All. F4

POS VIRTUALE INTERNET

SETEFI S.p.A

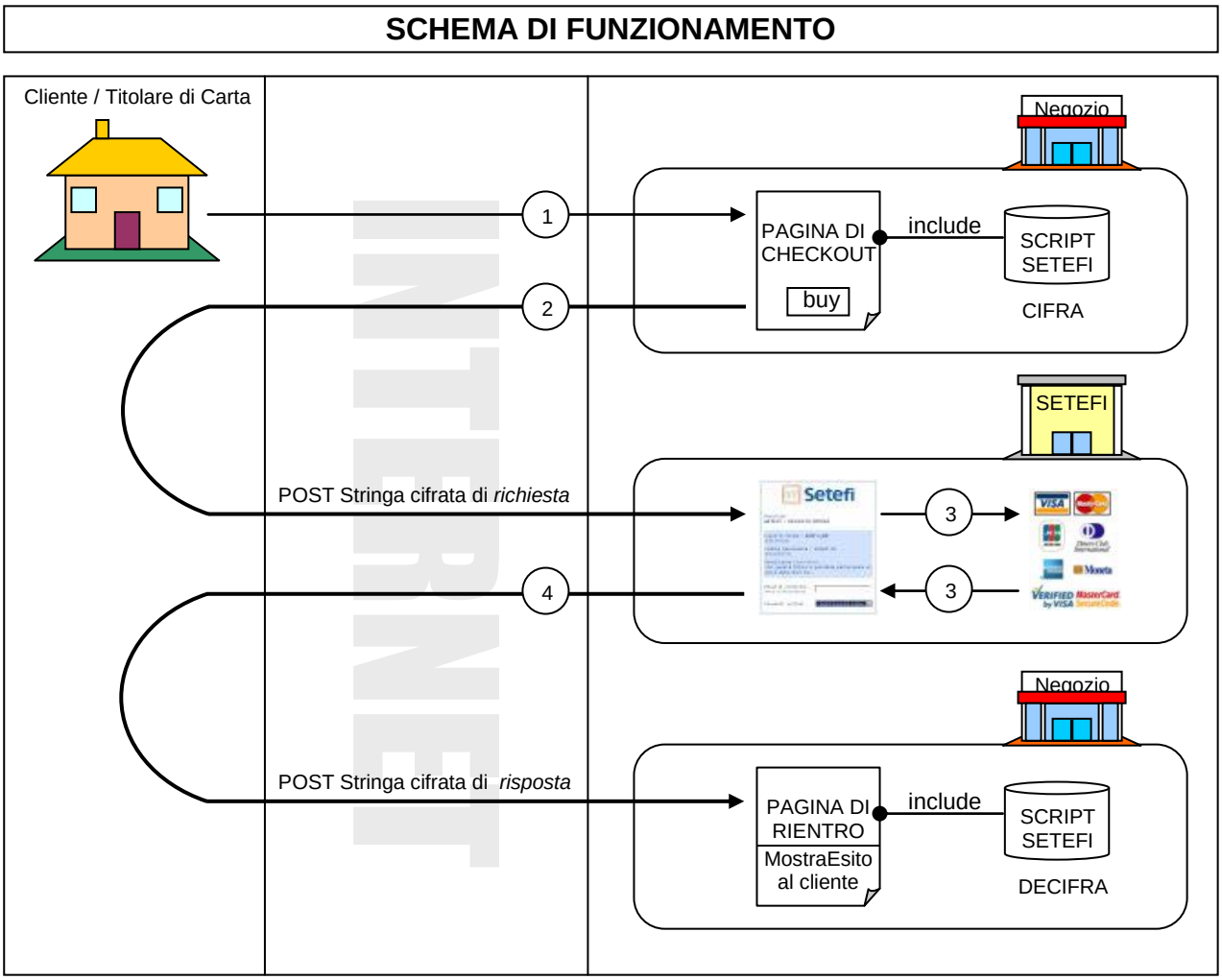
Indice

1. Soluzione proposta

Il principale obiettivo di questo progetto è fornire ai negozi virtuali presenti su Internet la possibilità di accettare pagamenti effettuati con carte di credito, lasciando a Setefi la fase di gestione e acquisizione del codice di carta di credito del cliente finale nonché del processo autorizzativo; in tal modo al commerciante Internet è garantita la gestione ottimale dei pagamenti con carte appartenenti ai circuiti più diffusi presenti in Italia.

