MonetaWeb 2.0

Marzo 2014

INDICE

Protocollo XML per pagamenti 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.

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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	'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

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 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	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	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:

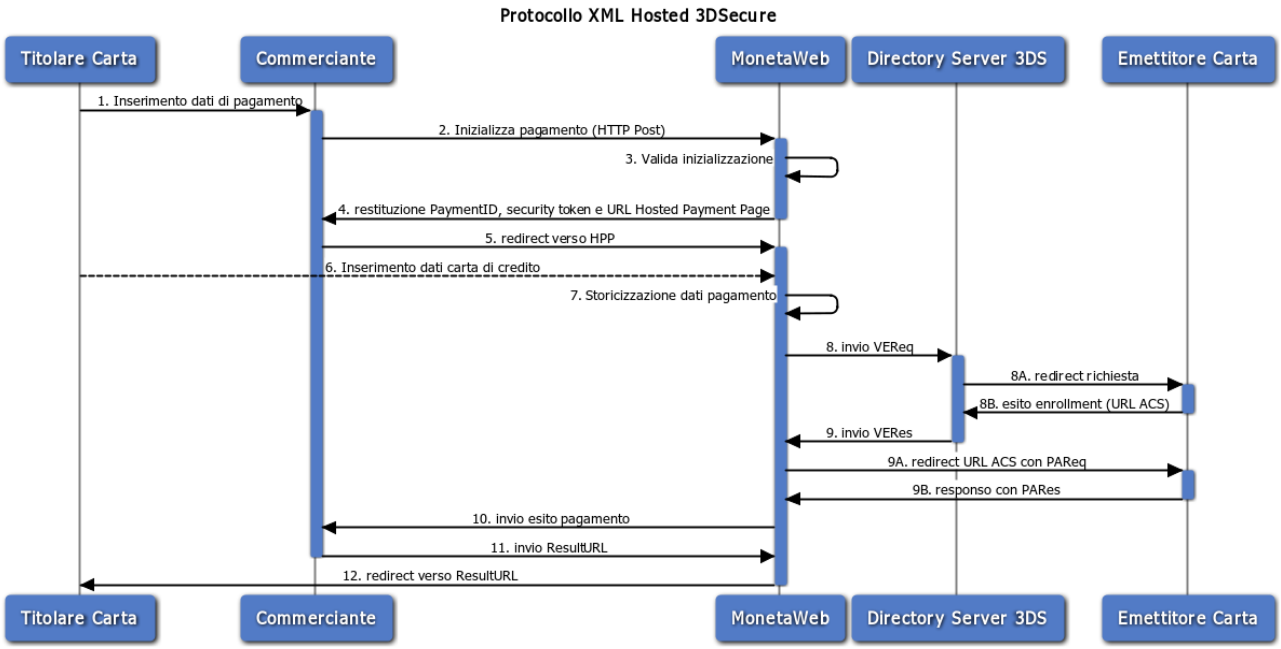
In caso di invio di parametri errati (es. terminale sconosciuto, password errata, importo invalido, …) MonetaWeb risponde con un messaggio di errore in formato XML.
Tale messaggio comprende:

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

Esempio messaggio di errore in fase di Inizializzazione:

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

Protocollo XML Hosted 3DSecure



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 (vedi pag. 4)
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 (vedi pag. 10)
12. Monetaweb redirige il titolare carta verso la ResultURL

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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

- 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	'978' (euro)		
language	Lingua in cui verrà visualizzata la Hosted Page ['ITA', 'DEU', 'FRA', 'SPA', 'USA']		
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>123456789012345678</paymentid>
    <securitytoken>80957febda6a467c82d34da0e0673a6e</securitytoken>
    <hostedpageurl>http://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. Tale url non deve essere impostato come parametro fisso della redirezione ma, per ogni pagamento, deve essere reperito dinamicamente dall'apposito tag.

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 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. Questo url può essere arricchito con dei parametri per consentire la corretta visualizzazione dell'esito stesso.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido, …) 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:

Transazione autorizzata:
authorizationcode=85963&cardcountry=ITALY&cardexpirydate=0115&cardtype=VISA&
customfield=some custom field&maskedpan=483054******1294&
merchantorderid=TRCK0001&paymentid=12345678901234567 8&responsecode=000&
result=APPROVED&rrn=85236952369525&securitytoken=80957febda6a467c82d34da0e0673a6e
&threedsecure=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 - NOT AUTHENTICATED, autenticazione 3D fallita - 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	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 123456xxxxxx7890)	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	char	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

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:

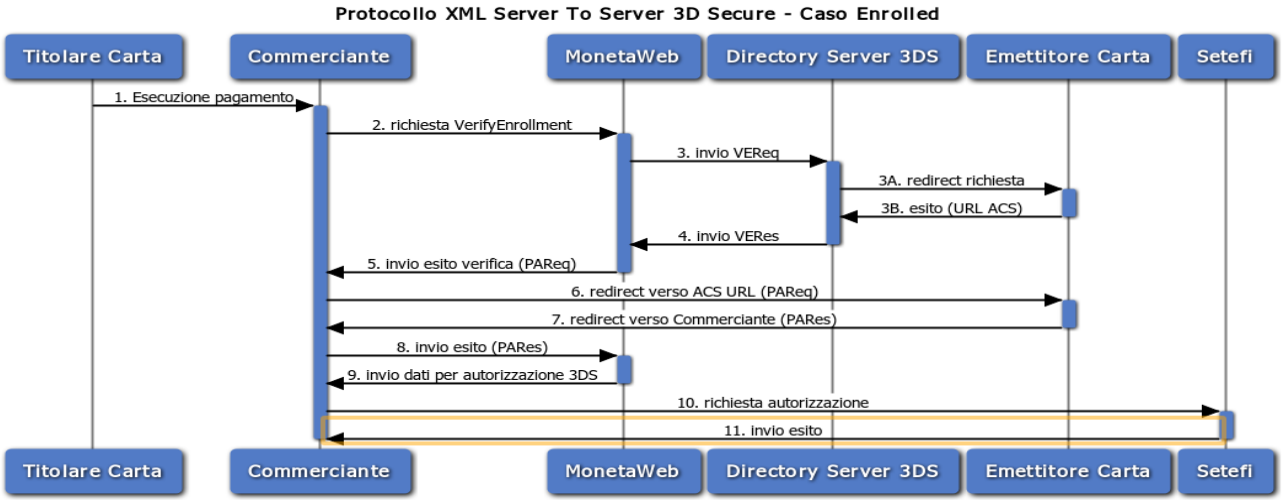
- un codice di errore
- una descrizione parlante dell'errore

Esempio messaggio di errore in fase di Inizializzazione:

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

Protocollo XML Server To Server 3D Secure

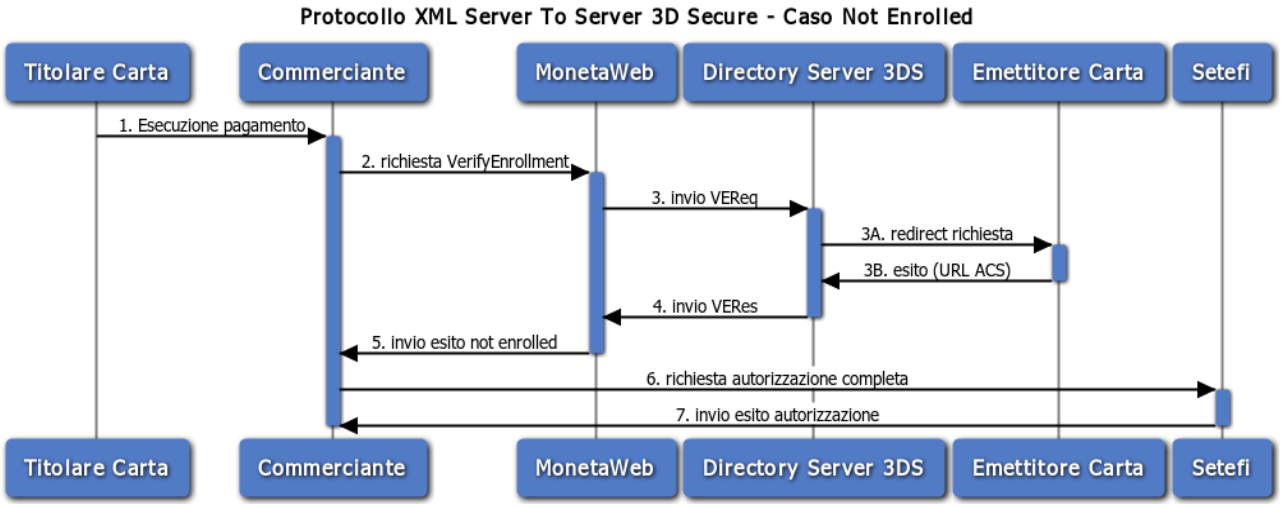
Caso Enrolled



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. 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 invia 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 Setefi una richiesta di autorizzazione 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 Setefi una richiesta di autorizzazione completa di tutti i dati (dati ordine, dati carta, flag ECI)
7. MonetaWeb processa la richiesta di autorizzazione e restituisce l'esito al Commerciante.

