Manuale di riferimento per l'integrazione con i MERCHANT SYSTEMS

Release n. 1.3.5
Luglio 2015

Revisioni

Data	Modifiche	Versione
27-07-2006	Prima stesura: unificazione manuale API e Pagamenti	1.0.0
06-10-2006	Aggiunta gestione storni multipli	1.0.1
16-03-2007	Aggiunta OPTION I per la gestione dell'aggiunta all'URLMS e all'URLDONE nel caso di autorizzazione concessa del parametro BPW_ISSUER_COUNTRY che contiene la nazione di provenienza dell'issuer	1.0.2
10-07-2007	Introdotta l'estensione delle API XML per la gestione delle autorizzazioni online VBV/SecureCode	1.1.0
25-07-2007	Introdotto campo facoltativo TIPOOP nella richiesta ELENCOCONTABILE	1.1.1
08-09-2008	Aggiunta OPTION L	1.1.1
22-01-2009	Aggiunto codice esito API per CVV2 mancante	1.1.1
18-03-2010	Oscuramento campi pan e cvv2 in risposta autorizzazioni con api	1.1.2
15-04-2012	Documentata option M per creazione alias pan	1.1.3
27-04-2012	Aggiunta restituzione in URLMS e URLDONE di data scadenza carta (introdotto campo DATASCAD), ultime quattro cifre del pan (introdotto campo PANTAIL), aliaspan eventualmente revocato (introdotto campo ALIASPANREV) .	1.1.4
31-05-2012	I dettagli della implementazione della funzionalità di Alias Pan sono demandati alla visualizzazione dei doc appropriati per l'integrazione	1.1.5
13-06-2012	Aggiunta dettagli per integrazione con circuito MyBank	1.1.6
31-07-2012	Aggiunta nuova option (OPTION P) per ritorno in URLMS e URDONE del response code autorizzativo ISO	1.1.7
30-11-2012	Aggiunta gestione circuito Postepay	1.1.8
21-12-2012	Aggiunta doc per OPTION N	1.1.9
13-02-2013	Aggiunta gestione transazioni PAYPASS nel messaggio AutorizzazioneOnlineVBV. Aggiunta campi facoltativi : - SERVIZIO : codice servizio per transazione PAYPASS. Valore: SV47 - XID: identificativo univoco della transazione 3D - CAVV (Cardholder Authentication Verification Value) - ECI (electronic commerce indicator) - PP_AUTHENTICATEMETHOD: Metodo di autenticazione usato dal titolare della carta. - PP_CARDENROLLMETHOD: metodo usato per validare la carta e il titolare al momento dell'aggiunta della carta nel wallet PAYPASS. - PARESSTATUS: Codice di esito dell'autenticazione del titolare - SCENROLLSTATUS: indica se l'issuer della carta supporta l'autenticazione 3D. - SIGNATUREVERIFICATION. Esito verifica della firma della PARes	1.2.0
12-09-2013	Introdotte le seguenti modifiche ai messaggi: - SITUAZIONEORDINE: mostra anche gli ordini pendenti MyBank (identificabili dal fatto che EsitoTrans e Stato assumono come valore il nuovo codice "99"). - SITUAZIONEORDINE, ELENCOAUTORIZZAZIONI, ELENCOCONTABILE: l'identificativo di transazione NUMAUT (lungo normalmente 6) può	1.2.1

	essere fino a 35 per le transazioni MyBank. - AUTORIZZAZIONEONLINE, AUTORIZZAZIONEDIFFERITA, AUTORIZZAZIONEONLINEVBV: definito un nuovo elemento facoltativo nel messaggio di richiesta IPADDRESS che viene passato al BackEnd. - AUTORIZZAZIONEONLINE, AUTORIZZAZIONEDIFFERITA, RICHIESTAAUTORIZZAZIONE, AUTORIZZAZIONEONLINEVBV, AUTORIZZAZIONEONLINEVBV2: se il negozio è abilitato al servizio SV53 nella risposta viene passato anche il campo ResponseCodeISO. - Integrato l'esito transazione 45 relativo al filtro carte estere (precedentemente in documento separato).	
29-10-2013	Integrata documentazione relativa al parametro LOCKCARD	1.2.2
18-12-2013	PAYPASS: Aggiornamento valori campi Authentication Method e Card Enrollment Method	1.2.3
30-01-2014	Aggiunto circuito 93 per deduzione automatica circuito della carta nelle richieste : AUTORIZZAZIONEONLINE AUTORIZZAZIONEDIFFERITA AUTORIZZAZIONEONLINEVBV	1.2.4
24-03-2014	Aggiunte modifiche per multiacquiring (campo ACQUIRER aggiuntivo e facoltativo nelle chiamate: AUTORIZZAZIONEONLINE AUTORIZZAZIONEDIFFERITA AUTORIZZAZIONEONLINEVBV AUTORIZZAZIONEONLINEVBV2	1.2.5
27-05-2014	Gestione transazioni sicure con AMEX (SafeKey)	1.2.6
03-12-2014	Aggiunto nel capitolo sul *Messaggio di conferma/esito dell'avvenuto pagamento* codice 04 per il tipo di carta Maestro e nota sui tipi per transazioni masterpass negli URL MS/DONE.	1.2.7
04-12-2014	Intregrazione di @pos/mybank con il nodo della p.a. - "*Redirect di avvio pagamento @POS*": aggiunta dei campi DESCRORD e IDVS; aggiunta della option "O". - "*C1 Generazione del MAC per i messaggi di redirect*": aggiunta dei campi DESCRORD e IDVS.	1.2.8
16/01/2015	Introduzione della OPTION "Q" per l'invio di informazioni aggiuntive nelle URLMS/DONE quando i pagamenti sono tramite Paypal	1.2.9
05/02/2015	Per le transazioni Paypal il campo BPW_HASH_PAN, quando presente, non contiene più l'hash del BILLINGAGREEMENTID, ma del PAYERID.	1.3.0
26/02/2015	Integrato *maccatura* esito redirect in caso di OPTION P	1.3.1
17/03/2015	Modifica messaggi STORNO e ELENCOCONTABILE per aggiunta nuovo campo DESCROP, descrizione aggiuntiva dell'operazione ad uso dell'esercente	1.3.2
14/05/2015	Redirect: nuova OPTION "R" per il MAC degli esiti negativi. API: nuovo messaggio "RECUPERAALIASPAN" per la ricerca di un alias partendo dall'ordine che lo ha creato.	1.3.3
18/06/2015	API: modifica messaggio CONTABILIZZAZIONE per aggiunta nuovo campo DESCROP, descrizione aggiuntiva dell'operazione ad uso dell'esercente	1.3.4

	Redirect: nuovo parametro DESCROP per la descrizione aggiuntiva dell'operazione ad uso dell'esercente, in caso di contabilizzazione immediata	
02/07/2015	API: modifica messaggi di autorizzazione per aggiunta nuovo parametro DESCROP per la descrizione aggiuntiva dell'operazione ad uso dell'esercente, in caso di contabilizzazione immediata	

Glossario

Backoffice	Usato per far riferimento alla funzioni di gestione di un negozio: resoconti, elenchi, interrogazioni , disposizioni etc.
CC	Carta di credito
Contabilizzazione	Operazione che crea gli effetti contabili per una transazione che era stata precedentemente autorizzata
Credit	Operazione contabile per la restituzione di una somma di denaro ad un cliente
GET	Operazione di comunicazione del protocollo HTTP
Hash	Insieme di N bit (es. 128, 160) ricavato da una stringa con un procedimento matematico in modo che a partire da stringhe diverse non si abbia mai lo stesso risultato
HTTP	Protocollo applicativo utilizzato per trasmettere le pagine web. Standard RFC 2068
MAC	Codice di autenticazione del messaggio
MD5	Algoritmo per la generazione di un identificativo univoco di 16 byte di un messaggio. Definito nella RFC 1321
Merchant system	Sistema software di gestione di un negozio virtuale. Negozio virtuale
SIA	Processor di FrontEnd: SIA Spa
POST	Operazione di comunicazione del protocollo HTTP
SHA-1	Secure Hash Algorithm. Algoritmo per la generazione di hash. Standard NIST FIPS 180-1
Split	Operazione per suddividere/ridurre un pagamento già effettuato.
SSL	Secure Socket Layer protocollo di trasporto standard ideato da Netscape Communication
Storno	Operazione di annullamento di una autorizzazione concessa con la restituizione del denaro e/o del limite di spesa al titolare della carta
URL	Universal resource locator
VBV	Verified By Visa, sistema di sicurezza Visa per l'autenticazione dei titolari di carta di credito durante acquisti Internet
SecureCode	Sistema di sicurezza per l'autenticazione dei titolari di carta di credito Mastercard e Maestro durante acquisti Internet (equivalente a VBV)
SafeKey	Sistema di sicurezza per l'autenticazione dei titolari di carta di credito AMEX durante acquisti Internet (equivalente a VBV)

Scopo

Il presente documento contiene le informazioni tecniche necessarie a chi sviluppa negozi virtuali, per effettuare l'integrazione fra il proprio sito e il servizio @POS. Destinatari del documento sono quindi figure prettamente tecniche. Questo manuale non contiene una descrizione vera e propria del servizio @POS che viene invece riportata negli appositi documenti.

Introduzione

Nel presente documento vengono descritte l'**interfaccia API Internet,** l'**opzione di Redirect** del sistema @POS e la relativa integrazione coi sistemi di gestione ordini lato merchant.
@POS è a tutti gli effetti un POS virtuale Internet che SIA fornisce direttamente ai venditori. Tramite esso i negozianti sono in grado di eseguire transazioni online con carta di credito utilizzando un PC ed una connessione ad Internet. Il sistema si propone sia come sostituto dello "scatolotto" fisico del POS tradizionale sia come gateway personalizzabile per transazioni con carte di credito. Per una descrizione generale delle funzionalità si veda il documento relativo.
Il servizio @POS è completato dalle funzionalità di una interfaccia grafica di back office.

Per quanto riguarda la sicurezza della tratta di comunicazione Internet il grado di affidabilità offerto è quello del protocollo SSL con cifratura a 128 bit.

Backoffice @POS

L'interfaccia grafica di back office è utilizzabile via browser dagli operatori dei negozi e permette di effettuare manualmente richieste di autorizzazione , storni, prospetti, contabilizzazioni, etc.

Invio logo

L'amministratore del back office dopo essersi autenticato tramite userid e password può inviare il logo del negozio accedendo al dettaglio negozio dall'area di gestione negozi. Il logo del negozio deve avere dimensioni massime di 140x70 pixel e minime di 70x70 pixel e pesantezza massima di 20K. Il logo del negozio apparirà nell'interfaccia grafica di backoffice utilizzata dagli operatori.

Messaggi e-Mail

A fronte dell'esecuzione da parte degli operatori del negozio di una operazione di pagamento tramite l'interfaccia grafica di back office, il server SIA può generare e spedire, al cliente e all'esercente, alcune e-mail.
I messaggi di e-mail non sono personalizzabili e vengono inviati solo nel caso di utilizzo del servizio tramite interfaccia grafica. Le richieste effettuate tramite API non inviano alcun tipo di e-mail.
L'e-mail al titolare verrà inviata solamente se all'atto della richiesta di autorizzazione tale campo sarà inserito dall'esercente nella maschera di richiesta autorizzazione e solo per il seguente caso:

Autorizzazione online concessa
1. E-mail transazione OK online al cliente

L'e-mail all'esercente verrà inviata all'indirizzo e-mail indicato dal venditore al momento dell'adesione al servizio ed in base alla configurazione dell'opzione di invio censita per il negozio. Tale opzione d'invio prevede una scelta tra le seguenti casistiche:
1. Mai
2. Sempre
3. Per soli esiti positivi

Il contenuto dei dati delle e-mail, dove applicabile, è il seguente:
- Data della transazione
- Numero d'ordine
- Importo
- Numero di autorizzazione
- Insegna negozio

Una eventuale variazione dell'indirizzo e-mail dell'esercente potrà essere effettuata comunicando il nuovo indirizzo a SIA.

Integrazione

Per integrazione si intende l'utilizzazione da parte di una applicazione software delle funzionalità offerte dal sistema @POS sotto forma di API.

Le URL delle API web sono le seguenti:
Ambiente di TEST: atpostest.ssb.it/atpos/apibo/apiBO.app
Ambiente di PRODUZIONE: atpos.ssb.it/atpos/apibo/apiBO.app

Dalla versione n. 1.4.0 dell'API @POS è anche possibile inviare richieste in formato XML.
Per inviare richieste in formato XML, le URL delle API del web sono le seguenti:
Ambiente di TEST: atpostest.ssb.it/atpos/apibo/apiBOXML.app
Ambiente di PRODUZIONE: atpos.ssb.it/atpos/apibo/apiBOXML.app

Nel presente capitolo viene descritta la modalità per integrare una propria applicazione con il sistema di API del servizio di pagamento @POS. L'utilizzo dell'API @POS è del tutto facoltativo.

Abilitazione API: L'amministratore del back office dopo essersi autenticato tramite userid e password può chiedere l'abilitazione all'utilizzo delle API @POS accedendo all'interno del profilo negozio, in particolare nel dettaglio negozio.

L'API è resa disponibile sotto forma di una web application che accetta chiamate in formato POST HTTP generate da una applicazione merchant. Tramite questo meccanismo possono essere effettuate le operazioni di: richiesta di autorizzazione, storno di un pagamento, contabilizzazione di una transazione autorizzata, verifica dello stato di una transazione e interrogazione dei movimenti effettuati da un merchant in un certo periodo, etc.
Dalla versione n. 1.4.0 dell'API @POS è anche possibile inviare richieste in formato XML. Queste devono essere inviate nel seguente modo:
POST con un parametro di nome **`data`** valorizzato con il messaggio XML in formato urlencoded.
Nelle pagine seguenti sono indicati i campi dei messaggi di richiesta, e i corrispondenti tracciati XML per effettuare una richiesta in formato XML. In tali tracciati, i valori dei tag sono forniti soltanto a titolo di esempio, eccetto il valore del tag <Operazione> che dev'essere esattamente pari a quanto indicato.
Indipendentemente da quale dei due formati si utilizzi per la richiesta, la risposta è sempre in XML.
Per quanto riguarda la sicurezza della tratta di comunicazione Internet il grado di affidabilità offerto è quello del protocollo SSL con cifratura a 128 bit, considerato "strong encryption".
Nel seguito viene illustrato il protocollo di comunicazione che dovrà essere utilizzato dalle applicazioni dei merchant per interfacciarsi al sistema. In particolare vengono riportati quali sono i passi da seguire per l'integrazione ed elencati i messaggi che vengono scambiati fra il sistema @POS e i merchant system.
Per integrazione si intende il meccanismo che permette di utilizzare l'API web messa a disposizione da SIA da una applicazione di propria realizzazione. Questa applicazione sarà probabilmente in grado dialogare con il sistema di gestione ordini, e prelevare da esso i dati necessari per l'esecuzione delle transazioni, nonché di aggiornarlo con gli esiti ricevuti online.

Le funzionalità messe a disposizione dei merchant system sono le seguenti:

Funzione	Descrizione
Conferma di autorizzazione differita	Permette di inoltrare richieste di autorizzazione a conferma di pagamenti con autorizzazioni differite.
Richiesta di autorizzazione on line	Permette di inoltrare le autorizzazioni verso i circuti autorizzativi
Richiesta di autorizzazione differita	Permette il caricamento di un ordine sul servizio @POS. Tale ordine dovrà poi essere confermato tramite una richiesta di conferma autorizzazione differita
Chiusura autorizzazione differita	Viene resa non più utilizzabile la autorizzazione differita per ulteriori conferme
Richiesta di storno di un pagamento	La richiesta di storno viene applicata dal sistema @POS ad un pagamento (autorizzazione), indifferentemente dal suo stato
Richiesta di contabilizzazione	Permette di inoltrare a @POS la richiesta per contabilizzare una autorizzazione con carta di credito precedentemente concessa con contabilizzazine differita.
Annullamento richiesta di contabilizzazione	Annulla una richiesta di contabilizzazione e rende l'autorizzazione con carta di credito nuovamente contabilizzabile
Split(divisione e/o riduzione) ordine con autorizzazione immediata	Rende possibile lo split shipment (divisione e/o riduzione) per un ordine che era stato eseguito con autorizzazione immediata: storna la autorizzazione immediata e piazza una nuova autorizzazine differita da confermare in pezzi
Verifica esito messaggio di richiesta	Fornendo il numero identificativo della richiesta voluta, restituisce l'esito del messaggio precedentemente inoltrato.

Elenco operazioni contabili	Ricava l'elenco delle operazioni di carattere contabile. Contiene quelle richieste e quelle già inviate agli acquirer distinte con uno stato
Elenco autorizzazioni richieste	Vengono visualizzate le richieste di autorizzazione inoltrate al sistema: 1. Con esito positivo 2. Con esito negativo 3. Autorizzazioni stornate 4. Tutte
Richiesta situazione di un ordine	Restituisce la situazione attuale di un ordine con tutte le operazioni di autorizzazione ad esso legate.

Di seguito viene illustrato schematicamente il processo seguito durante un'operazione di richiesta:

1. il merchant system recupera dalla sua base dati tutte le informazioni necessarie per effettuare la transazione, ad esempio: ID transazione, importo etc.
2. il merchant system formatta un messaggio HTTP che contiene tutti i campi specificati come obbligatori per l'operazione voluta, e lo invia tramite GET o POST a SIA. Nel messaggio sono presenti anche le informazioni di autenticazione
3. il server SSL di SIA elabora i dati della richiesta comunicandoli ai legacy system e risponde con un documento xml
4. il merchant system elabora il messaggio di esito ed eventualmente aggiorna la sua base dati

Gli elenchi completi dei campi dei vari messaggi sono riportati nei paragrafi ad essi dedicati.

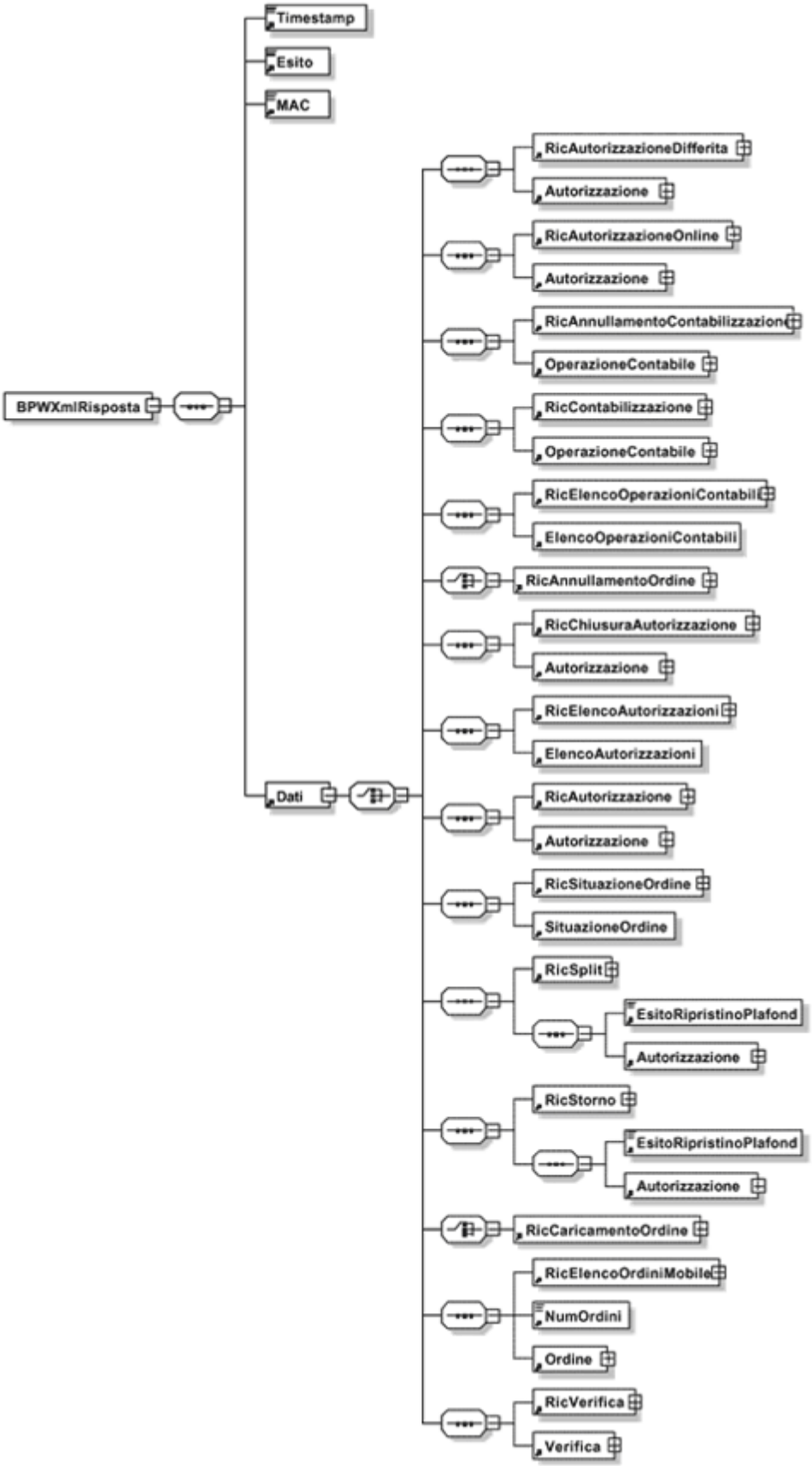
I messaggi di risposta alle richieste sono formattati in XML. Essi contengono tutti i dati della richiesta ed i dati della risposta.

Il prossimo capitolo contiene la descrizione del formato utilizzato per le risposte; in quelli seguenti sono illustrate approfonditamente le varie funzioni disponibili raggruppate in:

- Operazioni sulle autorizzazioni differite
- Operazioni sulle autorizzazioni immediate
- Consultazioni

I messaggi di risposta in XML

Nel presente viene data una descrizione generale del formato XML utilizzato per trasmettere i messaggi di risposta.e vengono illustrati nel dettaglio gli elementi che sono comuni a molti dei messaggi stessi
Nel diagramma che segue viene riportata una panoramica del formato XML sopra citato.


BPWXmlRisposta
Timestamp
Esito
MAC
Dati
RicAutorizzazioneDifferita
Autorizzazione
RicAutorizzazioneOnline
Autorizzazione
RicAnnullamentoContabilizzazion
OperazioneContabile
RicContabilizzazione
OperazioneContabile
RicElencoOperazioniContabil
ElencoOperazioniContabili
RicAnnullamentoOrdine
RicChiusuraAutorizzazione
Autorizzazione
RicElencoAutorizzazioni
ElencoAutorizzazioni
RicAutorizzazione
Autorizzazione
RicSituazioneOrdine
SituazioneOrdine
RicSplit
EsitoRipristinoPlafond
Autorizzazione
RicStorno
EsitoRipristinoPlafond
Autorizzazione
RicCaricamentoOrdine
RicElencoOrdiniMobile
NumOrdini
Ordine
RicVerifica
Verifica

Come si può vedere tutti i messaggi hanno un unico root element: BPWXmlRisposta. Ogni messaggio contiene tutti i dati salienti della richiesta , ed i dati forniti in risposta. Gli elementi della risposta sono presenti solo se non si verificano errori.

Il parsing delle risposte XML effettuato non deve essere validante: grazie alla evoluzione del sistema in futuro potranno essere aggiunti ulteriori elementi ai messaggi. Le applicazioni devono ignorare gli elementi sconosciuti senza provocare malfunzionamenti.

