Emesso da: CartaSi S.p.A.

Versione: 10.0

Emesso il: 04/03/2014

Specifiche tecniche di integrazione con il servizio di POS Virtuale

INDICE

1. Modifiche apportate 4

2. Introduzione 4

3. POS Virtuale 4

3.1. Soluzioni E-commerce WEB/Mobile 5
3.1.1. Front Office 5
3.1.2. Server to Server 6
3.1.3. Recurring Front Office 8
3.1.4. Recurring Server to Server 9
3.1.5. OneClickPay Front Office 10
3.1.6. OneClickPay Server to Server 10
3.1.7. Server to server con MPI MERCHANT 11

3.2. Soluzioni MOTO (Mail Order Telephone Order) 12
3.2.1. MOTO standard 12
3.2.2. MOTO Recurring standard 12
3.2.3. MOTO Server to server 13
3.2.4. MOTO Recurring Server to Server 14

3.3. Soluzioni Opzionali 15
3.3.1. MyBANK 15
3.3.2. Currency Choice 15
3.3.3. MCC (Multi Currency Conversion) 16
3.3.4. API Back Office 16

4. Messaggi 17

4.1. Firma dei messaggi 17

4.2. Struttura e Inoltro dei messaggi 17

4.3. Specifiche tecniche dei messaggi di pagamento 18
4.3.1. Messaggio avvio pagamento WEB Front Office 18
4.3.2. Messaggio esito pagamento WEB Front Office 25
4.3.3. Messaggio avvio pagamento Server to server 28
4.3.4. Messaggio AUTHRES gestione autenticazione 3D-Secure 32
4.3.5. Messaggio esito pagamento Server to server 35
4.3.6. Messaggio avvio pagamento AUTHONLYREQ 40
4.3.7. Messaggio esito pagamento AUTHONLYRES 43

4.4. Specifiche Messaggi operazioni dispositive e di interrogazione 46
4.4.1. Messaggio ECREQ 46
4.4.2. Messaggio ECRES 48
4.4.3. Messaggio INTREQ 50
4.4.4. Messaggio INTRES 51
4.4.5. Messaggio REPREQ 57

4.4.6. Messaggio REPRES 58

4.5. Messaggi opzione DCC 62
4.5.1. Messaggio verifica DCC Server to Server 62
4.5.2. Messaggio esito DCC Server to Server 63

5. Appendice 65

5.1. Codifica languageId 65

5.2. Codifica codici mccDivisa per DCC/MCC 65

5.3. Codifica tipo Transazione 66

5.4. Codifica messaggio dettaglio esito 67

5.5. Codifica tipo carta 68

5.6. Codifica codiceEsito e descrizioneEsito 68

1. Modifiche apportate

Versione	Data	Autore	Capitolo	Descrizione
10.0	**04/03/2014**	**Direzione POS e ATM**		Stesura

2. Introduzione

Il presente documento contiene le specifiche tecniche necessarie per integrare il proprio sito/gestionale con il servizio di POS Virtuale. Sono descritte brevemente le soluzioni offerte, il dettaglio tecnico dei messaggi del POS VIRTUALE, e la relativa integrazione coi sistemi di gestione ordini lato merchant.

Il documento è strutturato in due macro sezioni:

- la prima indica brevemente le soluzioni disponibili sul POS Virtuale e i messaggi necessari per essere integrate;
- la seconda evidenzia il dettaglio tecnico dei messaggi

La descrizione del servizio riportata ha lo scopo di inquadrare il contesto per gli addetti tecnici che dovranno effettuare l'integrazione dei sistemi merchant con il POS Virtuale.

3. POS Virtuale

Il POS Virtuale 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, anche su devices Mobile, e MOTO (Mail order – Telephone order).

Il sistema gestisce attualmente pagamenti con le carte appartenenti ai seguenti circuiti:

- Visa/Visa Electron
- MasterCard/Maestro
- American Express
- Diners
- Jcb (per il MOTO)

Il POS Virtuale gestisce, con gli acquirer abilitati (VISA, MASTERCARD, MAESTRO, Visa Electron e AMERICAN EXPRESS), le transazioni con i protocolli 3D Secure (3-Domain Secure) Verified by Visa, MasterCard Secure-Code e SafeKey American Express, che assicurano una maggiore tutela sugli acquisti in Internet in quanto, per concludere un pagamento, richiedono l'autenticazione del titolare della carta di credito.

L'elaborazione dei pagamenti autorizzati ai fini dell'accredito del corrispettivo viene, di norma, compiuto nel giorno lavorativo successivo a quello in cui il pagamento è avvenuto. E' facoltà del merchant posticipare la data dell'accredito dei movimenti, oppure stornare la transazione di pagamento qualora intervenissero ad esempio problemi logistici.

Per facilitare la gestione degli ordini, il POS VIRTUALE mette a disposizione dell'esercente lo strumento di Back office on-line, che permette di gestire le attività amministrative/controllo inerenti il negozio virtuale. Il Back office on-line è infatti un'Area Riservata al merchant, all'interno della quale, in modo semplice e rapido, è possibile consultare l'archivio dei pagamenti oltre a poterne disporre la contabilizzazione o lo storno. I codici di accesso al back office vengono forniti al merchant in fase di attivazione del servizio.

Nei seguenti capitoli vengono descritte le diverse soluzioni disponibili sul POS VIRTUALE

3.1. Soluzioni E-commerce WEB/Mobile

3.1.1. Front Office

Questa soluzione del POS Virtuale si basa su un meccanismo molto semplice: una volta terminata la fase di acquisto sul sito web/mobile dell'esercente, l'utente viene reindirizzato sul sito sicuro del POS Virtuale per effettuare il pagamento di quanto dovuto, e ritorna al negozio con l'esito del pagamento restituito dal "POS VIRTUALE" stesso. A questo punto il negozio darà il via al processo di invio della merce, di fruizione del servizio (download di informazioni, software, etc), o semplicemente a registrare l'avvenuto pagamento (donazioni, pagamento fatture, etc).

L'interazione con il merchant, come già precedentemente accennato, si basa su un meccanismo di delega: una volta che l'utente ha terminato la compilazione dell'ordine, il sito dell'esercente fa sì che il suo browser si colleghi automaticamente al "POS VIRTUALE" per accedere al servizio di pagamento on-line, comunicando tutti i dati necessari. A questo punto il "POS VIRTUALE" gestisce interamente il colloquio con il cliente relativo alla transazione. Il sistema effettua quindi il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendo la relativa risposta. Nel corso di questa fase, se l'acquirente ha aderito ai protocolli di sicurezza Verified by Visa, SecureCode MasterCard e SafeKey Amex, avviene anche l'autenticazione del titolare presso il sito dell'Issuer. L'utente ha la possibilità di portare a termine l'operazione o di annullarla; in entrambi i casi il suo browser verrà indirizzato verso le opportune pagine del sito di provenienza. L'esito positivo o negativo della richiesta di pagamento viene comunicato dal "POS VIRTUALE" con diverse modalità – di seguito descritte -, in base alla configurazione concordata in fase di configurazione del servizio.

Il POS Virtuale può comunicare l'esito del pagamento nelle seguenti modalità:

1. Reindirizza l'utente su un url indicato nel messaggi di avvio pagamento
2. Notifica diretta all' sito dell'esercente in modalità http server to server
3. E-Mail all'indirizzo fornito in fase di configurazione del servizio

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

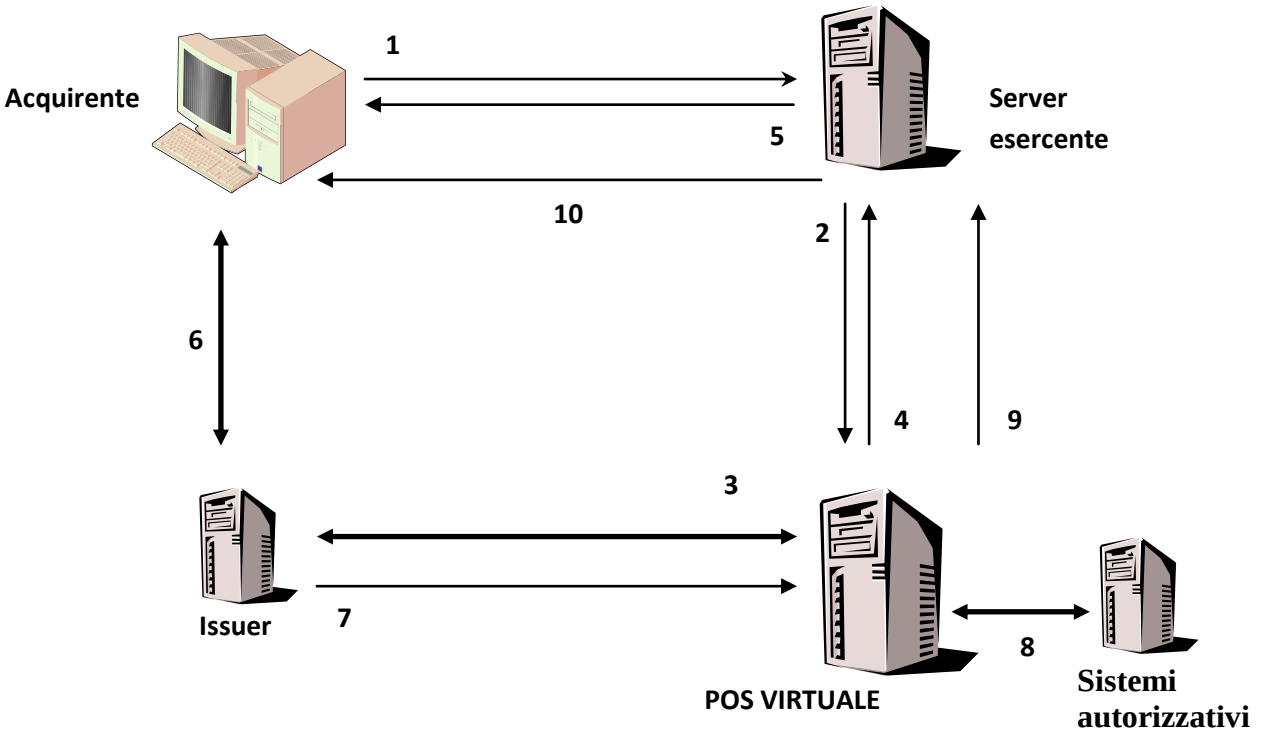
4.3.1. Messaggio avvio pagamento WEB Front Office
4.3.2. Messaggio esito pagamento WEB Front Office

3.1.2. Server to Server

Questa soluzione 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. Il negozio virtuale dell'esercente anche con la modalità server to server in presenza di carte abilitate al 3D-Secure deve cedere la navigazione dell'utente per la fase d'autenticazione del titolare in quanto è gestita interamente dall'Issuer che ha emesso la carta di credito.

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org

Il seguente diagramma riassume le varie fasi in cui è suddiviso il processo di pagamento se l'esercente sceglie 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/SafeKey. 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 POS VIRTUALE inviando tramite una chiamata server to server il messaggio avvio pagamento (cap.4 4.4.). Il messaggio contiene anche un campo CodTrans che identifica univocamente l'ordine.
3. Verifica dell'adesione al servizio Verified by Visa/SecureCode: il sistema POS VIRTUALE contatta i circuiti internazionali per verificare se la carta di credito dell'acquirente ha aderito o meno ai

protocolli di sicurezza. Se l'acquirente non si è registrato al servizio, POS VIRTUALE esegue immediatamente il pagamento, quindi il passo successivo sarà lo step 8. Se invece l'acquirente aderisce al servizio Verified by Visa/SecureCode/SafeKey, vengono eseguiti gli steps dal 4 al 7 .

Solo per acquirenti aderenti al Verified by Visa/SecureCode/SafeKey:

4. Restituzione della pagina di re direzione: POS VIRTUALE non inoltra il pagamento in quanto è subordinato all'autenticazione dell'acquirente, ma restituisce all'esercente il messaggio AuthRes (cap. 4.4.5.) contenente il codice di una pagina html che, eseguita dal browser dell'acquirente, lo re direziona verso l'applicazione dell'Issuer che deve verificarne l'identità. Il processo di pagamento si interrompe quindi per consentire l'autenticazione del titolare.
5. Re direzione dell'acquirente: l'applicazione dell'esercente restituisce al browser dell'acquirente l'html ricevuto da POS VIRTUALE 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 POS VIRTUALE 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 POS VIRTUALE effettuerà il pagamento, quindi il passo successivo sarà lo step 8.
8. Pagamento : POS VIRTUALE effettua il pagamento della transazione inviando la richiesta ai sistemi autorizzativi ed ottenendone la relativa risposta.
9. Notifica dell'esito all'esercente: POS VIRTUALE comunica l'esito della richiesta di pagamento all'esercente tramite il messaggio di esito pagamento (Cap. 4.4.6.). Se la fase di autenticazione non è avvenuta, il messaggio di esito viene inviato in risposta al messaggio di avvio pagamento (transazione sincrona), sulla stessa connessione in cui POS VIRTUALE 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 di esito sarà inviato al termine del pagamento (step8) su iniziativa del POS VIRTUALE tramite una chiamata server to server all'URL (urlPost) comunicato dall'esercente nel messaggio di apertura ordine. Inoltre in tal caso, al termine del pagamento il POS VIRTUALE redirige il browser del titolare verso il sito dell'esercente, all'URL (url) 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.

L'interazione con il merchant, come già precedentemente accennato, si basa su chiamate server tu server. La sicurezza dei messaggi scambiati è garantita dal Protocollo SSL 128 bit utilizzando certificati Server-side. Il POS VIRTUALE utilizzerà infatti per i propri URL un certificato SSL Server che garantirà la cifratura dei dati.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.4. Messaggio avvio pagamento Server to server
4.3.5. Messaggio gestione autenticazione 3D-Secure
4.3.6. Messaggio esito pagamento Server to server

3.1.3. Recurring Front Office

Tale soluzione consente al merchant di effettuare pagamenti ripetuti nel tempo, senza che l'utente debba nuovamente compiere l'operazione di pagamento vera e propria per continuare ad usufruire di un determinato servizio.

L'interazione con il merchant per la soluzione recurring prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione e-commerce analogamente a quanto descritto nella soluzione Front Office (cap. 3.1.2) dove il sito del merchant deve comunicare al POS Virtuale anche un num_contratto, per l'identificazione univoca del contratto di addebito ricorrente.

Durante il "Primo Pagamento" l'utente compie fisicamente la richiesta di pagamento. Nel corso di questa fase, se l'acquirente ha aderito ai protocolli di sicurezza Verified by Visa o SecureCode MasterCard o SafeKey di Amex, avviene anche l'autenticazione del titolare presso il sito dell'Issuer. Nell'esito del pagamento tra i dati forniti dal POS Virtuale è presente anche la data di scadenza della carta di credito utilizzata dall'utente: questo dato è utile al merchant per richiedere all'utente la nuova scadenza della carta rinnovata.

NB: è preciso compito dell'esercente prima del pagamento registrare l'autorizzazione del titolare carta all'addebito continuativo.

Le ricorrenze di pagamento ovvero pagamenti effettuati successivamente al primo che vengono innescati dal merchant non prevedono l'utilizzo dei codici di sicurezza 3D Secure e CV2, pertanto sono gestite in modalità SSL, e quindi non garantite al pari di transazione 3D-secure, secondo quanto riportato nell'apposito contratto di acquiring.

L'applicazione del merchant per le ricorrenze invia una richiesta http server to server passando tra l'altro il codice contratto che consentirà al POS Virtuale di recuperare "i dati sensibili" del cardholder dal DB ed effettua una richiesta di autorizzazione in alternativa è possibile gestire le ricorrenze tramite elaborazione di un file batch, per questa possibilità si rimanda al documento di specifiche: tracciato_autorizzazione_batch. Inoltre nel caso la carta di credito dell'utente è scaduta e il merchant ha recuperato dall'utente la nuova scadenza passa nel messaggio di richiesta pagamento la nuova data in modo che il POS Virtuale richiede il pagamento con la nuova scadenza e aggiorna la posizione in archivio. A seguito della richiesta di autorizzazione il POS Virtuale restituisce sulla stessa connessione del messaggio di richiesta l'esito della ricorrenza.