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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

- 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=Password1&operationtype=verifyenrollment&card=4511849990000022&cvv2=123&expiryyear=2014&expirymonth=12&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	'978' (euro)		
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	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
paymentid	Id associato alla sessione di pagamento	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 Setefi 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=Password1&operationtype=verifypares&paymentid=298597
096655040209&pares=eJydWFmzosqyfudXdKzzSPRmVGGHvU4UMyoIMolvTDKDCgry60+pPa
zdu(...)
```

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>298597096655040209</paymentid>
<cavv>AAACBSMAFQAAAAAAAAAVAAAAAAA=</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)

PAYTHREESTEP

All'interno del flow per i pagamenti Server to Server è la servlet esposta per la richiesta di autorizzazione; riceve in input tutti i dati del pagamento: dati ordine, dati carta, dati 3D Secure, ove presenti; restituisce in output l'esito del pagamento.

Esempio di richiesta:

```
id=99999999&password=Password1&operationtype=paythreestep&paymentid=
298597096655040209&amount=0.1&currencycode=978&merchantorderid=order001&d
escription=description&cardholdername=member&card=4511849990000022&expiry
year=2014&expirymonth=12&cvv2=123&customfield=customdata&eci=05&xid=eFtyU
1M8OWlhSzcmOWhNKCZXZF4=&cavv=AAACBSMAFQAAAAAAAAAVAAAAAAA=
```

Parametri di richiesta:

Nome	Descrizione	Tipo	Lunghezza
id	Id associato al terminale	char	8
password	Password associata all'id terminale	varchar	50
operationType	paythreestep	varchar	
paymentid	Id associato alla sessione di pagamento (restituito dalla Verify Enrollment)	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	'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	varchar	255
cavv	Firma del pagamento	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>402077780274</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	varchar	18
merchantorderid	Riferimento Operazione scelto dal Commerciante	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	Description	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255

Attivazione Pagamenti Ricorrenti e MonetaWallet

SPECIFICHE PER L'ATTIVAZIONE

Eseguendo una transazione MO.TO con CVV2, Hosted 3DSecure oppure Server To Server 3DSecure è possibile salvare i dati carta presso Setefi 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: • F: verifica fattibilità (feasibility) • C: creazione contratto (creation) • S: sostituzione carta (substitution)	char	1
walletid	Token carta (univoco)	varchar	18

Il salvataggio dei dati carta è condizionato al buon esito della richiesta di autorizzazione.
Nel caso in cui la richiesta di pagamento violi le regole della creazione di un walletID (Token carta già esistente, tipo carta non ammesso, superamento del numero di contratti consentiti per la stessa carta) il sistema restituirà il codice di errore “182”.

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 utilizzando il campo walletID al posto dei dati carta e valorizzando il recurringAction come in tabella sottostante:

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 “Tracciato File Pagamenti Ricorrenti”.

Conferma del pagamento (Richiesta di contabilizzazione)

Attraverso l’operazione di conferma è possibile richiedere la contabilizzazione di una transazione autorizzata. A seconda delle specificità del proprio business è possibile scegliere i seguenti tipi di contabilizzazione:

- 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. E’ possibile confermare operazioni relative alle precedenti giornate, purché non anteriori a 4 giorni di calendario
- A MEZZO FILE: dopo la fase di pagamento sarà necessario inviare a Setefi 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

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 il proprio terminale è stato configurato per avere una contabilizzazione di tipo esplicito sarà necessario procedere manualmente alla conferma delle autorizzazioni. A tal fine è possibile utilizzare a scelta:

- l’apposita funzionalità di backoffice http://www.monetaonline.it/monetaweb/backoffice
- l’apposito messaggio Server to Server descritto in questo capitolo

Indipendentemente dallo strumento di conferma esplicita scelto, è possibile:

- confermare la totalità dell’importo autorizzato
- confermare parzialmente l’importo autorizzato; in questo caso l‘importo non confermato non potrà poi essere recuperato

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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	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>
```

Storno contabile

Attraverso l'operazione di storno è possibile fare in modo che l'importo di una transazione precedentemente confermata venga riaccreditato sulla carta di credito del titolare.