Alcuni elementi come detto sono comuni a molti messaggi di risposta. In particolare di seguito vengono illustrati gli elementi <BPWXmlRisposta> , <Autorizzazione> ed <OperazioneContabile>

Elemento <BPWXmlRisposta>

Questo è il root element di tutti i documenti di risposta, esiste un unico elemento di questo tipo nel messaggio: di seguito viene riportato un esempio nel quale è stata eliminata la parte dell'elemento dati.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
.....
    </Dati>
</BPWXmlRisposta>
```

<BPWXmlRisposta>

- **<Timestamp>** la data e l'ora del messaggio di risposta formato yyyy-MM-ddTHH:mm:ss
- **<Esito>** l'esito dell'operazione di richiesta

Codice	Descrizione
00	Successo
01	Ordine, o ReqRefNum non trovato
02	ReqRefNum duplicato o non valido
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
05	Data errata, o periodo indicato vuoto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
08	Operatore indicato non trovato
09	IDTRANS indicato non fa riferimento al NUMORD passato
10	Importo indicato superiore al massimo consentito
11	Stato errato. Operazione non possibile nello stato attuale
12	Circuito non abilitato
13	Ordine duplicato
20	La carta è abilitata a VBV/SecureCode/SafeKey;la risposta contiene i dati per la redirezione verso sito ACS
21	Tempo massimo per inoltrare la richiesta VBV step 2 scaduto
35	Nessuno strumento di pagamento accettabile
37	CVV2 mancante: per il circuito scelto è obbligatorio

38	Alias dell'ordine non trovato o revocato
40	Xml vuoto o parametro ‘data’ mancante
41	Xml non parsabile
98	Errore applicativo
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **`<MAC>`** firma del timestamp e dell’esito (vedi appendice D11)
- **`<Dati>`** i dati della richiesta di autorizzazione e del messaggio di risposta

In caso di crash applicativi non previsti (esito 98), il tag **`<Dati>`** non è presente e il MAC assume valore NULL:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>98</Esito>
    <MAC>NULL</MAC>
</BPWXmlRisposta>
```

Elemento <Autorizzazione>

Questo elemento descrive una generica autorizzazione, sia immediata che differita.

Sotto viene riportato un esempio in XML di tale elemento

```
<Autorizzazione>
    <TipoPag>03</ TipoPag>
    <Tautor>I</Tautor>
    <IDtrans> C3556456584575645645656 36</IDtrans>
    <Circuito>01</Circuito>
    <NumOrdine>A398459</NumOrdine>
    <ImportoTrans>10000</ImportoTrans>
    <ImportoAutor>10000</ImportoAutor>
    <Valuta>978</Valuta>
    <ImportoContab>10000</ImportoContab>
    <ImportoStornato>100</ImportoStornato>          → presente se passato RELEASE=02 nella richiesta
    <EsitoTrans>00</EsitoTrans>
    <Timestamp>2001-07-09T21:05:44</Timestamp>
    <NumAut>A93485</NumAut>
    <AcqBIN>123450943</AcqBIN>
    <CodiceEsercente>0983473569324509</CodiceEsercente>
    <Stato>01</Stato>
    <ResponseCodeISO>00</ResponseCodeISO>
    <!-- Questa MAC firma la autorizzazione  -->
    <MAC>3204989a63de6ae849c930kd834oes83</MAC>
</Autorizzazione>
```

Di seguito sono riportati i sottoelementi con i rispettivi significati:

`<Autorizzazione>`

- **`<TipoPag>`** il tipo di pagamento concesso

Codice	Descrizione
03	SSL
04	VBV : esercente e consumatore aderenti VBV
05	SecureCode : esercente e consumatore aderenti a SecureCode
06	VBV Esercente : esercente aderente VBV e consumatore non aderente
07	SecureCode Esercente : esercente aderente SecureCode e consumatore non aderente
08	VBV Titolare non autenticato : esercente aderente VBV; il consumatore non si è autenticato correttamente
09	Mail order/Telephone order
13	SafeKey: esercente e consumatore aderenti a SafeKey
14	SafeKey Esercente: esercente aderente a SafeKey e consumatore non aderente
15	SafeKey Titolare non autenticato: esercente aderente a SafeKey; il consumatore non si è autenticato correttamente

- **<Tautor>** il tipo di autorizzazione concessa:
  D=Differita,
  I=Immediata
- **<IDtrans>** l'identificatore della transazione assegnato da @POS
- **<Circuito>** il codice del circuito:

Codice	Descrizione
01	Visa
02	Mastercard
04	Maestro
06	Amex
07	Diners
08	JCB
09	Pagobancomat
94	Postepay
96	MyBank
97	PayPal

- **<NumOrdine>** il codice dell'ordine
- **<ImportoTrans>** l'importo della transazione in centesimi di euro
- **<ImportoAutor>** l'importo autorizzato in centesimi di euro. Se autorizzazione negata è uguale a zero
- **<Valuta>** il codice ISO della valuta: 978=Euro
- **<ImportoContab>** l'importo contabilizzato in centesimi di euro.
- **<ImportoStornato>** l'importo stornato in centesimi di euro *(introdotto dalla Release 02. E' presente solo se nella richiesta viene specificato il parametro **RELEASE=02**)*
- **<EsitoTrans>** l'esito della transazione

Codice	Descrizione
00	Successo
01	Negata problemi nel messaggio di richiesta
02	Negata per problemi sull'anagrafica negozio
03	Negata per problemi di comunicazione con i circuiti autorizzativi
04	Negata dall'emittente della carta
05	Negata per numero carta errato
06	Errore imprevisto durante l'elaborazione della richiesta
45	Autorizzazione negata per filtro carte estere.
99	Autorizzazione in corso con MyBank

- **<Timestamp>** la data e l'ora della transazione in formato yyyy-mm-ggTHH:mm:ss
- **<NumAut>** il codice di autorizzazione (valorizzato in caso di esito positivo). E' una stringa di lunghezza massima 6 caratteri per tutti i circuiti escluso MyBank per il quale invece ha lunghezza fissa di 35 caratteri e contiene l'identificativo della transazione assegnato dal Validation Service. Non è significativo nel caso di transazione effettuata con circuito Paypal
- **<AcqBIN>** l'aquirer bin. Codice identificativo internazionale dell'acquirer
- **<CodEsercente>** il codice dell'esercente assegnato dall'acquirer
- **<Stato>** lo stato corrente della autorizzazione

Si differenzia se autorizzazione immediata o differita:

Immediata

Codice	Descrizione
00	Autorizzazione concessa, contabilizzabile
01	Autorizzazione negata
02	Autorizzazione contabilizzata da elaborare
03	Autorizzazione contabilizzata elaborata dal clearing
04	Autorizzazione stornata
21	Autorizzazione da stornare per errore nella transazione
99	Autorizzazione in corso con MyBank

Differita

Codice	Descrizione
10	Autorizzazione differita aperta
11	Autorizzazione differita chiusa

- **<ResponseCodeISO>** Informazione presente solo per le sezioni Autorizzazione in risposta ad un messaggio autorizzativo (Autorizzazione Online, Differita o VBV) e per i negozi che aderiscono al servizio "SV53 - Fornisci ResponseCodeISO nelle autorizzazioni con le API". Contiene il codice di esito ricevuto dal circuito di riferimento.

- **<MAC>** la firma dell'autorizzazione (vedi appendice D13)

Elemento <OperazioneContabile>

Questo elemento rappresenta una generica operazione contabile

```
<OperazioneContabile>
    <IDtrans>C5555358794</IDtrans>
    <TimestampRic>2001-07-04T22:02:55</TimestampRic>
    <TimestampElab>NULL</TimestampElab>
    <TipoOp>01</TipoOp>
    <Importo>10000</Importo>
    <Esito>00</Esito>
    <Stato>00</Stato>
    <DescrOp>StornoOrdineA398459Tentativo1</DescrOp>
    <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
    <MAC>12334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
    <Autorizzazione>
.....
```

```
        </Autorizzazione>
    </OperazioneContabile>
```

<OperazioneContabile>
L'elemento racchiude i dati relativi all'operazione contabile rappresentati dai seguenti elementi:

- **<IDtrans>** l'identificatore della transazione dell'operazione contabile
- **<TimestampRic>** la data e l'ora della richiesta formato yyyy-MM-ddTHH:mm:ss
- **<TimestampElab>** la data e l'ora dell'elaborazione formato yyyy-MM-ddTHH:mm:ss
- **<TipoOp>** il tipo di operazione contabile

Codice	Descrizione
01	Storno autorizzazione
02	Operazione di credit
03	Annullamento contabilizzazione
04	Operazione di contabilizzazione

- **<Importo>** l'importo dell'operazione contabile in centesimi di euro
- **<Esito>** esito della operazione

Codice	Descrizione
00	Successo
01	Termini scaduti
02	Negata per problemi sull'anagrafica negozio
03	Negata per problemi di comunicazione con i circuiti autorizzativi
04	Negata dall'emittente della carta
05	Plafond non ripristinato
06	Errore imprevisto durante l'elaborazione della richiesta

- **<Stato>** stato della operazione

Codice	Descrizione
00	Terminata con successo
01	Fallita

- **<DescrOp>** descrizione facoltativa eventualmente associata all'operazione contabile
- **<MAC>** la firma della operazione contabile (vedi appendice D12)
- **<Autorizzazione>** i dati dell'autorizzazione che è stata oggetto dell'operazione contabile

Richiesta di autorizzazione online

Il messaggio di richiesta di autorizzazione online permette di inoltrare ai circuiti richieste di autorizzazione.
I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

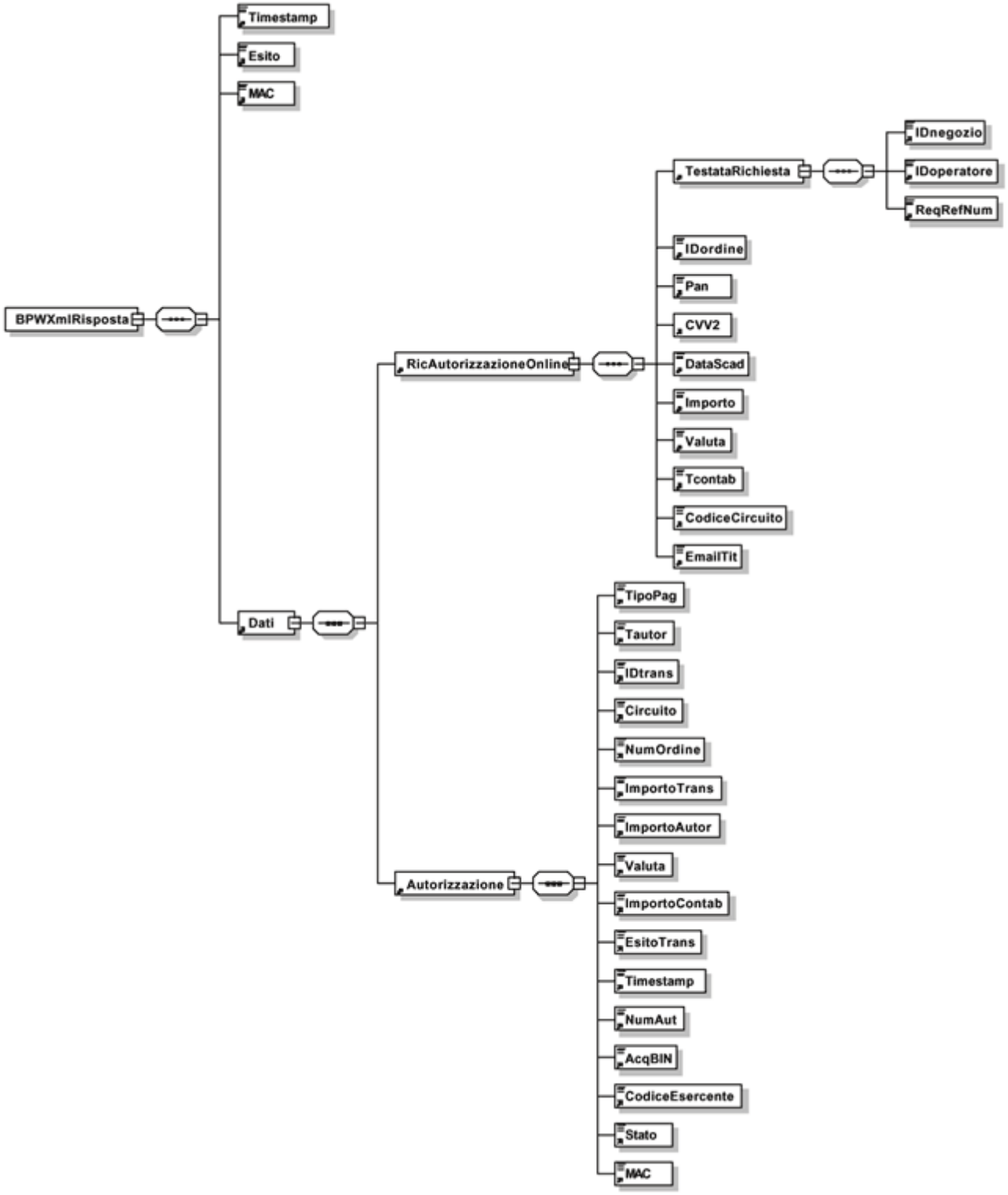
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "AUTORIZZAZIONEONLINE"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ggTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA , (Merchant ID)
IDORDINE	Y	Min. 1 Max.50	AN	Identificatore univoco dell'ordine
IDOPERATORE	Y	Min. 8 Max.18	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
PAN	Y	Min. 10 Max.19	AN	Numero della carta
CVV2	N	Min. 3 Max.4	N	Codice di controllo associato al numero della carta (opzionale)
DATASCAD	Y	4	N	Data di scadenza della carta – yyMM-
IMPORTO	Y	Min. 2 Max. 8	N	Importo espresso nell'unità minima della valuta (centesimi di euro). L'importo minimo è 10 centesimi. L'importo non deve essere preceduto da zeri.
VALUTA	Y	3	N	Valuta: codice ISO (EURO = 978).
TCONTAB	Y	1	AN	Tipo di contabilizzazione da utilizzare per questo ordine: • D Differita • I Immediata
CODICECIRCUITO	Y	2	N	Il circuito di autorizzazione della carta (ad es: 01 per VISA). Nel caso in cui il merchant non fosse in possesso del codice circuito è possibile delegare al sistema ATPOS il calcolo dello stesso semplicemente impostando come CODICECIRCUITO il valore 93.
EMAILTIT	N	Min. 7 Max. 50	AN	E-mail del titolare della carta (opzionale)
USERID	N	Min. 1 Max. 30	AN	Identificativo del titolare
ACQUIRER	N	5	N	Codice dell'acquirer con cui si vuole effettuare la transazione
IPADDRESS	N	Min. 7 Max. 15	AN	Indirizzo IP associato alla richiesta
DESCROP	N	100	AN	Descrizione aggiuntiva della contabilizzazione a discrezione dell'esercente, per autorizzazioni con contabilizzazione immediata. In caso di contabilizzazione differita il campo viene ignorato.
RELEASE	N	2	N	Release delle API: da valorizzare con "02"

MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D15

Richiesta di autorizzazione online in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
<Release>02</Release>
<Richiesta>
<Operazione>AUTORIZZAZIONEONLINE</Operazione>
<Timestamp>2005-02-08T12:02:00.000</Timestamp>
<MAC>115025d5a5b65df687790867bdece136</MAC>
</Richiesta>
    <Dati>
<RicAutorizzazioneOnline>
        <TestataRichiesta>
            <IDnegozio>000000000000003</IDnegozio>
            <IDoperatore>oper0001</IDoperatore>
            <ReqRefNum>123456789012345678901234522890000</ReqRefNum>
        </TestataRichiesta>
                    <IdOrdine>1234567890</IdOrdine>
                    <Pan>9998500000000015</Pan>
                    <CVV2>123</CVV2>
                    <DataScad>0409</DataScad>
                    <Importo>4450</Importo>
                    <Valuta>978</Valuta>
                    <Tcontab>I</Tcontab>
                    <CodiceCircuito>01</CodiceCircuito>
                    <EmailTit>indirizzo@societa.com</EmailTit>
                    <Userid>user1</Userid>
                    <DescrOp>RichiestaCallCenter1037</ DescrOp >
                </RicAutorizzazioneOnline>
            </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di autorizzazione è formattato in XML ed è schematizzato nella pagina successiva.



Come si può notare la risposta ad una richiesta di autorizzazione è sostanzialmente costituita da un elemento di tipo Autorizzazione.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento Autorizzazione non viene creato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di autorizzazione online:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <BPWXmlRisposta>
    <Timestamp>2003-04-09T12:02:38</Timestamp>
    <Esito>00</Esito>
  - <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>8A74330BA1A1A085581EAA2409D8DC68FCC4395E</MAC>
  - <Dati>
    - <!-- L'elemento che segue contiene i dati della richiesta fatta -->
    - <RicAutorizzazioneOnline>
      - <TestataRichiesta>
          <IDnegozio>000000000000003</IDnegozio>
          <IDoperatore>AD456123</IDoperatore>
          <ReqRefNum>200305019012345678901234522890000</ReqRefNum>
        </TestataRichiesta>
        <IDordine>p91</IDordine>
        <Pan>999850xxxxxx0015</Pan>
        <CVV2>000</CVV2>
        <DataScad>0409</DataScad>
        <Importo>4450</Importo>
        <Valuta>978</Valuta>
        <Tcontab>I</Tcontab>
        <CodiceCircuito>01</CodiceCircuito>
        <EmailTit>info@titolare.it</EmailTit>
        <Userid>user1</Userid>
        <DescrOp>RichiestaCallCenter1037</ DescrOp >
      </RicAutorizzazioneOnline>
    - <Autorizzazione>
        <TipoPag>03</TipoPag>
        <Tautor>I</Tautor>
        <IDtrans>8032180310AB0E30917930112</IDtrans>
        <Circuito>01</Circuito>
        <NumOrdine>pos91</NumOrdine>
        <ImportoTrans>4450</ImportoTrans>
        <ImportoAutor>4450</ImportoAutor>
        <Valuta>978</Valuta>
        <ImportoContab>0</ImportoContab>
        <ImportoStornato>100</ImportoStornato>
        <EsitoTrans>00</EsitoTrans>
        <Timestamp>2003-04-09T12:02:38</Timestamp>
        <NumAut>622851</NumAut>
        <AcqBIN>453997</AcqBIN>
        <CodiceEsercente>000000000000476</CodiceEsercente>
        <Stato>02</Stato>
      - <!-- Questa MAC firma i dati dell'autorizzazione -->
        <MAC>0EA6645D79E9752BE05800BE9CFE623CE3973395</MAC>
      </Autorizzazione>
  </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta . Possibili esiti:

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
37	CVV2 mancante
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
98	Errore applicativo
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito (vedi appendice D15)
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAutorizzazioneOnline>** i dati della richiesta di autorizzazione
- **<Autorizzazione>** i dati del messaggio di risposta

<RicAutorizzazioneOnline>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDordine>** l'identificatore dell'ordine
- **<Pan>** il numero della carta oscurato (in chiaro solo le prime sei cifre e le ultime quattro)
- **<CVV2>** il numero aggiuntivo della carta oscurato (sequenza di zeri di lunghezza pari alla lunghezza del campo nella richiesta)
- **<DataScad>** la data di scadenza della carta
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro
- **<Tcontab>** il tipo di contabilizzazione da utilizzare: D=Differita, I=Immediata
- **<CodiceCircuito>** il circuito autorizzativo della carta
- **<EmailTit>** l'e-mail del titolare
- **<Userid>** identificativo del titolare
- **<DescrOp>** descrizione facoltativa eventualmente associata alla contabilizzazione
- **<Acquirer>** codice acquirer

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<IDOperatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** l'identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati dell'autorizzazione. Per la sua descrizione si veda il paragrafo opportuno del capitolo "I messaggi di risposta in XML"

Richiesta di autorizzazione differita

Il messaggio di richiesta di autorizzazione differita permette di inoltrare ai circuiti richieste di autorizzazione.
I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "AUTORIZZAZIONEDIFFERITA"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ggTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA , (Merchant ID)
IDORDINE	Y	Min. 1 Max.50	AN	Identificatore univoco dell'ordine
IDOPERATORE	Y	Min. 8 Max.18	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
PAN	Y	Min. 10 Max.19	AN	Numero della carta
CVV2	N	Min. 3 Max.4	N	Codice di controllo associato al numero della carta (opzionale)
DATASCAD	Y	4	N	Data di scadenza della carta – yyMM-
IMPORTO	Y	Min. 2 Max. 8	N	Importo espresso nell'unità minima della valuta (centesimi di euro)
VALUTA	Y	3	N	Valuta: codice ISO (EURO = 978).
CODICECIRCUITO	Y	2	N	Il circuito di autorizzazione della carta (ad es: 01 per VISA). Nel caso in cui il merchant non fosse in possesso del codice circuito è possibile delegare al sistema ATPOS il calcolo dello stesso semplicemente impostando come CODICECIRCUITO il valore 93.
EMAILTIT	N	Min. 7 Max. 50	AN	E-mail del titolare della carta (opzionale)
USERID	N	Min. 1 Max. 30	AN	Udentificativo del titolare
ACQUIRER	N	5	N	Codice dell'acquirer con cui si vuole effettuare la transazione
IPADDRESS	N	Min. 7 Max. 15	AN	Indirizzo IP associato alla richiesta
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D16

Richiesta di autorizzazione differita in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>AUTORIZZAZIONEDIFFERITA</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicAutorizzazioneDifferita>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <IDoperatore>oper0001</IDoperatore>
                <ReqRefNum>123422229012345678901234567890000</ReqRefNum>
            </TestataRichiesta>
            <IDordine>1234567890</IDordine>
            <Pan>9998500000000015</Pan>
            <CVV2>123</CVV2>
            <DataScad>0409</DataScad>
            <Importo>7700</Importo>
            <Valuta>978</Valuta>
            <CodiceCircuito>01</CodiceCircuito>
            <EmailTit>indirizzo@societa.com</EmailTit>
            <Userid>user1 </Userid>
        </RicAutorizzazioneDifferita>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di autorizzazione è formattato in XML ed è schematizzato di seguito.

