

Emesso da: CartaSi S.p.A.
Area ICT

Versione: 007
Emesso il: 30/04/2010

Procedura d'adesione e utilizzo del servizio

INDICE

1. Modifiche apportate	4
1.1. Premessa	7
2. Introduzione	9
3. POS virtuale	9
4. E-commerce versione Front Office	11
4.1. Processo di pagamento esercenti E-COMMERCE - versione FULL	12
4.1.1. Definizione e apertura dell'ordine	14
4.1.2. Fase di pagamento e notifica dell'esito	15
4.2. Processo di pagamento esercenti E-COMMERCE versione LIGHT	16
4.2.1. Apertura dell'ordine	17
4.2.2. Fase di pagamento e notifica dell'esito	18
5. E-COMMERCE opzione server to server	19
5.1. Richiesta di pagamento	22
5.2. Autenticazione del titolare	23
5.3. Fase di pagamento e notifica dell'esito	24
6. MOTO opzione server to server	25
6.1. Richiesta di pagamento	26
6.2. Fase di pagamento e notifica dell'esito	26
7. MOTO opzione Back Office	27
8. Funzioni di Back Office	27
9. Attivazione del servizio	29
10. Struttura dei messaggi	30
10.1. Inoltro dei messaggi	30
10.2. Firma messaggi	31
10.3. Integrazione tramite Front Office	33
10.3.1. Formato del messaggio VPOSReqFull	33
10.3.2. Formato del messaggio VPOSRes Full	38
10.3.3. Formato del messaggio VPOSStart	39
10.3.4. Formato del messaggio VPOSReqLight	42

10.3.5.	Formato del messaggio VPOSNotification	49
10.3.6.	Formato del messaggio VPOSNotificationRes	58
10.3.7.	Formato del messaggio VPOSRes Light	59
10.4.	Integrazione tramite messaggi server to server	61
10.4.1.	Formato del messaggio AReq	62
10.4.2.	Formato del messaggio AuthRes	67
10.4.3.	Formato del messaggio ARes	69
10.4.4.	Formato del messaggio AResAck	77
10.4.5.	Formato del messaggio DCCReq	78
10.4.6.	Formato del messaggio DCCRes	79
10.5.	Integrazione messaggi server to server per esercenti che usano un proprio MPI	82
10.5.1.	Formato del messaggio AuthOnlyReq	84
10.5.2.	Formato del messaggio AuthOnlyRes	89
10.6.	Operazioni dispositive e di interrogazione	93
10.6.1.	Formato del messaggio EReq	93
10.6.2.	Formato del messaggio ECRes	97
10.6.3.	Formato del messaggio IntReq	100
10.6.4.	Formato del messaggio IntRes	101
APPENDICE A.....	109
A1 Carte accettate	109
A2 Tipi di transazioni	109
A3 Codici Divisa	110
A4 Lingue supportate	110

1. Modifiche apportate

Versione	Data	Autore	Capitolo	Descrizione
07	30/04/2010	ICT	1.1	Aggiunto riferimento ai servizi aggiuntivi di sicurezza AMEX
			3	Aggiunto riferimento a lista certificati SSL supportati
			10.3.5	Modificato messaggio VPosNotification per servizio DCC e per le informazioni di sicurezza AMEX
			10.4.1	Modificato messaggio AReq per il servizio DCC e aggiornato le specifiche per campi non obbligatori
			10.4.3	Aggiunti codici di risposta in ARes e i riferimenti alle informazioni relative ai servizi aggiuntivi di sicurezza AMEX
			10.4.5	Inseriti nuovi messaggi
			10.4.6	DCCReq e DCCRes per il nuovo servizio DCC (Dynamic Currency Conversion)
			10.5.1	Aggiornate le specifiche sul campo CVV2
			Appendice A2	Eliminato valore M.O.T.O.

06	29/01/2008	ICT	1.1	Inserita descrizione nuove funzionalità
			10.5	Reinserito capitolo 10.5 della vers.002
			A4	Aggiunte nuove lingue supportate(FRA-ESP-DEU)
			10.3.3 10.3.4 10.3.5 10.4.1 10.4.3	Modifiche relative all'introduzione della LIABILITY_SHIFT
			10.6.4	Errore nella richiesta (INTReq): Campo ID_OP duplicato (I casi "FA"e"RA" non si considerano)
005	21/01/2008		10.5.1 10.5.2 10.5.3 10.5.4	Variazione specifiche parametri e descrizione messaggio
005	21/01/2008		10.4.3 10.4.1	Variazione specifiche parametri e descrizione messaggio
005	21/01/2008		10.3.7	Aggiunta messaggio Error_url
005	21/01/2008		10.3.4 10.3.2 10.3.1	Variazione specifiche parametri
005	21/01/2008		10.2 9 4.2.1 4 3	Variazione testo
005	21/01/2008		2	Variazione mail
004	26/07/2006	ICT	10.3.4	Modificato valore parametro ACTION_CODE da AUT_CONT a AUT-CONT
003	20/02/2006	ICT		Eliminato capito 10.5

002	01/02/2006	ICT	10.5	Inserito nuovo msg server to server per esercenti che usano un proprio MPI
002	01/02/2006	ICT	10.6.4	Modificato tag da <RESPONSE> a <RESULT> nell'esempio dell'XML IntRes ed introdotto esempio XML per msg IntRes con esito negativo.
002	01/02/2006	ICT	10.6.1	Modificato tipo e lunghezza del campo ID_OP nel messaggio ECReq
002	01/02/2006	ICT	10.6.2	Modificato tipo e lunghezza del campo ID_OP nel messaggio ECRes
002	01/02/2006	ICT	10.6.3	Modificato tipo e lunghezza del campo ID_OP nel messaggio IntReq
002	01/02/2006	ICT	10.6.4	Modificato tipo e lunghezza del campo ID_OP nel messaggio IntRes

1.1. Premessa

La piattaforma di pagamento è stata aggiornata aumentando il livello di affidabilità e sicurezza inserendo alcune nuove funzionalità a disposizione degli esercenti: i servizi aggiuntivi di sicurezza e il servizio multilingua.

Servizi aggiuntivi di sicurezza VISA e MASTERCARD

Tale funzionalità fornisce agli esercenti informazioni più dettagliate circa la carta che effettua il pagamento, al fine di dare gli strumenti necessari per supportare eventuali politiche di gestione delle frodi.

Le informazioni fornite per ogni transazione sono le seguenti:

- tipologia della carta (consumer o commercial)
- provenienza della carta (area e nazione)
- per gli esercenti e-commerce certificati 3D Secure, l'appartenenza della transazione ad una delle eccezioni alla liability shift previste dai circuiti internazionali Visa e Mastercard.

Si ricorda che gli esercenti e-commerce certificati 3D Secure sono esonerati da qualsiasi responsabilità in caso di disconoscimento integrale della transazione, ad eccezione di alcuni casi espressamente previsti dai circuiti internazionali Visa e Mastercard (si veda il documento "Verified by Visa e Mastercard Secure Code - Istruzioni e regole" allegato al contratto di convenzionamento). Il nuovo servizio di X-Pay consente di visualizzare le transazioni che sicuramente rappresentano eccezioni alla policy dei circuiti. Si segnala tuttavia che, per motivi tecnici, non è possibile garantire che su tutte le transazioni non segnalate come eccezioni, ci sia effettivamente l'esonero dalla responsabilità in caso di disconoscimento (il numero di tali transazioni è tuttavia del tutto residuale sul totale delle operazioni gestite).

Si evidenzia inoltre che tali informazioni, al di là dell'utilizzo per la gestione delle frodi, non potranno essere utilizzate come elemento discriminante la vendita per non violare le regole dei circuiti internazionali

Le informazioni elencate sono rese disponibili nei seguenti modi:

- tramite back office (tipologia e provenienza della carta sono visualizzati nella maschera di dettaglio delle transazioni, mentre per gli esercenti e-commerce 3D Secure l'indicazione di eccezione liability è visualizzata sia nella maschera di dettaglio sia nella pagina di riepilogo ordini);

- elettronicamente tramite risposta al messaggio di richiesta autorizzazione, secondo le istruzioni riportate per ciascuna modalità di integrazione.

Servizi aggiuntivi di sicurezza American Express

Tale funzionalità fornisce all'esercente l'informazione relativa alla provenienza della carta AMEX (nazione).

L'informazione è resa disponibile nei seguenti modi:

- tramite back office (nella maschera di dettaglio delle transazioni);
- tramite risposta al messaggio di richiesta autorizzazione, secondo le istruzioni riportate per ciascuna modalità di integrazione.

Servizio multilingua

Il servizio consente di scegliere la lingua (inglese, francese, spagnolo o tedesco) in cui:

- visualizzare il back office X-Pay;
- nel caso di vendite e-commerce, proporre al Titolare le pagine di pagamento e inviare l'e-mail di conferma ordine.

Servizio DCC

Il servizio consente agli esercenti di offrire il pagamento nella divisa del Paese di emissione della carta.

Il servizio DCC può essere offerto per le seguenti divise:

- Dollaro USA
- Dollaro australiano
- Dollaro canadese
- Dollaro di Hong Kong
- Franco svizzero
- Yen
- Sterlina

2. Introduzione

Il presente Allegato descrive le procedure di adesione ed utilizzo del servizio di POS Virtuale, di seguito X-Pay, erogato da CartaSi. In particolare, vengono illustrate le caratteristiche del sistema, le modalità di attivazione del servizio e le istruzioni tecniche necessarie per effettuare l'integrazione fra il canale di vendita dell'esercente ed X-PAY.

CartaSi si riserva la facoltà di modificare il presente documento, dando visione delle successive versioni sul Portale Esercenti all'Indirizzo Internet www.cartasi.it.

Per qualsiasi informazione aggiuntiva o problema riguardante i contenuti del presente documento e successive versioni, nonché per acquisire le chiavi d'accesso al Back Office, l'esercente potrà usufruire del servizio di assistenza al numero verde esercenti di CartaSi 800.15.19.19 e al seguente indirizzo e-mail: vpos@si-servizi.it

3. POS virtuale

Il sistema X-PAY fornisce ai merchant, una piattaforma che permette di accettare e gestire in modo facile e sicuro i pagamenti effettuati con carta di credito attraverso vendite **e-commerce** e **MOTO** (Mail order - Telephon order).

Gli esercenti **E-COMMERCE** possono utilizzare le seguenti opzioni:

1. **Front Office:** Questa modalità prevede che, al momento del pagamento, il titolare venga re-indirizzato sulla piattaforma X-PAY che gestirà l'intero processo di pagamento, dalla raccolta dei dati della carta di credito all'inoltro ai circuiti internazionali fino alla comunicazione dell'esito del pagamento all'esercente ed al titolare. Tale soluzione consente la gestione in modalità sicura di tutte le fasi della transazione permettendo all'esercente di non dover gestire dati sensibili. La piattaforma risulta dotata di un certificato SSL (Secure Sockets Layer) 128 bit, è in grado di accettare sia pagamenti in modalità SSL, tramite re-direzione del compratore su server sicuro, sia nella modalità Verified by Visa/SecureCode secondo gli standard di sicurezza previsti da parte dei circuiti internazionali (VISA e MasterCard). Tale opzione d'integrazione è a sua volta disponibile in 2 versioni (FULL e LIGHT).

L'esercente avrà un accesso al portale www.cartasi.it per la gestione (incassi, storni, report, ecc...) dei pagamenti ricevuti.

2. **Server to server:** questa modalità prevede che il processo di comunicazione con il titolare sia gestito dall'applicazione dell'esercente che raccoglie i dati della carta di credito dell'acquirente e gestisce la richiesta di pagamento verso la piattaforma X-PAY tramite messaggi server to server per l'intero ciclo dell'ordine. Anche questa soluzione è in grado di accettare pagamenti in modalità SSL oppure Verified by Visa/SecureCode. L'esercente avrà un accesso al portale www.cartasi.it per la sola visualizzazione dei pagamenti ricevuti, la gestione di incassi, storni, ecc... sarà gestita sempre tramite messaggi server to server.

A seguito della certificazione PCI per la qualità, si sono introdotte restrizioni riguardanti i certificati SSL supportati dalla piattaforma.

Una lista completa è disponibile nel documento 'Lista certificati supportati XPay 99-8.doc' allegato a questo documento.

I protocolli di sicurezza Verified by Visa/SecureCode assicurano una maggiore tutela sugli acquisti in Internet in quanto richiedono l'autenticazione del titolare della carta di credito per poter effettuare un pagamento.

Quando l'ente emittente della carta di credito (Issuer) aderisce ai protocolli Verified by Visa/Secure Code attribuisce a tutti o ad una parte dei propri titolari un dato (tipicamente una password personale) che consentirà di verificarne con sicurezza l'identità. Questo dato gli sarà richiesto durante ogni acquisto effettuato presso un esercente aderente agli stessi protocolli di sicurezza. Durante il pagamento quindi, se il titolare è registrato al servizio Verified by Visa/Secure Code, dovrà essere rediretto verso un'applicazione del proprio Issuer in cui dovrà fornire il dato necessario alla sua autenticazione. L'esito di tale autenticazione sarà quindi restituito alla piattaforma di e-commerce che lo ha richiesto. In caso di esito positivo la transazione potrà essere conclusa, viceversa in caso di esito negativo la transazione non potrà essere conclusa e l'acquirente dovrà indicare un'altra carta di credito o un'altra modalità di pagamento per poter concludere l'acquisto.

Per gli **esercenti MOTO** il sistema dispone delle seguenti opzioni:

1. **Back Office:** questa modalità prevede che l'esercente si registri al Portale Esercenti (PE) e gestisca le transazioni MOTO (dalla presa in carico dell'ordine fino alla contabilizzazione)

utilizzando tutte le funzionalità messe a disposizione dall'applicativo di Back Office della piattaforma X-PAY.

2. **Server to server:** Le chiamate server to server sono rese disponibili sotto forma di una web application che accetta chiamate POST HTTPS di messaggi XML generati da una applicazione merchant. Tramite questo meccanismo l'esercente effettua le operazioni di richiesta autorizzazione, storno di un pagamento, contabilizzazione di una transazione autorizzata, storno di una transazione precedentemente autorizzata, verifica dello stato di una transazione e interrogazione dei movimenti effettuati da un merchant in un certo periodo, etc. Per quanto riguarda la sicurezza della tratta di comunicazione Internet il grado di affidabilità offerto è quello del protocollo SSL con cifratura a 128 bit.

Per tutti gli esercenti **e-commerce** e **MOTO** è disponibile una funzionalità di **Back Office**, nella quale è possibile fruire di servizi informativi e dispositivi (solo per versione Back Office), accessibile attraverso il PE mediante le chiavi di sicurezza (nome utente e password) fornite da CartaSi.

4. E-commerce versione Front Office

Rappresenta una delle modalità di integrazione possibili al sistema X-PAY in cui l'esercente (E-COMMERCE) delega la gestione della raccolta dati della carta di credito e quindi la comunicazione con l'acquirente al front end messo a disposizione dalla piattaforma X-PAY.

Il processo di pagamento prevede che l'acquirente acceda, via web, al sito di commercio elettronico dell'esercente e qui scelga il prodotto/i che desidera acquistare. Al momento del pagamento il consumatore viene re-indirizzato sul server sicuro della piattaforma X-PAY, il quale visualizza una pagina di pagamento in cui si riassumono i dati della transazione in corso (es. insegna del negozio ed importo della transazione) e si invita l'acquirente a concludere il pagamento indicando i dati della propria carta di credito. La redirectione del titolare può essere effettuata con 2 distinte modalità:

- **versione FULL**

Al momento del pagamento, l'applicazione dell'esercente apre l'ordine tramite la piattaforma X-PAY comunicando i dati della transazione in corso tramite una chiamata server to server e ne riceve un identificativo univoco (TRANSACTION_ID), quindi redireziona il browser dell'acquirente sulla pagina di pagamento X-PAY inoltrando l'identificativo ricevuto.

- **versione LIGHT**

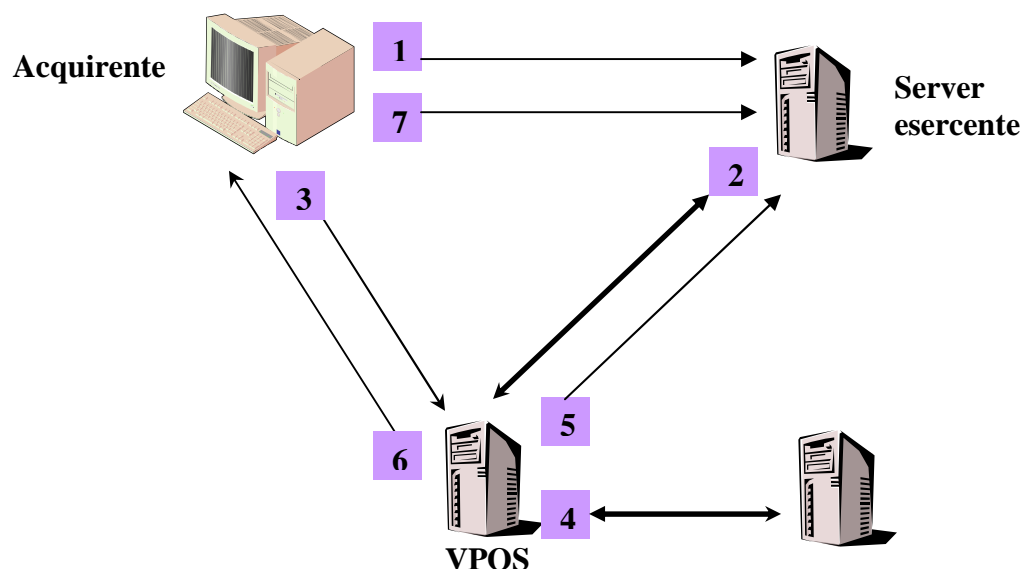
Al momento del pagamento l'acquirente viene direttamente rediretto sulla pagina di pagamento X-PAY CartaSi inoltrando tramite il proprio browser i dati relativi alla transazione in corso.

Al momento dell'adesione alla piattaforma X-PAY, l'esercente può decidere la modalità d'integrazione che preferisce; la differenza tra la versione FULL e la versione LIGHT riguarda esclusivamente la procedura da seguire per l'apertura dell'ordine, il processo di pagamento dopo la visualizzazione della pagina di pagamento è identico per entrambe le versioni.

Una volta inseriti dall'acquirente nella pagina di pagamento, i dati della carta di credito viaggiano su canale sicuro fino alla piattaforma X-PAY, che li usa per chiedere l'autorizzazione al pagamento sui normali circuiti autorizzativi. L'esito del pagamento viene infine comunicato all'esercente con messaggio di notifica in seguito descritto e all'acquirente tramite e-mail.

4.1. Processo di pagamento esercenti E-COMMERCE - versione FULL

Il seguente diagramma riassume le varie fasi in cui è suddiviso il processo di pagamento se l'esercente opta per la versione FULL del protocollo d'integrazione tramite Front End:



1. **Definizione dell'ordine:** l'acquirente "navigando" nel negozio virtuale dell'Esercente sceglie il/i prodotto/i da acquistare (riempiendo il "carrello"), definisce l'ordine di acquisto e decide di procedere con il pagamento.
2. **Apertura dell'ordine:** il server dell'esercente invia al server X-PAY una richiesta di pagamento (VPOSReqFull) contenente tutti i dati relativi all'acquisto. X-PAY verifica la validità del chiamante e dei dati del messaggio VPOSReqFull, attribuisce all'ordine in corso un identificativo univoco (TRANSACTION_ID) e lo comunica all'esercente insieme all'URL al quale redirigere l'acquirente.
3. **Pagina di pagamento:** Ottenuta risposta da X-PAY al messaggio VPOSReqFull, il server dell'esercente redireziona l'acquirente sulla pagina di inserimento dei dati della carta di credito VPPP (X-PAY Payment Page) inoltrando il messaggio VPOSStart, che non contiene i dati della transazione ma l'identificativo univoco restituito da X-PAY. L'acquirente deve quindi inserire i dati della carta di credito che intende utilizzare per il pagamento.
4. **Pagamento:** X-PAY effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta. Nel corso di questa fase avviene anche l'eventuale autenticazione a cui è soggetto il titolare se ha aderito ad un sistema di sicurezza (Verified by Visa o Secure Code) a condizione che l'esercente su cui sta effettuando il pagamento abbia aderito allo stesso protocollo.
5. **Notifica dell'esito all'esercente:** Se la richiesta di pagamento si conclude positivamente, il sistema X-PAY comunica all'esercente, mediante il messaggio VPOSNotification, l'esito della richiesta di autorizzazione in modo da consentirgli di procedere con l'ordine.
6. **Notifica dell'esito al titolare:** il sistema X-PAY comunica l'esito della transazione all'acquirente mediante una pagina ed un' e-mail contenente lo scontrino "virtuale" dell'acquisto avvenuto, quindi indirizza nuovamente il browser del titolare sul server dell'esercente.
7. **Ritorno al sito dell'esercente:** Il browser del titolare richiama la pagina di risposta realizzata dall'esercente.