Per effettuare uno storno è possibile utilizzare a scelta:

- l'apposita funzionalità di backoffice http://www.monetaonline.it/monetaweb/backoffice
- l'apposito messaggio Server to Server descritto in questo capitolo

Indipendentemente dallo strumento utilizzato è possibile:

- stornare la totalità dell'importo confermato
- stornare parzialmente l'importo confermato
- ripetere l'operazione di storno parziale fino a che la somma degli importi stornati non sarà pari all'importo della conferma iniziale

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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	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>
```

Annullamento dell'autorizzazione

Attraverso l'operazione di annullamento autorizzazione è possibile fare in modo che l'importo di una transazione precedentemente autorizzata venga riaccreditato sulla carta di credito del titolare.
Poiché questa operazione non agisce a livello contabile bensì autorizzativo, tramite lo scambio di messaggi online con i circuiti internazionali (Visa, MasterCard, Amex, Diners, …), questa funzionalità è IRREVERSIBILE.
In caso di erroneo annullamento di un'autorizzazione sarà quindi necessario chiedere al titolare di effettuare nuovamente il pagamento, reinserendo i dati delle carta di credito.

Per effettuare un annullamento autorizzazione è possibile utilizzare a scelta:

- l'apposita funzionalità di backoffice http://www.monetaonline.it/monetaweb/backoffice
- l'apposito messaggio Server to Server descritto in questo capitolo

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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	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>
```

Inquiry, interrogazione per transazione

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

Al fine di identificare univocamente il pagamento è necessario fornire tra i parametri di input un valore a scelta tra:

- il paymentId della transazione, fornito da MonetaWeb in fase di pagamento
- il merchantOrderId della transazione, fornito a MonetaWeb in fase di pagamento, purché univoco

Nel caso in cui il merchantOrderId non fosse sufficiente per identificare univocamente un pagamento verrebbe ritornato un messaggio di errore.

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

INVIO DEL MESSAGGIO DI INQUIRY

Esempio messaggio HTTP di inquiry:

id=99999999&password=99999999&operationType=inquiry&paymentId=123456789012345&merchantOrderId=TrackingNo12345

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' oppure 'inquirymybank' a seconda della modalità con cui era stato eseguita la transazione.	varchar	50
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 INQUIRY

Esempio messaggio XML di esito inquiry:

```
<response>
   <result>APPROVED</result>
   <paymentid>123456789012345</paymentid>
   <merchantorderid>TrackingNo12345</merchantorderid>
   <authorizationcode>123456</authorizationcode>
   <threedsecure>N</threedsecure>
   <responsecode>000</responsecode>
   <customfield>campoPersonalizzabile</customfield>
   <description>Descrizione</description>
   <rrn>123456789012</rrn>
   <cardcountry>ITALY</cardcountry>
   <maskedpan>123456******7890</maskedpan>
</response>
```

Parametri di risposta al messaggio di inquiry:

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 • NOT AUTHENTICATED, autenticazione 3D fallita • PARES ERROR, errore in fase di autenticazione 3D	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	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 inviato dal Commerciante in fase di pagamento	varchar	255
customfield	Campo libero inviato dal Commerciante in fase di pagamento	varchar	255
cardcountry	Nazionalità della carta di credito utilizzata	char	255
maskedpan	PAN mascherato della carta utilizzata in fase di pagamento	varchar	19
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
threedsecure	Livello di sicurezza della transazione: 'S' (transazione Full Secure), 'H' (transazione Half Secure), 'N' (transazione Not Secure)	char	1
cardholderip	IP del titolare carta (solo per le transazioni 3DSecure)	varchar	15
securitytoken	Token di sicurezza (solo per le transazioni 3DSecure)	varchar	32

