

## **SERVIZI DI COMMERCIO ELETTRONICO:**

Autorizzazione di Pagamenti su Siti Remoti

Codice documento : *specificheTecniche\_ver2.3*

<b>1. GENERALITÀ.....</b>	<b>2</b>
<b>2. SVOLGIMENTO DEL PAGAMENTO.....</b>	<b>2</b>
<b>3. MODALITÀ OPERATIVE.....</b>	<b>3</b>
<b>4. UTILIZZO DEL MAC (MESSAGE AUTHENTICATION CODE) .....</b>	<b>5</b>
<b>5. MODALITÀ DI AUTORIZZAZIONE.....</b>	<b>6</b>
<b>6. ADATTAMENTI AL SITO .....</b>	<b>6</b>

## 1. Generalità

Il sistema descritto si basa su tre principi:

- ❖ la **separazione dell'ambiente commerciale** (quello in cui i beni o servizi vengono proposti ai consumatori e in cui i consumatori compongono e trasmettono il loro ordine di acquisto) **dall'ambiente di pagamento** (quello in cui vengono scambiate le informazioni riservate con cui il consumatore dà mandato di pagamento);
- ❖ la **non intrusività**, ovvero la possibilità di funzionare senza installare alcuna componente software né presso il *merchant* né sulla postazione del consumatore intento all'acquisto. Il sistema è compatibile con qualunque tipo di server e di sistema operativo presente presso il *merchant*;
- ❖ l'utilizzo di soli **protocolli standard** nel dialogo con i consumatori: http/https mediante SSL (128 bit).

Il sistema gestisce attualmente pagamenti con carte **Visa, MasterCard, American Express, Diners e Jcb**. Sono in corso contatti con altri circuiti di pagamento internazionali.

I pagamenti negoziati vengono trattati solo in Euro.

Con gli acquirer che lo permetteranno (ad oggi Servizi Interbancari e Bankamericard) i pagamenti potranno essere effettuati secondo l'architettura e il protocollo SET. Sul circuito VISA EU infatti la responsabilità della transazione, quindi il rischio della stessa, si sposterà dall'acquirer (i.e. dal merchant) all'issuer.

## 2. Svolgimento del pagamento

Il sistema prevede che il consumatore acceda, via *web*, al sito del venditore e qui prenda visione di quanto in offerta.

Se il consumatore decide di acquistare, al momento del pagamento viene rimandato su un server sicuro (certificato da Verisign) localizzato presso CILME-MULTITEL, il quale propone al consumatore una pagina, graficamente omogenea al sito del venditore, in cui si pubblica il nome del venditore e l'importo della transazione e si invita il cliente, se intenzionato a procedere al pagamento con carta di credito, a introdurre i dati relativi allo strumento di pagamento.

I dati del pagamento viaggiano su canale cifrato ed autenticato tramite SSL fino a CILME-MULTITEL, che li usa per chiedere immediatamente l'autorizzazione al pagamento sui normali circuiti autorizzativi.

L'esito della richiesta viene comunicato al venditore e opzionalmente anche al consumer secondo modalità e formato concordate (posta elettronica e/o transazione on-line su internet, mediante protocollo http/https).

Nello scambio di informazioni tra CILME-MULTITEL e merchant, indipendentemente dalla modalità utilizzata, è possibile aggiungere la fase di autenticazione reciproca compiuta accodando ad ogni messaggio un MAC (Message Code Authentication) calcolato sui dati della transazione.

L'adozione di un MAC è fortemente consigliata in quanto consente di verificare, sia a CILME-MULTITEL che al merchant, che non siano stati manipolati i dati inviati all'url (i.e. importo, divisa, codTrans)

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

Per facilitare la gestione degli ordini CILME-MULTITEL SpA mette a disposizione dell' esercente lo strumento di **Amministrazione on-line** che permette di snellire le attività amministrative inerenti il negozio virtuale.

**Amministrazione on-line** è infatti un' Area Riservata al merchant, all'interno della quale, in modo semplice e rapido, è possibile consultare l'archivio dei pagamenti e-commerce oltre a poterne disporre la contabilizzazione o lo storno.

Una volta attivato il pos virtuale, CILME-MULTITEL invia all' esercente, insieme al manuale di utilizzo, i codici personali di accesso ad **Amministrazione on-line**.