Nei paragrafi successivi sono descritte più dettagliatamente le varie fasi del processo di pagamento.

4.1.1. Definizione e apertura dell'ordine

Quando l'acquirente, dopo aver scelto il prodotto/servizio dal catalogo dell'esercente, decide di procedere con il pagamento, il sistema dell'esercente deve inviare tramite una chiamata server to server il messaggio VPOSReqFull di richiesta di una nuova transazione al sistema X-PAY. In tale messaggio vengono comunicati in modalità sicura i parametri relativi al pagamento da effettuare tra cui:

- Codice identificativo dell'esercente
- Importo e divisa della transazione
- Tipo di transazione, che può assumere i seguenti valori:
 - **"Contabilizzazione implicita"**; a fronte di una autorizzazione alla spesa con esito positivo il sistema X-PAY provvede alla contabilizzazione addebitando la carta di credito dell'acquirente ed accreditando l'esercente.
 - **"Contabilizzazione esplicita"**; a fronte di una autorizzazione alla spesa con esito positivo è l'esercente che in un tempo successivo comunica in modo esplicito al sistema X-PAY di contabilizzare l'operazione, quindi di addebitare la carta di credito dell'acquirente accreditando l'esercente stesso.
- MAC(Codice d'autenticazione del messaggio). Nel processo di comunicazione tra l'esercente ed il sistema X-PAY vi è il rischio che un soggetto estraneo, in grado di intercettare il messaggio, cerchi di alterarne il contenuto, rispedendolo poi al destinatario finale. Questo rischio viene evitato introducendo un processo d'autenticazione tramite la "firma" dei messaggi che vengono trasmessi.
- L'URL che X-PAY deve utilizzare per comunicare all'esercente (tramite una chiamata server to server) l'esito della transazione (NotificationURL)
- L'URL alla quale inviare l'utente in caso di completamento della transazione (ResultURL)
- L'URL alla quale inviare l'utente in caso di annullamento del processo di pagamento e ritorno al negozio di provenienza (AnnulmentURL)
- L'URL alla quale inviare l'utente in caso di problemi nella visualizzazione della pagina di pagamento (errorURL)

La piattaforma X-PAY acquisisce i parametri ed effettua i controlli di identità del chiamante e di correttezza dei dati della transazione; in particolare il codice esercente comunicato deve appartenere ad un esercente abilitato all'utilizzo del sistema X-PAY, il parametro MAC deve essere corretto e l'indirizzo IP del chiamante deve coincidere con uno degli indirizzi IP che l'esercente ha indicato come propri attraverso l'ambiente di Back Office che il sistema X-PAY mette a sua disposizione.

Se i controlli vengono superati, X-PAY restituisce all'esercente un identificativo univoco del pagamento (TRANSACTION_ID) e l'URL della pagina di pagamento al quale deve essere re-indirizzato l'acquirente per effettuare il pagamento dell'acquisto in corso.

4.1.2. Fase di pagamento e notifica dell'esito

Ricevuta la risposta, il sistema dell'esercente deve far generare al browser dell'acquirente un messaggio di avvio del pagamento (VPOSStart) verso l'URL comunicato dal sistema X-PAY inoltrando l'identificativo univoco (TRANSACTION_ID) ricevuto. In caso di errore nel messaggio VPOSStart, X-PAY reindirige l'acquirente all'URL (errorURL) indicato nel messaggio di apertura dell'ordine, altrimenti visualizza all'acquirente la pagina di pagamento.

Da questo istante X-PAY acquisisce il controllo del colloquio con l'acquirente riguardo alla transazione.

Se la transazione si conclude con esito positivo, X-PAY comunica l'esito all'esercente con 2 distinte modalità:

- Tramite una chiamata diretta server to server
Alla ricezione dell'esito positivo della transazione da parte dei circuiti autorizzativi, X-PAY effettua una chiamata all'URL indicato dall'esercente nella chiamata di apertura dell'ordine (NotificationUrl) inoltrando il messaggio VPOSNotification contenente i dati dell'avvenuto pagamento. L'utilizzo di una comunicazione diretta server to server garantisce all'esercente la ricezione dell'esito della transazione indipendentemente dalle azioni dell'acquirente. Inoltre se si dovessero verificare errori di comunicazione durante l'inoltro del messaggio, X-PAY invierà all'esercente un'email di notifica dell'esito della transazione utilizzando l'indirizzo email che l'esercente ha indicato tramite l'ambiente di back office di X-PAY.
- Tramite il browser dell'acquirente
Al termine del pagamento, all'acquirente viene visualizzata una pagina di conferma che riassume i dati essenziali dell'avvenuto pagamento e contiene un link che lo riporta sul sito dell'esercente, all'URL comunicato nel messaggio di apertura dell'ordine (ResultURL). Quando l'acquirente viene

rediretto al negozio di provenienza (ResultURL) viene inoltrata una copia del messaggio VPOSNotification. L'acquirente riceverà inoltre un'e-mail di conferma contenente lo scontrino virtuale del pagamento.

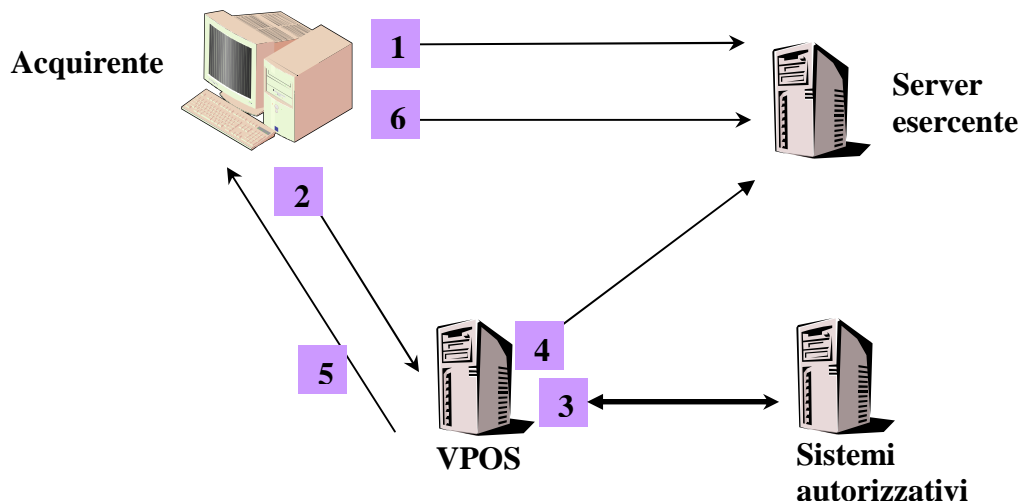
Il messaggio di notifica dell'esito della transazione (VPOSNotification) conterrà tra gli altri i seguenti dati:

- Codice autorizzativo : codice identificativo della autorizzazione assegnato dall'emittente della carta
- Tipo di carta: circuito della carta utilizzata dall'acquirente per il pagamento.
- Tipo di transazione : tipologia di transazione che indica il livello di sicurezza della transazione

Nessuna notifica è prevista se la transazione si conclude con esito negativo.

4.2. Processo di pagamento esercenti E-COMMERCE versione LIGHT

Il seguente diagramma riassume le varie fasi in cui è suddiviso il processo di pagamento se l'esercente opta per la versione LIGHT del protocollo d'integrazione tramite FrontEnd:



1. **Definizione dell'ordine:** l'acquirente "navigando" nel negozio virtuale dell'Esercente sceglie il/i prodotto/i da acquistare (riempiendo il "carrello"), definisce l'ordine di acquisto e decide di procedere con il pagamento.

2. **Pagina di pagamento:** il server dell'esercente redireziona immediatamente il titolare sulla pagina di inserimento dei dati della carta di credito VPPP (X-PAY Payment Page) inoltrando il messaggio VPOSReqLight, contenente tutti i dati della transazione in corso, compreso l'identificativo univoco dell'ordine (TRANSACTION_ID).
3. **Pagamento:** il sistema X-PAY effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta. Nel corso di questa fase avviene anche l'eventuale autenticazione a cui è soggetto il titolare se ha aderito ad un sistema di sicurezza (Verified by Visa o Secure Code) a condizione che l'esercente su cui sta effettuando il pagamento abbia aderito allo stesso protocollo.
4. **Notifica dell'esito all'esercente:** Se la richiesta di pagamento si conclude positivamente, X-PAY comunica all'esercente, mediante il messaggio VPOSNotification, l'esito della richiesta di autorizzazione in modo da consentirgli di procedere con l'ordine.
5. **Notifica dell'esito al titolare:** X-PAY comunica l'esito della transazione al titolare mediante una pagina ed un' e-mail contenente lo scontrino "virtuale" dell'acquisto avvenuto, quindi indirizza nuovamente il browser del titolare sul server dell'esercente.
6. **Ritorno al sito dell'esercente:** Il browser del titolare richiama la pagina di risposta realizzata dall'esercente.

Nel paragrafi successivi sono descritte più dettagliatamente le varie fasi del processo di pagamento.

4.2.1. Apertura dell'ordine

Quando l'acquirente, dopo aver scelto il prodotto/servizio dal catalogo dell'esercente, decide di procedere con il pagamento, il sistema dell'esercente lo redireziona verso la piattaforma X-PAY facendo generare al browser dell'acquirente un messaggio (VPOSReqLight) di richiesta di una nuova transazione. In tale messaggio vengono comunicati in modalità sicura i parametri relativi al pagamento da effettuare tra cui:

- Codice identificativo dell'esercente
- Identificativo univoco dell'ordine
- Importo e divisa della transazione

- Tipo di transazione, che può assumere i seguenti valori:
 - **"Contabilizzazione implicita"**; a fronte di una autorizzazione alla spesa con esito positivo il sistema X-PAY provvede alla contabilizzazione addebitando la carta di credito dell'acquirente ed accreditando l'esercente.
 - **"Contabilizzazione esplicita"**; a fronte di una autorizzazione alla spesa con esito positivo è l'esercente che in un tempo successivo comunica in modo esplicito al sistema X-PAY di contabilizzare l'operazione, quindi di addebitare la carta di credito dell'acquirente accreditando l'esercente stesso.
- MAC(Codice d'autenticazione del messaggio). Nel processo di comunicazione tra l'esercente ed il sistema X-PAY vi è il rischio che un soggetto estraneo, in grado di intercettare il messaggio, cerchi di alterarne il contenuto, rispedendolo poi al destinatario finale. Questo rischio viene evitato introducendo un processo d'autenticazione tramite la "firma" dei messaggi che vengono trasmessi.
- L'URL che X-PAY deve utilizzare per comunicare all'esercente l'esito della transazione (NotificationURL)
- L'URL alla quale inviare l'utente in caso di completamento della transazione (ResultURL)
- L'URL alla quale inviare l'utente in caso di annullamento del processo di pagamento e ritorno al negozio di provenienza (AnnulmentURL)
- L'URL alla quale inviare l'utente in caso di problemi nell'apertura dell'ordine (errorURL)

Il sistema X-PAY acquisisce i parametri ed effettua i controlli di identità del chiamante e di correttezza dei dati della transazione; in particolare il codice esercente X-Pay comunicato deve appartenere ad un esercente abilitato all'utilizzo del sistema X-PAY, il parametro MAC deve essere corretto.

Se i controlli vengono superati, X-PAY visualizza la pagina di pagamento in cui l'acquirente può inserire i dati della carta di credito; in caso contrario X-PAY reindirige l'acquirente all'URL (errorURL) indicato nel messaggio di apertura dell'ordine.

4.2.2. Fase di pagamento e notifica dell'esito

Dal momento in cui viene visualizzata la pagina di pagamento, X-PAY acquisisce il controllo del colloquio con l'acquirente riguardo alla transazione. Sia la fase di pagamento che la notifica dell'esito al titolare ed all'esercente sono identiche a quelle del protocollo versione FULL, quindi, se la transazione si

conclude con esito positivo, X-PAY comunica l'esito all'esercente con 2 distinte modalità:

- Tramite una chiamata diretta server to server
Alla ricezione dell'esito positivo della transazione da parte dei circuiti autorizzativi X-PAY effettua una chiamata all'URL indicato dall'esercente nella chiamata di apertura dell'ordine (NotificationUrl) inoltrando il messaggio VPOSNotification contenente i dati dell'avvenuto pagamento. L'utilizzo di una comunicazione diretta server to server garantisce all'esercente la ricezione dell'esito della transazione indipendentemente dalle azioni dell'acquirente. Inoltre se si dovessero verificare errori di comunicazione durante l'inoltro del messaggio, la piattaforma X-PAY invierà all'esercente un'email di notifica dell'esito della transazione utilizzando l'indirizzo email che l'esercente ha indicato tramite l'ambiente di back office di X-PAY.
- Tramite il browser dell'acquirente
Al termine del pagamento, all'acquirente viene visualizzata una pagina di conferma che riassume i dati essenziali dell'avvenuto pagamento e contiene un link che lo riporta sul sito dell'esercente, all'URL comunicato nel messaggio di apertura dell'ordine (ResultURL). Quando l'acquirente viene rediretto al negozio di provenienza (ResultURL) viene inoltrata una copia del messaggio VPOSNotification. L'acquirente riceverà inoltre un'e-mail di conferma contenente lo scontrino virtuale del pagamento.

Il messaggio di notifica dell'esito della transazione (VPOSNotification) conterrà tra gli altri i seguenti dati:

- Codice autorizzativo : codice identificativo della autorizzazione assegnato dall'emittente della carta
- Tipo di carta: circuito della carta utilizzata dall'acquirente per il pagamento.
- Tipo di transazione : tipologia di transazione che indica il livello di sicurezza della transazione

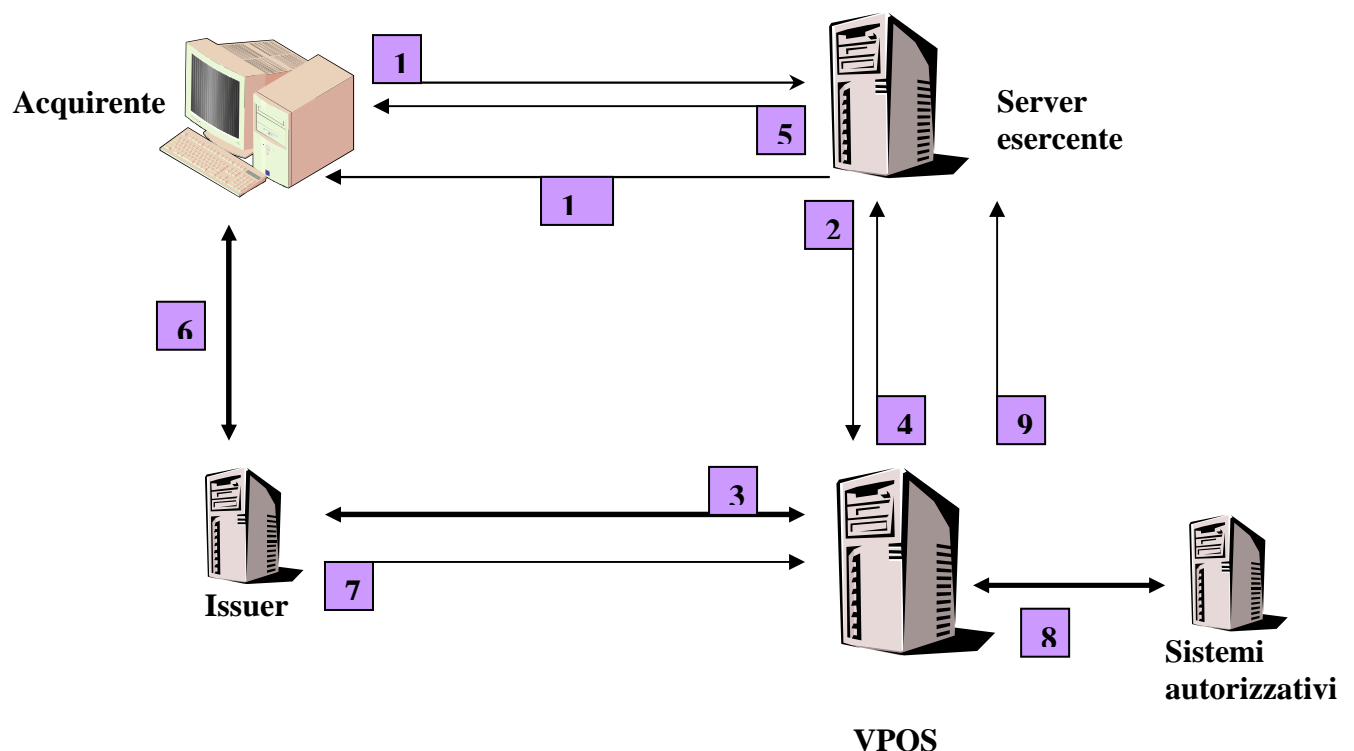
NB: Nessuna notifica è prevista se la transazione si conclude con esito negativo.

5. E-COMMERCE opzione server to server

Questa modalità di integrazione prevede che l'esercente gestisca tramite il proprio negozio virtuale la comunicazione con il titolare, quindi sia la richiesta dei dati della carta di credito che la comunicazione dell'esito del pagamento, ed utilizzi dei messaggi server to server verso la piattaforma X-PAY per richiedere il pagamento dell'ordine e riceverne l'esito.

Processo di pagamento per esercenti Verified by Visa/SecureCode

Il seguente diagramma riassume le varie fasi in cui è suddiviso il processo di pagamento se l'esercente opta per l'integrazione tramite messaggi server to server; il processo di pagamento segue fasi differenti se il titolare aderisce o meno al Verified by Visa/SecureCode. Infatti se il titolare ha aderito al protocollo di sicurezza il processo di pagamento comprende la fase d'autenticazione (steps da 4 a 7) svolta dall'ente emittente della carta di credito (Issuer).



1. **Definizione dell'ordine:** l'acquirente "navigando" nel negozio virtuale dell'Esercente sceglie il/i prodotto/i da acquistare (riempiendo il "carrello"), definisce l'ordine di acquisto e fornisce all'esercente i dati della carta di credito che intende utilizzare per il pagamento.
2. **Richiesta di pagamento:** l'applicazione dell'esercente spedisce i dati del pagamento che intende richiedere alla piattaforma X-PAY inviando tramite una chiamata server to server il messaggio AReq. Il messaggio contiene anche un campo TRANSACTION_ID che identifica univocamente l'ordine.

3. **Verifica dell'adesione al servizio Verified by Visa/SecureCode:** il sistema X-PAY contatta l'ente emittente della carta di credito per verificare se l'acquirente ha aderito o meno ai protocolli di sicurezza. Se l'acquirente non si è registrato al servizio, X-PAY effettua immediatamente il pagamento, quindi il passo successivo sarà lo step 8. Se invece l'acquirente aderisce al servizio Verified by Visa/SecureCode, vengono eseguiti gli steps dal 4 al 7.

Solo per acquirenti aderenti al Verified by Visa/SecureCode:

4. **Restituzione della pagina di redirectione:** X-PAY non inoltra il pagamento in quanto è subordinato all'autenticazione dell'acquirente, ma restituisce all'esercente il messaggio AuthRes contenente il codice di una pagina html che, eseguita dal browser dell'acquirente, lo redireziona verso l'applicazione dell'Issuer che deve verificarne l'identità. Il processo di pagamento si interrompe quindi per consentire l'autenticazione del titolare.
5. **Redirezione dell'acquirente:** l'applicazione dell'esercente restituisce al browser dell'acquirente l'html ricevuto da X-PAY nel messaggio AuthRes.
6. **Autenticazione:** l'acquirente visualizza la pagina dell'Issuer in cui gli viene richiesto il dato necessario per la sua autenticazione(es. password). La fase d'autenticazione del titolare è gestita interamente dall'Issuer che ha emesso la carta di credito.
7. **Notifica dell'esito dell'autenticazione:** l'applicazione dell'Issuer restituisce alla piattaforma X-PAY l'esito della fase d'autenticazione. Se l'acquirente non è stato in grado d'autenticarsi il pagamento non può essere inoltrato, quindi il passo successivo sarà lo step 9; viceversa se l'autenticazione si è conclusa positivamente X-PAY effettuerà il pagamento, quindi il passo successivo sarà lo step 8.
8. **Pagamento :** X-PAY effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta.
9. **Notifica dell'esito all'esercente:** X-PAY comunica l'esito della richiesta di pagamento all'esercente tramite il messaggio ARes.
Se la fase di autenticazione non è avvenuta, il messaggio ARes viene inoltrato in risposta al messaggio AReq, sulla stessa

connessione in cui X-PAY ha ricevuto la richiesta di pagamento.

