

Il servizio @POS

Storia SIA-SSB

Le origini della società risalgono alla Società Interbancaria per l'Automazione, brevemente SIA S.p.A., fondata nel 1977 per costruire e gestire la rete ed i servizi telematici relativi alle transazioni interbancarie, che conta tra gli azionisti tutti i principali gruppi bancari italiani. Dal conferimento da parte di SIA S.p.A. del ramo di attività relativo alla gestione dei servizi, separandola da quella della gestione della rete, nel 1992 nasce la Società per i Servizi Bancari S.p.A., brevemente SSB S.p.A., anch'essa controllata dalle banche. Nel mese di maggio del 2007, con effetti contabili e fiscali dal 1° Gennaio, SSB S.p.A. incorpora SIA S.p.A. ed assume la denominazione attuale SIA-SSB S.p.A., tornando a riunire in sé entrambi i rami di attività.

Nel maggio 2011 la società decide di semplificare la denominazione riutilizzando il nome SIA e diventando SIA S.p.A.

@POS

Modalità

Il servizio è in grado di accettare pagamenti:

- di tipo MO/TO (Mail Order/Telephone Order), tramite API XML e connessione server to server;
- in modalità redirect, utilizzando lo standard SSL;
- in modalità redirect, secondo i protocolli Verified by Visa e SecureCode di MasterCard;
- in modalità server to server secondo i protocolli Verified by Visa e SecureCode;
- con inserimento manuale da parte del merchant direttamente dal back-office di @POS(MO/TO).

Attori

1.VENDITORE

Il venditore/esercente è l'organizzazione commerciale che effettua la vendita di beni o servizi su Internet.

2.SIA-SSB

E' l'entità che, in relazione alle singole esigenze delle Banche e dei loro clienti (Internet Service Provider, imprese, professionisti, privati) gestisce l'infrastruttura di sicurezza del sistema e svolge il ruolo di gateway verso i circuiti autorizzativi.

3.BANCA DEL VENDITORE

E' la Banca presso la quale il venditore intrattiene il rapporto di conto corrente da accreditare a fronte delle vendite.

4. ACQUIRER

E' l'istituzione finanziaria che detiene il rapporto contrattuale con l'esercente al fine di consentire l'accettazione delle carte di pagamento appartenenti ad un determinato circuito.

5. ISSUER

E' l'istituzione finanziaria che detiene il rapporto contrattuale con il titolare della carta, ne cura il processo di emissione e di autorizzazione al pagamento.

Cosa succede nei circuiti autorizzativi

1. Soggetto Acquirer riceve dal POS (in Italia dal Gestore Terminali) installato presso un'esercente convenzionato, la richiesta autorizzativa per un pagamento negoziato con Carta emessa da un generico Soggetto Issuer.

La selezione dell'Acquirer corretto è compito del POS (in Italia tale operazione viene contribuita dal G.T.), che in funzione dei

parametri di acquiring, conosce quale è l'Acquirer verso cui instradare la richiesta autorizzativa.

La selezione dell'Acquirer è funzione del/dei profili contrattuali che l'esercente ha stabilito con la Banca Acquirer (convenzionamento tramite banca) o con l'Acquirer direttamente.

1. Soggetto Acquirer verifica che la Carta appartenente al Circuito Internazionale non sia emessa da se stesso (ovvero caso in cui il Soggetto Acquirer coincide con il Soggetto Issuer):

Se Acquirer coincide con Issuer -> autorizzazione ON-US

(in questo caso particolare si avrebbe un'analogia declinazione di schema 3-Side)

Se Acquirer non coincide con Issuer -> routing della transazione verso l'Issuer per il tramite della Rete Internazionale