1.1 Fase di autorizzazione

Per aderire al sistema sicuro progettato da Setefi S.p.A., il sito del commerciante deve predisporre due pagine web atte allo scambio di messaggi con il server Setefi; nella fattispecie una sarà utilizzata per preparare una stringa "cifrata" contenente i dati della transazione in corso, l'altra per decifrare il messaggio di risposta prodotto da Setefi.
Setefi fornisce al commerciante un file contenente le funzioni di cifratura e decifratura (utilizzate per lo scambio dei messaggi), che sarà utilizzato come script "lato server" nelle predette pagine.



1.2 Funzioni di cifratura e decifratura

Le funzioni di cifratura/decifratura fornite da Setefi sono attualmente disponibili per ambienti in grado di supportare le seguenti tecnologie:
- ASP
- PHP
- JAVA

Lo scambio dei messaggi tra il titolare di carta di credito e il pos virtuale Setefi avviene in maniera sicura grazie al protocollo SSL.

1.2.1 La funzione Rij_Client_CifraNew

Viene utilizzata per creare e criptare la stringa contenente i dati della transazione.
E' necessario fornire come parametri della funzione tutti i campi presenti nel tracciato record di pagina 5. La funzione restituisce in risposta una stringa cifrata, che dovrà essere inviata tramite post http al server Setefi (Esempio a pagina 7).

1.2.2 La funzione Rij_Client_DecifraNew

Viene utilizzata per ottenere la decifratura del messaggio di risposta prodotto da Setefi.
E' necessario fornire come parametro della funzione, il campo ricevuto dal post http inviato da Setefi tramite il browser (Esempio a pagina 8).

1.3 Gestione della URL di risposta

Per URL di "risposta" si intende l'indirizzo Internet abilitato dal commerciante alla ricezione del messaggio di esito elaborato da Setefi.

La URL può essere comunicata a Setefi oppure gestita dinamicamente per ogni richiesta di pagamento.

La gestione dinamica prevede l'inserimento di un campo "hidden" nella form contenente la stringa cifrata da inviare a Setefi. Il nome da assegnare al predetto campo deve essere "RETURL" e il suo contenuto deve corrispondere alla URL dalla quale il commerciante desidera interpretare il messaggio di risposta Setefi.

Es:

```
<FORM ACTION="https://www.monetaonline.it/MPI/MPIRequest.asp" METHOD="POST">
   <INPUT TYPE="HIDDEN" NAME="PaymentRequest" VALUE="<? echo $strCifrata; ?>">
   <INPUT TYPE="HIDDEN" NAME="RETURL" VALUE="<? echo $retURL; ?>">
   <INPUT TYPE="SUBMIT" VALUE="BUY NOW">
</FORM>
```

1.4 Campi per la chiamata della funzione Rij_Client_CifraNew

Contiene i dati della transazione in corso, tutti i campi del tracciato devono essere passati come parametro della funzione Rij_Client_CifraNew(..).

CAMPO	LUNGHEZZA MAX	VALORE DA IMPOSTARE	DESCRIZIONE	ESEMPIO
purchase_amount	12		Importo comprende anche i due decimali senza segni di punteggiatura	19,80 * 100 = 1980
Filler	1	"2"	Fisso a 2	
Filler	3	"978"	Fisso a 978	
rifOperazione	18		Riferimento operazione commerciante. **Deve essere univoco in assoluto**. E' anche, di norma, riportato nell'estratto conto del cliente	E' il riferimento dell'operazione noto anche al cliente finale. Esempio: numero fattura, codice operazione Internet, etc.
DataOperazione	6		Data operazione AAMMGG	030423 = 23 Aprile 2003
OraOperazione	6		Ora operazione HHMMSS	183000 = 18:30.00
NumOperazione	4		Numero progressivo operazione, gestito dal commerciante. Deve essere univoco nella giornata.	
Descrizione	64		Descrizione merce/servizio	Tenda igloo
Filler	19	""	Filler	
Filler	4	""	Filler	
Filler	2	""	Filler	
Filler	8	""	Filler	
Filler	2	""	Filler	
Filler	1	""	Filler	
Filler	3	""	Filler	
Filler	32	""	Filler	
Filler	28	""	Filler	
CodNazione	3	"380"	Fisso a 380	
Filler	15	""		
Filler	1	""		
Filler	3	""		
Filler	58	""		

1.5 Tracciato record messaggio di risposta da Setefi

Contiene la risposta di Setefi verso il commerciante.

