

# SETEFI

Marco Cantarini, Daniele Maccauro, Domenico Marzolla

19 Aprile 2012

# Introduzione

Il nostro obiettivo é quello di illustrare la struttura e le caratteristiche di fondo che stanno alla base delle transazioni online operate tramite Setefi, società del gruppo Intesa Sanpaolo che gestisce i pagamenti con moneta elettronica. Cominceremo con lo spiegare il protocollo SSL, utilizzato per scambiare messaggi in sicurezza, per poi passare a mostrare come effettivamente opera SETEFI. Nell'ultima parte del seminario parleremo di un esempio di applicazione che permette le operazioni di cifratura e decifratura delle varie informazioni riservate che Setefi scambia con i propri negozianti online.

# SSL - Secure Sockets Layer

SSL é un protocollo aperto e non proprietario introdotto da Netscape Communication nel Dicembre 1994, e si é imposto come standard de facto negli anni successivi. La versione 3.0 sviluppata nel 1996, evoluzione della 2.0 del 1994, é stata sottoposta all'IETF (Internet Engineering Task Force) per la standardizzazione. Il futuro di SSL é rappresentato dal protocollo TLSv1 (da molti considerato SSL 3.1) standardizzato nel 1998.

# Funzionalità

- **Autenticazione:** SSL garantisce l'autenticazione di due host tramite lo scambio di certificati di identità (opzionale).
- **Privatezza del collegamento:** i dati scambiati sul canale di comunicazione sono protetti utilizzando algoritmi di crittografia a chiave simmetrica. SSL mette a disposizione diversi livelli di sicurezza.
- **Integrità delle informazioni:** i dati vengono autenticati mediante un campo Message Authentication Code (MAC).

# Stati

Uno stato é una struttura dati che raccoglie tutti gli elementi che identificano una comunicazione. SSL identifica due tipi di stati:

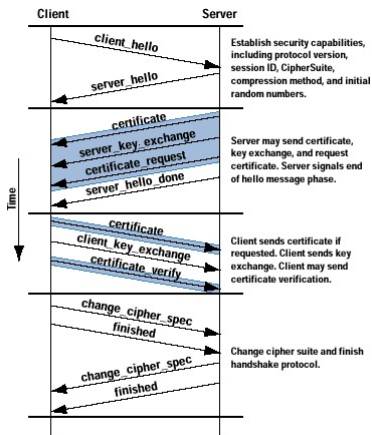
- **Sessione:** é un'associazione tra un client e un server. La sessione é creata tramite il protocollo di Handshake e definisce una serie di parametri di sicurezza, che possono essere condivisi tra piu' connessioni. Serve per evitare costose negoziazioni di nuovi parametri di sicurezza per ogni connessione.
- **Connessione:** Questo stato memorizza tutte le chiavi utilizzate nei processi crittografici. Ad ogni nuova connessione i campi vengono ricalcolati per produrre nuove e differenti sequenze. Ogni connessione é associata ad una sessione.

# Protocollo

Il protocollo SSL é stato progettato come somma di due protocolli distinti che assolvono a due precisi compiti:

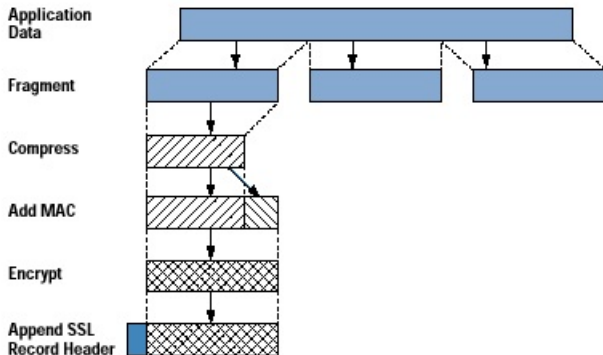
- **Handshake protocol:** La funzione principale del livello di handshake é quella di inizializzare tutti i parametri di comunicazione secondo il protocollo SSL. Ha il compito di selezionare la versione del protocollo, gli algoritmi di crittografia e di creare le chiavi di cifratura, in piú deve gestire la procedura di autenticazione.
- **Record protocol:** Il record protocol si occupa di cifrare, decifrare e verificare l'integritá dei messaggi.