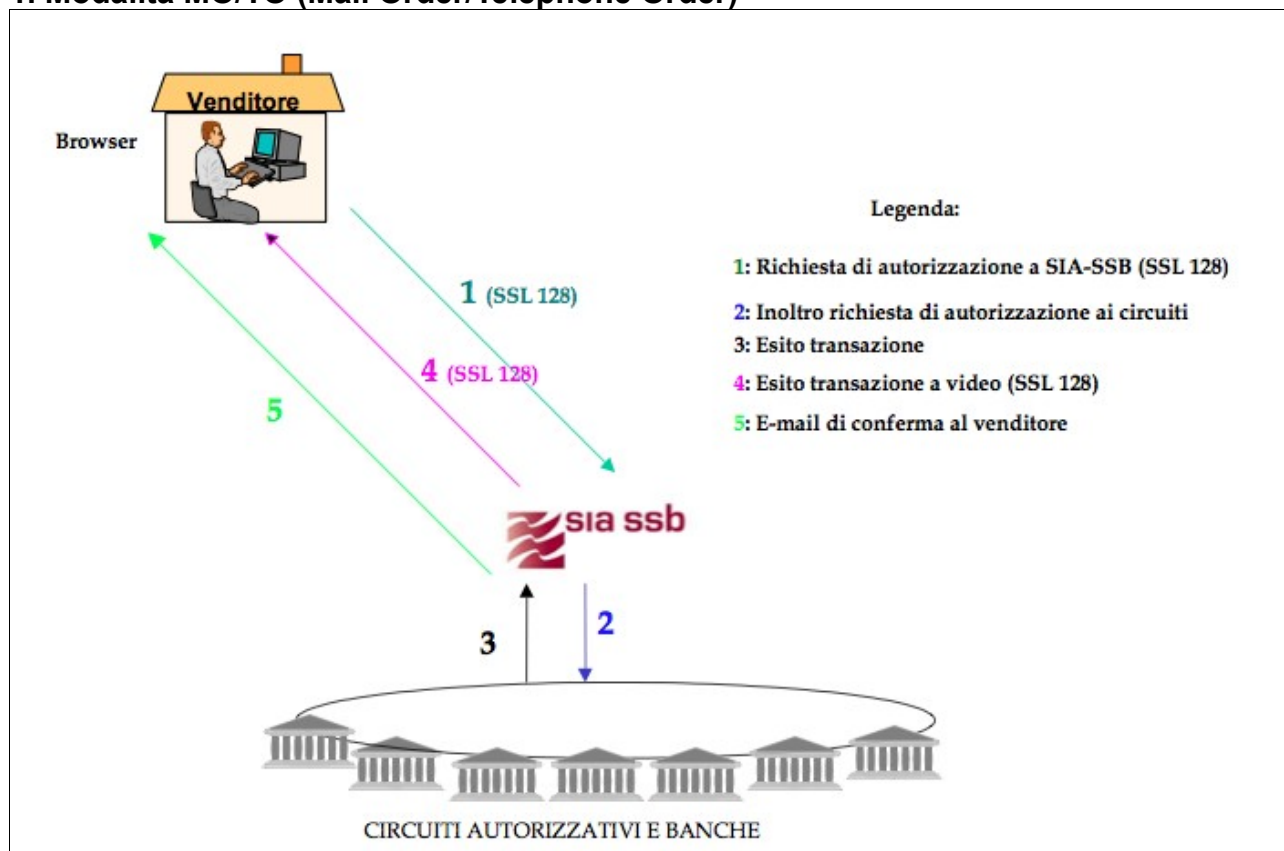
1. Ad autorizzazione concessa, l'Acquirer regola contabilmente con l'esercente convenzionato e con il Circuito Internazionale:

2. Acquirer accredita l'esercente al netto o al lordo delle commissioni, comunemente chiamate **MSC Merchant Service Charge**, sulla base di una tempistica definita preventivamente nell'ambito del contratto di convenzionamento

3. Acquirer addebita Issuer (tramite il Circuito Internazionale) al netto della commissione interbancaria multilaterale (o **MIF Multilateral Interchange Fee**)