### 3. Modalità operative

Il sito Internet remoto che debba farsi autorizzare pagamenti inserirà nella pagina che precede il pagamento un *link* all'URL

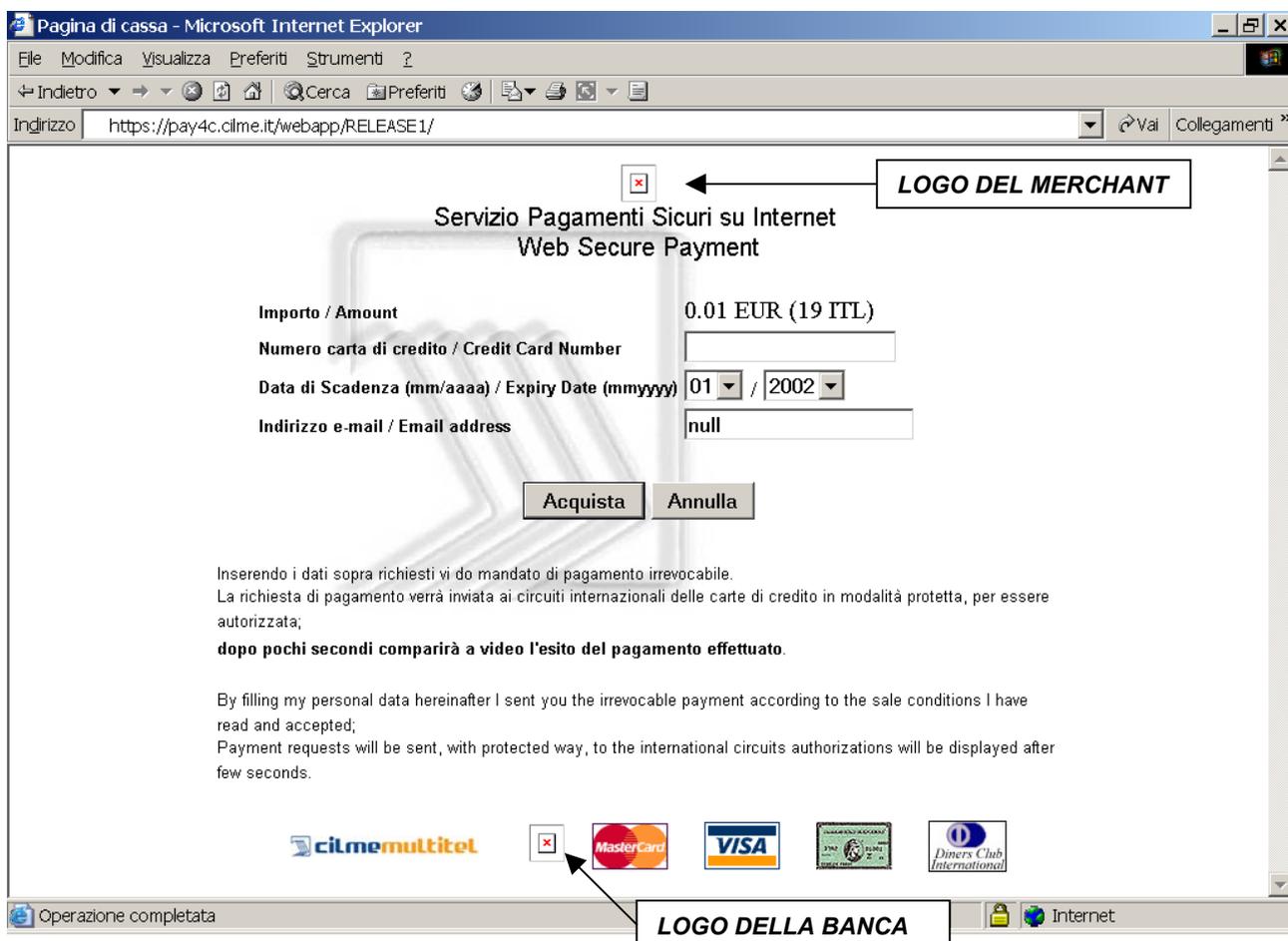
**<https://pay4c.cilme.it/webapp/RELEASE1/DispatcherServlet>**

passando i seguenti parametri con metodo post (consigliato) o metodo get:

- ⇒ “alias”= *insegna del negozio (valore fisso comunicato da CILME-MULTITEL nella fase di attivazione definitiva)*
- ⇒ “importo”= *importo da autorizzare*
- ⇒ “divisa”= *il codice della divisa in cui l'importo è espresso (EUR = Euro).*
- ⇒ “codTrans”= *codice di identificazione del pagamento composto da caratteri alfanumerici, **escluso il carattere #** (codice univoco per ogni richiesta di autorizzazione **min. 2 caratteri, max. 30 caratteri**)*