Come si può notare la risposta ad una richiesta di autorizzazione è sostanzialmente costituita da un elemento di tipo Autorizzazione.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento Autorizzazione non viene creato.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
 <BPWXmlRisposta>
     <Timestamp>2003-04-09T12:31:53</Timestamp>
     <Esito>00</Esito>
     <!-- Questa MAC firma il timestamp e l'esito -->
     <MAC>A267CA27F38D45DDFA0CBCE5E4FCF4757B31AF1A</MAC>
     <Dati>
       <!-- L'elemento che segue contiene i dati della richiesta fatta -->
       <RicAutorizzazioneDifferita>
           <TestataRichiesta>
              <IDnegozio>000000000000003</IDnegozio>
              <IDoperatore>AD435639</IDoperatore>
              <ReqRefNum>200305019012345678901234567890000</ReqReNum>
           </TestataRichiesta>
           <IDordine>Ordine 92</IDordine>
           <Pan>999850xxxxxx0015</Pan>
          <CVV2>000</CVV2>
           <DataScad>0409</DataScad>
           <Importo>7700</Importo>
           <Valuta>978</Valuta>
           <Tcontab>I</Tcontab>
           <CodiceCircuito>01</CodiceCircuito>
           <EmailTit>info@titolare.it</EmailTit>
           <Userid>user1</Userid>
        </RicAutorizzazioneDifferita>
        <Autorizzazione>
        <TipoPag>03</TipoPag>
           <Tautor>D</Tautor>
           <IDtrans>8032180310ABW81219P890320</IDtrans>
           <Circuito>01</Circuito>
           <NumOrdine>Ordine 92</NumOrdine>
           <ImportoTrans>7700</ImportoTrans>
           <ImportoAutor>0</ImportoAutor>
           <Valuta>978</Valuta>
           <ImportoContab>0</ImportoContab>
           <ImportoStornato>100</ImportoStornato>
           <EsitoTrans>00</EsitoTrans>
           <Timestamp>2003-04-09T12:31:53</Timestamp>
           <NumAut />
           <AcqBIN>453997</AcqBIN>
           <CodiceEsercente>000000000000476</CodiceEsercente>
           <Stato>10</Stato>
           <!-- Questa MAC firma i dati dell'autorizzazione -->
           <MAC>EFF17F3A871E1D9C2D62F59EFF5798624A27B795</MAC>
       </Autorizzazione>
     </Dati>
 </BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta . Possibili esiti:

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato

03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito (vedi appendice D16)
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAutorizzazioneDifferita>** i dati della richiesta di autorizzazione
- **<Autorizzazione>** i dati del messaggio di risposta

<RicAutorizzazioneDifferita>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDordine>** l'identificatore dell'ordine
- **<Pan>** il numero della carta oscurato (in chiaro solo le prime sei cifre e le ultime quattro)
- **<CVV2>** il numero aggiuntivo della carta oscurato (sequenza di zeri di lunghezza pari alla lunghezza del campo nella richiesta)
- **<DataScad>** la data di scadenza della carta
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro
- **<CodiceCircuito>** il circuito autorizzativo della carta
- **<EmailTit>** l'e-mail del titolare
- **<Userid>** identificativo del titolare

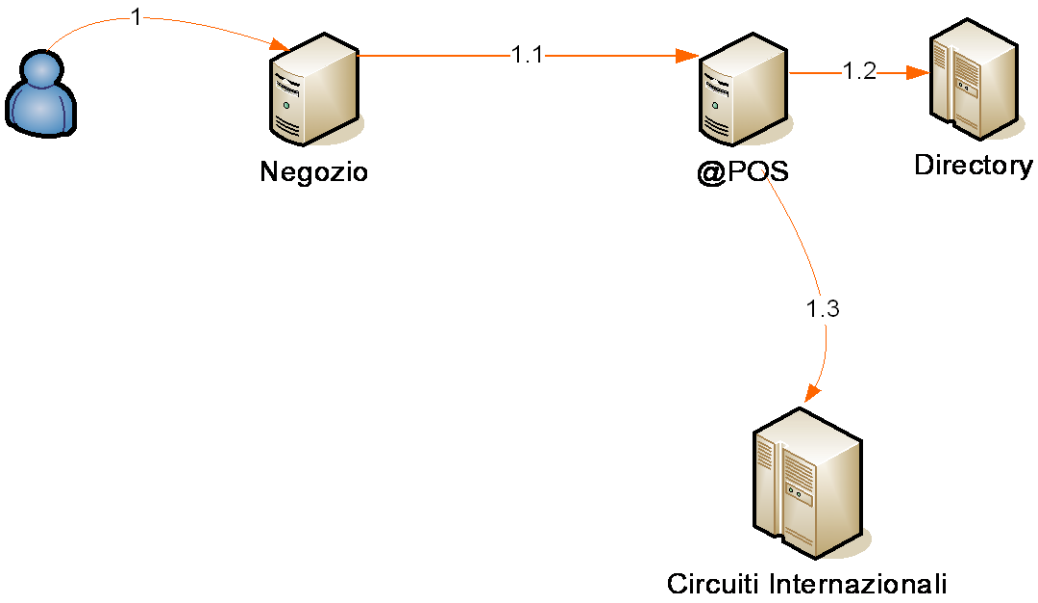
<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<IDOperatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** l'identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati dell'autorizzazione immediata richiesta. Per la sua descrizione si veda il paragrafo opportuno del capitolo "I messaggi di risposta in XML"

Le autorizzazioni Verified By Visa per le carte Visa, SecureCode per le carte Mastercard/Maestro e SafeKey per le carte Amex (di seguito VBV) si applicano solo alle carte Visa, Mastercard/Maestro e Amex che siano abilitate a tale sistema di sicurezza. Nonostante questa premessa l'integrazione @POS offre un'unica interfaccia per trattare tutti i tipi di carte di credito; ovviamente per le carte che risultano abilitate a VBV il comportamento del sistema è necessariamente particolare.

Di seguito viene riportato lo schema di funzionamento del sistema nei due scenari possibili.



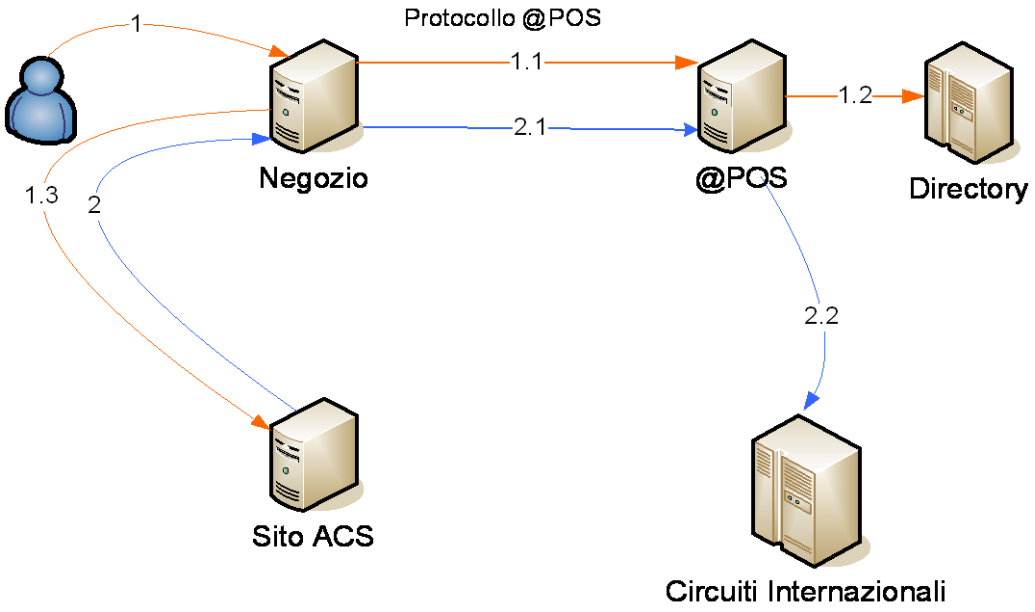
1. L'utente è connesso al sito del negozio ed inserisce i dati della carta di credito.

   1.1. Il negozio inizia il processo di richiesta autorizzazione, qualsiasi sia la carta, semplicemente inoltrando un messaggio di tipo AUTORIZZAZIONEONLINEVBV al sistema @POS

   1.2. Nel caso sia indicato che si tratta di una carta Visa/Mastercard/Maestro/Amex, @POS si collega alle directory opportune e verifica se la carta è abilitata al servizio VBV

   1.3. Se la carta non è abilitata a VBV (o non è Visa/Mastercard/Maestro/Amex VBV o si tratti di richiesta PAYPASS) @POS inoltra direttamente un messaggio autorizzativo ai circuiti internazionali. La risposta fornita al sito del negozio contiene l'esito della transazione. Lo scenario si conclude qui.

Se al passo 1.2 il sistema @POS rileva che la carta è abilitata al servizio VBV allora si innesca lo scenario VBV che prosegue così:



1.3. Se la carta è abilitata a VBV la risposta al messaggio di 1.1 invece di contenere il risultato della transazione contiene i dati per la redirect dell'utente verso il sito ACS dell'emittente della carta (Issuer). Il negozio crea i parametri **MD** (merchant data) e **TermURL** (URL di ritorno) ed esegue la redirect

2. L'utente, connesso al sito ACS, inserisce la sua password e viene rediretto nuovamente verso il sito del negozio portando con se i parametri **MD** e **PaRes**.

2.3. Il negozio, con i dati arrivati da ACS, compila un messaggio di tipo AUTORIZZAZIONEONLINEVBV2 e lo manda al sistema @POS. **Il messaggio 2.1 deve arrivare entro 8 minuti dal messaggio 1.1**

2.4. @POS decodifica i dati ACS, inoltra la richiesta di autorizzazione ai circuiti internazionali, e fornisce quindi l'esito della transazione come risposta al messaggio AUTORIZZAZIONEONLINEVBV2

In sostanza il negozio deve inoltrare le richieste di autorizzazione con dei messaggi AUTORIZZAZIONEONLINEVBV e verificare l'esito della risposta. Se la risposta è del tipo "carta abilitata VBV" deve intraprendere il workflow VBV e redirigere l'utente verso il sito ACS.

La redirezione in oggetto deve essere effettuata tramite POST con parametri opportuni.
Nella pagina seguente vi è una banale esemplificazione HTML/Javascript.

```
<html>
<head>
<script language="Javascript">
function OnLoadEvent()
{
document.downloadForm.submit();
}
</script>
</head>
<body OnLoad="OnLoadEvent();">
<form name="downloadForm" action="${URLACS}" method="POST">
        <input type="hidden" name="PaReq" value="${PAREQ}">
        <input type="hidden" name="TermUrl" value="http://www.sito.it/negozio/daacs">
        <input type="hidden" name="MD" value="base64">
</form>
</body>
</html>
```

I nomi **PaReq, TermUrl** ed **MD** sono parte dello standard VBV e devono essere così specificati. I valori tra ${} rappresentano i valori trasmessi dal sistema @POS.

TermUrl è la URL dove l'utente viene rediretto dopo l'autenticazione VBV da parte del sito ACS dell'issuer della carta. Non puo' contenere parametri, ne attributi.
MD sta per Merchant Data. Il merchant può valorizzarla come vuole, ACS restituirà quanto ricevuto. Il campo è considerato in Base64 perciò solo i caratteri facenti parte di tale codifica sono accettati.

Nei paragrafi successivi si trovano le specifiche di dettaglio dei messaggi @POS e delle relative risposte.

Il processo VBV completo prevede la presenza online del titolare della carta di credito, non sono perciò possibili autorizzazioni di questo tipo in "batch" automatizzati. Nonostante ciò l'interfaccia @POS prevede la possibilità di indicare che l'utente non è disponibile. In questo caso l'operazione verrà portata a termine solo se la carta non è abilitata al servizio VBV/SecureCode/SafeKey o se non è una carta Visa/Mastercard/Maestro/Amex VBV.

Richiesta di autorizzazione online VBV

Il messaggio di richiesta di autorizzazione online permette di inoltrare ai circuiti richieste di autorizzazione. Nel caso di carte Visa, Masterdard/Maestro o Amex VBV la richiesta può essere di tipo VBV.
I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "AUTORIZZAZIONEONLINEVBV"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ggTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA , (Merchant ID)
IDORDINE	Y	Min. 1 Max.50	AN	Identificatore univoco dell'ordine
IDOPERATORE	Y	Min. 8 Max.18	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
PAN	Y	Min. 10 Max.19	AN	Numero della carta
CVV2	N	Min. 3 Max.4	N	Codice di controllo associato al numero della carta (opzionale)
DATASCAD	Y	4	N	Data di scadenza della carta – yyMM-
IMPORTO	Y	Min. 2 Max. 8	N	Importo espresso nell'unità minima della valuta (centesimi di euro)
VALUTA	Y	3	N	Valuta: codice ISO (EURO = 978).
TCONTAB	Y	1	AN	Tipo di contabilizzazione da utilizzare per questo ordine: • D Differita • I Immediata
CODICECIRCUITO	Y	2	N	Il circuito di autorizzazione della carta (ad es: 01 per VISA). Nel caso in cui il merchant non fosse in possesso del codice circuito è possibile delegare al sistema ATPOS il calcolo dello stesso semplicemente impostando come CODICECIRCUITO il valore 93.
EMAILTIT	N	Min. 7 Max. 50	AN	E-mail del titolare della carta (opzionale)
USERID	N	Min. 1 Max. 30	AN	Identificativo del titolare
ACQUIRER	N	5	N	Codice dell'acquirer con cui si vuole effettuare la transazione
IPADDRESS	N	Min. 7	AN	Indirizzo IP associato alla richiesta

		Max. 15		
DESCROP	N	100	AN	Descrizione aggiuntiva della contabilizzazione a discrezione dell'esercente, per autorizzazioni con contabilizzazione immediata. In caso di contabilizzazione differita il campo viene ignorato.
RELEASE	N	2	N	Release delle API: da valorizzare con “02”
PRESENTE	N	1	A	Indica se l’utente titolare della carta è presente o meno e se può quindi essere coinvolto per l’autenticazione VBV. Valori possibili: S/N . Default a N
URLMERCHANT	N	255	AN	URL del sito del negozio. E’ obbligatorio se PRESENTE S e CIRCUITO 01 o 02. I caratteri accettati sono quelli permessi dalla seguente regula expression: `[A-Za-z0-9_\-/:. ]`
SERVIZIO	N	4	AN	Campo obbligatorio se si vuole specificare che si tratta di una richiesta di autorizzazione con servizio PAYPASS. In questo caso il valore da indicare è SV47
XID	N	40	AN	identificativo univoco della transazione 3D. Formato BASE 64.
CAVV	N	40	AN	Cardholder Authentication Verification Value: valore generato dall’issuer e presente a seguito di autenticazione 3D avvenuta con successo da parte del titolare della carta. Formato BASE 64
ECI	N	2	N	Electronic Commerce Indicator : Presente se il campo PARESSTATUS ha valore “Y” o “A”. Possibili valori per Visa sono: 1) 05 e 06 (Card Issuer Liability) 2) 07 (Merchant Liability) Possibili valori per Mastercard sono: 1) 01 (Merchant Liability) 2) 02 (Card Issuer Liability)
PP_AUTHENTICATEMETHOD	N	Min 3 Max 20	AN	Metodo di autenticazione usato dal titolare della carta. Possibili valori sono: 1) MERCHANT ONLY: Transazione non autenticata con metodi aggiuntivi 2) 3DS: Transazione autenticata con 3DS 3) NO AUTHENTICATION: Transazione non 3DS
PP_CARDENROLLMETHOD	N	Min 6 Max 20	AN	Metodo usato per validare la carta e il titolare al momento dell’aggiunta della carta nel wallet PAYPASS. Possibili valori sono: 1) Manual: Carta aggiunta manualmente nel wallet PAYPASS 2) Direct Provisioned : Carta aggiunta nel wallet PAYPASS attraverso un Issuer 3) 3DS Manual: Carta aggiunta manualmente nel wallet PAYPASS e verificata 3DS al momento dell’aggiunta. 4) NFC Tap: Carta PAYPASS aggiunta al wallet attraverso un NFC-enabled Ultrabook’s NFC reader.
PARESSTATUS	N	1	AN	Codice di esito dell’autenticazione del titolare. Possibili valori sono: 1) Y: Titolare autenticato con successo al 3D 2) N: Fallita autenticazione del titolare 3) A: Transazione con Attempt 4) U: Risultato della autenticazione non disponibile

SCENROLLSTATUS	N	1	AN	Indica se l'issuer della carta supporta l'autenticazione 3D. Possibili valori sono: 1) Y: carta abilitata a transazioni 3D 2) N: carta non abilitata a transazioni 3D 3) U: abilitazione non disponibile o non applicabile al tipo di carta
SIGNATUREVERIFICATION	N	1	AN	Esito della verifica della firma della PARes. Possibili valori sono: 1) Y: la firma della PARes è stata validata con successo 2) N: la firma della PARes non è stata validata con successo (es: certificato scaduto)
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D17

Richiesta di autorizzazione online VBV in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>AUTORIZZAZIONEONLINEVBV</Operazione>
        <Timestamp>2007-02-08T12:02:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicAutorizzazioneOnline>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <IDoperatore>oper0001</IDoperatore>
                <ReqRefNum>123456789012345678901234522890000</ReqRefNum>
            </TestataRichiesta>
            <IdOrdine>1234567890</IdOrdine>
            <Pan>9998500000000015</Pan>
            <CVV2>123</CVV2>
            <DataScad>0409</DataScad>
            <Importo>4450</Importo>
            <Valuta>978</Valuta>
            <Tcontab>I</Tcontab>
            <CodiceCircuito>01</CodiceCircuito>
            <EmailTit>indirizzo@societa.com</EmailTit>
            <Userid>user1</Userid>
            <DescrOp>RichiestaCallCenter1037</ DescrOp >
            <Presente>S</Presente >
            <URLMerchant >http://www.sito.com </URLMerchant>
        </RicAutorizzazioneOnline>
    </Dati>
</BPWXmlRichiesta>
```

Nel caso in cui la carta indicata nella richiesta non è abilitata a VBV (o non è Visa/Mastercard/Maestro/Amex VBV o si tratti di richiesta PAYPASS), il sistema procede immediatamente ad inoltrare la transazione ai circuiti. In questo caso la risposta conterrà il risultato vero e proprio della richiesta di autorizzazione.

Se la carta è abilitata a VBV la risposta del sistema sarà un elemento che contiene i dati necessari al sito dell'esercente per redirigere il compratore al sito dell'ACS dell'issuer della sua carta per l'autenticazione.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di autorizzazione online per transazione avvenuta per carta non abilitata a VBV o non Visa/Mastercard/Maestro/Amex VBV:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <BPWXmlRisposta>
    <Timestamp>2007-04-09T12:02:38</Timestamp>
    <Esito>00</Esito>
  - <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>8A74330BA1A1A085581EAA2409D8DC68FCC4395E</MAC>
  - <Dati>
    - <!-- L'elemento che segue contiene i dati della richiesta fatta -->
    - <RicAutorizzazioneOnline>
      - <TestataRichiesta>
          <IDnegozio>000000000000003</IDnegozio>
          <IDoperatore>AD456123</IDoperatore>
          <ReqRefNum>20030501901234567890123452289000</ReqRefNum>
        </TestataRichiesta>
        <IDordine>p91</IDordine>
        <Pan>999850xxxxxx0015</Pan>
        <CVV2>000</CVV2>
        <DataScad>0409</DataScad>
        <Importo>4450</Importo>
        <Valuta>978</Valuta>
        <Tcontab>I</Tcontab>
        <CodiceCircuito>01</CodiceCircuito>
        <EmailTit>info@titolare.it</EmailTit>
        <Userid>user1</Userid>
        <DescrOp>RichiestaCallCenter1037</ DescrOp>
        <Presente>S</Presente >
        <URLMerchant >http://www.sito.com</URLMerchant>
      </RicAutorizzazioneOnline>
    - <Autorizzazione>
        <TipoPag>03</TipoPag>
        <Tautor>I</Tautor>
        <IDtrans>8032180310AB0E30917930112</IDtrans>
        <Circuito>01</Circuito>
        <NumOrdine>pos91</NumOrdine>
        <ImportoTrans>4450</ImportoTrans>
        <ImportoAutor>4450</ImportoAutor>
        <Valuta>978</Valuta>
        <ImportoContab>0</ImportoContab>
        <ImportoStornato>0</ImportoStornato>
        <EsitoTrans>00</EsitoTrans>
        <Timestamp>2003-04-09T12:02:38</Timestamp>
        <NumAut>622851</NumAut>
        <AcqBIN>453997</AcqBIN>
        <CodiceEsercente>000000000000476</CodiceEsercente>
        <Stato>02</Stato>
      - <!-- Questa MAC firma i dati dell'autorizzazione -->
        <MAC>0EA6645D79E9752BE05800BE9CFE623CE3973395</MAC>
      </Autorizzazione>
  </Dati>
</BPWXmlRisposta>
```

Come si può notare la risposta ad una richiesta di autorizzazione è sostanzialmente costituita da un elemento di tipo Autorizzazione.

Richiesta di autorizzazione online VBV in formato XML (transazione con servizio PAYPASS)