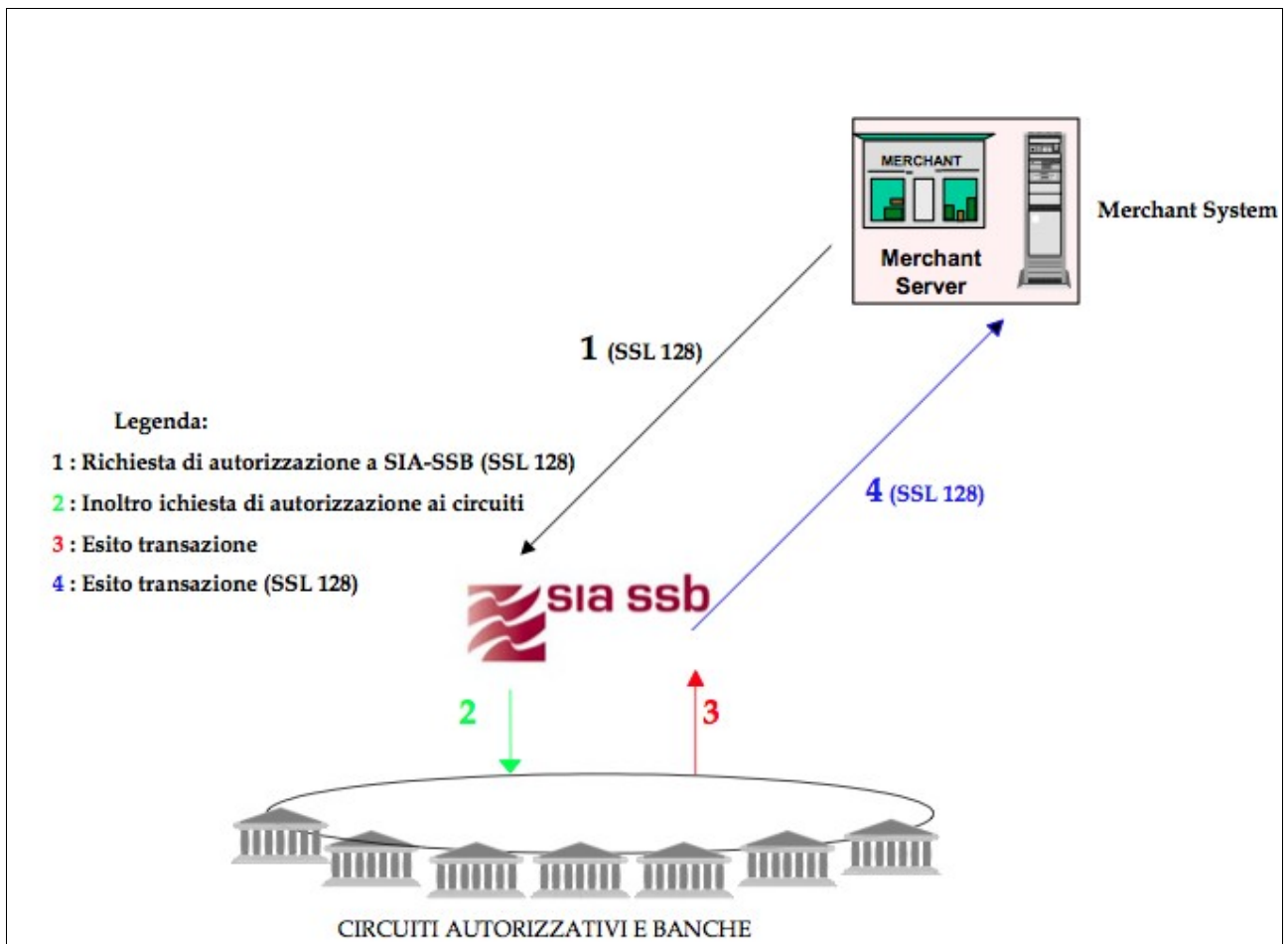
Schemi di funzionamento @POS

1. Modalità MO/TO (Mail Order/Telephone Order)



Il Merchant deve compilare i campi del form @POS, come da specifiche operative, inserire il numero di carta di credito e la relativa scadenza ed inoltrare il tutto verso SIA-SSB che processerà l'operazione.