# Handshake protocol



Note: Shaded transfers are optional or situation-dependent messages that are not always sent

## Record protocol



# Debolezze

- **Flessibilità:** attacchi di tipo drop change cipher spec message, sono legati alla facilitá nell'espugnare con forza bruta lo standard di cifratura RC4.
- **Compatibilitá:** attacchi di tipo version rollback.
- **Record protocol:** attacchi di tipo Denial of Service: quando si riceve un codice di autenticazione del messaggio (MAC) errato il livello Record di SSL termina la connessione.

## Debolezze

- **Flessibilità:** attacchi di tipo drop change cipher spec message, sono legati alla facilitá nell'espugnare con forza bruta lo standard di cifratura RC4.
- **Compatibilitá:** attacchi di tipo version rollback.
- **Record protocol:** attacchi di tipo Denial of Service: quando si riceve un codice di autenticazione del messaggio (MAC) errato il livello Record di SSL termina la connessione.

## Debolezze

- **Flessibilità:** attacchi di tipo drop change cipher spec message, sono legati alla facilità nell'espugnare con forza bruta lo standard di cifratura RC4.
- **Compatibilità:** attacchi di tipo version rollback.
- **Record protocol:** attacchi di tipo Denial of Service: quando si riceve un codice di autenticazione del messaggio (MAC) errato il livello Record di SSL termina la connessione.

# SETEFI

SETEFI leader del settore italiano dell'acquirer  
Si propone come unico interlocutore nei processi di incasso tramite  
POS  
Gestisce direttamente 10 milioni di card.

Organizzazione → lavora in maniera autonoma dalle banche

Normative:

- Esecuzione di ordini di pagamento, anche trasferimento di fondi, su un conto presso un prestatore di servizi di un utilizzatore.
- Esecuzione di transazioni monetarie legate ad una certa linea di pagamento accordata all'utilizzatore di servizi.
- Emissione e acquisizione di strumenti di pagamento.

## Servizi

- Garantire agli esercenti convenzionati gli importi relativi alle vendite mediante accettazione delle carte di credito.
- Ricevere le somme che spettano agli operatori commerciali a fronte dell'accettazione delle carte di credito.
- Curare il successivo trasferimento sul conto corrente bancario indicato dall'operatore commerciale.

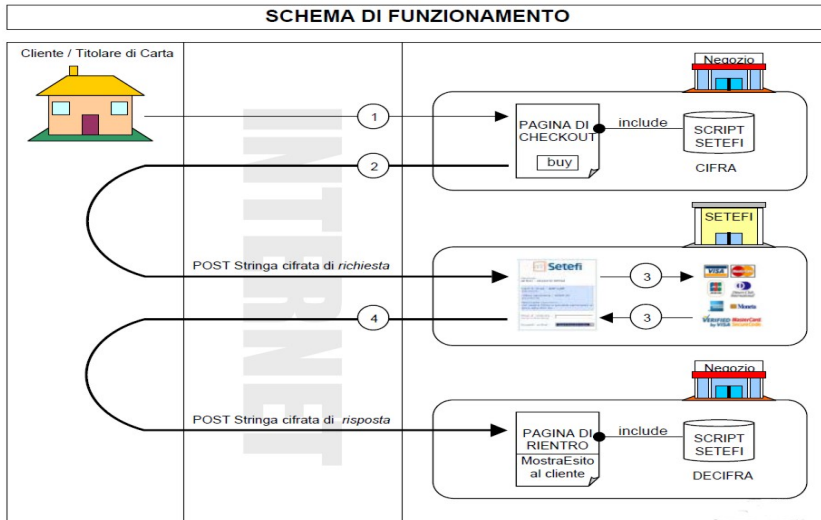
L'operatore paga una commissione del rischio assunto per eventuali insolvenze.

Gestione carte di pagamento → SETEFI gestisce 10 milioni di carte assicurando:

- Acquisto di plastiche vergini adeguate alle norme previste dai circuiti di pagamento.
- La personalizzazione delle plastiche mediante caricamento dati su microchip e banda magnetica.
- L'invio delle carte di pagamento alle filiali del Gruppo Intesa Sanpaolo o al domicilio del Titolare.
- Autorizzazione dei pagamenti.
- Il regolamento contabile delle transazioni.

Obiettivo principale: garantire ai negozi online la possibilità di accettare il pagamento attraverso 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.

## Come funzionano le transazioni



Virtualcard moneta online: servizio utilizzabile solo dai clienti del gruppo Intesa Sanpaolo che hanno una carta di pagamento "fisica". Consiste nella creazione di una card virtuale. Due tipologie possibili:

- Per singola operazione.
- A tempo.

