mercury payment services

MonetaWeb 2.0

Ottobre 2018

INDICE

1. Introduzione

MonetaWeb è un POS virtuale di ultima generazione progettato per chi, tramite un sito internet, vuole vendere merci o servizi gestendo i pagamenti on line con carta di credito.

Chi sceglie MonetaWeb avrà i seguenti benefici:

- *Facilità di integrazione*
- *Flessibilità*: gestione dei pagamenti online attraverso i principali circuiti internazionali. Potrà essere valutata, su richiesta del Cliente, un'eventuale estensione ai circuiti American Express, Diners e JCB;
- *Sicurezza*, grazie al rispetto degli standard di sicurezza definiti dai circuiti internazionali sul (Verified by Visa e Secure Code per il circuito Mastercard);
- *Trasparenza*, perché alla tradizionale rendicontazione cartacea si affianca una rendicontazione on line tramite il sito

MonetaWeb 2.0 è una piattaforma di pagamento elettronico che mette a disposizione dei clienti una suite di protocolli e un set di metodi di pagamento a seconda delle specifiche esigenze.

Tutte le trasmissioni di dati sensibili che coinvolgano il commerciante, i sistemi di Mercury Payment Services e il cliente finale, sono crittografate secondo il protocollo HTTPS, in linea con gli standard di sicurezza imposti dai Circuiti Internazionali. I Sistemi Mercury Payment Services sono inoltre sottoposti a verifiche di sicurezza periodiche e costantemente aggiornati per garantire la protezione da eventuali vulnerabilità rilevate a carico dei protocolli standard.

Dal 2014 Mercury Payment Services è certificata PCI-DSS.

Questo documento si propone come guida per gli *sviluppatori*, non tralasciando l'aspetto funzionale.

Di seguito analizzeremo in dettaglio i vari protocolli che MonetaWeb mette a disposizione, nonché le procedure per le attivazioni, conferme, autorizzazioni e storni dei pagamenti, la struttura del file utilizzato per le procedure batch (TRINIZ), i responsecode ISO e i codici di errore restituiti dalla piattaforma.

Questa documentazione tecnica è tutto quello che serve per poter comprendere i protocolli di pagamento on-line e poterli testare in totale autonomia.

2. Specifiche di utilizzo dei Servizi

I servizi esposti da MonetaWeb supportano il protocollo HTTP con cifratura del canale e utilizzano il formato NVP per la richiesta e il formato XML per la risposta.

Di seguito i dettagli tecnici per l'invocazione ai servizi:

SPECIFICHE DI CHIAMATA

Protocollo

HTTPS

Ad oggi la minima versione supportata è TLSv1.1 ed è **fortemente consigliato** utilizzare il protocollo TLSv1.2.

Metodo

POST

Content-Type

application/x-www-form-urlencoded

URL DI TEST

https://test.monetaonline.it/monetaweb/payment/2/xml

URL DI PRODUZIONE

https://www.monetaonline.it/monetaweb/payment/2/xml

SPECIFICHE DI RISPOSTA

I messaggi di risposta alla chiamata ad uno dei servizi sincroni utilizzano il formato XML.

All'interno del paragrafo di ogni protocollo di pagamento, sono riportati degli esempi con il tracciato corretto.

CERTIFICATI DI SICUREZZA

Assicurarsi di avere installato i certificati per gli ambienti di TEST e di PRODUZIONE, riportati di seguito:

Certificato di TEST per test.monetaonline.it

Il certificato di Root è: DigiCert Global Root CA

Numero di serie: 08 3b e0 56 90 42 46 b1 a1 75 6a c9 59 91 c7 4a

La CA intermedia è: Thawte RSA CA 2018

Numero di serie: 02 5a 8a ef 19 6f 7e 0d 6c 21 04 b2 1a e6 70 2b

Certificato di PRODUZIONE per www.monetaonline.it

Il certificato di Root è: DigiCert High Assurance EV Root CA

Numero di serie: 02 ac 5c 26 6a 0b 40 9b 8f 0b 79 f2 ae 46 25 77

La CA intermedia è: DigiCert SHA2 Extended Validation Server CA

Numero di serie: 0c 79 a9 44 b0 8c 11 95 20 92 61 5f e2 6b 1d 83

3. Protocolli di Pagamento

3.1. Protocollo per pagamenti E-commerce non sicuro e MO.TO.

Con la parola MO.TO. (Mail Order/Telephone Order) indichiamo i pagamenti effettuati in modalità Server to Server, nei quali non viene richiesta l'autenticazione 3DSecure del titolare. In questi casi, la fase di pagamento si esaurisce con l'invio verso MonetaWeb di un messaggio in POST contenente tutti i dati necessari per effettuare il pagamento e la ricezione di una risposta in modalità sincrona contenente l'esito del pagamento stesso. Nei casi in cui è previsto che il titolare sottoponga i dati relativi alla propria carta di credito direttamente al sistema del Commerciante, lo stesso è soggetto alle normative PCI; Mercury Payment Services si riserva la possibilità di richiedere un documento che ne attesti la certificazione.

INVIO DEL MESSAGGIO DI PAGAMENTO

Esempio messaggio HTTP di pagamento:

id=99999999&password=99999999&operationType=pay&amount=1.00&currencyCode=978&MerchantOrderId=TrackingNo12345&description=Descrizione&cardHolderName=NomeCognome&card=1234567890123456&cvv2=123&expiryMonth=09&expiryYear=2015&customField=campoPersonalizzabile

Parametri di chiamata del messaggio HTTP di pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'pay'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76€ = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (opzionale – default '978' [euro])	varchar	3
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento (opzionale)	varchar	255
cardHolderName	Nome del titolare carta	varchar	125
card	Numero carta di credito	varchar	19
cvv2	Codice di sicurezza della carta di credito	varchar	4
expiryMonth	Mese di scadenza della carta (mm)	char	2
expiryYear	Anno di scadenza della carta (aaaa)	char	4
customField	Campo libero (opzionale)	varchar	255

RICEZIONE DEL MESSAGGIO DI ESITO

Esempio messaggio XML di esito pagamento:

```
<response>
   <result>APPROVED</result>
   <authorizationcode>123456</authorizationcode>
   <paymentid>123456789012345678</paymentid>
   <merchantorderid>TrackingNo12345</merchantorderid>
   <customfield>campoPersonalizzabile</customfield>
   <rrn>123456789012</rrn>
   <responsecode>000</responsecode>
   <description>Descrizione</description>
   <cardcountry>ITALY</cardcountry>
   <cardtype>VISA</cardtype> (solo se il terminale è abilitato alla funzionalità)
</response>
```

Parametri di risposta al messaggio di Pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco della richiesta di autorizzazione su MonetaWeb.	varchar	18
result	Esito della transazione: - APPROVED, transazione autorizzata - NOT APPROVED, transazione negata - CAPTURED, transazione confermata	varchar	20
responsecode	Codice di risposta (es: ‘000’ se transazione autorizzata, in tutti gli altri casi transazione negata)	char	3
authorizationcode	Codice di autorizzazione, valorizzato solo se la transazione è stata autorizzata	varchar	6
merchantorderid	Riferimento Operazione inviato dal commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
rrn	Riferimento univoco della transazione generato dal Sistema Autorizzativo (da utilizzare in caso di contabilizzazione esplicita a mezzo file)	varchar	12
description	Descrizione del pagamento (opzionale)	varchar	255
customfield	Campo libero inviato dal commerciante in fase di Inizializzazione	varchar	255
cardcountry	Nazionalità della carta di credito utilizzata	char	255
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di pagamento:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore:

```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

3.2. Protocollo XML Hosted 3DSecure

Il protocollo XML Hosted 3DSecure prevede la possibilità di poter effettuare pagamenti in modalità sicura in tutte le fasi della transazione; infatti il protocollo permette di transare in rispetto dei più recenti protocolli di protezione (Verified by VISA e MasterCard SecureCode), che garantiscono la non ripudiabilità della maggior parte delle transazioni, e degli standard di sicurezza PCI (Payment Card Industry) DSS (Data Security Standards).

La pagina di pagamento di MonetaWeb è disponibile in versione Web o Mobile con riconoscimento automatico del device chiamante.

I sistemi operativi mobile supportati sono:

- *iOS* per iPad e iPhone delle versioni a partire dalla 4
- *Android* per dispositivi con versione 4 e successive
- *Windows Phone* per le versioni a partire dalla 7

La pagina consente due livelli di customizzazione:

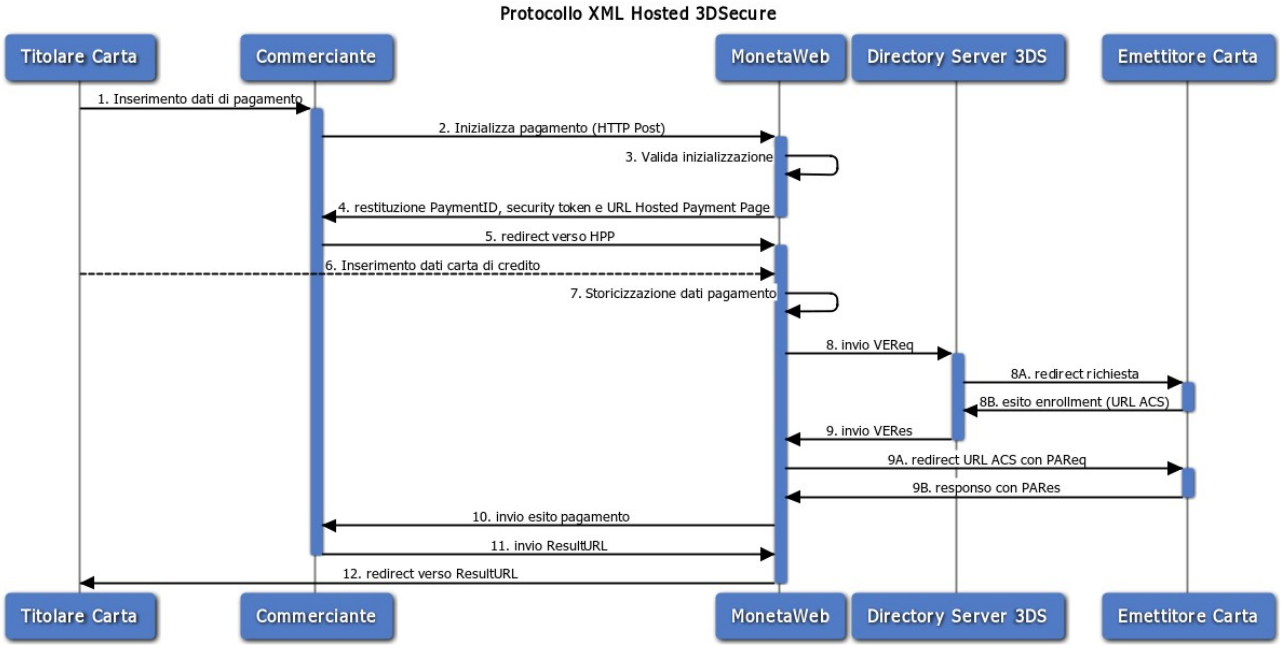
- Visualizzazione del logo del commerciante
- Personalizzazione dei file CSS, scaricabile attraverso le rispettive url:
  - [Web]: phoenix.css
  - [Mobile]: phoenix-mobile.css

Sia il logo che i file CSS modificati devono essere inviati via mail al servizio di supporto Commercio Elettronico per la validazione e la pubblicazione. Il logo deve essere in formato grafico (jpeg o png) e con una dimensione in larghezza massima di 350 pixel e altezza libera.

Il cookie generato dalla pagina di pagamento durante la navigazione è di tipo tecnico, quindi utilizzato solo a scopi statistici e non commerciali.

Per ulteriori dettagli, si rimanda alla consultazione del documento alla pagina:

http://www.mercurypayments.it/PortaleIstituzionale/file/cookie_policy.pdf.



1. Il titolare carta effettua un acquisto sul sito del commerciante; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante inizializza il pagamento con un messaggio HTTP Post
3. MonetaWeb valida l'inizializzazione
4. MonetaWeb restituisce il PaymentID, un security token e la URL della Hosted Payment Page
5. Il server del Commerciante redirige il titolare carta verso la HPP usando come parametro il PaymentID
6. Il titolare carta riempie la form con i dati sensibili della carta di credito
7. MonetaWeb storicizza i dati del pagamento
8. MonetaWeb invia una Verify Enrollment Request (VEReq) ai Directory Server dei Circuiti
   - 8A. I Directory Server dei Circuiti redirigono la richiesta verso l'Issuer
   - 8B. L'Issuer replica verso i Directory Server dei Circuiti con l'esito dell'enrollment e la URL dell'Access Control Server (ACS)
9. Directory Server dei Circuiti rispondono con una Verify Enrollment Response (VERes)
   - 9A. MonetaWeb redirige il titolare carta verso l'ACS dell'Issuer con la Payment Authentication Request (PAReq)
   - 9B. L'ACS risponde con la Payment Authentication Response (PARes)
10. MonetaWeb invia in modalità "server to server" l'esito del pagamento alla ResponseURL del Commerciante
11. MonetaWeb legge la ResultURL restituita dinamicamente dal Commerciante all'interno della pagina ResponseURL
12. Monetaweb redirige il titolare carta verso la ResultURL

Per le seguenti operazioni seguire le specifiche dei messaggi Server to Server indicate nei seguenti capitoli:

- conferma del pagamento
- storno contabile
- annullamento dell'autorizzazione
- inquiry

INIZIALIZZAZIONE DEL PAGAMENTO

La prima fase del pagamento consiste nell'invio a MonetaWeb dei dati preliminari del pagamento, come importo, valuta, riferimento ordine e url per la prosecuzione del pagamento stesso. A fronte della ricezione di questi dati, Monetaweb restituisce in output in formato XML un PaymentId univoco, un token di sicurezza e l'url della pagina per effettuare l'inserimento dei dati relativi alla carta di credito.

Esempio messaggio HTTP di Inizializzazione Pagamento:

id=99999999&password=99999999&operationType=initialize&amount=1.00&currencyCode=978&
language=ITA&responseToMerchantUrl=http://www.merchant.it/notify.jsp&
recoveryUrl=http://www.merchant.it/error.jsp&merchantOrderId=TRCK0001&description=Descrizio
ne&
cardHolderName=NomeCognome&cardHolderEmail=nome@dominio.com&
customField=campoPersonalizzabile

Parametri di chiamata del messaggio HTTP di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'initialize'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76 € = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (opzionale – default '978' [euro])	varchar	3
language	Lingua in cui verrà visualizzata la Hosted Page: • 'DEU' per TEDESCO, • 'FRA' per FRANCESE, • 'ITA' per ITALIANO, • 'POR' per PORTOGHESE, • 'RUS' per RUSSO, • 'SPA' per SPAGNOLO, • 'USA' per INGLESE	varchar	3
responseTomerchantUrl	Url verso cui notificare l'esito della transazione	varchar	2048
recoveryUrl	Url verso cui rediregere il titolare nel caso in cui non si riesca a ottenere una resultUrl in fase di notifica (opzionale)	varchar	2048
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento che verrà visualizzata nella pagina di pagamento in corrispondenza della voce "Descrizione" (opzionale)	varchar	255
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
cardHolderEmail	Indirizzo e-mail del titolare carta presso cui notificare l'esito del pagamento (opzionale)	varchar	125
customField	Campo libero che verrà restituito in fase di notifica (opzionale)	varchar	255

Esempio messaggio XML di risposta a Inizializzazione Pagamento:

```
<response>
     <paymentid>12345678901234567</paymentid>
    <securitytoken>80957febda6a467c82d34da0e0673a6e</securitytoken>
    <hostedpageurl>https://www.monetaonline.it/monetaweb/…</hostedpageurl>
</response>
```

Parametri di risposta al messaggio di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Id associato alla sessione di pagamento	varchar	18
securitytoken	Token di sicurezza	varchar	32
hostedpageurl	Url della pagina di pagamento verso cui ridirigere il titolare carta	varchar	255

Redirezione titolare carta alla pagina di pagamento:

A fronte della ricezione della risposta al messaggio di inizializzazione, è necessario redirigere la sessione web del titolare carta verso l'url specificato nel tag hostedPageUrl aggiungendo come parametro il paymentid. Tale url non deve essere impostato come parametro fisso della redirezione ma, per ogni pagamento, deve essere reperito dinamicamente dall'apposito tag. ATTENZIONE questa pagina non può essere inserita all'interno di un i-frame.

Una volta raggiunta questa pagina, il titolare carta inserirà i dati della propria carta di credito e, se la carta partecipa al protoccollo 3D Secure, verrà richiesto anche l'inserimento della relativa password 3D Secure.

NOTIFICA DELL'ESITO DEL PAGAMENTO

A fronte del corretto inserimento dei dati della carta di credito da parte del titolare, il pagamento viene processato da MonetaWeb e viene fornita al Commerciante una notifica dell'esito del pagamento stesso. La notifica viene effettuata tramite post HTTP in formato NVP (NameValue Pair) sull'url indicato nel parametro responseToMerchantUrl.

Tra i vari parametri passati in post, il securityToken è una quantità di sicurezza generata da MonetaWeb e comunicata al Commerciante sia in fase di risposta alla inizializzazione, sia in fase di notifica dell'esito; per scopi di sicurezza, si consiglia di verificare che il valore del securityToken ricevuto in fase di notifica corrisponda a quanto ricevuto in fase di inizializzazione.

Al fine di poter redirigere la sessione web del titolare verso una nuova pagina contenente l'esito della transazione, il Commerciante deve rispondere al messaggio di notifica, appena ricevuto da Monetaweb, con l'url della propria pagina di esito associando il 'paymentid' come parametro. Questo url può essere arricchito con dei parametri per consentire la corretta visualizzazione dell'esito stesso. Attenzione: la risposta non deve contenere codice HTML.

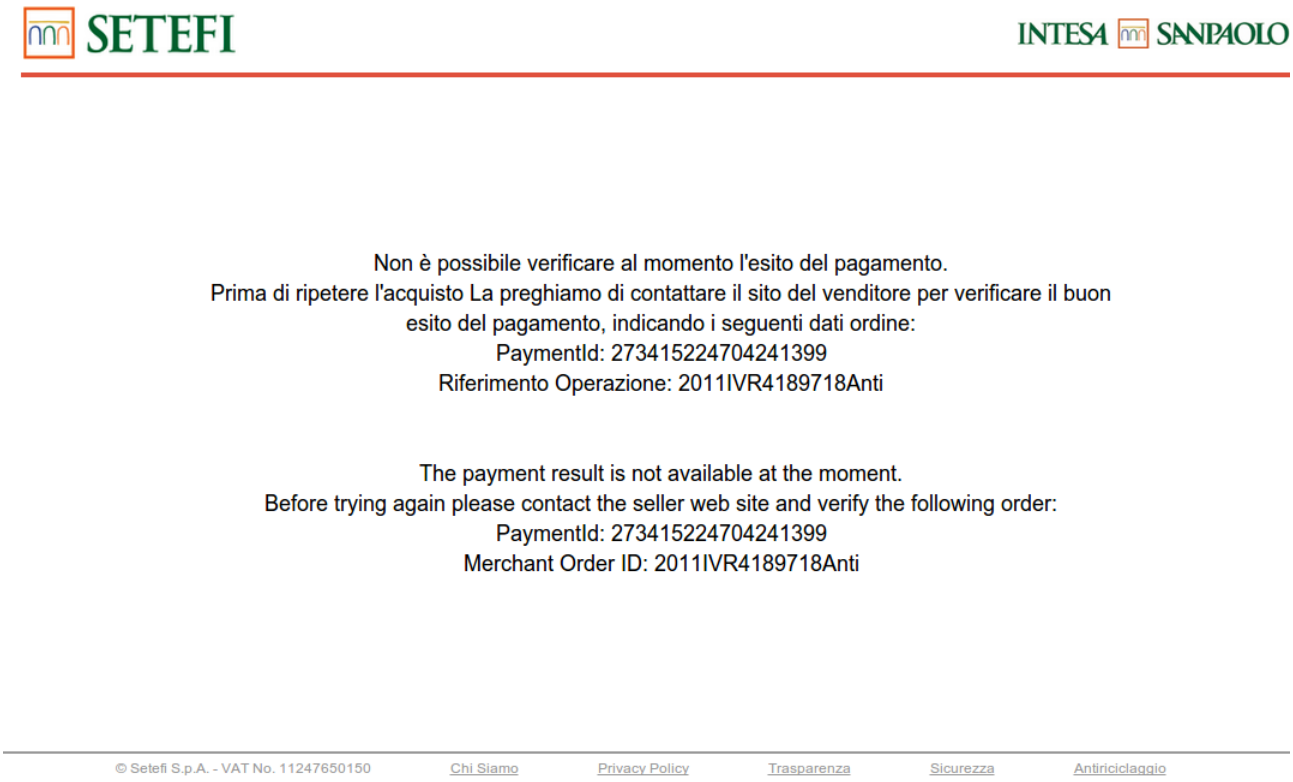
I nostri servizi, all'atto della notifica di un pagamento hosted verso la merchant response URL, una volta instaurata la connessione, attendono per 20 secondi di ricevere in risposta la URL per la redirezione finale. Allo scadere del timeout, la socket viene chiusa.

Nel caso in cui la response URL presenti un certificato self-signed o emesso da CA secondarie, è necessario fornire al supporto di MonetaWeb la catena completa in formato PEM codificati X509, pena, il fallimento della notifica dell'esito. Per eventuali import in ambiente di PRODUZIONE l'intervento andrà schedulato con almeno un mese di anticipo.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido, timeout nella risposta o certificato non riconosciuto) Monetaweb reindirizzerà il titolare verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro del messaggio di Inizializzazione. Qualora il parametro recoveryUrl non fosse stato valorizzato MonetaWeb rediregerà il titolare verso una pagina di cortesia, pubblicata direttamente sul server MonetaWeb.

Dalla pagina di dettaglio della transazione, dal portale di Back-Office, è possibile visualizzare gli errori di notifica con la relativa causale.

Ecco l'aspetto della pagina di cortesia MonetaWeb:



Esempio messaggio di esito del pagamento:

Transazione autorizzata:
authorizationcode=85963&cardcountry=ITALY&cardexpirydate=0115&cardtype=VISA&
customfield=some custom field&maskedpan=483054******1294&
merchantorderid=TRCK0001&paymentid=12345678901234567&8responsecode=000&
result=APPROVED&rrn=123456789012&securitytoken=80957febda6a467c82d34da0e0673a6e&t
hreedsecure=S

Pagamento annullato dal cardholder:
paymentid=882244493221440719, result=CANCELED, threedsecure=N

Parametri del messaggio HTTP di Notifica esito del pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito della transazione: - APPROVED, transazione autorizzata - NOT APPROVED, transazione negata - CAPTURED, transazione confermata - CANCELED, il cardholder ha annullato la transazione. *La risposta conterrà solo i parametri paymentid, result e threedsecure.*	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata, in tutti gli altri casi transazione negata)	char	3
authorizationcode	Codice di autorizzazione, valorizzato solo se la transazione è stata autorizzata	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
threedsecure	Livello di sicurezza della transazione: 'S' (transazione Full Secure), 'H' (transazione Half Secure), 'N' (transazione Not Secure)	char	1
rrn	Riferimento univoco della transazione generato dal Sistema Autorizzativo (da utilizzare in caso di contabilizzazione esplicita a mezzo file)	varchar	12
maskedpan	PAN mascherato della carta di credito utilizzata (nella forma 123456******7890)	varchar	19
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta)- ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
cardcountry	Nazionalità della carta di credito utilizzata	varchar	255
cardexpirydate	Data di scadenza della carta di credito utilizzata (nel formato mmaa)	varchar	4
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

CASI DI ERRORE

Fase di Inizializzazione:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di Inizializzazione:

```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

Fase di Notifica:

Nel caso in cui non sia possibile completare il pagamento (es. autenticazione 3DSecure fallita) MonetaWeb notifica il Commerciante con un messaggio di errore in formato NVP.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore
- il riferimento alla transazione

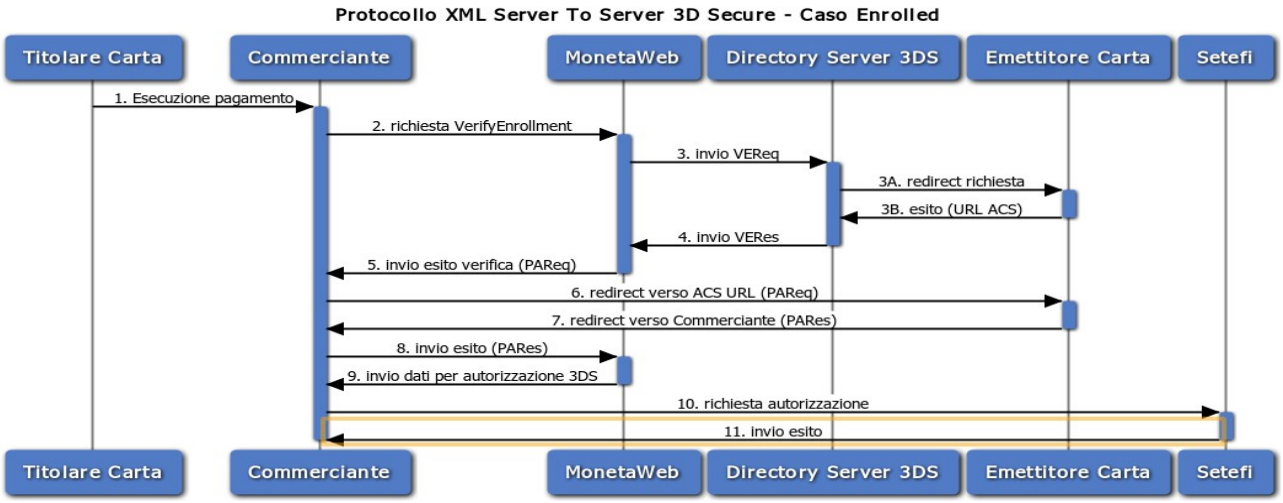
Esempio messaggio di errore in fase di Notifica:

errorcode=GV00004, errormessage=GV00004-PARes status not successful, paymentid=687192751812252579

3.3. Protocollo XML Server To Server 3D Secure

Il protocollo XML Server to Server 3D Secure consente al Commerciante di avere il controllo completo della transazione attraverso la chiamata a servizi sincroni e allo stesso tempo di beneficiare della protezione offerta dal protocollo 3D secure. Il protocollo prevede che il titolare sottoponga i dati relativi alla propria carta di credito direttamente al sistema del Commerciante, il quale è quindi soggetto alle normative PCI; Mercury Payment Services si riserva la possibilità di richiedere un documento che ne attesti la certificazione.

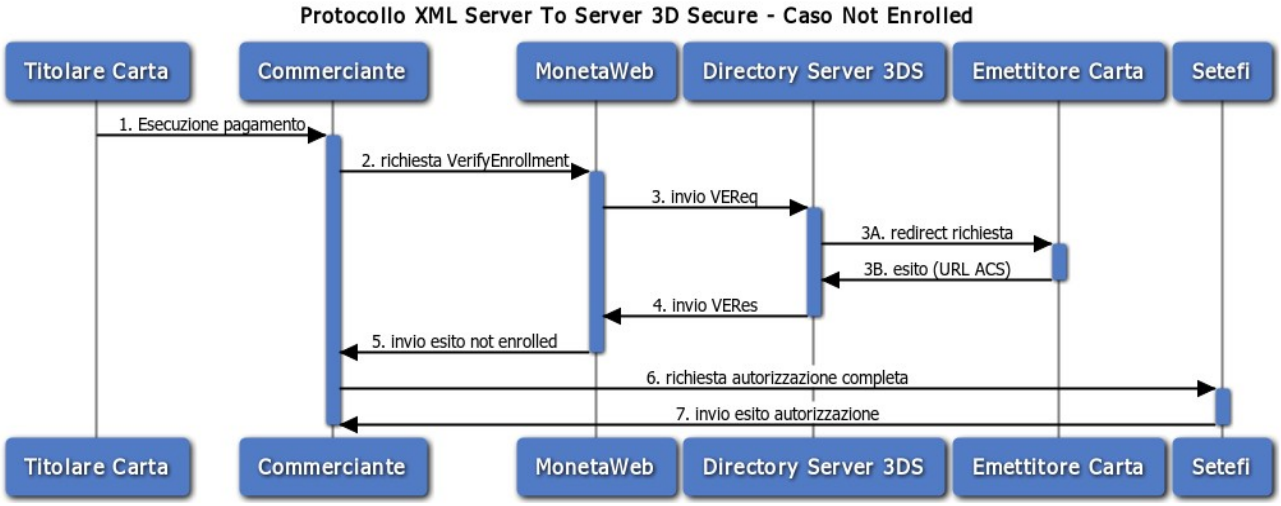
Caso Enrolled



1. Il titolare carta effettua un pagamento tramite il sito del Commerciante; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante invia un messaggio di tipo VerifyEnrollment a MonetaWeb per verificare la partecipazione della carta al protocollo 3D Secure
3. MonetaWeb invia una VEReq (Verify Enrollment Request) al dominio di interoperabilità Visa/Mastercard
   - 3A. Visa/Mastercard gira la richiesta all'Issuer
   - 3B. L'Issuer risponde a Visa/Mastercard con l'esito e la URL dell'ACS (Access Control Server)
4. Visa/Mastercard risponde con la VERes (Verify Enrollment Response)
5. MonetaWeb invia al server del Commerciante l'esito della verifica di partecipazione della carta al protocollo 3D Secure e la PAReq (Payment Authentication Request)
6. Il server del Commerciante redirige il titolare carta verso l'ACS dell'Issuer unitamente alla PAReq
7. Completata l'autenticazione, l'ACS redirige il titolare verso la pagina di ritorno del Commerciante passando come parametro la PARes (Payment Authentication Response)

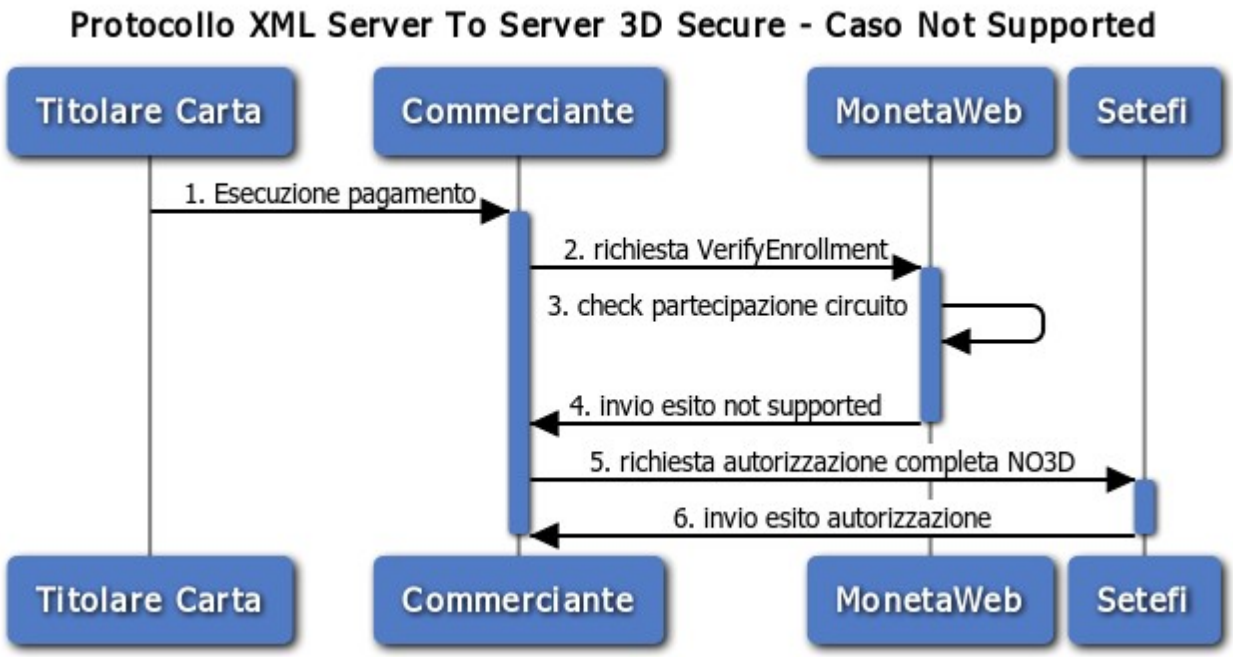
8. Il Server del Commerciante invia a MonetaWeb l'esito dell'autenticazione (PARes) tramite un messaggio di tipo verifyPares
9. MonetaWeb decifra e valida la PARes e risponde al Commerciante con i dati necessari a processare una richiesta di autorizzazione 3D Secure. In caso di autenticazione fallita, il pagamento deve essere interrotto.
10. Il Commerciante invia a Mercury Payment Services una richiesta di autorizzazione (operationtype=PAYTHREESTEP) completa di tutti i dati (dati ordine, dati carta, dati autenticazione 3D Secure)
11. MonetaWeb processa la richiesta di autorizzazione e restituisce l'esito al Commerciante.

Caso Not Enrolled



1. Il titolare carta effettua un pagamento tramite il sito del Commerciante; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante invia un messaggio di tipo VerifyEnrollment a MonetaWeb per verificare la partecipazione della carta al protocollo 3D Secure
3. MonetaWeb invia un messaggio VEReq (Verify Enrollment Request) al dominio di interoperabilità Visa/Mastercard
   3A. Visa/Mastercard gira la richiesta all'Issuer
   3B. L'Issuer risponde a Visa/Mastercard con l'esito della verifica
4. Visa/Mastercard risponde con il messaggio VERes (Verify Enrollment Response)
5. MonetaWeb risponde al Commerciante segnalando che la carta non deve effettuare l'autenticazione.
6. Il Commerciante invia a Mercury Payment Services una richiesta di autorizzazione (operationtype=PAYTHREESTEP) completa di tutti i dati (dati ordine, dati carta, flag ECI)
7. MonetaWeb processa la richiesta di autorizzazione e restituisce l'esito al Commerciante.

Caso Not Supported



1. Il titolare carta effettua un pagamento tramite il sito del Commerciante; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante invia un messaggio di tipo VerifyEnrollment a MonetaWeb
3. MonetaWeb verifica la partecipazione della carta al protocollo 3D Secure
4. MonetaWeb risponde al Commerciante segnalando che la carta non partecipa al protocollo 3DS
5. Il Commerciante invia a Mercury Payment Services una richiesta di autorizzazione NO3D (operationtype=PAY) completa di tutti i dati (dati ordine, dati carta, ...)
6. MonetaWeb processa la richiesta di autorizzazione e restituisce l'esito al Commerciante.

Per le seguenti operazioni seguire le specifiche dei messaggi Server to Server indicate nei seguenti capitoli:

- conferma del pagamento
- storno contabile
- annullamento dell'autorizzazione
- inquiry

VERIFY ENROLLMENT

All’interno del flow per i pagamenti Server to Server, è la servlet esposta per la verifica dell’enrollment della carta; riceve in input i dati del pagamento, compresi i dati sensibili relativi alla carta di credito e restituisce in output l'id univoco associato al pagamento, l’esito della verifica 3D Secure e, in caso di carta enrolled, il messaggio PaReq e la url dell’ACS.