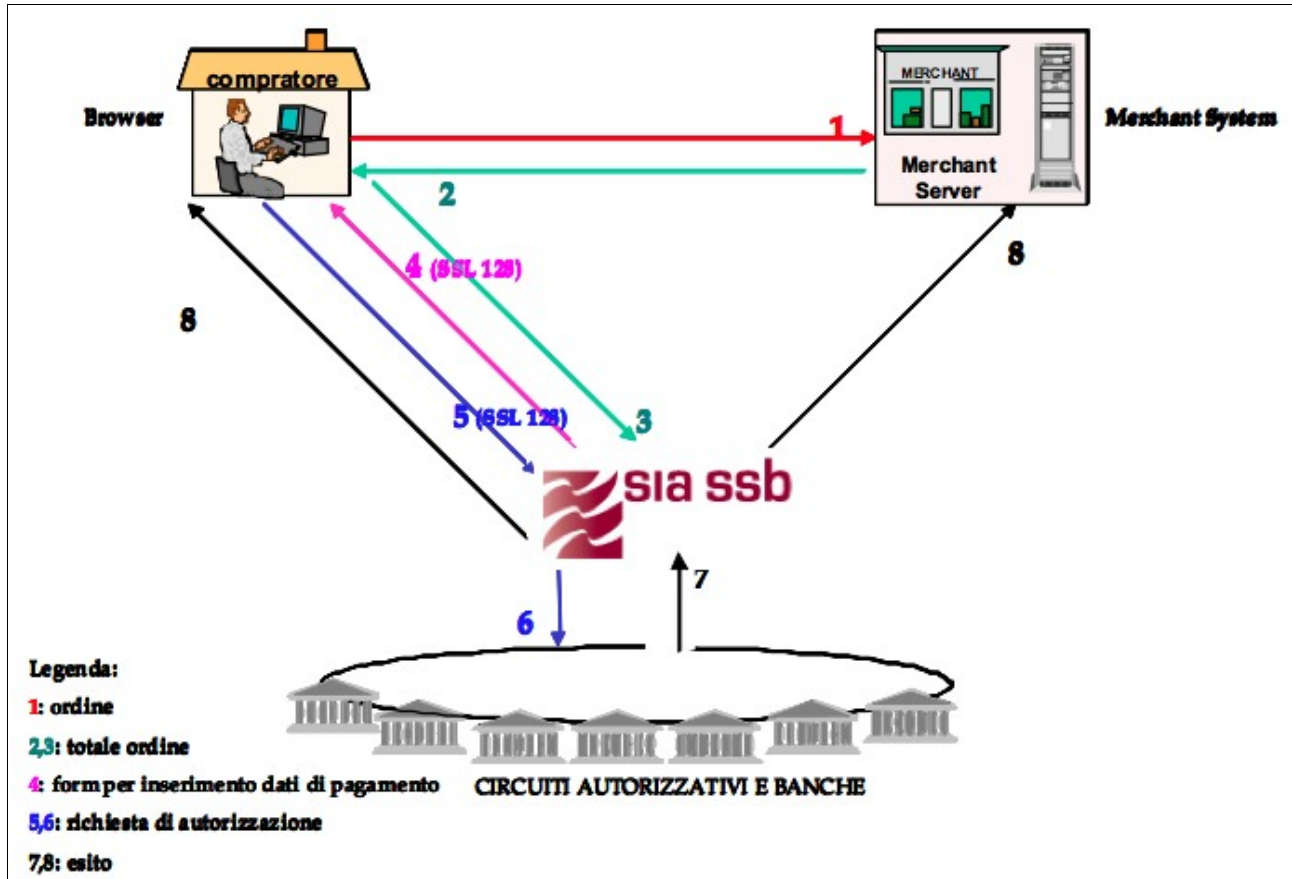
2. Modalità server-to-server con integrazione Merchant System



Sul server del venditore, deve essere presente un' applicazione che utilizza un client HTTPS per comunicare con il server SIA-SSB in modalità sicura tramite SSL 128 bit.

3. Modalità Redirect con Transazione SSL

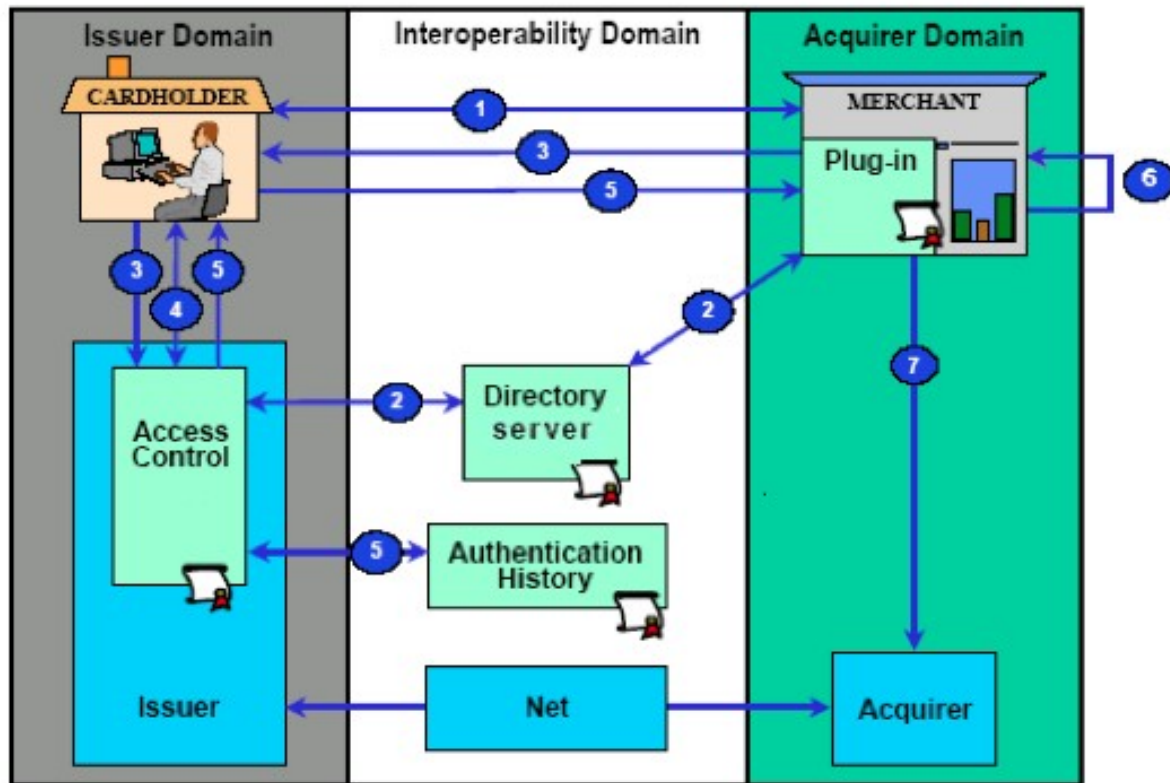
Il compratore al momento del pagamento viene re-indirizzato sulla pagina web di @POS, presente sul server sicuro di SIA-SSB, nella quale inserisce i dati della carta di debito/credito (numero carta, data scadenza ed eventuali quantità di sicurezza) ed ottiene on-line l'esito dell'operazione richiesta.