Viceversa se è avvenuta la fase d'autenticazione e quindi il pagamento si è interrotto per attendere l'esito di tale fase, il messaggio ARes sarà inviato al termine del pagamento (step8) su iniziativa di X-PAY tramite una chiamata server to server all'URL (NotificationUrl) comunicato dall'esercente nel messaggio di apertura ordine. Inoltre in tal caso, al termine del pagamento il sistema X-PAY reindirige il browser del titolare verso il sito dell'esercente, all'URL (ResultUrl) comunicato dall'esercente nel messaggio di apertura ordine.

10. **Notifica dell'esito al titolare:** l'applicativo dell'esercente comunica l'esito del pagamento all'acquirente.

Nel paragrafi successivi sono descritte più dettagliatamente le varie fasi del processo di pagamento.

5.1. Richiesta di pagamento

Quando l'acquirente, dopo aver scelto il prodotto/servizio dal catalogo dell'esercente, decide di procedere con il pagamento ed indica i dati della carta di credito che vuole utilizzare, il sistema dell'esercente deve inviare un messaggio server to server (AReq) di richiesta di una nuova transazione al sistema X-PAY inoltrando tutti i dati relativi alla transazione in corso, compresi i dati della carta di credito richiesti all'acquirente. In tale messaggio vengono comunicati in modalità sicura i parametri relativi al pagamento da effettuare tra cui:

- Codice identificativo dell'esercente
- Identificativo dell'ordine (TRANSACTION_ID)
- Dati della carta di credito (numero, data di scadenza ed eventuale codice di sicurezza della carta)
- Importo e divisa della transazione
- Tipo di transazione, che può assumere i seguenti valori:
 - **"Contabilizzazione implicita"**; a fronte di una autorizzazione alla spesa con esito positivo il sistema X-PAY provvede alla contabilizzazione addebitando la carta di credito dell'acquirente ed accreditando l'esercente.
 - **"Contabilizzazione esplicita"**; a fronte di una autorizzazione alla spesa con esito positivo è l'esercente che in un tempo successivo comunica in modo esplicito al sistema X-PAY di contabilizzare l'operazione, quindi di addebitare la carta di credito dell'acquirente accreditando l'esercente stesso.

- MAC(Codice d'autenticazione del messaggio). Nel processo di comunicazione tra l'esercente ed X-PAY vi è il rischio che un soggetto estraneo, in grado di intercettare il messaggio, cerchi di alterarne il contenuto, rispedendolo poi al destinatario finale. Questo rischio viene evitato introducendo un processo d'autenticazione tramite la "firma" dei messaggi che vengono trasmessi.
- L'URL alla quale inviare l'utente in caso di completamento della transazione (ResultURL) con autenticazione Verified by Visa/SecureCode
- L'URL che X-PAY deve utilizzare per comunicare all'esercente l'esito della transazione (NotificationURL) in caso di pagamento con autenticazione Verified by Visa/SecureCode

X-PAY acquisisce i parametri ed effettua i controlli di identità del chiamante e di correttezza dei dati della transazione; se i controlli vengono superati contatta l'ente emittente della carta di credito indicata dall'acquirente per verificare se la carta aderisce o meno ai protocolli di sicurezza.

5.2. Autenticazione del titolare

Se la carta non aderisce al servizio Verified by Visa/SecureCode il pagamento può essere immediatamente concluso; in tal caso X-PAY inoltra la richiesta di pagamento ai sistemi autorizzativi e restituisce all'esercente, sulla stessa connessione in cui ha ricevuto il messaggio AReq, l'esito della transazione, inoltrando il messaggio ARes.

Se invece l'acquirente aderisce al servizio Verified by Visa/SecureCode deve essere rediretto verso l'applicazione dell'Issuer per potersi identificare. La redirectione avviene tramite una pagina html che deve essere restituita al browser dell'acquirente per effettuare la chiamata verso l'Issuer. La piattaforma X-PAY restituisce quindi in risposta al messaggio AReq non l'esito della transazione, ma un differente messaggio AuthRes contenente l'html necessario per effettuare la redirectione. L'applicazione dell'esercente deve quindi restituire l'html ricevuto al browser dell'acquirente.

Da questo istante il processo d'autenticazione è interamente gestito dall'Issuer il quale, al termine di tale fase redireziona a sua volta il browser dell'acquirente verso un URL opportunamente predisposto dalla piattaforma X-PAY comunicando contestualmente l'esito della fase d'autenticazione. X-PAY elabora il messaggio ricevuto dall'Issuer per verificare se può proseguire o meno nel pagamento. Infatti se l'acquirente aderisce al Verified by Visa/SecureCode il pagamento può essere inoltrato solamente se l'utente che sta utilizzando la carta di credito è stato in grado

di fornire il dato necessario alla sua autenticazione (es. password).

5.3. Fase di pagamento e notifica dell'esito

Se l'acquirente si è autenticato correttamente oppure la fase d'autenticazione non è stata necessaria, X-PAY inoltra la richiesta di pagamento ai sistemi autorizzativi e ne riceve la relativa risposta.

In entrambi i casi o al termine della fase d'autenticazione o al termine del pagamento, X-PAY comunica all'esercente l'esito della transazione tramite il messaggio ARes contenente o i dati dell'avvenuto pagamento oppure il motivo per cui non è stato possibile effettuarlo (es. autenticazione fallita, autorizzazione negata per la carta di credito utilizzata, problemi tecnici ecc..).

Il messaggio ARes viene quindi inviato o in risposta al messaggio AReq sulla stessa connessione in cui è stato ricevuto tale messaggio, oppure tramite una chiamata server to server inoltrata da X-PAY al termine della fase di pagamento se il processo è stato interrotto dalla fase d'autenticazione è quindi non è stato possibile inviare una risposta immediata alla richiesta inoltrata dall'esercente.

In questo secondo caso X-PAY inoltrerà il messaggio ARes al NOTIFICATION_URL indicato dall'esercente nel messaggio di apertura ordine (AReq) e redirigerà il browser dell'acquirente, che per poter effettuare l'autenticazione è stato rediretto fuori dal sito di e-commerce dell'esercente, al RESULT_URL indicato anch'esso dall'esercente nel messaggio AReq. L'utilizzo di una comunicazione diretta server to server per inoltrare il messaggio ARes garantisce all'esercente la ricezione dell'esito della transazione indipendentemente dalle azioni dell'acquirente, mentre la redirezione del titolare gli consentirà di riacquisire la gestione della comunicazione con l'acquirente per presentargli l'esito della transazione.

Se si dovessero verificare errori di comunicazione durante l'inoltro del messaggio ARes, X-PAY invierà all'esercente un'email di notifica dell'esito della transazione utilizzando l'indirizzo email che l'esercente ha indicato tramite l'ambiente di back office di X-PAY.

Il messaggio di notifica dell'esito della transazione (ARes) conterrà tra gli altri i seguenti dati:

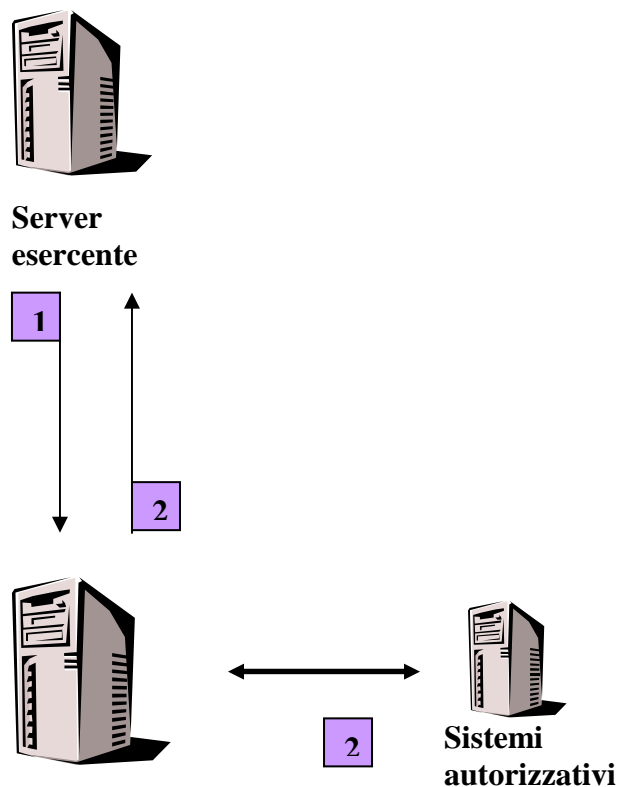
- Codice autorizzativo: codice identificativo della autorizzazione assegnato dall'emittente della carta
- Tipo di transazione: tipologia di transazione che indica il livello di sicurezza della transazione

6. MOTO opzione server to server

Questa modalità di integrazione prevede che l'esercente abbia ottenuto dall'acquirente tutti i dati della carta di credito e che gestisca tramite la piattaforma X-PAY, mediante dei messaggi server to server la fase di pagamento.

In particolare il diagramma sottostante evidenzia lo scambio di messaggi. Si distingue:

1. **Richiesta di pagamento:** l'applicazione dell'esercente spedisce i dati del pagamento che intende richiedere a X-PAY inviando tramite una chiamata server to server il messaggio AReq. Il messaggio contiene anche un campo TRANSACTION_ID che identifica univocamente l'ordine.
2. **Pagamento:** X-PAY effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta.
3. **Notifica dell'esito all'esercente:** X-PAY comunica l'esito della richiesta di pagamento all'esercente tramite il messaggio ARes. L'intero processo avviene mediante una chiamata sincrona.



VPOS

6.1. Richiesta di pagamento

L'esercente invia un messaggio server to server (AReq) alla piattaforma X-PAY indicando i dati relativi alla transazione, quali numero ordine, importo, valuta, numero di carta, data scadenza carta, CVV2, etc.

I dati vengono inoltrati in modalità sicura via SSL 128 bit verso X-PAY per la trasmissione verso i circuiti di pagamento.

6.2. Fase di pagamento e notifica dell'esito

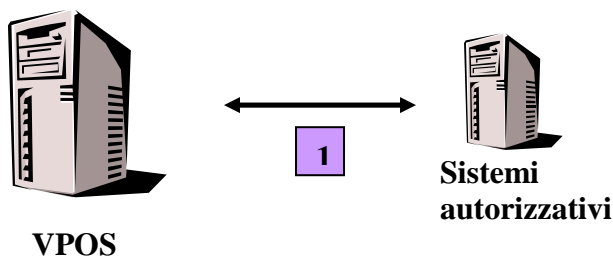
Il sistema X-PAY una volta ricevuti i dati della richiesta di pagamento inoltra la richiesta ai sistemi autorizzativi ottenendo la relativa risposta. A questo punto X-PAY comunica al server dell'esercente la risposta utilizzando il messaggio ARes contenente o i dati dell'avvenuto pagamento oppure il messaggio di errore che identifica il perché la richiesta non è potuta andare a buon fine. Va ricordato che l'intero processo avviene con una chiamata sincrona.

7. MOTO opzione Back Office

Per gli esercenti MOTO il Back Office del sistema X-PAY permette di gestire l'intero processo di pagamento mediante l'uso di un unico ambiente. Questa modalità di integrazione ha una serie di vantaggi che sono:

- Nessun hardware/software installato c/o i punti vendita
- Upgrade e nuove funzionalità gestite direttamente dalla piattaforma
- Immediata verifica da parte del merchant del buon esito della transazione (autorizzazione immediata)

Il processo di pagamento, come illustrato di seguito consiste in un'interazione tra la piattaforma di pagamento e i sistemi autorizzati. L'esercente ha la possibilità di effettuare, attraverso la funzionalità di gestione dell'ordine, più richieste di autorizzazione/contabilizzazione ottenendo l'esito direttamente da Back Office in modo immediato. Va ricordato infatti che tutte le richieste che avvengono tra X-PAY e il sistema autorizzativo sono delle chiamate sincrone.



Pagamento: X-PAY effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta.

8. Funzioni di Back Office

X-PAY di CartaSi mette a disposizione degli esercenti un ambiente di back office per la fase di operatività (gestione delle transazioni in modo facile ed efficace) , configurazione e modifica profilo.

L'esercente che invece dispone di un proprio sistema informativo potrà usufruire di alcune delle funzionalità di back office (operatività e reportistica) mediante integrazione con API (server to server).

Relativamente alle funzionalità disponibili nel back office del sistema X-PAY si possono distinguere funzionalità di:

- **ACCESSO AL SISTEMA:** l'accesso al sistema di back office avviene direttamente tramite browser sul portale esercenti CartaSi autenticandosi mediante user-id e password.
- **FUNZIONALITA' DI GESTIONE DEGLI ORDINI:** la disposizione di incasso dall'esercente all'acquirente a (di seguito indicato come **contabilizzazione**) può avvenire o al momento stesso della transazione, se l'esercente ha aperto l'ordine richiedendo la contabilizzazione implicita oppure in un momento successivo, se l'esercente ha aperto l'ordine richiedendo la contabilizzazione esplicita. In quest'ultimo caso l'esercente potrà, tramite X-PAY, eseguire successivamente le seguenti operazioni:
 1. annullamento totale o parziale della transazione. Non essendo stata contabilizzata la transazione, questa operazione ha come effetto quello di ripristinare il plafond della carta.
 2. contabilizzazione totale o parziale della transazione. Questa operazione conferma la transazione precedentemente autorizzata e ne rende effettivo l'incasso, cioè l'accredito dell'importo all'esercente ed il conseguente addebito al titolare della carta di credito.

Inoltre l'esercente potrà tramite X-PAY effettuare lo storno (totale o parziale) di una transazione precedentemente contabilizzata; l'importo stornato verrà rimborsato al titolare della carta e addebitato sul conto corrente dell'esercente. Si distinguono le operazioni sopra descritte a seconda della tipologia dell'esercente:

- o **E-COMMERCE:** permette all'operatore di gestire direttamente le transazioni con i circuiti di pagamento. In particolare gli operatori hanno la facoltà di richiedere operazioni di storno autorizzativo, contabilizzazioni (per le sole transazioni in cui la richiesta di contabilizzazione è esplicita) e storni contabili (riaccredito all'acquirente di un determinato importo) parziali o totali per un importo precedentemente autorizzato.
- o **MOTO:** permette all'operatore di effettuare e gestire tutto il tracking dell'ordine dalla richiesta di

autorizzazione alla contabilizzazione (esplicita o implicita) e relative operazioni di storno.

- **FUNZIONALITA' DI REPORTISTICA:** Accanto alle funzionalità dispositive per la gestione operativa degli ordini, sono disponibili anche le funzionalità di reportistica e storico degli ordini ricevuti, prospetti statistici sugli ordini e filtri per la ricerca degli ordini.
- **FUNZIONALITA' DI CONFIGURAZIONE:** I parametri che l'esercente può configurare sono:
 - o **Profilo:** Tramite questa funzionalità l'esercente visualizza i dati riassuntivi del suo convenzionamento al sistema X-PAY e può aggiornare i dati tecnici che consentono alla operatori di CartaSi di mettersi in contatto con la struttura dell'esercente per risolvere qualsiasi problema. Inoltre l'esercente potrà modificare gli indirizzi e@mail, per essere informato di qualsiasi transazione autorizzata ma che per motivi tecnici non si è potuta concludere positivamente.
 - o **Indirizzi IP:** questa funzionalità è obbligatoria per i soli esercenti che utilizzano il Front Office di X-PAY in modalità full. Consente di censire un massimo di dieci indirizzi IP che verranno ritenuti validi nella comunicazione dei messaggi autorizzativi.
 - o **Modifica pagina di pagamento:** Questa funzionalità permette agli esercenti che si integrano con X-PAY CartaSi in modalità FULL oppure LIGHT di personalizzare la pagina di pagamento scegliendo il logo, l'insegna e il colore di sfondo.
 - o **Parametri opzionali:** consente all'esercente di definire quali informazioni sono obbligatorie e quali invece sono facoltative per poter effettuare correttamente una transazione. Tali informazioni permettono quindi di personalizzare la struttura della transazione; saranno memorizzate negli archivi X-PAY ed usate nella reportistica come filtri di ricerca personalizzati.

9. Attivazione del servizio

Con la sottoscrizione della contrattualistica e l'integrazione tecnica descritta nelle pagine seguenti, l'esercente acquisisce il diritto di fruire del Servizio.

I dati indispensabili al fine dell'attivazione del servizio si distinguono a seconda della modalità di integrazione con la piattaforma di pagamento di CartaSi:

1. SERVER TO SERVER (esercenti e-commerce e MOTO):

- a. **Chiavi MAC:** servono per autenticare i messaggi trasmessi tra l'applicazione software dell'esercente e il sistema X-PAY.
- b. **TERMINAL_ID:** identifica univocamente il "negoziato virtuale" dell'esercente su X-PAY, è assegnato da CartaSi in fase di attivazione.
- c. **VERSION_CODE:** identificativo della versione software da utilizzare

2. PAGINA DI PAGAMENTO versione FULL: Prima di utilizzare il servizio, il merchant dovrà configurare tramite il Back Office, gli indirizzi IP del/dei propri server in modo tale che venga assicurata la chiamata tramite il controllo degli IP.

- a. **Chiavi MAC** servono per autenticare i messaggi trasmessi tra l'applicazione software dell'esercente e il sistema X-PAY.
- b. **TERMINAL_ID:** identifica univocamente il "negoziato virtuale" dell'esercente su X-PAY, è assegnato da CartaSi in fase di attivazione.
- c. **VERSION_CODE:** identificativo della versione software da utilizzare

3. PAGINA DI PAGAMENTO versione LIGHT:

- a. **Chiavi MAC:** servono per autenticare i messaggi trasmessi tra l'applicazione software dell'esercente e il sistema X-PAY.
- b. **TERMINAL_ID:** identifica univocamente il "negoziato virtuale" dell'esercente su X-PAY, è assegnato da CartaSi in fase di attivazione.
- c. **VERSION_CODE:** identificativo della versione software da utilizzare

Per quanto concerne le chiavi di sicurezza (accesso al back office e chiavi MAC), l'esercente è responsabile per ogni conseguenza dannosa che possa derivare dall'uso illecito delle stesse.

10. Struttura dei messaggi

10.1. Inoltro dei messaggi

La tipologia dei messaggi scambiati tra X-PAY e gli applicativi esercente, descritti nei prossimi paragrafi, differisce in base alla modalità d'integrazione come già descritto precedentemente:

- **Integrazione tramite Front Office**

Si tratta di messaggi http inviati con metodo POST, in modalità SSL, codificati con lo standard application/x-www-form-urlencoded

- **Integrazione tramite chiamate server to server**

Si tratta di messaggi xml inviati con metodo POST, in modalità SSL, codificati con lo standard ISO-8859-15

La sicurezza dei messaggi scambiati è garantita dal Protocollo SSL 128 bit utilizzando certificati Server-side. X-PAY utilizzerà infatti per i propri URL un certificato SSL Server che garantirà la cifratura dei dati; l' esercente dovrà a sua volta utilizzare un certificato Server per gli urls che ricevono chiamate da parte di X-PAY. Il certificato utilizzato dall' esercente deve essere emesso da una delle Certification Authority riconosciute. In caso contrario l' esercente deve fornire il/i certificato/i della/e Certification Authority che garantiscono l' autenticità del proprio certificato.

L' esercente è responsabile della custodia del proprio certificato, dei suoi rinnovi e dell' inoltro a CartaSi entro tempi ragionevoli di eventuali certificati intermedi per consentire l' installazione dei certificati rinnovati in sostituzione di quelli scaduti.

Nei paragrafi successivi vengono dettagliati i campi che costituiscono i vari messaggi. Le tabelle descrittive dei messaggi contengono le seguenti colonne:

- La colonna **Nome parametro** riporta l' identificativo con il quale una specifica informazione deve essere inserita nel messaggio.
- La colonna **Obb** specifica se l' informazione è **Obbligatoria** (in caso di omissione deve essere rifiutata l' elaborazione della transazione) o **Facoltativa**.
- La colonna **Formato** indica la tipologia e la lunghezza del parametro.