CAMPO	POSIZIONE	LUNGHEZZA	DESCRIZIONE
statoTrans	1	3	Se = 000 allora la transazione è andata a buon fine
Data	4	8	Formato AAAAMMGG
Ora	12	6	Formato HHMMSS
Filler	18	6	
Cod. Autoriz.	24	6	Se autorizzata è valorizzato
Descrizione esito	30	29	Descrive lo stato dell'esito eventualmente da presentare al cliente
Rif. Setefi	59	12	Codice di riferimento attribuito da Setefi alla transazione.
Filler	71	4	
Tipo pagamento	75	1	Modalità: 1 = Half Secure (Mastercard) 2 = Full Secure (Mastercard) 5 = Full Secure (Visa) 6 = Half Secure (Visa) 7 = Not Secure (Visa, Mastercard)
Filler	76	8	
Purchase_amount	84	12	Importo – uguale a quello impostato in fase di richiesta dal commerciante
Filler	96	4	
RifOperazione	100	18	Riferimento operazione – uguale a quello impostato in fase di richiesta dal commerciante
DataOperazione	118	6	Data operazione AAMMGG – uguale a quella impostata in fase di richiesta dal commerciante
OraOperazione	124	6	Ora operazione HHMMSS – uguale a quella impostata in fase di richiesta dal commerciante
NumOperazione	130	4	Numero progressivo operazione – uguale a quello impostato in fase di richiesta dal commerciante
Descrizione	134	64	Descrizione merce/servizio – uguale a quella impostata in fase di richiesta dal commerciante
Filler	198	179	
Messaggio	377	80	Messaggio di risposta eventualmente da presentare al cliente

1.6 Codice di esempio (Rij_Client_CifraNew)

CHIAMATA ALLA FUNZIONE "JAVASCRIPT" Rij_Client_CifraNew INCLUSA NEL FILE STFTEST.php , in una pagina PHP

```
function
Rij_Client_CifraNew($purchase_amount,$nDecimali,$codDivisa,$rifOperazione,$DataOperazione,$OraOperazione,$NumOperazione,$
Descrizione,$PAN,$Expiry,$Recur_frequency,$endRecur,$Installments,$Device_category,$CVV2,$IntCarta,$UCAF,$codNazione,$CaD
ivCH,$NDecCH,$CodDivCH,$Fillo)
{
	$lenSingleKey=64;
	$DaCifrare="";

	$KeyFileName = AssegnaTID();
	//$KeyFileName = "/";
	//$KeyFileName.=AssegnaTID();
	$KeyFileName.=".key";

	$DaCifrare.=FormattaStringa(AssegnaTID(), 8);
	$DaCifrare.= FormattaNumero($purchase_amount, 12);
	$DaCifrare.= FormattaNumero($nDecimali, 1);
	$DaCifrare.= FormattaNumero($codDivisa, 3);
	$DaCifrare.= FormattaStringa($rifOperazione, 18);
	$DaCifrare.= FormattaNumero($DataOperazione, 6);
	$DaCifrare.= FormattaNumero($OraOperazione, 6);
	$DaCifrare.= FormattaNumero($NumOperazione, 4);
	$DaCifrare.= FormattaStringa($Descrizione, 64);
	$DaCifrare.= FormattaStringa($PAN, 19);
	$DaCifrare.= FormattaNumero($Expiry, 4);
	$DaCifrare.= FormattaNumero($Recur_frequency, 2);
	$DaCifrare.= FormattaNumero($endRecur, 8);
	$DaCifrare.= FormattaNumero($Installments, 2);
	$DaCifrare.= FormattaNumero($Device_category, 1);
	$DaCifrare.= FormattaStringa($CVV2, 3);
	$DaCifrare.= FormattaStringa($IntCarta, 32);
	$DaCifrare.= FormattaStringa($UCAF, 28);
	$DaCifrare.= FormattaNumero($codNazione, 3);
	$DaCifrare.= FormattaNumero($CaDivCH, 15);
	$DaCifrare.= FormattaNumero($NDecCH, 1);
	$DaCifrare.= FormattaNumero($CodDivCH, 3);
	$DaCifrare.= FormattaStringa($Fillo, 58);

	$SetefiBuffer = AssegnaBuffer();
	$numChiavi=(StrLen($SetefiBuffer))/$lenSingleKey;
	mt_srand((double)microtime()*1000000);
	$KeyId = mt_rand(1,$numChiavi);

	$posKey=($KeyId-1)*$lenSingleKey;
	$KeyValue=substr($SetefiBuffer,$posKey,$lenSingleKey);
	$InText = $DaCifrare;

	// Da Ottone
	$ctlen=StrLen($InText);
	$bindata='';
	for ($i=0;$i<StrLen($KeyValue);$i+=2)
	{
	   $bindata.=chr(hexdec(substr($KeyValue,$i,2)));
	}

	//echo $InText . "<BR>";

	$cAES = new CAES;
	$sCipherText = $cAES->Encrypt($bindata, $InText);

	$outHexOk = Bin2Hex($sCipherText);//i primi 4 caratteri(8 in hex)
	//echo $outHexOk ."<BR>";
	$outHexOk=substr($outHexOk,8,StrLen($outHexOk)-8);

	$KeyIdTx = FormattaNumero($KeyId,4);
	$ctlenTx = FormattaNumero($ctlen,4);
	$fileNameStrip = FormattaStringa($KeyFileName,12);

	$outHexOk.=$ctlenTx;
	$outHexOk.=$fileNameStrip;
	$outHexOk.=$KeyIdTx;

	return $outHexOk;
}
```