Questa modalità di pagamento garantisce una maggior sicurezza nella transazione sia al titolare delle carte che all'esercente in quanto i dati della carta utilizzata per il pagamento transitano solo sul server sicuro di SIA-SSB.

4. Modalità Redirect con Transazione Verified by VISA/SecureCode

In questa modalità di pagamento, del tutto simile a quella descritta nel precedente capitolo, il sistema @POS rileva che la carta utilizzata è abilitata al servizio VbV/SC innescando così il flusso di seguito riportato.



Step 1:

il titolare chiede di effettuare un acquisto su un sito di un esercente abilitato ai servizi VbV/SC ed inserisce i dati della carta di credito dando inizio alla transazione;

Step 2:

il sito dell'esercente si collega attraverso la componente Merchant Plug-In (MPI) al Directory Server (di Visa o Mastercard) che verifica se la carta aderisce al servizio VbV/SC (contattando l'ACS appropriato);

Step 3:

se la carta aderisce al servizio, l'MPI invia una richiesta d'autenticazione del titolare all'ACS

(Access Control Server) attraverso una redirect del browser del titolare;

Step 4:

l'ACS richiede la password al titolare e la verifica;

Step 5:

l'ACS restituisce un identificativo univoco della transazione (CAVV) e l'esito dell'autenticazione all'MPI attraverso una redirect del browser del titolare;

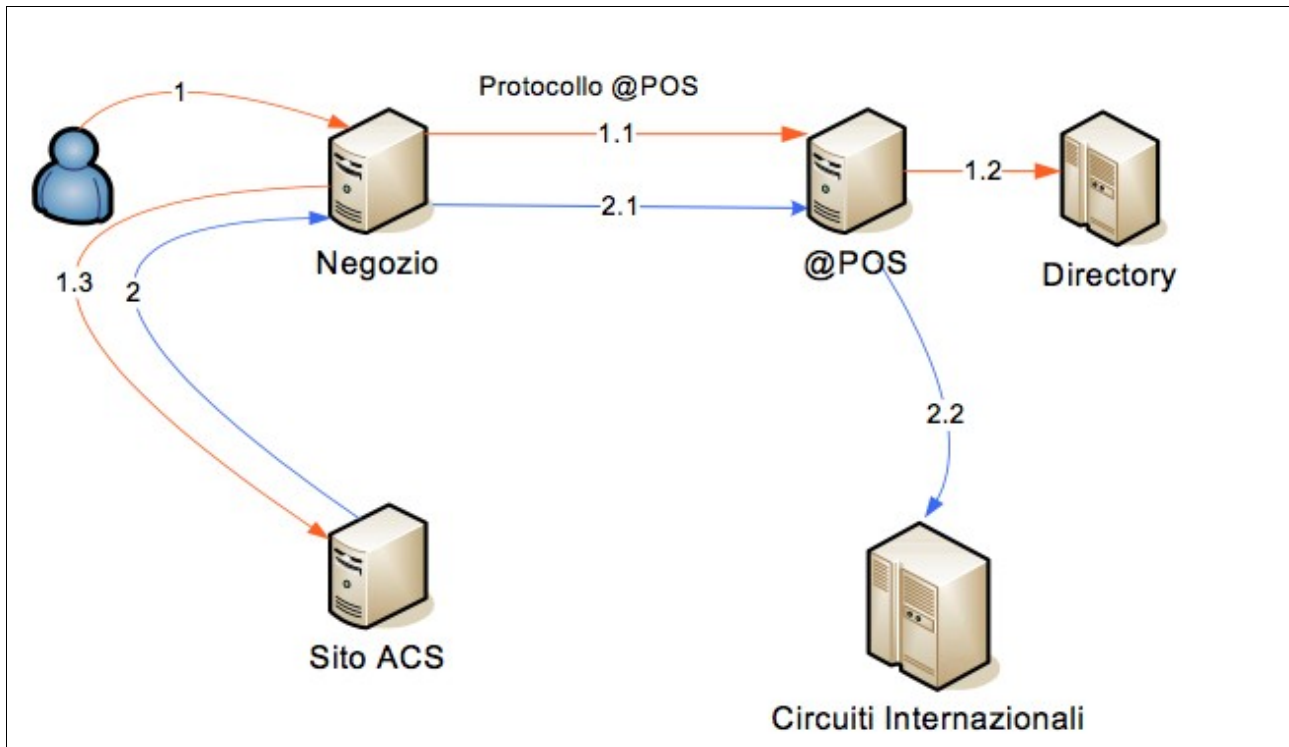
Step 6:

il Merchant Server Plug-in verifica la risposta dell'ACS;

Step 7:

se l'autenticazione ha avuto esito positivo, il sito dell'esercente prosegue con il normale processo autorizzativi.

5. Modalità Server-to-server Verified by VISA/SecureCode



1. Il compratore è connesso al sito del negozio e inserisce i dati della carta di credito.

1.1.

semplicemente inoltrando un messaggio al sistema @POS;

Il negozio inizia il processo di richiesta autorizzazione, qualsiasi sia la carta,

1.2.

Nel caso di carta VISA e MasterCard, @POS si collega alle directory opportune e verifica se la

carta è abilitata al servizio VBV

1.2b.

Se la carta non è abilitata a VBV/SC (o non è VISA/MC) @POS inoltra direttamente un messaggio autorizzativo ai circuiti internazionali (2.2). La risposta fornita al sito del negozio contiene l'esito della transazione.

1.3.

risultato della transazione contiene i dati per la redirect del compratore verso il sito ACS dell'Issuer .

2. L'utente, connesso al sito ACS, inserisce la sua password e viene rediretto nuovamente verso il sito del negozio.

2.1.

Il negozio, con le informazioni arrivate da ACS, compila il messaggio e lo inoltra al sistema @POS.

2.2.

@POS decodifica i dati ACS, inoltra la richiesta di autorizzazione ai circuiti internazionali, e fornisce quindi l'esito della transazione in risposta al messaggio pervenuto.

BACK-OFFICE

Oltre a supportare le modalità di pagamento sopra descritte, @POS mette a disposizione del commerciante un servizio di Back-office.

Tale servizio ha una struttura gerarchica basata sulla distinzione tra negozi che compongono, nel loro insieme, l'esercizio commerciale.

In modo trasversale la struttura organizzativa degli utenti che hanno accesso al back-office è basata sulla distinzione tra amministratore e operatori .

ESERCIZIO E NEGOZI

La struttura su cui è basato il back office gestionale prevede che un unico esercente possa distinguere al suo interno diversi negozi virtuali di e-commerce. Questo non implica necessariamente che a ogni negozio sia associato un sito web o un'area del sito diversa, ma può essere anche una suddivisione interna dell'esercizio commerciale che raggruppa i prodotti in vendita in diverse vetrine virtuali.

In questo modo l'esercente può mantenere traccia della segmentazione delle vendite all'interno della propria gamma di prodotti/servizi.

Infatti, all'atto della redirect del consumatore al momento del pagamento, tra le informazioni trasmesse al sistema POS virtuale è prevista anche l'informazione relativa al negozio (tra quelli presenti nell'organizzazione dell'esercente) da cui è stato generato l'ordine.

Nel caso in cui l'esercente non ritenga opportuno usufruire dell'articolazione dell'esercizio commerciale in diversi negozi, può ovviamente mantenere la completa corrispondenza tra esercizio e negozio. In questo caso l'esercizio commerciale definito dalla ragione sociale viene identificato con un unico negozio all'interno del back office.

Qualora, invece, l'esercente opti per una gestione delle transazioni in funzione di una segmentazione in negozi, l'esercente, in qualità di amministratore del sistema di back office ha la possibilità di limitare l'operatività degli operatori solo ad alcuni negozi, mantenendo all'interno del suo staff una chiara separazione delle responsabilità.