10.2. Firma messaggi

Ogni messaggio scambiato tra X-PAY ed il sistema dell' esercente contiene un campo MAC (Message Authentication Code). Il MAC è una quantità di sicurezza, generata in base ai parametri indicati nel singolo messaggio e ad una chiave segreta (Chiave per MAC) condivisa tra l' esercente e X-PAY, che consente di verificare che il messaggio proviene effettivamente dal mittente atteso e che non è stato alterato da una terza parte.

Il metodo utilizzato per generare il MAC di un dato messaggio è il seguente: viene calcolata la stringa risultante dal concatenamento dei parametri indicati e di una chiave segreta condivisa tra X-PAY e l' esercente. Tale chiave viene comunicata in maniera sicura all' esercente al momento dell' attivazione del servizio. Nella descrizione di ogni tipologia di messaggio sono invece indicati i parametri da utilizzare per il calcolo del MAC ed in quale ordine effettuare la relativa concatenazione. L'ordine con cui i parametri vengono concatenati per produrre il MAC deve essere esattamente quello indicato nella descrizione del messaggio in quanto è significativo nella generazione del MAC.

Per produrre il MAC si esegue l'hash dei dati concatenati come su descritto utilizzando un algoritmo di hashing standard, lo SHA-1 (Secure Hash Algorithm); il risultato della funzione di hash deve essere convertito in esadecimale, quindi tutti i caratteri devono essere trasformati in maiuscolo. Il risultato è una stringa di 40 caratteri che deve essere allegata al messaggio.

E' precisa responsabilità del destinatario del messaggio verificare la correttezza del MAC e quindi l'autenticità e l'integrità dei dati ricevuti. Alla ricezione del messaggio il destinatario deve calcolare il MAC, utilizzando la chiave segreta di cui è in possesso e i parametri che sono necessari a seconda del tipo di messaggio e verificare che coincida con il MAC ricevuto dal mittente. Solo se i 2 valori coincidono il destinatario deve proseguire con l'elaborazione del messaggio ricevuto.

Esempio di calcolo del MAC di un messaggio VPOSReq:

Dati della transazione:

TERMINAL_ID = ESE_WEB_00000001
TRANSACTION_ID = 01234abcdefg01234567
AMOUNT = 000000009
CURRENCY = 978
VERSION_CODE = 01.00
CO_PLATFORM = L
ACTION_CODE = AUT
EMAIL = nome_cognome@tiscali.it

Chiave segreta:

228829EWDKLSJDJD392132

Stringa ottenuta concatenando i dati della transazione e la chiave segreta:

ESE_WEB_0000000101234abcdefg0123456700000000997801.00LAUTnome_cognome@tiscali.it228829EWDKLSJDJD392132

Risultato della funzione standard di hashing SHA-1:

[B@12717ee-

Stringa convertita in esadecimale e maiuscole:

7A923F33473062F74EDC0CB05A7D1F7F611D5E3D

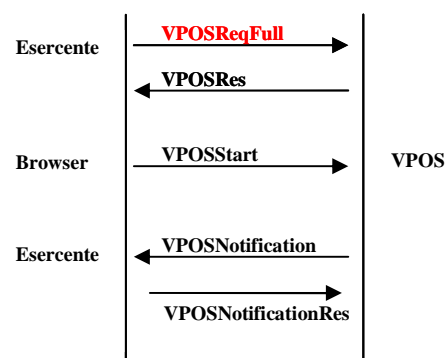
10.3. Integrazione tramite Front Office

Questo paragrafo contiene il dettaglio dei messaggi scambiati tra l'applicativo dell' esercente e la piattaforma X-PAY se l' esercente opta per la modalità d' integrazione tramite uso del front-end X-PAY, in una delle 2 versioni possibili, FULL o LIGHT.

10.3.1. Formato del messaggio VPOSReqFull

Modalità d' integrazione : Front-End – versione Full

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio di inizializzazione della transazione inviato dall' esercente al sistema X-PAY per comunicare i dati del pagamento e deve contenere i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	00000000502420 04	Codice identificativo dell' esercente e all' interno della piattaforma X-PAY
ACTION_CODE	0	Alfanumerico massimo 8 caratteri	AUT	Tipo di transazione richiesta. Sono consentiti i seguenti

Nome parametro	Obb	Formato	Esempio	Descrizione
				valori: AUT : si richiede una transazione con contabilizzazione esplicita AUT-CONT : si richiede una transazione con contabilizzazione implicita
AMOUNT	0	Alfanumerico 9 caratteri fissi (gli ultimi 2 caratteri rappresentano i 2 decimali, non deve essere inserito alcun separatore, né tra parti intere e parti decimali, né per le migliaia)	000123056 (per indicare una transazione di 1230,56 €)	importo della transazione
CURRENCY	0	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta dell'operazione, vedere l'Appendice A3 per i possibili valori
LANGUAGE	0	Alfanumerico 3 caratteri fissi	ITA	Lingua da utilizzare nelle pagine visualizzate da X-PAY all'acquirente, vedere l'Appendice A4 per i

Nome parametro	Obb	Formato	Esempio	Descrizione
				possibili valori.
NOTIFICATION_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/NotificationUrl	URL che deve essere utilizzato da X-PAY per comunicare all'esercente l'esito della transazione
RESULT_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/ResultUrl	URL alla quale l'acquirente viene rediretto in caso di completamento della transazione con esito positivo.
ERROR_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/errorUrl	URL alla quale l'acquirente viene rediretto in caso di errore nella visualizzazione della pagina di pagamento.
ANNULMENT_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/annulmentUrl	URL alla quale l'acquirente viene rediretto nel caso in cui decida di annullare la richiesta di pagamento.
VERSION_CODE	0	Alfanumerico 5 caratteri fissi	01.00	Versione software della piattaforma

Nome parametro	Obb	Formato	Esempio	Descrizione
				di pagamento X-PAY utilizzata, la versione a cui si riferisce il presente documento è la 01.00
EMAIL	F	Alfanumerico massimo 100 caratteri	rossi@tiscali.it	Indirizzo e-mail dell'acquirente, se comunicato verrà utilizzato per pre-valorizzare il campo e-mail della pagina di pagamento.
DESC_ORDER	F	Alfanumerico massimo 200 caratteri	Macchina digitale	Descrizione dell'ordine in corso, la descrizione viene visualizzata dove previsto nella login per le transazioni 3D-Secure
CO_PLATFORM	O	Alfanumerico 1 carattere fisso	F	Per la modalità d'integrazione e descritta dalla presente tabella deve essere F (FULL)
OPTION FIELDS	F	Alfanumerici (massimo 200 l'uno)		Campi aggiuntivi che l'esercente

Nome parametro	Obb	Formato	Esempio	Descrizione
				ha configurato tramite il back-office.
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DE D95C7EE8C5507A 9E1F2970BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC ed il relativo ordine per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - AMOUNT
 - CURRENCY
 - VERSION_CODE
 - CO_PLATFORM
 - ACTION_CODE
 - EMAIL
 - Chiave per MAC
- **Option Fields** : informazioni aggiuntive che l' esercente intende comunicare durante l'apertura dell'ordine oppure desidera che siano richieste all'acquirente nella pagina di pagamento. Queste informazioni saranno memorizzate negli archivi di X-PAY insieme agli altri dati dell'ordine. La loro configurazione può essere effettuata dall'esercente tramite il Back Office a sua disposizione (nella sezione Configurazione/Inserimento parametri); l'esercente deve indicare per ogni informazione aggiuntiva il nome del parametro con cui sarà trasmessa a X-PAY, il parametro deve avere come prefisso "OPTION_". L'utilizzo di tali parametri consente all'esercente di personalizzare la struttura della transazione con informazioni proprietarie che potrà utilizzare per effettuare ricerche o reportistiche con parametri personalizzati.

Esempio:

```

TERMINAL_ID=0000000050242004&ACTION_CODE=AUT&AMOUNT=000123056&CURRENCY=978&LANGUAGE=ITA&RESULT_URL=https://www.merchant.it/ResultUrl&NOTIFICATION_URL=https://www.merchant.it/NotificationUrl&ERROR_URL=https://www.merchant.it/errorUrl&ANNULMENT_URL=https://www.merchant.it/annulmentUrl&OPTION_CATEGORIA=macchine fotografiche&MAC=70C4F1F621A5DEDED95C7EE8C5507A9E1F2970BCFE&VERSION_

```

CODE=01.00&EMAIL=rossi@tiscali.it&ORDER_DESC=Macchina digitale&CO_PLATFORM=F

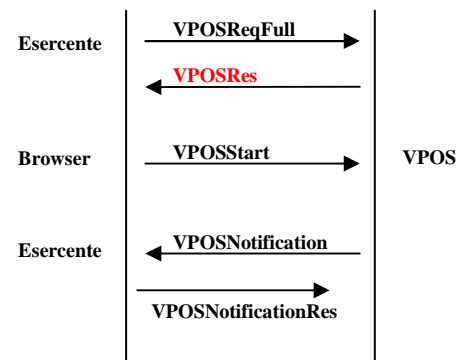
n.b.

L'esempio è riferito ad un esercente che ha configurato un parametro opzionale con nome OPTION_CATEGORIA

10.3.2. Formato del messaggio VPOSRes Full

Modalità d'integrazione : Front-End – versione Full

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio inviato da X-PAY all'esercente come risposta alla ricezione del messaggio VPOSReqFull sulla stessa connessione in cui è stata ricevuta la richiesta. La risposta di X-PAY contiene i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
PAYMENT_URL	0	Alfanumeric o massimo 260 caratteri	https://www .X-PAY.it	URL della pagina di pagamento a cui l'esercente deve redirezionare il titolare per procedere al pagamento
TRANSACTION_ID	0	Alfanumeric o 20 caratteri fissi	T0000000000 000000001	codice univoco identificativo dell'ordine che deve essere utilizzato in tutti i successivi messaggi scambiati tra l'esercente ed X-PAY.
RESPONSE	0	Alfanumeric o Massimo 3 caratteri	0	Codice esito della richiesta, per i relativi codici vedere la tabella sottostante

- **TRANSACTION_ID:** Il campo TRANSACTION_ID è in chiave univoca con il TERMINAL_ID dell'esercente. Non è obbligatorio avere una progressione di valori regolare.
- **Response:** risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

Codice	Descrizione
0	Operazione elaborata correttamente
1	Errore generico nel parsing del messaggio
2	Errore tecnico
3	Ordine non valido
4	Lingua mancante o valore non ammesso
5	url errato
6	Chiamata da IP non configurato
7	Errore nei campi opzionali
8	MAC errato
9	Parametro VERSION_CODE non corretto
10	Parametro ACTION_CODE non corretto
11	Importo mancante o valore non ammesso
12	Divisa mancante o valore non ammesso
13	e-mail non corretta
15	Errore nel parametro TRANSACTION_ID
16	Errore nel parametro TERMINAL_ID
17	Max numero di operazioni concesse con lo stesso campo TRANSACTION_ID(*)

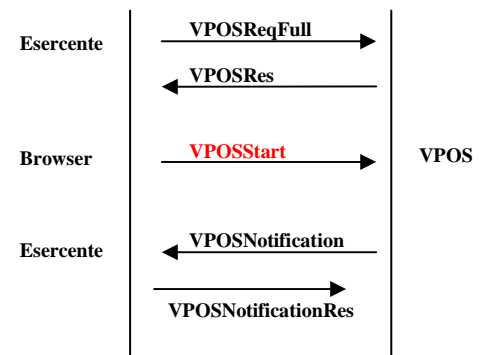
(*) Il valore massimo di autorizzazioni concesse con lo stesso ID_TRANSAZIONE viene impostato da X-PAY CartaSi.

Esempio:

PAYMENT_URL=https://www.X-PAY.it/XPServlet&TRANSACTION_ID=T00000000000000000001&RESPONSE=0

10.3.3. Formato del messaggio VPOSStart

Modalità d'integrazione : Front-End – versione Full
Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio che il sistema dell'esercente deve far generare al browser dell'acquirente dopo aver aperto l'ordine sulla piattaforma X-PAY ed averne ottenuto un identificativo univoco con il messaggio VPOSRes. Il messaggio VPOSStart deve essere inviato verso l'URL comunicato da X-PAY (PAYMENT_URL) sempre nel messaggio VPOSRes e contiene i seguenti campi:

Nome parametro	OBB	Formato	Esempio	Descrizione
TERMINAL_ID	O	Alfanumerico 16 caratteri fissi	0000000050242004	Codice identificativo dell' esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	O	Alfanumerico 20 caratteri fissi	T000000000000000000001	codice univoco identificativo dell'ordine attribuito da X-PAY
CO_PLATFORM	O	Alfanumerico 1 carattere fisso	F	Per la modalità d'integrazione descritta dal presente messaggio deve essere F (FULL)
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DED95C7E E8C5507A9E1F2970BCFE	Codice di sicurezza
MESSAGE_TYPE	F	Alfanumerico 3 caratteri fissi	C00	Codice che identifica la tipologia del messaggio. Per la ricezione delle informazioni relative alla Liability Shift, il

Nome parametro	OBB	Formato	Esempio	Descrizione
				valore deve essere >= 'C00'

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio sono i seguenti:

- TERMINAL_ID
- TRANSACTION_ID
- CO_PLATFORM
- Chiave per MAC

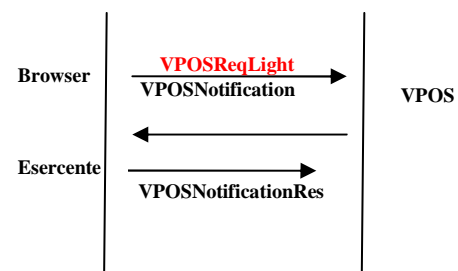
HTML di esempio:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1252">
<title>Prova X-PAY</title>
</head>
<p><b>X-PAYXPP (Full version)</b></p>
<body>
<form action="https://www.X-PAY.it/XPServlet" method="POST">
TERMINAL_ID:&nbsp;
  <input type="text" name="TERMINAL_ID" value="0000000050242004"
size="16" maxlength="16">
  <br>
TRANSACTION_ID:&nbsp;
  <input type="text" name="TRANSACTION_ID"
value="T00000000000000000001" size="20" maxlength="20">
  <br>
CO_PLATFORM: &nbsp;
<input type="text" name="CO_PLATFORM" value="F" size="1"
maxlength="1"><br>  <br>
<input type="text" name="MAC"
value="70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE" size="40"
maxlength="40"><br>  <br>
<input type="text" name="MESSAGE_TYPE" value="C00" size="3"
maxlength="3"><br>  <br>
<input type="submit" value="AUTH. ORDINE ACQUISTO!"
name="submitButton">
</form>
</body>
</html>
```

10.3.4. Formato del messaggio VPOSReqLight

Modalità d'integrazione : Front-End – versione Light

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio di inizializzazione della transazione che l'esercente, che ha optato per la versione Light del protocollo, deve fa generare al browser del titolare e deve contenere i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	00000000502420 04	Codice identificativo dell'esercente all'interno della piattaforma X- PAY
TRANSACTION_ID	0	Alfanumerico 20 caratteri fissi	T00000000000000 000001	codice univoco identificativo dell'ordine che deve essere utilizzato in tutti i successivi messaggi scambiati tra l'esercente ed X-PAY.
ACTION_CODE	0	Alfanumerico massimo 8 caratteri	AUT	Tipo di transazione richiesta. Sono consentiti i seguenti valori: AUT : si richiede una transazione con contabilizzazi one esplicita AUT-CONT : si richiede una transazione con contabilizzazi one implicita
AMOUNT	0	Alfanumerico 9 caratteri fissi (gli ultimi 2 caratteri rappresentano i 2 decimali,	000123056 (per indicare una transazione di 1230,56 €)	importo della transazione

Nome parametro	Obb	Formato	Esempio	Descrizione
		non deve essere inserito alcun separatore, né tra parti intere e parti decimali, né per le migliaia)		
CURRENCY	0	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta dell'operazione, vedere l'Appendice A3 per i possibili valori
LANGUAGE	0	Alfanumerico 3 caratteri fissi	ITA	Lingua da utilizzare nelle pagine visualizzate da X-PAY all'acquirente, vedere l'Appendice A4 per i possibili valori
NOTIFICATION_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/NotificationUrl	URL che deve essere utilizzato da X-PAY per comunicare all'esercente l'esito della transazione
RESULT_URL	0	Alfanumerico massimo 260 caratteri	https://www.merchant/ResultUrl	URL alla quale l'acquirente viene rediretto in caso di completamento della transazione con esito positivo.

Nome parametro	Obb	Formato	Esempio	Descrizione
ERROR_URL	O	Alfanumerico massimo 260 caratteri	https://www.merchant/errorUrl	URL alla quale l'acquirente viene rediretto in caso di errore nell'apertura dell'ordine.
ANNULMENT_URL	O	Alfanumerico massimo 260 caratteri	https://www.merchant/annulmentUrl	URL alla quale l'acquirente viene rediretto nel caso in cui decida di annullare la richiesta di pagamento.
VERSION_CODE	O	Alfanumerico 5 caratteri fissi	01.00	Versione software della piattaforma di pagamento X-PAY utilizzata, la versione a cui si riferisce il presente documento è la 01.00
EMAIL	F	Alfanumerico massimo 100 caratteri	rossi@tiscali.it	Indirizzo e-mail dell'acquirente, se comunicato verrà utilizzato per pre-valorizzare il campo e-mail della pagina di pagamento.
DESC_ORDER	F	Alfanumerico massimo 200 caratteri	Macchina digitale	Descrizione dell'ordine in corso
CO_PLATFORM	O	Alfanumerico 1 carattere fisso	F	Per la modalità d'integrazione descritta

Nome parametro	Obb	Formato	Esempio	Descrizione
				dalla presente tabella deve essere L (Light)
OPTION FIELDS	F	Alfanumerici (massimo 200 l'uno)		Campi aggiuntivi che l'esercente ha configurato tramite il back-office.
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DE D95C7EE8C5507A 9E1F2970BCFE	Codice di sicurezza
MESSAGE_TYPE	F	Alfanumerico 3 caratteri fissi	C00	Codice che identifica la tipologia del messaggio. Per la ricezione delle informazioni relative alla Liability Shift, il valore deve essere >= 'C00'

- **TRANSACTION_ID** : Il campo TRANSACTION_ID è in chiave univoca con il campo TERMINAL_ID. Non è obbligatorio avere una progressione di valori regolare.
- **MAC** : I parametri utilizzati per il calcolo del MAC ed il relativo ordine per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - AMOUNT
 - CURRENCY
 - VERSION_CODE
 - CO_PLATFORM
 - ACTION_CODE
 - EMAIL
 - Chiave per MAC
- **Option Fields** : informazioni aggiuntive che l'esercente intende comunicare durante l'apertura dell'ordine oppure

desidera che siano richieste all'acquirente nella pagina di pagamento. Queste informazioni saranno memorizzate negli archivi di X-PAY insieme agli altri dati dell'ordine. La loro configurazione può essere effettuata dall'esercente tramite il Back Office a sua disposizione (nella sezione Configurazione/Inserimento parametri); l'esercente deve indicare per ogni informazione aggiuntiva il nome del parametro con cui sarà trasmessa a X-PAY, il parametro deve avere come prefisso "OPTION_". L'utilizzo di tali parametri consente all'esercente di personalizzare la struttura della transazione con informazioni proprietarie che potrà utilizzare per effettuare ricerche o reportistiche con parametri personalizzati.

HMTL di esempio:

```
<html>
<head><meta      http-equiv="Content-Type"      content="text/html;
charset=windows-1252">
<title>Test X-PAY</title></head>
<p><b>Test X-PAY</b></p>
<body>
<form action="https://www.X-PAY.it/XPServlet" method="POST">
TERMINAL_ID:&nbsp;
<input  type="text"    name="TERMINAL_ID"    value="0000000050242004"
size="16" maxlength="16"> <br>
TRANSACTION_ID:&nbsp;
<input                                type="text"                                name="TRANSACTION_ID"
value="T00000000000000000001" size="20" maxlength="20"><br>
ACTION_CODE:&nbsp;
<input  type="text"    name="ACTION_CODE"    value="AUT"    size="10"
maxlength="10"> <br>
AMOUNT:&nbsp;
<input  type="text"    name="AMOUNT"    value="000123056"    size="9"
maxlength="9"><br>
CURRENCY: default(Euro=978)&nbsp;
<input  type="text"    name="CURRENCY"    value="978"    size="3"
maxlength="3"><br>
LANGUAGE: &nbsp;
<input  type="text"    name="LANGUAGE"    value="ITA"    size="3"
maxlength="3"><br>
RESULT_URL (URL OK): &nbsp;
<input                                type="text"                                name="RESULT_URL"
value="https://www.merchant.it/ResultUrl" size="40"><br>
NOTIFICATION_URL: &nbsp;
<input                                type="text"                                name="NOTIFICATION_URL"
value="https://www.merchant.it/NotificationUrl" size="40"><br>
ERROR_URL: &nbsp;
<input                                type="text"                                name="ERROR_URL"
value="https://www.merchant.it/errorUrl" size="40" ><br>
ANNULMENT_URL: &nbsp;
<input                                type="text"                                name="ANNULMENT_URL"
value="https://www.merchant.it/annulmentUrl" size="40"><br>
CATEGORIA:&nbsp;
<input  type="text"    name="OPTION_CATEGORIA"    value="Macchine
Fotografiche" size="40"><br>
MAC: &nbsp;
<input                                type="text"                                name="MAC"
value="70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE" size="40"
maxlength="40"><br>
VERSION_CODE: &nbsp;
<input  type="text"    name="VERSION_CODE"    value="01.00"    size="5"
maxlength="5"><br>
```



```
EMAIL: &nbsp;


```

n.b.

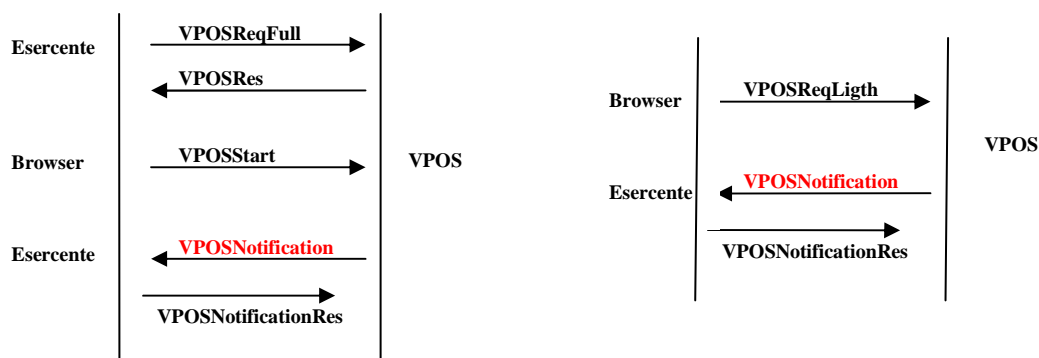
L'esempio è riferito ad un esercente che ha configurato un parametro opzionale con nome OPTION_CATEGORIA

10.3.5. Formato del messaggio VPOSNotification

Modalità d'integrazione : Front-End – versione Full

Front-End – versione Light

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio inoltrato da X-PAY agli URL (NOTIFICATION_URL e RESULT_URL) specificati dall'esercente nel messaggio di apertura dell'ordine (VPOSReqFull o VPOSReqLight), per potergli comunicare l'esito **positivo** della transazione. La comunicazione verso il NOTIFICATION_URL avviene tramite una chiamata diretta server to server, quella verso il RESULT_URL avviene tramite il browser dell'acquirente.

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	0000000050242004	Codice identificat ivo dell'eserce nte all'interno della piattaforma X-PAY
TRANSACTION_ID	0	Alfanumerico 20 caratteri fissi	T000000000000000 0001	codice univoco identificat ivo dell'ordine attribuito da X-PAY o dall'eserce nte
RESPONSE	0	Alfanumerico Massimo 15 caratteri	TRANSACTION_OK	Esito della Transazione , può assumere i seguenti valori: TRANSACTION _OK = transazione autorizzata
AUTH_CODE	0	Alfanumerico Massimo 10 caratteri	901867	codice dell'autori zzazione ricevuto dall'emitte nte della carta di credito. Può contenere degli spazi
TRANSACTION_DATE	0	Alfanumerico 19 caratteri fissi Formato gg/mm/aaaa hh.mm.ss	06/07/2005 16.55.56	Data della transazione
CARD_TYPE	0	Alfanumerico	VISA	Il tipo di

Nome parametro	Obb	Formato	Esempio	Descrizione
		Massimo 10 caratteri		carta utilizzata per il pagamento, vedere l'Appendice A1 per i possibili valori.
AMOUNT	O	Alfanumerico 9 caratteri fissi (gli ultimi 2 caratteri rappresentano i 2 decimali, non deve essere inserito alcun separatore, né tra parti intere e parti decimali, né per le migliaia)	000123056 (per indicare una transazione di 1230,56 €)	importo della transazione
CURRENCY	O	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta dell'operazione, vedere l'Appendice A3 per i possibili valori
AMOUNT_DCC	F	Alfanumerico di lunghezza 9	000012345	Importo nella valuta scelta dal titolare Esempi formato: 000012345 JPY = 12345 JPY 000012345 USD = 123, 45 USD (la divisa JPY

Nome parametro	Obb	Formato	Esempio	Descrizione
				non ha decimali)
EXCHANGE_RATE	F	Numerico (8,4)	999.9999	Tasso di cambio applicato
MARK_UP	F	Numerico (8,4)	99.1234	
MARK_UP_DEC	F	Numerico di lunghezza 1	4	Cifre decimali mark-up
TRANSACTION_TYPE	O	Alfanumerico Massimo 20 caratteri	VBV_FULL	Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice A2 per i possibili valori.
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DED9 5C7EE8C5507A9E1F 2970BCFE	Codice di sicurezza
REGION	F	Alfanumerico massimo 50 caratteri	Europe	Regione di appartenenza della carta E' presente nel messaggio solo se la transazione è richiesta con carte appartenenti ai circuiti VISA e MASTERCARD e nel corrispondente

Nome parametro	Obb	Formato	Esempio	Descrizione
				messaggio di richiesta (VPOSStart per l'integrazione Full o VPOSReqLight per l'integrazione Light) è stato inserito il parametro facoltativo Message_Typ e con un valore >='C00'
COUNTRY	F	Alfanumerico massimo 50 caratteri	Italy	Paese di emissione della carta. E' presente nel messaggio solo se nel corrispondente messaggio di richiesta (VPOSStart per l'integrazione Full o VPOSReqLight per l'integrazione Light) è stato inserito il parametro facoltativo Message_Typ e con un valore

Nome parametro	Obb	Formato	Esempio	Descrizione
				>='C00'. Nel caso di transazione con carta appartenent e al circuito AMEX, il campo può assumere solo i seguenti valori: "ITALY", "NO ITALY"
PRODUCT_TYPE	F	Alfanumerico massimo 50 caratteri	Consumer	Tipologia di Prodotto. E' presente nel messaggio solo se la transazione è richiesta con carte appartenent i ai circuiti VISA e MASTERCARD e nel corrisponde nte messaggio di richiesta (VPOSStart per l'integrazi one Full o VPOSReqLigh t per l'integrazi one Light)

Nome parametro	Obb	Formato	Esempio	Descrizione
				<p>è stato inserito il parametro facoltativo Message_Typ e con un valore >='C00'</p>
LIABILITY_SHIFT	F	Alfanumerico massimo 4 caratteri (" ", "N", "N.A.")	N	<p>Flag che definisce se la transazione è in Liability Shift. La risposta "N", valida per i circuiti VISA e MASTERCARD, definisce che per questa transazione non si applica la regola di trasferire la responsabilità dall'Acquirer all'Issuer</p> <p>Nel caso di transazione con carta appartenente al circuito AMEX, il campo assume il valore "N.A."</p>

Nome parametro	Obb	Formato	Esempio	Descrizione
				essendo non applicabile il concetto di Liability Shift E' presente nel messaggio solo se nel corrispondente messaggio di richiesta (VPOSStart per l'integrazione Full o VPOSReqLight per l'integrazione Light) è stato inserito il parametro facoltativo Message_Type e con un valore >='C00'

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - RESPONSE
 - AMOUNT
 - CURRENCY
 - Chiave per MAC

- **AUTH_CODE** : codice dell'autorizzazione ricevuto dall'emittente della carta di credito utilizzata dall'acquirente. Non è un codice univoco.

Esempio:

```
TERMINAL_ID=0000000050242004&TRANSACTION_ID=T0000000000000000001&RESPONSE=TRANSACTION_OK&AUTH_CODE=901867&TRANSACTION_DATE=06/07/200516.55.56&CARD_TYPE=VISA&AMOUNT=000123056&CURRENCY=978&TRANSACTION_TYPE=VBV_FULL&MAC=70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE&REGION=Europe&COUNTRY=Italy&PRODUCT_TYPE=Consumer&LIABILITY_SHIFT=N
```

In caso di errori di comunicazione nell'inoltro del messaggio VPOSNotification, X-PAY inoltrerà un'e-mail all'indirizzo configurato a tale scopo dall'esercente tramite il back Office a sua disposizione. L'email conterrà gli stessi dati del messaggio VPOSNotification e ne sostituirà definitivamente l'invio. L'e-mail avrà sempre lo stesso formato e sintassi, così da poter essere facilmente processata da parte degli applicativi dell'esercente.

Di seguito viene riportata la sintassi utilizzata:

Oggetto e-mail:

VPOSNOTIFICATION - TRANSACTION_ID

Testo e-mail:

```
TERMINAL_ID:
TRANSACTION_ID:
RESPONSE:
AUTH_CODE:
TRANSACTION_DATE:
CARD_TYPE:
AMOUNT:
CURRENCY:
AMOUNT_DCC:
EXCHANGE_RATE:
MARK_UP:
MARK_UP_DEC:
TRANSACTION_TYPE:
MAC:
REGION:
COUNTRY:
PRODUCT_TYPE:
LIABILITY_SHIFT:
```

Esempio di email:

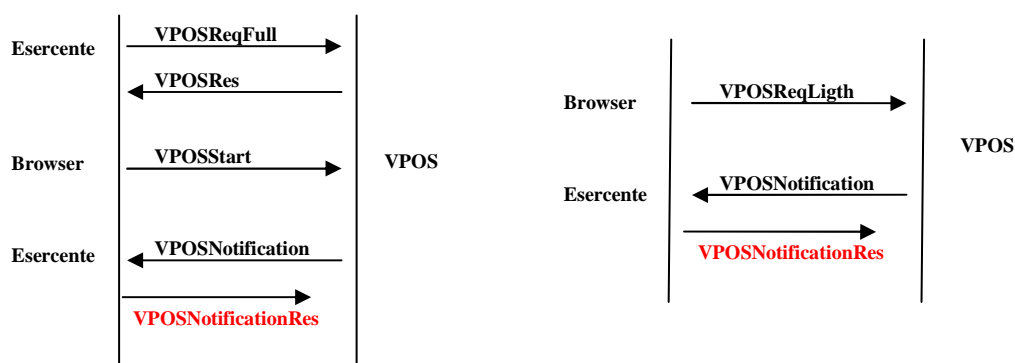
VPOSNOTIFICATION - T00000000000000000001

TERMINAL_ID: 0000000050242004
 TRANSACTION_ID: T00000000000000000001
 RESPONSE: TRANSACTION_OK
 AUTH_CODE: 901867
 TRANSACTION_DATE: 06/07/2005 16.55.56
 CARD_TYPE: VISA
 AMOUNT: 000123056
 CURRENCY: 978
 AMOUNT_DCC: 000012345
 EXCHANGE_RATE: 10.2
 MARK_UP: 12.6
 MARK_UP_DEC: 1
 TRANSACTION_TYPE: VBV_FULL
 MAC: 70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE
 REGION: Europe
 COUNTRY: Italy
 PRODUCT_TYPE: Consumer
 LIABILITY_SHIFT: N

10.3.6. Formato del messaggio VPOSNotificationRes

Modalità d'integrazione : Front-End – versione Full
 Front-End – versione Light

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio inoltrato dall'esercente a X-PAY come risposta all'avvenuta ricezione del messaggio VPOSNotification, inviato sulla stessa connessione in cui è stato inoltrato il messaggio di X-PAY.

Nome parametro	Obb	Formato	Esempio	Descrizione
----------------	-----	---------	---------	-------------

RESPONSE	0	Alfanumerico Massimo 3 caratteri	0	Codice di esito dell'elaborazione del messaggio VPOSNotification, per i relativi codici vedere la tabella sottostante.
----------	---	-------------------------------------	---	--

- **RESPONSE** risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

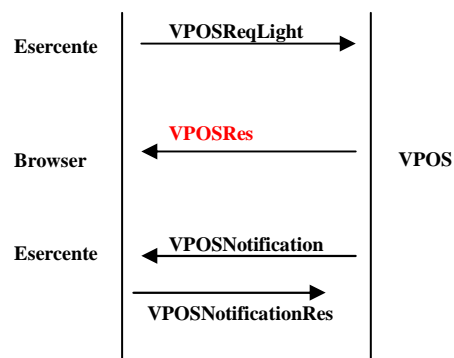
Codice	Descrizione
0	Operazione elaborata correttamente

Esempio: RES
RESPONSE=0

10.3.7. Formato del messaggio VPOSRes Light

Modalità d'integrazione : Front-End – versione Light

Tipologia di messaggio : messaggio http inviato con metodo POST, in modalità SSL



Rappresenta il messaggio inviato da X-PAY all' esercente come risposta alla ricezione del messaggio VPOSReqLight indirizzando il browser sull'indirizzo ERROR_URL indicato nel messaggio di VPOSReqLight. La risposta di X-PAY contiene i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico o 16 caratteri fissi	0000000050242004	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	0	Alfanumerico o 20 caratteri	T00000000000000000001	codice univoco identificativo dell'ordine che deve essere

Nome parametro	Obb	Formato	Esempio	Descrizione
		fissi		utilizzato in tutti i successivi messaggi scambiati tra l'esercente ed X-PAY.
RESPONSE	0	Alfanumeric o Massimo 3 caratteri	0	Codice esito della richiesta, per i relativi codici vedere la tabella sottostante

- **TRANSACTION_ID:** Il campo TRANSACTION_ID è in chiave univoca con il TERMINAL_ID dell'esercente. Non è obbligatorio avere una progressione di valori regolare.
- **Response:** risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

Codice	Descrizione
0	Operazione elaborata correttamente
1	Errore generico nel parsing del messaggio
2	Errore tecnico
3	TRANSACTION_ID duplicato
4	Lingua mancante o valore non ammesso
5	url errato
6	Chiamata da IP non configurato
7	Errore nei campi opzionali
8	MAC errato
9	Parametro VERSION_CODE non corretto
10	Parametro ACTION_CODE non corretto
11	Importo mancante o valore non ammesso
12	Divisa mancante o valore non ammesso
13	e-mail non corretta
15	Errore nel parametro TRANSACTION_ID
16	Errore nel parametro TERMINAL_ID
17	Max numero di operazioni concesse con lo stesso campo TRANSACTION_ID(*)

(*) Il valore massimo di autorizzazioni concesse con le stesso ID_TRANSAZIONE viene impostato da X-PAY CartaSi.

Esempio:

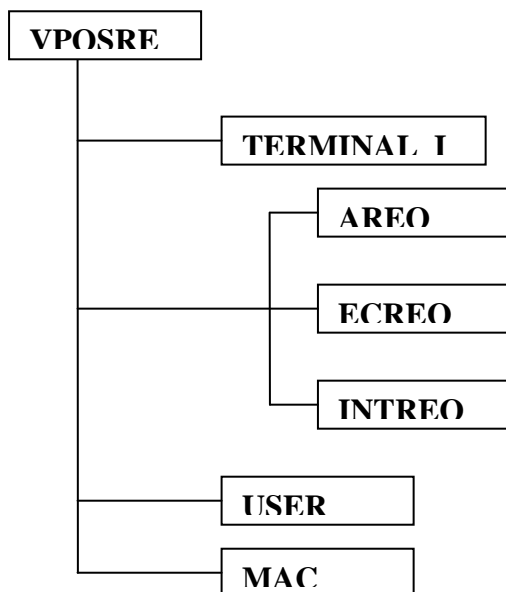
PAYMENT_URL=https://www.esercente.it/errore.php?TERMINAL_ID=WEB_9999999999&TRANSACTION_ID=T00000000000000000001&RESPONSE=3

10.4. Integrazione tramite messaggi server to server

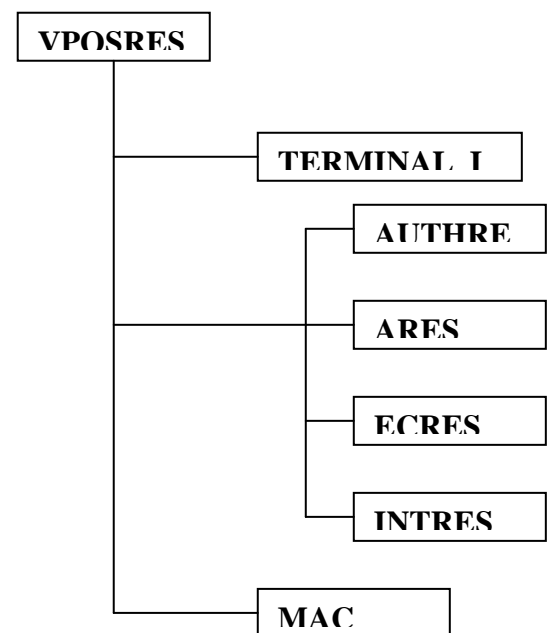
Questo paragrafo contiene il dettaglio dei messaggi scambiati tra l'applicativo dell'esercente e la piattaforma X-PAY se l'esercente opta per la modalità d'integrazione tramite chiamate server to server.

Tutti i messaggi previsti per questa modalità d'integrazione sono in formato XML e sono costituiti da una parte di elementi comuni a cui si aggiunge un elemento specifico della richiesta/risposta che si vuole inoltrare. I formati dei messaggi di richiesta e di risposta sono i seguenti:

Messaggio xml di richiesta



Messaggio xml di risposta



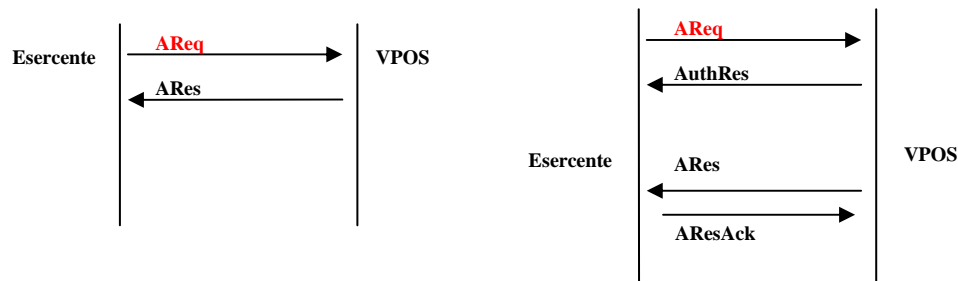
n.b.

fa eccezione il messaggio VPOSack che ha una struttura differente rispetto agli altri messaggi.

10.4.1. Formato del messaggio AReq

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Rappresenta il messaggio di richiesta di un nuovo pagamento che l'applicativo dell'esercente deve inoltrare a X-PAY tramite una chiamata server to server e deve contenere i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	00000000502420 04	Codice identificativo dell'esercente all'interno della piattaforma X- PAY
TRANSACTION_ID	0	Alfanumerico 20 caratteri fissi	T0000000000000 000001	codice univoco che identifica l'ordine dell'esercente
REQUEST_TYPE	0	Alfanumerico 2 caratteri fissi	FA	Valori Possibili: FA : Primo Tentativo RA : Retry di richiesta di pagamento
ACTION_CODE	0	Alfanumerico massimo 8 caratteri	AUT	Tipo di transazione richiesta. Sono consentiti i seguenti valori: AUT : si richiede una

Nome parametro	Obb	Formato	Esempio	Descrizione
				transazione con contabilizzazione esplicita AUT-CONT : si richiede una transazione con contabilizzazione implicita
PAN	0	Alfanumerico massimo 19 caratteri	1234567890123456	Numero della carta soggetta alla richiesta di pagamento. Controllo formale sul PAN è in carico all'esercente, la ricezione di un dato formalmente errato restituisce un RESPONSE=1
EXPIRE_DATE	0	Alfanumerico 4 caratteri fissi Formato : YYMM	0605 (per indicare come data di scadenza il maggio 2006)	Data di scadenza della carta soggetta alla richiesta di pagamento
CVV2	0	Alfanumerico Massimo 4	1234	Codice di sicurezza della carta soggetta alla richiesta di pagamento
AMOUNT	0	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2 decimali e non è usato il separatore tra parti intere e parti	000123056 (per indicare una transazione di 1230,56 €)	importo del pagamento richiesto

Nome parametro	Obb	Formato	Esempio	Descrizione
		decimali)		
CURRENCY	0	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta del pagamento, vedere l'Appendice A3 per i possibili valori
NOTIFICATION_URL	0	Alfanumerico massimo 100 caratteri	https://www.merchant/NotificationUrl	URL che deve essere utilizzato da X-PAY per comunicare all'esercente l'esito della transazione in caso di transazione Verified by Visa/SecureCode Il parametro non risulta obbligatorio nel caso di integrazione MOTO
RESULT_URL	0	Alfanumerico massimo 100 caratteri	https://www.merchant/ResultUrl	URL alla quale l'acquirente viene rediretto al termine del pagamento in caso di transazione Verified by Visa/SecureCode Il parametro non risulta obbligatorio nel caso di integrazione MOTO
VERSION_CODE	0	Alfanumerico 5 caratteri fissi	01.00	Versione software della piattaforma di

Nome parametro	Obb	Formato	Esempio	Descrizione
				pagamento X-PAY utilizzata, la versione a cui si riferisce il presente documento è la 01.00
DESC_ORDER	F	Alfanumerico massimo 200 caratteri	Macchina digitale	Descrizione dell'ordine in corso
LIABILITY	F	Alfanumerico di un carattere	Y	Flag di richiesta dati relativi al protocollo di LIABILITY SHIFT nell'ambito dell'autenticazione 3D-SECURE
TICKET	F	Alfanumerico di 25 caratteri	1214390171406_API	Numero del ticket della richiesta del servizio DCC
DCC_FLAG	F	Alfanumerico di un carattere	3	Flag di richiesta servizio DCC
USER	F	Alfanumerico massimo 20 caratteri	User001	Operatore dell'esercente che ha richiesto l'operazione (solo per esercenti M.O.T.O.)
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DE D95C7EE8C5507A 9E1F2970BCFE	Codice di sicurezza

- **TRANSACTION_ID:** identifica univocamente l'ordine dell'esercente. Non è obbligatorio avere una progressione di valori regolare.
- **REQUEST_TYPE:**

L'esercente può inviare una richiesta di pagamento per un dato ordine più volte solo per uno dei seguenti motivi:

- perdita della risposta al messaggio AReq, per Time-Out o altri motivi
- retry del pagamento dopo un'autorizzazione negata

L'esercente deve inviare il primo messaggio AReq relativo ad un determinato ordine valorizzando ad "FA" il campo REQUEST_TYPE, mentre per gestire un nuovo tentativo può inoltrare nuovamente un AReq utilizzando lo stesso TRANSACTION_ID ma valorizzando ad "RA" il campo REQUEST_TYPE.

In questo caso X-PAY, se il pagamento relativo al TRANSACTION_ID è avvenuto con esito positivo, restituisce lo stesso esito che ha restituito per la prima richiesta di pagamento dell'esercente. Nel caso in cui l'autorizzazione sia invece stata rifiutata, X-PAY elabora nuovamente la richiesta di pagamento e ne restituisce l'esito.

Se l'esercente effettua un retry del pagamento di un dato ordine, il nuovo messaggio deve contenere esattamente gli stessi valori del primo messaggio, gli unici campi per i quali è ammessa una variazione sono il campo REQUEST_TYPE (che deve avere il valore "RA") e i campi relativi alla carta di credito (PAN, EXPIRE_DATE, CVV2) per consentire all'esercente di poter gestire il caso in cui, dopo un'autorizzazione negata, l'acquirente corregga i dati della carta di credito da utilizzare per il pagamento.

In ogni caso il valore del campo TRANSACTION_ID non potrà essere duplicato per diverse Richieste AReq con il campo REQUEST_TYPE valorizzato ad "FA". In questo caso la transazione verrà rifiutata da X-PAY.

Il Timeout, o qualsiasi situazione riprovata, devono essere sempre gestite dall'applicativo dell'esercente utilizzando questa tecnica di retry, al fine di evitare di abbattere inutilmente il Plafond della carta del compratore a causa di problemi tecnici a lui non imputabili.

- **MAC:** i campi utilizzati per il calcolo del MAC di questo messaggio sono:
 - TERMINAL_ID
 - TRANSACTION_ID
 - ACTION_CODE
 - PAN
 - EXPIRE_DATE
 - CVV2
 - AMOUNT
 - CURRENCY
 - VERSION_CODE
 - USER
 - Chiave per MAC

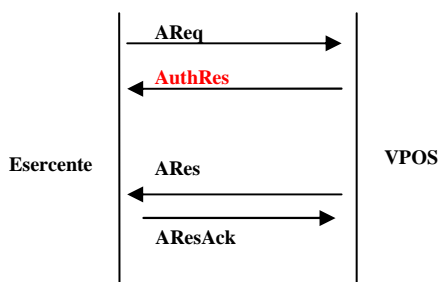
Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <AREQ>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <ACTION_CODE>AUT</ACTION_CODE>
    <PAN>1234567890123456</PAN>
    <EXPIRE_DATE>0605</EXPIRE_DATE>
    <CVV2>123</CVV2>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <NOTIFICATION_URL>https://www.merchant/NotificationUrl</NOTIFICATION_URL>
    <RESULT_URL>https://www.merchant/ResultUrl</RESULT_URL>
    <VERSION_CODE>01.00</VERSION_CODE>
    <DESC_ORDER>Macchina digitale</DESC_ORDER>
    <LIABILITY>Y</LIABILITY>
    <TICKET>1214390171406_API </TICKET>
    <DCC_FLAG>Y</DCC_FLAG>
  </AREQ>
  <USER>User001</USER>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

10.4.2. Formato del messaggio AuthRes

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Questo messaggio viene restituito da X-PAY in risposta al messaggio AReq se il pagamento non può essere inoltrato in quanto deve essere preceduto dalla fase d'autenticazione dell'acquirente prevista dai protocolli Verified by Visa/SecureCode. Il messaggio

viene inoltrato usando la stessa connessione con cui è stato ricevuto il messaggio AReq ed ha il seguente formato:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	O	Alfanumerico 16 caratteri fissi	0000000050242004	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	O	Alfanumerico 20 caratteri fissi	T000000000000000000000001	codice univoco che identifica l'ordine dell'esercente
HTML_CODE	O	Alfanumerico		Codice html da restituire al browser dell'acquirent e per redirigerlo verso l'applicativo dell'Issuer.
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DE D95C7EE8C5507A 9E1F2970BCFE	Codice di sicurezza

- **MAC:** i campi utilizzati per il calcolo del MAC di questo messaggio sono:
 - TERMINAL_ID
 - TRANSACTION_ID
 - HTML_CODE
 - Chiave per MAC

Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<TERMINAL_ID>0000000050242004</TERMINAL_ID>
<AUTHRES>
<TRANSACTION_ID>T000000000000000000000001</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
<html>
<head></head>
<body onLoad='onLoadHandler();'>
```

```

<form name="pareqform"
action="https://www.isuer.it/pareq/3ba191706590dcac020134afc6620577a3bc50
7ddcfcece88/3ds/vereqauthid=4d5441774d4441784d6a4133" method="POST">
<noscript><br><br><center><!--<h1>3D secure Transaction</h1><h3>Submit to
continue</h3>--><h1>Transazione 3D-Secure</h1><h3>Submit per
continuare</h3>
<input type="submit" value="Submit"/></center></noscript>
<input type="hidden" name="PaReq"
value="eNpVUmlvgjAQ/r5fQfguLS8OMEcNiptkwshkS/aRlEZJBLTAdPvlaxHmvKTJPXfXe+
6eFuaX8qB8Md4UdeWpuoZVhVW0zotq56nv6dPEUefkAdI9ZyzYMtpxRiBiTZPtMFLknhq+JpM
XY7PdiLOIT6NNnMS0TESlkPhv7ERg4CCCQjMAjVD04nSfVS2BjJ4WYUysqem6NqABQsl4GBAH
Y/yIR9MBXcNQZSUjsZgqH+HWB9RDoHVXtftybMA4GNALo+IHS2/Y4Q+h8Pms0423WFFrRApIpQ
LdRkk56jWhlKXISp59m/EPvThT45yhYeYBkBerZy4iB8RS7+lTB9swyZ4YJqI9DVsoZCNawK/
a6AjhKdn/I3ExU/M+AUJyLF/kmru2IZUYE7HKsKyYqhJh/PuSsoSTyl8t1GPtKED6Hqb9ZiTl
kHNBtr+VaCk5boaHeK2pgWzqWZRM2IdXvc5KmeOJhR9d7HgkAydtoeFg0/Abh3f2SX/mGwEM=
"/>
<input type="hidden" name="MD" value="EI4FEI4AAAAA514TEST000000000000-
3500500000900047"/>
<input type="hidden" name="TermUrl" value="https://www.X-
PAY.it/VPOSVPOS/responseACS.jsp"/>
</form></body><SCRIPT language='javascript' function
onLoadHandler(){document.pareqform.submit(); } </script></html>
]]>
</HTML_CODE>
</AUTHRES>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>