Esempio di richiesta:

id=99999999&password=99999999&operationtype=verifyenrollment&card=4349940199997007&cvv2=892&expiryyear=2018&expirymonth=02&cardholdername=member&amount=0.1&currencycode=978&description=description&customfield=customdata&merchantorderid=order001

Parametri di richiesta:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	verifyenrollment	varchar	-
amount	Importo della transazione; si utilizza il punto come separatore dei decimali (es: 1428,76€= "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (opzionale – default '978' [euro])	varchar	3
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento (opzionale)	varchar	255
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
card	Numero carta di credito	varchar	19
cvv2	Codice di sicurezza della carta di credito	varchar	4
expiryMonth	Mese di scadenza della carta (mm)	char	2
expiryYear	Anno di scadenza della carta (aaaa)	char	4
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

Esempi di risposta:

Caso Enrolled

<response>
<result>ENROLLED</result>
<paymentid>702655129270232529</paymentid>
<customfield>customdata</customfield>
<description>description</description>
<merchantorderid>order001</merchantorderid>
<PAReq>eJxVkt1u4jAQhV8Fcb(...)</PAReq>
<url>http://www.bank.com/acs/insertPassword?brand=Visa</url>
</response>

Caso Not Enrolled

<response>
<result>NOT ENROLLED</result>
<paymentid>336725896310532529</paymentid>
<customfield>customdata</customfield>
<description>description</description>
<merchantorderid>order001</merchantorderid>
<eci>01</eci>
</response>

Caso Not Supported (Circuito non partecipante)

<response>
<result>NOT SUPPORTED</result>
<customfield>customdata</customfield>
<description>description</description>
<merchantorderid>order001</merchantorderid>
</response>

Parametri di risposta:

Nome	Descrizione	Tipo	Lunghezza
result	Esito della verifica di partecipazione al protocollo 3D Secure: • 'ENROLLED' = la carta aderisce al protocollo 3D Secure ed è provvista di credenziali di autenticazione • 'NOT ENROLLED' = la carta aderisce al protocollo 3D Secure, ma non è provvista di credenziali di autenticazione • 'NOT SUPPORTED' = la carta non aderisce al protocollo 3D Secure	varchar	20
paymentid	Id associato alla sessione di pagamento	varchar	18
customfield	Campo libero (opzionale)	varchar	255
description	Descrizione del pagamento (opzionale)	varchar	255
merchantorderid	Riferimento Operazione scelto dal Commerciante (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
eci	Electronic Commerce Indicator: indicatore del livello di sicurezza della transazione; viene restituito solo nel caso NOT ENROLLED	char	2
PaReq	Solo in caso di result ENROLLED: messaggio cifrato da inviare al sistema di autenticazione dell'emittente della carta (ACS)	varchar	max
url	URL della pagina di autenticazione esposta dalla Banca emittente (Solo per il caso ENROLLED)	varchar	2083

AUTENTICAZIONE 3D SECURE, REDIREZIONE DEL TITOLARE

In caso di carta enrolled, il Commerciante deve redirigere il titolare verso la URL della pagina di autenticazione esposta dalla Banca emittente; di seguito un esempio di costruzione del form:

```
<form name="redirect" action="<%=acsUrl%>" method="POST">
<input type=hidden name="PaReq" value="<%=pareq%>" >
<input type=hidden name="TermUrl" value="<%=termURL%>" >
<input type=hidden name="MD" value="<%=paymentId%>" >
</form>
```

Parametri della POST:

Nome	Descrizione	Tipo	Lunghezza
PaReq	Messaggio cifrato che contiene i dati del pagamento	varchar	max
TermUrl	Url di ritorno verso la quale l'ACS della Banca restituirà l'esito.	varchar	2083
MD	Id associato alla sessione di pagamento (paymentID)	varchar	18

Al termine dell'autenticazione, il titolare sarà redirezionato verso la TermUrl portando con sé due parametri: MD, identificativo della sessione di autenticazione e PaRes (Payer Authentication Response), esito cifrato dell'autenticazione. La PaRes dovrà essere girata a Mercury Payment Services per la validazione, la decodifica e l'estrazione dei valori necessari ad effettuare la richiesta di autorizzazione in modalità full/half secure.

VERIFY PARES

All’interno del flow per i pagamenti Server to Server, è la servlet esposta per la validazione del messaggio PaRes e la restituzione dei parametri 3D Secure legati alla firma del pagamento; riceve in input il messaggio PaRes, restituito dall’ACS e contenente l’esito dell’autenticazione, e ne restituisce in output una versione decriptata e semplificata.

Esempio di richiesta:

```
id=99999999&password=99999999&operationtype=verifypares&paymentid=29859709665504020
9&pares=eJydWFmzosqyfudXdKzzSPRmVGGHvU4UMyoIMolvTDKDCgry60+pPazdu(...)
```

Parametri di richiesta:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all’id terminale	varchar	50
paymentid	Id associato alla sessione di pagamento	varchar	18
operationType	verifypares	varchar	50
PaRes	Messaggio cifrato ottenuto in risposta dal sistema di autenticazione dell’emittente della carta (ACS)	varchar	max

Esempio di risposta:

<response>
<paymentid>29859709665504020 9</paymentid>
<cavv>AAACBSMAFQAAAAAAAAVAAAAAAA=</cavv>
<cavvalgo>2</cavvalgo>
<eci>05</eci>
<merchantacquirerbin>494330</merchantacquirerbin>
<currency>978</currency>
<xid>eFtyU1M8OWlhSzcmOWhNKCZXZF4=</xid>
<purchasedate>20140120 15:07:33</purchasedate>
<purchaseamount>100</purchaseamount>
<exponent>2</exponent>
<time>20140120 15:07:33</time>
<status>Y</status>
<pan>0000000000005019</pan>
<vendorcode>123456</vendorcode>
<version>1.0.2</version>
</response>

Parametri di risposta:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Id associato alla sessione di pagamento	varchar	18
cavv	Firma del pagamento	varchar	255
cavvalgo	Algoritmo di cifratura del cavv	char	2
eci	Electronic Commerce Indicator: indicatore del livello di sicurezza della transazione	char	02
merchantacquirerbin	Codice identificativo dell'Acquirer	char	6
currency	Valuta	char	3
xid	Id univoco associato al processo 3D Secure	varchar	255
purchasedate	Data di acquisto (aaaammgg hh:mm:ss)	date	-
purchaseamount	Importo	decimal	-
exponent	Numero di decimali	int	1
time	Timestamp (aaaammgg hh:mm:ss)	date	-
status	Esito dell'auteticazione: • Y, autenticazione completata con successo • N, autenticazione fallita • A, Enrollment durante il pagamento • U, problema tecnico durante l'autenticazione	char	1
pan	Pan mascherato	varchar	19
vendorcode	Codice identificativo del vendor MPI	varchar	255
version	Versione del protocollo 3D Secure	varchar	10

Comportamento atteso sulla base dell'esito dell'autenticazione:

Status Pares	Azione richiesta
Y	Richiesta di autorizzazione in modalità 3D (Full Secure)
N	Interrompere il pagamento
A	Richiesta di autorizzazione in modalità 3D (Half Secure)
U	Richiesta di autorizzazione in modalità NO 3D (eci 07)

PAY

All'interno del flow per i pagamenti Server to Server è la servlet esposta per la richiesta di autorizzazione nel caso di circuiti non partecipanti al 3D Secure (verifyenrollment con result = [**NOT SUPPORTED**]); riceve in input tutti i dati del pagamento: dati ordine, dati carta (l'eci è opzionale, se presente, deve essere valorizzato con '07'); restituisce in output l'esito del pagamento.

PAYTHREESTEP

All'interno del flow per i pagamenti Server to Server è la servlet esposta per la richiesta di autorizzazione nel caso la carta abbia eseguito l'autenticazione sul sito dell'Issuer (verifyenrollment con result = [**ENROLLED, NOT ENROLLED**]); riceve in input tutti i dati del pagamento: dati ordine, dati carta e dati 3D Secure; restituisce in output l'esito del pagamento.

Esempio di richiesta:

id=99999999&password=99999999&operationtype=paythreestep&paymentid=29859709665504020 9&amount=0.1&currencycode=978&merchantorderid=order001&description=description&cardholdername=member&card=4349940199997007&expiryyear=2018&expirymonth=02&cvv2=123&customfield=customdata&eci=05&xid=eFtyU1M8OWlhSzcmOWhNKCZXZF4=&cavv=AAACBSMAFQAAAAAAAAVAAAAAAA=

Parametri di richiesta:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	• Pay solo per i casi con result NOT SUPPORTED • Paythreestep solo per i casi con result ENROLLED, NOT ENROLLED.	varchar	-
paymentid	Id associato alla sessione di pagamento (restituito dalla Verify Enrollment), da utilizzare solo nel caso PAYTHREESTEP	varchar	18

amount	Importo della transazione; utilizzare il punto come separatore dei decimali (es: 1428,76 € = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (opzionale – default '978' [euro])	varchar	3
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento (opzionale)	varchar	255
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
card	Numero carta di credito	varchar	19
cvv2	Codice di sicurezza della carta di credito	varchar	4
expiryMonth	Mese di scadenza della carta (mm)	char	2
expiryYear	Anno di scadenza della carta (aaaa)	char	4
customField	Campo libero (opzionale)	varchar	255
eci	Electronic Commerce Indicator: indicatore del livello di sicurezza della transazione.	char	2
xid	Id univoco associato al processo 3D Secure, da utilizzare solo nel caso PAYTHREESTEP (ove restituito nella PaRes)	varchar	255
cavv	Firma del pagamento, da utilizzare solo nel caso PAYTHREESTEP (ove restituito nella PaRes)	varchar	255

L'ECI deve essere valorizzato con il valore ricevuto nella verifyenrollment nel caso di NO 3D e con il valore ricevuto nella verifypares nel caso di transazione sicura (FULL o HALF).

Esempio di risposta:

<response>
<result>APPROVED</result>
<authorizationcode>695683</authorizationcode>
<paymentid>176244506440940209</paymentid>
<merchantorderid>order001</merchantorderid>
<rrn>123456789012</rrn>
<responsecode>000</responsecode>
<cardcountry>ITALY</cardcountry>
<description>description</description>
<customfield>customdata</customfield>
</response>

Parametri di risposta:

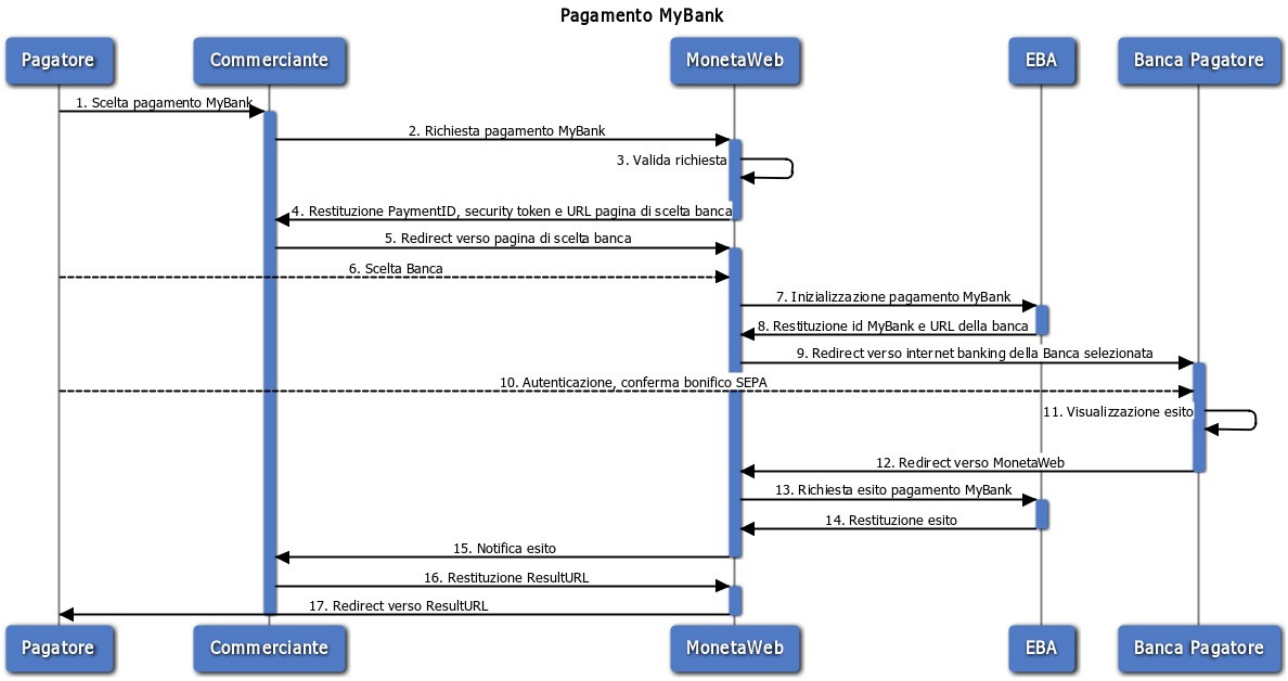
Nome	Descrizione	Tipo	Lunghezza
result	Esito della transazione: • APPROVED, transazione autorizzata • NOT APPROVED, transazione negata • CAPTURED, transazione confermata	varchar	20
authorizationcode	Codice di autorizzazione, valorizzato solo se la transazione è stata autorizzata	varchar	6
paymentid	Id associato alla sessione di pagamento (nel caso PAYTHREESTEP corrisponde al valore restituito dalla Verify Enrollment)	varchar	18
merchantorderid	Riferimento Operazione scelto dal Commerciante (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
rrn	Riferimento univoco della transazione generato dal Sistema Autorizzativo (da utilizzare in caso di contabilizzazione esplicita a mezzo file)	varchar	12
responsecode	Codice di risposta (es: ‘000’ per transazione autorizzata, negata altrimenti)	char	3
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
cardcountry	Nazionalità della carta di credito utilizzata	char	255
description	Descrizione	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

3.4. Pagamento MyBank (SEPA Credit Transfert)

MyBank è un servizio di pagamento online promosso da Eba Clearing e sostenuto dalle principali banche europee, tra cui Intesa Sanpaolo.

MyBank è una soluzione ideata per facilitare l'uso online degli strumenti di pagamento SEPA nelle operazioni di e-commerce ed e-government. Si basa su una modalità operativa che veicola le autorizzazioni elettroniche (e-authorization), relative ai pagamenti per l'e-commerce, tramite lo schema SEPA Credit Transfer.

MyBank consente al venditore online di avere subito la conferma dell'ordine di bonifico. I dettagli del pagamento relativo all'acquisto saranno automaticamente visualizzati sul sistema di online banking della propria banca e il cliente potrà confermare i dettagli della transazione autorizzando il bonifico. L'autorizzazione elettronica del cliente compratore sarà considerata irrevocabile consentendo da subito la spedizione della merce o la prestazione del servizio.



1. Il Pagatore effettua un acquisto sul sito del Commerciante scegliendo MyBank come strumento di pagamento
2. Il server del Commerciante inizializza il pagamento
3. MonetaWeb valida l'inizializzazione
4. MonetaWeb restituisce al Commerciante il PaymentID, un security token e la URL della pagina di scelta Banca
5. Il server del Commerciante redirige il Pagatore verso la pagina di scelta Banca
6. Il Pagatore sceglie la Banca tra quelle disponibili
7. MonetaWeb contatta il Routing Service di EBA
8. Il Routing Service di EBA restituisce l'id myBank e URL della banca
9. Il Pagatore viene rediretto sull'internet banking della Banca selezionata
10. Il Pagatore si autentica e trova un bonifico SEPA precompilato, conferma il pagamento

11. Il Pagatore riceve in tempo reale dalla Banca l'esito del bonifico.
12. La Banca redirige il Pagatore verso MonetaWeb
13. MonetaWeb contatta il Routing Service di EBA per conoscere l'esito del bonifico
14. Il Routing Service di EBA invia l'esito richiesto a MonetaWeb
15. MonetaWeb invia in modalità “server to server” l’esito del pagamento alla ResponseURL sul server del Commerciante
16. Il Commerciante invia sulla stessa socket la ResultURL del Commerciante
17. Monetaweb redirige il Pagatore verso la pagina di esito del Commerciante (ResultURL)

INIZIALIZZAZIONE DEL PAGAMENTO MYBANK

La prima fase del pagamento consiste nell’invio a MonetaWeb dei dati preliminari del pagamento, come importo, riferimento operazione etc. A fronte della ricezione di questi dati, Monetaweb restituisce in output in formato XML un PaymentId univoco, un token di sicurezza e l’url della pagina di scelta Banca.

Esempio messaggio HTTP di Inizializzazione Pagamento:

id=99999999&password=99999999&operationType=initializemybank&amount=1.00&responseTomerchantUrl=http://www.merchant.it/notify.jsp&recoveryUrl=http://www.merchant.it/error.jsp&merchantOrderId=TRCK0001&description=Descrizione&cardHolderName=NomeCognome&cardHolderEmail=nome@dominio.com&customField=campoPersonalizzabile

Parametri di chiamata del messaggio HTTP di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'initializemybank'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76 € = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
responseToMerchantUrl	Url verso cui notificare l'esito della transazione	varchar	2048
recoveryUrl	Url verso cui rediregere il titolare nel caso in cui non si riesca a ottenere una resultUrl in fase di notifica (opzionale)	varchar	2048
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento che verrà visualizzata nella causale del bonifico a discrezione della Banca. Il set dei caratteri accettato è la codifica ISO UTF-8. I caratteri ammissibili sono alfanumerici e solo il seguente set di simboli ammessi: / - ? : ( ) . , ' + Spazio (opzionale)	varchar	128
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
cardHolderEmail	Indirizzo e-mail del titolare carta presso cui notificare l'esito del pagamento (opzionale)	varchar	125
customField	Campo libero (opzionale)	varchar	255

Esempio messaggio XML di risposta a Inizializzazione Pagamento:

```
<response>
    <paymentid>123456789012345678</paymentid>
    <securitytoken>80957febda6a467c82d34da0e0673a6e</securitytoken>
    <hostedpageurl>https://www.monetaonline.it/monetaweb/mybank/selection</hostedpageurl>
</response>
```

Parametri di risposta al messaggio di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Id associato alla sessione di pagamento	varchar	18
securitytoken	Token di sicurezza	varchar	32
hostedpageurl	Url della pagina di scelta Banca	varchar	255

Redirezione pagatore alla pagina di scelta Banca:

A fronte della ricezione della risposta al messaggio di inizializzazione, è necessario redirigere la sessione web del pagatore verso l'url specificato nel tag hostedpageurl, alla quale va appeso il parametro paymentid. Tale url non deve essere considerata come valore fisso ma, per ogni pagamento, deve essere reperita dinamicamente dall'apposito tag.