Nota: un pagamento ricorrente NON è una rateizzazione di un importo, ma la ripetizione di un pagamento che consente al Cardholder di rinnovare la fruizione di un servizio, che pagherà quindi in anticipo rispetto al consumo dello stesso.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

Primo pagamento:
- 4.3.1. Messaggio avvio pagamento WEB Front Office
- 4.3.2. Messaggio esito pagamento WEB Front Office

Ricorrenze:
- 4.3.4. Messaggio avvio pagamento Server to server
- 4.3.6. Messaggio esito pagamento Server to server

3.1.4. Recurring Server to Server

Tale soluzione consente al merchant di effettuare pagamenti ripetuti nel tempo, senza che l'utente debba nuovamente compiere l'operazione di pagamento vera e propria per continuare ad usufruire di un determinato servizio.

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org

L'interazione con il merchant per la soluzione recurring prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione e-commerce analogamente a quanto descritto nella soluzione E-commerce Server to server (cap. 3.1.2) dove il sito del merchant deve comunicare al POS Virtuale anche un num_contratto, per l'identificazione univoca del contratto di addebito ricorrente.

Durante il "Primo Pagamento" l'utente compie fisicamente la richiesta di pagamento, Nel corso di questa fase, se l'acquirente ha aderito ai protocolli di sicurezza Verified by Visa o SecureCode MasterCard o SafeKey, avviene anche l'autenticazione del titolare presso il sito dell'Issuer. Nell'esito del pagamento tra i dati forniti dal POS Virtuale è presente anche la data di scadenza della carta di credito utilizzata dall'utente, questo dato è utile al merchant per richiedere all'utente la nuova scadenza della carta rinnovata.

NB: è preciso compito dell'esercente prima del pagamento registrare l'autorizzazione del titolare carta all'addebito continuativo.

Le ricorrenze di pagamento ovvero pagamenti effettuati successivamente al primo che vengono innescati dal merchant non prevedono l'utilizzo dei codici di sicurezza 3D Secure e CV2, pertanto sono gestite in modalità SSL, e quindi non garantite al pari di transazione 3D-secure, secondo quanto riportato nell'apposito contratto di acquiring.

L'applicazione del merchant per le ricorrenze invia una richiesta http server to server passando tra l'altro il codice contratto che consentirà al POS Virtuale di recuperare "i dati sensibili" del cardholder dal DB ed effettua una richiesta di autorizzazione in alternativa è possibile gestire le ricorrenze tramite elaborazione di un file batch, per questa possibilità si rimanda al documento di specifiche: tracciato_autorizzazione_batch. Inoltre nel caso la carta di credito dell'utente è scaduta e il merchant ha recuperato dall'utente la nuova scadenza passa nel messaggio di richiesta pagamento la nuova data in modo che il POS Virtuale richiede il pagamento con la nuova scadenza e aggiorna la posizione in archivio. A seguito della richiesta di autorizzazione il POS Virtuale restituisce sulla stessa connessione del messaggio di richiesta l'esito della ricorrenza.

Nota: un pagamento ricorrente NON è una rateizzazione di un importo, ma la ripetizione di un pagamento che consente al Cardholder di rinnovare la fruizione di un servizio, che pagherà quindi in anticipo rispetto al consumo dello stesso.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.4. Messaggio avvio pagamento Server to server

4.3.5. Messaggio gestione autenticazione 3D-Secure (solo per primo pagamento)
4.3.6. Messaggio esito pagamento Server to server

3.1.5. OneClickPay Front Office

Tale soluzione consente la possibilità di memorizzare i dati della carta di credito del titolare durante il primo acquisto effettuato presso il merchant, in modo che per i successivi pagamenti il Titolare non debba inserire nuovamente i dati della carta.

L'interazione con il merchant per la soluzione OneclickPay prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione e-commerce analogamente a quanto descritto nella soluzione E-commerce Front Office (cap. 3.1.1) dove il sito del merchant deve comunicare al POS Virtuale anche un num_contratto e codice gruppo per l'identificazione univoca della registrazione al OneClickPay dell'utente.

Durante il "Primo Pagamento" l'utente compie fisicamente la richiesta di pagamento. Nel corso di questa fase, se l'acquirente ha aderito ai protocolli di sicurezza Verified by Visa o SecureCode MasterCard o SafeKey Amex, avviene anche l'autenticazione del titolare presso il sito dell'Issuer. Nell'esito del pagamento tra i dati forniti dal POS Virtuale è presente anche la data di scadenza della carta di credito utilizzata dall'utente, questo dato è utile al merchant per richiedere all'utente la nuova scadenza della carta rinnovata o generare un nuovo primo pagamento quando risulta scaduta.

Per i successivi pagamenti il sito del merchant reindirizza l'utente sulle pagina di pagamento del POS Virtuale analogamente al primo pagamento/registrazione, il POS Virtuale tramite il codice contratto abbina la carta precedentemente registrata e chiede all'utente solo l'inserimento del CVV2 e dove previsto effettuerà anche l'autenticazione 3D-Secure.

La funzionalità prevede anche la gestione di un gruppo di profili/terminali dove il titolare è abilitato al servizio OneClickPay, quindi un merchant che ad esempio gestisce più di un sito e-commerce abilitando il OneClickPay su un gruppo di terminali l'utente che ha eseguito il primo pagamento/registrazione su uno di questi risulta abilitato anche sugli altri terminali legati al codice gruppo.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.1. Messaggio avvio pagamento WEB Front Office
4.3.2. Messaggio esito pagamento WEB Front Office

3.1.6. OneClickPay Server to Server

Tale soluzione consente la possibilità di memorizzare i dati della carta di credito del titolare durante il primo acquisto effettuato presso il merchant, in modo che per i successivi pagamenti il Titolare non debba inserire nuovamente i dati della carta.

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org

L'interazione con il merchant per la soluzione OneclickPay prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione e-commerce analogamente a quanto descritto nella soluzione E-commerce Server to Server (cap. 3.1.2) dove il sito del merchant deve comunicare al POS Virtuale anche un num_contratto e codice gruppo per l'identificazione univoca della registrazione al OneClickPay dell'utente.

Durante il "Primo Pagamento" l'utente compie fisicamente la richiesta di pagamento, Nel corso di questa fase, se l'acquirente ha aderito ai protocolli di sicurezza Verified by Visa o SecureCode MasterCard o SafeKey Amex, avviene anche l'autenticazione del titolare presso il sito dell'Issuer. Nell'esito del pagamento tra i dati forniti dal POS Virtuale è presente anche la data di scadenza della carta di credito utilizzata dall'utente, questo dato è utile al merchant per richiedere all'utente la nuova scadenza della carta rinnovata o generare un nuovo primo pagamento quando risulta scaduta.

Per i successivi pagamenti, il sito del merchant invia una richiesta http server to server al POS VIRTUALE analogamente al primo pagamento/registrazione, però non deve più richiedere all'utente l'inserimento del numero di carta e scadenza ma solo il CVV2, quindi invia la richiesta al POS Virtuale completa del codice contratto abbinato all'utente e codice gruppo. Il processo da qui in poi è analogo a un pagamento server to server standard descritto nel cap. 3.1.2 nel diagramma da 4 passaggio in avanti.

La funzionalità prevede anche la gestione di un gruppo di profili/terminali dove il titolare è abilitato al servizio OneClickPay, quindi un merchant che ad esempio gestisce più di un sito e-commerce abilitando il OneClickPay su un gruppo di terminali l'utente che ha eseguito il primo pagamento/registrazione su uno di questi risulta abilitato anche sugli altri terminali legati al codice gruppo.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.4. Messaggio avvio pagamento Server to server
4.3.5. Messaggio gestione autenticazione 3D-Secure
4.3.6. Messaggio esito pagamento Server to server

3.1.7. Server to server con MPI MERCHANT

Questa soluzione e-commerce server to server può essere utilizzata da quei merchant che dispongono di un proprio MPI (Merchant Plug In) che gestisce la fase di autenticazione dei titolari con i protocolli 3D-Secure. Utilizzano quindi il POS Virtuale per l'inoltro delle richieste di autorizzazione passando anche i dati ottenuti precedenemente dal processo 3D-Secure.

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org

L'interazione con il merchant, si basa su chiamate server tu server sincrone. La sicurezza dei messaggi scambiati è garantita dal Protocollo SSL 128 bit utilizzando certificati Server-side. Il POS VIRTUALE utilizzerà infatti per i propri URL un certificato SSL Server che garantirà la cifratura dei dati.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.7. Messaggio avvio pagamento AUTHONLYREQ
4.3.8. Messaggio esito pagamento AUTHONLYRES

3.2. Soluzioni MOTO (Mail Order Telephone Order)

3.2.1. MOTO standard

Questa modalità è destinata agli esercenti che devono gestire transazioni telefoniche o per corrispondenza. L'esercente accede al back-office della piattaforma VPOS tramite username e password fornite da CartaSi e gestisce le transazioni M.O.T.O. (dalla presa in carico dell'ordine fino alla contabilizzazione) senza dover effettuare alcuna implementazione.

Per maggiori dettagli operativi del servizio si rimanda al manuale di utilizzo del back Office

3.2.2. MOTO Recurring standard

Tale soluzione consente al merchant di effettuare pagamenti ripetuti nel tempo, senza che l'utente debba nuovamente comunicare i dati della sua carta di credito al merchant via mail, telefono, ecc. per continuare ad usufruire di un determinato servizio.

L'interazione con il merchant per la soluzione recurring prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione M.O.T.O. Durante il "Primo Pagamento", il merchant effettua la richiesta di pagamento, compilando una pagina predefinita all'interno dell'area di back office. Il merchant indicherà quindi – oltre ai dati della carta forniti dal titolare – anche il "Numero Contratto", che il POS Virtuale associa ai dati della carta per le successive ricorrenze. Il merchant dovrà inserire il codice contratto sul proprio gestionale che utilizzerà per inviare le richieste di addebito successive.

NB: è preciso compito dell'esercente prima del pagamento registrare l'autorizzazione del titolare carta all'addebito continuativo.

L'applicazione del merchant per le ricorrenze invia una richiesta http server to server passando tra l'altro il codice contratto che consentirà al POS Virtuale di recuperare "i dati sensibili" del cardholder dal DB ed effettua una richiesta di autorizzazione. Inoltre nel caso la carta di credito dell'utente è scaduta e il merchant ha recuperato dall'utente la nuova scadenza passa nel messaggio di richiesta pagamento la nuova data in modo che il POS Virtuale richiede il pagamento con la nuova scadenza e aggiorna la posizione in archivio. A seguito della richiesta di autorizzazione il POS Virtuale restituisce sulla stessa connessione del messaggio di richiesta l'esito della ricorrenza.

Nota: un pagamento ricorrente NON è una rateizzazione di un importo, ma la ripetizione di un pagamento che consente al Cardholder di rinnovare la fruizione di un servizio, che pagherà quindi in anticipo rispetto al consumo dello stesso.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

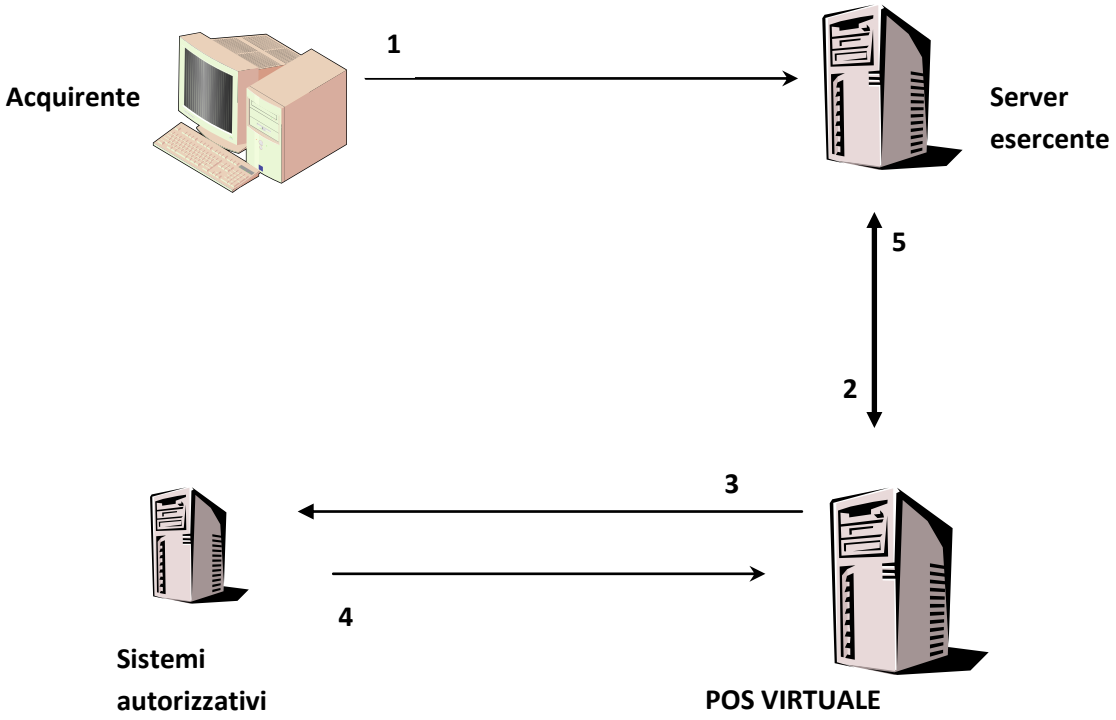
4.3.4. Messaggio avvio pagamento Server to server
4.3.6. Messaggio esito pagamento Server to server

3.2.3. MOTO Server to server

Questa soluzione è destinata a chi desiderasse integrare sul proprio sistema la funzione di richiesta autorizzazione di pagamenti tramite carta di credito, i cui dati siano stati comunicati dal titolare carta al merchant via mail, telefono, ecc … prevede che l'esercente gestisca tramite il proprio sistema gestionale sia la richiesta dei dati della carta di credito che la comunicazione dell'esito del pagamento

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org.

l seguente diagramma riassume le varie fasi in cui è suddiviso il processo di pagamento:



1. Definizione dell'ordine: l'acquirente, dopo aver concordato con il merchant il tipo di acquisto e il relativo importo, fornisce al merchant stesso (via mail, telefono, fax) i dati della carta di credito che intende utilizzare per il pagamento.
2. Richiesta di pagamento: il merchant inserisce i dati della carta di credito sul proprio sistema, che spedisce i dati del pagamento alla piattaforma POS VIRTUALE tramite una chiamata server to server (messaggio avvio pagamento, cfr. Cap. 5.1). Il messaggio contiene anche il parametro codTrans che identifica univocamente ciascun ordine.
3. Pagamento: POS VIRTUALE invia la richiesta ai sistemi autorizzativi.
4. Esito richiesta: POS VIRTUALE riceve dai sistemi autorizzativi l'esito della richiesta di autorizzazione.
5. Notifica dell'esito all'esercente: POS VIRTUALE comunica al sistema dell'esercente, sulla stessa connessione in cui ha ricevuto la richiesta di pagamento, l'esito della richiesta di autorizzazione, tramite il messaggio di esito pagamento (cfr. Cap. 5.2).
6. Notifica dell'esito al titolare: se richiesto dall'esercente, POS VIRTUALE invia una mail di "esito pagamento" all'esercente stesso e al titolare carta (cfr. Cap. 5.4).

L'interazione con il merchant, come già precedentemente accennato, si basa su chiamate server tu server. La sicurezza dei messaggi scambiati è garantita dal Protocollo SSL 128 bit utilizzando certificati Server-side. Il POS VIRTUALE utilizzerà infatti per i propri URL un certificato SSL Server che garantirà la cifratura dei dati.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.4. Messaggio avvio pagamento Server to server
4.3.6. Messaggio esito pagamento Server to server

3.2.4. MOTO Recurring Server to Server

Tale soluzione consente al merchant di effettuare pagamenti ripetuti nel tempo, senza che l'utente debba nuovamente comunicare i dati della sua carta di credito al merchant via mail, telefono, ecc. per continuare ad usufruire di un determinato servizio.

