Cim Italia spa
Centrale Interbancaria Monetica

COMMERCIO ELETTRONICO

Autorizzazione di Pagamenti su Siti Remoti

Versione 3.1

Cim Italia spa
Centrale Interbancaria Monetica

INDICE

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, Maestro 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 permettono (ad oggi Servizi Interbancari e Bankamericard) i pagamenti possono essere effettuati secondo l'architettura e gli standards **VerifiedByVISA** e **SecureCode**. Sul circuito VISA EU e MASTERCARD EU infatti, aderendo a questi standards, la responsabilità della transazione, quindi il rischio della stessa, si sposta dall'acquirer (i.e. dal merchant) all'issuer (i.e. alla compagnia) (per i dettagli cfr Appendice A)

Nel ruolo di FEP (Front-End Processor) Esercente, Cim Italia è altresì in grado di gestire i pagamenti secondo le specifiche **BankPass Web** consentendo quindi al consumatore di effettuare acquisti utilizzando anche lo strumento PagoBancomat

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 Cim Italia, il quale propone al consumatore una pagina in cui viene mostrata l'insegna del negozio, l'importo della transazione e l'identificativo della transazione, invitandolo, se intenzionato a procedere al pagamento, ad indicare i propri dati.

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

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

L'esito della richiesta viene comunicato al merchant e opzionalmente anche al consumer secondo modalità e formato concordate (posta elettronica e/o transazione on-line su internet e/o comunicazione server to server, mediante protocollo http/https).
Nello scambio di informazioni tra Cim Italia e merchant, indipendentemente dalla modalità utilizzata, è obbligatorio 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 obbligatoria in quanto consente di verificare, sia a Cim Italia 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 dell'accredito dei movimenti oppure stornare la transazione di pagamento qualora intervenissero ad esempio problemi logistici.

Per facilitare la gestione degli ordini Cim Italia 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, Cim Italia 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://ecommerce.cim-italia.it/ecomm/DispatcherServlet

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

alias = *insegna del negozio (valore fisso comunicato da Cim Italia nella fase di attivazione definitiva)*

importo = *importo da autorizzare (obbligatorio)*

divisa = *il codice della divisa in cui l'importo è espresso (EUR = Euro). (obbligatorio)*

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****) (obbligatorio)*

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)*

url_back = *in questa variabile è possibile indicare un indirizzo che verrà richiamato alla pressione del tasto "annulla" presente sulla pagina di cassa a cui verranno accodati i seguenti parametri:*

Variabile	**Valorizzazione**
importo	*importo da autorizzare*
divisa	EUR
codTrans	*codice identificativo del pagamento assegnato dal gestore del negozio*
esito	ANNULLO

Se tale parametro non viene valorizzato, alla pressione del tasto "annulla", non verrà effettuata nessuna operazione. (facoltativo)

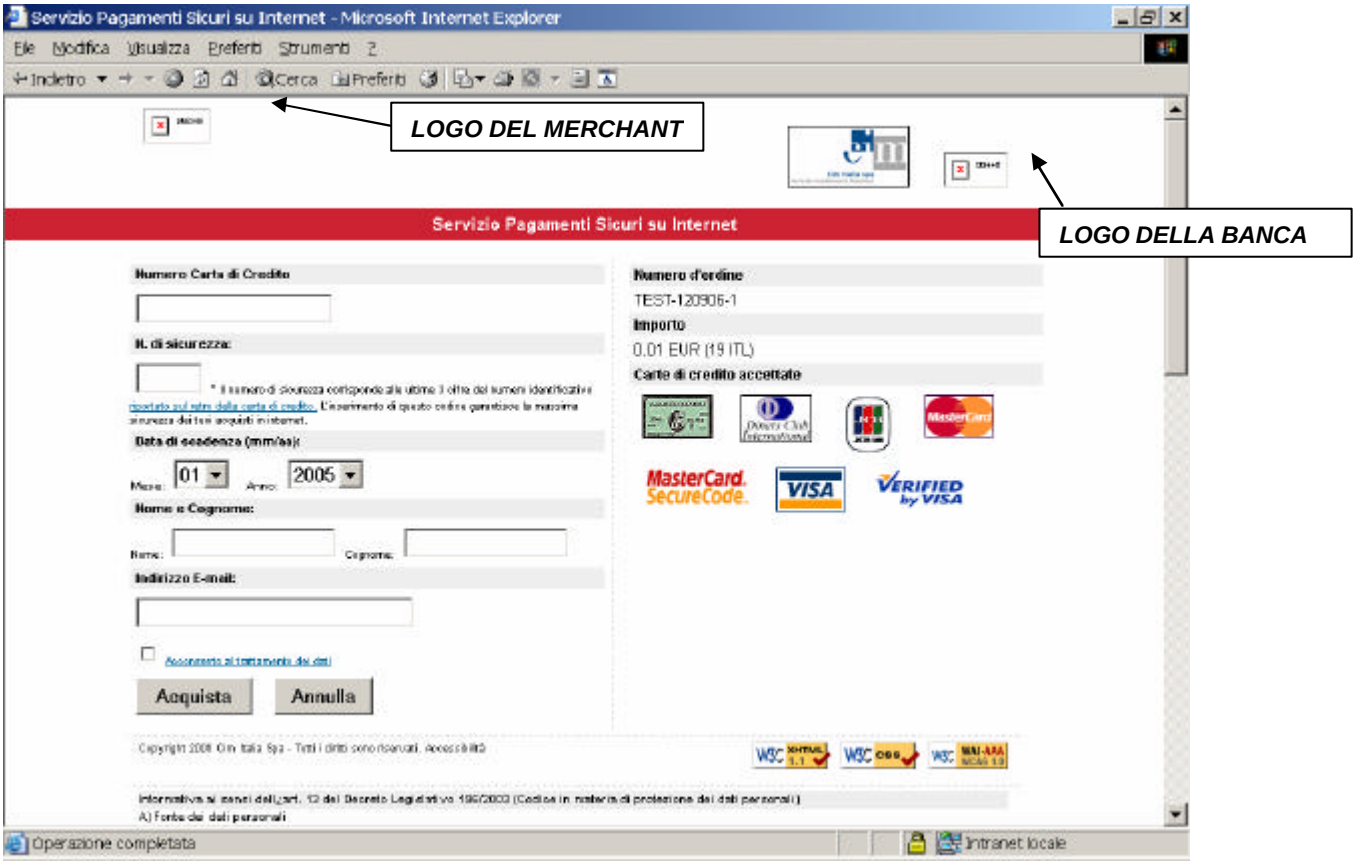
languageId = *identificativo della lingua che verrà visualizzata sulla pagina di cassa; le diverse lingue disponibili sono:*