- ⇒ "mail" = l'indirizzo e-mail dell'acquirente al quale inviare l'esito del pagamento (facoltativo)
- ⇒ "url" = url del programma a cui inviare i parametri di risposta con il risultato della transazione (solo se le esigenze del merchant richiedono questo tipo di esito) (facoltativo)
- ⇒ "session\_id" = identificativo della sessione (facoltativo)
- ⇒ "mac" = Message Code Authentication (facoltativo)

Richiamando questo url viene eseguita in CILME-MULTITEL l'applicazione che genera la pagina di cassa personalizzata, secondo lo standard sottostante :



Si ricorda che dal 1 gennaio 2002, relativamente alle transazioni elettroniche, vengono accettate solo quelle con importi espressi in Euro.

Devono quindi essere adottati gli standard di rappresentazione degli importi, convenendo perciò che le ultime due cifre rappresentino la parte decimale dell'ammontare (senza inserire né virgola né punto decimale).

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

*per farsi autorizzare un pagamento di 50 Euro ci si deve riferire all'URL*

**https://pay4c.cilme.it/webapp/RELEASE1/DispatcherServlet?alias=valore&importo=5000&divisa=EUR&codTrans=990101-00001&mail=xxx@xxxx.it&url=http://www.xxxxx.it&session\_id=xxxxxxxx&mac=yyyy**

*per farsi autorizzare un pagamento di 50,12 Euro ci si deve riferire all'URL*

**https://pay4c.cilme.it/webapp/RELEASE1/DispatcherServlet?alias=valore&importo=5012&divisa=EUR&codTrans=990101-00001&mail=xxx@xxxx.it&url=http://www.xxxxx.it&session\_id=xxxxxxxx&mac=yyyy**

Dopo aver rimandato il compratore a tale URL, il *service provider* che gestisce il sito remoto si disinteressa di come avvenga il pagamento. Egli riceverà in modalità da concordare (mail, transazione *on line* su Internet) l'esito della richiesta. In caso di esito positivo il pagamento viene garantito dalle compagnie delle carte di credito, secondo le norme fissate nei documenti contrattuali.

#### 4. Utilizzo del MAC (Message Authentication Code)

Il MAC (Message Authentication Code), viene utilizzato per rendere non decifrabili i parametri passati tra i due siti interessati dal colloquio https, CILME-MULTITEL e il merchant.

Il MAC generato dall'algoritmo MD5 è in formato binario e per essere spedito tramite protocollo http viene codificato in Base64 e poi codificato secondo lo standard "x-www-form-urlencoded" (dalle specifiche del W3C).

Nel colloquio tra esercente e CILME-MULTITEL per l'invio dei dati dell'ordine, necessari per il pagamento, i campi che devono essere "maccati" sono nell'ordine codTrans , divisa, importo.

Per cui esemplificando, se

codTrans=testCILME534,

divisa=EUR,

importo=1

e la stringa segreta/ chiave = "esempiodicalcolomac";

allora il campo mac sarà

MAC=

metodo\_urlencoded(metodo\_base64(metodo\_MD5("codTrans=testCILME534divisa=EURimporto=1esempiodicalcolomac")))

e vale "ZjRkZDdkNWNmYThlZmYyNTJiN2U1ZmI2MDJINjM5NDI%3D"

Il parametro mac per essere inviato tramite il protocollo http necessita di un altro metodo\_urlencoded del valore ottenuto in precedenza e dunque, secondo l'esempio riportato sopra, il risultato sarà:

ZjRkZDdkNWNmYThlZmYyNTJiN2U1ZmI2MDJINjM5NDI%253D

Nel colloquio tra CILME-MULTITEL e esercente per la notifica dell'ordine, i campi vengono "maccati" nel seguente ordine: codTrans, esito, importo, divisa, data, orario, codAut.

## 5. Modalità di autorizzazione

Il consumatore interessato al pagamento, selezionando l'URL, si vedrà proporre (da un server CILME-MULTITEL) una pagina in cui inserire i propri dati (PAN della carta oppure prossimamente l'attivazione del wallet nel caso SET-3D) da utilizzare per il pagamento. Questi dati vengono trasmessi direttamente a CILME-MULTITEL, sotto protezione SSL o SET (non transitano dal *service provider*).