```

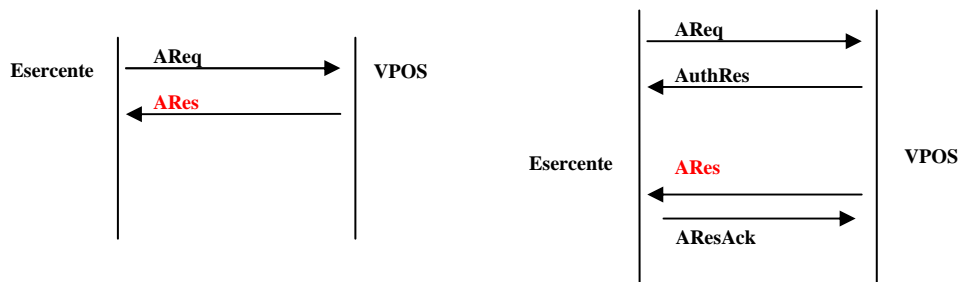
n.b.

gli elementi in *italico* non fanno parte dell'html da restituire al browser del titolare, indicano al parser xml di ignorare il contenuto del tag in quanto contiene caratteri specifici del protocollo xml.

10.4.3. Formato del messaggio ARes

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



X-PAY fornirà all' esercente il risultato del pagamento in 2 modalità differenti a seconda che sia avvenuta o meno la fase d'autenticazione

- Fase d'autenticazione non avvenuta
Il messaggio ARes viene inoltrato usando la stessa connessione con cui è stato ricevuto il messaggio AReq
- Fase d'autenticazione avvenuta
Il messaggio ARes viene inoltrato da X-PAY tramite una chiamata server to server al NotificationURL indicato dall'esercente nel messaggio AReq, al termine della fase d'autenticazione e del successivo pagamento. Inoltre, quando reindirige il browser dell'acquirente verso il ResultURL (comunicato dall'esercente nel messaggio di apertura dell'ordine) X-PAY inoltra una copia del messaggio ARes.

La seguente tabella descrive i campi inclusi nel messaggio:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	000000005024 2004	Codice identificativo dell'esercente all'interno della piattaforma X- PAY
TRANSACTION_ID	0	Alfanumerico 20 caratteri fissi	T00000000000 00000001	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
REQUEST_TYPE	0	Alfanumerico 2 caratteri fissi	FA	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
RESPONSE	0	Alfanumerico Massimo 3 caratteri	0	Risultato del pagamento richiesto, per i possibili valori vedere tabella sottostante
AUTH_CODE	0	Alfanumerico Massimo 10 caratteri	098765	E' il codice Autorizzazione ottenuto dall'emittente della carta di credito. In caso di pagamento con esito negativo

Nome parametro	Obb	Formato	Esempio	Descrizione
				sarà spedita una stringa vuota. Il campo può contenere degli spazi sono da considerare per effettuare operazioni sull'ordine.
AMOUNT	0	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2 decimali)	000123056 (per indicare una transazione di 1230,56 €)	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
CURRENCY	0	Alfanumerico 3 caratteri fissi	978	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
TRANSACTION_DATE	0	Alfanumerico 19 caratteri fissi Formato gg/mm/aaaa hh.mm.ss	06/07/2005 16.55.56	Data della transazione
TRANSACTION_TYPE	0	Alfanumerico Massimo 20 caratteri	VBV_FULL	Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice A2 per i possibili valori. In caso di pagamento con esito negativo sarà spedita una stringa vuota
REGION	F	Alfanumerico massimo 50 caratteri	Europe	Regione di appartenenza della carta. E' presente nel

Nome parametro	Obb	Formato	Esempio	Descrizione
				<p>messaggio solo se la transazione è richiesta con carte appartenenti ai circuiti VISA e MASTERCARD e nel corrispondente messaggio AREQ di richiesta è stato inserito il tag facoltativo Liability</p>
COUNTRY	F	Alfanumerico massimo 50 caratteri	Italy	<p>Paese di emissione della carta.</p> <p>E' presente nel messaggio solo se nel corrispondente messaggio AREQ di richiesta è stato inserito il tag facoltativo Liability</p> <p>Nel caso di transazione con carta appartenente al circuito AMEX, il campo può assumere solo i seguenti valori: "ITALY", "NO ITALY"</p>
PRODUCT_TYPE	F	Alfanumerico massimo 50 caratteri	Consumer	<p>Tipologia di Prodotto.</p> <p>E' presente nel messaggio solo</p>

Nome parametro	Obb	Formato	Esempio	Descrizione
				<p>se la transazione è richiesta con carte appartenenti ai circuiti VISA e MASTERCARD e nel corrispondente messaggio AREQ di richiesta è stato inserito il tag facoltativo Liability</p>
LIABILITY_SHIFT	F	Alfanumerico massimo un carattere ("", "N")	N	<p>Flag che definisce se la transazione è in Liability Shift. La risposta "N" definisce che per questa transazione non si applica la regola di trasferire la responsabilità dall'Acquirer all'Issuer.</p> <p>E' presente nel messaggio solo se nel corrispondente messaggio AREQ di richiesta è stato inserito il tag facoltativo Liability</p> <p>Nel caso di transazione con carta appartenente al circuito AMEX, il campo assume</p>

Nome parametro	Obb	Formato	Esempio	Descrizione
				il valore "N.A."
MAC	0	Alfanumerico 40 caratteri fissi	70C4F1F621A5 DED95C7EE8C5 507A9E1F2970 BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - RESPONSE
 - AUTH_CODE
 - AMOUNT
 - CURRENCY
 - Chiave per MAC

NB: il calcolo del MAC è fondamentale per l'esito **RESPONSE=0**, in caso di esiti 1 e 16 essendoci un errore formale o il codice **TERMINAL_ID** non è riconoscibile nel messaggio XML ricevuto dall'esercente il calcolo del MAC non è attendibile.

- **RESPONSE:** Risultato del pagamento richiesto, può assumere i seguenti valori:

Codice	Descrizione
0	Pagamento eseguito correttamente
1	Errore nel pagamento : Formato del messaggio errato o campo mancante o errato
3	Errore nel pagamento: Campo TRANSACTION_ID duplicato (caso "FA") o non trovato (caso "RA")
16	Errore nel pagamento: Campo TERMINAL_ID sconosciuto o non abilitato
18	Errore nel pagamento : pagamento rifiutato dall'ente emittente della carta di credito
2	Errore nel pagamento: Errore imprevisto durante l'elaborazione della richiesta
8	Errore nel pagamento: MAC errato
19	Errore nel pagamento : Autenticazione VbV/SC fallita, pagamento non inoltrato
20	Errore nel pagamento : Autenticazione VbV/SC non possibile, pagamento non inoltrato
17	Errore nel pagamento: Massimo numero di operazioni concesse nel caso RA (*)

22	Errore nel Pagamento: Esercente non convenzionato con il circuito della carta di credito proposta
00	Autorizzazione già avvenuta nel tentativo precedente
40	Ticket già utilizzato
001	Tasso di cambio scaduto
010	Esercente non abilitato al servizio DCC

(*) Il numero massimo di operazione concesse viene impostato dalla piattaforma di pagamento

Esempio di pagamento positivo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <ARES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>0</RESPONSE>
    <AUTH_CODE>098765</AUTH_CODE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
    <TRANSACTION_TYPE>VBV_FULL</TRANSACTION_TYPE>
    <REGION>Europe</REGION>
    <COUNTRY>Italy</COUNTRY>
    <PRODUCT_TYPE>Consumer</PRODUCT_TYPE>
    <LIABILITY_SHIFT>N</LIABILITY_SHIFT>
  </ARES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Esempio di pagamento negato:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <ARES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>21</RESPONSE>
    <AUTH_CODE></AUTH_CODE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
    <TRANSACTION_TYPE></TRANSACTION_TYPE>
  </ARES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

In caso di errori di comunicazione nell'inoltro del messaggio ARes, X-PAY inoltrerà un'e-mail comunicata dall'esercente a CartaSi in fase di adesione al servizio. L'email conterrà gli stessi dati del messaggio ARes e ne sostituirà definitivamente l'invio. L'e-mail avrà sempre lo stesso formato e sintassi, così da poter essere facilmente processata da parte degli applicativi dell'esercente.

Nel caso in cui il messaggio di richiesta AReq contenga il tag opzionale LIABILITY, l'e-mail conterrà a sua volta i dati relativi alla funzionalità di LIABILITY SHIFT.

Di seguito viene riportata la sintassi utilizzata:

Oggetto e-mail:

ARes - TRANSACTION_ID

Testo e-mail:

TERMINAL_ID:

TRANSACTION_ID:

REQUEST_TYPE:

RESPONSE:

AUTH_CODE:

AMOUNT:

CURRENCY:

TRANSACTION_DATE:

TRANSACTION_TYPE:

MAC:

REGION:

COUNTRY:

PRODUCT_TYPE:

LIABILITY_SHIFT:

Esempio di email:

ARes - T00000000000000000001

TERMINAL_ID: 0000000050242004

TRANSACTION: T00000000000000000001

REQUEST_TYPE: FA

RESPONSE: 0

AUTH_CODE: 098765

AMOUNT: 000123056

CURRENCY: 978

TRANSACTION_TYPE: VBV_FULL

MAC: 70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE

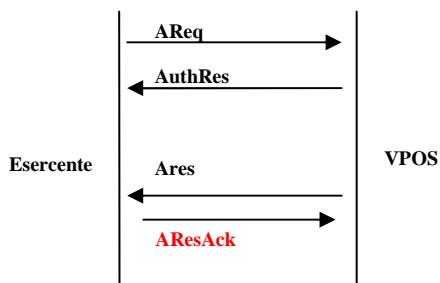
REGION: Europe

COUNTRY: Italy
 PRODUCT_TYPE: Consumer
 LIABILITY_SHIFT: N

10.4.4. Formato del messaggio AResAck

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Rappresenta il messaggio inoltrato dall' esercente a X-PAY come risposta all'avvenuta ricezione del messaggio ARes, quando questo messaggio viene inviato dopo la fase d'autenticazione Verified by Visa/Secure Code. Il messaggio contiene solo un campo:

Nome parametro	Obb	Formato	Esempio	Descrizione
RESPONSE	0	Alfanumerico Massimo 3 caratteri	0	Codice di esito dell'elaborazione del messaggio AResAck, per i relativi codici vedere la tabella sottostante.