NB: L'utilizzo di questa modalità operativa è subordinata all'ottenimento della certificazione PCI (Payment Card Industry) DSS (Data Security Standard) da parte dell'esercente, questa certificazione è richiesta dai circuiti internazionali per favorire e migliorare la protezione dei dati di titolari di carta. Per ulteriori informazioni si rimanda al sito: https://www.pcisecuritystandards.org

L'interazione con il merchant per la soluzione recurring prevede un "Primo Pagamento" o registrazione dell'utente che effettua con una transazione M.O.T.O. Server to server analogamente a quanto descritto nella soluzione M.O.T.O. Server to server (cap. 3.2.3) dove il gestionale del merchant deve comunicare al POS Virtuale anche un num_contratto, per l'identificazione univoca del contratto di addebito ricorrente.

Nell'esito del pagamento tra i dati forniti dal POS Virtuale è presente anche la data di scadenza della carta di credito utilizzata dall'utente, questo dato è utile al merchant per richiedere all'utente la nuova scadenza della carta rinnovata.

NB: è preciso compito dell'esercente prima del pagamento registrare l'autorizzazione del titolare carta all'addebito continuativo.

L'applicazione del merchant per le ricorrenze invia una richiesta http server to server passando tra l'altro il codice contratto che consentirà al POS Virtuale di recuperare "i dati sensibili" del cardholder dal DB ed effettua una richiesta di autorizzazione. Inoltre nel caso la carta di credito dell'utente è scaduta e il merchant ha recuperato dall'utente la nuova scadenza passa nel messaggio di richiesta pagamento la nuova data in modo che il POS Virtuale richiede il pagamento con la nuova scadenza e aggiorna la posizione in archivio. A seguito della richiesta di autorizzazione il POS Virtuale restituisce sulla stessa connessione del messaggio di richiesta l'esito della ricorrenza.

Nota: un pagamento ricorrente NON è una rateizzazione di un importo, ma la ripetizione di un pagamento che consente al Cardholder di rinnovare la fruizione di un servizio, che pagherà quindi in anticipo rispetto al consumo dello stesso.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.4. Messaggio avvio pagamento Server to server
4.3.6. Messaggio esito pagamento Server to server

3.3. Soluzioni Opzionali

3.3.1. MyBANK

MyBANK é un sistema paneuropeo di pagamento per l'e-commerce, complementare all'utilizzo delle carte, che consente ai consumatori di tutta Europa di effettuare acquisti presso gli esercenti convenzionati direttamente tramite il proprio servizio di Internet Banking , in tutta l'Area unica dei pagamenti in euro (SEPA)[1]

Il servizio viene integrato al pos virtuale sia nelle pagine di pagamento sia nel back office operativo, consentendo agli esercenti che adottano la soluzione "chiavi in mano" di disporre del nuovo servizio senza necessità di integrazioni aggiuntive ed agli esercenti integrati in modalità server to server di aggiungere il nuovo servizio in modo semplice e veloce.

Il pagamento tramite il servizio MyBank può avvenire tramite:

1- il SEPA Credit Transfer (SCT) il nuovo strumento di pagamento di base per l'esecuzione di bonifici in euro fra i clienti detentori di conti all'interno dell'area SEPA. In Italia il SEPA Credit Transfer ha sostituito il Bonifico Ordinario Nazionale
2- Il SEPA Direct Debit (SDD) lo strumento d'incasso europeo, che ha sostituito il RID, e che permette di raggiungere tutti i conti bancari nell'area SEPA che ammettono addebito diretto.(es addebiti ricorrenti)

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.1. Messaggio avvio pagamento WEB Front Office
4.3.2. Messaggio esito pagamento WEB Front Office

1 - Fanno parte dell'Area unica dei pagamenti in euro (SEPA) i 28 Stati membri dell'UE, insieme a Islanda, Liechtenstein, Principato di Monaco, Norvegia e Svizzera

3.3.2. Currency Choice

Currency Choice è il servizio nato dalla collaborazione tra CartaSi e **Global Blue**, che permette ai titolari di carte di credito internazionali Visa e MasterCard, di fare acquisti nella propria valuta con un tasso di cambio garantito al momento del pagamento.

Il servizio Currency Choice è attualmente disponibile in 37 valute

L'utilizzo del servizio per gli esercenti non in modalità Server to Server ha impatti tecnici limitati in quanto è il POS Virtuale a gestire tutto il processo di conversione e messaggistica verso l'utente mentre per gli esercenti con soluzioni Server to Server è necessario prevedere una fase preparatoria al processo standard.

L'applicativo dell'esercente deve inoltrare al POS Virtuale, per conoscere la disponibilità al DCC (Dynamic Currency Conversion), a fronte della carta inserita dal titolare, dell'eventuale valuta associata e del relativo controvalore, tramite una chiamata server to server. Ottenuto l'esito l'esercente può procedere con la richiesta di autorizzazione valorizzando opportunamente i dati ottenuti.

NB: Nella modalità Server to Server è preciso compito dell'esercente mostrare tutte le indicazioni/disclaimer e notifiche email agli utenti previsti da CartaSi nelle apposite linee guida.

Per l'integrazione con questa soluzione il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.1. Messaggio avvio pagamento WEB Front Office
4.3.2. Messaggio esito pagamento WEB Front Office

3.3.3. MCC (Multi Currency Conversion)

Il servizio MCC permette agli esercenti di gestire siti con prodotti/servizi a catalogo in valuta differente dall'euro, i cliente pagheranno l'importo indicato nella divisa scelta dall'esercente e quest'ultimo riceverà l'accredito in euro secondo il tasso di cambio applicato al momento dell'acquisto.

L'utilizzo del servizio per gli esercenti ha impatti tecnici limitati in quanto è il POS Virtuale a gestire tutto il processo di conversione.

L'applicativo dell'esercente deve inoltrare al POS Virtuale, l'importo e il codice divisa con cui vuole eseguire il pagamento, al terminale della transazione l'esercente riceverà l'indicazione del tasso di cambio applicato e relativo controvalore in euro che le verrà accreditato.

Per l'integrazione con questa soluzione (disponibile sia in modalità FrontOffice che server to server) il dettaglio dei messaggi scambiati con il POS Virtuale vengono descritti nei capitoli:

4.3.1. Messaggio avvio pagamento WEB Front Office
4.3.2. Messaggio esito pagamento WEB Front Office
4.3.4. Messaggio avvio pagamento Server to server
4.3.6. Messaggio esito pagamento Server to server

3.3.4. API Back Office

Il POS Virtuale mette a disposizione degli esercenti l'ambiente di back office per la gestione delle transazioni ricevute, inoltre per gli esercenti che dispongono di un proprio sistema informativo possono usufruire di alcune delle funzionalità di back office (operatività e reportistica) mediante integrazione con API (server to server).

I messaggi API server to server sono utilizzabili indipendentemente dalla modalità con cui è stata inoltrata dall'esercente la richiesta di pagamento (modalità standard o server to server, WEB o M.O.T.O., ecc…).

Le funzionalità dispositive disponibili sono:

- Incasso: per gli esercenti che in fase di attivazione del servizio hanno richiesto l'incasso esplicito possono richiedere la 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.
- Annullo: per una transazione che non è stata contabilizzata l'esercente può richiederne l'annullo, questa operazione ha come effetto quello di ripristinare il plafond della carta(se gestito dall'emittente della carta e non decorsi i termini).

- Storno: l'esercente può 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.

Accanto alle funzionalità dispositive per la gestione operativa degli ordini, sono disponibili anche le funzionalità di reportistica e storico degli ordini ricevuti.

- Verifica ordine: questa richiesta permette all'esercente di conoscere la situazione attuale di un ordine e lo stato di tutte le operazioni ad esso associate.
- Elenco ordini: questa richiesta permette all'esercente di richiedere l'elenco completo delle transazioni filtrato per opportuni parametri.

4. Messaggi

4.1. Firma dei messaggi

Ogni messaggio scambiato tra il POS Virtuale 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 il POS Virtuale, 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 il POS Virtuale 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. 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.

In ogni messaggio descritto viene riportata la modalità di calcolo per lo specifico messaggio.

4.2. Struttura e Inoltro dei messaggi

La tipologia dei messaggi scambiati tra il POS Virtuale 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 redirect http inviati con metodo GET/POST, in modalità SSL.
- Integrazione tramite chiamate server to server: Si tratta di messaggi http inviati con metodo GET/POST, in modalità SSL.
- Integrazione API: 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. Il POS Virtuale utilizzerà, infatti, per i propri URL un certificato SSL Server che garantirà la cifratura dei dati.

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

- NOME: La colonna nome riporta l'identificativo del parametro con il quale una specifica informazione deve essere inserita nel messaggio.
- OBB.: La colonna Obb specifica se l'informazione è obbligatoria i valori possono essere:
  SI: in caso di omissione viene rifiutata l'elaborazione della richiesta. F
  NO: è un dato facoltativo è a discrezione dell'esercente la valorizzazione.
  C: condizionato la sua obbligatorietà è legata al tipo di servizio che viene richiesto.
- DESCRIZIONE: descrive sinteticamente il parametro.
- FORMATO: indica la tipologia e la lunghezza del parametro.

4.3. Specifiche tecniche dei messaggi di pagamento

4.3.1. Messaggio avvio pagamento WEB Front Office

MESSAGGIO:

La tabella riportata sotto riporta tutti i campi necessari per realizzare il messaggio di avvio pagamento per i pagamenti WEB Front Office, primo pagamento WEB Front Office Recurring e pagamenti Web Front Office OneClickPay.

La URL delle pagine di pagamento messe a disposizione dal VIRTUAL POS, verso la quale dovrà essere indirizzato il browser dell'utente, è:

https://ecommerce.keyclient.it/ecomm/ecomm/DispatcherServlet

Il primo passo che il merchant deve compiere è far generare al browser del cliente un messaggio di avvio del processo di pagamento verso il POS VIRTUALE. Questo può essere fatto sia con una redirect, o un link, (utilizzando quindi il metodo HTTP GET), sia attraverso l'invio di un form con campi nascosti (che può utilizzare il metodo HTTP POST).

Il messaggio di avvio della transazione che arriva al POS Virtuale dal browser dell'utente deve contenere i campi indicati nella tabella seguente.

NOME	Obb	Descrizione	Formato

<table>
<tr><td>alias</td><td>SI</td><td>Codice identificativo del negozio (valore fisso comunicato da CartaSi nella fase di attivazione definitiva)</td><td>AN Max 30 CRT</td></tr>
<tr><td>importo</td><td>C</td><td>importo da autorizzare espresso in centesimi di euro senza separatore, i primi 2 numeri a destra rappresentano gli euro cent, es.: 5000 corrisponde a 50,00 €. Campo obbligatorio ad esclusione di utilizzo servizio MCC</td><td>N Max 7 CRT</td></tr>
<tr><td>divisa</td><td>C</td><td>Il codice della divisa in cui l'importo è espresso unico valore ammesso: EUR (Euro). Campo obbligatorio ad esclusione per l' utilizzo servizio MCC</td><td>AN 3 CRT</td></tr>
<tr><td>codTrans</td><td>SI</td><td>codice di identificazione del pagamento composto da caratteri alfanumerici, <u>escluso il carattere #.</u> Il codice dev'essere univoco per ogni richiesta di autorizzazione, solo in caso di esito negativo dell'autorizzazione il merchant può riproporre la stessa richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi.</td><td>AN min 2 - Max 30 CRT</td></tr>
<tr><td>url</td><td>SI</td><td>url del merchant verso la quale il POS Virtuale indirizza l'utente al completamento della transazione passando,in GET, i parametri di risposta con il risultato della transazione. Si veda il capitolo 4.3.2. Messaggio esito pagamento WEB Front Office che descrive il formato del messaggio di esito</td><td>AN Max 500 CRT</td></tr>
<tr><td>url_back</td><td>SI</td><td>url del merchant verso la quale il POS Virtuale indirizza l'utente che decide di abbandonare la transazione durante la fase di pagamento sulla pagina di cassa(esito=ANNULLO) o in caso la chiamata contiene errori formali(esito=ERRORE). l'url verrà chiamata accodando i seguenti parametri:
<table>
<tr><th>Variabile</th><th>Valorizzazione</th></tr>
<tr><td>importo</td><td>importo da autorizzare</td></tr>
<tr><td>divisa</td><td>EUR</td></tr>
<tr><td>codTrans</td><td>codice identificativo del pagamento assegnato dal merchant</td></tr>
<tr><td>esito</td><td>Valori possibili: ANNULLO o ERRORE</td></tr>
</table>
NB: in caso di esito=ANNULLO l'esercente può decidere di rimandare l'utente sulla pagina di pagamento con il medesimo codice transazione.</td><td>AN Max 200 CRT</td></tr>
<tr><td>mac</td><td>SI</td><td>Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC</td><td>AN 40 CRT</td></tr>
<tr><td>mail</td><td>NO</td><td>l'indirizzo e-mail dell'acquirente al quale inviare l'esito del pagamento</td><td>AN Max 150 CRT</td></tr>
<tr><td>languageId</td><td>NO</td><td>identificativo della lingua che verrà visualizzata sulla pagina di cassa; le lingue disponibili sono quelle riportate nell'appendice: 5.1 .

Se tale campo non viene specificato o viene lasciato vuoto verranno visualizzati i testi secondo quando definito come</td><td>AN Max 7 CRT</td></tr>
</table>

		default in fase di configurazione del servizio.	
urlpost	NO	*url del merchant verso la quale il POS Virtuale invia al completamento della transazione passando, in modalità server to server con metodo POST, i parametri di risposta con l'esito della transazione.* *Si veda il capitolo 4.3.2. Messaggio esito pagamento WEB Front Office (solo se le esigenze del merchant richiedono questo tipo di esito) che descrive il formato del messaggio di esito.*	AN Max 500 CRT
num_contratto	C	*codice univoco assegnato dal merchant per l'abbinamento con l' archivio contenente i dati sensibili della carta di credito. Campo da utilizzare solo per il servizio di recurring payment e OneClickPay.*	AN Max 30 CRT
tipo_servizio	C	*Se valorizzato verranno salvati i dati necessari per gestire le riscossioni .* *Può assumere i seguenti valori:* *1) "paga_rico": per pagamenti ricorrenti, cioè se sarà poi il merchant a disporre le ripetizioni (ad es. domiciliazioni, abbonamenti, ecc.);* *2) "paga_multi": per il servizio ricorrenti dove gli addebiti ricorsivi possono avvenire su un terminale differente da quello del primo pagamento/registrazione. Con questo valore è necessario valorizzare il parametro "gruppo".* *2) "paga_oc3d": per il servizio "oneclickpay", ovvero sarà il titolare della carta a scatenare le successive ricorrenze senza digitare nuovamente i dati della carta. Con questo valore è necessario valorizzare il parametro "gruppo.* *Campo da utilizzare solo per il servizio di recurring payment e OneClickPay.*	AN Max 30 CRT
gruppo	C	*Valorizzare solo se tipo_servizio: "paga_multi" e "paga:oc3d"* *Il valore del "gruppo" viene assegnato in fase di attivazione da CartaSi*	AN Min 5 - Max 30 CRT
descrizione	NO	*campo in cui il merchant può specificare una descrizione del tipo di servizio offerto. Questo campo verrà riportato anche nel testo della mail inviata al cardholder*	AN Max 300 CRT
session_id	NO	*identificativo della sessione*	AN Max 200 CRT
Note1	NO	*campo in cui il merchant può riportare informazioni relative all'ordine. Questo dato verrà riportato anche nel report interrogabile dal back Office*	AN Max 300 CRT
Note2	NO	*campo in cui il merchant può riportare informazioni relative all'ordine. Questo dato verrà riportato anche nel report interrogabile dal back Office*	AN Max 300 CRT