AMMINISTRATORE E OPERATORI

In sede di convenzionamento al servizio l'esercente indica il responsabile amministratore del servizio di back office, specificando i dati personali dello stesso.

Vengono quindi fornite all'esercente le chiavi di accesso (user-id e password) al back office che permettono all'esercente di autenticarsi sul sito e di usufruire di tutte le funzionalità che il servizio offre.

Tra le funzioni specifiche accessibili solamente all'amministratore ci sono quelle che riguardano la gestione degli operatori, ovvero quegli utenti che all'interno della organizzazione dell'esercente avranno accesso al back office usufruendo di funzionalità limitate, così come definite dall'amministratore stesso.

L'amministratore crea i profili degli operatori e ne definisce visibilità (i.e. negozi gestibili all'interno dell'esercizio) e operatività (funzioni cui è abilitato nella gestione dei negozi su cui ha visibilità).

Le operatività disponibili sono sostanzialmente di due tipi:

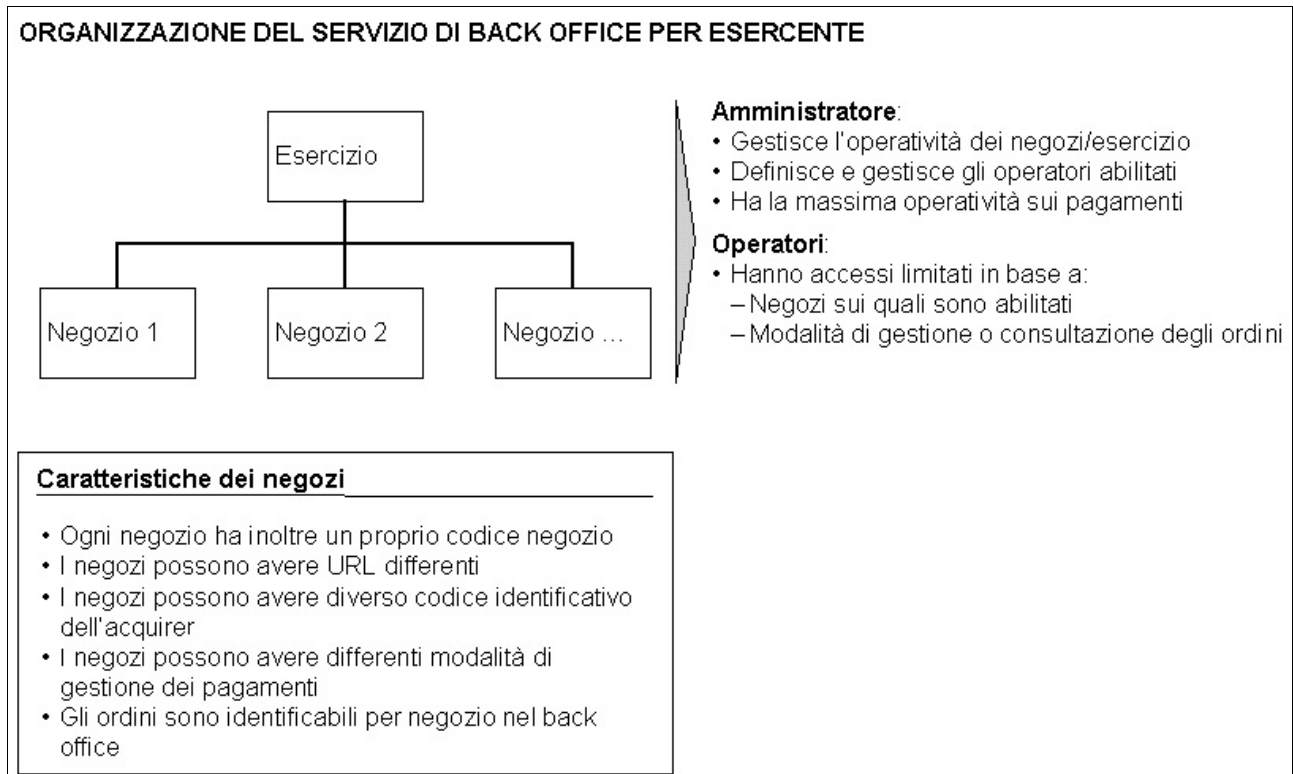
- abilitazione alla consultazione: consente all'operatore solo l'accesso alle reportistiche e statistiche degli ordini del negozio senza poter disporre o operare sulle transazioni di pagamento;
- abilitazione alla gestione: permette all'operatore di operare sugli ordini in modo dispositivo usufruendo di tutte le funzionalità legate alla gestione delle transazioni di pagamento.