languageId	descrizione
ITA	Italiano
ENG	Inglese
SPA	Spagnolo
FRA	Francese
GER	Tedesco
JPN	Giapponese
ITA-ENG	Italiano/Inglese

Se tale campo non viene specificato o viene lasciato vuoto verranno visualizzati i testi in italiano/inglese

mac = *Message Code Authentication (obbligatorio)*

Richiamando questo url viene eseguita in Cim Italia l'applicazione che genera la pagina di cassa secondo lo standard sottostante :



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://ecommerce.cim-italia.it/ecomm/DispatcherServlet?alias=valore**&importo**=5000
&divisa=EUR**&codTrans**=990101-00001**&mail=**xxx@xxxx.it**&url=**http://www.xxxxx.it
&session_id=xxxxxxxx**&mac=**yyyy**&languageId**=ITA

per farsi autorizzare un pagamento di 50,12 Euro ci si deve riferire all'URL
https://ecommerce.cim-italia.it/ecomm/DispatcherServlet?alias=valore**&importo**=5012
&divisa=EUR**&codTrans=**990101-00001**&mail=**xxx@xxxx.it**&url=**http://www.xxxxx.it
&session_id=xxxxxxxx**&mac=**yyyy**&languageId**=ENG

Dopo aver rimandato il compratore a tale URL, il *service provider* che gestisce il sito remoto si disinteressa di come avviene il pagamento. Egli riceverà in modalità da concordare (mail, transazione *on* line su Internet e/o comunicazione server to server) 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. Notifica dell'esito

Di seguito vengono riportate le diverse modalità di restituzione dell'esito del pagamento.

4.1. Esito tramite e-mail

Il merchant riceverà una mail con il riferimento dell'insegna del suo negozio e i parametri importo, divisa, codice transazione, nome, cognome e indirizzo e-mail di chi ha effettuato il pagamento, tipo di carta utilizzato, 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 Cim Italia l'indirizzo e-mail a cui inviare gli esiti dei pagamenti.

4.2. Transazioni on line su Internet

Con questa modalità, l'esito della richiesta di pagamento, viene comunicato da Cim Italia al merchant tramite e-mail e reindirizzando l'acquirente ad un URL, al quale vengono inviati, in modalità GET, una serie di parametri:

Nome campo	**Descrizione**	**Formato**	**Valori**
importo	Importo	5000 (50 euro)	
data	Data della transazione	yyyymmdd	
divisa	Divisa	3 caratteri	EUR
session_id	identificativo della sessione		
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	
$BRAND	tipo di carta utilizzato	Da 3 a 10 caratteri	VISA, MasterCard, Amex, Diners, Jcb
nome	nome di chi ha effettuato il pagamento	Da 1 a 30 caratteri	
cognome	cognome di chi ha effettuato il pagamento	Da 1 a 30 caratteri	
email	indirizzo e-mail di chi ha effettuato il pagamento	Da 1 a 150 caratteri	
mac	Message Code Authentication		

Tale Url viene definito dal merchant e comunicato dinamicamente, tramite il parametro url, al momento della chiamata della pagina di pagamento (vedere l'esempio riportato al paragrafo "modalità operative").