Note3	NO	*campo in cui il merchant può riportare informazioni relative all'ordine. Questo dato verrà riportato anche nel report interrogabile dal back Office*	AN Max 300 CRT
Parametri aggiuntivi	NO	*Possono essere specificati n parametri aggiuntivi che verranno restituiti nei messaggi di esito. Non c'è un limite al numero di parametri aggiuntivi ma la lunghezza complessiva della stringa composta dai nomi dei parametri e il loro valore complessivamente non deve superare i 4000 caratteri.*	AN Max 4000 CRT
OPTION_CF	C	*campo in cui il merchant invia al Virtual Pos il codice fiscale dell'utente, necessario se attivo il controllo(controllo di sicurezza opzionale attivabile su richiesta) tra codice fiscale e numero di PAN associati. Questo dato verrà riportato anche nel report interrogabile dal back Office*	AN 16 CRT
selectedcard	NO	*Se presente il campo nella chiamata valorizzato con uno dei valori riportati nell'appendice 5.5 (solo i circuiti con cui il merchant ha attiva una convenzione) la pagina di pagamento viene mostrata consentendo all'utente di effettuare il pagamento solo con il circuito di pagamento indicato.*	AN Max 12 CRT
TCONTAB	NO	*Il campo identifica la modalità di incasso che l'esercente vuole applicare alla singola transazione, se valorizzato con: I (immediata) la transazione se autorizzata viene anche incassata senza altri interventi da parte dell'esercente e senza considerare il profilo di default impostato sul terminale. Se valorizzato con D (differita) o non viene inserito il campo la transazione se autorizzata viene gestita secondo quanto definito dal profilo del terminale.*	AN 1 CRT
mccImporto	C	*importo da autorizzare espresso nella valuta desiderata partendo da destra con la frazione minore prevista dalla valuta stessa, per esempio il dollaro prevede 2 cifre decimali mentre lo Yen non prevede alcuna cifra decimale, quindi per indicare un pagamento di 10 dollari americani, si dovrà indicare un mccImporto="1000", mentre per indicare un pagamento di 10 Yen sarà sufficiente inviare un mccImporto="10". Campo obbligatorio da valorizzare solo per l'utilizzo del servizio MCC*	N Max 7 CRT
mccDivisa	C	*Il codice della divisa in cui l'importo è espresso, i valori ammessi sono riportati nell'appendice 5.2. Campo obbligatorio da valorizzare solo per l'utilizzo del servizio MCC*	AN 3 CRT
infoc	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla compagnia in base ad accordi preventivi con la compagnia stessa*	AN Max 35 CRT
infob	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla banca in base ad accordi preventivi con la banca stessa*	AN mac 20 CRT

Tabella campi aggiuntivi MYBANK – SDD

Si riporta nella seguente tabella i campi aggiuntivi necessari all'aperture di un mandato SDD

NOME	Obb	Descrizione	Formato
mandateId	SI	*Identificativo univoco mandato assegnato dal Merchant*	AN Max 35 CRT
mandateRequestId	SI	*Identificativo univoco della richiesta sul mandateId assegnato dal Merchant*	AN Max 35 CRT
sequenceType	SI	*Tipo mandato (recurrent o One off)*	Valori ammessi: -RCUR (RECURRENT) -OOFF (one off)
frequencyType	NO	*Frequenza della rata SDD*	Valori ammessi: -YEAR -WEEK -QURT -MINTH -MIAN -INDA -FRTN -DAIL -ADHO
durationStartDate	NO	*Data inizio validità Mandato*	Formato date SSAA-MM-GG
durationEndDate	NO	*Data fine validità mandato*	Formato date SSAA-MM-GG
firstCollectionDate	NO	*Data primo addebito rata*	Formato date SSAA-MM-GG
finalCollectionDate	NO	*Data ultimo addebito rata*	Formato date SSAA-MM-GG
collectionAmount	NO	*Importo fisso da incassare dal conto del debitore*	Numerico 18 (senza virgola, ultimi due caratteri rappresentano i decimali)
maxAmount	NO	*Importo massimo*	Numerico 18 (senza virgola, ultimi due caratteri rappresentano i decimali)
country	SI	*Paese indirizzo del creditore/Merchant*	AN Max 5 CRT

address	SI	*Indirizzo del creditore/Merchant*	AN Max 70 CRT
ultimateCreditorName	NO	*Nome creditore legato al conto*	AN Max 70 CRT
ultimateCreditorId	NO	*Id creditore legato al conto*	AN Max 70 CRT
debtorName	SI	*Nome del debitore*	AN Max 70 CRT
messageNameIdType	SI	*Identificativo messaggio*	AN Max 35 CRT; valori ammessi: -"pain.009.001.03" per generazione mandato -"pain.010.001.03" per modifica mandato -"pain.011.001.03" per cancellazione mandato
timeout	NO	*Merchant timeout specifico di quella autorizzazione.* *Se non presente viene utilizzato quello di default*	es PT15M con valori compresi tra 5 e 30 minuti;

NB: i valori ei campi: "url" e "urlpost" devono cominciare con "http://" o "https//"; le porte utilizzate non possono essere diverse da quelle standard: 80 o 443.
Per una corretta gestione delle chiamate si ricorda di attenersi agli standard RFC 2396 e RFC 3986

Si vedano gli esempi che seguono (riportati per semplicità con metodo get):

per la richiesta di autorizzazione di 50 Euro ci si deve riferire all'URL:
https://ecommerce.keyclient.it/ecomm/ecomm/DispatcherServlet?alias=valore&importo=5000&divisa=EUR&codTrans=990101-00001&mail=xxx@xxxx.it&url=http://www.xxxxx.it&session_id=xxxxxxxx&mac=yyyy&languageId=ITA

per la richiesta di autorizzazione di 50,12 Euro ci si deve riferire all'URL:

https://ecommerce.keyclient.it/ecomm/ecomm/DispatcherServlet?alias=valore&importo=5012&divisa=EUR&codTrans=990101-00001&mail=xxx@xxxx.it&url=http://www.xxxxx.it&session_id=xxxxxxxx&mac=yyyy&languageId=ENG
Dopo aver rimandato il compratore a tale URL, il merchant resta in attesa dell'esito di pagamento, che riceverà in modalità da concordare (mail, on line su Internet e/o comunicazione server to server). In caso di

esito positivo, il pagamento viene garantito dalle compagnie delle carte di credito, secondo le norme fissate nei documenti contrattuali.

CALCOLO MAC:

Per il messaggio di avvio transazione, il testo da firmare deve contenere i campi:

- **codTrans**
- **divisa (mccDivisa in caso di servizio MCC)**
- **importo (mccImporto in caso di servizio MCC)**
- **stringa segreta**

Il mac sarà calcolato nel seguente modo:

> *mac= HASH SHA(codTrans=<valore codTrans>divisa=<valore divisa>importo=<valore importo><chiave segreta")*

Un esempio di tale stringa potrebbe essere:

> *"codTrans=ordtest534divisa=EURimporto=1esempiodicalcolomac"*

il campo mac sarà:

> *mac= HASH SHA("codTrans=ordtest534divisa=EURimporto=1esempiodicalcolomac")*

Il valore ottenuto sarà:

> *"5e6523d39ad4a58b0a5ae7caabb49adbe2a30406"*

4.3.2. Messaggio esito pagamento WEB Front Office

MESSAGGIO:

Qui viene descritto il formato del messaggio di esito transazione inviato per le modalità: WEB Front Office(tutte) e PayMail. L'esercente può scegliere di configurare la ricezione/visualizzazione dell'esito del pagamento da parte del "POS VIRTUALE" in una o più delle seguenti modalità:

- E-Mail: l'esercente riceverà una mail con i dettagli delle transazioni al recapito mail comunicato in fase di configurazione
- On-line su internet: l'utente, una volta concluso il pagamento, viene reindirizzato direttamente sul sito dell'esercente, all'indirizzo indicato nel messaggio di avvio pagamento (nome campo "url"). L'utente quindi ritorna al sito dell'esercente portando con sé i parametri (si veda la tabella sotto) che attestano la conclusione della transazione
- On-line server to server: l'esercente può ricevere l'esito direttamente dal "POS VIRTUALE" in modalità server to server. La chiamata contiene gli stessi parametri della modalità precedente, e viene eseguita verso l'indirizzo indicato nel messaggio di avvio pagamento (nome campo: "urlpost"), che attesta la conclusione della transazione (si veda tabella sotto).

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo del negozio passato nel messaggio di avvio pagamento*	AN Max 30 CRT
importo	SI	*importo transazione preso dal messaggio di avvio pagamento. In caso di servizio MCC sarà riportato il controvalore in euro ottenuto secondo il tasso di cambio riportato nel campo dccRate.*	N Max 7 CRT
divisa	SI	*Il codice della divisa in cui l'importo è espresso (EUR = Euro)*	AN 3 CRT
codTrans	SI	*codice associato al pagamento preso dal messaggi odi avvio pagamento*	AN Min 2 - Max 30 CRT
session_id	NO	*identificativo della sessione preso dal messaggio di avvio*	AN Max 200 CRT
brand	SI	*tipo di carta utilizzata dall'utente per eseguire il pagamento. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.5*	AN Max 12 CRT
nome	NO	*nome di chi ha effettuato il pagamento*	AN Max 30 CRT
cognome	NO	*cognome di chi ha effettuato il pagamento*	AN Max 30 CRT
mail	NO	*indirizzo e-mail di chi ha effettuato il pagamento*	AN Max 150 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT

num_contratto	C	*Numero contratto preso dal messaggio di avvio. Campo presente solo per il servizio di recurring payment e OneClickPay.*	AN Min 5 - Max 30 CRT
esito	SI	*esito del pagamento (OK o KO)*	AN 2 CRT
data	SI	*Data della transazione*	aaaammgg
orario	SI	*Ora della transazione*	hhmmss
codAut	C	*Codice dell'autorizzazione assegnato dall'emittente della carta di credito, presente solo con autorizzazione concessa*	AN Min 2 Max 6 CRT
pan	NO	*Numero carta di credito mascherato in chiaro solo le prime 6 e ultime 4 cifre*	AN Max 19 CRT
scadenza_pan	NO	*Scadenza carta di credito.*	aaaamm
regione	NO	*Se abilitato viene restituito la macroregione di appartenenza della carta usata per il pagamento(es.: Europa)*	AN Max 30 CRT
nazionalita	NO	*Riporta la nazionalità della carta che ha eseguito il pagamento.*	AN 3 CRT codifica ISO 3166-1 alpha-3
messaggio	NO	*Riporta una breve descrizione dell' esito del pagamento. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.4*	AN Max 30 CRT
hash	C	*Se previsto dal profilo dell'esercente viene restituito questo campo valorizzato con l'hash del PAN della carta utilizzata per il pagamento.*	AN 28 CRT
check	NO	*Viene valorizzato nel caso uno o più controlli previsti dal profilo dell'esercente non vengono superati.* *Controllo presenza del PAN carta su altri codici contratti sarà valorizzato con: "PGP", in base al profilo merchant il controllo se non superato può bloccare la transazione o solo notificare la presenza del pan sul altro num_contratto.* *Superati tutti i controlli il campo non sarà valorizzato.*	AN 3 CRT
codiceConvenzione	NO	*Codice esercente assegnato dall'acquirer. Dove previsto.*	AN Max 12 crt
descrizione	NO	*se viene indicata in INPUT dal merchant viene restituita anche in OUTPUT altrimenti il campo è nullo*	AN Max 300 CRT
Parametri aggiuntivi	NO	*Possono essere specificati n parametri aggiuntivi che verranno restituiti nei messaggi di esito. Non c'è un limite al numero di parametri aggiuntivi ma la lunghezza complessiva della stringa composta dai nomi dei parametri e il loro valore complessivamente non deve superare i 4000 caratteri.*	AN Max 4000 CRT
languageId	NO	*Valore preso dal messaggio di avvio pagamento.*	AN Max 7 CRT
TipoTransazione	NO	*Tipo di transazione, indica la modalità con cui è avvenuto il pagamento, vedere l'Appendice 5.3 per i possibili valori. In caso di pagamento con esito negativo sarà spedita una stringa vuota*	AN Max 12 CRT

tipoProdotto	NO	*Se abilitato viene restituito la descrizione del tipo carta usata per il pagamento (es.: consumer)*	AN Max 50 CRT
dccRate	C	*Tasso di cambio applicato basato sui tassi di cambio emessi da Global Blu. Presente solo per il servizi MCC e DCC*	AN MAX 15 CRT
mccDivisa	C	*Il codice della divisa in cui mccImporto è espresso (es.: 840=USD). Presente solo per il servizi MCC e DCC. Per i valori ammessi si veda l'appendice: 5.2*	AN 3 CRT
mccImporto	C	*Riporta l'importo in divisa espresso nel messaggio di avvio pagamento. Presente solo per il servizio MCC.*	N Max 7 CRT
dccAmount	C	*Riporta il valore dell'importo convertito nella divisa del pagatore che ha scelto di transare con l'importo convertito. La divisa utilizzata è quella riportata nel campo dccCurrency.*	N Max 7 CRT
dccCurrency	C	*Il codice della divisa in cui il dccAmount è espresso (es.: 840=USD). Presente solo per il servizi MCC e DCC. Per i valori ammessi si veda l'appendice: 5.2*	AN 3 CRT
infoc	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla compagnia in base ad accordi preventivi con la compagnia stessa*	AN Max 35 CRT
infob	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla banca in base ad accordi preventivi con la banca stessa*	AN mac 20 CRT

CALCOLO MAC:

Per il messaggio di esito transazione, il testo da firmare deve contenere i campi:

- **codTrans**
- **esito**
- **importo**
- **divisa**
- **data**
- **orario**
- **codAut**
- **stringa segreta**

Il mac sarà calcolato nel seguente modo:

> *mac= HASH SHA(codTrans=<valore codTrans>esito=<valore esito> importo=<valore importo>divisa=<valore divisa>data=<valore data>orario<valore orario>codAut=<valore codAut><chiave segreta")*

Un esempio di tale stringa potrebbe essere:

> *"codTrans=ORD_01esito=OKimporto=10divisa=EURdata=20110616orario=174003codAut=TESTOKesempiodicalcolomac"*

il campo mac sarà:

mac= HASH SHA("codTrans=ORD_01esito=OKimporto=10divisa=EURdata=20110616orario=174003codAut=TESTOKesempiodicalcolomac")

Il valore ottenuto sarà:

"d8614a933b63486417245fc313f810068ceb5804"

4.3.3. Messaggio avvio pagamento Server to server

MESSAGGIO:

Rappresenta il messaggio di richiesta di un nuovo pagamento che l'applicativo dell'esercente deve inviare al POS VIRTUALE tramite una chiamata https in GET o POST server to server e deve contenere i campi descritti nella tabella della pagina seguente.