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>
```

Tracciato TRINIZ

Il file è costruito secondo le specifiche ed il tracciato di seguito riportate.

TRINIZCCCCCDDDDDDHHHHHHTE45001A

COINIZCCCCCDDDDDDHHHHHH200150

0MMMMMMMMMTTTTTTTT0010001DDDDDDHHHH 000000010AAAAAA
10RRRRRRRRRRRROOOOOOOOOOOOOOOOOO

0MMMMMMMMMTTTTTTTT0010002DDDDDDHHHH 000010000AAAAAA
10RRRRRRRRRRRROOOOOOOOOOOOOOOOOO

0MMMMMMMMMTTTTTTTT0010003DDDDDDHHHH 000000100AAAAAA
17RRRRRRRRRRRROOOOOOOOOOOOOOOOOO

COFINECCCCC0001000050000000100100000000000000000000000100DDDDDDDDDDDD

TRFINECCCCC00007

Legenda:

CCCCC = Codice Cliente
MMMMMMMMM = Codice Commerciante
TTTTTTTT = Codice Terminale
DDDDDD = Data (ggmmaa)
HHHHHH = Ora (hhmmss)
HHHH = Ora (hhmm)
AAAAAA = Codice Autorizzazione
RRRRRRRRRRR = Retrieval Reference Number
OOOOOOOOOOOOOOOOO = Riferimento Operazione

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). Tutti i record sono lunghi 126 caratteri e terminano con i due caratteri CRLF (lunghezza totale del record 128).

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, per più di 9999 transazioni una seconda contabile (COINIZ-COFINE), la chiusura del flusso con record TRFINE.

Ogni file TRINIZ può contenere al massimo 10 contabili (COINIZ-COFINE), in quanto il totalizzatore finale delle righe è lungo 5 caratteri, quindi può contenere al massimo 9999x10=99990 transazioni. Al superamento della soglia di 99990 transazioni è necessario creare un altro TRINIZ.

ESEMPIO

- TRINIZ inizio trasmissione
- COINIZ inizio contabile
- 0 dettaglio (1 o più)
- COFINE fine contabile
- TRFINE fine trasmissione

MSG TRINIZ – inizio trasmissione

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“TRINIZ”
2	07	5	N	Codice Cliente (generato e comunicato da Setefi)
3	12	6	N	Data creazione file (ggmmaa)
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)
8	31	1	A	“A”
9	32	95	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 Setefi)
3	12	6	N	Data creazione file (ggmmaa)
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)
7	28	2	N	“50” (euro)
8	30	97	A	Spazi vuoti

MSG 0 – Record di dettaglio

Comporre il record di dettaglio in base allo scopo del file, successivamente vengono descritte alcune tipologie di MSG 0 (per contabilizzazione via file, pagamenti ricorrenti).

MSG COFINE – fine contabile

Nr.	Posizione	Lunghezza	Tipo	Descrizione
1	01	6	A	“COFINE”
2	07	5	N	Codice Cliente (generato e comunicato da Setefi)
3	12	1	N	“0”
4	13	3	N	Numero progressivo della contabile corrispondente (uguale al campo 6 di COINIZ)
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)
10	63	6	N	Data contabile (ggmmaa)
11	69	58	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 Setefi)
3	12	5	N	Totale record da TRINIZ a TRFINE (inclusi)
4	17	110	A	Spazi vuoti

MSG 0 – 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 Setefi)
3	11	8	N	Codice Terminale (generato e comunicato da Setefi)
4	19	3	N	Numero progressivo della contabile corrispondente (uguale al campo 6 di COINIZ)