1.7 Codice di esempio (Rij_Client_DecifraNew)

CHIAMATA ALLA FUNZIONE "JAVASCRIPT" Rij_Client_DecifraNew INCLUSA NEL FILE STFTEST.php, in una pagina PHP

```
function Rij_Client_DecifraNew($CifText)
{

	$lenSingleKey = 64;

	$cf = $CifText;
	$KeyId = substr($cf,StrLen($cf)-4,4);
	settype($KeyId, "integer");
	//KeyIdNum = parseInt(KeyId,10);
	$cf=substr($cf,0,StrLen($cf)-16);
	$LenStr = substr($cf,StrLen($cf)-4,4);
	$cf=substr($cf,0,StrLen($cf)-4);

	//echo 'Stringa Cifrata: <br>'.$cf.'<br>';

	$SetefiBuffer = AssegnaBuffer();
	$posKey = ($KeyId-1)*$lenSingleKey;
	$KeyValue = substr($SetefiBuffer,$posKey,$lenSingleKey);

	$bindata='';
	for ($i=0;$i<StrLen($KeyValue);$i+=2)
	{
	   $bindata.=chr(hexdec(substr($KeyValue,$i,2)));
	}

	$binTesto='';
	for ($u=0;$u<StrLen($cf);$u+=2)
	{
	   $binTesto.=chr(hexdec(substr($cf,$u,2)));
	}

	//SC 20040408 - Concateno il testo con la lunghezza in chiaro.
	$binTesto = $binTesto.$LenStr;

	$cAES = new CAES;

	$sMessage = $cAES->Decrypt($bindata, $binTesto);

	return $sMessage;
}
```

2 Contabilizzazione

Il commerciante può in funzione delle proprie esigenze, avvalersi di uno dei tre differenti metodi di contabilizzazione delle transazioni autorizzate.

I primi due metodi utilizzano le funzioni di contabilizzazione presenti sul sito www.monetaonline.it e sono:

- Il primo metodo, implicito, prevede la contabilizzazione automatica a fine giornata di tutte le richieste autorizzate nella stessa giornata e non cancellate dal commerciante tramite l'apposita funzione presente sul sito www.monetaonline.it.

- Il secondo metodo, esplicito, richiede che il commerciante effettui personalmente la contabilizzazione delle operazioni autorizzate tramite l'apposita funzione presente sul sito www.monetaonline.it. Il commerciante può confermare operazioni autorizzate anche nelle precedenti giornate, purché non anteriori a 20 giorni di calendario.

Il terzo metodo, esplicito a mezzo archivio elettronico, richiede la creazione di tale archivio a cura del commerciante. L'archivio deve contenere tutte e sole le operazioni autorizzate che si intendono contabilizzare, e può essere successivamente inviato a SETEFI tramite modalità da concordare.