L'URL da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/ServletS2S

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo del negozio (valore fisso comunicato da CartaSi nella fase di attivazione definitiva)*	AN Max 30 CRT
importo	C	*importo da autorizzare espresso in centesimi di euro senza sparatore, i primi 2 numeri a destra rappresentano gli euro cent, es.: 5000 corrisponde a 50,00 €. Campo obbligatorio ad esclusione di utilizzo servizio MCC*	N Max 7 CRT
divisa	C	*Il codice della divisa in cui l'importo è espresso unico valore ammesso:EUR (Euro). Campo obbligatorio ad esclusione di utilizzo servizio MCC*	AN 3 CRT
codTrans	SI	*codice di identificazione del pagamento composto da caratteri alfanumerici,* ***escluso il carattere #.*** *Il codice dev'essere univoco per ogni richiesta di autorizzazione, solo in caso di esito negativo dell'autorizzazione il merchant può riproporre la stessa richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi.*	AN Min 2 - Max 30 CRT
mail	NO	*l'indirizzo e-mail dell'acquirente al quale inviare l'esito del pagamento*	AN Max 150 CRT
url	C	*url del merchant verso la quale il POS VIRTUALE indirizza l'utente al completamento della transazione passando,in GET, i parametri di risposta con il risultato della transazione. Si veda il capitolo 4.3.6. Messaggio esito pagamento Server to server che descrive il formato del messaggio di esito*	AN Max 500 CRT

pan	C	*Numero della carta di credito. Obbligatorio solo per Primo Pagamento(PP) e per Pagamento Singolo(PA)*	AN Max 19 CRT
scadenza	SI	*Data di scadenza della carta di credito*	aaaamm
cv2	C	*Codice CVV2/CVC2 composto da 3 numeri riportato sul retro delle carte di credito VISA, MASTERCARD, MAESTRO, DINERS e JCB. 4DBC composto da 4 numeri riportato sul fronte delle carte AMERICAN EXPRESS.L'obbligatorietà dipende dalle regole previste dai singoli acquirer.*	N Max 4 CRT
Parametri aggiuntivi	NO	*Possono essere specificati n parametri aggiuntivi che verranno restituiti nei messaggi di esito. Non c'è un limite al numero di parametri aggiuntivi ma la lunghezza complessiva della stringa composta dai nomi dei parametri e il loro valore complessivamente non deve superare i 4000 caratteri.*	AN Max 4000 CRT
urlpost	C	*url del merchant verso la quale il POS VIRTUALE invia l'XML di notifica al completamento della transazione passando, in modalità server to server con metodo POST, i parametri di risposta con l'esito della transazione. La notifica a tale url verrà effettuata soltanto in presenza di una procedura asincrona ovvero transazione con carta 3D-Secure. Per quanto riguarda invece le transazioni con carte NO 3D-Secure l'XML con l'esito del pagamento viene restituito direttamente al "chiamante" (procedura sincrona).* *Si veda il capitolo 4.3.6. Messaggio esito pagamento Server to server che descrive il formato del messaggio di esito*	AN Max 500 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT
num_contratto	C	*codice dell'archivio contenente i dati sensibili (PAN, scadenza), necessario per la gestione degli addebiti "ricorrenti". Obbligatorio se "tipo_servizio"=paga_rico, paga_multi o paga_oc3d.* *Da non indicare se "tipo_servizio" non valorizzato (e quindi "tipo_richiesta"=PA)*	AN Min 5 - Max 30 CRT
tipo_servizio	C	*Se valorizzato verranno salvati i dati necessari per gestire le riscossioni .* *Può assumere i seguenti valori:* *1) "paga_rico": per pagamenti ricorrenti, cioè se sarà poi il merchant a disporre le ripetizioni (ad es. domiciliazioni, abbonamenti, ecc.);* *2) "paga_multi": per il servizio ricorrenti dove gli addebiti ricorsivi possono avvenire su un terminale differente da quello del primo pagamento/registrazione. Con questo valore è necessario valorizzare il parametro "gruppo".* *2) "paga_oc3d": per il servizio "oneclickpay", ovvero sarà il titolare della carta a scatenare le successive ricorrenze senza digitare nuovamente i dati della carta. Con questo valore è necessario valorizzare il parametro "gruppo.* *Campo da utilizzare solo per il servizio di recurring payment e*	AN Max 30 CRT

		OneClickPay.	
gruppo	C	*Valorizzare solo se tipo_servizio: "paga_multi" e "paga:oc3d" Il valore del "gruppo" viene assegnato in fase di attivazione da CartaSi*	AN Min 5 - Max 30 CRT
tipo_richiesta	SI	*PP (primo pagamento)* *PR (pagamento ricorrente)* *PA (pagamento singolo)*	AN 2 CRT
descrizione	NO	*se viene indicata in INPUT dal merchant viene restituita anche in OUTPUT altrimenti il campo è nullo*	AN Max 300 CRT
mccImporto	C	*importo da autorizzare espresso nella valuta desiderata partendo da destra con la frazione minore prevista dalla valuta stessa, per esempio il dollaro prevede 2 cifre decimali mentre lo Yen non prevede alcuna cifra decimale, quindi per indicare un pagamento di 10 dollari americani, si dovrà indicare un mccImporto="1000", mentre per indicare un pagamento di 10 Yen sarà sufficiente inviare un mccImporto="10". Campo obbligatorio da valorizzare solo per l'utilizzo del servizio MCC*	N Max 7 CRT
mccDivisa	C	*Il codice della divisa in cui l'importo è espresso, i valori ammessi sono riportati nell'appendice: 5.2. Campo obbligatorio da valorizzare solo per l'utilizzo del servizio MCC*	AN 3 CRT
PPO	NO	*Valori ammessi: Y o N. Se presente e valorizzato con Y Identifica una carta proveniente dal wallet MasterPass di MasterCard quindi il campo CVV2 diventa facoltativo. valorizzato con N identifica una carta acquisita direttamente dal merchant*	AN Max 4 CRT
OPTION_CF	C	*campo in cui il merchant invia al Virtual Pos il codice fiscale dell'utente, necessario se attivo il controllo(controllo di sicurezza opzionale attivabile su richiesta) tra codice fiscale e numero di PAN associati. Questo dato verrà riportato anche nel report interrogabile dal back Office*	AN 16 CRT
selectedcard	NO	*Se presente il campo nella chiamata valorizzato con uno dei valori riportati nell'appendice 5.5(solo i circuiti con cui il merchant ha attiva una convenzione) il pagamento viene consentito solo con il circuito di pagamento indicato.*	AN Max 12 CRT
TCONTAB	NO	*Il campo identifica la modalità di incasso che l'esercente vuole applicare alla singola transazione, se valorizzato con: I (immediata) la transazione se autorizzata viene anche incassata senza altri interventi da parte dell'esercente e senza considerare il profilo di default impostato sul terminale. Se valorizzato con D (differita) o non viene inserito il campo la transazione se autorizzata viene gestita secondo quanto definito dal profilo del terminale.*	AN 1 CRT

infoc	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla compagnia in base ad accordi preventivi con la compagnia stessa*	AN Max 35 CRT
infob	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla banca in base ad accordi preventivi con la banca stessa*	AN Max 20 CRT

NB: i valori ei campi: "url" e "urlpost" devono cominciare con "http://" o "https//"; le porte utilizzate non possono essere diverse da quelle standard: 80 o 443.
Per una corretta gestione delle chiamate si ricorda di attenersi agli standard RFC 2396 e RFC 3986

Si vedano gli esempi che seguono (riportati per semplicità con metodo GET):

richiesta autorizzazione di 1,00 Euro:

*https://ecommerce.keyclient.it/ecomm/ecomm/ServletS2S?alias=payment_test-soft&importo=100&divisa=EUR&codTrans=ID000000000025482A&mail=prova@prova.it&url=http://www.test-shoponline.aa/esito_url&urlpost=http://www.test-shoponline.aa/esito_urlpost&pan=525599******9992&scadenza=201506&cv2=123&tipo_richiesta=PA&mac=c3f2b5e07d6e3683578214bcdc93d7fcbeee2686*

richiesta autorizzazione di 12,45 Euro con parametro aggiuntivo:

*https://ecommerce.keyclient.it/ecomm/ecomm/ServletS2S?alias=payment_test-soft&importo=1245&divisa=EUR&codTrans=ID000000000025483A&mail=prova@prova.it&url=http://www.test-shoponline.aa/esito_url&urlpost=http://www.test-shoponline.aa/esito_urlpost&parametro1=valore1&pan=525599******9992&scadenza=201506&cv2=123&tipo_richiesta=PA&mac=f1ada78358acaaea85b0bb029bd74bec963c5452*

Dopo aver inviato la richiesta a tale URL, il merchant resta in attesa dell'esito di pagamento(cap. 4.3.6.), che riceverà in modalità sincrona quindi sulla stessa connessione in presenza di carte non aderenti al 3D-secure. Con carte iscritte riceverà in risposta, sempre sulla stessa connessione il messaggio AUTHRES (cap. 4.3.5.) contenete il codice HTML da stampare sul browser dell'utente.

CALCOLO MAC:
Per il messaggio di avvio transazione, il testo da firmare deve contenere i campi:

- **codTrans**
- **divisa (mccDivisa in caso di servizio MCC)**
- **importo (mccImporto in caso di servizio MCC)**
- **stringa segreta**

Il mac sarà calcolato nel seguente modo:

> *mac= HASH SHA(codTrans=<valore codTrans>divisa=<valore divisa>importo=<valore importo><chiave segreta")*

Un esempio di tale stringa potrebbe essere:

"codTrans=ID000000000125484Adivisa=EURimporto=100esempiodicalcolomac"

allora il campo mac sarà:

mac= HASH SHA("codTrans=ID000000000125484Adivisa=EURimporto=100esempiodicalcolomac")

Il valore ottenuto sarà:

"b1b46a7f201dc30c6ce40b552bd9042be8d39a44"

4.3.4. Messaggio AUTHRES gestione autenticazione 3D-Secure

MESSAGGIO:

Questo messaggio XML viene restituito dal POS VIRTUALE in risposta al messaggio di avvio transazione se il pagamento non può essere inoltrato in quanto deve essere preceduto dalla fase d'autenticazione della carta di credito del titolare prevista dai protocolli 3D-Secure. Il messaggio viene inoltrato usando la stessa connessione con cui è stato ricevuto il messaggio avvio transazione, i parametri presenti nel messaggio sono descritti nella seguente tabella.

NOME	Obb	Descrizione	Formato
TERMINAL_ID	SI	*Codice identificativo del negozio (valore fisso comunicato da CartaSi nella fase di attivazione definitiva)*	AN max 30 crt
TRANSACTION_ID	SI	*codice di identificazione del pagamento passato nel messaggio di avvio transazione nel campo codTrans.*	AN Max 30 crt
HTML_CODE	SI	*Codice HTML da restituire al browser dell'utente per reindirizzarlo verso la pagina di autenticazione dell'issuer.*	--
MAC	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 crt

NB: Il parsing delle risposte XML effettuato non deve essere validante: grazie alla evoluzione del sistema in futuro potranno essere aggiunti ulteriori elementi ai messaggi. Le applicazioni devono ignorare gli elementi sconosciuti senza provocare malfunzionamenti.

Esempio di XML restituito:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<TERMINAL_ID>7182815</TERMINAL_ID>
<AUTHRES>
<TRANSACTION_ID>ID000000000025486A</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">

<html>
<head>
<title>MDpay default response template for web</title>
</head>
```

```
<body bgcolor="#02014E" OnLoad="OnLoadEvent();" >
<form name="downloadForm"

action="https://acscartasi.ssb.it:443/pareq/3c39e31733373131633430313331313139363030650333430/3d
s/vereqauthid=31376271324E6B684F3255447533507576647O6C56644F513D3D"
    method="POST">
 <input type="hidden"
      name="PaReq"

value="eJxVUm1PwjAQ/iuE79Lry9qNHE3QYVxUQtCp38zcGlgiY3SDwL+3HUO06Yd77qXPPXfF17U1Jn4x+d4aj
c+mabKVGZTFZCiUlMBhqHExXZqdxoOxTbmtNB3BiCG5QFdk83VWtRqzfHebzLWIeACApIe4MTaJNfQnUAGTC
m4EBxUC5UjOcayyjdGKhiykAZlOYb7dV609aR669y4A9/Zbr9u2HhOCxAMk1yYWe281rvhYFvqjivm8uF+9J7O
nr+Uhjsu0rN/SNnpMJ0h8BhZZazQD2t0BDcagxsIJ7PyYbTyrnqXLgRPuVZ0dWHue6RlQH/jrQDdPa6r8pCMVus
4vCM2x3lbGZTiCXxsL0+Q6ieH3sECEcvpJOVMgQyFZxIXryKchuSq8e/BDz1s3PsalDKWKJAUKgkkplN9AF/OspRs
cDUB2tB4g8dWkXy7pV++sf1/iB2NMqeE=">
 <input type="hidden"
      name="TermUrl"
          value="https://svil-ecommerce.keyclient.it:443/mdpaympi/MerchantServer?msgid=4766030">
 <input type="hidden"
      name="MD"
          value="D6A7882ACB6D8D32645DA85B381FD3AD.ecdvas">
 <!-- To support javascript unaware/disabled browsers -->
 <noscript>
  <center>Please click the submit button below.<br>
  <input type="submit" name="submit" value="Submit"></center>
 </noscript>
</form>

<SCRIPT LANGUAGE="Javascript" >
<!-- about:blank -->
<!--
function OnLoadEvent() {
    document.downloadForm.submit();
}
//-->
</SCRIPT>
</body>
</html>
]]>
</HTML_CODE>
</AUTHRES>
<MAC>e1c2597cb5fe1f066e0008469f0b70659de6be85</MAC>
</VPOSRES>
```

NB: 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.

CALCOLO MAC:

Per il messaggio AUTHRES, il testo da firmare deve contenere i tag e relativo valore per i seguenti campi:

- **TERMINAL_ID**
- **TRANSACTION_ID**

- **HTML_CODE**
- **stringa segreta**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<TERMINAL_ID>valore</TERMINAL_ID><TRANSACTION_ID>valore</TRANSACTION_ID><HTML_CODE>valore</HTML_CODE>stringa segreta)

Un esempio di calcolo mac per un messaggio AUTHRES sarà:

```
mac= HASH SHA('<TERMINAL_ID>7182815</TERMINAL_ID>
<TRANSACTION_ID>ID0000000000025469A</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">

<html>
<head>
<title>MDpay default response template for web</title>
</head>
<body bgcolor="#02014E" OnLoad="OnLoadEvent();" >
<form name="downloadForm"

action="https://acscartasi.ssb.it:443/pareq/3c63af6a333731316334303136333131333033306137
130/3ds/vereqauthid=33377337556F4D48656B7659417264576D436547387835513D3D"
    method="POST">
 <input type="hidden"
      name="PaReq"

value="eJxVUttOAjEQ/RXCq5Hetu2WDE0QTOBBggiJ+mI23cZdlQW6RcGvt10W1KYPc+bSOXOmsCyct
eMHa/bOarizdZ292k6ZD7qJFAIz1tUwHy7sTsOndXW5qTTp4R4FdIahyJkiq7yGzOxupjOdKMYxBtRCW
Fs3HWvcHi45FRJfJwzLFBMG6BSHKltbLUlKU8IBNQjMZl95d9QsDe+dAezdhy683/YRAhQBoF8S83206l
B8KHO9eptMlth+PS9oYRS5vyoen/xMjPz3+wBQzIA881ZTTJrbIaLPcT8JtBo/ZOvYVd+uFp0weJzq5IBt7
DM8ARIDfx0Q9HS2MketZBqYnxHYw3ZT2ZARFLzYkNva6OkYXw7liVDDF8KoxDIRCWNYBUYxDdDvhK
NJFN34IB9lQiilpCRBUyK4Ys0GmljsWgbhwny8aRsBoFiN2uWidvXB+vclfgA8Gam7">
 <input type="hidden"
      name="TermUrl"
          value="https://svil-
ecommerce.keyclient.it:443/mdpaympi/MerchantServer?msgid=4766033">
 <input type="hidden"
      name="MD"
          value="4E7311C0EEF2F0C861D81963B419C637.ecdvas">
 <!-- To support javascript unaware/disabled browsers -->
 <noscript>
  <center>Please click the submit button below.<br>
  <input type="submit" name="submit" value="Submit"></center>
 </noscript>
</form>
```