Una volta raggiunta questa pagina, il pagatore dovrà selezionare la Banca su cui effetuare il bonifico. Nel caso in cui il Pagatore non trovasse la propria Banca nell'elenco di quelle partecipanti, vi è la possibilità di passare al pagamento con carta di credito. In questo caso il tracciato della notifica di risposta sarà quello del pagamento con carta. È possibile inibire il passaggio al pagamento con carta di credito, inviando una richiesta al servizio di supporto Commercio Elettronico.

NOTIFICA DELL'ESITO DEL PAGAMENTO

Una volta autenticatosi sull'home banking, il pagatore troverà un bonifico SEPA precompilato che potrà confermare. Ricevuto l'esito del bonifico dalla Banca, il pagatore, per proseguire, dovrà cliccare il pulsante predisposto dalla Banca e sarà rediretto su una pagina di transizione di MonetaWeb. A questo punto viene fornita al Commerciante una notifica dell'esito del pagamento stesso. La notifica viene effettuata tramite post HTTP in formato NVP (NameValue Pair) sull'url indicato nel parametro responseToMerchantUrl.

Tra i vari parametri passati in post, il securityToken è una quantità di sicurezza generata da MonetaWeb e comunicata al Commerciante sia in fase di risposta alla inizializzazione, sia in fase di notifica dell'esito; per scopi di sicurezza, si consiglia di verificare che il valore del securityToken ricevuto in fase di notifica corrisponda a quanto ricevuto in fase di inizializzazione.

Al fine di poter redirigere la sessione web del pagatore verso una nuova pagina contenente l'esito della transazione, il Commerciante deve rispondere al messaggio di notifica, appena ricevuto da Monetaweb, con l'url della propria pagina di esito associando il 'paymentid' come parametro. Questo url può essere arricchito con dei parametri custom per consentire la corretta visualizzazione dell'esito stesso. Attenzione: la risposta non deve contenere codice HTML.

I nostri servizi, all'atto della notifica di un pagamento hosted verso la merchant response URL, una volta instaurata la connessione, attendono per 20 secondi di ricevere in risposta la URL per la redirezione finale. Allo scadere del timeout, la socket viene chiusa.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido e timeout nella risposta) Monetaweb reindirizzerà il titolare verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro del messaggio di Inizializzazione. Qualora il parametro recoveryUrl non fosse stato valorizzato MonetaWeb rediregerà il titolare verso una pagina di cortesia, pubblicata direttamente sul server MonetaWeb.

Il protocollo MyBank, definito dal consorzio EBA, prevede che la risposta verso il Commerciante venga inviata solo dopo che il Pagatore (Intestatario del conto) abbia fatto ritorno dalla pagina della Banca che ha scelto per effettuare il bonifico. Nei casi in cui il Pagatore non faccia ritorno dalla pagina della propria Banca e interrompa quindi il processo di pagamento, come da protocollo, il gateway offre la possibilità, attraverso lo strumento di inquiry, di conoscere in qualsiasi momento lo stato della transazione. L'integrazione MyBank è soggetta a certificazione e pertanto aderisce al protocollo del consorzio EBA.

Parametri del messaggio HTTP di Notifica esito del pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito della transazione: • AUTHORISED: bonifico autorizzato dalla Banca del pagatore • ERROR: bonifico non completato poiché negato dalla Banca del pagatore • AUTHORISINGPARTYABORTED: bonifico abbandonato dal pagatore (a seguito dell'accesso al portale della Banca) • CANCELED*: pagamento annullato dal pagatore (prima dell'accesso al portale della Banca). La risposta conterrà solo i parametri paymentid e result. • TIMEOUT: pagamento non confermato entro il limite stabilito (in genere di 15 minuti) • PENDING: pagamento in attesa che la Banca comunichi l'esito	varchar	32
description	Descrizione del pagamento inviato dal Commerciante in fase di Inizializzazione	varchar	128
authorizationcode	End-to-end ID del pagamento	varchar	35
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
mybankid	Identificativo univoco del pagamento rilasciato dal circuito myBank	numeric	35
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

Update automatico delle transazioni MyBank:

Tutti i pagamenti MyBank assumono lo stato PENDING (sui sistemi Mercury Payment Services) in attesa che la Banca comunichi l'esito del bonifico. Il pagatore ha tempo 15 minuti, dall'inizio della transazione, per confermare il bonifico. Oltre questo limite lo stato del pagamento sarà impostato a TIMEOUT dalla Banca.
Se il bonifico verrà autorizzato (AUTHORISED) o negato (ERROR) dalla Banca oppure annullato (AUTHORISINGPARTYABORTED) dal pagatore sull'homebanking, lo stato sarà aggiornato coerentemente.
Quando il pagatore non raggiunge o non fa ritorno dalla pagina della Banca, lo stato resterà PENDING sui sistemi Mercury Payment Services, ma il merchant non riceverà notifica.
Un batch automatico aggiornerà, ogni 8 minuti, interrogando i servizi MyBank, lo stato di eventuali pagamenti pending. È possibile forzare l'aggiornamento dello stato di un pagamento in stato pending in qualsiasi momento attraverso il servizio di inquirymybank.
Il pagamento potrà assumere lo stato CANCELED nei seguenti scenari:

- Qualora non fosse possibile associare uno stato finale ad un pagamento (aggiornamento batch, il Commerciante non riceverà alcuna notifica)
- Qualora il pagatore dovesse abbandonare la sessione prima della scelta Banca (aggiornamento batch, il Commerciante non riceverà alcuna notifica)
- Qualora il pagatore dovesse cliccare su “Annulla la transazione” dalla pagina di scelta banca (Il commerciante riceverà relativa notifica)

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di Inizializzazione:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell’errore

Esempio messaggio di errore in fase di Inizializzazione:

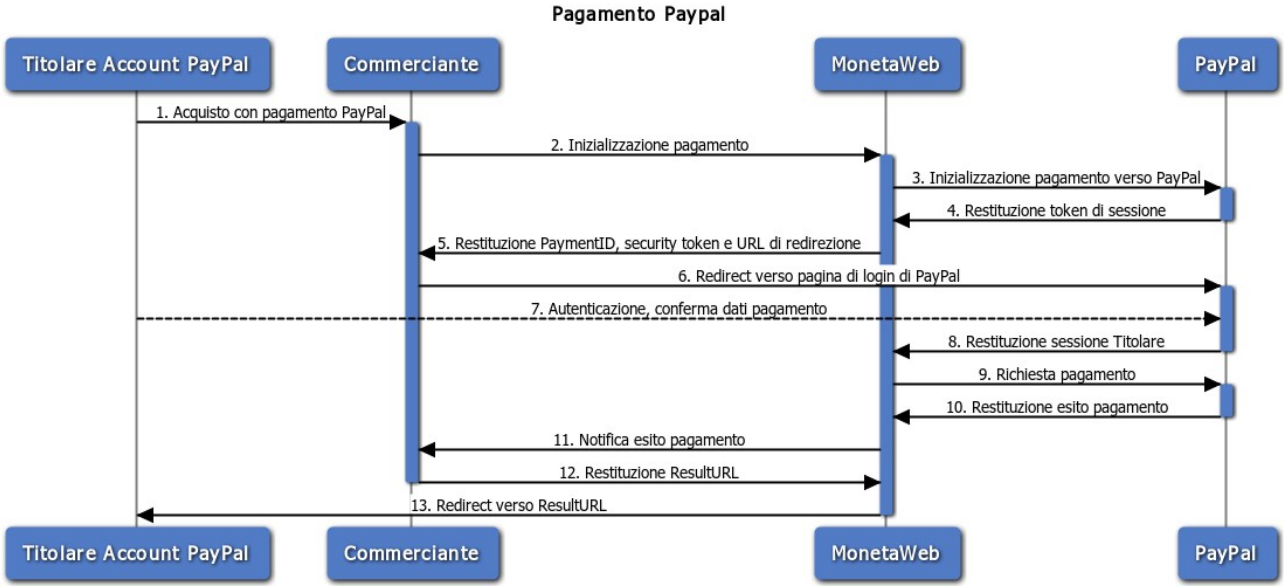
```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

3.5. Pagamento PayPal

Paypal è un servizio di trasferimento di denaro nato proprio per rendere più sicure le transazioni online sia per i compratori, sia per i venditori. E' possibile spedire e ricevere denaro in tutta sicurezza non fornendo i numeri della carta di credito ma solamente l'indirizzo e-mail.

Cliccando su Guida PayPal è possibile scaricare la guida contenente le indicazioni per la configurazione del profilo e la pubblicazione del pulsante di pagamento, attività propedeutiche all'integrazione con MonetaWeb.

Per il passaggio in PRODUZIONE comunicare il proprio "Codice conto commerciante" PayPal a Commercio Elettronico. Per poter risalire al proprio "Codice conto commerciante", una volta loggati alla piattaforma PayPal™, nella sezione "Profilo" troverete l'omonima dicitura con un codice alfanumerico.



1. Il titolare carta effettua un acquisto sul sito del Commerciante, scegliendo PayPal come strumento di pagamento; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante inizializza il pagamento con un messaggio HTTP Post
3. MonetaWeb inizializza il pagamemento verso PayPal
4. PayPal restituisce un tocken di sessione
5. Monetaweb restituisce al Commerciante il PaymentID, il security token e la URL per la redirezione del titolare
6. Il server del Commerciante redirige il titolare carta verso la login page di PayPal
7. Il titolare carta inserisce le proprie credenziali PayPal, sceglie lo strumento di pagamento e l'eventuale indirizzo di spedizione e autorizza il pagamento
8. PayPal restitusce a MonetaWeb la sessione del Titolare
9. MonetaWeb invia a PayPal una richiesta di pagamento
10. PayPal processa il pagamento e restituisce un esito a MonetaWeb
11. MonetaWeb notifica in modalità "server to server" l'esito del pagamento alla ResponseURL del Commerciante
12. Il Commerciante restituisce a MonetaWeb la ResultURL
13. Monetaweb redirige il titolare carta verso la ResultURL per la visualizzazione dell'esito finale.

INIZIALIZZAZIONE DEL PAGAMENTO

La prima fase del pagamento consiste nell'invio a MonetaWeb dei dati preliminari del pagamento, come importo, valuta, riferimento ordine e url per la prosecuzione del pagamento stesso. A fronte della ricezione di questi dati, Monetaweb restituisce in output in formato XML un PaymentId univoco, un token di sicurezza e l'url della pagina verso cui redirigere il titolare.

Esempio messaggio HTTP di Inizializzazione Pagamento:

id=99999999&password=99999999&operationType=initializepaypal&amount=1.00&responseToMerchantUrl=http://www.merchant.it/notify.jsp&
recoveryUrl=http://www.merchant.it/error.jsp&merchantOrderId=TRCK0001&description=Descrizione&
cardHolderName=NomeCognome&cardHolderEmail=nome@dominio.com&
customField=campoPersonalizzabile

Parametri di chiamata del messaggio HTTP di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'initializepaypal'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76 € = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
ResponseToMerchantUrl	Url verso cui notificare l'esito della transazione	varchar	2048
recoveryUrl	Url verso cui rediregere il titolare nel caso in cui non si riesca a ottenere una resultUrl in fase di notifica (opzionale)	varchar	2048
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento (opzionale)	varchar	255
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
cardHolderEmail	Indirizzo e-mail del titolare carta presso cui notificare l'esito del pagamento (opzionale)	varchar	125
customField	Campo libero (opzionale)	varchar	255
shippingname *	Nome della persona associata all'indirizzo (consigliato in caso di spedizione)	varchar	32
shippingstreet *	Indirizzo di spedizione (consigliato in caso di spedizione)	varchar	100
shippingcity *	Nome della città (consigliato in caso di spedizione)	varchar	40

shippingstate *	Nome dello Stato o provincia (consigliato in caso di spedizione)	varchar	40
shippingzip *	Codice di avviamento postale (CAP) del paese di spedizione (consigliato negli Stati Uniti e nei Paesi laddove richiesto, in caso di spedizione)	varchar	20
shippingcountry *	Codice del Paese di spedizione, es. IT, NL, ES … (consigliato in caso di spedizione)	varchar	2
Shippingphone *	Riferimento telefonico (consigliato in caso di spedizione)	varchar	20

** I campi riguardanti l'indirizzo di spedizione possono abilitare la protezione venditore fornita da PayPal. Per maggiori informazioni a riguardo si prega di fare diretto riferimento a PayPal.*

Esempio messaggio XML di risposta a Inizializzazione Pagamento:

<response>
<paymentid>945288470910940699</paymentid>
<hostedpageurl>https://www.monetaonline.it/monetaweb/hosted/thirdparty</hostedpageurl>
<securitytoken>07dc08f9bde84c7aa0481d8e604c91e9</securitytoken>
</response>

Parametri di risposta al messaggio di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Id associato alla sessione di pagamento	varchar	18
securitytoken	Token di sicurezza	varchar	32
hostedpageurl	Url della pagina verso cui ridirigere il titolare carta	varchar	255

Redirezione titolare carta alla pagina di PayPal:

A fronte della ricezione della risposta al messaggio di inizializzazione, è necessario redirigere la sessione web del titolare carta verso la url specificata nel tag hostedPageUrl aggiungendo come parametro il paymentid. Tale url non deve essere impostato come parametro fisso della redirezione ma, per ogni pagamento, deve essere reperito dinamicamente dall'apposito tag.

NOTIFICA DELL'ESITO DEL PAGAMENTO

Sulla base delle scelte operate dal titolare, attraverso il proprio account, PayPal processa il pagamento e ne comunica l'esito a MonetaWeb; il Commerciante riceve quindi una notifica tramite post HTTP in formato NVP (NameValue Pair) sull'url indicato nel parametro responseToMerchantUrl.

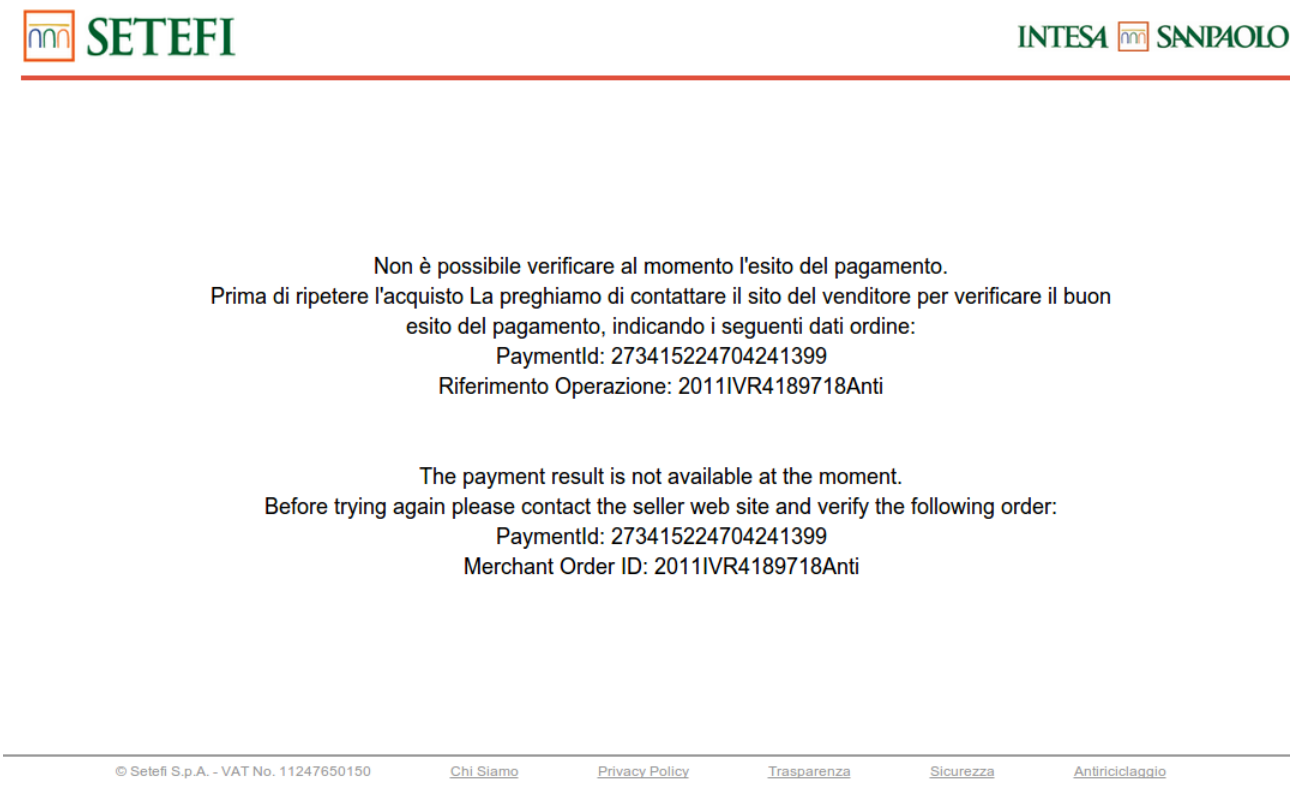
Tra i vari parametri passati in post, il securityToken è una quantità di sicurezza generata da MonetaWeb e comunicata al Commerciante sia in fase di risposta alla inizializzazione, sia in fase di notifica dell'esito; per scopi di sicurezza, si consiglia di verificare che il valore del securityToken ricevuto in fase di notifica corrisponda a quanto ricevuto in fase di inizializzazione.

Al fine di poter redirigere la sessione web del titolare verso una nuova pagina contenente l'esito della transazione, il Commerciante deve rispondere al messaggio di notifica, appena ricevuto da Monetaweb, con l'url della propria pagina di esito associando il 'paymentid' come parametro. Questo url può essere arricchito con dei parametri per consentire la corretta visualizzazione dell'esito stesso. Attenzione: la risposta non deve contenere codice HTML.

I nostri servizi, all'atto della notifica di un pagamento hosted verso la merchant response URL, una volta instaurata la connessione, attendono per 20 secondi di ricevere in risposta la URL per la redirezione finale. Allo scadere del timeout, la socket viene chiusa.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido e timeout nella risposta) Monetaweb reindirizzerà il titolare verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro del messaggio di Inizializzazione. Qualora il parametro recoveryUrl non fosse stato valorizzato MonetaWeb rediregerà il titolare verso una pagina di cortesia, pubblicata direttamente sul server MonetaWeb.

Ecco l'aspetto della pagina di cortesia MonetaWeb:



Esempio messaggio di esito del pagamento:

Message sent to merchant at url [http://www.merchant.it/notify.jsp] with data: {authorizationcode=, cardcountry=, cardexpirydate=, cardtype=PAYPAL, customfield=some custom field, maskedpan=, merchantorderid=2011IVR4189718Anti, paymentid=945288470910940699, responsecode=000, result=APPROVED, rrn=, securitytoken=07dc08f9bde84c7aa0481d8e604c91e9, threedsecure=N}

Parametri del messaggio HTTP di Notifica esito del pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito della transazione: - APPROVED, transazione autorizzata - CAPTURED, transazione confermata - PENDING, transazione sospesa in attesa di verifica (Per eventuali aggiornamenti fare ricorso al backoffice di Paypal)	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata, in tutti gli altri casi transazione negata)	char	3
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
cardcountry	Nazionalità della carta di credito utilizzata	varchar	255
cardexpirydate	Data di scadenza della carta di credito utilizzata (nel formato mmaa)	varchar	4
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

CASI DI ERRORE

Fase di Inizializzazione:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di inizializzazione:

```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

Fase di notifica:

Nel caso di transazione negata dal sistema PayPal, MonetaWeb notifica il Commerciante con un messaggio di errore in formato NVP.
Tale messaggio comprende:

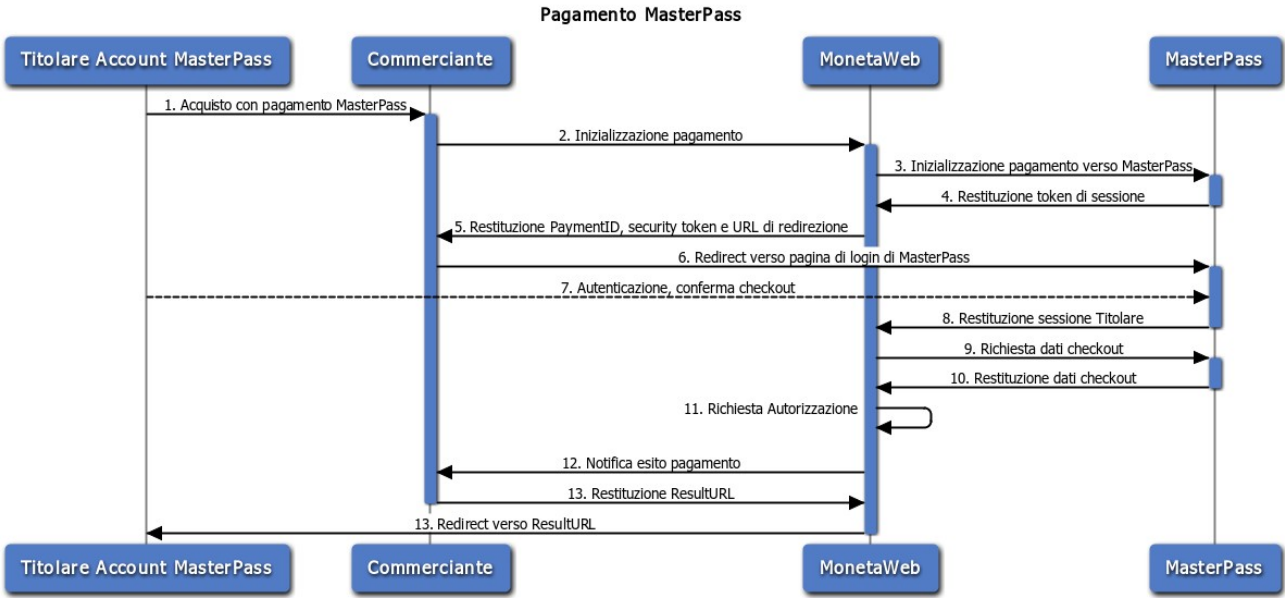
- un codice di errore
- una descrizione parlante dell'errore
- il riferimento alla transazione

Esempio messaggio di errore in fase di Notifica:

errorcode=PP10001, errormessage=Paypal error [10417]: Instruct the customer to retry the transaction using an alternative payment method from the customers PayPal wallet. The transaction did not complete with the customers selected payment method., paymentid=687192751812252579

3.6. Pagamento MasterPass

MasterPass è la soluzione interoperabile per lo shopping online offerta da MasterCard che consente di fare acquisti in modo semplice, rapido e sicuro. Attraverso MasterPass il Commerciante avrà accesso ai wallet esposti dai principali Istituti Bancari.



1. Il titolare carta effettua un acquisto sul sito del Commerciante, scegliendo MasterPass come strumento di pagamento; i dati del pagamento sono trasmessi al server del Commerciante
2. Il server del Commerciante inizializza il pagamento con un messaggio HTTP Post
3. MonetaWeb inizializza il pagamemento verso MasterPass
4. MasterPass restituisce un token di sessione
5. Monetaweb restituisce al Commerciante il PaymentID, il security token e la URL per la redirezione del titolare
6. Il server del Commerciante redirige il titolare carta verso la login page di MasterPass
7. Il titolare carta inserisce le proprie credenziali MasterPass, sceglie lo strumento di pagamento e l'eventuale indirizzo di spedizione e conferma il checkout
8. MasterPass restituisce la sessione del Titolare a MonetaWeb
9. MonetaWeb richiede i dati di checkout a MasterPass
10. MasterPass restituisce i dati di checkout
11. MonetaWeb elabora i dati carta, di spedizione e di billing da MasterPass e processa il pagamento
12. MonetaWeb notifica in modalità “server to server” l’esito del pagamento alla ResponseURL del Commerciante
13. Il Commerciante risponde a MonetaWeb inviando la ResultURL
14. Monetaweb redirige il titolare carta verso la ResultURL per la visualizzazione dell'esito finale.

INIZIALIZZAZIONE DEL PAGAMENTO

La prima fase dell'operazione consiste nell’invio a MonetaWeb dei dati preliminari del pagamento, come importo, riferimento ordine e url per la prosecuzione del pagamento stesso. A fronte della ricezione di questi dati, Monetaweb restituisce in output in formato XML un PaymentId univoco, un token di sicurezza e l’url della pagina di scelta Banca.

Esempio messaggio HTTP di Inizializzazione Pagamento:

id=99999999&password=99999999&operationType=initializemasterpass&amount=1.00&currency Code=978&responseToMerchantUrl=http://www.merchant.it/notify.jsp&recoveryUrl=http://www.merchant.it/error.jsp&merchantOrderId=TRCK0001&description=Descrizione&cardHolderName=Nome Cognome&cardHolderEmail=nome@dominio.com&customField=campoPersonalizzabile.

Parametri di chiamata del messaggio HTTP di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'initializemasterpass'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76 € = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (opzionale – default '978' [euro])	varchar	3
ResponseToMerchantUrl	Url verso cui notificare l'esito della transazione	varchar	2048
recoveryUrl	Url verso cui rediregere il titolare nel caso in cui non si riesca a ottenere una resultUrl in fase di notifica (opzionale)	varchar	2048
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento (opzionale)	varchar	255
cardHolderName	Nome del titolare carta (opzionale)	varchar	125
cardHolderEmail	Indirizzo e-mail del titolare carta presso cui notificare l'esito del pagamento (opzionale)	varchar	125
customField	Campo libero (opzionale)	varchar	255

Esempio messaggio XML di risposta a Inizializzazione Pagamento:

```
<response>
        <paymentid>12345678901234567</paymentid>
        <securitytoken>80957febda6a467c82d34da0e0673a6e</securitytoken>
        <hostedpageurl>http://www.monetaonline.it/monetaweb/masterpass</hostedpageurl>
</response>
```

Parametri di risposta al messaggio di Inizializzazione Pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Id associato alla sessione di pagamento	varchar	18
securitytoken	Token di sicurezza	varchar	32
hostedpageurl	Url della MasterPass sign-in page	varchar	255

Redirezione titolare carta alla MasterPass sign-in page:

A seguito della ricezione della risposta al messaggio di inizializzazione, è necessario redirigere la sessione web del cardholder verso l'url specificato nel tag hostedPageUrl aggiungendo come parametro il paymentid. Tale url non deve essere impostato come parametro fisso della redirezione ma, per ogni pagamento, deve essere reperito dinamicamente dall'apposito tag.

NOTIFICA DELL'ESITO DEL PAGAMENTO

Una volta autenticatosi nel wallet abilitato Masterpass il cardholder visualizza il riepilogo dell' acquisto, sceglie la carta con cui pagare ed effettua il checkout.

La richiesta di autorizzazione viene elaborata da monetaweb che fornisce al commerciante una notifica dell'esito del pagamento stesso. La notifica viene effettuata tramite post HTTP in formato NVP (NameValue Pair) sull'url indicato nel parametro responseToMerchantUrl.

Tra i vari parametri passati in post, il securityToken è una quantità di sicurezza generata da MonetaWeb e comunicata al commerciante sia in fase di risposta all'inizializzazione, sia in fase di notifica dell'esito; per scopi di sicurezza, si consiglia di verificare che il valore del securityToken ricevuto in fase di notifica corrisponda a quanto ricevuto in fase di inizializzazione.

Al fine di poter redirigere la sessione web del pagatore verso una nuova pagina contenente l'esito della transazione, il commerciante deve rispondere al messaggio di notifica appena ricevuto da Monetaweb con l'url della propria pagina di esito. Questo url può essere arricchito con dei parametri per consentire la corretta visualizzazione dell'esito stesso. Attenzione: la risposta non deve contenere codice HTML.

I nostri servizi, all'atto della notifica di un pagamento hosted verso la merchant response URL, una volta instaurata la connessione, attendono per 20 secondi di ricevere in risposta la URL per la redirezione finale. Allo scadere del timeout, la socket viene chiusa.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido e timeout nella risposta) Monetaweb reindirizzerà il titolare verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro del messaggio di Inizializzazione. Qualora il parametro recoveryUrl non fosse stato valorizzato MonetaWeb rediregerà il titolare verso una pagina di cortesia, pubblicata direttamente sul server MonetaWeb.

Ecco l'aspetto della pagina di cortesia MonetaWeb:

Esempio messaggio di esito del pagamento:

Message sent to merchant at url [http://www.merchant.it/notify.jsp] with data: {authorizationcode=000001, cardcountry=ITALY, cardexpirydate=1214, customfield=null, maskedpan=123456******4321, merchantorderid=000001, paymentid=0000000000000000001, responsecode=000, result=APPROVED, rrn=123456789012, securitytoken=SecurityToken001, threedsecure=S}

Parametri del messaggio HTTP di Notifica esito del pagamento:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito della transazione: - APPROVED, transazione autorizzata - NOT APPROVED, transazione negata - CAPTURED, transazione confermata - CANCELED, il cardholder ha annullato la transazione	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata, in tutti gli altri casi transazione negata)	char	3
authorizationcode	Codice di autorizzazione, valorizzato solo se la transazione è stata autorizzata	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
threedsecure	Livello di sicurezza della transazione: 'S' (transazione Full Secure), 'H' (transazione Half Secure), 'N' (transazione Not Secure)	char	1
rrn	Riferimento univoco della transazione generato dal Sistema Autorizzativo (da utilizzare in caso di contabilizzazione esplicita a mezzo file)	varchar	12
maskedpan	PAN mascherato della carta di credito utilizzata (nellaforma 123456******7890)	varchar	19
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
cardcountry	Nazionalità della carta di credito utilizzata	varchar	255
cardexpirydate	Data di scadenza della carta di credito utilizzata (nel formato mmaa)	varchar	4
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

CASI DI ERRORE

Fase di Inizializzazione:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di Inizializzazione:

```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

Fase di Notifica:

Nel caso in cui non sia possibile completare il pagamento (es. autenticazione 3DSecure fallita) MonetaWeb notifica il Commerciante con un messaggio di errore in formato NVP.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore
- Il riferimento univoco del pagamento

Esempio messaggio di errore in fase di Notifica:

errorcode=GV00004, errormessage=GV00004-PARes status not successful, paymentid=123456789012345678

4. MonetaWallet (Tokenizzazione) - Pagamenti Ricorrenti

4.1. Attivazione

Eseguendo una transazione MO.TO con CVV2, Hosted 3DSecure oppure Server To Server 3DSecure è possibile salvare i dati carta presso Mercury Payment Services e riutilizzarli tramite un token (walletid) per pagamenti successivi (ricorrenti o con wallet).

E' sufficiente popolare i parametri aggiuntivi recurringAction e walletid oltre ai parametri standard previsti dal protocollo di pagamento :

Nome	Descrizione	Tipo	Lunghezza
recurringAction	Azione da svolgere sul contratto. I valori possibili sono: • C: creazione contratto (creation) • S: sostituzione carta (substitution) • N: pagamemento one shot senza salvataggio carta/contratto (none)	char	1
walletid	Token carta (univoco – non associare un valore in caso di pagamento one shot [recurringAction=N])	varchar	18

Il salvataggio dei dati carta è condizionato al buon esito della richiesta di autorizzazione. A walletid differenti può essere associata la stessa carta.

L'associazione tra codice walletid e carta viene rimossa automaticamente dopo 6 anni di inutilizzo.

I limiti degli importi coincidono con quelli relativi al plafond della carta di credito associata.

4.2. Pagamenti Successivi

SPECIFICHE PER I PAGAMENTI SUCCESSIVI ONLINE

I pagamenti successivi all'attivazione di un pagamento ricorrente o al salvataggio di una carta (MonetaWallet) possono essere effettuati:

- con una transazione MO.TO; il campo walletID sostituisce i dati carta.
- con una transazione Hosted; il campo walletID consente di prepopolare la pagina di pagamento con i dati carta. Al titolare carte sarà richiesto solamente l'inserimento del CVV2/CVC2/4DBC, ove previsto. Il campo CardHolderName è obbligatorio.

Per tutte le modalità, il campo recurringAction va valorizzato come in tabella:

Nome	Descrizione	Tipo	Lunghezza
recurringAction	Azione da svolgere sul contratto. I valori possibili sono: W: pagamento con wallet (wallet)	char	1
walletid	Token carta	varchar	18

SPECIFICHE PER I PAGAMENTI SUCCESSIVI VIA BATCH

Nel caso di pagamenti ricorrenti, le richieste di addebito successive all'attivazione possono essere processate anche via file, secondo il tracciato descritto nel paragrafo MSG DETAIL – Record di dettaglio per Pagamenti Rata.

4.3. Cancellazione

La cancellazione wallet permette di eliminare un wallet precedentemente attivato.

Al fine di identificare univocamente il wallet da cancellare è necessario fornire i seguenti parametri di input:

- l'id terminale.
- la password.
- l'operationType relativo alla cancellazione del wallet.
- l'id del wallet da cancellare

INVIO DEL MESSAGGIO DI CANCELLAZIONE WALLET

Esempio messaggio HTTP della cancellazione wallet:
id=99999999&password=99999999&operationType=deletewallet&walletid=wallet001

Parametri di chiamata del messaggio HTTP di cancellazione wallet:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'deletewallet'	varchar	50
walletid	Identificativo univoco del wallet che si desidera cancellare	varchar	18

RICEZIONE DEL MESSAGGIO DI ESITO DELLA CANCELLAZIONE WALLET

Esempio messaggio XML di esito cancellazione wallet:

```
<response type="valid">
   <result>WALLET DELETED</result>
   <walletid>wallet001</walletid>
</response>
```

Parametri di risposta al messaggio di cancellazione wallet:

Nome	Descrizione	Tipo	Lunghezza
walletid	Identificativo univoco del wallet cancellato	varchar	18
result	Esito della cancellazione: • WALLET DELETED, esito di successo della cancellazione del wallet	varchar	20

4.4. Notifica dell'esito in caso di fallimento

Nel caso in cui non sia possibile completare la creazione del contratto o la sostituzione della carta da associare, MonetaWeb restituisce al Commerciante, in modalità sincrona (formato XML) o asincrona (format NVP) a seconda del protocollo, una notifica standard con in aggiunta i seguenti parametri:

- il codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di esito in caso di fallimento:

Nel caso in cui la richiesta violi le regole di creazione di un walletID o sostituzione carta, il sistema restituirà il codice esito "182", il dettaglio del fallimento viene esposto dai parametri errorcode ed errormessage.

Di seguito un esempio di notifica asincrona in formato NVP:

result=NOT APPROVED&paymentid=74279276258427018 9&walletid=WalletIsExample&
merchantorderid=OrderId&rn=123456789123&responsecode=182&**errorcode=WS00063&**
errormessage=Wallet Already Exists

Di seguito un esempio di notifica sincrona in formato XML:

```
<response>
        <result>NOT APPROVED</result>
        <paymentid>74279276258427018 9</paymentid>
        <walletid>WalletIsExample</walletid>
        <merchantorderid>OrderId</merchantorderid>
        <rrn>123456789123</rrn>
        <responsecode>182</responsecode>
        <errorcode>WS00063</errorcode>
        <errormessage>Wallet Already Exists</errormessage>
</response>
```

L'elenco dei codici di errori ammissibili sono riportati nell'appendice H - Codici di Errore Monetawallet

4.5. Notifica in caso di errore

Comportamento del sistema in caso di errore in fase di pagamenti successivi o cancellazione wallet:

In caso di errori legati alle operazioni in ambito di pagamenti ricorrenti o MonetaWallet, MonetaWeb risponde con un messaggio di errore in formato XML.

Tale messaggio comprende:
- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di pagamenti successivi o cancellazione wallet:

```
<error>
        <errorcode>WS00061</errorcode>
        <errormessage>Wallet not found</errormessage>
</error>
```

5. Processi di Contabilizzazione e Storno

I metodi di pagamento precedentemente descritti supportano differenti modalità di contabilizzazione per richiedere la liquidazione degli importi. A seconda delle specificità del proprio business è possibile scegliere tra le seguenti modalità:

- IMPLICITA: contestualmente alla fase di pagamento, ogni transazione autorizzata viene implicitamente confermata.

- ESPLICITA: dopo la fase di pagamento sarà necessario procedere alla conferma esplicita delle transazioni autorizzate che si desidera vengano contabilizzate e liquidate. **In caso di modifica a favore di una contabilizzazione implicita, occorre confermare manualmente, attraverso il portale di Back-Office, le transazioni che ricadono nel gap non gestito dalla nuova configurazione.**

- A MEZZO FILE: dopo la fase di pagamento sarà necessario inviare a Mercury Payment Services un file contenente i dati delle sole transazioni autorizzate che si desidera vengano contabilizzate e liquidate.

- DIFFERITA: ogni transazione autorizzata viene implicitamente confermata dopo un numero prestabilito di giorni. **In caso di riduzione dei giorni di contabilizzazione rispetto una configurazione precedente, oppure di modifica a favore di una contabilizzazione implicita, occorre confermare manualmente, attraverso il portale di Back-Office, le transazioni che ricadono nel gap non gestito dalla nuova configurazione.**

La tabella seguente mostra per ciascun metodo di pagamento le modalità di contabilizzazione compatibili e gli eventuali limiti temporali, dal rilascio dell'autorizzazione, entro i quali processare la richiesta.

	Implicita	Esplicita	Via File	Differita
Carta di Credito / MasterPass	Sì	4 giorni	4 giorni	4 giorni
MyBank	Sì	No	No	No
PayPal	Sì	29 giorni	No	No

Se una transazione autorizzata non viene confermata, il plafond della carta di credito resterà bloccato per un importo pari a quello autorizzato. Dopo un certo numero di giorni l’autorizzazione decadrà e l’importo bloccato tornerà disponibile; tale numero di giorni è variabile in base alla banca emittente della carta di credito utilizzata.

Se a seguito di una conferma si ha la necessità di riaccreditare un titolare per l'importo del pagamento o parte di esso, occorre effettuare un'operazione di storno, a partire dal giorno contabile successivo alla data di conferma.

6. Servizi di Gestione del Pagamento

Di seguito verranno discusse le operazioni disponibili, a seguito di un pagamento, esposte da MonetaWeb attraverso delle apposite API.

6.1. Conferma del pagamento (Richiesta di contabilizzazione)

Attraverso l'operazione di conferma è possibile richiedere la contabilizzazione di una transazione autorizzata. La Conferma può essere richiesta una sola volta e la somma da contabilizzare può essere totale o parziale.

L'operazione di Conferma è supportata dai seguenti metodi di pagamento:

- Carta di Credito
- MasterPass
- PayPal

INVIO DEL MESSAGGIO DI CONFERMA PAGAMENTO

Esempio messaggio HTTP di conferma pagamento:

id=99999999&password=99999999&operationType=confirm&amount=1.00&currencyCode=978&merchantOrderId=TrackingNo12345&paymentId=123456789012345

Parametri di chiamata del messaggio HTTP di conferma pagamento:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'confirm'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76€ = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencyCode	'978' (euro)	varchar	3
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
paymentId	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di pagamento	varchar	18
customField	Campo libero (opzionale)	varchar	255
description	Descrizione del pagamento (opzionale)	varchar	255

RICEZIONE DEL MESSAGGIO DI ESITO CONFERMA

Esempio messaggio XML di esito conferma:

```
<response>
  <result>CAPTURED</result>
  <authorizationcode>123456</authorizationcode>
  <paymentid>123456789012345</paymentid>
  <merchantorderid>TrackingNo12345</merchantorderid>
  <responsecode>000</responsecode>
  <customfield />
  <description />
</response>
```

Parametri di risposta al messaggio di conferma:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito della conferma: - CAPTURED, transazione confermata	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata)	char	3
authorizationcode	Codice di autorizzazione	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento inviato dal Commerciante in fase di Inizializzazione	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di conferma:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, tentativo di confermare un pagamento già confermato, tentativo di confermare un pagamento per un importo maggiore rispetto a quanto autorizzato, …) MonetaWeb risponde con un messaggio di errore in formato XML.

Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di conferma:

```
<error>
  <errorcode>GW00176</errorcode>
  <errormessage>Failed Previous Captures check.</errormessage>
</error>
```

6.2. Storno contabile

Attraverso l'operazione di storno è possibile riaccreditare l'importo di una transazione già contabilizzata sullo strumento di pagamento originariamente utilizzato dal titolare. Lo Storno può essere totale o parziale e, in quest'ultimo caso, può essere ripetuto fino al raggiungimento dell'importo contabilizzato.

L'operazione di Storno è supportata dai seguenti metodi di pagamento:

- Carta di Credito
- MasterPass
- PayPal

INVIO DEL MESSAGGIO DI STORNO CONTABILE

Esempio messaggio HTTP di storno:

id=99999999&password=99999999&operationType=voidconfirmation&amount=1.00&currencyCode=978&merchantOrderId=TrackingNo12345&paymentId=123456789012345

Parametri di chiamata del messaggio HTTP di storno:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	'voidconfirmation'	varchar	50
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76€= "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencyCode	'978' (euro)	Varchar	3
merchantOrderId	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
paymentId	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di pagamento	varchar	18
customField	Campo libero (opzionale)	varchar	255
description	Descrizione del pagamento (opzionale)	varchar	255

RICEZIONE DEL MESSAGGIO DI ESITO STORNO CONTABILE

Esempio messaggio XML di esito storno:

```
<response>
   <result>VOIDED</result>
  <authorizationcode>123456</authorizationcode>
  <paymentid>123456789012345</paymentid>
  <merchantorderid>TrackingNo12345</merchantorderid>
  <responsecode>000</responsecode>
  <customfield />
  <description />
</response>
```

Parametri di risposta al messaggio di storno:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito dello storno: - VOIDED, pagamento stornato	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata)	char	3
authorizationcode	Codice di autorizzazione	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento inviato dal Commerciante in fase di Inizializzazione	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di storno:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, tentativo di stornare un pagamento già completamente stornato, …) MonetaWeb risponde con un messaggio di errore in formato XML.

Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di storno:

```
<error>
   <errorcode>GW00181</errorcode>
   <errormessage>Operation Failed.</errormessage>
</error>
```

6.3. Annullamento dell'autorizzazione

Attraverso l’operazione di annullamento autorizzazione è possibile rilasciare l’importo di una transazione precedentemente autorizzata affinché l'emittente lo renda nuovamente disponibile sulla carta di credito del titolare.

L'operazione di Annullamento dell'autorizzazione è supportata dai seguenti metodi di pagamento:

- Carta di Credito
- MasterPass

L'operazione di Annullamento dell'autorizzazione è IRREVERSIBILE.

NOTA: l'efficacia dell'operazione di annullamento dell'autorizzazione dipende sia dal tipo di carta utilizzata sia dalle politiche della Banca emittente; si raccomanda di effettuare l'annullamento dell'autorizzazione nei giorni immediatamente successivi al rilascio dell'autorizzazione, in alternativa l'operazione potrebbe essere rifiutata.

INVIO DEL MESSAGGIO DI ANNULLAMENTO AUTORIZZAZIONE

Esempio messaggio HTTP di annullamento autorizzazione:

id=99999999&password=99999999&operationType=voidauthorization&paymentId=123456789012345

Parametri di chiamata del messaggio HTTP di annullamento autorizzazione:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all’id terminale	varchar	50
operationType	voidauthorization	varchar	-
paymentId	Identificativo univoco dell’ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di pagamento	varchar	18
customField	Campo libero (opzionale)	varchar	255
description	Descrizione del pagamento (opzionale)	varchar	255

RICEZIONE DEL MESSAGGIO DI ESITO ANNULLAMENTO AUTORIZZAZIONE

Esempio messaggio XML di esito annullamento autorizzazione:

```
<response>
   <result>AUTH VOIDED</result>
  <authorizationcode>123456</authorizationcode>
  <paymentid>123456789012345</paymentid>
  <merchantorderid>TrackingNo12345</merchantorderid>
  <responsecode>000</responsecode>
  <customfield />
  <description />
</response>
```

Parametri di risposta al messaggio di annullamento autorizzazione:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito dello storno: - AUTH VOIDED, autorizzazione annullata	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata)	char	3
authorizationcode	Codice di autorizzazione	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
description	Descrizione del pagamento inviato dal Commerciante in fase di Inizializzazione	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di annullamento autorizzazione:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, tentativo di annullare un pagamento già annullato, tentativo di annullare un pagamento non autorizzato, …) MonetaWeb risponde con un messaggio di errore in formato XML.

Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di annullamento autorizzazione:

```
<error>
  <errorcode>GW00179</errorcode>
  <errormessage>Failed Previous Voids check.</errormessage>
</error>
```

6.4. Annullamento della conferma con rilascio del plafond

Attraverso l'operazione di Annullamento della conferma con rilascio del plafond è possibile annullare la conferma contabile pendente (solamente se effettuata nella giornata corrente in modalità implicita o esplicita) e contestualmente ottenere l'annullamento dell'autorizzazione e il conseguente rilascio in tempo reale del plafond della carta di credito del titolare.

L'operazione di Annullamento della conferma con rilascio del plafond è supportata dai seguenti metodi di pagamento:

- Carta di Credito
- MasterPass

L'operazione di Annullamento della conferma con rilascio del plafond è IRREVERSIBILE.

INVIO DEL MESSAGGIO DI ANNULLAMENTO DELLA CONFERMA CON RILASCIO DEL PLAFOND

Esempio messaggio HTTP di forced void authorization:

id=99999999&password=*99999999*&operationType=forcedvoidauthorization&paymentId=123456789012345

Parametri di chiamata del messaggio HTTP di forced void authorization:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	forcedvoidauthorization	varchar	-
paymentId	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di pagamento	varchar	18

RICEZIONE DEL MESSAGGIO DI ESITO ANNULLAMENTO DELLA CONFERMA CON RILASCIO DEL PLAFOND

Esempio messaggio XML di esito forced void authorization:

```
<response>
   <result>AUTH VOIDED</result>
  <authorizationcode>123456</authorizationcode>
  <paymentid>123456789012345</paymentid>
  <merchantorderid>TrackingNo12345</merchantorderid>
  <responsecode>000</responsecode>
</response>
```

Parametri di risposta al messaggio di forced void authorization:

Nome	Descrizione	Tipo	Lunghezza
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18
result	Esito dello storno: - AUTH VOIDED, autorizzazione annullata	varchar	20
responsecode	Codice di risposta (es: '000' se transazione autorizzata)	char	3
authorizationcode	Codice di autorizzazione	varchar	6
merchantorderid	Riferimento Operazione (viene restituito se valorizzato nella richiesta)	varchar	18

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di forced void authorization:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, tentativo di annullare un pagamento già annullato, tentativo di annullare un pagamento non autorizzato, tentativo di annullare un pagamento confermato oltre la stessa giornata…) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di forced void authorization:

```
<error>
  <errorcode>GW00179</errorcode>
  <errormessage>Failed Previous Voids check.</errormessage>
</error>
```

6.5. Inquiry, interrogazione per transazione

Attraverso il messaggio sincrono di inquiry è possibile ottenere a posteriori le informazioni sull'esito di un pagamento.

Si consiglia di effettuare l'operazione di inquiry al termine della durata massima di una sessione di pagamento, ovvero dopo 20 minuti dalla generazione del paymentid.

INVIO DEL MESSAGGIO DI INQUIRY

Esempio messaggio HTTP di inquiry:
id=99999999&password=99999999&operationType=inquiry&paymentId=123456789012345

Parametri di chiamata del messaggio HTTP di inquiry:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	Inquiry, per pagamenti con Carta di Credito e Masterpass	varchar	50
	Inquirymybank, per pagamenti MyBank		
paymentId	Identificativo univoco di sessione generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di pagamento	varchar	18

RICEZIONE DEL MESSAGGIO DI ESITO INQUIRY

Esempio messaggio XML di esito inquiry:

<response>
<result>APPROVED</result>
<paymentid>434166330386052949</paymentid>
<transactiontime>2015-10-23T09:55:17.837+0200</transactiontime>
<amount>0.10</amount>
<currencycode>978</currencycode>
<merchantorderid>2011IVR4189718Anti</merchantorderid>
<authorizationcode>888620</authorizationcode>
<threedsecure>H</threedsecure>
<responsecode>000</responsecode>
<customfield>some custom field</customfield>
<description>some description</description>
<rrn>123456789012</rrn>
<cardcountry>ITALY</cardcountry>
<cardbrand>MC</cardbrand>
<cardtype>MONETA</cardtype>
<maskedpan>539832**1283</maskedpan>
<securitytoken>925a86bbbf0444809dbc37ab08ee1d87</securitytoken>
<cardholderip>192.168.99.202</cardholderip>
</response>

Esempio messaggio XML di esito inquirymybank:

<response>
<amount>0.10</amount>
<authorizationcode>888621</authorizationcode>
<currencycode>978</currencycode>
<customfield>some custom field</customfield>
<description>Some description</description>
<merchantorderid>2011IVR4189718Anti</merchantorderid>
<mybankid>7844111</mybankid>
<paymentid>423129329528760639</paymentid>
<result>AUTHORISED</result>
<securitytoken>6afebc810bcf48bd9aff71d39c223dc4</securitytoken>
<selectedbank>Intesa San Paolo</selectedbank>
<transactiontime>2016-03-03 16:51:51.746</transactiontime>
</response>

Parametri di risposta al messaggio di inquiry:

Nome	Descrizione	Tipo	Lunghezza
result	Esito della transazione: • APPROVED, transazione autorizzata • NOT APPROVED, transazione negata • AUTH VOIDED, transazione annullata • CAPTURED, transazione confermata • VOIDED, transazione stornata • NOT AUTHENTICATED, autenticazione 3D fallita • PARES ERROR, errore in fase di autenticazione 3D • CANCELED: pagamento annullato dal titolare/pagatore • AUTHORISED: bonifico MyBank autorizzato dalla Banca del pagatore [solo per pagamento MyBank] • ERROR: bonifico MyBank non completato poiché negato dalla Banca del pagatore [solo per pagamento MyBank] • AUTHORISINGPARTYABORTED: bonifico MyBank abbandonato dal pagatore (a seguito dell'accesso al portale della Banca) [solo per pagamento MyBank] • TIMEOUT: bonifico MyBank non completato per superamento del tempo limite a disposizione [solo per pagamento MyBank] • PENDING: pagamento in attesa di esito [solo per i pagamenti MyBank]	varchar	32
paymentid	Identificativo univoco dell'ordine generato da MonetaWeb, corrisponde allo stesso campo ricevuto in risposta durante la fase di Inizializzazione	varchar	18

transactiontime	Ora della richiesta dell'autorizzazione (yyyy-MM-dd'T'HH:mm:ss.SSS±HH:mm) [Formato ISO 8601]	date	-
amount	Importo della transazione utilizzando il punto come separatore dei decimali (es: 1428,76€ = "1428.76"). La parte decimale può variare a seconda della valuta.	decimal	18,4
currencycode	Codice numerico della currency (es. '978' [euro])	varchar	3
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)	varchar	18
authorizationcode	Codice di autorizzazione, valorizzato solo se la transazione è stata autorizzata	varchar	6
threedsecure	Livello di sicurezza della transazione: 'S' (transazione Full Secure), 'H' (transazione Half Secure), 'N' (transazione Not Secure)	char	1
responsecode	Codice di risposta (es: ‘000’ se transazione autorizzata, in tutti gli altri casi transazione negata)	char	3
customfield	Campo libero inviato dal Commerciante in fase di pagamento	varchar	255
description	Descrizione libera inviata dal Commerciante in fase di pagamento	varchar	255
rrn	Riferimento univoco della transazione generato dal Sistema Autorizzativo (da utilizzare in caso di contabilizzazione esplicita a mezzo file)	varchar	12
cardcountry	Nazionalità della carta di credito utilizzata	char	255
cardbrand	Circuito e tipologia della carta di credito utilizzata ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Visa', 'JCB']	varchar	10
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
maskedpan	PAN mascherato della carta utilizzata in fase di pagamento	varchar	19
securitytoken	Token di sicurezza (solo per le transazioni 3DSecure)	varchar	32
cardholderip	IP del titolare carta (solo per le transazioni 3DSecure)	varchar	15
mybankid	ID transazione EBA (solo per MyBank)	varchar	35
selectedbank	Banca selezionata dal Pagatore (solo per MyBank)	varchar	511

CASI DI ERRORE

Comportamento del sistema in caso di errore in fase di inquiry:

In caso di invio di parametri errati (es. terminale sconosciuto, password errata, riferimento transazione non univoco, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di inquiry:

```
<error>
    <errorcode>GW00201</errorcode>
    <errormessage>Transaction not found.</errormessage>
</error>
```

Appendice

A. Ambiente di test

Per i pagamenti standard il sistema simula una richiesta di autorizzazione senza verificare la data scadenza e il cvv; l'esito della transazione viene determinato sulla base dell'importo valorizzato:

- se importo = 9999 -> transazione negata
- se importo = 9998 -> Errore 500
- se importo <> 9999/9998 -> transazione autorizzata

Per i pagamenti ricorrenti e per l'utilizzo di MonetaWallet, il sistema effettua una richiesta di autorizzazione in ambiente di test verificando tutti i dati carta.

Il nome titolare carta può essere qualsiasi.

Come codice di autorizzazione (*authorizationcode)* è possibile ricevere in risposta il valore *"fakews".*

Nell'ottica di garantire una maggiore segregazione tra gli ambienti di TEST e PRODUZIONE, l'ambiente di TEST accetta solo il set di carte di credito sotto riportate. Tutte le altre carte riceveranno l'esito NOT APPROVED con response code 111 – Numero Carta non Valido.

CARTE DI TEST

Circuito	Numero Carta	Data Scadenza	CVV	Verifica 3D Secure	Password 3D Secure	Esito
VISA	4349940199990739	08/2020	700	ENROLLED	valid	OK
VISA	4349940199990747	08/2020	243	ENROLLED	valid	OK
MC	5398320199998163	08/2020	564	ENROLLED	valid	OK
MC	5398320199998171	08/2020	637	ENROLLED	valid	OK
MC	5398320199998189	08/2020	099	ENROLLED	valid	OK
AMEX	375200000000003	12/2018	5861	NOT SUPPORTED	-	OK
DINERS	36961902064030	02/2021	250	NOT SUPPORTED	-	OK

CREDENZIALI DI TEST

Back Office: https://test.monetaonline.it/monetaweb/backoffice

Use Case	Codice Commerciante	Codice Utente	Password Back Office	Terminale	Password Terminale
Hosted 3D - contabilizzazione esplicita	009999999	009999999	Setefi14	99999999	99999999
Hosted 3D - contabilizzazione implicita	009999100	009999100	Setefi14	99999100	Setefi01
Hosted NO 3D - contabilizzazione esplicita	009999101	009999101	Setefi14	99999101	Setefi01
Hosted NO 3D - contabilizzazione implicita	009999102	009999102	Setefi14	99999102	Setefi01
MOTO - contabilizzazione esplicita	99999906	99999906	Setefi14	99999906	Password1
MOTO - contabilizzazione implicita	99999907	99999907	Setefi14	99999907	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Primo pagamento - Hosted 3D - contabilizzazione esplicita	001723477	001723477	Setefi14	93026293	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Primo pagamento - Hosted 3D - contabilizzazione implicita	001723477	001723477	Setefi14	93029357	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Primo pagamento - Hosted NO 3D / MOTO - contabilizzazione esplicita	001723477	001723477	Setefi14	93026294	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Pagamenti successivi - MOTO - contabilizzazione esplicita	001723477	001723477	Setefi14	93026295	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Primo pagamento - Hosted NO 3D / MOTO - contabilizzazione implicita	001723477	001723477	Setefi14	93211525	Password1
MonetaWallet (tokenizzazione) Pagamenti Ricorrenti: Pagamenti successivi - MOTO - contabilizzazione implicita	001723477	001723477	Setefi14	93211526	Password1

CREDENZIALI PAYPAL DI TEST

Le credenziali di accesso al portale di PayPal di TEST sono:

PayPal: https://www.sandbox.paypal.com

Utente PayPal di TEST:

- Indirizzo email: paypal.test@setefi.it
- Password: setefiPP

Back Office PayPal di TEST:

- Indirizzo email: setefi+paypal-merchant2@xpeppers.com
- Password: provaprova

CREDENZIALI MASTERPASS DI TEST

Durante un pagamento Masterpass occorre cliccare su “Masterpass by MasterCard” nell'elenco proposto.

Se non si è già in possesso di una propria utenza di TEST, seguire la procedura di registrazione guidata a partire dalla seguente url:

MasterpassSandboxRegistrationURL

Per poter registrare con successo un account di TEST occorre disporre delle seguenti informazioni:

- Nome e Cognome (anche inventati)
- indirizzo email (esistente e utilizzabile)
- numero di cellulare (esistente e utilizzabile)

Il numero di cellulare verrà utilizzato per l'invio di un codice di sicurezza via sms. Se non si ha momentaneamente a disposizione il cellulare con sé, è possibile richiedere il codice di sicurezza via mail. L'indirizzo mail verrà utilizzato per l'nvio di un mail di notifica dell'avvenuto pagamento.

Per completare la registrazione occorre inserire una carta di credito. Nell'ambiente di TEST di Masterpass si possono aggiungere SOLO le seguenti carte:

Circuito	Numero Carta	Data Scadenza	CVV
VISA	4440000009900010	12/2028	111
VISA	4440000010099018	12/2028	111
VISA	4440000042200014	12/2028	111
VISA	4440000042200022	12/2028	349

MC	5506900140100107	12/2028	670
MC	5506900140100206	12/2028	278
MC	5204740009900048	12/2028	145
MC	5204740009900055	12/2028	008
AMEX	340000099900036	12/2028	5861
AMEX	340000099900028	12/2028	5534
AMEX	340000099900044	12/2028	2134
AMEX	340000099900051	12/2028	5567

I dati relativi a data scadenza e cvv sono fittizi e vengono indicati solo come esempio di formato.

PAGAMENTO MYBANK IN TEST

Poichè nessuna delle banche partecipanti espone pubblicamente il proprio ambiente di test, MonetaWeb mette a disposizione in ambiente di test alcune banche fittizie che permettono di ottenere gli esiti previsti dal protocollo MyBank.

Alias Banca	Esito MyBank
Fakebank_ERROR	ERROR
Fakebank_AUTHORISINGPARTYABORTED	AUTHORISINGPARTYABORTED
Fakebank_PENDING	PENDING
Fakebank_AUTHORISED	AUTHORISED
Fakebank_TIMEOUT	TIMEOUT

B. Tracciato TRINIZ

Il tracciato TRINIZ è il formato ufficiale con cui avviene lo scambio di informazioni off-line tra il Commerciante e MonetaWeb. A fronte dell'elaborazione del file di ingresso fornito dal Commerciante viene restituito un file di esito.

Per quanto concerne il **nome del file** si può scegliere tra un nome custom o la dicitura di default che ha la seguente nomenclatura INSEGNA_AAAAMMGGHHMMSS, dove:

- INSEGNA: Nome dell'insegna del Commerciante (indicato da Mercury Payment Services),
- AAAA è l'anno,
- MM è il mese,
- GG è il giorno,
- HH è l'ora,
- MM sono i minuti,
- SS sono i secondi.

L'estensione è opzionale.

Per quanto riguarda il **nome del file di esito**, si può scegliere tra un nome custom oppure lo stesso nome del file di ingresso. **L'estensione** è opzionale.

Per il file delle conferme contabili, la schedulazione di invio del file di ingresso è giornaliera.

Per il file dei pagamenti rata e delle autorizzazioni a mezzo file, la schedulazione di invio del file di ingresso può essere:

- Giornaliera.
- Settimanale.
- Mensile.

Il **protocollo** da utilizzare per lo scambio dei file è da concordare scrivendo all'indirizzo gap@mercurypayments.it.

Effettuate tutte le scelte, occorre inviare una mail al servizio di supporto Commercio Elettronico specificando:

- *Nome del file in ingresso*: default o indicare il nome custom.
- *Nome del file di esito*: default o indicare il nome custom.
- *Schedulazione invio del file in ingresso*:
  - Giornaliera: ora di invio (HH:MM).
  - Settimanale (solo per i pagamenti rata e le autorizzazioni a mezzo file): giorno della settimana (es. Lunedì).
  - Mensile (solo per i pagamenti rata e le autorizzazioni a mezzo file): giorno del mese (GG).

- *Gli indirizzi email dei destinatari* se si desidera email di notifica di presa in carico del file in ingresso (opzionale).
- *Gli indirizzi email dei destinatari* se si desidera email di notifica di generazione del file di esito (opzionale).

L'invio del file deve rispettare la schedulazione anche in assenza di transazioni, occorre processare un file contenente solo i record di testa e coda.

Per la validazione formale di un file di esempio in ambiente di test occorre:

- usare il Codice Cliente: 99999
- inviare il file via mail al servizio di supporto Commercio Elettronico

Struttura del File

Il file è strutturato e, in base alla compilazione del record di dettaglio, può avere diverse finalità.

Il file è codificato con caratteri ASCII, ciascun record termina con CRLF (CR = codice ASCII 13 decimale; LF = codice ASCII 10 decimale).

I record del tracciato di Conferma Contabile hanno lunghezza fissa a 126 caratteri e terminano con i due caratteri CRLF (lunghezza totale del record 128).

I record del tracciato dei Pagamenti Rata e delle Autorizzazioni a mezzo file hanno lunghezza fissa a 190 caratteri e terminano con i due caratteri CRLF (lunghezza totale del record 192).

I campi alfanumerici (Tipo = A) vanno allineati a sinistra e riempiti a destra con spazi vuoti, mentre i campi numerici (Tipo = N) vanno allineati a destra e riempiti a sinistra con zeri.

Ogni blocco contabile (COINIZ-COFINE) può contenere al massimo 9999 transazioni, in quanto il progressivo transazione è lungo 4 caratteri. Al superamento della soglia di 9999 transazioni è necessario creare un nuovo blocco contabile.

La struttura del file prevede: l'apertura del record TRINIZ, l'apertura del record COINIZ, la scrittura dei record di dettaglio, la scrittura del record COFINE, la chiusura del flusso con record TRFINE.

DETTAGLIO DELLA STRUTTURA

Record	Prefisso di record	Descrizione
Inizio trasmissione	TRINIZ	Record di apertura del file.
Inizio contabile	COINIZ	Record di apertura blocco contabile
Dettaglio	-	Record di dettaglio
Fine contabile	COFINE	Record di apertura blocco contabile
Fine trasmissione	TRFINE	Record di chiusura del file.

MSG TRINIZ – inizio trasmissione

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“TRINIZ”
2	07	5	N	Codice Cliente (generato e comunicato da Mercury Payment Services)
3	12	6	N	Data creazione file (ggmmaa, es. 16 per l'anno 2016)
4	18	6	N	Ora creazione file (hhmmss)
5	24	1	A	“T”
6	25	3	A	“E45”
7	28	3	N	Numero progressivo della trasmissione del file batch (parte da 001, fino a 999 e poi riparte da 001, deve essere sempre diverso da 000 ed esiste il vincolo della consecutività, in modo da riscontrare eventuali mancate trasmissioni)
8	31	1	A	“A”
9	32	1	A	Spazi vuoti
10	33	1	A	“D” (solo per clienti che gestiscono il MultiCurrency) altrimenti spazi vuoti
11	34	1	A	“R” (solo per clienti che gestiscono i pagamenti ricorrenti) altrimenti spazi vuoti
12	35	92 per il tracciato di Conferma Contabile 156 per il tracciato dei Pagamenti Rata e delle Autorizzazioni a mezzo file	A	Spazi vuoti

MSG COINIZ – inizio contabile

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“COINIZ”
2	07	5	N	Codice Cliente (generato e comunicato da Mercury Payment Services)
3	12	6	N	Data creazione file (ggmmaa, es. 16 per l'anno 2016)
4	18	6	N	Ora creazione file (hhmmss)
5	24	1	N	Impostato con l’ultima cifra dell’anno (es: 2 per il 2012)
6	25	3	N	Numero progressivo della contabile all’interno del file (parte da 001 e deve essere incrementato di uno, creando un nuovo blocco contabile COINIZ-COFINE, solo al raggiungimento di 9999 transazioni nel record di dettaglio)
7	28	2	N	“50” (euro)
8	30	97 per il tracciato di Conferma Contabile 161 per il tracciato dei Pagamenti Rata e delle Autorizzazioni a mezzo file	A	Spazi vuoti

MSG DETAIL – Record di dettaglio

Comporre il record di dettaglio in base allo scopo del file, successivamente vengono descritte alcune tipologie di MSG DETAIL (per contabilizzazione via file, pagamenti rata, ecc...).

MSG COFINE – fine contabile

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“COFINE”
2	07	5	N	Codice Cliente (generato e comunicato da Mercury Payment Services)
3	12	1	N	“0”
4	13	3	N	Numero progressivo della contabile corrispondente (Deve essere riportato lo stesso progressivo indicato nel COINIZ, vedi inizio contabile numero 6)
5	16	5	N	Totale record da COINIZ a COFINE (inclusi)
6	21	12	N	Totale importi contabilizzazioni (le ultime 2 cifre corrispondono ai decimali)
7	33	12	N	Zeri
8	45	12	N	Totale importi storni (le ultime 2 cifre corrispondono ai decimali)
9	57	6	N	Data creazione file (ggmmaa, es. 16 per l'anno 2016)
10	63	6	N	Data contabile (ggmmaa, es. 16 per l'anno 2016) [coincide con data creazione file]
11	69	58 per il tracciato di Conferma Contabile 122 per il tracciato dei Pagamenti Rata e delle Autorizzazioni a mezzo file	A	Spazi vuoti

MSG TRFINE – Fine trasmissione

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“TRFINE”
2	07	5	N	Codice Cliente (generato e comunicato da Mercury Payment Services)
3	12	5	N	Totale record da TRINIZ a TRFINE (inclusi)
4	17	110 per il tracciato di Conferma Contabile 174 per il tracciato dei Pagamenti Rata e delle Autorizzazioni a mezzo file	A	Spazi vuoti

MSG DETAIL – Record di dettaglio per Conferme contabili per contabilizzazione a mezzo file

I commercianti che utilizzano questo metodo richiedono la contabilizzazione inviando un archivio contenente le operazioni autorizzate da contabilizzare.
Per ciascun movimento di dettaglio autorizzato contenuto nell'archivio si procederà alla relativa contabilizzazione (addebito/accredito).

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	1	N	"0"
2	02	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	11	8	N	Codice Terminale (generato e comunicato da Mercury Payment Services)
4	19	3	N	Numero progressivo della contabile corrispondente (Deve essere riportato lo stesso progressivo indicato nel COINIZ di appartenenza, vedi inizio contabile numero 6)
5	22	4	N	Numero progressivo della transazione (parte da 0001 fino a 9999, a seguito del quale occorre creare un altro blocco contabile COINIZ-COFINE con il progressivo incrementato di 1)
6	26	6	N	Data transazione (ggmmaa, es. 16 per l'anno 2016)
7	32	4	N	Ora transazione (hhmm)
8	36	23	A	Spazi vuoti
9	59	9	N	Importo (le ultime 2 cifre corrispondono ai decimali)
10	68	6	A	Codice Autorizzazione = al campo "Auth" presente nel messaggio di risposta da Mercury Payment Services
11	74	3	A	Spazi vuoti
12	77	1	A	"1"
13	78	1	A	"0" (contabilizzazione) "7" (storno)
14	79	12	A	Retrieval Reference Number = al campo "rrn" presente nel messaggio di risposta da Mercury Payment Services
15	91	18	A	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)
16	109	18	A	Spazi vuoti

MSG DETAIL – Record di dettaglio per Pagamenti Rata

I commercianti possono richiedere di effettuare addebiti succcesivi all'attivazione, inviando un archivio elettronico. Per ciascun record di dettaglio, si procederà alla richiesta di addebito.

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	1	N	“0”
2	02	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	11	8	N	Codice Terminale (generato e comunicato da Mercury Payment Services)
4	19	3	N	Numero progressivo della contabile corrispondente (Deve essere riportato lo stesso progressivo indicato nel COINIZ di appartenenza, vedi inizio contabile numero 6)
5	22	4	N	Numero progressivo della transazione (parte da 0001 fino a 9999, a seguito del quale occorre creare un altro blocco contabile COINIZ-COFINE con il progressivo incrementato di 1)
6	26	6	N	Data creazione file (ggmmaa, es. 16 per l'anno 2016)
7	32	4	N	Ora creazione file (hhmm)
8	36	23	A	Spazi vuoti
9	59	9	N	Importo (le ultime 2 cifre corrispondono ai decimali)
10	68	6	A	Codice Autorizzazione in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato se la transazione è stata autorizzata; - spazi vuoti se l’autorizzazione è stata negata
11	74	3	A	Spazi vuoti
12	77	1	A	“1”
13	78	1	A	Tipo operazione -0 acquisto -7 storno
14	79	12	A	RRN (Retrieval Reference Number) in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato

15	91	18	A	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto - per la vecchia gestione dei pagamenti ricorrenti è il codice contratto)
16	109	18	A	Spazi vuoti
17	127	30	A	A disposizione del cliente
18	157	3	A	Response Code in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato con il Response Code (Vedi appendice "Response Code ISO")
19	160	8	A	Data autorizzazione (aaaammgg) in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato
20	168	18	A	Walletid creato dai Commercianti e utilizzato al posto del PAN
21	186	5	A	Spazi vuoti

MSG DETAIL – Record di dettaglio per Autorizzazioni a mezzo file

I commercianti che utilizzano questo metodo richiedono l'autorizzazione inviando un archivio contenente le operazioni da autorizzare.
Per ciascun movimento di dettaglio contenuto nell'archivio si procederà alla relativa autorizzazione.
