D4
SHA1: D2:32:09:AD:23:D3:14:23:21:74:E4:0D:7F:9D:62:13:97:86:63:3A

****

Verisign
Creation date: 3-feb-2004
Owner: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Serial number: 70bae41d10d92934b638ca7b03ccbabf
Valid from Mon Jan 29 01:00:00 CET 1996 until Wed Aug 02 01:59:59 CEST 2028
Certificate fingerprints:
MD5: 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
SHA1: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

****

Verisign
Creation date: 8-lug-2005
Owner: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Issuer: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Serial number: 7dd9fe07cfa81eb7107967fba78934c6
Valid from Mon May 18 02:00:00 CEST 1998 until Wed Aug 02 01:59:59 CEST 2028
Certificate fingerprints:
MD5: A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
SHA1: 85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F

****

Verisign Intermediate CA
Creation date: 3-feb-2004
Owner: OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSign International Server CA - Class 3, OU="VeriSign, Inc.", O=VeriSign Trust Network
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Serial number: 78ee48de185b2071c9c9c3b51d7bddc1
Valid from Thu Apr 17 02:00:00 CEST 1997 until Tue Oct 25 01:59:59 CEST 2011
Certificate fingerprints:
MD5: 81:C8:88:53:0A:FC:AD:91:6F:BE:71:D9:41:7B:F1:0C
SHA1: DE:0F:3A:63:CA:D1:38:41:E9:B6:2C:94:50:2C:B1:89:D7:66:1E:49

****

Verisign per MasterCard
Creation date: 4-feb-2004
Owner: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Serial number: 2ad667e4e45fe5e576f3c98195eddc0
Valid from Wed Nov 09 01:00:00 CET 1994 until Fri Jan 08 00:59:59 CET 2010
Certificate fingerprints:
MD5: 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
SHA1: 44:63:C5:31:D7:CC:C1:00:67:94:61:2B:B6:56:D3:BF:82:57:84:6F

****

Visa eRoot
Creation date: 15-mar-2005
Owner: CN=Visa eCommerce Root, OU=Visa International Service Association, O=VISA, C=US
Issuer: CN=Visa eCommerce Root, OU=Visa International Service Association, O=VISA, C=US
Serial number: 1386354d1d3f06f2c1f96505d5901c62
Valid from Wed Jun 26 04:18:36 CEST 2002 until Fri Jun 24 02:16:12 CEST 2022
Certificate fingerprints:
MD5: FC:11:B8:D8:08:93:30:00:6D:23:F9:7E:EB:52:1E:02
SHA1: 70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62

****

Visa GP Root
Creation date: 23-dic-2002
Owner: CN=GP Root 2, OU=Visa International Service Association, O=VISA, C=US
Issuer: CN=GP Root 2, OU=Visa International Service Association, O=VISA, C=US
Serial number: 31e
Valid from Thu Aug 17 00:51:00 CEST 2000 until Sun Aug 16 01:59:00 CEST 2020
Certificate fingerprints:
MD5: 35:48:95:36:4A:54:5A:72:96:8E:E0:64:CC:EF:2C:8C
SHA1: C9:0D:1B:EA:88:3D:A7:D1:17:BE:3B:79:F4:21:0E:1A:58:94:A7:2D

****

Visa Intermediate CA
Creation date: 15-mar-2005
Owner: CN=e-Visa, OU=Visa International Service Associations, O=VISA, C=US
Issuer: CN=Visa eCommerce Root, OU=Visa International Service Association, O=VISA, C=US
Serial number: afcd07d6289db09bc1b60caddfb9340c
Valid from Thu Jul 01 20:07:28 CEST 2004 until Mon Jun 30 20:07:28 CEST 2014
Certificate fingerprints:
MD5: FD:8D:A9:63:ED:0C:B8:62:1F:54:4A:09:49:3C:0F:76
SHA1: B5:2A:51:72:61:11:6E:03:3B:6D:E9:48:36:C8:51:8F:A9:6A:1F:B6