```
<SCRIPT LANGUAGE="Javascript" >
<!-- about:blank -->
<!--
function OnLoadEvent() {
    document.downloadForm.submit();
}
//-->
</SCRIPT>
</body>
</html>
]]>
</HTML_CODE>esempiodicalcolomac');
```

Il valore ottenuto sarà:
"3ac3b7e96e25e8cd7f620717c5591291ae280119"

4.3.5. Messaggio esito pagamento Server to server

Il messaggio di esito viene inoltrato dal POS VIRTUALE tramite una chiamata server to server all'indirizzo riportato nel campo "urlpost" indicato dall'esercente nel messaggio di avvio transazione, al termine della fase d'autenticazione e del successivo pagamento. Inoltre, quando redirige il browser dell'acquirente verso l'indirizzo riportato nel campo url (comunicato dall'esercente nel messaggio di apertura dell'ordine) il POS VIRTUALE posta nel parametro xml il messaggio XML indicato di seguito.

L'XML contenente l'esito del pagamento è composto da due sezioni:

- StoreRequest
- StoreResponse

In StoreRequest sono replicati i campi del messaggio di avvio transazione, con eccezione del campo "pan" che sarà valorizzato con le sole ultime 4 cifre e del campo cv2 che sarà sostituito con il carattere "*" :

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo del negozio (valore fisso comunicato da CartaSi nella fase di attivazione definitiva)*	AN Max 30 CRT
importo	SI	*importo da autorizzare espresso in centesimi di euro senza sparatore, i primi 2 numeri a destra rappresentano gli euro cent, es.: 5000 corrisponde a 50,00 €*	N Max 7 CRT
divisa	SI	*Il codice della divisa in cui l'importo è espresso (EUR = Euro)*	AN 3 CRT
codTrans	SI	*codice di identificazione del pagamento composto da caratteri alfanumerici,* ***escluso il carattere #.*** *Il codice dev'essere univoco per ogni richiesta di autorizzazione, solo in caso di esito negativo dell'autorizzazione il merchant può riproporre la stessa richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi.*	AN Max 30 CRT
mail	NO	*l'indirizzo e-mail dell'acquirente al quale inviare l'esito del pagamento*	AN Max 150 CRT

pan	SI	*Numero della carta di credito parziale, vengono riportati solo gli ultimi 4 digit*	N 4 CRT
scadenza	SI	*Data di scadenza della carta di credito*	aaaamm
cv2	C	*Codice CVV2/CVC2 composto da 3 numeri riportato sul retro delle carte di credito VISA, MASTERCARD, MAESTRO, DINERS e JCB. 4DBC composto da 4 numeri riportato sul fronte delle carte AMERICAN EXPRESS. Viene riportato mascherato con: **	N Max 4 CRT
num_contratto	C	*codice dell'archivio contenente i dati sensibili (PAN, scadenza), necessario per la gestione degli addebiti "ricorrenti". Obbligatorio se "tipo_servizio"=paga_rico, paga_multi o paga_oc3d.* *Da non indicare se "tipo_servizio" non valorizzato (e quindi "tipo_richiesta"=PA)*	AN Min 5 - Max 30 CRT
tipo_servizio	C	*Se valorizzato verranno salvati i dati necessari per gestire le riscossioni .* *Può assumere i seguenti valori:* *1) "paga_rico": per pagamenti ricorrenti, cioè se sarà poi il merchant a disporre le ripetizioni (ad es. domiciliazioni, abbonamenti, ecc.);* *2) "paga_multi": per il servizio ricorrenti dove gli addebiti ricorsivi possono avvenire su un terminale differente da quello del primo pagamento/registrazione. Con questo valore è necessario valorizzare il parametro "gruppo".* *2) "paga_oc3d": per il servizio "oneclickpay", ovvero sarà il titolare della carta a scatenare le successive ricorrenze senza digitare nuovamente i dati della carta. Con questo valore è necessario valorizzare il parametro "gruppo.* *Campo da utilizzare solo per il servizio di recurring payment e OneClickPay.*	AN Max 30 CRT
gruppo	C	*Valorizzare solo se tipo_servizio: "paga_multi" e "paga:oc3d"* *Il valore del "gruppo" viene assegnato in fase di attivazione da CartaSi*	AN Min 5 - Max 30 CRT
tipo_richiesta	SI	*PP (primo pagamento)* *PR (pagamento ricorrente)* *PA (pagamento singolo)*	AN 2 CRT
descrizione	NO	*se viene indicata in INPUT dal merchant viene restituita anche in OUTPUT altrimenti il campo è nullo*	AN Max 300 CRT
PPO	NO	*Valori ammessi: Y o N. Se presente e valorizzato con Y Identifica una carta proveniente dal wallet MasterPass di MasterCard quindi il campo CVV2 diventa facoltativo. valorizzato con N identifica una carta acquisita direttamente dal merchant*	AN Max 4 CRT

In StoreResponse sono presenti i tag descritti nella seguente tabella:

NOME	Obb	Descrizione	Formato

tipoCarta	SI	*Tipo di carta utilizzata dall'utente per eseguire il pagamento. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.5*	AN Max 12 CRT
TipoTransazione	NO	*Tipo di transazione, indica il livello la modalità con cui è avvenuto il pagamento, vedere l'appendice 5.3 per i possibili valori. In caso di pagamento con esito negativo sarà spedita una stringa vuota*	AN 12 CRT
regione	NO	*Se abilitato viene restituito la macroregione di appartenenza della carta usata per il pagamento(es.: Europa)*	AN Max 6 CRT
paese	NO	*Se abilitato viene restituito il codice ISO 3166-1 alpha-3 che identifica la nazione della carta usata per il pagamento.*	AN 3 CRT codifica ISO 3166-1 alpha-3
tipoProdotto	NO	*Se abilitato viene restituito la descrizione del tipo carta usata per il pagamento (es.: consumer)*	AN 60 CRT
check	NO	*Viene valorizzato nel caso uno o più controlli previsti dal profilo dell'esercente non vengono superati.* *Controllo presenza del PAN carta su altri codici contratti sarà valorizzato con: "PGP", in base al profilo merchant il controllo se non superato può bloccare la transazione o solo notificare la presenza del pan sul altro num_contratto.* *Superati tutti i controlli il campo non sarà valorizzato.*	AN 3 CRT
codiceConvenzione	NO	*Codice esercente assegnato dall'acquirer. Dove previsto.*	AN Max 12 CRT
hash	NO	*Se previsto dal profilo dell'esercente viene restituito questo campo valorizzato con l'hash del PAN della carta utilizzata per il pagamento.*	AN 28 CRT
codiceAutorizzazione	SI	*Codice dell'autorizzazione assegnato*	AN Max 6 CRT
dataOra	SI	*Data e ora della transazione*	aaaammggThhmmss
codiceEsito	SI	*Esito della transazione. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.6*	N Max 3 CRT
descrizioneEsito	SI	*Descrizione esito della transazione. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.6*	AN Max 200 CRT
dettaglioEsito	NO	*Riporta una breve descrizione dell' esito del pagamento. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.4*	AN Max 200 CRT
ParametriAggiuntivi	NO	*Possono essere specificati n parametri aggiuntivi che verranno restituiti nei messaggi di esito. Non c'è un limite al numero di parametri aggiuntivi ma la lunghezza complessiva della stringa composta dai nomi dei parametri e il loro valore complessivamente non deve superare i 4000 caratteri.*	AN Max 4000 CRT

infoc	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla compagnia in base ad accordi preventivi con la compagnia stessa*	AN Max 35 CRT
infob	NO	*Informazione aggiuntiva relativa al singolo pagamento. Tale informazione può essere veicolata alla banca in base ad accordi preventivi con la banca stessa*	AN mac 20 CRT
dccRate	C	*Tasso di cambio applicato basato sui tassi di cambio emessi da Global Blu. Presente solo per il servizi MCC e DCC*	AN MAX 15 CRT
mccDivisa	C	*Il codice della divisa in cui l'importo è espresso, i valori ammessi sono riportati nell'appendice: 5.2. Campo obbligatorio da valorizzare solo per l'utilizzo del servizio MCC*	AN 3 CRT
mccImporto	C	*Riporta l'import in divisa espresso nel messaggio di avvio pagamento. Presente solo per il servizio MCC.*	N Max 7 CRT
dccAmount	C	*Riporta il valore dell'importo convertito nella divisa del pagatore che ha scelto di transare con l'importo convertito. La divisa utilizzata è quella riportata nel campo dccCurrency.*	N Max 7 CRT
dccCurrency	C	*Il codice della divisa in cui il dccAmount è espresso (es.: 840=USD). Presente solo per il servizi MCC e DCC. Per i valori ammessi si veda l'appendice: 5.2*	AN 3 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT

NB: Il parsing delle risposte XML effettuato non deve essere validante: grazie alla evoluzione del sistema in futuro potranno essere aggiunti ulteriori elementi ai messaggi. Le applicazioni devono ignorare gli elementi sconosciuti senza provocare malfunzionamenti

ESEMPI

Di seguito un esempio di XML di risposta per esito positivo:

```
- <RootResponse>
    - <StoreRequest>
        <alias>payment_test_XXXX</alias>
        <codTrans>XXXXXXXX-1</codTrans>
        <divisa>EUR</divisa>
        <importo>1</importo>
        <mail>xxxxx.xxxx@xxxx.it</mail>
        <scadenza>202508</scadenza>
        <pan>9992</pan>
        <cv2>***</cv2>
        < num_contratto >123456789</ num_contratto >
        < tipo_richiesta > PP </ tipo_richiesta >
        < tipo_servizio > paga_multi </ tipo_servizio >
        < gruppo >XXXX</ gruppo >
```

```
            < descrizione >sdfgfddf gdfgdfdfggdfgdfdf</ descrizione >
        </StoreRequest>
        - <StoreResponse>
            <tipoCarta>MasterCard</tipoCarta>
            <codiceAutorizzazione>TESTOK</codiceAutorizzazione>
            <dataOra>20090618T160701</dataOra>
            <codiceEsito>0</codiceEsito>
            <descrizioneEsito>autorizzazione concessa</descrizioneEsito>
            <ParametriAggiuntivi>
                <parametro1>XXXXX</parametro1>
                <parametro2>XXXXX</parametro2>
            </ParametriAggiuntivi>
            <mac>gdfdfdgdfgdfgdfgdfr3434g345gedggdf=</mac>
        </StoreResponse>
</RootResponse>
```

E un XML di risposta per esito negativo

```
- <RootResponse>
    - <StoreRequest>
        <alias>payment_test_XXXX</alias>
        <codTrans>XXXXXXXX-1</codTrans>
        <divisa>EUR</divisa>
        <importo>1</importo>
        <mail>xxxxx.xxxx@xxxx.it</mail>
        <scadenza>202508</scadenza>
        <pan>9992</pan>
        <cv2>***</cv2>
        < num_contratto >123456789</ num_contratto >
        < tipo_richiesta > PP </ tipo_richiesta >
        < tipo_servizio > paga_multi </ tipo_servizio >
        < gruppo >XXXX</ gruppo >
        < descrizione >sdfgfddf gdfgdfdfggdfgdfdf</ descrizione >
    </StoreRequest>
    - <StoreResponse>
        <tipoCarta>MasterCard</tipoCarta>
        <codiceAutorizzazione/>
        <dataOra>20090618T160701</dataOra>
        <codiceEsito>103</codiceEsito>
        <descrizioneEsito>autorizzazione negata dell'emittente della carta</descrizioneEsito>
        <ParametriAggiuntivi>
            <parametro1>XXXXX</parametro1>
            <parametro2>XXXXX</parametro2>
        </ParametriAggiuntivi>
        <mac>gdfdfdgdfgdfgdfgdfr3434g345gedggdf </mac>
    </StoreResponse>
</RootResponse>
```

CALCOLO MAC:

Per il messaggio di esito transazione server to server, il testo da firmare deve contenere i campi:

- **codTrans**

- **divisa**
- **importo**
- **codAut (nel messaggio di esito XML corrisponde al campo: codiceAutorizzazione)**
- **data (nel messaggio di esito XML corrisponde ai valori che precendono il valore "T" nel campo: dataOra)**
- **orario (nel messaggio di esito XML corrisponde ai valori che seguono il valore "T" nel campo: dataOra)**
- **stringa segreta**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(codTrans=<valore codTrans>divisa=<valore divisa> importo=<valore importo>codAut=<valore codAut>data=<valore data>orario<valore orario> <chiave segreta)

Un esempio di tale stringa potrebbe essere:

codTrans=MC9divisa=EURimporto=1codAut=data=20120202orario=161341esempiodicalcolomac

il campo mac sarà:

mac= HASH SHA(codTrans=MC9divisa=EURimporto=1codAut=data=20120202orario=161341esempiodicalcolomac)

Il valore ottenuto sarà:

9053bd3274c87fc3d810f2f4ecf9fc4f8a28420b

4.3.6. Messaggio avvio pagamento AUTHONLYREQ

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.

L'URL da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/XPayServlet

Rappresenta il messaggio XML 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	Obb	Descrizione	Formato
TERMINAL_ID	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN Max 30 CRT
TRANSACTION_ID	SI	*codice univoco che identifica l'ordine dell'esercente*	AN Max 30 CRT
REQUEST_TYPE	SI	*Valori Possibili:* *FA: Primo Tentativo* *RA :Retry di richiesta di pagamento*	AN 2 CRT
ACTION_CODE	NO	*Tipo di transazione richiesta. Sono consentiti i seguenti valori:* ***VERI:** si richiede una transazione di sola verifica autorizzativa*	AN Max 10 CRT
PAN	SI	*Numero della carta soggetta alla richiesta di pagamento*	N Max 19 CRT

EXPIRE_DATE	SI	*Data di scadenza della carta soggetta alla richiesta di pagamento*	aamm
CVV2	C	*Codice di sicurezza della carta soggetta alla richiesta di pagamento*	N Max 4 CRT
AMOUNT	SI	*importo del pagamento richiesto, è una stringa di 9 numeri fissi* *(gli ultimi 2 numeri rappresentano i 2 decimali e non è usato il separatore tra parti intere e parti decimali)*	AN Max 9 CRT
CURRENCY	SI	*Codice ISO della valuta del pagamento, unico valore attualmente gestito è 978 (Euro)*	N 3 CRT
PPO	NO	*Valori ammessi: Y o N. Se presente e valorizzato con Y Identifica una carta proveniente dal wallet MasterPass di MasterCard quindi il campo CVV2 diventa facoltativo. valorizzato con N identifica una carta acquisita direttamente dal merchant*	AN Max 4 CRT
ECI	C	*Electronic Commerce Indicator*	AN 2 CRT
XID	C	*Identificativo dell'ordine*	28 byte base64 encoding
CAVV	C	*Cardholder Autentication verification value*	28 byte base64 encoding
VERSION_CODE	SI	*Versione software della piattaforma di pagamento VPOS utilizzata, la versione a cui si riferisce il presente documento è la 01.00*	AN 5 CRT
MAC	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT

Campi:**ECI**, **XID** e **CAVV** questi tre campi vengono valorizzati per le transazioni 3D-SECURE Di seguito viene riportata la corretta valorizzazione:

Transazioni: 3D Secure

VISA	Status	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	00	NO	NO

PARes	U	30	NO	NO

Transazioni: SSL

		Eci	Cavv	Xid
		20	NO	NO

Descrizione esito VERes/PARes:

Mess. 3D Secure	VERes	Transaction
	N	Card not enrolled
	U	Unable to supply status / no response
Mess. 3D Secure	PARes	
	Y	CH passed authentication
	A	Attempt
	N	CH Failed authentication
	U	Unable to authenticate CH/ no response

Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
        <TERMINAL_ID>0000000050242004</TERMINAL_ID>
        <AUTHONLYREQ>
                <TRANSACTION_ID>T0000000000000000001</TRANSACTION_ID>
                <REQUEST_TYPE>FA</REQUEST_TYPE>
                <ACTION_CODE>VERI</ACTION_CODE>
                <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>
```

CALCOLO 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**
- **Stringa segreta**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore TERMINAL_ID ><valore TRANSACTION_ID><valore PAN><valore EXPIRE_DATE><valore CVV2><valore AMOUNT><valore CURRENCY><valore ECI><valore XID><valore CAVV><valore VERSION_CODE><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

3444151204420442363200220444123456789012345150112300000000197811NDY2NzM5MDYzICAgICAgICAgICA=AAABASEngxMzYmJJWSeDAAAAAAA=01.00esempiodicalcolomac

allora il campo mac sarà:

mac= HASH SHA(3444151204420442363200220444123456789012345150112300000000197811NDY2NzM5MDYzICAgICAgICAgICA=AAABASEngxMzYmJJWSeDAAAAAAA=01.00esempiodicalcolomac)

Il valore ottenuto sarà:

8FA9B7217C6B9400F08F48652CB7B5278FA5976F

4.3.7. Messaggio esito pagamento AUTHONLYRES

Questo messaggio XML 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:

NOME	Obb	Descrizione	Formato
TERMINAL_ID	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN Max 30 CRT
TRANSACTION_ID	SI	*codice univoco che identifica l'ordine dell'esercente*	AN Max 30 CRT
REQUEST_TYPE	SI	*Valori Possibili:* *FA: Primo Tentativo* *RA :Retry di richiesta di pagamento*	AN 2 CRT
RESPONSE	SI	*Risultato del pagamento richiesto, per i possibili valori vedere tabella sottostante*	AN Max 3 CRT

AUTH_CODE	SI	*E' il codice Autorizzazione ottenuto dall'emittente della carta di credito. In caso di pagamento con esito negativo sarà spedita una stringa vuota*	AN Min 2 - Max 6 CRT
AMOUNT	SI	*importo del pagamento richiesto, è una stringa di 9 numeri fissi* *(gli ultimi 2 numeri rappresentano i 2 decimali e non è usato il separatore tra parti intere e parti decimali)*	AN Max 9 CRT
CURRENCY	SI	*Codice ISO della valuta del pagamento, unico valore attualmente gestito è 978 (Euro)*	N 3 CRT
PPO	NO	*Valori ammessi: Y o N. Se presente e valorizzato con Y Identifica una carta proveniente dal wallet MasterPass di MasterCard quindi il campo CVV2 diventa facoltativo. valorizzato con N identifica una carta acquisita direttamente dal merchant*	AN Max 4 CRT
ECI	C	*Electronic Commerce Indicator*	AN 2 CRT
XID	C	*Identificativo dell'ordine*	28 byte base64 encoding
CAVV	C	*Cardholder Autentication verification value*	28 byte base64 encoding
TRANSACTION_DATE	SI	*Data della transazione*	gg/mm/aaaa hh.mm.ss
TRANSACTION_TYPE	SI	*Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice 5.3 per i possibili valori. In caso di pagamento con esito negativo sarà spedita una stringa vuota*	AN 30 CRT
MAC	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT

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

RESPONSE	**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 negate per medesimo TRANSACTION_ID caso RA **(*)**

(*) Il numero massimo di operazioni e 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>T000000000000000001</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>T000000000000000001</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>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del MAC di questo messaggio sono:

- **TERMINAL_ID**
- **TRANSACTION_ID**
- **RESPONSE**
- **AUTH_CODE**
- **AMOUNT**
- **CURRENCY**
- **Stringa segreta**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore TERMINAL_ID ><valore TRANSACTION_ID><valore RESPONSE><valore AUTH_CODE><valore AMOUNT><valore CURRENCY><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

3444151435843580245767543580TESTOK000000001978QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac= HASH SHA(3444151435843580245767543580TESTOK000000001978QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

85713826D82C61C067909ECA64DBC17E42B23F9B

4.4. Specifiche Messaggi operazioni dispositive e di interrogazione

4.4.1. Messaggio ECREQ

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.