Di seguito un esempio di richiesta di autorizzazione online per transazione con servizio PAYPASS:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>AUTORIZZAZIONEONLINEVBV</Operazione>
        <Timestamp>2007-02-08T12:02:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicAutorizzazioneOnline>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <IDoperatore>oper0001</IDoperatore>
                <ReqRefNum>12345678901234567890123452289000</ReqRefNum>
            </TestataRichiesta>
            <Dati3D>
                <Servizio>SV47</Servizio>
                <Eci>05</Eci>
                <Xid>B8B7CBEF5344497639ECB60679A239C7507C8DE0</Xid>
                <CAVV>17000101066123000000032920612310000000000</CAVV>
                <ParesStatus>Y</ParesStatus>
                <ScEnrollStatus>Y</ScEnrollStatus>
                <SignatureVerification>Y</SignatureVerification>
            </Dati3D>
            <DatiPaypass>
                <PP_AuthenticateMethod>3DS</PP_AuthenticateMethod>
                <PP_CardEnrollMethod>Direct Provisioned</PP_CardEnrollMethod>
            </DatiPaypass>
            <IdOrdine>1234567890</IdOrdine>
            <Pan>9998500000000015</Pan>
            <CVV2>123</CVV2>
            <DataScad>0409</DataScad>
            <Importo>4450</Importo>
            <Valuta>978</Valuta>
            <Tcontab>I</Tcontab>
            <CodiceCircuito>01</CodiceCircuito>
            <EmailTit>indirizzo@societa.com</EmailTit>
            <Userid>user1</Userid>
        </RicAutorizzazioneOnline>
    </Dati>
</BPWXmlRichiesta>
```

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di autorizzazione online per transazione con servizio PAYPASS:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
 <BPWXmlRisposta>
    <Timestamp>2007-04-09T12:02:38</Timestamp>
    <Esito>00</Esito>
    <!--  Questa MAC firma il timestamp e l'esito  -->
    <MAC>8A74330BA1A1A085581EAA2409D8DC68FCC4395E</MAC>
    <Dati>
      - <!--  L'elemento che segue contiene i dati della richiesta fatta  -->
       <RicAutorizzazioneOnline>
          <TestataRichiesta>
             <IDnegozio>000000000000003</IDnegozio>
             <IDoperatore>AD456123</IDoperatore>
             <ReqRefNum>20030501901234567890123452289000</ReqRefNum>
          </TestataRichiesta>
          <Dati3D>
```

```
            <Servizio>SV47</Servizio>
            <Eci>05</Eci>
            <Xid>B8B7CBEF5344497639ECB60679A239C7507C8DE0</Xid>
            <CAVV>17000101066123000000032920612310000000000</CAVV>
            <ParesStatus>Y</ParesStatus>
            <ScEnrollStatus>Y</ScEnrollStatus>
            <SignatureVerification>Y</SignatureVerification>
         </Dati3D>
         <DatiPaypass>
            <PP_AuthenticateMethod>3DS</PP_AuthenticateMethod>
            <PP_CardEnrollMethod>Direct Provisioned</PP_CardEnrollMethod>
      </DatiPaypass>
      <IDordine>p91</IDordine>
      <Pan>999850xxxxxx0015</Pan>
      <CVV2>000</CVV2>
      <DataScad>0409</DataScad>
      <Importo>4450</Importo>
      <Valuta>978</Valuta>
      <Tcontab>I</Tcontab>
      <CodiceCircuito>01</CodiceCircuito>
      <EmailTit>info@titolare.it</EmailTit>
      <Userid>user1</Userid>
   </RicAutorizzazioneOnline>
   <Autorizzazione>
      <TipoPag>03</TipoPag>
      <Tautor>I</Tautor>
      <IDtrans>8032180310AB0E30917930112</IDtrans>
      <Circuito>01</Circuito>
      <NumOrdine>pos91</NumOrdine>
      <ImportoTrans>4450</ImportoTrans>
      <ImportoAutor>4450</ImportoAutor>
      <Valuta>978</Valuta>
      <ImportoContab>0</ImportoContab>
      <ImportoStornato>0</ImportoStornato>
      <EsitoTrans>00</EsitoTrans>
      <Timestamp>2003-04-09T12:02:38</Timestamp>
      <NumAut>622851</NumAut>
      <AcqBIN>453997</AcqBIN>
      <CodiceEsercente>000000000000476</CodiceEsercente>
      <Stato>02</Stato>
      <!-- Questa MAC firma i dati dell'autorizzazione -->
      <MAC>0EA6645D79E9752BE05800BE9CFE623CE3973395</MAC>
   </Autorizzazione>
</Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta . Possibili esiti:

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
20	La carta è abilitata a VBV;la risposta contiene i dati per la redirezione verso sito ACS
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito (vedi appendice D11)
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAutorizzazioneOnline>** i dati della richiesta di autorizzazione
- **<Autorizzazione>** i dati del messaggio di risposta

<RicAutorizzazioneOnline>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDordine>** l'identificatore dell'ordine
- **<Pan>** il numero della carta oscurato (in chiaro solo le prime sei cifre e le ultime quattro)
- **<CVV2>** il numero aggiuntivo della carta oscurato (unasequenza di zeri di lunghezza pari alla lunghezza del campo nella richiesta)
- **<DataScad>** la data di scadenza della carta
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro
- **<Tcontab>** il tipo di contabilizzazione da utilizzare: D=Differita, I=Immediata
- **<CodiceCircuito>** il circuito autorizzativo della carta
- **<EmailTit>** l'e-mail del titolare
- **<Userid>** identificativo del titolare se presente nelle richiesta
- **<DescrOp>** descrizione facoltativa eventualmente associata alla contabilizzazione
- **<Acquirer>** codice acquirer se presente nella richiesta
- **<Presente>** utente presente o meno se presente nelle richiesta
- **<URLMerchant>** Url merchant se presente nelle richiesta

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<IDOperatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** l'identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati dell'autorizzazione. Per la sua descrizione si veda il paragrafo opportuno del capitolo "I messaggi di risposta in XML"

Come precedentemente esposto, la risposta nel caso in cui la carta passata sia abilitata a VBV contiene i dati per la redirezione verso il sito dell'ACS dell'Issuer della carta. Del tipo:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <BPWXmlRisposta>
    <Timestamp>2007-04-09T12:02:38</Timestamp>
    <Esito>20</Esito>
   - <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>8A74330BA1A1A085581EAA2409D8DC68FCC4395E</MAC>
   - <Dati>
      - <!-- L'elemento che segue contiene i dati della richiesta fatta -->
      - <RicAutorizzazioneOnline>
         - <TestataRichiesta>
            <IDnegozio>000000000000003</IDnegozio>
            <IDoperatore>AD456123</IDoperatore>
            <ReqRefNum>20030501901234567890123452289000</ReqRefNum>
         </TestataRichiesta>
         <IDordine>p91</IDordine>
         <Pan>999850xxxxxx0015</Pan>
         <CVV2>000</CVV2>
         <DataScad>0409</DataScad>
         <Importo>4450</Importo>
         <Valuta>978</Valuta>
         <Tcontab>I</Tcontab>
         <CodiceCircuito>01</CodiceCircuito>
         <EmailTit>info@titolare.it</EmailTit>
         <Userid>user1</Userid>
         <Presente>S</Presente >
         <URLMerchant >http://www.sito.com</URLMerchant>
</RicAutorizzazioneOnline>
      - <VBVRedir>
         - <!-- L'elemento che segue contiene i dati in base64 della PaReq VBV -->
            <PaReq>agd83kjdhs899lijsfnsky33kslmdfhkaanqcpt03hsxmcnduhasncy
      Agqposcnha830fkvkfsky33kslmdhdhgfhsdfas3hsxmcnduhdfgcy
      </ PaReq >
         <URLAcs>http://www.issuer.com/acs</URLAcs >
         - <!-- Questa MAC firma i dati della redir -->
         <MAC>0EA6645D79E9752BE05800BE9CFE623CE3973395</MAC>
       </VBVRedir >
   </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi VBVRedir è riportato nel seguito:

<VBVRedir>
Questo elemento racchiude i dati relativi alla redirezione VBV:

- **<PaReq>** sono i dati VBV in Base64 da inviare tramite **POST** al sito ACS dell'Issuer della carta
- **<URLAcs>** è la URL del sito ACS dell'Issuer della carta. L'utente deve essere rediretto verso questa URL nelle modalità precedentemente esposte.
- **<MAC>** firma dell'elemento VBVRedir (vedi appendice D19)

Richiesta di autorizzazione online VBV step 2

Il messaggio di richiesta di autorizzazione online VBV step 2 permette di inoltrare ai circuiti richieste di autorizzazione VBV una volta ottenuta l'autenticazione dell'utente da parte del sito ACS dell'issuer della carta. **Il messaggio AUTORIZZAZIONEONLINEVBV2 deve arrivare entro 8 minuti da quando è stato inviato il messaggio AUTORIZZAZIONEONLINEVBV originale.**

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "AUTORIZZAZIONEONLINEVBV2"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ggTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA , (Merchant ID)
IDOPERATORE	Y	Min. 8 Max.18	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
REQREFNUMORIG	Y	32	N	Identificatore univoco della richiesta originale che ha prodotto la richiesta di redirezione verso ACS.
PARES	Y			E' la PARES restituita dal sito ACS dell'issuer della carta dopo l'autenticazione dell'utente.
ACQUIRER	N	5	N	Codice dell'acquirer con cui si vuole effettuare la transazione
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D18

Richiesta in formato XML:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>AUTORIZZAZIONEONLINEVBV2</Operazione>
        <Timestamp>2005-02-08T12:02:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>

    <Dati>
        <RicAutorizzazioneVBV>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <IDoperatore>oper0001</IDoperatore>
                <ReqRefNum>123456789012345678901234522890000</ReqRefNum>
            </TestataRichiesta>
            < ReqRefNumOrig >123456789012345678901234522890000</ ReqRefNumOrig >
            <PaRes>Ssdfljlkj45098asdkgr09adsflkj9v26sfaheu73tags52gq7asgdhsdhvadghasags</ PaRes >
        </ RicAutorizzazioneVBV >
    </Dati>
</BPWXmlRichiesta>
```

La risposta al messaggio VBV step 2 è identica alla risposta che si otterrebbe da un messaggio di richiesta autorizzazione online per la quale sia stato inoltrato ai circuiti il messaggio di richiesta autorizzazione.
Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di autorizzazione online VBV step 2:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <BPWXmlRisposta>
    <Timestamp>2007-04-09T12:02:38</Timestamp>
    <Esito>00</Esito>
   - <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>8A74330BA1A1A085581EAA2409D8DC68FCC4395E</MAC>
   - <Dati>
      - <!-- L'elemento che segue contiene i dati della richiesta fatta -->
        <RicAutorizzazioneVBV>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <IDoperatore>oper0001</IDoperatore>
                <ReqRefNum>12345678901234567890123452289000</ReqRefNum>
            </TestataRichiesta>
            < ReqRefNumOrig >12345678901234567890123452289000</ ReqRefNumOrig >
            <PaRes>Ssdfljlkj45098asdkgr09adsflkj9v26sfaheu73tags52gq7asgdhsdhvadghasags</ PaRes >
        </ RicAutorizzazioneVBV >
      - <Autorizzazione>
            <TipoPag>06</TipoPag>
            <Tautor>I</Tautor>
            <IDtrans>8032180310AB0E30917930112</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>pos91</NumOrdine>
            <ImportoTrans>4450</ImportoTrans>
            <ImportoAutor>4450</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>0</ImportoContab>
            <ImportoStornato>100</ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2003-04-09T12:02:38</Timestamp>
            <NumAut>622851</NumAut>
            <AcqBIN>453997</AcqBIN>
            <CodiceEsercente>000000000000476</CodiceEsercente>
            <Stato>02</Stato>
          - <!-- Questa MAC firma i dati dell'autorizzazione -->
            <MAC>0EA6645D79E9752BE05800BE9CFE623CE3973395</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Per l'elemento Esito di BPWXmlRisposta viene aggiunto il valore 07, perciò complessivamente si ha quanto di seguito.

- **<Esito>** l'esito dell'operazione richiesta . Possibili esiti:

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	ReqRefNumOrig non trovato: non fa riferimento ad una richiesta di autorizzazione VBV oppure è passato troppo

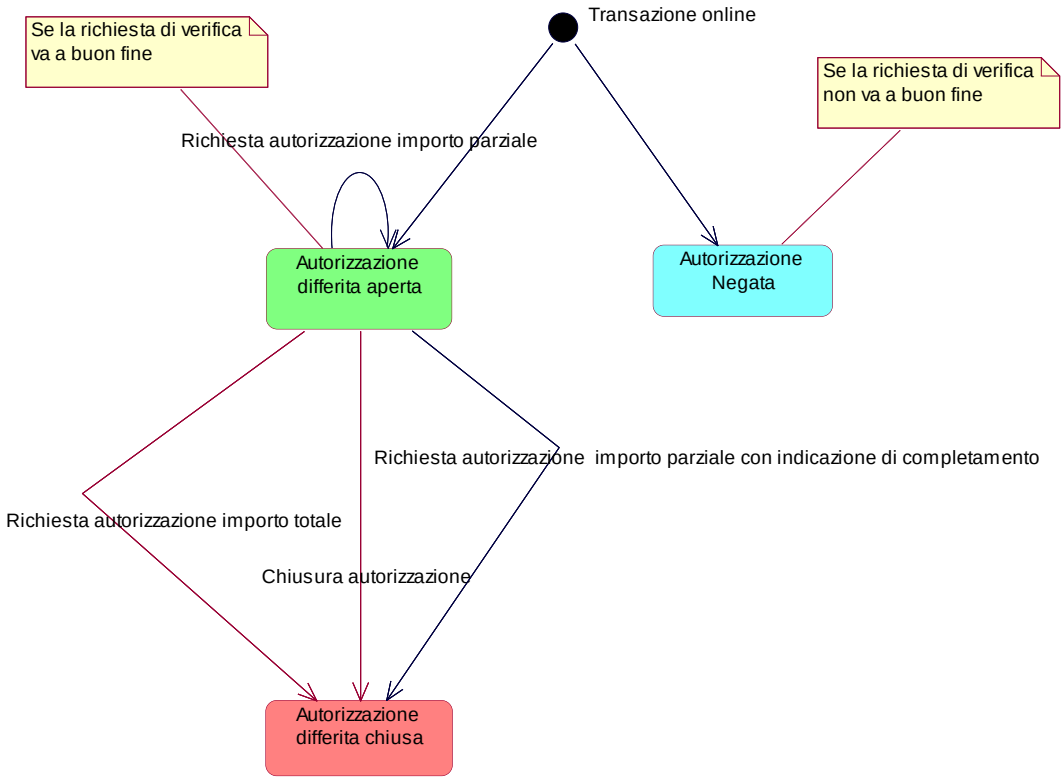
	tempo dalla richiesta originale
21	Tempo massimo per inoltrare la richiesta VBV step 2 scaduto
40	Xml vuoto o parametro ‘data’ mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

Per la descrizione di **`<Autorizzazione>`** si veda il paragrafo opportuno del capitolo “I messaggi di risposta in XML”

Operazioni sulle Autorizzazioni differite

Nel presente paragrafo vengono illustrate le operazioni che possono essere utilizzate per la gestione delle autorizzazioni di tipo differito.

Nel seguente diagramma di stato sono riportate le operazioni eseguibili sulle autorizzazioni differite:



La transazione online è quella che per la quale viene effettuata una richiesta di autorizzaizone verso i circuti l'autorizzazione per l'importo inviato dall'esercente ; l'autorizzazione differita, inserisce l'ordine nel sistema ed effettua la verifica della validità della carta. Non viene mandato nessun messaggio di autorizzazione ai circuiti internazionali.

La autorizzazione differita può essere a questo punto utilizzata per eseguire operazioni di autorizzazione vere e proprie in un numero a piacere fino a raggiungere un importo autorizzato pari al suo importo totale.

La autorizzazione differita può essere "chiusa", ovvero resa non più utilizzabile, tramite un messaggio di chiusura autorizzazione, oppure indicando in una richiesta di autorizzazione che non ne seguiranno altre.

Se si esegue una operazione di storno su una autorizzazione richiesta usando una autorizzazione differita viene ripristinato il totale ancora autorizzabile sulla transazine differita originale.

Le operazioni possibili sono:

- Richiesta conferma autorizzazione
- Chiusura autorizzazione differita

Richiesta di conferma autorizzazione

Il messaggio di richiesta di autorizzazione permette di inoltrare ai circuiti richieste di autorizzazione a conferma di pagamenti che erano stati effettuati con la modalità di autorizzazione differita. Nel messaggio di richiesta occorre indicare se seguiranno nuove richieste, oppure se quella presentata conclude l'ordine. Tramite questo messaggio è possibile effettuare richieste di autorizzazione fino ad un importo massimo complessivo pari a quello originariamente specificato nella transazione di autorizzazione differita effettuata online dal cliente.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "RICHIESTAAUTORIZZAZIONE"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID (MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	25	AN	Identificativo della transazione di autorizzazione differita effettuata online dal cliente
NUMORD	Y	Min. 1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
IMPORTO	N	Min. 2 Max. 8	N	Importo espresso nell'unità minima della valuta (centesimi di euro)
VALUTA	Y	3	N	Valuta: codice ISO (EURO = 978). Deve essere identica a quella della transazione originale
TCONTAB	Y	1	AN	Tipo di contabilizzazione da utilizzare per questo ordine: • D Differita • I Immediata
FINEORDINE	Y	1	A	Segnalazione di fine ordine: • S Ordine chiuso definitivamente • N Ordine ancora aperto
RELEASE	N	N	2	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D1

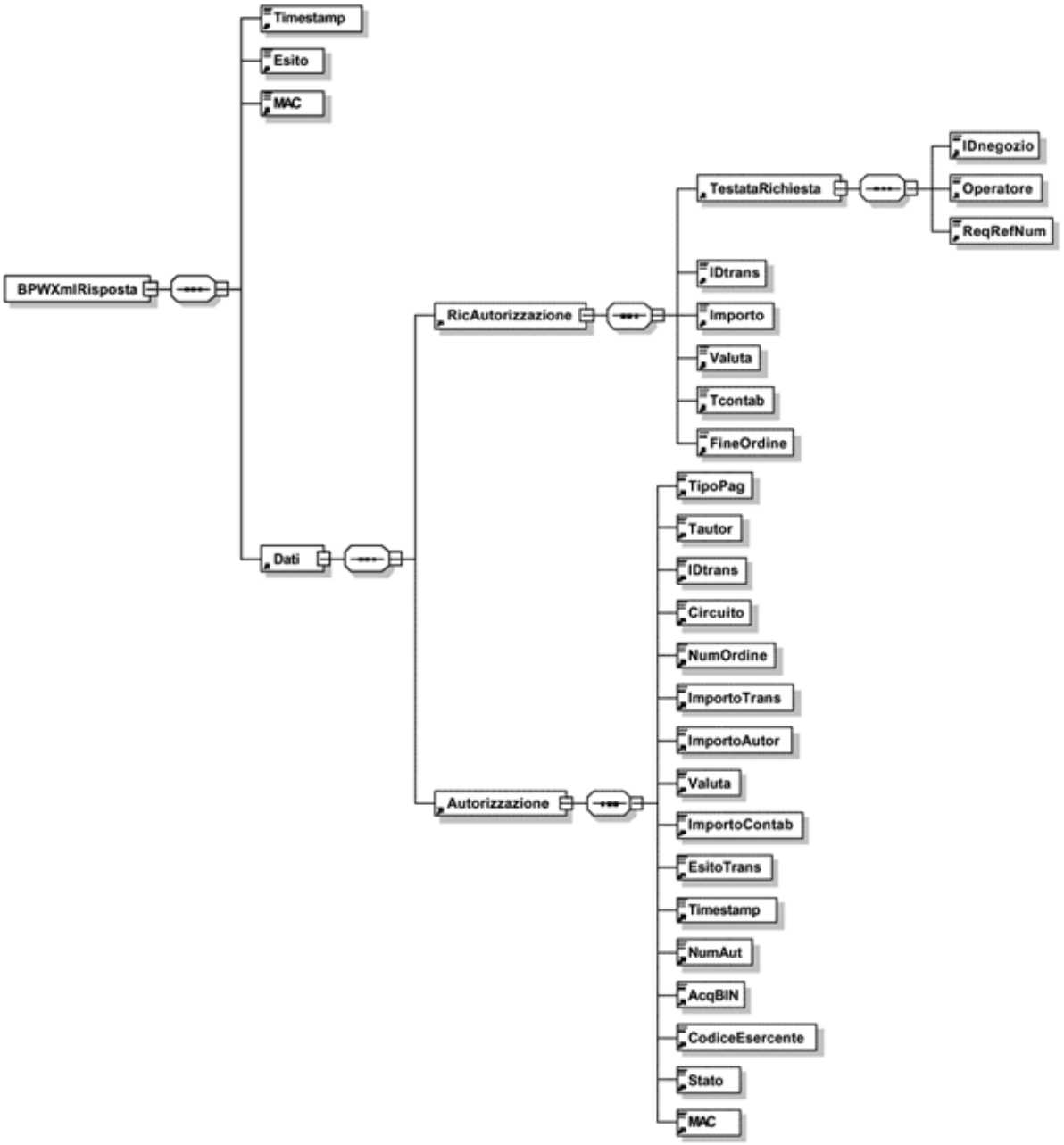
Richiesta di autorizzazione in formato XML

*** ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.**

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>RICHIESTAAUTORIZZAZIONE</Operazione>
```

```
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicAutorizzazione>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>123422229012345678901234567890000</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>1234567890</IDtrans>
            <NumOrdine>9998500000000015</NumOrdine>
            <Importo>7700</Importo>
            <Valuta>978</Valuta>
            <Tcontab>D</Tcontab>
            <FineOrdine>S</FineOrdine>
        </RicAutorizzazione>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di autorizzazione è formattato in XML ed è schematizzato nella pagina successiva.



Come si può notare la risposta ad una richiesta di autorizzazione è sostanzialmente costituita da un elemento di tipo Autorizzazione.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento Autorizzazione non viene creato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di autorizzazione:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicAutorizzazione>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>200305014962046909345843058345 64</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>C39564565845756456416 5636</IDtrans>
            <Importo>10000</Importo>
            <Valuta>978</Valuta>
            <Tcontab>I</Tcontab>
            <FineOrdine>1</FineOrdine>
        </RicAutorizzazione>
        <Autorizzazione>
            <Tautor>I</Tautor>
            <IDtrans>C3956456584575645645656 36</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>10000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>10000</ImportoContab>
            <ImportoStornato>100</ ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>01</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>3204989a63de6ae849c9</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta . Possibili esiti:

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile

99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito (vedi appendice D11)
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAutorizzazione>** i dati della richiesta di autorizzazione
- **<Autorizzazione>** i dati del messaggio di risposta

<RicAutorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di autorizzazione differita
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro
- **<Tcontab>** il tipo di contabilizzazione da utilizzare: D=Differita, I=Immediata
- **<FineOrdine>** segnalazione di fine ordine

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** l'identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati dell'autorizzazione immediata richiesta. Per la sua descrizione si veda il paragrafo opportuno del capitolo "I messaggi di risposta in XML"

Chiusura autorizzazione differita

L'operazione di chiusura di una autorizzazione differita rende non più utilizzabile per ulteriori autorizzazioni la transazione di autorizzazione differita indicata. In definitiva comunica al sistema che l'ordine in questione è da considerarsi chiuso.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

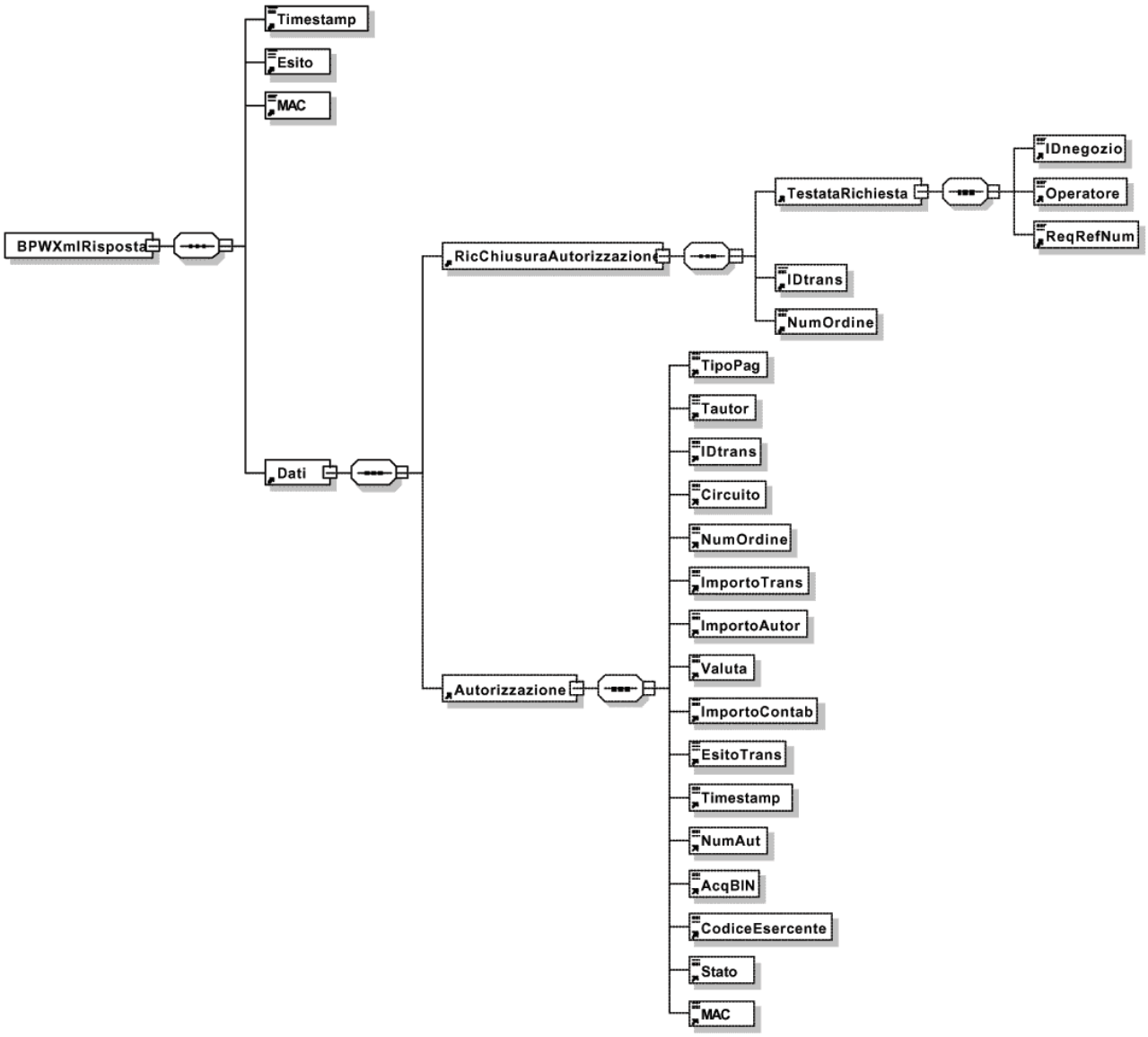
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "CHIUSURADIFFERITA"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID (MID).
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	25	AN	Identificatore della transazione di autorizzazione differita effettuata online dal cliente
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D2

Richiesta di chiusura autorizzazione differita in formato XML

* ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>CHIUSURADIFFERITA</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicChiusuraAutorizzazione>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>12345678901234567890123456789000</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>1234567890</IDtrans>
            <NumOrdine>9998500000000015</NumOrdine>
        </RicChiusuraAutorizzazione>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di chiusura autorizzazione è formattato in XML ed è schematizzato qui di seguito.