5	22	4	N	Numero progressivo della transazione (parte da 0001)
6	26	6	N	Data transazione (ggmmaa)
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 Setefi
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 Setefi
15	91	18	A	Riferimento Operazione = al "merchantorderid" presente nel messaggio di richiesta autorizzazione inviato a Setefi
16	109	18	A	Spazi vuoti

MSG 0 – Record di dettaglio per Pagamenti Ricorrenti

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 Setefi)
3	11	8	N	Codice Terminale (generato e comunicato da Setefi)
4	19	3	N	Numero progressivo della contabile corrispondente (uguale al campo 6 di COINIZ)
5	22	4	N	Numero progressivo della transazione (parte da 0001)
6	26	6	N	Data transazione (ggmmaa)
7	32	4	N	Ora transazione (hhmm)
8	36	19	A	Numero carta (solo clienti che gestiscono l'archivio carte)
9	55	4	N	Data scadenza (aamm) (solo clienti che gestiscono l'archivio carte)
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 Setefi: - 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

Nr.	Posizione	Lunghezza	Tipo	Descrizione
15	79	12	A	RRN (Retrieval Reference Number) in fase di richiesta dal Cliente: - riempito con spazi vuoti; in fase di risposta da Setefi: - valorizzato
16	91	18	A	Riferimento Operazione (per la vecchia gestione dei pagamenti ricorrenti è il codice contratto)
17	109	18	A	Spazi vuoti
18	127	30	A	A disposizione del cliente
19	157	3	A	Responde Code, “000” se la transazione è stata autorizzata
20	160	8	A	Data autorizzazione (aaaammgg)
21	168	18	A	Walletid creato dai Commercianti e utilizzato al posto del PAN
22	186	5	A	Spazi vuoti

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 <> 9999 -> 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.

CARTE DI TEST

Circuito	Numero Carta	Data Scadenza	CVV	Password 3D Secure	Esito
VISA	4830540099991310	01/2016	557	valid	OK
VISA	4830540099991294	01/2016	952	valid	OK
VISA	4943319600239756	02/2015	256	-	OK
VISA	4943319600243857	02/2015	134	-	OK
MC	5533890199999896	02/2015	678	valid	OK
MC	5398320199991093	01/2017	295	valid	OK
MC	5533890199999870	02/2015	132	valid	OK
MC	5209569603136146	02/2015	127	-	OK

Response Code ISO

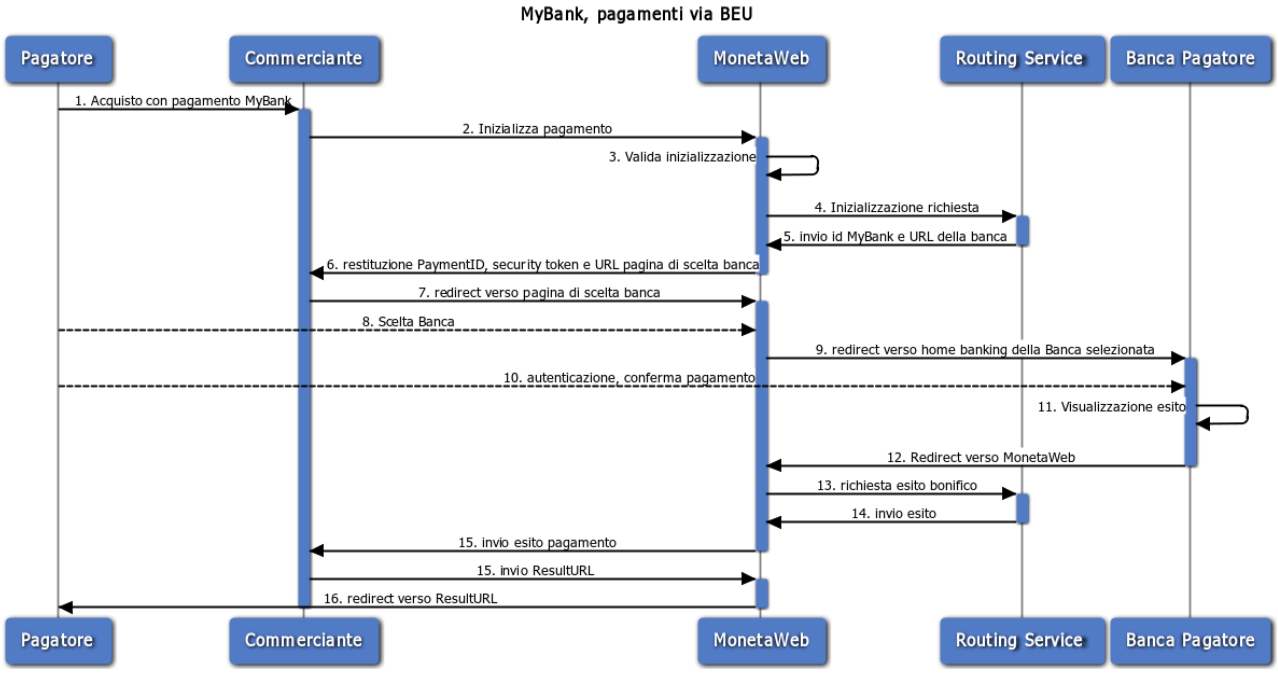
000	TRANSAZIONE AUTORIZZATA
100	AUTORIZZAZIONE NEGATA (GENERICO)
101	CARTA SCADUTA
102	SOSPETTA FRODE
104	CARTA NON VALIDA
107	CHIAMARE EMITTENTE
109	MERCHANT NON VALIDO
110	IMPORTO NON VALIDO
111	NUMERO CARTA NON VALIDO
116	DISPONIBILITA' INSUFFICIENTE
117	CODICE SEGRETO ERRATO
119	OPERAZIONE NON PERMESSA
120	OPERAZIONE NON PERMESSA
122	OPERAZIONE NON PERMESSA
129	SOSPETTA CARTA CONTRAFFATTA
200	AUTORIZZAZIONE NEGATA
208	CARTA SMARRITA

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.

Codici di errore MonetaWeb

10000	GET METHOD IS INVALID
GW00457	ACTION NOT SUPPORTED
GW00167	INVALID CURRENCY CODE DATA
GW00305	INVALID CURRENCY CODE
GW00461	INVALID TRANSACTION AMOUNT
GW00150	MISSING REQUIRED DATA