L'URL da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/XPayBo

Il messaggio deve avere il seguente formato:

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo dell'esercente all'interno della piattaforma di POS virtuale*	AN Max 30 CRT
codTrans	SI	*codice univoco identificativo dell'ordine attribuito dal Virtual POS o dall'esercente (dipende dalla modalità d'integrazione scelta dall'esercente)*	AN Max 30 CRT
request_type	SI	*Valori Possibili:* *FA: Primo Tentativo* *RA :Retry di richiesta di pagamento*	AN 2 CRT fissi
id_op	SI	*Identificativo univoco dell'operazione richiesta, l'identificativo è unico per tutti i tipi di operazione*	N Max 10
type_op	SI	*Tipo di operazione richiesta, per i possibili valori vedere tabella sottostante*	AN 1 CRT
importo	SI	*Importo per cui è stata precedentemente richiesta l'autorizzazione al pagamento*	AN 9 CRT fissi
divisa	SI	*Codice ISO della valuta con cui è stata precedentemente richiesta l'autorizzazione al pagamento.*	AN 3 CRT fissi

codAut	SI	*Codice di autorizzazione ricevuto dall'esercente in risposta alla richiesta di pagamento*	AN Max 10 CRT
importo_op	SI	*Importo che l'esercente vuole sia soggetto all'operazione indicata, quindi il base al tipo di operazione richiesta è l'importo da contabilizzare/annullare/stornare.*	AN 9 CRT fissi
user	NO	*Operatore dell'esercente che ha richiesto l'operazione*	AN Max 20 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

type_op: i tipi di operazione gestiti da VPOS sono i seguenti:

type_op	Descrizione
R	Annullamento
P	Contabilizzazione
C	Storno contabile

Esempio:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
        <alias>0000000050242004</alias>
        <ECREQ>
                <codTrans>T0000000000000000001</codtrans>
                <request_type >FA</request_type>
                <id_op>0000000001</id_op>
                <type_op>C</type_op>
                <importo>000123056</importo>
                <divisa>978</divisa>
                <codAut>098765</codAut>
                <import_op>000120056</importo_op>
        </ECREQ>
        <user>User001</user>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSREQ>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **alias**
- **codTrans**
- **id_op**

- **type_op**
- **importo**
- **divisa**
- **codAut**
- **importo_op**
- **user**
- **Chiave per mac**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore alias ><valore codTrans><valore id_op><valore type_op><valore importo><valore divisa><valore codAut><valore importo_op><valore user><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

34441512493524935079893249351111111111P000000001978TESTOK000000001User001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac= HASH SHA(34441512493524935079893249351111111111P000000001978TESTOK000000001User001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

30E3B1EC1E2CA495882B9E5EF66EDD278B7B91E5

4.4.2. Messaggio ECRES

Questo messaggio viene restituito da Virtual POS 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 il Virtual POS includerà nel messaggio:

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN Max 30 CRT
codTrans	SI	*Valore indicato nel messaggio ECReq di riferimento*	AN Max 30 CRT
request_type	SI	*Valore indicato nel messaggio ECReq di riferimento*	AN 2 CRT fissi
esitoRichiesta	SI	*risultato dell'operazione richiesta. Per i possibili valori vedere tabella sottostante.*	AN Max 3 CRT
id_op	SI	*Valore indicato nel messaggio ECReq di riferimento*	N Max 10 CRT
type_op	SI	*Valore indicato nel messaggio ECReq di riferimento*	AN 1 CRT
importo_op	SI	*Valore indicato nel messaggio ECReq di riferimento*	AN 9 CRT fissi
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

- **esitoRichiesta** : 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 alias 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 codTrans 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>
<alias>0000000050242004</alias>
<ECRES>
<codTrans>T0000000000000000001</codTrans>
<request_type>FA</request_type>
<esitoRichiesta>0</esitoRichiesta>
<id_op>0000000001</id_op>
<type_op>C</type_op>
<importo_op>000120056</importo_op>
</ECRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

Esempio risultato negativo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<alias>0000000050242004</alias>
<ECRES>
<codTrans>T0000000000000000001</codTrans>
<request_type>FA</request_type>
<esitoRichiesta>32</esitoRichiesta>
<id_op>0000000001</id_op>
<type_op>C</type_op>
<importo_op>000120056</importo_op>
</ECRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
```

</VPOSRES>

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **alias**
- **codTrans**
- **esitoRichiesta**
- **id_op**
- **type_op**
- **importo_op**
- **Chiave per mac**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore alias ><valore codTrans><valore esitoRichiesta><valore id_op><valore type_op><valore importo_op><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

34441513751375119408121375105111111115P000000001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac= HASH SHA(34441513751375119408121375105111111115P000000001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

D2F08FDAF70F15120A7D1084C3579F0AABC24D68

4.4.3. Messaggio INTREQ

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

L'URL da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/XPayBo

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo dell'esercente all'interno della piattaforma del POS virtuale*	AN Max 30 CRT
codTrans	SI	*Codice univoco identificativo dell'ordine del quale l'esercente vuole conoscere la situazione.*	AN Max 30 CRT
id_op	SI	*Identificativo univoco dell'interrogazione richiesta*	N Max 10
type_op	SI	*Valorizzato sempre a V (Verifica stato ordine)*	AN 1 CRT
user	NO	*Operatore dell'esercente che ha richiesto l'interrogazione*	AN Max 20 CRT

mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
        <alias>0000000050242004</alias>
        <INTREQ>
                <codTrans>T0000000000000000001</codTrans>
                <id_op>0000000001</id_op>
                <type_op>V</type_op>
        </INTREQ>
        <user>User001</user>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSREQ>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **alias**
- **codTrans**
- **id_op**
- **type_op**
- **user**
- **Chiave per mac**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore alias ><valore codTrans><valore id_op><valore type_op><valore type_op><valore user><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

34441512493524935079893249355500000001VUser001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac= HASH SHA(34441512493524935079893249355500000001VUser001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

D8C5ED9FB446060F1794F11111F745EC75980AA4

4.4.4. Messaggio INTRES

Questo messaggio viene restituito dal POS Virtuale 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 alias, sempre presente, contenente il codice identificativo dell'esercente all'interno della piattaforma del POS Virtuale
- 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 codTrans 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 seguente tabella contiene la descrizione degli elementi che il POS Virtuale includerà nel messaggio (escluso l'elemento OPERATIONS_LIST):

NOME	Obb	Descrizione	Formato
codTrans	SI	*Valore indicato nel messaggio IntReq di riferimento*	AN Max 30 CRT
esitoRichiesta	SI	*risultato dell'interrogazione richiesta. Per i possibili valori vedere tabella sottostante.*	AN Max 3 CRT
tipoCarta	SI	*Il tipo di carta utilizzata per il pagamento.*	AN Max 12 CRT
tipoTransazione	SI	*Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice 5.3 per i possibili valori.*	AN Max 20 CRT
importo	SI	*Importo della richiesta di pagamento.*	AN 9 CRT fissi
divisa	SI	*Codice ISO della valuta della richiesta di pagamento.*	AN 3 CRT fissi
codAut	SI	*Codice di autorizzazione della richiesta di pagamento.*	AN Max 10 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	40 CRT fissi

- **esitoRichiesta** : 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 alias 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 codTrans sconosciuto (non esiste un pagamento con esito positivo

	associato all'ordine indicato) n.b. in tal caso gli elementi tipoCarta, tipoTransazione, importo, divisa, codAut del messaggio conteranno una stringa vuota e gli elementi OPTION FIELDS non saranno presenti.
3	Errore nella richiesta: Campo id_op duplicato
32	codTrans 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	Obb	Descrizione	Formato
id_op	SI	*Valore indicato nel messaggio ECReq che ha originato l'operazione o stringa vuota per operazioni non effettuate tramite ECReq.*	N Max 10
type_op	SI	*Tipo di operazione, per i possibili valori vedere tabella sottostante*	AN 1 CRT
importo_op	SI	*Importo dell'operazione*	AN 9 CRT fissi
divisa	SI	*Codice ISO della valuta dell'operazione.*	AN 3 CRT fissi
dataOra	SI	*Data in cui è stata eseguita l'operazione*	Formato: gg/mm/aaaa hh.mm.ss
result	SI	*Stato dell'operazione, per i possibili valori vedere tabella sottostante*	AN Max 3 CRT
user	NO	*Operatore dell'esercente che ha richiesto l'operazione*	AN Max 20 CRT
codiceEsito	C	*Esito della transazione. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.6 – prevista solo per type_op=A*	N MAX 3 CRT
descrizioneEsito	C	*Esito della transazione. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.6 – prevista solo per type_op=A*	AN Max 200 CRT
dettaglioEsito	C	*Riporta una breve descrizione dell' esito del pagamento. I valori possibili sono quelli riportati nella tabella dell'appendice: 5.4 – prevista solo per type_op=A*	AN Max 200 CRT

type_op: i tipi di operazione gestiti da VPOS sono i seguenti:

type_op	Descrizione
A	Autorizzazione al pagamento
R	Annullamento
P	Contabilizzazione
C	Storno contabile

result: i tipi di operazione gestiti da VPOS sono i seguenti:

type_op	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 dal VPOS 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.

Esempio di XML con esito positivo:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
    <alias>0000000050242004</alias>
    <INTRES>
        <codTrans>T0000000000000000001</codTrans>
        <esitoRichiesta>0</esitoRichiesta>
        <tipoCarta>VISA</ tipoCarta >
        <tipoTransazione>VBV_FULL</tipoTransazione>
        <importo>000123056</importo>
        <divisa>978</divisa>
        <codAut>098765</codAut>
         <OPERATIONS_LIST NUMELM="3">
            <OPERATION>
                <id_op></id_op>
                <type_op>A</type_op>
                <importo_op>000123056</importo_op>
                <divisa>978</divisa>
                <dataOra>06/07/2005 16.55.56</dataOra>
                <result>E</result>
                <user>User001</user>
                <codiceEsito>0</codiceEsito>
                <descrizioneEsito>autorizzazione concessa</descrizioneEsito>
                <dettaglioEsito>Message OK</dettaglioEsito>
            </OPERATION>
            <OPERATION>
                <id_op></id_op>
                <type_op>P</type_op>
                <importo_op>000123056</importo_op>
                <divisa>978</divisa>
```

```
                    <dataOra>06/07/2005 16.56.20</dataOra>
                    <result>E</result>
                    <user>User001</user>
                </OPERATION>
                <OPERATION>
                    <id_op>0000000001</id_op>
                    <type_op>C</type_op>
                    <importo_op>000120056</importo_op>
                    <divisa>978</divisa>
                    <dataOra>07/07/2005 16.56.20</dataOra>
                    <result>E</result>
                    <user>User001</user>
                </OPERATION>
            </OPERATIONS_LIST>
        </INTRES>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

Esempio di XML con esito negativo

```
<VPOSRES>
<alias>0000000050242004</alias>
        <INTRES>
            <codTrans>T0000000000000000001</codTrans>
            <esitoRichiesta>21</esitoRichiesta>
            <tipoCarta>VISA</tipoCarta>
            <tipoTransazione>VBV_FULL</tipoTransazione>
            <importo>000123056</importo>
            <divisa>978</divisa>
            <codAut></codAut>
            <codiceEsito>103</codiceEsito>
            <descrizioneEsito>autorizzazione negata dall'emittente della carta</descrizioneEsito>
            <dettaglioEsito>Auth. Denied</dettaglioEsito>
        </INTRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **Campo alias**
- **Campo codTrans del tag INTRES**
- **Campo esitoRichiesta del tag INTRES**
- **Campo importo del tag INTRES**
- **Campo divisa del tag INTRES**
- **Campo codAut 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 importo_op**
- **Campo divisa**
- **Campo result**
- **Campo user**
- **Chiave per mac**

I tag OPERATION devono essere considerati nell'ordine in cui sono stati inseriti nel messaggio VPOSRes inoltrato dal POS Virtuale.

Il mac sarà calcolato nel seguente modo:

> mac= HASH SHA <valore alias><valore codTrans><valore esitoRichiesta><valore importo><valore divisa><valore codAut><valore NUMELM><valore id_op><valore type_op><valore importo_op><valore divisa><valore result><valore user><Chiave per mac>)

Un esempio di tale stringa potrebbe essere:

> 3444151375137511940812137510000000001978TESTOK25550000008A000000001978EUser00151 11111115P000000001978DUser001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

> mac= HASH SHA(3444151375137511940812137510000000001978TESTOK25550000008A000000001978EUser0 015111111115P000000001978DUser001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

E3030D9555917EF67954F2935D4D663638D44A79

4.4.5. Messaggio REPREQ

Questo messaggio può essere utilizzato dall'applicativo dell'esercente per richiedere l'elenco completo delle transazioni filtrato per opportuni parametri.

Per questo tipo di richieste non è possibile fornire indicazioni sui tempi di risposta non essendo strutturati con vincoli di quantità è logico pensare che un numero elevato di richieste contemporanee possano alterare sensibilmente la risposta. ***Non si fanno quindi ipotesi di SLA per questo genere di servizio***.

L'URL da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/XPayBo

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN Max 30 CRT
id_op	SI	*Identificativo dell'interrogazione richiesta*	N Max 10
type_op	SI	*Indica il tipo di operazione per cui si richiede il report. Se valorizzato assumi i valori:* ▪ *A= autorizzazione* ▪ *R = storno autorizzativo* ▪ *P = incasso* ▪ *C = storno contabile* *T = tutte le operazioni*	AN 1 CRT
user	NO	*Operatore dell'esercente che ha richiesto l'interrogazione*	AN Max 20 CRT
start_date (*)	SI	*Data e ora di inizio*	Formato: YYYY-MM-DDThh:mm:ss
Finish_date (*)	SI	*Data e ora di fine*	Formato: YYYY-MM-DDThh:mm:ss
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

(*) La piattaforma di pagamento VPOS mette a disposizione degli esercenti i dati con una profondità di 12 mesi. Per cui il range di validità della data richiesta deve essere al più di un anno.