Come si può notare la risposta ad una richiesta di chiusura autorizzazione differita è sostanzialmente costituita da un elemento di tipo Autorizzazione, che riporterà come stato corrente quello di "chiusa".
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento Autorizzazione non viene creato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di chiusura di una autorizzazione:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-04-13T12:01:02</Timestamp>
    <Esito>00</Esito>
    <MAC>ddb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <RicChiusuraAutorizzazione>
            <TestataRichiesta>
                <IDnegozio>12837837461</IDnegozio>
                <Operatore>9823479</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <IDtrans> C39564325845757564564565636</IDtrans>
            <NumOrdine>A398459</NumOrdine>
        </RicChiusuraAutorizzazione>
        <Autorizzazione>
            <Tautor>D</Tautor>
            <IDtrans> C39564565845757564564565636</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>5000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>5000</ImportoContab>
            <ImportoStornato>5000</ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>03</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>aab3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAutorizzazione>** i dati della richiesta di chiusura autorizzazione
- **<Autorizzazione>** i dati del messaggio di risposta

<RicAutorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di chiusura autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di richiesta
- **<NumOrdine>** il codice dell'ordine

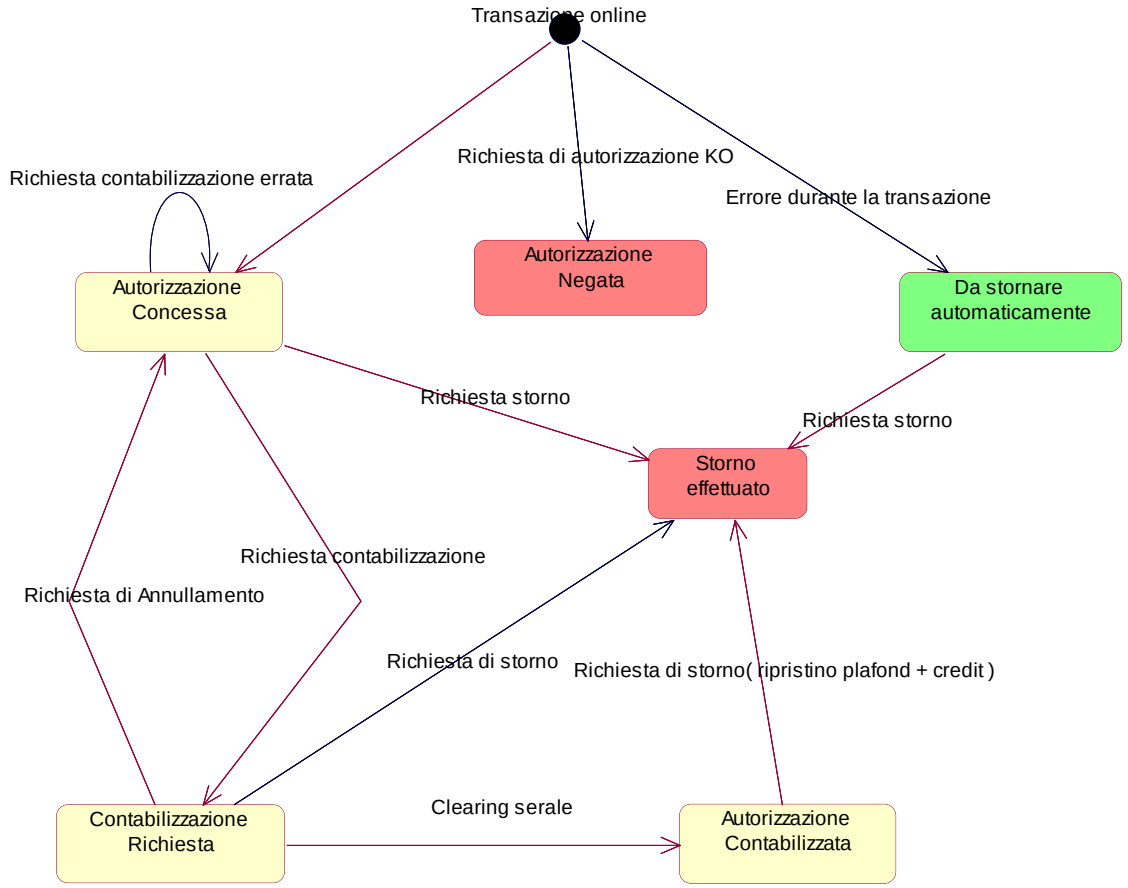
<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** l'identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati dell'autorizzazione differita che è stata oggetto della richiesta di chiusura.

Operazioni sulle Autorizzazioni immediate

Il presente paragrafo illustra le operazioni che sono possibili sulle autorizzazioni vere e proprie (autorizzazioni immediate). Sotto viene riportato un diagramma di stato.



La transazione online è quella effettuata on line dall'esercente verso i ciruciti autorizzativi, oppure la transazione scaturita da un messaggio di richiesta di autorizzazione a conferma di una differita.

Le operazioni possibili sono:

- richiesta di contabilizzazione
- richiesta di annullamento contabilizzazione
- richiesta di storno una autorizzazione
- richiesta di split (divisione e/o riduzione) di una autorizzazione

Richiesta di contabilizzazione

L'operazione di richiesta di contabilizzazione fa si che il sistema @POS inoltri all'acquirer di competenza la richiesta di contabilizzazione di una autorizzazione precedentemente concessa con contabilizzazione differita. Le richieste contabili vengono mandate agli acquirer in modo batch durante le elaborazioni notturne. Le richieste di contabilizzazioni per la giornata corrente sono inoltrabili fino alle ore 24:00. Le richieste di contabilizzazione riguardano i pagamenti tramite carta di credito.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "CONTABILIZZAZIONE"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	25	AN	Identificativo della transazione di autorizzazione effettuata dal cliente
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
IMPORTO	Y	Min.2 Max.8	N	Importo espresso nell'unità minima della valuta (centesimi di euro)
VALUTA	Y	3	N	Valuta: codice ISO (EUR = 978)
DESCROP	N	100	AN	Descrizione aggiuntiva dell'operazione a discrezione dell'esercente
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D4

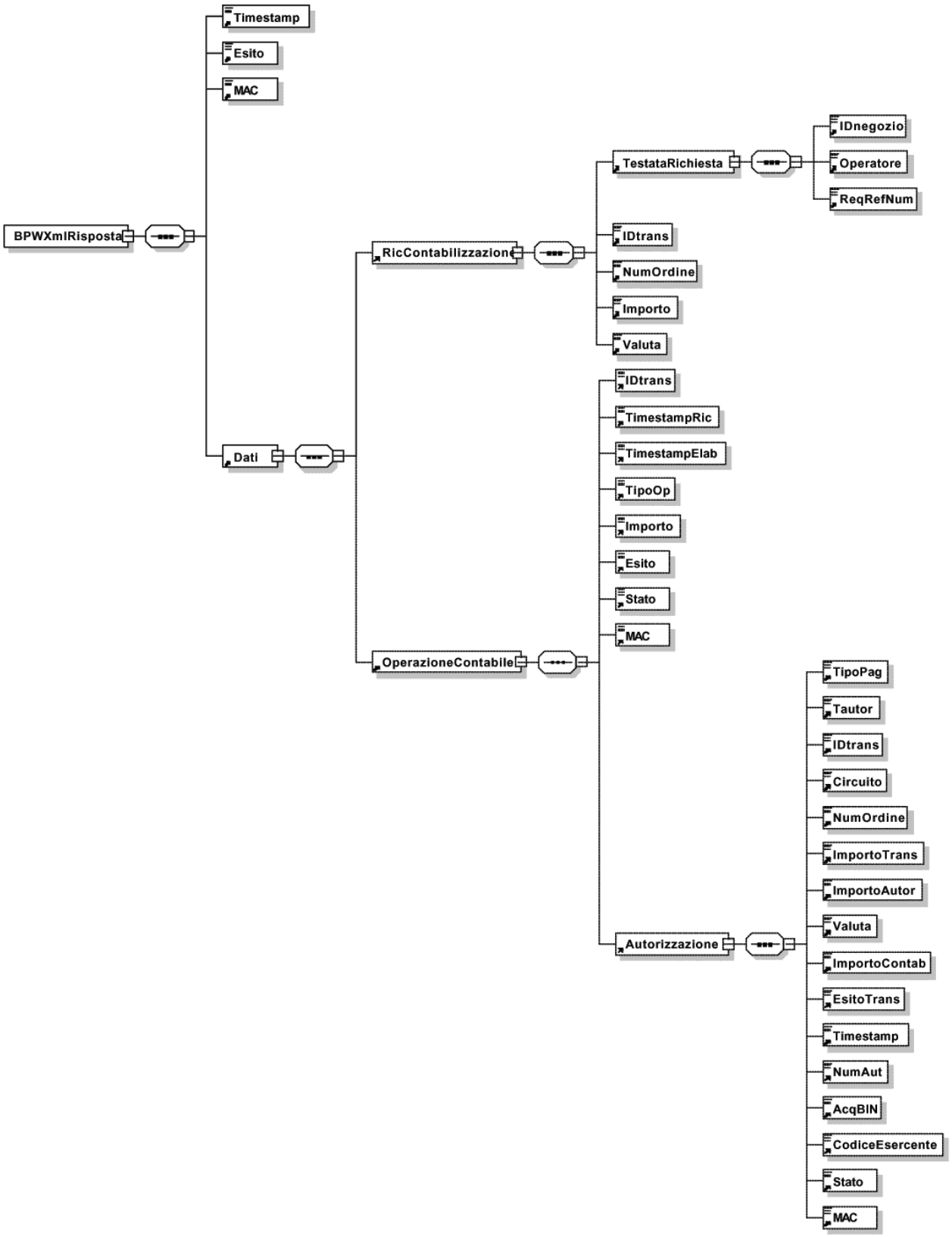
Richiesta di contabilizzazione in formato XML

*** ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.**

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>CONTABILIZZAZIONE</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicContabilizzazione>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
```

```
            <Operatore> oper0001</Operatore>
            <ReqRefNum>20041212123456789012346787900000</ReqRefNum>
        </TestataRichiesta>
        <IDtrans>1234567890</IDtrans>
        <NumOrdine>9998500000000015</NumOrdine>
        <Importo>7700</Importo>
        <Valuta>978</Valuta>
        <DescrOp>RichiestaCallCenter1037</ DescrOp >
    </RicContabilizzazione>
  </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di contabilizzazione è formattato in XML ed è schematizzato qui di seguito.



La risposta ad una richiesta di contabilizzazione è costituita da un elemento di tipo OperazioneContabile che riporta i dati dell'operazione compiuta.

Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento OperazioneContabile non viene generato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di contabilizzazione:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicContabilizzazione>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <IDtrans> C39564325845757564564565636</IDtrans>
            <NumOrdine>A398459</NumOrdine>
            <Importo>7000</Importo>
            <Valuta>978</Valuta>
        </RicContabilizzazione>
        <OperazioneContabile>
            <IDtrans>C9435879294</IDtrans>
            <TimestampRic>2001-07-04T12:02:55</TimestampRic>
            <TimestampElab>NULL</TimestampElab>
            <TipoOp>20</TipoOp>
            <Importo>7000</Importo>
            <Esito>00</Esito>
            <Stato>03</Stato>
            <DescrOp>RichiestaCallCenter1037</ DescrOp >
            <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
            <MAC>12334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
            <Autorizzazione>
                <Tautor>I</Tautor>
                <IDtrans> C39564565845757564564565636</IDtrans>
                <Circuito>01</Circuito>
                <NumOrdine>A398459</NumOrdine>
                <ImportoTrans>10000</ImportoTrans>
                <ImportoAutor>10000</ImportoAutor>
                <Valuta>978</Valuta>
                <ImportoContab>7000</ImportoContab>
                <ImportoStornato>100</ImportoStornato>
                <EsitoTrans>00</EsitoTrans>
                <Timestamp>2001-07-09T21:05:44</Timestamp>
                <NumAut>A93485</NumAut>
                <AcqBIN>123450943</AcqBIN>
                <CodiceEsercente>09834509</CodiceEsercente>
                <Stato>01</Stato>
                <!-- Questa MAC firma la autorizzazione  -->
                <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
            </Autorizzazione>
        </OperazioneContabile>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta

<Esito> l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di contabilizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicContabilizzazione>** i dati relativi alla richiesta di contabilizzazione
- **<Operazionecontabile>** i dati relativi all'operazione contabile

<RicContabilizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di contabilizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di richiesta contabilizzazione
- **<NumOrdine>** il codice dell'ordine
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<OperazioneContabile>
Questo elemento racchiude i dati relativi all'operazione contabile effettuata. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Annullamento richiesta di contabilizzazione

L'operazione di annullamento di una richiesta di contabilizzazione può avvenire entro le ore 24:00 della giornata nella quale è stata inoltrata la richiesta in oggetto. Questa operazione annulla la richiesta di contabilizzazione e rende l'autorizzazione nuovamente contabilizzabile. Le richieste di annullamento contabilizzazione riguardano i pagamenti tramite carta di credito.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

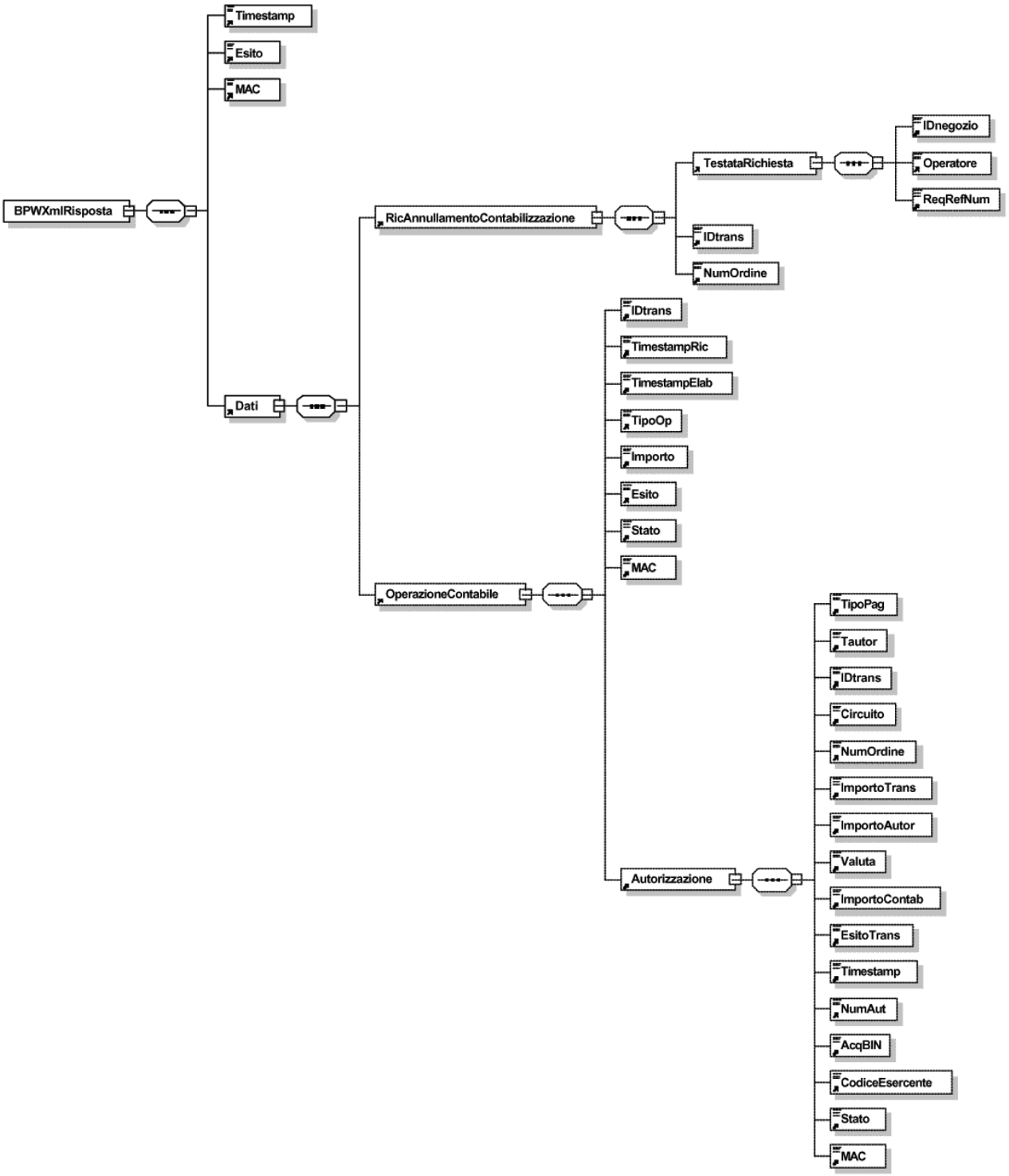
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y			Operazione richiesta: valorizzato con "ANNULLAMENTOCONTABILIZZAZIONE "
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	11	AN	Identificativo della transazione di contabilizzazione effettuata dal cliente
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D5

Richiesta di annullamento di una richiesta di contabilizzazione in formato XML

* ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>ANNULLAMENTOCONTABILIZZAZIONE</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicAnnullamentoContabilizzazione>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>12345678901234567890123456789000</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>1234567890</IDtrans>
            <NumOrdine>9998500000000015</NumOrdine>
        </RicAnnullamentoContabilizzazione>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di annullamento contabilizzazione è formattato in XML.



La risposta ad una richiesta di contabilizzazione è costituita da un elemento di tipo OperazioneContabile che riporta i dati dell'operazione compiuta.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione l'elemento OperazioneContabile non viene generato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di annullamento di contabilizzazione:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicAnnullamentoContabilizzazione>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <IDtrans> C9435879294</IDtrans>
            <NumOrdine>A398459</NumOrdine>
        </RicAnnullamentoContabilizzazione>
        <OperazioneContabile>
            <IDtrans>C5555358792</IDtrans>
            <TimestampRic>2001-07-04T22:02:55</TimestampRic>
            <TimestampElab>NULL</TimestampElab>
            <TipoOp>40</TipoOp>
            <Importo>7000</Importo>
            <Esito>00</Esito>
            <Stato>SGN03</Stato>
            <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
            <MAC>12334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
            <Autorizzazione>
                <Tautor>I</Tautor>
                <IDtrans> C3956456584575645645656 36</IDtrans>
                <Circuito>01</Circuito>
                <NumOrdine>A398459</NumOrdine>
                <ImportoTrans>10000</ImportoTrans>
                <ImportoAutor>10000</ImportoAutor>
                <Valuta>978</Valuta>
                <ImportoContab>0</ImportoContab>
                <ImportoStornato>0</ImportoStornato>
                <EsitoTrans>00</EsitoTrans>
                <Timestamp>2001-07-09T21:05:44</Timestamp>
                <NumAut>A93485</NumAut>
                <AcqBIN>123450943</AcqBIN>
                <CodiceEsercente>09834509</CodiceEsercente>
                <Stato>01</Stato>
                <!-- Questa MAC firma la autorizzazione  -->
                <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
            </Autorizzazione>
        </OperazioneContabile>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato

04	Autenticazione API errata, MAC non corretto
05	Data errata, o periodo indicato vuoto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di autorizzazione e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di autorizzazione e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicAnnullamentoContabilizzazione>** i dati relativi alla richiesta di annullamento contabilizzazione
- **<Operazionecontabile>** i dati relativi all'operazione contabile

<RicAnnullamentoContabilizzazione>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di annullamento contabilizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di richiesta annullamento contabilizzazione
- **<NumOrdine>** il codice dell'ordine

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<OperazioneContabile>
Questo elemento racchiude i dati relativi all'operazione contabile effettuata. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Richiesta di storno di un pagamento

La richiesta di storno di un pagamento viene applicata dal sistema @POS ad una autorizzazione concessa. Le transazioni che si nascondono dietro questa operazione sono differenti a seconda dello stato della autorizzazione in oggetto. Se l'autorizzazione non è ancora stata contabilizzata avverrà una transazione di ripristino plafond; se l'autorizzazione è stata contabilizzata nella giornata corrente, e non è quindi ancora stata inviata all'acquirer, avverranno le transazioni di ripristino plafond ed annullamento contabilizzazione. Se l'autorizzazione è già stata contabilizzata dall'acquirer avverranno le operazioni di ripristino plafond e di credit del titolare.
Dopo uno storno parziale del pagamento saranno possibili solo ulteriori storni parziali fino al raggiungimento del massimo importo stornabile. In questo caso si tratterà di storni multipli. Gli storni multipli non sono consentiti sui circuiti di debito (Pagobancomat).

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "STORNO"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	25	AN	Identificativo della transazione di autorizzazione sulla quale fare lo storno
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
IMPORTO	Y	Min.2 Max.8	N	Importo da stornare espresso nell'unità minima della valuta (centesimi di euro)
VALUTA	Y	3	N	Valuta: codice ISO (EUR = 978)
DESCROP	N	100	AN	Descrizione aggiuntiva dell'operazione a discrezione dell'esercente
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D3

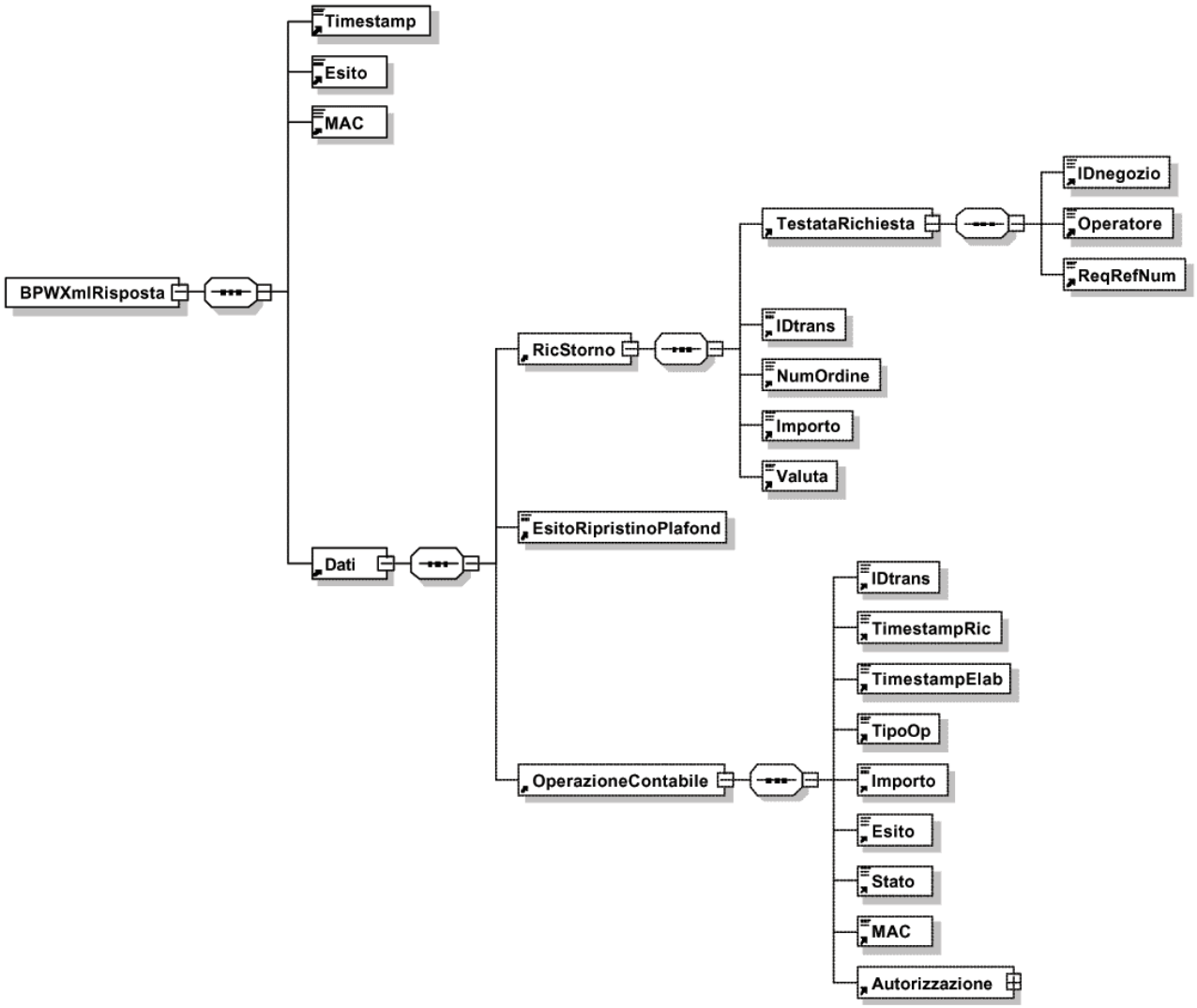
Richiesta di storno in formato XML

*** ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.**

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>STORNO</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
```

```
        <RicStorno>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>12345678901234567890123456789000</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>1234567890</IDtrans>
            <NumOrdine>9998500000000015</NumOrdine>
            <Importo>7700</Importo>
            <Valuta>978</Valuta>
            <DescrOp>RichiestaCallCenter1038</ DescrOp >
        </RicStorno>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di storno pagamento è formattato in XML ed è schematizzato qui di seguito.