****

Visa PIT
Creation date: 9-ott-2006
Owner: CN=pit-root, OU=PIT, O=Caradas, C=US
Issuer: CN=pit-root, OU=PIT, O=Caradas, C=US
Serial number: 2cbb12b8d6f9c09d0027732412a69525ee1acab6
Valid from Fri May 07 18:23:50 CEST 2004 until Mon May 05 18:23:50 CEST 2014
Certificate fingerprints:
MD5: 5C:E9:8F:83:24:7E:64:94:87:54:BE:F3:96:E8:38:FC
SHA1: 28:E4:AC:FD:4E:FF:6A:27:26:5C:97:2B:88:A7:1B:0E:86:8A:C5:D3

****

Starfield
Creation date: 4-giu-2007
Owner: EMAILADDRESS=practices@starfieldtech.com, CN=Starfield Secure Certification Authority, OU=http://www.starfieldtech.com/repository, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US
Issuer: EMAILADDRESS=info@valicert.com, CN=http://www.valicert.com/, OU=ValiCert Class 2 Policy Validation Authority, O="ValiCert, Inc.", L=ValiCert Validation Network
Serial number: 104
Valid from Wed Jan 14 22:05:21 CET 2004 until Tue Jan 09 22:05:21 CET 2024
Certificate fingerprints:
MD5: 7A:A5:BA:4F:BC:0A:C5:3C:56:E9:50:A0:13:6A:88:A9
SHA1: 44:6A:2A:00:C1:BB:A3:6D:59:D1:C1:78:A6:7A:27:C5:0E:6D:03:DF

****

Globalsign
Creation date: 19-feb-2007
Owner: CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2
Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2
Serial number: 400000000010f8626e60d
Valid from Fri Dec 15 09:00:00 CET 2006 until Wed Dec 15 09:00:00 CET 2021
Certificate fingerprints:
MD5: 94:14:77:7E:3E:5E:FD:8F:30:BD:41:B0:CF:E7:D0:30
SHA1: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE

****

Globalsign Root
Creation date: 19-feb-2007
Owner: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Issuer: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
Serial number: 20000000000d678b79405
Valid from Tue Sep 01 14:00:00 CEST 1998 until Tue Jan 28 13:00:00 CET 2014
Certificate fingerprints:
MD5: AB:BF:EA:E3:6B:29:A6:CC:A6:78:35:99:EF:AD:2B:80
SHA1: 2F:17:3F:7D:E9:96:67:AF:A5:7A:F8:0A:A2:D1:B1:2F:AC:83:03:38

****

Valicert
Creation date: 4-giu-2007
Owner: EMAILADDRESS=info@valicert.com, CN=http://www.valicert.com/, OU=ValiCert Class 2 Policy Validation Authority, O="ValiCert, Inc.", L=ValiCert Validation Network
Issuer: EMAILADDRESS=info@valicert.com, CN=http://www.valicert.com/, OU=ValiCert Class 2 Policy Validation Authority, O="ValiCert, Inc.", L=ValiCert Validation Network
Serial number: 1
Valid from Sat Jun 26 02:19:54 CEST 1999 until Wed Jun 26 02:19:54 CEST 2019
Certificate fingerprints:
MD5: A9:23:75:9B:BA:49:36:6E:31:C2:DB:F2:E7:66:BA:87
SHA1: 31:7A:2A:D0:7F:2B:33:5E:F5:A1:C3:4E:4B:57:E8:B7:D8:F1:FC:A6

****

MasterCard
Creation date: 4-feb-2004
Owner: CN=MasterCard SecureCode Test Root, O=MasterCard International Incorporated Test System, C=US
Issuer: CN=MasterCard SecureCode Test Root, O=MasterCard International Incorporated Test System, C=US
Serial number: 3d86dd48
Valid from Tue Sep 17 09:46:46 CEST 2002 until Fri Sep 14 08:46:46 CEST 2012
Certificate fingerprints:
MD5: 91:A1:6F:94:75:C1:A5:DA:87:DD:23:2C:13:40:C4:60
SHA1: 3A:9B:2A:86:85:9C:AE:F1:9B:4D:CF:D0:29:8D:61:45:07:54:A1:54