- RESPONSE : risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

Codice	Descrizione
0	Operazione elaborata correttamente

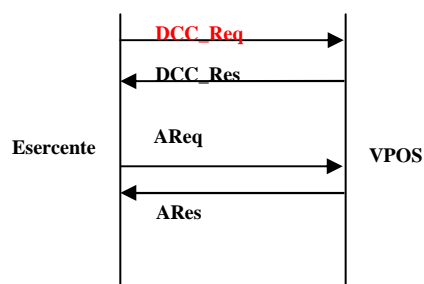
Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<ARESACK>
  <RESPONSE>0</RESPONSE>
</ARESACK>
```

10.4.5. Formato del messaggio DCCReq

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Per il servizio DCC è necessario prevedere una fase preparatoria al processo standard.

DCCReq rappresenta il messaggio di richiesta del servizio DCC (Dynamic Currency Conversion) che l'applicativo dell'esercente deve inoltrare a X-PAY, per conoscere la disponibilità, a fronte della carta inserita dal titolare, dell'eventuale valuta associata e del relativo controvalore, tramite una chiamata server to server e deve contenere i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	0000000050242004	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
PAN	0	Alfanumerico massimo 19 caratteri	1234567890123456	Numero della carta soggetta alla richiesta di pagamento. Controllo formale sul PAN è in carico all'esercente

Nome parametro	Obb	Formato	Esempio	Descrizione
AMOUNT	0	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2 decimali e non è usato il separatore tra parti intere e parti decimali)	000123056 (per indicare una transazione di 1230,56 €)	importo del pagamento richiesto
USER	F	Alfanumerico massimo 20 caratteri	User001	Operatore dell'esercente che ha richiesto l'operazione (solo per MOTO)
MAC	0	Alfanumerico 40 caratteri fissi	70C4F1F621A5DED9 5C7EE8C5507A9E1F 2970BCFE	Codice di sicurezza

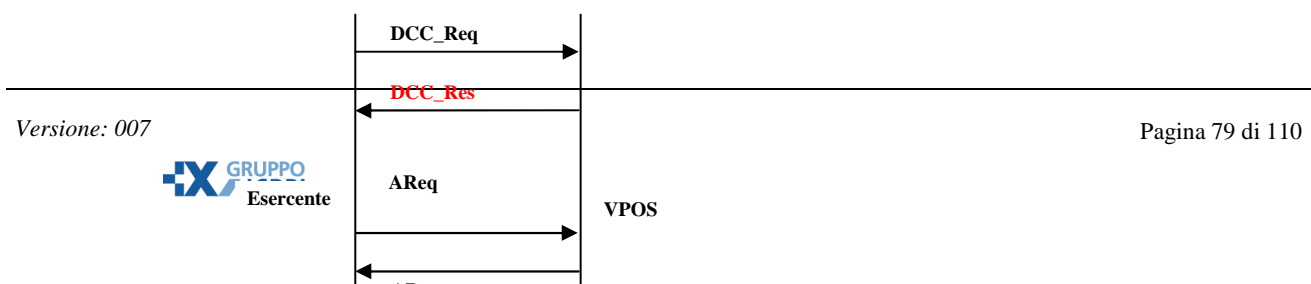
Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <DCCREQ>
    <PAN>1234567890123456</PAN>
    <AMOUNT>000123056</AMOUNT>
  </DCCREQ>
  <USER>User001</USER>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

10.4.6. Formato del messaggio DCCRes

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



X-PAY fornisce all' esercente il risultato alla richiesta del servizio DCC in 2 modalità differenti a seconda che sia disponibile o non disponibile il servizio DCC

- Servizio DCC disponibile

Il messaggio DCCRes viene costruito come segue:

```
<xml version=\"1.0\" encoding=\"ISO-8859-15\">
  <VPOSRES>
    <TERMINAL_ID>FIELD_TERMINAL_ID</TERMINAL_ID>
    <DCCRES>
      <RESPONSE>FIELD_RESPONSE</RESPONSE>
      <TICKET>FIELD_TICKET</TICKET>
      <CURRENCY_DCC>FIELD_CURRENCY_DCC</CURRENCY_DCC>
      <AMOUNT_DCC>FIELD_AMOUNT_DCC</AMOUNT_DCC>
      <EXCHANGE_RATE>FIELD_EXCHANGE_RATE</EXCHANGE_RATE>
      <EXCHANGE_RATE_EXPIRE>FIELD_EXPIRE</EXCHANGE_RATE_EXPIRE>
      <MARK_UP>FIELD_MARK_UP</MARK_UP>
      <MARK_UP_DEC>FIELD_PRECISION</MARK_UP_DEC>
    </DCCRES>
    <MAC>FIELD_MAC</MAC>
  </VPOSRES>
```

- Servizio DCC non disponibile

Il messaggio DCCRes viene costruito come segue

```
<?xml version=\"1.0\" encoding=\"ISO-8859-15\"?>
  <VPOSRES>
    <TERMINAL_ID>FIELD_TERMINAL_ID</TERMINAL_ID>
    <DCCRES>
      <RESPONSE>FIELD_RESPONSE</RESPONSE>
    </DCCRES>
    <MAC>FIELD_MAC</MAC>
  </VPOSRES>
```


La seguente tabella descrive i campi inclusi nel messaggio:

Nome parametro	Obb	Formato	Esempio	Descrizione
RESPONSE	0	Alfanumerico Massimo 3 caratteri	0	Risultato del servizio DCC richiesto, per i possibili valori vedere tabella sottostante
TICKET	0	Alfanumerico di 25 caratteri	1214390171406_A PI	Numero del ticket della richiesta del servizio DCC
CURRENCY_DCC	0	Alfanumerico di lunghezza 3	USD	Codice divisa estera (USD, JPY...)
AMOUNT_DCC	0	Alfanumerico di lunghezza 9	000012345	Importo nella valuta scelta dal titolare Esempi formato: 000012345 JPY = 12345 JPY 000012345 USD = 123, 45 USD (la divisa JPY non ha decimali)
EXCHANGE_RATE	0	Numerico (8,4)	999.9999	Tasso di cambio applicato
EXCHANGE_RATE_EXPIRE	0	Data	20080712110059	Data e orario di scadenza tasso di cambio
MARK_UP	0	Numerico (8,4)	999.9999	
MARK_UP_DEC	0	Numerico di lunghezza 1	4	Cifre decimali mark-up
MAC	0	Alfanumerico 40 caratteri fissi	70C4F1F621A5 DED95C7EE8C5 507A9E1F2970 BCFE	Codice di sicurezza

- RESPONSE - Questo campo può assumere i seguenti valori:

Codice	Descrizione
000	DCC disponibile

001	DCC non disponibile (per esercente abilitato al DCC)
010	Esercente non abilitato al DCC

Esempio:

- **n.1** - Caso servizio Dcc disponibile:

```
<xml version=\"1.0\" encoding=\"ISO-8859-15\">
  <VPOSRES>
    <TERMINAL_ID>FIELD_TERMINAL_ID</TERMINAL_ID>
    <DCCRES>
      <RESPONSE>000</RESPONSE>
      <TICKET>123459771149_API</TICKET>
      <CURRENCY_DCC>USD</CURRENCY_DCC>
      <AMOUNT_DCC>000012345</AMOUNT_DCC>
      <EXCHANGE_RATE>10.09</EXCHANGE_RATE>
      <EXCHANGE_RATE_EXPIRE>20081008120611</EXCHANGE_RATE_EXPIRE>
      <MARK_UP>2.60</MARK_UP>
      <MARK_UP_DEC>2</MARK_UP_DEC>
    </DCCRES>
    <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
  </VPOSRES>
```

- **n.2** - Caso servizio DCC non disponibile:

```
<?xml version=\"1.0\" encoding=\"ISO-8859-15\"?>
  <VPOSRES>
    <TERMINAL_ID>FIELD_TERMINAL_ID</TERMINAL_ID>
    <DCCRES>
      <RESPONSE>001</RESPONSE>
    </DCCRES>
    <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
  </VPOSRES>
```

10.5. Integrazione messaggi server to server per esercenti che usano un proprio MPI

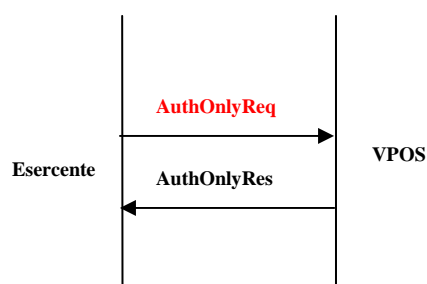
In questo paragrafo viene descritto il messaggio messo a disposizione degli applicativi dell'esercente che utilizza la piattaforma VPOS di CartaSi per l'invio delle richieste di autorizzazione. In questo caso l'esercente è dotato di un MPI

(Merchant Plug In) e gestisce la fase di autenticazione del titolare.

10.5.1. Formato del messaggio AuthOnlyReq

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Rappresenta il messaggio di richiesta di autorizzazione che l'applicativo dell'esercente deve inoltrare al VPOS tramite una chiamata server to server e deve contenere i seguenti campi:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	O	Alfanumerico 16 caratteri fissi	00000000502420 04	Codice identificativo dell'esercente all'interno della piattaforma VPOS
TRANSACTION_ID	O	Alfanumerico 20 caratteri fissi	T0000000000000 000001	codice univoco che identifica l'ordine dell'esercente
REQUEST_TYPE	O	Alfanumerico 2 caratteri fissi	FA	Valori Possibili: FA: Primo Tentativo RA :Retry di richiesta di pagamento
PAN	O	Alfanumerico massimo 19 caratteri	12345678901234 56	Numero della carta soggetta alla richiesta

Nome parametro	Obb	Formato	Esempio	Descrizione
				di pagamento
EXPIRE_DATE	O	Alfanumerico 4 caratteri fissi Formato : YYMM	0605 (per indicare come data di scadenza il maggio 2006)	Data di scadenza della carta soggetta alla richiesta di pagamento
CVV2	F	Alfanumerico Massimo 4	1234	Codice di sicurezza della carta soggetta alla richiesta di pagamento NB: Il TAG <CVV2> all'interno dell'XML di richiesta deve essere SEMPRE presente. La valorizzazione del tag è, invece, facoltativa.
AMOUNT	O	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2 decimali e non è usato il separatore tra parti intere e parti decimali)	000123056 (per indicare una transazione di 1230,56 €)	importo del pagamento richiesto
CURRENCY	O	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta del pagamento, vedere l'Appendice A3 per i possibili valori

Nome parametro	Obb	Formato	Esempio	Descrizione
ECI	F	Alfanumerico 2 fisso	30	Electronic Commerci Indicator
XID	F	28 byte base 64 encoding fisso	20002232324ER2345678	Identificativo dell'ordine
CAVV	F	28 byte base 64 encoding fisso	12345655545454QWE1QWQWERDFSA	Cardholder Authentication verification value
VERSION_CODE	O	Alfanumerico 5 caratteri fissi	01.00	Versione software della piattaforma di pagamento VPOS utilizzata, la versione a cui si riferisce il presente documento è la 01.00
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE	Codice di sicurezza

- **TRANSACTION_ID:** identifica univocamente l'ordine dell'esercente. Non è obbligatorio avere una progressione di valori regolare.

- **REQUEST_TYPE:**

L'esercente può inviare una richiesta di pagamento per un dato ordine più volte solo per uno dei seguenti motivi:

- o perdita della risposta al messaggio AuthOnlyReq, per Time-Out o altri motivi

L'esercente deve inviare il primo messaggio AuthOnlyReq relativo ad un determinato ordine valorizzando ad "FA" il campo REQUEST_TYPE, mentre per gestire un nuovo tentativo può inoltrare nuovamente un AuthOnlyReq utilizzando lo stesso TRANSACTION_ID ma valorizzando ad "RA" il campo REQUEST_TYPE.

In questo caso il VPOS restituisce lo stesso esito che ha restituito per la prima richiesta di pagamento dell'esercente.

Se l'esercente effettua un retry del pagamento di un dato ordine, il nuovo messaggio deve contenere esattamente gli stessi valori del primo messaggio, gli unici campi per i quali è ammessa una variazione è il campo REQUEST_TYPE.

In ogni caso il valore del campo TRANSACTION_ID non potrà essere duplicato per diverse Richieste AuthOnlyReq con il campo

REQUEST_TYPE valorizzato ad "FA". In questo caso la transazione verrà rifiutata dal VPOS.

Il Timeout, o qualsiasi situazione riprovata, devono essere sempre gestite dall'applicativo dell'esercente utilizzando questa tecnica di retry, al fine di evitare di abbattere inutilmente il Plafond della carta del compratore a causa di problemi tecnici a lui non imputabili.

- **ECI, XID e CAVV** parametri non obbligatori. La valorizzazione di questi tre campi avviene se la transazione è 3D-SECURE Di seguito viene riportata la corretta valorizzazione:

3D Secure

VISA		Eci	Cavv	Xid
VERes	N	30	NO	NO
VERes	U	20	NO	NO
PARes	Y	11	SI	SI
PARes	A	31	SI	SI
PARes	N	00	NO	NO
PARes	U	20	NO	NO
MasterCard/Maestro				
VERes	N	30	NO	NO
VERes	U	30	NO	NO
PARes	Y	11	SI	SI
PARes	A	30	NO	NO
PARes	N	30	NO	NO
PARes	U	30	NO	NO

SSL

		Eci	Cavv	Xid
		20	NO	NO

Mess. Secure	3D	VERes	Transaction
	N		Card not enrolled
	U		Unable to supply status / no response

Mess. Secure	3D	PARes	
	Y		CH passed authentication

	A	Attempt
	N	CH Failed authentication
	U	Unable to authenticate CH/ no response

Nella seguente tabella viene riportata la corretta valorizzazione del campo ECI per i circuiti VISA e MASTERCARD:

VISA	Pos 1	Pos 2	MasterCard	Pos 1	Pos 2
6	3	0	XX1	3	0
6	3	1	XX1	3	0
5	1	1	XX2	1	1
7	2	0	XX2	1	0
Not Authorized	0	0	XX0	2	0

- **MAC:** i campi utilizzati per il calcolo del MAC di questo messaggio sono:
 - TERMINAL_ID
 - TRANSACTION_ID
 - PAN
 - EXPIRE_DATE
 - CVV2
 - AMOUNT
 - CURRENCY
 - ECI
 - XID
 - CAVV
 - VERSION_CODE

Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <AUTHONLYREQ>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <PAN>1234567890123456</PAN>
    <EXPIRE_DATE>0605</EXPIRE_DATE>
    <CVV2>123</CVV2>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <ECI>30</ECI>
```



```

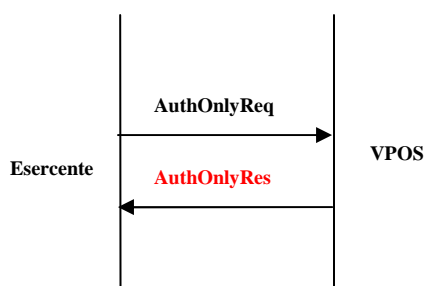
<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
<VERSION_CODE>01.00</VERSION_CODE>
</AUTHONLYREQ>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>

```

10.5.2. Formato del messaggio AuthOnlyRes

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL



Questo messaggio viene restituito dalla piattaforma VPOS in risposta al messaggio AuthOnlyReq utilizzando la stessa connessione con cui è stato ricevuto tale messaggio e contiene l'esito dell'operazione di autorizzazione richiesta.

La seguente tabella elenca i parametri che il VPOS includerà nel messaggio:

La seguente tabella descrive i campi inclusi nel messaggio:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	000000005024 2004	Codice identificativo dell'esercente all'interno della piattaforma VPOS
TRANSACTION_ID	0	Alfanumerico 20 caratteri fissi	T00000000000 00000001	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
REQUEST_TYPE	0	Alfanumerico 2 caratteri fissi	FA	Valorizzato con lo stesso valore ricevuto nel

Nome parametro	Obb	Formato	Esempio	Descrizione
				messaggio AReq
RESPONSE	O	Alfanumerico Massimo 3 caratteri	0	Risultato del pagamento richiesto, per i possibili valori vedere tabella sottostante
AUTH_CODE	O	Alfanumerico Massimo 10 caratteri	098765	E' il codice Autorizzazione ottenuto dall'emittente della carta di credito. In caso di pagamento con esito negativo sarà spedita una stringa vuota
AMOUNT	O	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2 decimali)	000123056 (per indicare una transazione di 1230,56 €)	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
CURRENCY	O	Alfanumerico 3 caratteri fissi	978	Valorizzato con lo stesso valore ricevuto nel messaggio AReq
ECI	F	Alfanumerico 2 fisso	30	Electronic Commerci Indicator
XID	F	Alfanumerico 20 fisso	20002232324E R2345678	Identificativo dell'ordine
CAVV	F	28 byte base 64 encoding fisso	123456555454 54QWE1QWQWER DFSA	Cardholder Autentication verification value
TRANSACTION_DATE	O	Alfanumerico 19 caratteri fissi Formato gg/mm/aaaa hh.mm.ss	06/07/2005 16.55.56	Data della transazione
TRANSACTION_TY	O	Alfanumerico	VBV_FULL	Tipo di

Nome parametro	Obb	Formato	Esempio	Descrizione
PE		Massimo 20 caratteri		transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice A2 per i possibili valori. In caso di pagamento con esito negativo sarà spedita una stringa vuota
MAC	0	Alfanumerico 40 caratteri fissi	70C4F1F621A5 DED95C7EE8C5 507A9E1F2970 BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - RESPONSE
 - AUTH_CODE
 - AMOUNT
 - CURRENCY
- **RESPONSE**: Risultato del pagamento richiesto, può assumere i seguenti valori:

Codice	Descrizione
0	Pagamento eseguito correttamente
1	Errore nel pagamento : Formato del messaggio errato o campo mancante o errato
3	Errore nel pagamento: Campo TRANSACTION_ID duplicato (caso "FA") o non trovato (caso "RA")
16	Errore nel pagamento: Campo TERMINAL_ID sconosciuto o non abilitato
18	Errore nel pagamento : pagamento rifiutato dall'ente emittente della carta di credito
2	Errore nel pagamento: Errore imprevisto durante l'elaborazione della richiesta
8	Errore nel pagamento: MAC errato

17	Max numero di operazioni concesse caso RA (*)
----	---

(*) Il numero massimo di operazione concesse viene impostato dalla piattaforma di pagamento

Esempio di pagamento positivo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <AUTHONLYRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>0</RESPONSE>
    <AUTH_CODE>098765</AUTH_CODE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
    <TRANSACTION_TYPE>VBV_FULL</TRANSACTION_TYPE>
    <ECI>30</ECI>
    <XID>20002232324ER2345678</XID>
    <CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
  </AUTHONLYRES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Esempio di pagamento negato:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <AUTHONLYRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>21</RESPONSE>
    <AUTH_CODE></AUTH_CODE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
    <TRANSACTION_TYPE></TRANSACTION_TYPE>
    <ECI>30</ECI>
```