FUNZIONALITA' DI GESTIONE

Una volta effettuato il login direttamente sul sito di SIA-SSB per il back-office, l'amministratore

potrà usufruire di diverse funzioni di vario tipo (che accenniamo soltanto), come:

- funzionalità di supporto
- funzionalità di gestione ordini
- funzionalità dispositive



SSL

Il protocollo SSL è nato al fine di garantire la privacy delle comunicazioni su Internet, infatti permette alle applicazioni client/server di comunicare in modo da prevenire le intrusioni, le manomissioni e le falsificazioni dei messaggi. Il protocollo SSL garantisce la sicurezza del collegamento mediante tre goals fondamentali:

- **Privatezza del Collegamento:** Per assicurare un collegamento sicuro tra due utenti coinvolti in una comunicazione, i dati vengono protetti utilizzando algoritmi di crittografia a chiave simmetrica (ad es. DES, RC4, ecc.);
- **Autenticazione:** L'autenticazione dell'identità nelle connessioni può essere eseguita usando la crittografia a chiave pubblica (per es. RSA, DSS ecc.). In questo modo i client sono sicuri di comunicare con il server corretto, prevenendo eventuali interposizioni. Inoltre è prevista la certificazione sia del server che del client;
- **Affidabilità:** Il livello di trasporto include un controllo sull'integrità del messaggio basato su un apposito MAC (Message Authentication Code) che utilizza funzioni hash sicure (per es. SHA, MD5 ecc.). In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

Una comunicazione tramite protocollo SSL prevede varie fasi:

- 1 - Il client che si connette al Server ne richiede l'autenticazione spedendo oltre alla richiesta, la lista dei sistemi crittografici supportati e altri dati casuali
- 2 - Il server risponde inviando al client il metodo di crittografia scelto fra quelli supportati dal client oltre al proprio certificato ed un eventuale richiesta di autenticazione del client
- 3 - Il client provvede a verificare la validità del certificato ricevuto e in caso positivo invia l'ok al server (ed eventualmente provvederà ad identificarsi)

- 4 - Il server genera una chiave simmetrica di sessione che spedisce al client crittata con la propria chiave privata secondo il metodo di crittografia pattuito
- 5 - La comunicazione procede tramite la chiave simmetrica di sessione ormai a disposizione di entrambe le parti

BEAST ATTACK

Il primo attacco al protocollo SSL/TLS in grado di decriptare le richieste di tipo HTTPS è stato presentato alla Ekoparty Security Conference tenutasi in Argentina nel settembre 2011. Julian Rizzo e Thai Doug sono i due ricercatori che hanno proposto tale tipo di attacco denominato BEAST, acronimo di Browser Exploit Against SSL & TLS.

BEAST è un particolare attacco Man-In-The-Middle, esso prevede che sia iniettato un JAVA script nel computer della vittima il quale collaborando con uno sniffer, provvede ad intercettare i pacchetti rivolti verso siti di interesse (es: paypal) e a decrittare i cookies di autenticazione relativi.

La fase di decriptaggio sfrutta una debolezza dei sistemi crittografici a blocchi. Rizzo e Doug nelle loro prime simulazioni riuscivano a decriptare byte per byte i cookies impiegando all'incirca 2 secondi a byte, per un totale di circa mezz'ora a cookie. In implementazioni successive sono riusciti a ridurre il tempo di decriptaggio sotto i 10 minuti.

L'attacco per tanto rappresenta una grave minaccia per la confidenzialità delle informazioni inviate tramite protocollo SSL, fortunatamente nelle versioni SSL 3.0 e TLS successive alla 1.0 tale debolezza non è più presente e l'attacco BEAST non può avere successo.

*definizione di cookie: file di testo di piccola dimensione inviati da un server ad un client e poi rimandati indietro dal client al server ogni volta che il client accede allo stesso server. Questi vengono utilizzati per aggiungere uno stato ad un protocollo privo di stato. Senza i cookie non vi sarebbe differenza in una pagina caricata prima di effettuare un login, dalla stessa pagina caricata dopo.

Fonti

http://it.wikipedia.org/wiki/SIA_S.p.A.

http://www.bancamarche.it/download/POS_01.pdf

<http://closetopay.wordpress.com/>

http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

http://it.wikipedia.org/wiki/Transport_Layer_Security