****

UTN
Creation date: 26-ott-2006
Owner: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Issuer: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Serial number: 44be0c8b500024b411d3362afe650afd
Valid from Fri Jul 09 20:10:42 CEST 1999 until Tue Jul 09 20:19:22 CEST 2019
Certificate fingerprints:
MD5: 4C:56:41:E5:0D:BB:2B:E8:CA:A3:ED:18:08:AD:43:39
SHA1: 04:83:ED:33:99:AC:36:08:05:87:22:ED:BC:5E:46:00:E3:BE:F9:D7

****

UTN Subordinate CA
Creation date: 26-ott-2006
Owner: CN=Network Solutions Certificate Authority, O=Network Solutions L.L.C., C=US
Issuer: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Serial number: 10e776e8a65a6e377e050306d43c25ea
Valid from Mon Apr 10 02:00:00 CEST 2006 until Sat May 30 12:48:38 CEST 2020
Certificate fingerprints:
MD5: F9:11:12:B1:6A:5C:B1:0B:5E:AD:56:A9:AC:C4:06:33
SHA1: D6:C1:D1:45:29:E2:62:30:69:FD:DE:A6:0C:0F:F6:88:43:29:9C:4A

Appendice E – Certificato CA dell'ambiente di test

Nel caso di utilizzo dell'ambiente di test in modalità SSL, in alcuni sistemi ed ambienti applicativi, è necessario preventivamente inserire il certificato della CA utilizzata per l'emissione del certificato SSL all'interno del repository delle CA attendibili.

Il certificato in formato PEM è il seguente:

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIBADANBgkqhkiG9w0BAQQFADCBjDELMAkGA1UEBhMCSVQx
DzANBgNVBAcTBlBhZG92YTEPMA0GA1UECxMGQ1RWIENBMSMwIQYDVQQKExpDb25z
b3J6aW8gVHJpdmVuZXRvIFMucC5BLjEPMA0GA1UEAxMGQ1RWIENBMSUwIwYJKoZI
hvcNAQkBFhZlLWNvbW1lcmNlQGNvbnN0cml2Lml0MB4XDTA1MTIxMjA5MTYwNFoX
DTE1MTIxMDA5MTYwNFowgYwxCzAJBgNVBAYTAklUMQ8wDQYDVQQHEwZQYWRvdmEx
DzANBgNVBAsTBkNUViBDQTEjMCEGA1UEChMaQ29uc29yemlvIFRyaXZlbmV0byBT
LnAuQS4xDzANBgNVBAMTBkNUViBDQTElMCMGCSqGSIb3DQEJARYWZS1jb21tZXJj
ZUBjb25zdHJpdi5pdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1KM117XS
TThcO5P0+tNTiEmjp/O8cKnYiPKmZae8Ggfc/0cYBFoZhqlfBAEgy3cwHYA3ymYk
PoYKrCkDoCs6/1VMtIizexXIoX64CbORlrJKmPXoBjQX5heXrV4hyD5RrHRjVsR/
dHqoeSp1Crf3aKwX510lFA9qa1f3zAIfZ4UCAwEAAaOB7DCB6TAdBgNVHQ4EFgQU
COIc93lgG6MGlB9UIzWPM4g1mQEwgbkGA1UdIwSBsTCBroAUCOIc93lgG6MGlB9U
IzWPM4g1mQGhgZKkgY8wgYwxCzAJBgNVBAYTAklUMQ8wDQYDVQQHEwZQYWRvdmEx
DzANBgNVBAsTBkNUViBDQTEjMCEGA1UEChMaQ29uc29yemlvIFRyaXZlbmV0byBT
LnAuQS4xDzANBgNVBAMTBkNUViBDQTElMCMGCSqGSIb3DQEJARYWZS1jb21tZXJj
ZUBjb25zdHJpdi5pdIIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GB
AHXpciEHNuszpwK8Gq0L7FDlilXVbaXF56oOgDKTL71o+lAhKvVawW6Cb3IVskzt
w8wh1wOeuQrNYbXZR2tiEfnUHGnl7si0UeugfEwnDxe4wtO3vgeaSowWu3YuC37t
Y7l6a1UBVPrm9/c2gWOIVtS7e00axa7wVGxpdugNFflg
-----END CERTIFICATE-----
```