PY20001	INVALID ACTION TYPE
PY01063	CURRENCY CODE NOT NUMERIC
PY00167	INVALID CURRENCY CODE DATA
PY20008	INVALID CURRENCY CODE
PY20000	MISSING REQUIRED DATA
PY20002	INVALID AMOUNT
GW00161	INVALID CARD/MEMBER NAME DATA
GW00999	INVALID PAYMENT REQUEST
GW00160	INVALID BRAND
GW00858	MISSING REQUIRED DATA CVV
GW00203	INVALID ACCESS: MUST USE POST METHOD
GW00859	MISSING REQUIRED DATA EXPIRY YEAR - EXPIRATION YEAR IS REQUIRED
GW00460	TRANPORTAL ID REQUIRED
GW00456	INVALID TRANPORTAL ID
GW00454	TRANPORTAL PASSWORD REQUIRED

MyBank, pagamenti via BEU



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 contatta il Routing Service di EBA
5. Il Routing Service restituisce l'id myBank e URL della banca
6. MonetaWeb restituisce al Commerciante il PaymentID, un security token e la URL della pagina di scelta Banca
7. Il server del Commerciante redirige il Pagatore verso la pagina di scelta Banca
8. Il Pagatore sceglie la Banca tra quelle disponibilie
9. Il Pagatore viene rediretto sull'home banking della Banca selezionata
10. Il Pagatore si autentica e trova un bonifico SEPA precompilato, conferma il pagamento e riceve in tempo reale dalla Banca l'esito del bonifico.
11. La Banca redirige il Pagatore verso MonetaWeb
12. MonetaWeb contatta il Routing Service di EBA per conoscere l'esito del bonifico
13. Il Routing Service di EBA invia l'esito richiesto a MonetaWeb
14. MonetaWeb invia in modalità "server to server" l'esito del pagamento alla ResponseURL sul server del Commerciante

15. Il Commerciante invia sulla stessa socket la ResultURL del Commerciante
16. Monetaweb redirige il Pagatore verso la pagina di esito del maerchant (ResultURL)

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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=mybank&amount=1.00&currencyCode=978&
language=ITA&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
currencyCode	'978' (euro)	varchar	3
language	Lingua in cui verrà visualizzata la pagina di scelta Banca ['ITA', 'DEU', 'FRA', 'SPA', 'USA']	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>123456789012345678</paymentid>
    <securitytoken></securitytoken>
    <hostedpageurl>http://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 carta 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.

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 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. Questo url può essere arricchito con dei parametri custom per consentire la corretta visualizzazione dell'esito stesso.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido, …) Monetaweb reindirizzerà il pagatore verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro del messaggio di Inizializzazione.

Nel caso in cui, in fase di Inizializzazione del pagamento, il parametro recoveryUrl non fosse stato valorizzato, MonetaWeb rediregerà il pagatore verso una pagina di cortesia, pubblicata direttamente sul server MonetaWeb.

Esempio pagina di ricezione dell'esito:

```
<%
// parsing del messaggio di risposta
String paymentID = request.getParameter("paymentid");
String result = request.getParameter("result");
String responseCode = request.getParameter("responsecode");
String authorizationCode = request.getParameter("authorizationcode");
```

```
String merchantOrderId = request.getParameter("merchantorderid");
String threeDSecure = request.getParameter("threedsecure ");
String rrn = request.getParameter("rrn");
String maskedPan = request.getParameter("maskedpan");
String cardCountry = request.getParameter("cardcountry");
String customField = request.getParameter("customfield");
String securityToken = request.getParameter("securitytoken");

// verifica della corrispondenza del securityToken
// storicizzazione dell'esito del pagamento
// url per la redirezione del titolare sulla pagina web di
// visualizzazione dell'esito

out.println("http://www.merchant.it/result.jsp" + "?paymentId=" + paymentId);
%>
```

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: visualizza tutti i bonifici autorizzati dalla • Error: visualizza solamente i bonifici non completati perché negati dalla Banca del pagatore • Aborted: visualizza solamente i bonifici abbandonati dal pagatore • Timeout: visualizza solamente i bonifici non completati per superamento del tempo limite a disposizione • Pending: visualizza solamente i bonifici in attesa di esito	varchar	20
responsecode	Codice di risposta (es: '000' se bonifico autorizzato,, in tutti gli altri casi transazione negata)	char	3
authorizationcode	Codice di autorizzazione, valorizzato solo se il bonifico è stato autorizzata	varchar	6
merchantorderid	Riferimento Operazione inviato dal Commerciante in fase di Inizializzazione	varchar	18
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

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:

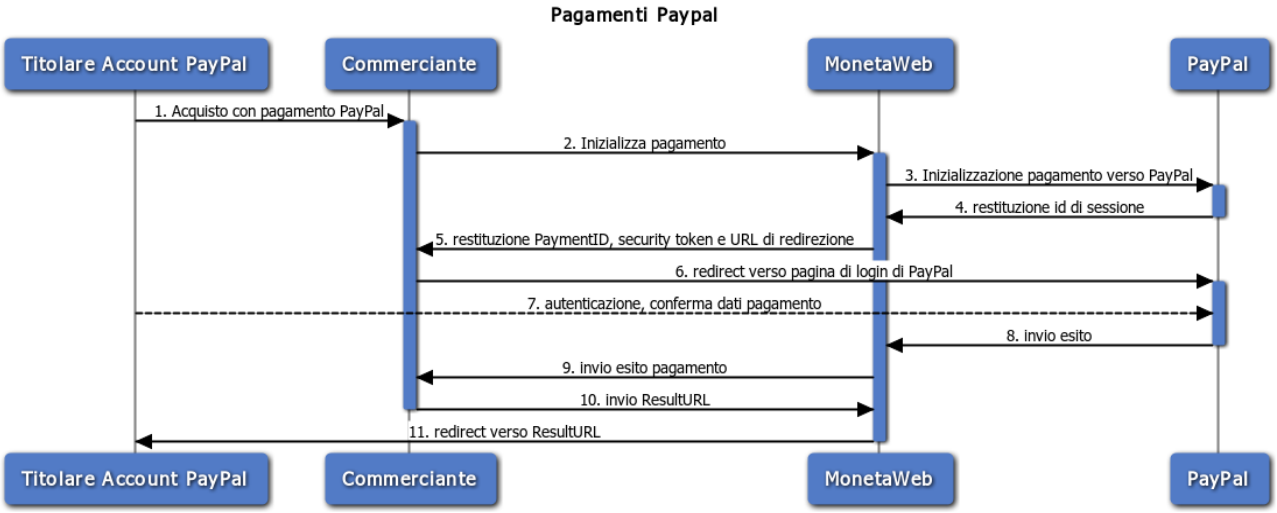
```
<error>
  <errorcode>XYZ123</errorcode>
  <errormessage>Invalid amount</errormessage>
</error>
```

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

Pagamenti PayPal



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 id 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 processa il pagamento e restituisce un esito a MonetaWeb
9. MonetaWeb invia in modalità “server to server” l’esito del pagamento alla ResponseURL del Commerciante
10. Il Commerciante risponde a MonetaWeb inviando la ResultURL
11. Monetaweb redirige il titolare carta verso la ResultURL per la visualizzazione dell'esito finale.

SPECIFICHE PER L'INVIO DEI MESSAGGI

Protocollo
HTTP

Metodo
POST

Content-Type
URL Encoded (legacy): application/www-form-urlencoded or 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

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&currencyCode=978&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
currencyCode	'978' (euro)		
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 (obbligatorio se si usa l'indirizzo di spedizione)	varchar	32
shippingstreet	Indirizzo di spedizione (obbligatorio se si usa l'indirizzo di spedizione)	varchar	100
shippingcity	Nome della città (obbligatorio se si usa l'indirizzo di spedizione)	varchar	40
shippingstate	Nome dello Stato o provincia (obbligatorio se si usa l'indirizzo di spedizione)	varchar	40
shippingzip	Codice di avviamento postale (CAP) del paese di spedizione (obbligatorio negli Stati Uniti e nei Paesi laddove richiesto)	varchar	20
shippingcountry	Codice del Paese di spedizione, es. IT, NL, ES … (obbligatorio se si usa l'indirizzo di spedizione)	varchar	2
shippingphone	Numero di telefono (opzionale)	varchar	20

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. 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 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. Questo url può essere arricchito con dei parametri per consentire la corretta visualizzazione dell'esito stesso.

Nel caso in cui la comunicazione dell'url di redirezione del titolare dovesse fallire (indisponibilità della pagina responseToMerchantUrl, contenuto della pagina responseToMerchantUrl non valido, …) Monetaweb reindirizzerà il titolare verso la pagina recoveryUrl, che viene comunicata dal Commerciante stesso tramite l'apposito parametro (opzionale) 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://localhost:8080/phoenix-0.0/demo/ica/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 - NOT APPROVED, transazione negata - CAPTURED, transazione confermata - PENDING, transazione sospesa in attesa di verifica	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	varchar	18
cardtype	Circuito e tipologia della carta di credito utilizzata (su richiesta) - ['Amex', 'Diners', 'Maestro', 'Mastercard', 'Moneta', 'Visa', 'BAPAYPAL', 'PAYPAL']	varchar	10
customfield	Campo libero inviato dal Commerciante in fase di Inizializzazione	varchar	255
securitytoken	Token di sicurezza	varchar	32

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>
```