Per poter richiedere questo servizio, occorre essere in possesso della certificazione PCI-DSS.

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	1	N	"0"
2	02	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	11	8	N	Codice Terminale (generato e comunicato da Mercury Payment Services)
4	19	3	N	Numero progressivo della contabile corrispondente (Deve essere riportato lo stesso progressivo indicato nel COINIZ di appartenenza, vedi inizio contabile numero 6)

5	22	4	N	Numero progressivo della transazione (parte da 0001 fino a 9999, a seguito del quale occorre creare un altro blocco contabile COINIZ-COFINE con il progressivo incrementato di 1)
6	26	6	N	Data transazione (ggmmaa, es. 16 per l'anno 2016)
7	32	4	N	Ora transazione (hhmm)
8	36	19	A	Numero carta (Solo per clienti che gestiscono l'archivio carte) altrimentri spazi vuoti
9	55	4	N	Data scadenza (aamm, es. 16 per l'anno 2016) (Solo per clienti che gestiscono l'archivio carte) altrimentri spazi vuoti
10	59	9	N	Importo (le ultime 2 cifre corrispondono ai decimali)
11	68	6	A	Codice Autorizzazione in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato se la transazione è stata autorizzata; - spazi vuoti se l'autorizzazione è stata negata
12	74	3	A	Spazi vuoti
13	77	1	A	"1"
14	78	1	A	Tipo operazione -0 acquisto -7 storno
15	79	12	A	RRN (Retrieval Reference Number) in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato
16	91	18	A	Riferimento Operazione (può contenere solo lettere e numeri e deve essere univoco in assoluto)

17	109	3	A	Response code in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Mercury Payment Services: - valorizzato con il Response Code (Vedi appendice "Response Code ISO")
18	112	2	A	Spazi vuoti
19	114	3	A	Codice valuta (solo per clienti che gestiscono il multicurrency) altrimenti spazi vuoti
20	117	9	N	Importo in valuta – le ultime 2 cifre corrispondono ai decimali (solo per clienti che gestistono il multicurrency) altrimenti spazi vuoti
21	126	65	A	Spazi vuoti

C. Tracciato Gestione Stato Contratto/Wallet ID e Allineamento Carte

Il tracciato Gestione Stato Contratto/Wallet ID e allineamento Carte è il formato ufficiale con cui avviene la procedura off-line di modifica dello stato del Contratto/Wallet ID e l'allineamento carte per poter mantenere aggiornati i dati delle carte di credito, utilizzando i mezzi più efficaci messi a disposizione dai circuiti.

I due tracciati, seppur con struttura simile, sono indipendenti l'uno dall'altro, necessitando di una configurazione dedicata, e la loro attivazione deve avvenire separatamente.

Il file è strutturato ed è utilizzato bidirezionalmente, tra MonetaWeb ed il Merchant, per sottomettere l'elaborazione e riceverne l'esito.

Per quanto concerne il **nome del file** si può scegliere tra un nome custom (purché i due tracciati abbiano nomi distinti) o la dicitura di default che ha la seguente nomenclatura INSEGNA_TIPO_AAAAMMGGHHMMSS, dove:

- INSEGNA: Nome dell'insegna del Commerciante (indicato da Mercury Payment Services),
- TIPO: tipo di tracciato tra:
  - ALL: per il file di allineamento carte.
  - UPD: per il file di modifica stato del contratto/wallet id.
- AAAA è l'anno,
- MM è il mese,
- GG è il giorno,
- HH è l'ora,
- MM sono i minuti,
- SS sono i secondi.

L’estensione è opzionale.

Per quanto riguarda il **nome del file di esito**, si può scegliere tra un nome custom oppure lo stesso nome del file di ingresso. **L’estensione** è opzionale.

L'invio del file relativo al dettaglio modifica stato del contratto/wallet id è libero. Se invece si desidera essere notificati in caso di non ricezione del file, occorre comunicare la schedulazione di invio, che segue le stesse politiche della schedulazione di invio del file di allineamento carte.

Per il file di allineamento carte, la schedulazione di invio del file di ingresso può essere:

- Giornaliera.
- Settimanale.
- Mensile.

Il **protocollo** da utilizzare per lo scambio dei file è da concordare scrivendo all'indirizzo gap@mercurypayments.it.

Effettuate tutte le scelte, occorre inviare una mail al servizio di supporto Commercio Elettronico specificando:

- *Nome del file in ingresso*: default o indicare il nome custom.
- *Nome del file di esito*: default o indicare il nome custom.
- *Schedulazione invio del file in ingresso*:
  - Giornaliera: ora di invio (HH:MM).
  - Settimanale: giorno della settimana (es. Lunedì).
  - Mensile: giorno del mese (GG).
- *Gli indirizzi email dei destinatari* se si desidera email di notifica di presa in carico del file in ingresso (opzionale).
- *Gli indirizzi email dei destinatari* se si desidera email di notifica di generazione del file di esito (opzionale).

L'invio del file deve rispettare la schedulazione anche in assenza di transazioni, occorre processare un file contenente solo i record di testa e coda.

Per la validazione formale di un file di esempio in ambiente di test occorre inviare il file via mail al servizio di supporto Commercio Elettronico.

Struttura del File

Il file è codificato con caratteri ASCII, ciascun record termina con CRLF (CR = codice ASCII 13 decimale; LF = codice ASCII 10 decimale).

- 00 RECORD DI TESTA
- 05 RECORD DI DETTAGLIO
- 99 RECORD DI CODA

I campi alfanumerici (Tipo = A) vanno allineati a sinistra e riempiti a destra con spazi vuoti, mentre i campi numerici (Tipo = N) vanno allineati a destra e riempiti a sinistra con zeri.

Di seguito vedremo in dettaglio le tre sezioni del tracciato, di cui quello di dettaglio verrà specificato per le due diverse procedure possibili.

Record di Testa

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	2	A	“00” Tipo Record
2	03	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	12	8	A	Data Creazione File YYYYMMDD
4	20	3	N	Progressivo flusso, chiave univoca valorizzabile da 001 a 999 (deve essere sempre diverso da 000 ed esiste il vincolo della consecutività, in modo da riscontrare eventuali mancate trasmissioni)
5	23	98	A	Spazi vuoti

Record di Coda

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	2	A	“99” Tipo Record
2	03	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	12	8	A	Data Creazione File YYYYMMDD
4	20	3	N	Progressivo flusso, chiave univoca valorizzabile da 001 a 999 (deve essere sempre diverso da 000 ed esiste il vincolo della consecutività, in modo da riscontrare eventuali mancate trasmissioni)
5	23	7	N	Totale record contenuti nel flusso (inclusi record di testa e coda)
6	30	91	A	Spazi vuoti

Record di Dettaglio Modifica Stato Contratto/Wallet ID

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	2	A	“05” Tipo Record
2	03	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	12	18	A	Merchant Order ID
4	30	1	A	Stato del Contratto/Wallet ID richiesto dal merchant : 1. In fase di richiesta valorizzato dal Cliente: • A – Attivo • S – Sospeso, i pagamenti effettuati con un Contratto/Wallet ID in questo stato vengono negati. È possibile riattivare un Contratto/Wallet ID con questo stato. • C – Chiuso, il cambio di stato non è reversibile. Un Contratto/Wallet ID con questo stato non può più essere riattivato. • ' ' - Non specificato, serve per richiedere la valorizzazione dello stato del Contratto/Wallet ID su Mercury Payment Services senza modificarne il valore. 2. In fase di risposta da MonetaWeb: • valorizzato col valore in fase di richiesta

5	31	1	A	Stato del Contratto/Wallet ID risposto da MonetaWeb: 1. In fase di richiesta dal Cliente: • riempito con spazi vuoti 2. In fase di risposta da MonetaWeb, verrà sempre valorizzato con lo stato che risulta sui nostri sistemi dopo aver effettuato le eventuali modifiche comandate dal merchant: • A - Attivo • S – Sospeso, i pagamenti effettuati con un Contratto/Wallet ID in questo stato vengono negati. È possibile riattivare un Contratto/Wallet ID con questo stato. • C – Chiuso, il cambio di stato non è reversibile. Un Contratto/Wallet ID con questo stato non può più essere riattivato. • N - Non Presente, se il codice Contratto/Wallet ID non viene trovato.
6	32	8	N	Data Ultima Modifica [YYYYMMDD]: 1. In fase di richiesta dal Cliente: • riempito con zeri 2. In fase di risposta da MonetaWeb: • valorizzata con la data di elaborazione. Se non è possibile effettuare la modifica (ad esempio per riattivazione di un Contratto/Wallet ID chiuso) sarà impostata la data di ultima modifica. In assenza di modifiche, viene restituita la data di attivazione.
7	40	72	A	Spazi vuoti

Record di Dettaglio Allineamento Carte

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	2	A	“05” Tipo Record
2	03	9	N	Codice Commerciante (generato e comunicato da Mercury Payment Services)
3	12	8	N	Codice Terminale (generato e comunicato da Mercury Payment Services)
4	20	19	A	Pan (per i clienti che gestiscono l'archivio carte) altrimenti spazi vuoti
5	39	4	A	Scadenza (per i clienti che gestiscono l'archivio carte) altrimenti spazi vuoti
6	43	1	A	Esito Allineamento: 3. In fase di richiesta dal Cliente: • riempito con spazi vuoti 2. In fase di risposta da MonetaWeb: • ‘0’ - L’allineamento è avvenuto correttamente • ’5’ - Non è stato possibile allineare i dati della carta • ’E’ - Pan carta non conforme / WALLET ID non presente
7	44	19	A	Pan Aggiornato (per i clienti che gestiscono l'archivio carte) : 1. In fase di richiesta dal Cliente: • riempito con spazi vuoti 2. In fase di risposta da MonetaWeb: • valorizzato Per i clienti che non gestiscono l'archivio carte sarà riempito con spazi vuoti

8	63	4	A	Scadenza Aggiornata (per i clienti che gestiscono l'archivio carte) : 1. In fase di richiesta dal Cliente: • riempito con spazi vuoti 2. In fase di risposta da MonetaWeb: • valorizzato, se esistente Per i clienti che non gestiscono l'archivio carte sarà riempito con spazi vuoti
9	67	3	A	1. In fase di richiesta dal Cliente: • riempito con spazi vuoti 2. In fase di risposta da MonetaWeb: • MON: Carta emessa da Intesa Sanpaolo • VAU: Carta appartenente al circuito VISA (ad esclusione di quelle emesse da Intesa Sanpaolo) • Response Code: in tutti gli altri casi (Vedi appendice "Response Code ISO")
10	70	7	N	Progressivo Record Dettaglio (parte da 0000001 fino ad un massimo di 9999999 record)
11	77	18	A	Valorizzato con: • Wallet id • spazi vuoti per i clienti che gestiscono l'archivio carte
12	95	26	A	Spazi vuoti

D. Elenco valute ammesse

La possibilità di effettuare pagamenti in valuta è disponibile attualmente solo per i brand VISA e MASTERCARD e solo per le seguenti valute:

Currency	Codice ISO	Nome Valuta	Paese
756	CHF	Franco Svizzero	Svizzera, Liechtenstein, Italia (Campione d'Italia)
978	EUR	Euro	Tutti i Paesi dell'Unione Monetaria Europea
826	GBP	Sterlina Britannica (o Lira Sterlina)	Regno Unito
840	USD	Dollaro Statunitense	Stati Uniti d'America, Samoa Americane, Territorio Britannico dell'Oceano Indiano, Ecuador, El Salvador, Guam,Haiti, Isole Marshall, Micronesia, Isole Marianne Settentrionali, Palau, Panamá, Timor Est, Isole Turks e Caicos,Isole Vergini Statunitensi

E. Risorse Grafiche (Pulsanti e Loghi)

Al fine di poter personalizzare le pagine di checkout e pagamento del merchant, sono disponibili le risorse grafiche dei loghi e pulsanti ufficiali e sempre aggiornati, scaricabili attraverso le rispettive url:

- Pulsanti di Checkout
- Loghi di Circuiti

F. Response Code ISO

000	Transazione Autorizzata
100	Autorizzazione Negata (Generico)
101	Carta Scaduta o Data Scadenza Invalida
102	Sospetta Frode
104	Carta non Valida
106	Numero Tentativi PIN Superato
109	Merchant non Valido
110	Importo non Valido
111	Numero Carta non Valido
115	Funzione Richiesta non Supportata
116	Disponibilità Insufficiente
117	Codice Segreto Errato
118	Carta Inesistente
119	Operazione non Permessa al Titolare Carta
120	Operazione non Permessa al Terminale
121	Limite Importo Superato
122	Operazione non Permessa
123	Numero Pagamenti Superato
124	Operazione non Permessa
125	Carta Inattiva
126	PIN Block Invalido
129	Sospetta Carta Contraffatta
182	Errore Wallet (Vedi appendice “Codici Errori MonetaWallet” per dettagli)
200	Autorizzazione Negata
202	Sospetta Frode
204	Carta Limitata
208	Carta Smarrita
209	Carta Rubata
210	Sospetta Carta Contraffatta
888	Pending
902	Transazione Invalida
903	Transazione Ripetuta
904	Errore di Formato
906	Cutover in Corso
907	Malfunzionamento Emittente

908	Routing non Disponibile
909	Malfunzionamento di Sistema
911	Timeout Emittente
913	Trasmissione Duplicata
999	Errore Creazione Contratto per Parametri Merchant

Non è consigliabile dettagliare i Response Code verso il titolare carta, in quanto indicare la ragione di una negazione significa fornire ai malintenzionati uno strumento per effettuare una frode. Suggeriamo di distinguere solamente tra esito positivo e negativo, consigliando eventualmente al titolare carta di ripetere la transazione prestando attenzione ai dati inseriti o di contattare direttamente la propria banca.
La lista completa dei codici di errore ISO è disponibile su richiesta.

G. Codici di errore MonetaWeb

10000	GET method is invalid.
GV00004	PARes Status not Successful.
GV00005	Missing Pares Data.
GV00006	Incorrect Pares Data.
GV00007	Incorrect Data. Verify enrollment data and pay data mismatch.
GV00008	Pares status N cannot be authorized.
GV00013	Invalid Payment ID.
GV00015	Expired Payment ID.
GW00008	Invalid Data Request.
GW00150	Missing required data.
GW00151	Invalid TrackId.
GW00158	Card Number Not Numeric.
GW00159	Card Number Missing.
GW00160	Invalid Brand.
GW00161	Invalid Card/Member Name data.
GW00162	Currency not supported by brand.
GW00163	Invalid Address data.
GW00164	Invalid Email.
GW00166	Invalid Card Number data.
GW00167	Transaction Id Not Numeric.
GW00175	Invalid Result Code.
GW00176	Transaction Already Captured.
GW00177	Transaction is not yet captured.
GW00179	Transaction Already Cancelled.
GW00180	Void Authorization Failed. Check the Transaction Status.
GW00181	Operation Failed.
GW00182	Transaction Already Voided.
GW00187	Invalid Electronic Commerce Indicator.
GW00201	Transaction not found.
GW00203	Invalid access: Must use POST method.

GW00206	More than one result found.
GW00264	Terminal not enabled for Recurrent Payment.
GW00265	Missing Recurrent Payment Data.
GW00266	Invalid Recurrent Payment Data.
GW00267	Invalid Wallet Merchant Payment Data.
GW00268	Invalid Request: walletId and card cannot be present together.
GW00269	Missing field mandatereferenceid.
GW00270	Invalid currency code.
GW00271	Amend twice is not Allowed.
GW00305	Invalid Currency Code.
GW00358	Invalid mandatereferenceid to cancel: [%]
GW00359	Invalid mandatereferenceid to amend: [%]
GW00401	Missing Required Data.
GW00453	Legacy Terminal not allowed.
GW00454	Terminal password required.
GW00455	Terminal disabled.
GW00456	Invalid Terminal ID.
GW00457	Action not supported.
GW00458	Field [%] lenght is not between % and %
GW00459	Action invalid.
GW00460	Terminal ID required.
GW00461	Invalid Transaction Amount.
GW00470	Payment Frequency invalid.
GW00480	Date invalid.
GW00488	Error with internal transaction origin.
GW00856	Invalid Card Verification Code.
GW00858	Missing required data - CVV.
GW00859	Missing required data - Expiry Year.
GW00860	Missing required data - Expiry Month.
GW00874	Invalid Expiration Date.
GW00999	Invalid Payment Request.
PP10001	PayPal Generic Error.

PY20000	Missing Required Data.
PY20001	Invalid Operation Type.
PY20002	Invalid Amount.
PY20003	Missing Operation Type.
PY20008	Invalid Currency Code.
PY20010	Invalid Merchant URL.
PY20084	Invalid Payment ID Error.

H. Codici di errore MonetaWallet (Tokenizzazione) - Pagamenti Ricorrenti

ErrorCode	***ErrorMessage***
WS00010 - WS00044	Generic Error
WS00051	Unregistered Merchant
WS00052	Inactive Merchant
WS00061	Wallet not found
WS00062	Inactive Wallet
WS00063	Wallet Already Exists
WS00064	Wallet not found for Substitution
WS00065	Inactive Wallet for Substitution
WS00071	Invalid Card Type
WS00072	Card Exceeds Max Wallet Limit
WS00073	Card is in Black List
WS00074	Exceeds Monthly Amount Limit
WS00075	Minimum Amount Not Reached
WS00076	Exceeds Max Amount Limit
WS00077	Invalid Country
WS00078	Card and Pos country should match
WS00081	Installment Already Exists
WS00091	Secure Activation Required