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
    <alias>0000000050242004</alias>
    <REPREQ>
        <id_op>1010</id_op>
        <type_op>A</type_op>
        <start_date>2006-05-15T09:00:00</start_date>
        <finish_date>2006-05-25T18:00:00</finish_date>
    </REPREQ>
    <user>User001</user>
```

<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE**</mac>**
</VPOSREQ>

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **alias**
- **id_op**
- **type_op**
- **user**
- **start_date**
- **finish_date**
- **Chiave per mac**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore alias ><valore id_op><valore type_op><valore user><valore start_date><valore finish_date><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

34441518800000001TUser0012013-02-20T14:00:002013-02-20T16:00:00QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac=HASH SHA(34441518800000001TUser0012013-02-20T14:00:002013-02-20T16:00:00QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

62922FEF3D06CEB54322880E1B0C5AB786A56D6B

4.4.6. Messaggio REPRES

Questo messaggio viene restituito dal POS Virtuale in risposta al messaggio RepReq utilizzando la stessa connessione con cui è stato ricevuta la richiesta e contiene il dettaglio del report richiesto.

Il messaggio sarà costituito dai seguenti elementi:

- un elemento alias, sempre presente, contenente il codice identificativo dell'esercente all'interno della piattaforma VPOS
- un elemento REPRES, sempre presente, composto da una lista di elementi ognuno corrispondente ad una specifica operazione (AUTH, MOV, ANNULMENT_AUTH, ANNULMENT_MOV). Ognuno di questi elementi contiene un attributo che indica il numero di transazioni presenti per la specifica operazione, eventualmente 0 se la ricerca non ha dato alcun esito.
- Ogni elemento ELEMENT_AUTH, ELEMENT_MOV, ELEMENT_ANNULMENT_AUTH, ELEMENT_ANNULMENT_MOV ripetuto per NUMELEM contiene i dati specifici della singola transazione.
- un elemento mac sempre presente, contenente il codice di sicurezza del messaggio.

La seguente tabella contiene la descrizione degli elementi che il POS Virtuale includerà nel messaggio:

NOME	Obb	Descrizione	Formato
alias	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN Max 30 CRT
esitoRichiesta	SI	*Risultato dell'interrogazione richiesta. Per i possibili valori vedere tabella sottostante.*	AN Max 3 CRT
mac	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

La struttura dell'elemento ELEMENT_AUTH, ELEMENT_MOV, ELEMENT_ANNULMENT_AUTH ed ELEMENT_ANNULMENT_MOV viene di seguito riportata:

NOME	Obb	Descrizione	Formato
codTrans	SI	*Identificativo dell'ordine all'interno della piattaforma VPOS*	AN Max 30 CRT
result	SI	*Stato dell'operazione richiesta.*	AN Max 3 CRT
tipoCarta	SI	*Il tipo di carta utilizzata per il pagamento.*	AN Max 12 CRT
tipoTransazione	SI	*Tipo di transazione, indica il livello di sicurezza con cui è avvenuto il pagamento, vedere l'Appendice 5.3 per i possibili valori.*	AN Max 20 CRT
importo	SI	*Importo della richiesta.*	AN 9 CRT fissi
divisa	SI	*Codice ISO della valuta della richiesta di pagamento.*	AN 3 CRT fissi
codAut	NO	*Codice di autorizzazione della richiesta di pagamento.*	AN Max 10 CRT
dataOra	No	*Data in cui è stata eseguita l'operazione*	Formato: gg/mm/aaaa hh.mm.ss
user	NO	*Operatore dell'esercente che ha richiesto l'operazione*	AN Max 20 CRT

result: i tipi di operazione gestiti da VPOS sono i seguenti:

type_op	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 dal VPOS 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.

esitoRichiesta : 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 alias sconosciuto o non abilitato
2	Errore nella ricerca: Errore imprevisto durante l'elaborazione della richiesta
8	Errore nella ricerca: mac errato
30	Numero di occorrenze restituite troppo elevato. Impossibile elaborare la richiesta (*)
32	codTrans chiuso per time-out, l'utente non ha completato il pagamento entro 30 minuti dalla generazione dell'ordine.
31	Errore nel campo start_date oppure finish_date per tipo formato o range superiore all'anno

(*) Al fine di ottimizzare i tempi di risposta la piattaforma VPOS non considera valide le richieste che restituiscono un numero di occorrenze (elementi) maggiore di 5000. In questo caso l'esercente dovrà riproporre la richiesta modificando i filtri costituiti dai campi start_date, finish_date e tipoTransazione

Esempio di XML con esito positivo per una richiesta in cui l'esercente vuole un report di tutte le operazioni effettuate. Si distinguono i tag AUTH = Autorizzazioni, MOV = Movimenti, ANNULMENT_AUTH = Storni autorizzativi, ANNULMENT_MOV = Storni contabili.

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
        <alias>0000000050242004</alias>
        <REPRES>
        <AUTH NUMELM="1">
         <ELEMENT_AUTH>
                <codTrans>T0000000000000000001</codTrans>
                <codiceEsito>0</codiceEsito>
                <result>E</result>
                <tipoCarta>VISA</tipoCarta>
                <tipoTransazione>VBV_FULL</tipoTransazione>
                <importo>000023056</importo>
                <divisa>978</divisa>
                <codAut>098765</codAut>
                <dataOra>06/07/2005 16.55.56</dataOra>
                <user>User001</user>
          </ELEMENT_AUTH>
        </AUTH>
        <MOV NUMELM="1">
         <ELEMENT_MOV>
                <codTrans>T0000000000000000001</codTrans>
                <codiceEsito>0</codiceEsito>
                <result>E</result>
                <tipoCarta>VISA</tipoCarta>
                <tipoTransazione>VBV_FULL</tipoTransazione>
                <importo>000023056</importo>
                <divisa>978</divisa>
```

```
            <codAut>098765</codAut>
            <dataOra>06/07/2005 16.55.56</dataOra>
            <user>User001</user>
        </ELEMENT_MOV>
    </MOV>
    <ANNULMENT_AUTH NUMELM="1">
        <ELEMENT__ANNULMENT_AUTH>
            <codTrans>T00000000000000000001</codTrans>
            <codiceEsito>0</codiceEsito>
            <result>E</result>
            <tipoCarta>VISA</tipoCarta>
            <tipoTransazione>VBV_FULL</tipoTransazione>
            <importo>000023056</importo>
            <divisa>978</divisa>
            <codAut>098765</codAut>
            <dataOra>06/07/2005 16.55.56</dataOra>
            <user>User001</user>
        </ELEMENT_ANNULMENT_AUTH>
    </ANNULMENT_AUTH>
    <ANNULMENT_MOV NUMELM="1">
        <ELEMENT__ANNULMENT_MOV>
            <codTrans>T00000000000000000001</codTrans>
            <codiceEsito>0</codiceEsito>
            <result>E</result>
            <tipoCarta>VISA</tipoCarta>
            <tipoTransazione>VBV_FULL</tipoTransazione>
            <importo>000023056</importo>
            <divisa>978</divisa>
            <codAut>098765</codAut>
            <dataOra>06/07/2005 16.55.56</dataOra>
            <user>User001</user>
        </ELEMENT_ANNULMENT_MOV>
    </ANNULMENT_MOV>
</REPRES>
<esitoRichiesta>0</esitoRichiesta>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

Esempio di XML con esito negativo per una richiesta in cui i dati richiesti dall'esercente superano il limite consentito

```
<VPOSRES>
    <alias>0000000050242004</alias>
    <REPRES/>
    <esitoRichiesta>30</esitoRichiesta>
    <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del mac di questo messaggio sono:

- **alias**
- **esitoRichiesta**
- **Chiave per mac**

Il mac sarà calcolato nel seguente modo:
mac= HASH SHA(<valore alias ><valore esitoRichiesta><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:
34441510QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:
mac=HASH SHA(34441510QKXQWGUFCKBQYHOPBNJTM

Il valore ottenuto sarà:

EABDFEDD60515D3D1BE8331E72321F8D71C61AE2

4.5. Messaggi opzione DCC

4.5.1. Messaggio verifica DCC Server to Server

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

L'url da chiamare è:

https://ecommerce.keyclient.it/ecomm/ecomm/ServletDCCREQ

DCCReq rappresenta il messaggio di richiesta del servizio DCC (Dynamic Currency Conversion) che l'applicativo dell'esercente deve inoltrare al POS Virtuale, 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	Obb	Descrizione	Formato
TERMINAL_ID	SI	*Codice identificativo dell'esercente all'interno della piattaforma VPOS*	AN 30 CRT
PAN	SI	*Numero della carta soggetta alla richiesta di pagamento. Controllo formale sul PAN è in carico all'esercente*	AN Max 19 CRT
AMOUNT	SI	*importo del pagamento richiesto*	Stringa 9 numeri fissi (gli ultimi 2 numeri rappresentano i 2

			decimali e non è usato il separatore tra parti intere e parti decimali)
USER	NO	*Operatore dell'esercente che ha richiesto l'operazione (solo per MOTO)*	AN Max 20 CRT
MAC	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN 40 CRT fissi

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>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del MAC di questo messaggio sono:

- **TERMINAL_ID**
- **PAN**
- **AMOUNT**
- **Chiave per MAC**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore TERMINAL_ID ><valore PAN><valore AMOUNT><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

3444151400609000000000200000001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac=HASH SHA(3444151400609000000000200000001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

F05D2CB70B7B87E5D5B5EFFF9F342EAE2556B301

4.5.2. Messaggio esito DCC Server to Server

VPOS 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.

La seguente tabella descrive i campi inclusi nel messaggio

NOME	Obb	Descrizione	Formato
RESPONSE	SI	*Risultato del servizio DCC richiesto, per i possibili valori vedere tabella sottostante*	AN Max 3 CRT
TICKET	SI	*Numero del ticket della richiesta del servizio DCC*	AN di 25 CRT
CURRENCY_DCC	SI	*Codice divisa estera (USD, JPY…)*	AN di lunghezza 3
AMOUNT_DCC	SI	*Importo nella valuta scelta dal titolare Esempi formato:* *000012345 JPY = 12345 JPY* *000012345 USD = 123, 45 USD* *(la divisa JPY non ha decimali)*	AN di lunghezza 9
EXCHANGE_RATE	SI	*Tasso di cambio applicato*	Numerico (8,4)
EXCHANGE_RATE _EXPIRE	SI	*Data e orario di scadenza tasso di cambio*	Data
MARK_UP	SI	*Valore fornito da Global Blue*	Numerico (8,4)
MARK_UP_DEC	SI	*Cifre decimali mark-up*	N 1 CRT
MAC	SI	*Message Code Authentication Campo di firma della transazione. Per il calcolo si vedano le indicazioni in calce a questo capitolo: CALCOLO MAC*	AN40 CRT fissi

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>1223459771149_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>
```

CALCOLO MAC:

I campi utilizzati per il calcolo del MAC di questo messaggio sono:

- **TERMINAL_ID**
- **PAN**
- **AMOUNT**
- **Chiave per MAC**

Il mac sarà calcolato nel seguente modo:

mac= HASH SHA(<valore TERMINAL_ID ><valore PAN><valore AMOUNT><Stringa segreta>)

Un esempio di tale stringa potrebbe essere:

34441514006090000000002000000001QKXQWGUFCKBQYHOPBNJTM

allora il campo mac sarà:

mac=HASH SHA(34441514006090000000002000000001QKXQWGUFCKBQYHOPBNJTM)

Il valore ottenuto sarà:

F05D2CB70B7B87E5D5B5EFFF9F342EAE2556B301

5. Appendice

5.1. Codifica languageId

Codifica campo languageId per visualizzare le pagine di cassa nelle differenti lingue disponibili:

languageId	Descrizione
ITA	Italiano
ENG	Inglese
SPA	Spagnolo
FRA	Francese
GER	Tedesco

5.2. Codifica codici mccDivisa per DCC/MCC

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
986	BRL	Brazil real (1994-)
702	SGD	Singapore dollar
784	AED	United Arab Emirates dirham
901	TWD	Taiwan new dollar
682	SAR	Saudi Arabia riyal
360	IDR	Indonesia rupiah
764	THB	Thailand baht
414	KWD	Kuwait dinar
458	MYR	Malaysia ringgit
634	QAR	Qatar riyal
484	MXN	Mexico peso
710	ZAR	South Africa rand
410	KRW	Korea, South won
985	PLN	Polish Zloty
356	INR	India rupee
608	PHP	Philippines peso
203	CZK	Czech Republic koruna
554	NZD	New Zealand dollar
152	CLP	Chile peso
946	RON	Romanian New Leu
348	HUF	Hungary forint
170	COP	Colombia peso
048	BHD	Bahrain dinar
818	EGP	Egypt pound
191	HRK	Croatia kuna
428	LVL	Latvia lat
862	VEF	Venezuelan Bolivar Fuerte
400	JOD	Jordan dinar
032	ARS	Argentina peso (1991-)
446	MOP	Macao (Macau) pataca
208	DKK	Corona Danese

5.3. Codifica tipo Transazione

tipoTransazione	Descrizione
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.
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.
M.O.T.O.	Questo valore viene utilizzato se non si tratta di una transazione di tipo commercio elettronico (che prevede la presenza dell'acquirente che acquista tramite il proprio browser) ma di una transazione Mail Order Telephone Order, in cui i dati della carta di credito sono comunicati dall'acquirente all'esercente.
AMEX_FULL	L'esercente è abilitato al protocollo SafeKey di AMEX, il titolare della carta di credito è registrato al servizio e si è correttamente autenticato.
AMEX_MERCHANT	L'esercente è abilitato al protocollo SafeKey di AMEX, ma il titolare della carta non è attivo al servizio.

5.4. Codifica messaggio dettaglio esito

Messaggio/dettaglio Esito	descrizione
Message OK	Transazione autorizzata
Controllo CF	Il PAN della carta è già associato ad altro codice Fiscale
Controllo PAN	Al codice Fiscale indicato sono già associate un numero massimo(numero accordato con CartaSi) di carta
Controllo BLACKLIST	Transazione bloccata per applicazione regole balcklist se previsto dal profilo esercente.
Controllo CF/PAN	Errore sul controllo tra Codice Fiscale e PAN, ad esempio il controllo è attivo e non viene passato dal merchant il codice Fiscale
Auth. Denied	Transazione non autorizzata
Impossibile eseguire la Post di Notifica	Transazione bloccata se il profilo dell'esercente prevede l'annullamento della transazione in caso di notifica server to server verso l'urlpost fallita.
3D Secure annullato da utente	Autenticazione 3D-Secure non completata correttamente o annullata dall'utente.
Carta non autorizzata causa applicazione regole BIN table	Transazione bloccata se non superato il controllo BIN table abilitato sul profilo esercente.

Problema 3DSecure	Impossibile completare la transazione per problemi sul 3D-Secure, ad esempio l'utente non rientra dalla fase di autenticazione o problemi sull'attivazione del profilo esercente al servizio.
expired card	Carta scaduta o data di scadenza errata
invalid merchant	Codice Esercente acquirer non correttamente abilitato o revocato.
transaction not permitted	transazione non permessa
not sufficient funds	Transazione negata per mancata disponibilità di fondi sulla carta per l'importo richiesto.
Technical problem	Problema tecnico sui sistemi autorizzativi
Host not found	Sistema autorizzativo issuer non disponibile.
Transazione chiusa per time-out	La transazione si è conclusa dopo il time-out settato sul profilo dell'esercente.
Controllo PAN/CONTRATTO	Transazione bloccata per applicazione regola check su verifica presenza PAN su altro num_contratto se previsto dal profilo esercente.

5.5. Codifica tipo carta

brand/tipoCarta/selectedcard
VISA
MasterCard
Amex
Diners
Jcb
Maestro
MYBANK(solo per brand)
SCT(solo per selectedcard)
SDD(solo per selectedcard)

5.6. Codifica codiceEsito e descrizioneEsito

codiceEsito	**DescrizioneEsito**
0	Autorizzazione concessa
20	Ordine non presente
101	Parametri errati o mancanti
102	PAN errato

103	Autorizzazione negata dall'emittente della carta
104	Errore generico
108	Ordine già registrato
109	Errore tecnico
110	Numero contratto già presente
111	Mac errato
112	Transazione negata per autenticazione VBV/SC fallita o non possibile
113	Numero contratto non presente in archivio
114	Merchant non abilitato al pagamento multiplo sul gruppo
115	Codice Gruppo non presente
116	3D Secure annullato da utente
117	Carta non autorizzata causa applicazione regole BIN Table
118	Controllo Blacklist (oppure *Controllo PAN* oppure *Controllo CF* oppure *Controllo CF/PAN)* -> esito riservato all'applicazione dei filtri
119	Esercente non abilitato ad operare in questa modalità
120	Circuito non accettato, nel messaggio di richiesta è stato indicato di accettare il pagamento con un circuito mentre il pan della carta è di altro circuito.
121	Transazione chiusa per timeout(solo su INTRES)
122	Numero di tentativi di retry sul medesimo codTrans esauriti(solo su INTRES)
400	Auth. Denied (solo su INTRES)
401	expired card (solo su INTRES)
402	restricted card (solo su INTRES)
403	invalid merchant (solo su INTRES)
404	transaction not permitted (solo su INTRES)
405	not sufficient funds (solo su INTRES)
406	Technical Problem (solo su INTRES)
407	Host not found (solo su INTRES)