Come si può notare la risposta ad una richiesta di storno di un pagamento è costituita da due elementi: l'esito della operazione di ripristino plafond e l'eventuale operazione contabile compiuta per restituire il denaro al titolare.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione gli elementi di risposta contenuti in Dati non vengono creati.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di storno di una autorizzazione che era già stata contabilizzata:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicStorno>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
```

```
            <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
        </TestataRichiesta>
        <IDtrans> C3556456584575646456563 6</IDtrans>
        <NumOrdine>A398459</NumOrdine>
        <Importo>10000</Importo>
        <Valuta>978</Valuta>
    </RicStorno>
    <EsitoRipristinoPlafond>00</EsitoRipristinoPlafond>
    <OperazioneContabile>
        <IDtrans>C5555358793</IDtrans>
        <TimestampRic>2001-07-04T22:02:55</TimestampRic>
        <TimestampElab>NULL</TimestampElab>
        <TipoOp>01</TipoOp>
        <Importo>10000</Importo>
        <Esito>00</Esito>
        <Stato>00</Stato>
        <DescrOp>RichiestaCallCenter1038</ DescrOp >
        <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
        <MAC>12334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
        <Autorizzazione>
            <Tautor>I</Tautor>
            <IDtrans> C3956456584575645645656 36</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>10000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>0</ImportoContab>
            <ImportoStornato>0</ ImportoStornato >
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>01</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Autorizzazione>
    </OperazioneContabile>
  </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile

Nel caso di storni multipli (cioè richieste di storno su autorizzazioni già parzialmente stornate) deve essere posta particolare attenzione ai seguenti casi:

- storno con importo non specificato: l'esito sarà 03 (non sono cioè ammessi storni totali dopo storni parziali).
- storno su autorizzazione già totalmente stornata: l'esito sarà 00.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di storno e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di storno e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicStorno>** i dati relativi alla richiesta di storno di autorizzazione
- **<EsitoRipristinoPlafond>** l'esito del ripristino del plafond
- **<Operazionecontabile>** i dati relativi all'operazione contabile

<RicStorno>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di storno autorizzazione rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di richiesta di storno
- **<NumOrdine>** il codice dell'ordine
- **<Importo>** l'importo dell'autorizzazione richiesta in centesimi di euro
- **<Valuta>** il codice ISO della valuta: 978=Euro

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<OperazioneContabile>
Questo elemento è facoltativo: è presente solo se per eseguire lo storno è stato necessario effettuare una operazione contabile. Nel caso sia presente esso racchiude i dati relativi all'operazione contabile effettuata. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Richiesta di split (divisione e/o riduzione) ordine

L'operazione rende possibile lo split (divisione e/o riduzione) shipment per un ordine che era stato eseguito con autorizzazione immediata: annulla la autorizzazione immediata e piazza una nuova autorizzazione differita da confermare in pezzi

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

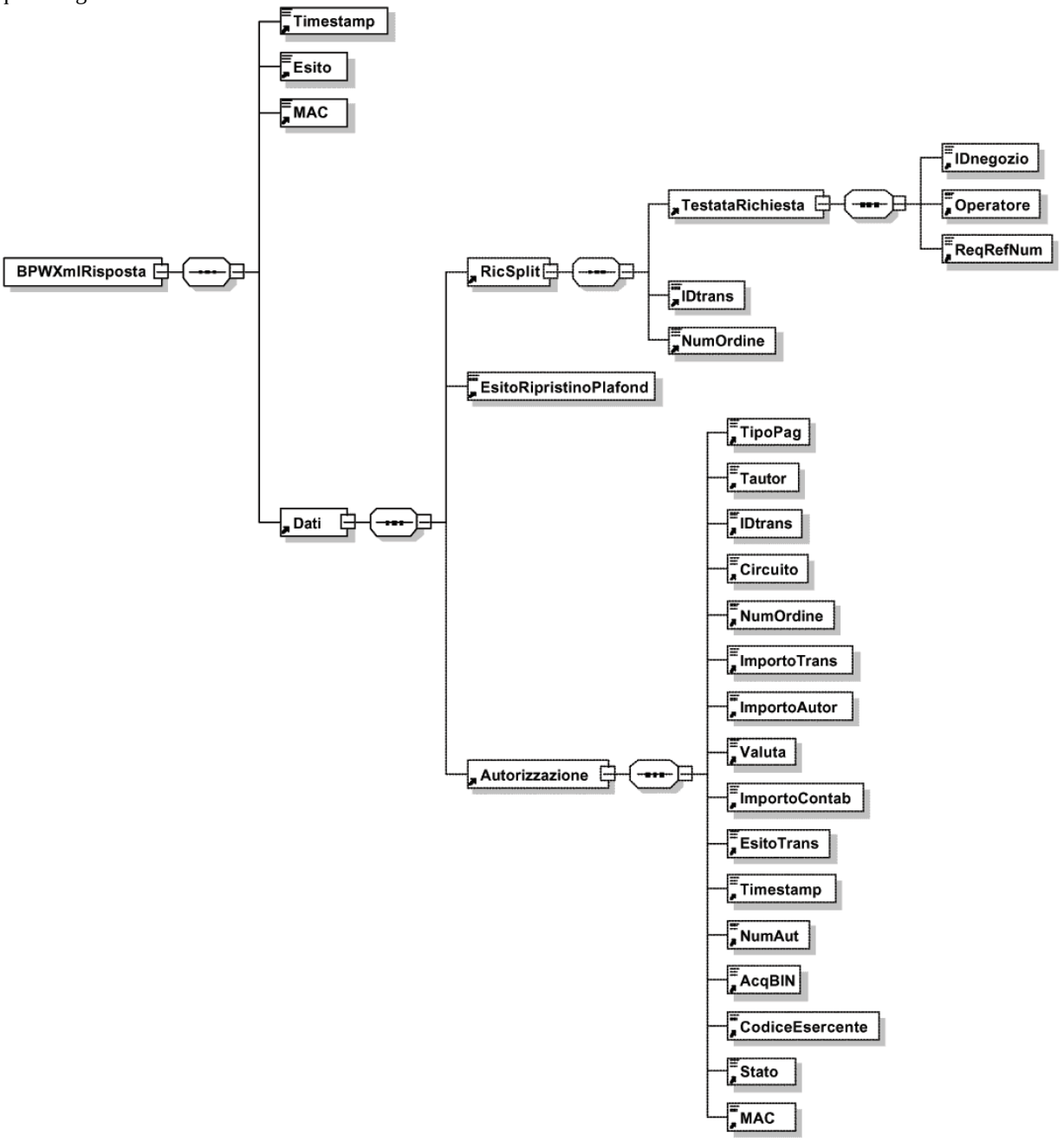
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y			Operazione richiesta: valorizzato con "SPLIT"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDTRANS	Y	25	AN	Identificativo della transazione di autorizzazione effettuata dal cliente
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D6

Richiesta di split in formato XML

* ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>SPLIT</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <!-- L'elemento che segue contiene i dati della richiesta fatta -->
        <RicSplit>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>12345678901234567890123456789000</ReqRefNum>
            </TestataRichiesta>
            <IDtrans>1234567890</IDtrans>
            <NumOrdine>9998500000000015</NumOrdine>
        </RicSplit>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di split (divisione e/o riduzione) ordine è formattato in XML ed è schematizzato qui di seguito.



La risposta ad una richiesta di split (divisione e/o riduzione) di una autorizzazione immediata è costituita da due elementi: l'esito della operazione di ripristino plafond e l'autorizzazione differita creata.
Nel caso in cui l'IDTRANS della transazione originale non esista, o si verifichi un errore di autenticazione gli elementi di risposta contenuti in Dati non vengono creati.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di split (divisione e/o riduzione):

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
```

```
    <Timestamp>2001-04-13T12:01:02</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ddb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicSplit>
            <TestataRichiesta>
                <IDnegozio>12837837461</IDnegozio>
                <Operatore>9823479</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <IDtrans> C3556456584575645645656 36</IDtrans>
            <NumOrdine>A398459</NumOrdine>
        </RicSplit>
        <!-- L'lemento che segue riporta l'esito della operazione di ripristino plafond della carta. Lo split viene effettuato a
prescindere dall'esito di tale operazione -->
        <EsitoRipristinoPlafond>00</EsitoRipristinoPlafond>
        <!-- L'lemento che segue contiene i dati della nuova autorizzazione differita che e' stata creata -->
        <Autorizzazione>
            <Tautor>D</Tautor>
            <IDtrans> C3956456584575645645656 36</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>5000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>5000</ImportoContab>
            <ImportoStornato>100</ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>02</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>aab3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11

- **<Dati>** i dati della richiesta di split (divisione e/o riduzione) e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di split (divisione e/o riduzione) e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicSplit>** i dati relativi alla richiesta di split (divisione e/o riduzione)
- **<EsitoRipristinoPlafond>** l'esito del ripristino del plafond
- **<Autorizzazione>** i dati dell'autorizzazione

<RicSplit>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di split (divisione e/o riduzione) rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<IDtrans>** l'identificatore della transazione di richiesta di split (divisione e/o riduzione)
- **<NumOrdine>** il codice dell'ordine

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

Richiesta verifica esito richiesta

Fornendo il numero identificativo della richiesta voluta, restituisce l'esito del messaggio precedentemente inoltrato.

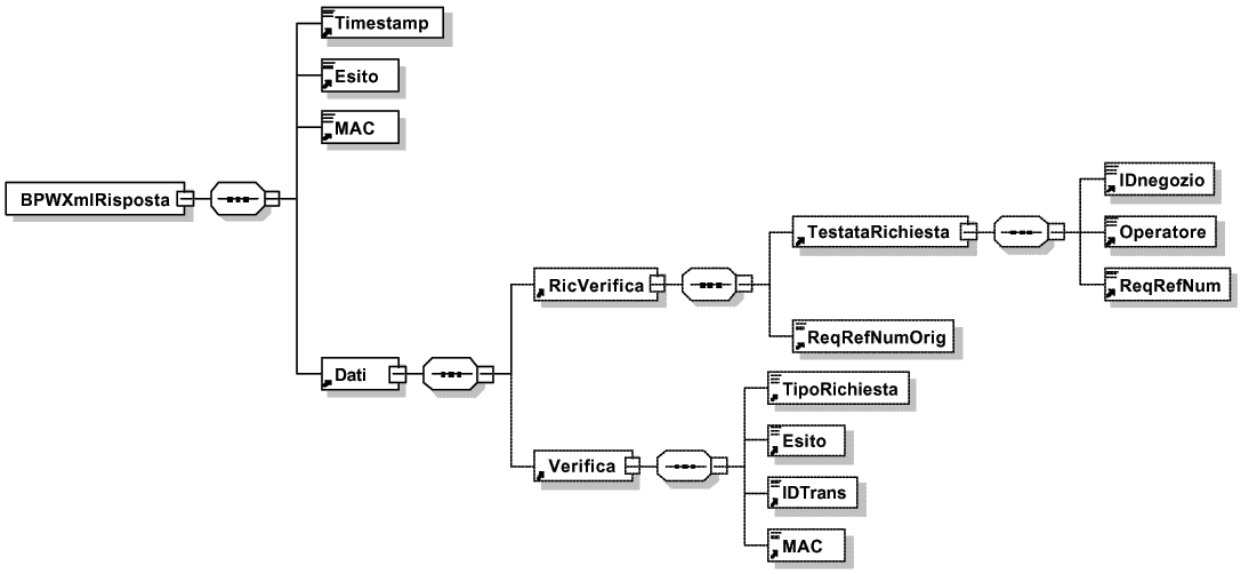
I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "VERIFICA"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH.mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	AN	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
REQREFNUMORIG	Y	32	AN	Identificativo della richiesta da verificare
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D7

Richiesta di verifica esito in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>VERIFICA</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicVerifica>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>123456789012345678901234567890000</ReqRefNum>
            </TestataRichiesta>
            <ReqRefNumOrig>09876543210987654321098765432100</ReqRefNumOrig>
        </RicVerifica>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di verifica richiesta contabile è formattato in XML.



Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di esito richiesta:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <RicVerifica>
            <TestataRichiesta>
                <IDnegozio>4357394875</IDnegozio>
                <Operatore>43985739</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <ReqRefNumOrig>20030501496204690934584305836927</ReqRefNumOrig>
        </RicVerifica>
        <Verifica>
            <TipoRichiesta>01</TipoRichiesta>
            <Esito>00</Esito>
            <IDTrans> C39564565845756456456563 6</IDTrans>
            <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Verifica>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

`<BPWXmlRisposta>`
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **`<Timestamp>`** la data e l'ora del messaggio di risposta
- **`<Esito>`** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo

02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	ReqRefNum non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di split (divisione e/o riduzione) e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di split (divisione e/o riduzione) e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicVerifica>** i dati relativi alla richiesta di verifica
- **<Verifica>** i dati dell'autorizzazione
- **<TipoRichiesta>** il tipo di richiesta da verificare

Tipo	Descrizione
1	Autorizzazione
2	Chiusura autorizzazione
3	Storno
4	Contabilizzazione
5	Annullamento contabile
6	Split

- **<Esito>** l'esito della richiesta da verificare
- **<IDTrans>** l'idtrans della richiesta da verificare
- **<MAC>** firma della verifica

Elenco operazioni contabili

Questa operazione permette di ricavare l'elenco delle operazioni di carattere contabile. Con tale termine si intendono le richieste di contabilizzazione e di credit inoltrate al sistema.
Vengono elencate sia quelle già inviate agli acquirer sia quelle ancora da inoltrare. Queste ultime si distinguono per la data di elaborazione non valorizzata.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "ELENCOCONTABILE"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
DATAINIZIO	Y	10	D	Data di inizio periodo, formato yyyy-MM-dd
DATAFINE	Y	10	D	Data di fine periodo, formato yyyy-MM-dd
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
TIPOOP	N	2	AN	Tipo di operazione da estrarre. I valori possibili sono : 01 02 03 04 e fanno riferimento al campo <TipoOp> dell'elemento <OperazioneContabile>. Si veda il capitolo "I messaggi di risposta in XML"
DESCROP	N	100	AN	Limita la ricerca alle sole operazioni aventi la descrizione aggiuntiva indicata (vedere messaggio di storno)
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D8

Richiesta elenco contabile in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRichiesta>
    <Release>02</Release>
    <Richiesta>
        <Operazione>ELENCOCONTABILE</Operazione>
        <Timestamp>2005-03-04T11:20:00.000</Timestamp>
        <MAC>115025d5a5b65df687790867bdece136</MAC>
    </Richiesta>
    <Dati>
        <RicElencoOperazioniContabili>
            <TestataRichiesta>
                <IDnegozio>000000000000003</IDnegozio>
                <Operatore> oper0001</Operatore>
                <ReqRefNum>12345678901234567890123456789000</ReqRefNum>
            </TestataRichiesta>
            <DataInizio>2003-12-01</DataInizio>
            <DataFine>2003-12-31</DataFine>
            <TipoOp>03</TipoOp>
            <DescrOp>RichiestaCallCenter1038</ DescrOp >
        </RicElencoOperazioniContabili>
    </Dati>
</BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di elenco operazioni contabili è formattato in XML.

La risposta ad una richiesta di elenco contabile è costituita da un insieme di elementi di tipo OperazioneContabile.
Nel caso in cui si verifichi un errore l'elemento ElencoOperazioniContabili non viene creato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta dell'elenco delle operazioni contabili:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicElencoOperazioniContabili>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <DataInizio>2001-01-01</DataInizio>
            <DataFine>2001-07-10</DataFine>
        </RicElencoOperazioniContabili>
        <ElencoOperazioniContabili NumeroElementi="2"/>
        <OperazioneContabile>
            <IDtrans>C9435879295</IDtrans>
            <TimestampRic>2001-07-04T12:02:55</TimestampRic>
            <TimestampElab>2001-07-04T23:02:55</TimestampElab>
            <TipoOp>21</TipoOp>
            <Importo>10000</Importo>
            <Esito>00</Esito>
            <Stato>03</Stato>
            <DescrOp>RichiestaCallCenter1038</ DescrOp >
            <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
            <MAC>12dd4c3a4ab34c3a4abc4c3a4ab3ffa1</MAC>
            <Autorizzazione>
                <Tautor>I</Tautor>
                <IDtrans> C3956456584575645645656 36</IDtrans>
                <Circuito>01</Circuito>
                <NumOrdine>A398459</NumOrdine>
                <ImportoTrans>10000</ImportoTrans>
                <ImportoAutor>10000</ImportoAutor>
                <Valuta>978</Valuta>
                <ImportoContab>8000</ImportoContab>
                <ImportoStornato>100</ImportoStornato>
                <EsitoTrans>00</EsitoTrans>
                <Timestamp>2001-07-09T21:05:44</Timestamp>
                <NumAut>A93485</NumAut>
                <AcqBIN>123450943</AcqBIN>
                <CodiceEsercente>09834509</CodiceEsercente>
                <Stato>01</Stato>
                <!-- Questa MAC firma la autorizzazione  -->
                <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
            </Autorizzazione>
        </OperazioneContabile>
        <OperazioneContabile>
            <IDtrans>C9435879384</IDtrans>
            <TimestampRic>2001-17-04T12:02:55</TimestampRic>
            <TimestampElab>2001-17-04T23:02:55</TimestampElab>
            <TipoOp>20</TipoOp>
            <Importo>2000</Importo>
            <Esito>00</Esito>
            <Stato>00</Stato>
```

```
            <DescrOp>RichiestaCallCenter1038</ DescrOp >
            <!-- Questa MAC firma i dati dell'operazione contabile sopra riportati  -->
            <MAC>aa334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
            <Autorizzazione>
                <Tautor>I</Tautor>
                <IDtrans> C39564565845756456456563 6</IDtrans>
                <Circuito>01</Circuito>
                <NumOrdine>A398459</NumOrdine>
                <ImportoTrans>10000</ImportoTrans>
                <ImportoAutor>10000</ImportoAutor>
                <Valuta>978</Valuta>
                <ImportoContab>8000</ImportoContab>
                <ImportoStornato>100</ImportoStornato>
                <EsitoTrans>00</EsitoTrans>
                <Timestamp>2001-07-09T21:05:44</Timestamp>
                <NumAut>A93485</NumAut>
                <AcqBIN>123450943</AcqBIN>
                <CodiceEsercente>09834509</CodiceEsercente>
                <Stato>01</Stato>
                <!-- Questa MAC firma la autorizzazione  -->
                <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
            </Autorizzazione>
        </OperazioneContabile>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta "00" elenco eseguito

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
05	Data errata, o periodo indicato vuoto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di elenco operazioni contabili e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di elenco operazioni contabili e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicElencoOperazioniContabili>** i dati relativi alla richiesta di elenco operazioni contabili
- **<OperazioniContabili>** i dati relativi alle operazioni contabili

<RicElencoOperazioniContabili>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di elenco operazioni contabili rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<DataInizio>** data di inizio periodo dell'elenco
- **<DataFine>** data di fine periodo dell'elenco

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<ElencoOperazioniContabili>
Questo elemento contiene il numero di elementi che costituiscono l'elenco richiesto

<OperazioneContabile>
Esistono tante occorrenze di questo elemento quante sono le operazioni contabili che costituisco l'elenco generato. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Elenco autorizzazioni

Questa operazione permette di ricavare l'elenco delle richieste di autorizzazione inoltrate dal sistema @POS ai circuiti di pagamento internazionali o nazionali in un dato periodo.
E' possibile indicare se si desidera ottenere tutte le autorizzazioni, solo quelle autorizzate, solo quelle negate, oppure solo quelle stornate.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

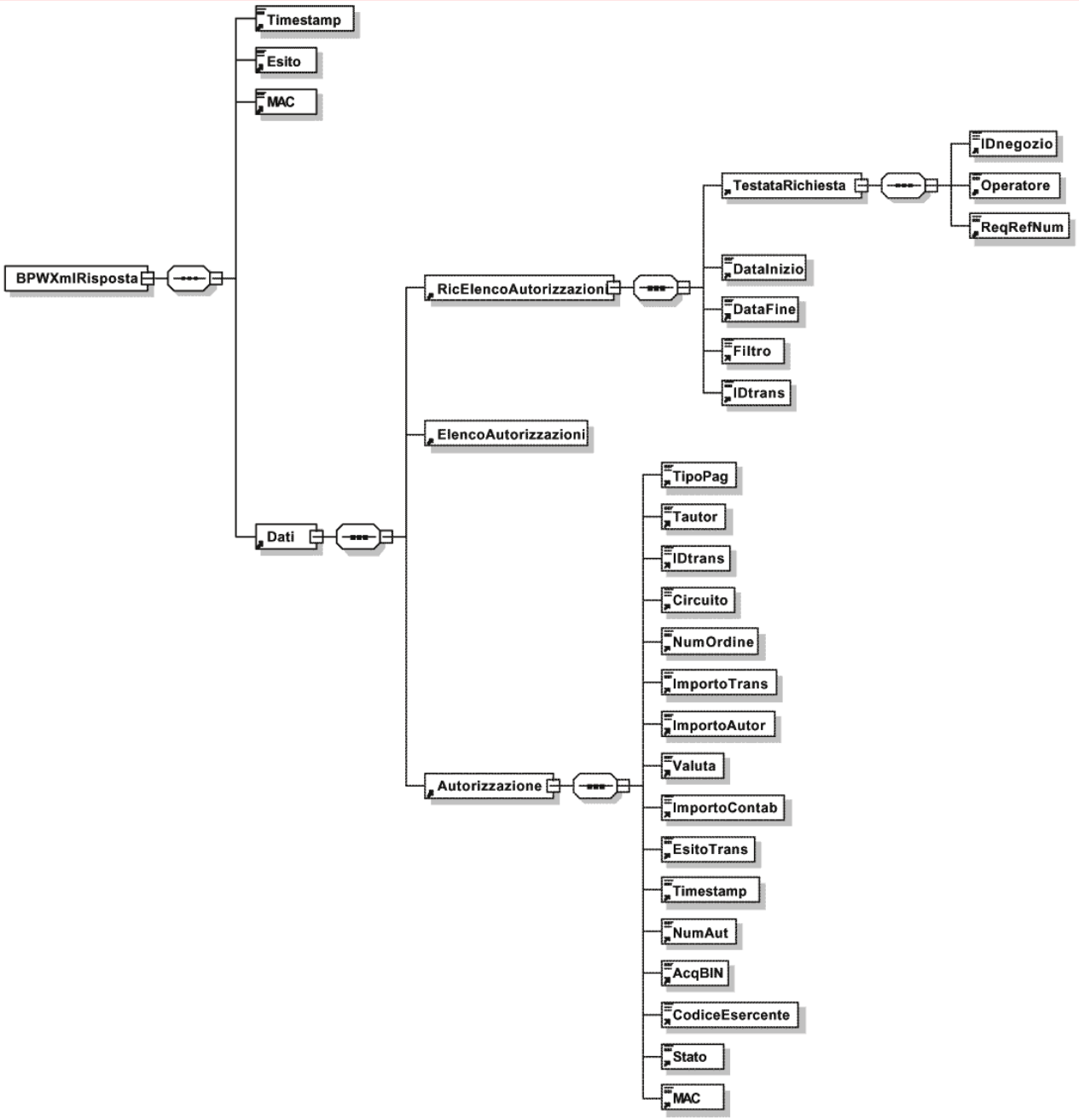
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "ELENCOAUTORIZZAZIONI"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
DATAINIZIO	N	10	D	Data di inizio periodo, formato yyyy-MM-dd
DATAFINE	N	10	D	Data di fine periodo, formato yyyy-MM-dd
FILTRO	Y	1	N	Tipo di elenco richiesto: 1. Solo quelle con esito POSITIVO 2. Solo quelle con esito negativo 3. Solo quelle stornate 4. Tutte
IDTRANS	N	25	AN	Identificativo univoco della transazione. Se presente il sistema ignorerà gli eventuali campi filtro, data e ora per recuperare la transazione indicata
ORAINIZIO	N	5	D	Ora di inizio periodo, formato HH.mm
ORAFINE	N	5	D	Ora di fine periodo, formato HH.mm
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D9

La ricerca puo' essere effettuata con una delle seguenti alternative:
1) Campo IDTRANS specificato: la ricerca sara' fatta considerando come parametro discriminante solo tale campo (ignorando eventuali campi filtro,data e ora)
2) Campo IDTRANS non specificato: la ricerca sara' fatta considerando i parametri FILTRO, DATAINIZIO, DATAFINE, ORAINIZIO, ORAFINE. I campi FILTRO, DATAINIZIO, DATAFINE sono in questo caso obbligatori mentre ORAINIZIO e ORAFINE possono non essere indicati.