4.3. Comunicazione server to server

Questa modalità permette al server di Cim Italia di dialogare e scambiare dati in modalità POST direttamente con il server del merchant.
I parametri che vengono inviati al server del merchant sono:

Nome campo	**Descrizione**	**Formato**	**Valori**
importo	Importo	5000 (50 euro)	
data	Data della transazione	yyyymmdd	
divisa	Divisa	3 caratteri	EUR
session_id	identificativo della sessione		
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	
$BRAND	tipo di carta utilizzato	Da 3 a 10 caratteri	VISA, MasterCard, Amex, Diners, Jcb
nome	nome di chi ha effettuato il pagamento	Da 1 a 30 caratteri	
cognome	cognome di chi ha effettuato il pagamento	Da 1 a 30 caratteri	
email	indirizzo e-mail di chi ha effettuato il pagamento	Da 1 a 150 caratteri	
mac	Message Code Authentication		

4.4. Invio di un file XML o TXT

Questo tipo di notifica prevede che venga inviato ad uno o più indirizzi di posta elettronica un file in formato XML o TXT contenente tutte le transazioni di pagamento (contabilizzazioni e storni) effettuate sino alla mezzanotte della giornata precedente all'invio. L'indirizzo e-mail viene comunicato a Cim Italia in fase di attivazione.

5. Utilizzo del MAC (Message Authentication Code)

Il MAC (Message Authentication Code), viene utilizzato per rendere non modificabili i parametri passati tra i due siti interessati dal colloquio https, Cim Italia 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 Cim Italia per l'invio dei dati dell'ordine, necessari per il pagamento, i campi che devono essere "maccati" sono nell'ordine codTrans , divisa, importo e stringa segreta.

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 "ZjRkZDdkNWNmYThlZmYyNTJiN2U1ZmI2MDJlNjM5NDI%3D"

Il parametro mac per essere inviato in modalità GET 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:
ZjRkZDdkNWNmYThlZmYyNTJiN2U1ZmI2MDJlNjM5NDI%253D

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

6. Attivazione Pos Virtuale

Al fine di rafforzare la sicurezza del servizio il web server di Cim Italia 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://www.netscape.com .

Per quanto riguarda invece l'attivazione del pos virtuale, il *service provider* deve :

1. comunicare a Cim Italia 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 utilizzino il canale per verifiche su carte di credito,

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

3. inviare a Cim Italia (ecommerce@cim-italia.it) n. 1 **logo** relativo al **negozio virtuale** di dimensioni h 50 x L 70 pixel e n. 1 logo di dimensioni a scelta,

4. ricevere da Cim Italia la **chiave** da utilizzare per implementare l'algoritmo di calcolo del MAC.

Appendice A – Funzionamento del servizio 3D Secure

L'esercente che aderisce a 3D Secure viene **esonerato da qualsiasi responsabilità** sulla base delle regole stabilite dai circuiti internazionali**:** infatti, nel caso in cui il titolare della carta di credito dovesse contestare una spesa, la responsabilità della transazione passa dall'acquirer alla società che ha emesso la carta di credito: un processo denominato **liability shift.**

La liability shift viene applicata secondo le regole Visa e MasterCard riassunte di seguito.

Per Visa la liability shift viene applicata nei seguenti due casi:

1) l'esercente, la società che ha emesso la carta, il titolare della carta di credito, **aderiscono tutti a 3D Secure (VBV)**;
2) l'esercente aderisce a VBV, ma la società che ha emesso la carta o il titolare non aderiscono a VBV.
   Esistono alcune **eccezioni**, a questo secondo caso, per le quali la liability shift non viene applicata. Questo può succedere per:
   A) i pagamenti effettuati sui nuovi canali (es. mobile)
   B) le carte aziendali extraeuropee durante le transazioni internazionali
   C) le carte anonime prepagate

Per MasterCard la liability shift viene sempre applicata purchè l'esercente aderisca a 3D Secure (MasterCard Secure Code).

Esiste una **sola eccezione,** che riguarda le carte emesse in USA, Canada, Messico, Centro America, Caraibi e Sud America.
Per le carte emesse in questi Paesi, affinché la liability shift sia valida, sono necessarie contemporaneamente le tre seguenti condizioni:

A) l'esercente aderisce a MasterCard Secure Code
B) la società che ha emesso la carta aderisce a MasterCard Secure Code
C) il titolare della carta di credito si è autenticato correttamente.

Sia per le carte Visa, sia per le carte MasterCard, una volta completata la fase d'autenticazione tramite password, la transazione prosegue nel **normale processo autorizzativo**.

Glossario

Acquirer
Società che fornisce all'esercente il servizio per l'accettazione dei pagamenti con carta di credito