## Come si utilizza



- Acquisto online.
- Utilizzo dati Virtual Card.

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. Le due funzioni sono:

- 1 Rij Client CifraNew
- 2 Rij Client DecifraNew

## Rij\_Client\_CifraNew

- La prima funzione, 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 seguente.

## Rij\_Client\_CifraNew

- La prima funzione, 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 seguente.

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 commerciale. <b>Deve essere univoco in assoluto.</b> 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	***		



## 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.

## 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.

## Codice di esempio (Rij\_Client\_DecifraNew)

CHIAMATA ALLA FUNZIONE "JAVASCRIPT" Rij\_Client\_DecifraNew INCLUSA NEL FILE 55555555.asp, in una pagina ASP

```
<%response buffer=true
Response.Expires=-1%>
<!-- #include FILE = ".\555555555.mph" -->
<%
dim campoDaDecifrare, stDecifrata, risposta
campoDaDecifrare = request.form("PaymentResponse")

if campoDaDecifrare <> "" then
  strDecifrata = Rij_Client_DecifraNew(campoDaDecifrare)

  if left(strDecifrata,3)="000" then
    Se i primi 3 caratteri del msg decifrato sono uguali a "000" allora la transazione è andata a buon fine
    risposta = "LA TRANSAZIONE E' ANDATA A BUON FINE"
  else
    risposta = "ATTENZIONE LA TRANSAZIONE NON E' ANDATA A BUON FINE"
  end if

else
  response.write "ERRORE, campo da decifrare VUOTO"
end if
%>
<html>
<head>
<title>Negozio Demo</title>
</head>
<body bgcolor="#FFFFFF" text="#000000" leftmargin="0" topmargin="0">
<%
response.write risposta
%>
</body>
</html>
```

### CODICE ELABORATO

```
<html>
<head>
<title>Negozio Demo</title>
</head>
<body bgcolor="#FFFFFF" text="#000000" leftmargin="0" topmargin="0">
LA TRANSAZIONE E' ANDATA A BUON FINE / ATTENZIONE LA TRANSAZIONE NON E' ANDATA A BUON FINE
</body>
</html>
```

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 ed è diverso da "000000"
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: 5 = 3Dsecure 6 = 3Dsecure 7 = Normale
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

## Gestione 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, di nome RETURL contenente l'URL.

Es:

```
<form name="PaymentRequestForm" action="https://www.monetaonline.it/MPI/MPIRequest.asp" method="POST">  
<input type="hidden" name="PaymentRequest" value="F383298A89239C893932832.....">  
<input type="hidden" name="RETURL" value="http://www.sitopreferito.it/risposta_php">  
<input type="submit" name="Submit" value="buy now">  
</form>
```

## Contabilizzazione

Il commerciante può avvalersi di uno dei tre differenti metodi di contabilizzazione delle transazioni autorizzate:

- Il primo metodo, implicito, prevede la contabilizzazione automatica a fine giornata di tutte le richieste autorizzate nella stessa giornata e non cancellate dal commerciante.
- Il secondo metodo, esplicito, richiede che il commerciante effettui personalmente la contabilizzazione delle operazioni autorizzate e 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.

## Contabilizzazione

Il commerciante può avvalersi di uno dei tre differenti metodi di contabilizzazione delle transazioni autorizzate:

- Il primo metodo, implicito, prevede la contabilizzazione automatica a fine giornata di tutte le richieste autorizzate nella stessa giornata e non cancellate dal commerciante.
- Il secondo metodo, esplicito, richiede che il commerciante effettui personalmente la contabilizzazione delle operazioni autorizzate e 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.

## Contabilizzazione

Il commerciante può avvalersi di uno dei tre differenti metodi di contabilizzazione delle transazioni autorizzate:

- Il primo metodo, implicito, prevede la contabilizzazione automatica a fine giornata di tutte le richieste autorizzate nella stessa giornata e non cancellate dal commerciante.
- Il secondo metodo, esplicito, richiede che il commerciante effettui personalmente la contabilizzazione delle operazioni autorizzate e 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.

## Contabilizzazione

Il commerciante può avvalersi di uno dei tre differenti metodi di contabilizzazione delle transazioni autorizzate:

- Il primo metodo, implicito, prevede la contabilizzazione automatica a fine giornata di tutte le richieste autorizzate nella stessa giornata e non cancellate dal commerciante.
- Il secondo metodo, esplicito, richiede che il commerciante effettui personalmente la contabilizzazione delle operazioni autorizzate e 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.