Richiesta elenco autorizzazioni in formato XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
    <BPWXmlRichiesta>
        <Release>02</Release>
        <Richiesta>
            <Operazione>ELENCOAUTORIZZAZIONI</Operazione>
            <Timestamp>2005-03-04T11:20:00.000</Timestamp>
            <MAC>115025d5a5b65df687790867bdece136</MAC>
        </Richiesta>
        <Dati>
            <RicElencoAutorizzazioni>
                <TestataRichiesta>
                    <IDnegozio>000000000000003</IDnegozio>
                    <Operatore>oper0001</Operatore>
                    <ReqRefNum>12345678901234567890123452289000</ReqRefNum>
                </TestataRichiesta>
                <DataInizio>2003-12-01</DataInizio>
                <DataFine>2003-12-31</DataFine>
                <Filtro>1</Filtro>
                <IDtrans/>
                <OraInizio>00.00</OraInizio>
                <OraFine>18.25</OraFine>
            </RicElencoAutorizzazioni>
        </Dati>
    </BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di elenco autorizzazioni è formattato in XML ed è schematizzato qui di seguito.



La risposta ad una richiesta di elenco delle autorizzazione è costituita da un insieme di elementi di tipo Autorizzazione. Nel caso in cui si verifichi un errore l'elemento ElencoAutorizzazioni non viene creato.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta di elenco delle autorizzazioni:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <!-- L'lemento che segue contiene i dati della richiesta fatta -->
        <RicElencoAutorizzazioni>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>200305014962046909345843058345 64</ReqRefNum>
            </TestataRichiesta>
            <DataInizio>2001-01-01</DataInizio>
            <DataFine>2001-07-10</DataFine>
            <OraInizio>10.00</OraInizio>
            <OraFine>18.30</OraFine>
            <Filtro>1</Filtro>
            <IDtrans> C39564565845757564564565636</IDtrans>
        </RicElencoAutorizzazioni>
        <ElencoAutorizzazioni NumeroElementi="2"/>
        <Autorizzazione>
            <Tautor>I</Tautor>
            <IDtrans> C39564565845757564564565636</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>10000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>10000</ImportoContab>
            <ImportoStornato>100</ ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>01</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>4ab34c3a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Autorizzazione>
        <Autorizzazione>
            <Tautor>D</Tautor>
            <IDtrans> C39564565845757564564565636</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>5000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>5000</ImportoContab>
            <ImportoStornato>100</ ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>03</Stato>
            <!-- Questa MAC firma la autorizzazione  -->
            <MAC>aab3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>

E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
05	Data errata, o periodo indicato vuoto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di elenco autorizzazioni e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di elenco autorizzazioni e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicElencoAutorizzazioni>** i dati relativi alla richiesta di elenco autorizzazioni
- **<ElencoAutorizzazioni>** i dati relativi all'elenco autorizzazioni

< RicElencoAutorizzazioni>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati riferiti alla richiesta di elenco autorizzazioni rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<DataInizio>** la data di inizio periodo dell'elenco
- **<DataFine>** la data di fine periodo dell'elenco
- **<OraInizio>** ora di inizio periodo dell'elenco, se indicata nella richiesta
- **<OraFine>** ora di fine periodo dell'elenco, se indicata nella richiesta
- **<Filtro>** il tipo di elenco richiesto
  1 – Autorizzazioni con esito positivo (Stati : 00 – 02 – 03 – 10)
  2 – Autorizzazioni negate (Stati : 01 – 21)
  3 – Autorizzazioni stornate (Stati : 04 – 05 – 20)
  4 – Tutte le autorizzazioni
- **<IDtrans>** ID della transazione da cercare

<TestataRichiesta>

Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDNegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<ElencoAutorizzazioni>
Questo elemento, se presente, contiene nell'attributo NumeroElementi il numero di autorizzazioni che sono riportate.

<Autorizzazione>
Esistono N occorrenze di questo elemento. Ognuna di esse racchiude i dati di una autorizzazione dell'elenco. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Richiesta situazione di un ordine

Questa operazione restituisce la situazione attuale di un ordine con tutte le operazioni di autorizzazione ad esso legate. Lo scopo principale di questo messaggio è quello di rendere possibile ai merchant system la verifica dello stato di eventuali ordini rimasti "pending" durante il pagamento.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

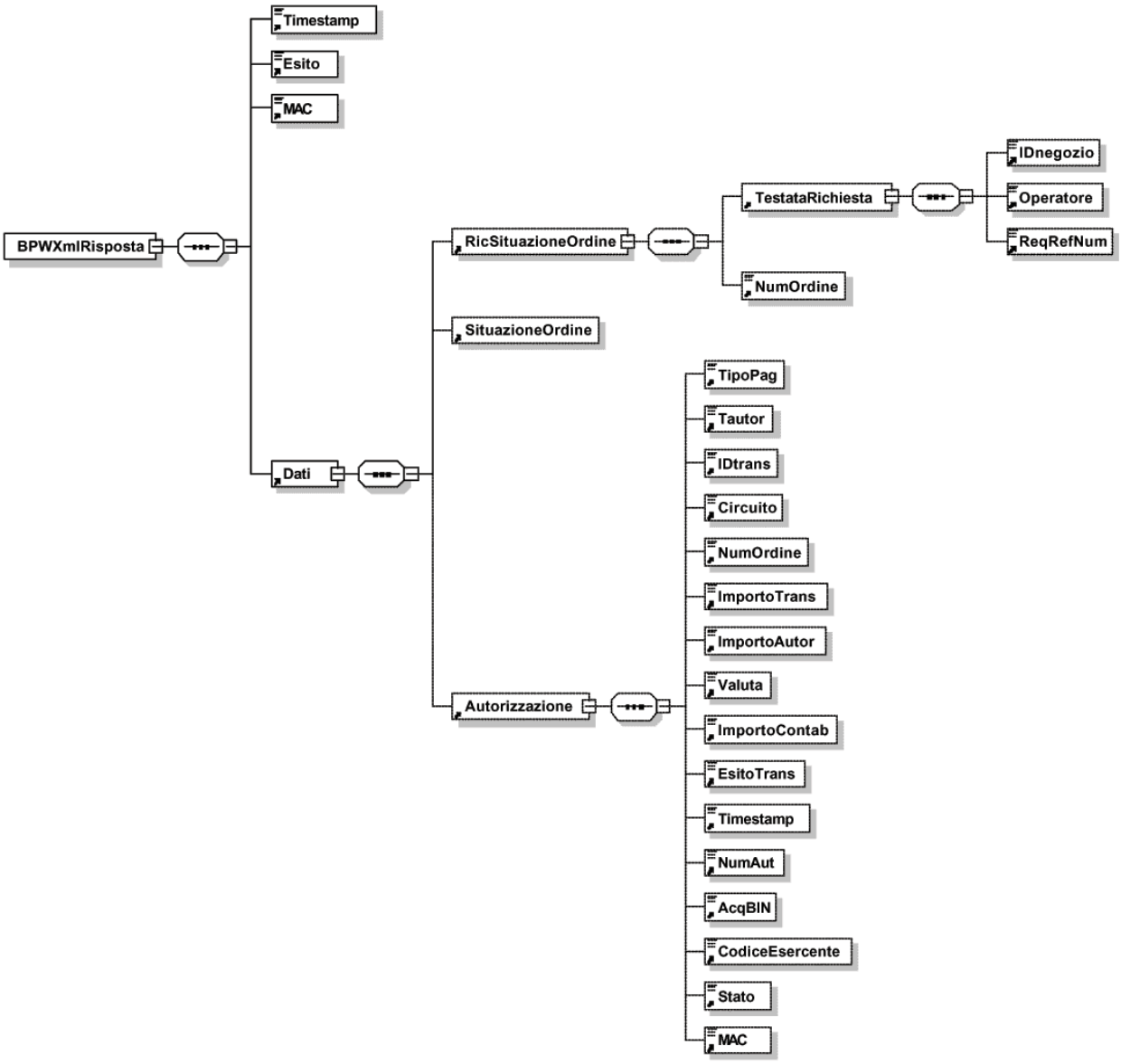
Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta: valorizzato con "SITUAZIONEORDINE"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio del merchant assegnato da SIA, Merchant ID(MID)
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente . Può essere usato per il recupero delle informazioni in merito alla richiesta fatta anche nel caso di mancata risposta. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
NUMORD	Y	Min.1 Max.50	AN	Identificatore univoco dell'ordine corrispondente all'IDTRANS passato
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione.Per il calcolo si veda appendice D10

Richiesta situazione di un ordine in formato XML

* ATTENZIONE: nel tracciato XML al campo NUMORD corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
    <BPWXmlRichiesta>
        <Release>02</Release>
        <Richiesta>
          <Operazione>SITUAZIONEORDINE</Operazione>
          <Timestamp>2005-03-04T11:20:00.000</Timestamp>
          <MAC>115025d5a5b65df687790867bdece136</MAC>
         </Richiesta>
         <Dati>
           <RicSituazioneOrdine>
            <TestataRichiesta>
                    <IDnegozio>000000000000003</IDnegozio>
                    <Operatore>oper0001</Operatore>
                    <ReqRefNum>12345678901234567890123452289000</ReqRefNum>
                </TestataRichiesta>
                <NumOrdine>9998500000000015</NumOrdine>
            </RicSituazioneOrdine>
          </Dati>
      </BPWXmlRichiesta>
```

Il messaggio di risposta alla richiesta di situazione ordine è formattato in XML ed è schematizzato qui di seguito.



La risposta ad una richiesta di situazione ordine è costituita da un insieme di elementi di tipo Autorizzazione: questi sono le varie autorizzazioni che sono legate al numero d'ordine indicato. Nel caso si tratti di un ordine elaborato con autorizzazione immediata sarà presente una sola autorizzazione.
Nel caso in cui si verifichi un errore non sarà presente alcun elemento Autorizzazione.

Di seguito viene riportato un esempio di file generato dalla risposta alla richiesta della situazione di un ordine:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<BPWXmlRisposta>
```

```
    <Timestamp>2001-07-04T12:02:55</Timestamp>
    <Esito>00</Esito>
    <MAC>ffb3553a4ab34c3a4ab34c3a4ab34c3a</MAC>
    <Dati>
        <RicSituazioneOrdine>
            <TestataRichiesta>
                <IDnegozio>23486788</IDnegozio>
                <Operatore>A4348B</Operatore>
                <ReqRefNum>20030501496204690934584305834564</ReqRefNum>
            </TestataRichiesta>
            <NumOrdine>12348A33</NumOrdine>
        </RicSituazioneOrdine>
        <SituazioneOrdine NumeroElementi="2"/>
        <Autorizzazione>
            <Tautor>I</Tautor>
            <IDtrans> C3556456584575645645656 36</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>10000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>10000</ImportoContab>
            <ImportoStornato>100</ ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-09T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>01</Stato>
            <MAC>12334c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
        </Autorizzazione>
        <Autorizzazione>
            <Tautor>D</Tautor>
            <IDtrans> C3556456584575645645656 36</IDtrans>
            <Circuito>01</Circuito>
            <NumOrdine>A398459</NumOrdine>
            <ImportoTrans>10000</ImportoTrans>
            <ImportoAutor>5000</ImportoAutor>
            <Valuta>978</Valuta>
            <ImportoContab>5000</ImportoContab>
            <ImportoStornato>100</ ImportoStornato>
            <EsitoTrans>00</EsitoTrans>
            <Timestamp>2001-07-02T21:05:44</Timestamp>
            <NumAut>A93485</NumAut>
            <AcqBIN>123450943</AcqBIN>
            <CodiceEsercente>09834509</CodiceEsercente>
            <Stato>03</Stato>
            <MAC>bbb34c3a4ab34c3a4ab34c3a4ab3ffa1</MAC>
        </Autorizzazione>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
01	Ordine, o ReqRefNum non trovato
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
07	Idtrans non trovato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile
99	Operazione fallita, vedere l'esito specifico allegato all'elemento <Dati> della risposta.

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di situazione ordine e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di situazione ordine e del messaggio di risposta rappresentati dai seguenti elementi:

- **<RicSituazioneOrdine>** i dati relativi alla richiesta di situazione ordine
- **<SituazioneOrdine>** i dati relativi alla situazione ordine (numero autorizzazioni)
- <Autorizzazione> autorizzazione associata all'ordine

< RicSituazioneOrdine>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati riferiti alla richiesta di situazione ordine rappresentati dai seguenti elementi:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata
- **<NumOrdine>** numero ordine di cui si vuole la situazione

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDnegozio>** l'identificatore del negozio(MID)
- **<Operatore>** l'identificatore dell'operatore(User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<Autorizzazione>
Possono esistere più elementi di questo tipo. Ogni elemento rappresenta una autorizzazione legata all'ordine passato. Per la descrizione dettagliata si veda il capitolo "I messaggi di risposta in XML"

Richiesta di recupero alias pan

Questa operazione restituisce l'alias pan generato dall'autorizzazione di un determinato ordine del negozio.

I campi da specificare nel messaggio HTTP di richiesta sono i seguenti:

Campo	Obbligatorio	Dim.	Tipo	Descrizione
OPERAZIONE	Y		A	Operazione richiesta. Da valorizzare con "RECUPERAALIASPAN"
TIMESTAMP	Y	23	AN	Timestamp locale del tipo yyyy-MM-ddTHH:mm:ss.SSS
IDNEGOZIO	Y	15	AN	Identificatore del negozio assegnato da SIA [MID]
OPERATORE	Y	8	AN	Indica chi ha richiesto l'operazione. Deve essere passata la User ID di un operatore valido assegnato da @POS.
REQREFNUM	Y	32	N	Identificatore univoco della richiesta gestito dall'esercente. I primi 8 caratteri devono avere il formato yyyyMMdd con la data della richiesta.
IDORDINE	Y	Max.50	AN	Identificatore univoco dell'ordine da ricercare.
RELEASE	N	2	N	Release delle API: da valorizzare con "02"
MAC	Y	32/40	AN	Campo di firma della transazione. Per il calcolo si veda appendice D20

Richiesta recupero alias pan in formato XML

* ATTENZIONE: nel tracciato XML al campo IDORDINE corrisponde un tag di nome NumOrdine, per compatibilità con il tracciato XML di risposta.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
    <BPWXmlRichiesta>
        <Release>02</Release>
        <Richiesta>
          <Operazione>RECUPERAALIASPAN</Operazione>
          <Timestamp>2015-05-04T11:20:00.000</Timestamp>
          <MAC>115025d5a5b65df687790867bdece136</MAC>
         </Richiesta>
         <Dati>
           <RicSituazioneOrdine>
             <TestataRichiesta>
                    <IDnegozio>000000000000003</IDnegozio>
                    <Operatore>oper0001</Operatore>
                    <ReqRefNum>12345678901234567890123452289000</ReqRefNum>
                </TestataRichiesta>
                <NumOrdine>9998500000000015</NumOrdine>
            </RicSituazioneOrdine>
        </Dati>
    </BPWXmlRichiesta>
```

Nella risposta, che è in formato XML, viene inserito l'elemento <**DatiAliasPan**> (presente se e solo se la richiesta di autorizzazione e la creazione alias pan hanno esito positivo).

Esempio risposta API XML in cui viene restituito il codice alias pan:

```
<BPWXmlRisposta>
    <Timestamp>2015-04-14T12:22:29</Timestamp>
    <Esito>00</Esito>
    <!-- Questa MAC firma il timestamp e l'esito -->
    <MAC>8CB2123794B2BD1BB0064469C7D58776</MAC>
    <Dati>
        <!-- L'elemento che segue contiene i dati della richiesta fatta -->
        <RicRecuperaAliasPan>
            <TestataRichiesta>
                <IDnegozio>120500000511889</IDnegozio>
                <Operatore> AF06TSTAPI1</Operatore>
                <ReqRefNum>20150414122156000000000000000004</ReqRefNum>
            </TestataRichiesta>
            <NumOrdine>1234567890000</NumOrdine>
        </RicRecuperaAliasPan>
        <DatiAliasPan>
            <AliasPan>0000203536626636411</AliasPan>
            <AliasPanDataScad>1505</AliasPanDataScad>
            <AliasPanTail>7090</AliasPanTail>
            <!--  Questa MAC firma l'alias del pan  -->
            <MAC>0C34C72514DD753029B186B1282FFD5E</MAC>
        </DatiAliasPan>
    </Dati>
</BPWXmlRisposta>
```

Il significato degli elementi è il seguente:

<BPWXmlRisposta>
E' il root element del documento, esiste un unico elemento di questo tipo nel messaggio, esso è composto dai seguenti elementi:

- **<Timestamp>** la data e l'ora del messaggio di risposta
- **<Esito>** l'esito dell'operazione richiesta

Codice	Descrizione
00	Successo
02	ReqRefNum duplicato od errato
03	Formato messaggio errato, campo mancante o errato
04	Autenticazione API errata, MAC non corretto
06	Errore imprevisto durante l'elaborazione della richiesta
38	Ordine non trovato o alias revocato
40	Xml vuoto o parametro 'data' mancante
41	Xml non parsabile

- **<MAC>** firma del timestamp e dell'esito. Vedi appendice D11
- **<Dati>** i dati della richiesta di recupero alias pan e del messaggio di risposta

<Dati>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati della richiesta di recupero alias e del messaggio di risposta rappresentati dai seguenti elementi:

- **< RicRecuperaAliasPan>** i dati relativi alla richiesta di recupero alias
- **< DatiAliasPan>** i dati relativi all'alias recuperato

<RecuperaAliasPan>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati riferiti alla richiesta di recupero alias pan rappresentati dal seguente elemento:

- **<TestataRichiesta>** i dati relativi alla richiesta inviata

- **<NumOrdine>** identificativo dell'ordine che ha generato l'alias

<TestataRichiesta>
Esiste un unico elemento di questo tipo nel messaggio e racchiude i dati relativi alla richiesta inviata rappresentati dai seguenti elementi:

- **<IDnegozio>** l'identificatore del negozio (MID)
- **<Operatore>** l'identificatore dell'operatore (User ID)
- **<ReqRefNum>** identificatore univoco della richiesta gestito dall'esercente

<DatiAliasPan>
Esiste un unico elemento di questo tipo nel messaggio di risposta ed è così composto:

- **<AliasPan>** Alias Pan. Stringa numerica di lunghezza 19
- **<AliasPanDataScad>** Data scadenza. Stringa numerica di lunghezza 4, in formato AAMM
- **<AliasPanTail>** Ultime 4 cifre del pan.
- **<MAC>** Firma dell'elemento DatiAliasPan

Integrazione Redirect @POS

L'interfacciamento tra il negozio virtuale ed il sistema @POS avviene per mezzo di semplici messaggi http. Una volta che l'utente finale ha terminato la fase di acquisto il negozio virtuale reindirizza il browser verso il sistema @POS. Il reindirizzamento (redirect) può avvenire tramite una form, un link, o una vera e propria redirect http (response 30x). Nel reindirizzamento vengono passati una serie di parametri che permettono al sistema @POS di riconoscere la provenienza della richiesta e di predisporre quanto necessario a far si che il cliente possa portare a termine la transazione di pagamento. A questo punto il compratore è chiamato a compilare una semplice form contenente i dati della carta di credito, il tipo di carta (fra quelle accettate dal negozio), il suo indirizzo e-mail etc. L'utente ha comunque la possibilità di annullare l'operazione e di tornare al negozio.
Ad operazione conclusa il titolare sarà "rimandato" al sito di provenienza con i dati necessari a verificare l'avvenuto pagamento, e contemporaneamente il sistema @POS provvederà ad inviare al negozio una notifica via http.

Per rendere possibile l'indirizzamento del browser dell'utente verso le pagine corrette del negozio virtuale, nel primo messaggio inviato al sistema @POS il negozio virtuale inserisce tre campi speciali che contengono tre URL:

- La URL verso la quale mandare l'utente in caso di annullamento del processo di pagamento e ritorno alla modifica del carrello (URLBACK)
- La URL verso la quale mandare l'utente in caso di completamento della transazione con esito positivo (URLDONE)
- La URL che il sistema @POS deve utilizzare per notificare direttamente al negozio l'esito della transazione compiuta (URLMS)

Le URL di accesso al servizio sono le seguenti:
Ambiente di TEST: http://atpostest.ssb.it/atpos/pagamenti/main?PAGE=MASTER
Ambiente di PRODUZIONE: https://atpos.ssb.it/atpos/pagamenti/main?PAGE=MASTER

Messaggi e-Mail

A fronte dell'esecuzione da parte dei consumatori di una operazione di pagamento, il server SIA può generare e spedire, al cliente e all'esercente, alcune e-mail.
L'invio delle e-mail all'esercente è configurabile in fase di adesione del negozio al servizio e prevede una scelta tra le seguenti casistiche:

1. Mai
2. Sempre
3. Per soli esiti positivi
4. Sempre (formato dati XML)
5. Per soli esiti positivi (formato dati XML)

Una eventuale variazione dell'indirizzo e-mail dell'esercente potrà essere effettuata comunicando il nuovo indirizzo a SIA.

L'invio delle e-mail al consumatore invece avviene sempre, secondo i seguenti due casi:

Autorizzazione online concessa
1. E-mail transazione OK online al cliente

Autorizzazione online negata
2. E-mail transazione negata online al cliente (riportante il motivo della negazione)

Le informazioni presenti nei messaggi di e-mail possono essere in formato standard o in formato XML.

Nel caso di formato standard il contenuto, dove applicabile, è il seguente:

- Data della transazione
- Numero d'ordine
- Importo
- Numero di autorizzazione
- Insegna negozio

Il formato XML è invece previsto solo per l'invio e-mail all'esercente e corrisponde all'elemento Autorizzazione delle API @POS. Il subject delle e-mail in tale formato sarà: "Autorizzazione: numero ordine <NumeroOrdine>"

I messaggi inviati da SIA non sono personalizzabili.