```

<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
</AUTHONLYRES>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>

```

10.6. Operazioni dispositive e di interrogazione

In questo paragrafo vengono descritti i messaggi messi a disposizione degli applicativi dell'esercente per richiedere un'operazione dispositiva o eseguire delle interrogazioni per conoscere la situazione di un ordine.

I messaggi server to server sono utilizzabili indipendentemente dalla modalità con cui è stata inoltrata dall'esercente la richiesta di pagamento (modalità FULL, LIGHT o server to server).

10.6.1. **Formato del messaggio ECRReq**

Modalità d'integrazione : server to server

Tipologia del messaggio : xml inviato tramite post http in modalità SSL

Questo messaggio deve essere inviato dall'applicativo dell'esercente per effettuare richieste di contabilizzazione, annullamento o storno contabile di una transazione per la quale ha precedentemente effettuato un pagamento con esito positivo.

Il messaggio deve avere il seguente formato:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico 16 caratteri fissi	00000000502420 04	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	0	Alfanumerico 20 caratteri fisso	T0000000000000 000001	codice univoco identificativo dell'ordine

Nome parametro	Obb	Formato	Esempio	Descrizione
				attribuito da X-PAY o dall'esercente (dipende dalla modalità d'integrazione scelta dall'esercente)
REQUEST_TYPE	O	Alfanumerico 2 caratteri fissi	FA	Valori Possibili: FA: Primo Tentativo RA :Retry di richiesta di pagamento
ID_OP	O	Numerico Max 10	123	Identificativo univoco dell'operazione e richiesta, l'identificativo è unico per tutti i tipi di operazione
TYPE_OP	O	Alfanumerico 1 carattere fisso	C	Tipo di operazione richiesta, per i possibili valori vedere tabella sottostante
AMOUNT	O	Alfanumerico 9 caratteri fisso	000123056 (per indicare 1230,56 €)	Importo per cui è stata precedentemente e richiesta l'autorizzazione al pagamento
CURRENCY	O	Alfanumerico 3 caratteri fissi	978	Codice ISO della valuta con cui è stata precedentemente e richiesta l'autorizzazione al

Nome parametro	Obb	Formato	Esempio	Descrizione
				pagamento.
AUTH_CODE	0	Alfanumerico Massimo 10 caratteri	098765	Codice di autorizzazione ricevuto dall'esercente in risposta alla richiesta di pagamento
AMOUNT_OP	0	Alfanumerico 9 caratteri fisso	000120056 (per indicare una transazione di 1200,56 €)	Importo che l'esercente vuole sia soggetto sia all'operazione indicata, quindi il base al tipo di operazione richiesta è l'importo da contabilizzare /annullare/stornare.
USER	F	Alfanumerico massimo 20 caratteri	User001	Operatore dell'esercente che ha richiesto l'operazione
MAC	0	Alfanumerico 40 caratteri fissi	70C4F1F621A5DE D95C7EE8C5507A 9E1F2970BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - ID_OP
 - TYPE_OP
 - AMOUNT
 - CURRENCY
 - AUTH_CODE
 - AMOUNT_OP
 - USER
 - Chiave per MAC

- **AUTH_CODE:** Valore ricevuto dall'esercente quanto ha inoltrato la richiesta di pagamento, il campo può contenere degli spazi non dev'essere effettuato il trim ma utilizzato il campo così come passato da X-Pay nel messaggio ARES.
- **TYPE_OP:** i tipi di operazione dispositiva gestiti da X-PAY attraverso questo messaggio sono i seguenti:

Codice	Descrizione
R	Annullamento della transazione Questa operazione ha come effetto quello di ripristinare il plafond della carta utilizzata dall'acquirente, se l'ente emittente della carta di credito supporta tale funzionalità. L'importo da annullare deve essere minore o uguale all'importo per cui è stato richiesto il pagamento, al quale vanno sottratti gli eventuali importi per cui è stata precedentemente richiesta la contabilizzazione o l'annullamento.
P	Contabilizzazione Questa operazione conferma la transazione precedentemente autorizzata e ne rende effettivo l'incasso, cioè l'accredito dell'importo all'esercente ed il conseguente addebito al titolare della carta di credito. L'importo da incassare deve essere minore o uguale all'importo per cui è stato richiesto il pagamento al quale vanno sottratti gli eventuali importi per cui è stata richiesta un'operazione di annullamento o di contabilizzazione.
C	Storno Contabile Questa operazione ha come effetto quello di addebitare l'importo indicato all'esercente e riaccreditare lo stesso importo sulla carta del titolare. L'importo da stornare deve essere minore o uguale alla somma degli importi per i quali è stato richiesto precedentemente la contabilizzazione dalla quale vanno sottratti gli eventuali importi per cui è già stato richiesto uno storno.

- **AMOUNT_OP:** Indicare l'importo effettivo da contabilizzare/annullare/stornare. Possono essere richieste diverse operazioni facendo riferimento al pagamento originario, purché si rispettino i seguenti limiti:
 - la somma complessiva degli importi annullati e contabilizzati deve essere uguale o minore all'importo autorizzato.

- la somma complessiva degli importi stornati deve essere uguale o minore alla somma degli importi contabilizzati.
- **ID_OP:** Contatore univoco che identifica la richiesta di operazione dispositiva inoltrata. In caso di perdita del risultato, per Time-Out o altri motivi, l'applicazione dell'esercente deve inoltrare nuovamente un ECREq usando lo stesso ID_OP e valorizzando ad "RA" il campo REQUEST_TYPE. In questo caso X-PAY restituirà lo stesso esito (negativo o positivo) dell'operazione precedentemente eseguita utilizzando il messaggio ECRes. In ogni caso il valore del campo ID_OP non potrà essere duplicato per diverse richieste con il campo REQUEST_TYPE valorizzato ad "FA". In questo caso l'operazione verrà rifiutata da X-PAY. Non è obbligatorio avere una progressione di valori regolare. In caso di RESPONSE=1 bisogna inoltrare nuovamente il messaggio con un nuovo ID_OP.

Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <ECREQ>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <ID_OP>0000000001</ID_OP>
    <TYPE_OP>C</TYPE_OP>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <AUTH_CODE>098765</AUTH_CODE>
    <AMOUNT_OP>000120056</AMOUNT_OP>
  </ECREQ>
  <USER>User001</USER>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

10.6.2. Formato del messaggio ECRes

Questo messaggio viene restituito da X-PAY in risposta al messaggio ECREq utilizzando la stessa connessione con cui è stato ricevuto tale messaggio e contiene l'esito dell'operazione richiesta.

La seguente tabella elenca i parametri che X-PAY includerà nel messaggio:

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	0	Alfanumerico o 16 caratteri fissi	0000000050242004	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	0	Alfanumerico o 20 caratteri fisso	T000000000000000000000001	Valore indicato nel messaggio EReq di riferimento
REQUEST_TYPE	0	Alfanumerico o 2 caratteri fisso	FA	Valore indicato nel messaggio EReq di riferimento
RESPONSE	0	Alfanumerico o Massimo 3 caratteri	0 (numero 0)	risultato dell'operazione richiesta. Per i possibili valori vedere tabella sottostante.
ID_OP	0	Numerico Max 10 caratteri	123444	Valore indicato nel messaggio EReq di riferimento
TYPE_OP	0	Alfanumerico o 1 carattere fisso	C	Valore indicato nel messaggio EReq di riferimento
AMOUNT_OP	0	Alfanumerico o 9 caratteri fisso	000120056 (per indicare una transazione di 1200,56 €)	Valore indicato nel messaggio EReq di riferimento
MAC	0	Alfanumerico o 40 caratteri fissi	70C4F1F621A5DED9 5C7EE8C5507A9E1F 2970BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio ed il relativo ordine sono i seguenti:
 - TERMINAL_ID
 - TRANSACTIONID
 - RESPONSE

- o ID_OP
- o TYPE_OP
- o AMOUNT_OP
- o Chiave per MAC

NB: il calcolo del MAC è fondamentale per l'esito **RESPONSE=0**, in caso di esiti 1 e 16 essendoci un errore formale o il codice **TERMINAL_ID** non è riconoscibile nel messaggio XML ricevuto dall'esercente il calcolo del MAC non è attendibile.

- **RESPONSE** : risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

Codice	Descrizione
0	Richiesta eseguita correttamente
1	Errore nella richiesta : Formato del messaggio errato o campo mancante o errato
3	Errore nella richiesta: Campo ID_OP duplicato (caso "FA") o non trovato (caso "RA")
16	Errore nella richiesta: Campo TERMINAL_ID sconosciuto o non abilitato
18	Errore nella richiesta : operazione negata dall'emittente della carta di credito
2	Errore nella richiesta: Errore imprevisto durante l'elaborazione della richiesta
8	Errore nella richiesta: MAC errato
21	Errore nell'operazione: Campo TRANSACTION_ID sconosciuto
22	Errore nell'operazione: operazione non eseguibile (es. storno superiore all'incasso)

Esempio di risultato positivo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <ECRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>0</RESPONSE>
    <ID_OP>0000000001</ID_OP>
    <TYPE_OP>C</TYPE_OP>
    <AMOUNT_OP>000120056</AMOUNT_OP>
  </ECRES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Esempio risultato negativo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <ECRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <REQUEST_TYPE>FA</REQUEST_TYPE>
    <RESPONSE>32</RESPONSE>
    <ID_OP>0000000001</ID_OP>
    <TYPE_OP>C</TYPE_OP>
    <AMOUNT_OP>000120056</AMOUNT_OP>
  </ECRES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

10.6.3. Formato del messaggio IntReq

Modalità d'integrazione : API

Tipologia del messaggio : xml inviato tramite post http in modalità SSL

Questo messaggio può essere utilizzato dall'applicativo dell'esercente per richiedere a X-PAY la situazione attuale di un ordine e lo stato di tutte le operazioni ad esso associate.

Nome parametro	Obb	Formato	Esempio	Descrizione
TERMINAL_ID	O	Alfanumerico 16 caratteri fissi	0000000050242004	Codice identificativo dell'esercente all'interno della piattaforma X-PAY
TRANSACTION_ID	O	Alfanumerico 20 caratteri fisso	T00000000000000000001	Codice univoco identificativo dell'ordine del quale l'esercente vuole conoscere la situazione.
ID_OP	O	Numerico Max 10	4343	Identificativo univoco dell'interrogazione richiesta

Nome parametro	Obb	Formato	Esempio	Descrizione
TYPE_OP	O	Alfanumerico 1 carattere fisso	V	Valorizzato sempre a V (Verifica stato ordine)
USER	F	Alfanumerico massimo 20 caratteri	User001	Operatore dell'esercente che ha richiesto l'interrogazione
MAC	O	Alfanumerico 40 caratteri fissi	70C4F1F621A5DED9 5C7EE8C5507A9E1F 2970BCFE	Codice di sicurezza

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio ed il relativo ordine sono i seguenti:
 - TERMINAL_ID
 - TRANSACTION_ID
 - ID_OP
 - TYPE_OP
 - USER
 - Chiave per MAC

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <INTREQ>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <ID_OP>0000000001</ID_OP>
    <TYPE_OP>V</TYPE_OP>
  </INTREQ>
  <USER>User001</USER>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

10.6.4. Formato del messaggio IntRes

Questo messaggio viene restituito da X-PAY in risposta al messaggio IntReq utilizzando la stessa connessione con cui è stato ricevuta la richiesta e contiene la lista delle operazioni che sono state richieste per l'ordine indicato con il relativo stato.

Il messaggio sarà costituito dai seguenti elementi:

- un elemento **TERMINAL_ID**, sempre presente, contenente il codice identificativo dell'esercente all'interno della piattaforma X-PAY
- un elemento **INTRES**, sempre presente, contenente i dati generali della transazione e la lista delle operazioni eseguite per la transazione indicata. La lista delle operazioni è contenuta nell'elemento di tipo **OPERATIONS_LIST**, sempre presente se il **TRANSACTION_ID** esiste, costituito da elementi di tipo **OPERATION** e da un attributo **NUMELM** che indica il numero di elementi di tipo **OPERATION** presenti nella lista (eventualmente 0 se la ricerca non ha dato alcun esito). La struttura dell'elemento **OPERATION** è dettagliata di seguito.

La lista conterrà un elemento di tipo **OPERATION** per ognuna delle operazioni che sono state richieste relativamente all'ordine indicato o attraverso uno dei messaggi di apertura dell'ordine **AReq/VPOSReqFull/VPOSReqLight** (che possono originare operazioni di tipo autorizzazione al pagamento e contabilizzazione) o attraverso un messaggio **ECReq** (che può originare operazioni di tipo contabilizzazione, annullamento, storno). La lista conterrà solo le operazioni che hanno avuto esito positivo.

- un elemento **MAC** sempre presente, contenente il codice di sicurezza del messaggio.

La struttura del messaggio **VPOSRes** per questa tipologia di risposta è descritta dalla seguente figura:

XPAYRES

TERMINAL_ID	
INTRES	
TRANSACTION_ID	
RESPONSE	
CARD_TYPE	
TRANSACTION_TYPE	
AMOUNT	
CURRENCY	
AUTH_CODE	
OPTION_NAME	
OPERATIONS_LIST	
NUMELM	
OPERATION	
ID_OP	
TYPE_OP	
AMOUNT_OP	
CURRENCY	
TIMESTAMP	
RESPONSE	
USER	
MAC	

La seguente tabella contiene la descrizione degli elementi che X-PAY includerà nel messaggio (escluso l'elemento OPERATIONS_LIST):

Nome parametro	Obb	Formato	Esempio	Descrizione
TRANSACTION_ID	0	Alfanumerico o 20 caratteri fisso	T000000000000 00000001	Valore indicato nel messaggio IntReq di riferimento
RESPONSE	0	Alfanumerico o Massimo 3 caratteri	0 (numero 0)	risultato dell'interrogazione richiesta. Per i possibili valori vedere tabella sottostante.
CARD_TYPE	0	Alfanumerico o Massimo 10 caratteri	VISA	Il tipo di carta utilizzata per il pagamento, vedere l'Appendice A1 per i possibili valori.
TRANSACTION_TYPE	0	Alfanumerico o Massimo 20 caratteri	VBV_FULL	Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice A2 per i possibili valori.
AMOUNT	0	Alfanumerico o 9 caratteri fisso	000123056 (per indicare 1230,56 €)	Importo della richiesta di pagamento.
CURRENCY	0	Alfanumerico o 3 caratteri fissi	978	Codice ISO della valuta della richiesta di pagamento.
AUTH_CODE	0	Alfanumerico o Massimo 10 caratteri	098765	Codice di autorizzazione della richiesta di pagamento.

- **RESPONSE** : risultato dell'operazione richiesta. Questo campo può assumere i seguenti valori:

Codice	Descrizione
0	Operazione elaborata correttamente

1	Errore nella ricerca: Formato del messaggio errato o campo mancante o errato
16	Errore nella ricerca: Campo TERMINAL_ID sconosciuto o non abilitato
2	Errore nella ricerca: Errore imprevisto durante l'elaborazione della richiesta
8	Errore nella ricerca: MAC errato
21	Errore nella ricerca: Campo TRANSACTION_ID sconosciuto (non esiste un pagamento con esito positivo associato all'ordine indicato) n.b. in tal caso gli elementi CARD_TYPE, TRANSACTION_TYPE, AMOUNT, CURRENCY, AUTH_CODE del messaggio conterranno una stringa vuota e gli elementi OPTION_FIELDS non saranno presenti.
3	Errore nella richiesta: Campo ID_OP duplicato
32	TRANSACTION_ID chiuso per time-out, l'utente non ha completato il pagamento entro 30 minuti dalla generazione dell'ordine.

La struttura dell'elemento OPERATION è la seguente:

Nome parametro	Obb	Formato	Esempio	Descrizione
ID_OP	0	Numerico Max 10	3343434	Valore indicato nel messaggio EReq che ha originato l'operazione o stringa vuota per operazioni di pagamento e/o contabilizzazione e derivate da un messaggio AReq o VPOSReqFull/VPOSReqLigth.
TYPE_OP	0	Alfanumerico o 1 carattere fisso	C	Tipo di operazione, per i possibili valori vedere tabella sottostante
AMOUNT_OP	0	Alfanumerico o 9 caratteri fisso	000123056 (per indicare 1230,56 €)	Importo dell'operazione

Nome parametro	Obb	Formato	Esempio	Descrizione
CURRENCY	O	Alfanumeric o 3 caratteri fissi	978	Codice ISO della valuta dell'operazione, vedere l'Appendice A3 per i possibili valori
TIMESTAMP	O	Alfanumeric o 19 caratteri fissi Formato gg/mm/aaaa hh.mm.ss	06/07/2005 16.55.56	Data in cui è stata eseguita l'operazione
RESULT	O	Alfanumeric o Massimo 3 caratteri	0	Stato dell'operazione, per i possibili valori vedere tabella sottostante
USER	F	Alfanumeric o massimo 20 caratteri	User001	Operatore dell'esercente che ha richiesto l'operazione

- **TYPE_OP:** i tipi di operazione gestiti da X-PAY sono i seguenti:

Codice	Descrizione
A	Autorizzazione al pagamento
R	Annullamento
P	Contabilizzazione
C	Storno Contabile

- **RESULT:** stato dell'operazione, può assumere i seguenti valori:

Codice	Descrizione
E	Eseguita, questo stato viene utilizzato per le operazioni di tipo autorizzazione e storno autorizzativo, che vengono eseguite immediatamente.
D	Da Inviare, questo stato viene utilizzato per le operazioni di tipo contabilizzazione e storno contabile.

	Queste operazioni infatti vengono prese in carico da X-PAY e successivamente rese effettive tramite la generazione di un file contabile che deve essere inviato all'ente emittente della carta di credito. L'operazione si trova in questo stato se non è ancora stata inserita in un file contabile.
I	Inviata, questo stato viene utilizzato per le operazioni di tipo contabilizzazione e storno contabile. L'operazione si trova in questo stato se è stata inserita in un file contabile.

- **MAC** : I parametri utilizzati per il calcolo del MAC per questo tipo di messaggio ed il relativo ordine sono i seguenti:
 - Campo `TERMINAL_ID`
 - Campo `TRANSACTION_ID` del tag `INTRES`
 - Campo `RESPONSE` del tag `INTRES`
 - Campo `AMOUNT` del tag `INTRES`
 - Campo `CURRENCY` del tag `INTRES`
 - Campo `AUTH_CODE` del tag `INTRES`
 - Campo `NUMELM` del tag `OPERATIONS_LIST`
 - Per ogni elemento `OPERATION` del tag `OPERATIONS_LIST` si considerano inoltre i seguenti campi:
 - Campo `ID_OP`
 - Campo `TYPE_OP`
 - Campo `AMOUNT_OP`
 - Campo `CURRENCY`
 - Campo `RESULT`
 - Campo `USER`

I tag `OPERATION` devono essere considerati nell'ordine in cui sono stati inseriti nel messaggio `VPOSRes` inoltrato da X-PAY.

NB: il calcolo del MAC è fondamentale per l'esito `RESPONSE=0`, in caso di esiti 1 e 16 essendoci un errore formale o il codice `TERMINAL_ID` non è riconoscibile nel messaggio XML ricevuto dall'esercente il calcolo del MAC non è attendibile.

Esempio di XML con esito positivo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
  <TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <INTRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <RESPONSE>0</RESPONSE>
    <CARD_TYPE>VISA</CARD_TYPE>
    <TRANSACTION_TYPE>VBV_FULL</TRANSACTION_TYPE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <AUTH_CODE>098765</AUTH_CODE>
    <OPERATIONS_LIST NUMELM="3">
      <OPERATION>
        <ID_OP></ID_OP>
        <TYPE_OP>A</TYPE_OP>
        <AMOUNT_OP>000123056</AMOUNT_OP>
        <CURRENCY>978</CURRENCY>
        <TIMESTAMP>06/07/2005 16.55.56</TIMESTAMP>
        <RESULT>E</RESULT>
        <USER>User001</USER>
      </OPERATION>
      <OPERATION>
        <ID_OP></ID_OP>
        <TYPE_OP>P</TYPE_OP>
        <AMOUNT_OP>000123056</AMOUNT_OP>
        <CURRENCY>978</CURRENCY>
        <TIMESTAMP>06/07/2005 16.56.20</TIMESTAMP>
        <RESULT>E</RESULT>
        <USER>User001</USER>
      </OPERATION>
      <OPERATION>
        <ID_OP>0000000001</ID_OP>
        <TYPE_OP>C</TYPE_OP>
        <AMOUNT_OP>000120056</AMOUNT_OP>
        <CURRENCY>978</CURRENCY>
        <TIMESTAMP>07/07/2005 16.56.20</TIMESTAMP>
        <RESULT>E</RESULT>
        <USER>User001</USER>
      </OPERATION>
    </OPERATIONS_LIST>
  </INTRES>
  <MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Esempio di XML con esito negativo

```
<VPOSRES>
<TERMINAL_ID>0000000050242004</TERMINAL_ID>
  <INTRES>
    <TRANSACTION_ID>T00000000000000000001</TRANSACTION_ID>
    <RESPONSE>22</RESPONSE>
    <CARD_TYPE>VISA</CARD_TYPE>
    <TRANSACTION_TYPE>VBV_FULL</TRANSACTION_TYPE>
    <AMOUNT>000123056</AMOUNT>
    <CURRENCY>978</CURRENCY>
    <AUTH_CODE>098765</AUTH_CODE>
  </INTRES>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Appendice A

A1 Carte accettate

La seguente tabella contiene i valori possibili per campo CARD_TYPE:

Codice
MAESTRO
VISA
MASTERCARD
AMEX

A2 Tipi di transazioni

La seguente tabella contiene i valori possibili per campo TRANSACTION_TYPE:

Codice	Descrizione
VBV_FULL	L'esercente è abilitato al protocollo Verified by Visa, il titolare della carta di credito è registrato al servizio e si è correttamente autenticato
SC_FULL	L'esercente è abilitato al protocollo Secure Code, il titolare della carta di credito è registrato al servizio e si è correttamente autenticato.
VBV_MERCHANT	L'esercente è abilitato al protocollo Verified by Visa, ma il titolare o l'ente emittente della carta di credito non partecipano al servizio.
SC_MERCHANT	L'esercente è abilitato al protocollo Secure Code, ma il titolare o l'ente emittente della carta di credito non partecipano al servizio.
NO_3DSECURE	L'esercente non è abilitato all'utilizzo dei protocolli di sicurezza Verified by Visa e Secure Code o non è stato possibile utilizzare i protocolli.

A3 Codici Divisa

La seguente tabella contiene i valori possibili per campo CURRENCY

Codice divisa numerico	Codice divisa alfanumerico	Descrizione
978	EUR	EURO
036	AUD	Australian Dollar
124	CAD	Canadian Dollar
344	HKD	Hong Kong Dollar
392	JPY	Japan Yen
756	CHF	Swiss Franc
826	GBP	Pound Sterling
840	USD	US Dollar

A4 Lingue supportate

La seguente tabella contiene i valori possibili per campo LANGUAGE

Codice	Descrizione
ITA	Italiano
ENG	Inglese
FRA	Francese
ESP	Spagnolo
DEU	Tedesco