La richiesta di autorizzazione (non SET) viene compiuta da CILME-MULTITEL sugli stessi canali utilizzati per i pagamenti POS.

I pagamenti non autorizzati verranno trattati secondo modalità indicate dal *service provider* (risposta negativa al consumatore, risposta di cortesia che consenta un successivo contatto da parte del venditore...).

## 6. Adattamenti al Sito

Al fine di rafforzare la sicurezza del servizio il web server di CILME-MULTITEL accetta solo connessioni da browser con livello di codifica pari a 128 bit. Si consiglia pertanto di avvisare gli acquirenti (tramite ad esempio una nota sulla home page del negozio virtuale) di aggiornare la versione del proprio browser affinché sia in grado di gestire connessioni SSL 128bit.

Per quanto riguarda il browser Internet Explorer è possibile eseguire l'aggiornamento collegandosi all'url <http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp>; invece per Netscape l'url di riferimento è il seguente : <http://home.netscape.com/download>.

Per quanto riguarda invece l'attivazione del pos virtuale, il *service provider* deve comunicare a CILME-MULTITEL :

1.

l' **IP address** da cui provengono le richieste di autorizzazione (cioè l'IP address del *service provider*) e il "nome" relativo all'IP address, per evitare che terzi estranei usino il canale per verifiche su carte di credito,

2.

la modalità ed eventualmente il formato di **restituzione degli esiti** dei pagamenti (e-mail, transazioni *on line* su Internet, comunicazione server to server)

### Risposta via e-mail

Il merchant riceverà una mail con il riferimento dell'insegna del suo negozio e i parametri importo, divisa, codice transazione, esito del pagamento (positivo o negativo), data della transazione, ora della transazione e codice di autorizzazione (quest'ultimo solo se il pagamento ha avuto esito positivo).

Il merchant deve comunicare a CILME-MULTITEL l'indirizzo e-mail a cui inviare gli esiti dei pagamenti.

### Transazioni on line su Internet

Con questa modalità, l'esito della richiesta di pagamento, viene comunicato da CILME-MULTITEL al merchant tramite e-mail e reindirizzando l'acquirente ad un URL, a cui sono accodati, nell'ordine, una serie di parametri:

<b>Nome campo</b>	<b>Descrizione</b>	<b>Formato</b>	<b>Valori</b>
importo	Importo		
data	Data della transazione	yyyymmdd	
divisa	Divisa	3 caratteri	EUR
codTrans	Codice transazione	Da 2 a 30 caratteri	
orario	Ora della transazione	hhmmss	
esito	Esito della transazione	2 caratteri	OK o KO
codAut	Codice dell'autorizzazione assegnato	Da 2 a 6 caratteri	

Tale Url viene definito dal merchant e può essere sempre lo stesso per ogni transazione oppure, in alternativa, comunicato dinamicamente, tramite il parametro url, al momento della chiamata della pagina di pagamento (vedere modalità descritte nell'esempio riportato al paragrafo "modalità operative").

### Comunicazione server to server

Questa modalità permette al server di CILME – MULTITEL di dialogare e scambiare dati direttamente con il server del merchant.

I parametri che vengono inviati al server del merchant sono nell'ordine:

<b>Nome campo</b>	<b>Descrizione</b>	<b>Formato</b>	<b>Valori</b>
codTrans	Codice transazione	Da 2 a 30 caratteri	
importo	Importo		
divisa	Divisa	3 caratteri	EUR
codAut	Codice dell'autorizzazione assegnato	Da 2 a 6 caratteri	
data	Data della transazione	yyyymmdd	
orario	Ora della transazione	hhmmss	
esito	Esito della transazione	2 caratteri	OK o KO

3.  
chi, CILME-MULTITEL o il *service provider*, mostra al consumatore le **condizioni di vendita** imposte dalla legge italiana (diritto di recesso, privacy...).

Inoltre, per l'attivazione del pos virtuale, il merchant deve :

4.  
inviare a CILME-MULTITEL ([quimercato@cilmemultitel.it](mailto:quimercato@cilmemultitel.it)) n. 1 **logo** relativo al **negozio virtuale** di dimensioni h 50 x L 70 pixel e n. 1 logo di dimensioni a scelta.

5.  
Nel caso venga scelto di adottare l'autenticazione dei messaggi, quindi l'utilizzo di un **MAC**, deve essere scambiata, tra CILME-MULTITEL e l'esercente, la **chiave** da utilizzare per l'algoritmo.