Redirect di avvio pagamento @POS

Il primo passo che il merchant system deve compiere è far generare al browser del cliente un messaggio di avvio del processo di pagamento verso SIA. Questo può essere fatto sia con una redirezione, od un link, (utilizzando quindi il metodo HTTP GET) sia attraverso l'invio di una form con campi nascosti (che può utilizzare il metodo HTTP POST).

Il messaggio di avvio della transazione che arriva a SIA dal browser dell'utente deve contenere i seguenti campi:

Nome	Obbligatorio	Descrizione
IMPORTO	S	Importo espresso nell'unità minima della valuta (centesimi di euro). Lunghezza minima 2 massima 8
VALUTA	S	Valuta: codice ISO (EUR = 978)
NUMORD	S	Identificativo univoco dell'ordine: deve essere un codice alfa-numerico lungo al massimo 50 caratteri. **La sua univocità deve essere garantita per almeno 5 anni**. I caratteri ammessi sono lettere, cifre, "-" e "_". Viene applicata la regular expression [a-zA-Z0-9\-_]
IDNEGOZIO	S	Identificatore del negozio del merchant assegnato dalla BANCA, Codice Riconoscimento Negozio(CRN)
URLBACK	S	URL completa verso la quale eseguire una redirect per rimandare l'utente al negozio (può comprendere tutti gli eventuali parametri da passare) nel caso di annullamento del processo di pagamento. Lunghezza massima 254 caratteri
URLDONE	S	URL completa verso la quale redirigere il browser del cliente a transazione avvenuta con successo (può comprendere tutti gli eventuali parametri da passare). Il sistema appende ad essa i parametri dell'esito. Lunghezza massima 254 caratteri
URLMS	S	URL del merchant system verso la quale SIA effettua la GET o POST di conferma dell'avvenuto pagamento. (può contenere eventuali parametri impostati dal negozio). Il sistema appende ad essa i parametri dell'esito. Lunghezza massima 400 caratteri
TCONTAB	S	Tipo di contabilizzazione da utilizzare per questo ordine: • D differita • I immediata Vedi appendice E
TAUTOR	S	Tipo di autorizzazione da utilizzare per questo ordine: • D differita • I immediata Vedi appendice E
MAC	S	Campo di firma della transazione: rende immodificabile da parte dell'utente finale i dati dell'ordine. Per il calcolo si veda appendice C1.
LINGUA	N	Lingua nella quale devono essere mostrati i messaggi di interazione con l'utente finale. Il campo è facoltativo; di default la lingua è quella Italiana.

		Attualmente sono disponibili: ITA italiano EN inglese
EMAILESERC	N	Contiene l'indirizzo e-mail al quale inviare la e-mail di esito della transazione. Se non è presente viene utilizzato quello disponibile nella anagrafica SIA del negozio. Lunghezza minima 7 caratteri alfanumerici massima 50
OPTIONS	N	Contiene gli indicatori delle opzioni aggiuntive che si intende attivare per il pagamento in corso. L'ordine con il quale appaiono le opzioni e' indifferente. Il contenuto del campo non e' case sensitive. Vedere paragrafo corrispondenti per dettagli ulteriori
LOCKCARD	N	Contiene il codice circuito corrispondente al tipo di strumento di pagamento con cui l'esercente desidera che venga effettuato il pagamento. I valori possibili per questo parametro sono: **01** – Visa **02** – Mastercard **04** – Maestro **05** – Cirrus **06** – American Express **07** – Diners **08** – JCB **10** – Aura **49** – Paypass **94** – Postepay **96** – MyBank **97** – Paypal **CC** – Carte di credito **NC** – Altri strumenti di pagamento Se viene indicato come strumento predefinito una carta di credito l'utente verrà inviato alla pagina di scelta dello strumento di pagamento con il campo circuito preselezionato e non modificabile. Per i circuiti **49** - Paypass e **97** – Paypal l'utente verrà rediretto automaticamente alla pagina di login del relativo strumento di pagamento, senza che venga visualizzata la pagina di scelta dello strumento. Per il circuito **96** – MyBank l'utente verrà inviato alla pagina di scelta della propria banca, senza che venga visualizzata la pagina di scelta dello strumento. Indicando il circuito **CC** la pagina di scelta dello strumento di pagamento conterrà e permetterà di scegliere solo le carte di credito. Indicando il circuito **NC** la pagina di scelta dello strumento di pagamento conterrà e permetterà di selezionare solo i circuiti diversi da carte di credito.

		Se il campo è valorizzato con **NC** e si verifica un errore durante il processo di pagamento l'utente viene inviato alla pagina URLBACK.
COMMIS	N	Importo della commissione sul servizio espresso nell'unità minima della valuta (centesimi di euro). Si tenga presente che il parametro IMPORTO è comprensivo della commissione. NOTA BENE: il parametro COMMIS, se presente, è significativo se e solo se è stata impostata anche l'opzione aggiuntiva OPTIONS = F (pagamento con commissione su servizio). Lunghezza minima 1 massima 8.
EMAIL	N	Indirizzo di e-mail del cliente. Se il campo non è presente verrà richiesto all'utente insieme ai dati della carta di credito. Lunghezza minima 7 caratteri alfanumerici massima 50.
DESCRORD	N	Descrizione ordine (vedere OPTIONS O). Lunghezza massima 140.
IDVS	N	Identificativo validation service per transazioni mybank. Se presente fa saltare la pagina di scelta della banca mybank redirigendo l'utente sulla home banking associata all'identificativo ricevuto. Lunghezza massima 35.
DESCROP	N	Descrizione aggiuntiva dell'operazione di contabilizzazione, a discrezione dell'esercente (solo per contabilizzazione immediata). Lunghezza massima 100.

Obbligatorio: S = si, N = no

Nota: i nomi dei campi delle tabelle sopra riportate sono tutti maiuscoli e sono case sensitive.

L'ordine nel quale appaiono i campi nel messaggio di avvio è indifferente.

Nel processo di comunicazione tra il merchant e SIA vi è il rischio che un soggetto estraneo, intercettato il messaggio, cerchi di alterarne il contenuto, rispedendolo poi al destinatario finale. Questo evento può essere scoperto introducendo un processo di autenticazione tramite un MAC (Message Authentication Code) dei messaggi che vengono trasmessi.

Il metodo seguito per generare il MAC è il seguente: viene calcolato un hash MD5 o SHA-1 della stringa risultante dal concatenamento dei parametri da trasmettere e di una stringa segreta (stringa di 50 caratteri, condivisa da SIA e dal singolo merchant system). Il destinatario, possedendo la stessa stringa segreta, può verificare il MAC e quindi l'autenticità dei parametri ricevuti.
Esistono due stringhe segrete in possesso dell'esercente:

- "**chiave di avvio**": è la stringa per il calcolo del MAC nei messaggi di avvio pagamento sopra descritto
- "**chiave di esito-API**": è la stringa per la verifica del MAC nei messaggi di esito emessi da SIA e per l'uso delle API @POS

I metodi per calcolare il MAC relativo alle richieste di pagamento e agli esiti (comunicati da SIA) sono indicati rispettivamente nelle appendici C1 e C2 di questo documento. Le stringhe segrete vengono comunicate, in maniera sicura, al negozio da SIA al momento dell'attivazione del servizio.

Il contenuto dei campi URLDONE , URLBACK ed URLMS è a completa discrezione del negozio. Per quanto riguarda URLDONE ed URLMS si tenga presente che i dati identificativi dell'ordine vengono comunque appesi da SIA in fondo a queste due stringe come viene documentato nel paragrafo sottostante. La lunghezza massima di URLDONE e URLBACK è di 254 caratteri mentre dell'URLMS è di 400 caratteri.

Se le stringhe originali che rappresentano le URL del merchant system comprendono parametri o dei caratteri particolari, esse dovranno essere passate in formato MIME application/x-www-form-urlencoded (I caratteri particolari sono trasformati in %XX). La conversione avviene automaticamente a carico dei browser se si utilizza la submit di una form, mentre se si utilizza una redirect deve essere realizzata a cura del negozio virtuale.

La redirezione del browser dell'utente verso le URL URLDONE ed URLBACK è effettuata tramite il metodo HTTP GET.

Le URL URLDONE e URLBACK devono cominciare con "http://" o "https//" (o un qualsiasi altro schema HTTP valido interpretabile dai browser).
La URL URLMS deve cominciare con http:// o "https://; **la porta utilizzata non può essere diversa da quella standard: 80 per http, 443 per https**.
I valori sopra indicati devono comunque rispettare la prima indicazione , cioè devono essere trasmessi in formato MIME application/x-www-form-urlencoded.

Campo OPTIONS

Il campo OPTIONS permette di attivare varie opzioni aggiuntive per il pagamento in corso. Le opzioni sono indicate tramite una lettera dell'alfabeto. Le opzioni oggi disponibili sono:

- **B** – Il sistema accetta due ulteriori campi nel messaggio in ingresso: NOME e COGNOME. Il valore di tali campi, se presenti, viene memorizzato associato all'ordine in corso. I campi non sono modificabili dal cliente e non sono visualizzati. Per garantire la non modificabilità dei valori i campi entrano a par parte della stringa per il calcolo del MAC. I campi NOME e COGNOME non sono comunque obbligatori.

- **F** – Il sistema accetta la valorizzazione del campo COMMIS indicante l'importo della commissione sul servizio.

- **G** – In caso di autorizzazione concessa il sistema invece di mostrare l'esito della transazione al consumatore effettua la redirezione immediata presso URLDONE in modo che il negozio virtuale possa mostrare un proprio "scontrino" personalizzato. In caso di autorizzazione negata all'utente viene riproposta la schermata di inserimento carta.

- **I** – Nel caso di autorizzazione concessa, il sistema aggiunge alle informazioni già presenti nell'URLMS e nell'URLDONE anche il campo BPW_ISSUER_COUNTRY che contiene l'informazione della nazione di provenienza dell'issuer.

- **L** – Nel caso di ordine duplicato il sistema invia una URLMS con codice di esito 07.

- **M** – L'utilizzo della OPTION M è associata alla abilitazione al servizio di ALIAS PAN (a discrezione della banca aderente). Nel caso di autorizzazione concessa viene generato un Alias Pan che viene restituito nella URLMS ed URLDONE nel campo ALIASPAN. Per i dettagli relativi a tale funzionalità aggiuntiva fare riferimento al manuale specifico di integrazione.

- **N** – In caso di autorizzazione negata il sistema, invece di mostrare l'esito della transazione al consumatore, effettua la redirezione immediata verso URLDONE.

- **O** – Richiede, nelle transazioni myBank, di inserire nel campo D13 (*remittance information*) il valore del campo DESCRORD (descrizione ordine) invece del NUMORD (numero d'ordine), come da comportamento ordinario.

- **P** – Viene restituito, in URLMS E URDONE, il campo RESPONSE_CODE_AUT che rappresenta il codice di risposta ritornato dal backend autorizzativo.

- **Q –** per i pagamenti effettuati con Paypal il sistema aggiunge nelle URLMS e URLDONE anche le seguenti informazioni aggiuntive: PAYERID, PAYER e PAYERSTATUS.

- **R –** Il MAC viene calcolato ed inviato negli URLMS e URLDONE anche in caso di esito negativo. Le regole di *maccatura* sono le medesime adottate dallo scenario positivo.

L'ordine con il quale le opzioni appaiono non è rilevante.
Le opzioni possono essere indifferentemente indicate con lettere maiuscole o minuscole: *OPTIONS=b* equivale a *OPTIONS=B*

Esempio

L'esempio sotto riportato non è funzionante: fornisce solo una indicazione di massima di come poter avviare il processo di pagamento tramite una form.

```
<html>
<body>
<br><center>
@POS

<form action="http://atpostest.ssb.it/atpos/pagamenti/main" method="POST">

        <input type="hidden" name="PAGE" value="MASTER">
        IMPORTO=1050<br>
        <input type="hidden" name="IMPORTO"  value="5000">
        VALUTA=978<br>
        <input type="hidden" name="VALUTA"  value="978">
        LINGUA=ITA<br>
        <input type="hidden" name="LINGUA"  value="ITA">
        IDNEGOZIO=000000000000001<br>
        <input type="hidden" name="IDNEGOZIO"  value="129280000000211">
        NUMORD=7893133444445<br>

        <input type="hidden" name="NUMORD"  value="7893133444445">

        <input type="hidden" name="URLDONE"
value="http://demo.demo.net/mimesys/urlok.html?oper=900">
        <input type="hidden" name="URLBACK"
value="http://demo.demo.net/demoshop/backfromtl.html?IdShop=00000000000">
        <input type="hidden" name="URLMS"
value="http://demo.ssb.net/index.html?EMAILCLI=prova@demo.net&CARRELLO=02">
        <input type="hidden" name="TCONTAB" value="D">
        <input type="hidden" name="TAUTOR" value="I">
        <input type="hidden" name="OPTIONS" value="G">
        <input type="hidden" name="EMAIL" value="prova@demo.net">
        <input type="hidden" name="EMAILESERC" value="prova2@demo.net">
        <input type="hidden" name="MAC" value="376b61c1189ca70ef88e49c5d3631be7">

        <input type=submit value="Avvia..." >
</form>
</body>
</html>
```

Le URL nei campi hidden devono essere riportate normalmente perché i browser provvedono automaticamente ad eseguire la necessaria codifica quando l'utente esegue la submit.

Messaggio di conferma/esito dell'avvenuto pagamento

L'esito dell'operazione, in caso di autorizzazione concessa, viene comunicato al merchant system tramite due distinti percorsi. Il primo passa dal browser dell'utente, il secondo avviene direttamente dal server di SIA verso il negozio.

In particolare l'esito viene comunicato al merchant utilizzando gli indirizzi indicati nei parametri URLDONE e URLMS, il primo viene contattato, a discrezione dell'acquirente, solo al termine della transazione; il secondo invece viene contattato dal server di SIA, indipendentemente dalle azioni del cliente, non appena il circuito autorizzativo risponde alla richiesta inoltrata dal sistema @POS. L'utilizzo del secondo indirizzo dà una buona certezza che l'esito della transazione venga comunicato al merchant system indipendentemente dalle azioni del cliente.

In fase di adesione si può scegliere se utilizzare URLMS per ottenere comunicazione tramite questo meccanismo solo per le transazioni con esito positivo, o per tutte le transazioni: con esito positivo e negativo. L'opzione consigliata è la prima: comunicazione dei soli esiti positivi.

Nel caso si scelga la seconda opzione bisogna tener presente il fatto che il cliente, in caso di insuccesso della prima transazione, può eseguire diversi tentativi di pagamento consecutivi per uno stesso ordine. In questo caso il merchant system si vedrebbe comunicare N esiti negativi per gli N insuccessi, ed alla fine un esito positivo.

Il messaggio di conferma della transazione contiene i seguenti dati:

Nome campo	**Descizione**
NUMORD	numero d'ordine: valore copiato dal campo del messaggio di avvio NUMORD
IDNEGOZIO	Codice Riconoscimento Negozio(CRN): valore copiato dall'omonimo campo del messaggio di avvio
AUT	Numero autorizzazione: identificativo della autorizzazione assegnato dall'emittente della carta (solo in caso di esito positivo). Se l'autorizzazione non è stata concessa, il campo è valorizzato con "NULL". E' una stringa di lunghezza massima 6 caratteri per tutti i circuiti escluso MyBank per il quale invece ha lunghezza fissa di 35 caratteri e contiene l'identificativo della transazione assegnato dal Validation Service. Non è significativo nel caso di transazione effettuata con circuito Paypal.
IMPORTO	Importo: valore copiato dall'omonimo campo del messaggio di avvio
VALUTA	Valuta: valore copiato dall'omonimo campo del messaggio di avvio
IDTRANS	Identificativo della transazione assegnato dal sistema @POS. E' una stringa di 25 caratteri
MAC	Valore per l'autenticazione del messaggio di conferma. Per il calcolo si veda l'appendice C2. E' una stringa di 32 o 40 caratteri
ESITO	Esito della transazione. Vedi pagina successiva
TAUTOR	Tipo di autorizzazione: I immediata D differita. Valore copiato dall'omonimo campo del messaggio di avvio
TCONTAB	Tipo di contabilizzazione: I immeditata D differita. Valore copiato dall'omonimo campo del messaggio di avvio
CARTA	Tipo di carta utilizzata dal cliente per il pagamento. Vedi pagina successiva
BPW_TIPO_TRANSAZIONE	Questo campo indica il tipo di transzione effettuato (cfr. tabella valori campo BPW_TIPO_TRANSAZIONE)
BPW_ISSUER_COUNTRY	Questo campo è presente nell'URLMS e nell'URLDONE solo se richiesto tramite options (I) e solo su autorizzazioni concesse; indica la nazione di provenienza dell'issuer della carta
PAYERID	Per OPTION "Q" e pagamenti tramite Paypal. Informazione aggiuntiva

	sull'acquirente. Stringa alfanumerica di massimo 13 caratteri.
PAYER	Per OPTION "Q" e pagamenti tramite Paypal. Informazione aggiuntiva sull'acquirente. Stringa alfanumerica di massimo 127 caratteri.
PAYERSTATUS	Per OPTION "Q" e pagamenti tramite Paypal. Informazione aggiuntiva sull'acquirente. Stringa alfanumerica di massimo 10 caratteri.
BPW_HASH_PAN	Hash MD5 della carta o, per transazioni paypal, del payerid, se il negozio è abilitato al servizio.

Il messaggio che il merchant system si vedrà recapitare alle URL URLMS ed URLDONE sarà così costituito:

URLMS:
URLMS + &<conferma> + &MAC=<mac>

URLDONE:
URLDONE +&<conferma> + &MAC=<mac>

Dove:
<conferma> = "NUMORD=<numero d'ordine> + &IDNEGOZIO=<merchant id> + &AUT=<numero autor> +&IMPORTO=<importo> +&IDTRANS= <id.transazione>&VAL=<valuta>&<TAUTOR>=<tipo autorizzazione>&ESITO=<esito>&BPW_TIPO_TRANSAZIONE =<tipo transazione>& BPW_ISSUER_COUNTRY =<nazione dell'issuer (se presente)>&CARTA=<tipo carta><TCONTAB>=<tipo contabil>"

Il campo ESITO può assumere i seguenti valori:

Codice	**Descrizione**
00	Successo
01	*Negata dal sistema*
02	*Negata per problemi sull'anagrafica negozio*
03	*Negata per problemi di comunicazione con i circuiti autorizzativi*
04	*Negata dall'emittente della carta*
05	*Negata per numero carta errato*
06	*Errore imprevisto durante l'elaborazione della richiesta*
07	*Ordine duplicato*

Nota: nella attuale implementazione l'unico valore assunto da ESITO in URLDONE è 00

Il campo CARTA può assumere i seguenti valori:

Codice	**Descrizione**
01	Visa
02	Mastercard
04	Maestro
06	Amex
07	Diners
08	JCB
10	Carta Aura
94	Postepay
96	MyBank
97	Paypal

Il campo BPW_TIPO_TRANSAZIONE può assumere i seguenti valori:

Codice	**Descrizione**

TT01	SSL
TT06	VBV
TT07	Secure Code
TT08	VBV Esercente
TT09	Secure Code Esercente
TT10	VBV Titolare non autenticato
TT11	Mail Order Telephone Order
TT13	SafeKey
TT14	SafeKey Esercente
TT15	SafeKey Titolare non autenticato

NOTA: in caso di transazioni con carte provenienti da wallet MasterPass il codice tipo transazione invece di essere nel formato "TTnn" sarà nel formato "TMnn". I numeri ed il significato del tipo di transazione restano invariati.

Ad URLMS ed URLDONE verrà appeso un "?" punto interrogativo nel caso in cui non sia già presente.

NOTA BENE: i nomi dei campi sono tutti maiuscoli e case sensitive; non deve essere fatta nessuna assunzione riguardo l'ordine con il quale i parametri sono passati nelle GET o POST HTTP.

Il campo MAC non viene calcolato nel caso in cui l'esito della transazione sia negativo, a meno che non sia stata richiesta la OPTION "R". Esso viene quindi normalmente valorizzato con la stringa costante "NULL".

Per ulteriori informazioni relative al calcolo e alla verifica del MAC per i messaggi di esito vedere l'appendice C2.

E' preciso compito del negozio ricalcolare il MAC utilizzando la stringa segreta "esito-API" in suo possesso, e verificare che esso coincida con quello inserito nel messaggio arrivato. In mancanza di questo processo di verifica è possibile che il merchant system consideri validi messaggi di conferma non autenticamente spediti da SIA ma inviati da terzi.

Nello sviluppo della integrazione si tenga presente che i messaggi HTTP recapitati ad URLDONE, URLMS ed URLBACK potranno in futuro, grazie all'evoluzione del sistema, presentare parametri aggiuntivi non inizialmente presenti. **Le applicazioni devono quindi ignorare eventuali parametri da loro non riconosciuti senza presentare malfunzionamenti**. Per evitare la sovrapposizione dei nomi dei parametri con quelli già utilizzati dagli esercenti, ogni eventuale nuovo parametro avrà il prefisso "**BPW_". L'uso di tale prefisso per i nomi dei propri parametri presenti in URLDONE, URLMS, od URLBACK può precludere la compatibilità dell'integrazione con le future versioni del sistema.**

Nel caso in cui la comunicazione al merchant system tramite URLMS fallisse non sono previsti meccanismi di ripetizione del messaggio. Il sito ha la possibilità di interrogare il sistema @POS tramite l'API @POS per verificare lo stato di eventuali ordini rimasti in stato "pending" durante la fase di pagamento.

Appendice B (Riferimenti)

Di seguito vengono indicate varie fonti dalla quali è possibile attingere risorse eventualmente utili per l'integrazione in un merchant system.

SIA S.p.A. non fornisce nessun tipo di garanzia né di supporto relativamente ai prodotti di terze parti sotto indicati.

Per ottenere l'hash MD5 o l'hash SHA-1 che costituisce il MAC il server SIA utilizza l'oggetto Java MessageDigest del JDK SUN.

Un modulo per calcolare hash MD5 in PERL è reperibile alla URL:

http://www.perl.com/CPAN-local/modules/by-module/MD5/

Alcuni moduli (commerciali) per calcolare l'hash MD5 in visual basic sono reperibili agli indirizzi:

http://www.aspencrypt.com/index.html
http://www.hotscripts.com/ASP/Scripts_and_Components/Security_Systems/
http://www.anei.com/aneimd5.asp
http://www.aspin.com/func/search?qry=md5&cat=all&IMAGE1.x=25&IMAGE1.y=7

In PHP3 è disponibile nelle librerie standard la funzione **md5** per effettuare il calcolo dell'hash su di una stringa.

Per la definizione dello standard MD5 si può consultare:

http://www.columbia.edu/~ariel/ssleay/rfc1321.html

Per la definizione dello standard SHA-1 si può consultare:

http://csrc.nist.gov/cryptval/shs.html

D1 Generazione del MAC per il messaggio RICHIESTAAUTORIZZAZIONE

Il MAC che deve essere trasmesso allegato ai messaggi di tipo RICHIESTAAUTORIZZAZIONE viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di RICHIESTAAUTORIZZAZIONE, il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD
- IMPORTO (se presente)
- VALUTA
- TCONTAB
- FINEORDINE

Il MAC sarà:

MAC = Hash (OPERAZIONE=RICHIESTAAUTORIZZAZIONE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>& OPERATORE=<operatore>& REQREFNUM=<numero richiesta>&IDTRANS=<idtrans>&NUMORD=<numero d'ordine>&IMPORTO=<importo> &VALUTA=<valuta>&TCONTAB=<tipo contab>&FINEORDINE=<fine ordine>&< stringa segreta **>)**

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=RICHIESTAAUTORIZZAZIONE&TIMESTAMP=2002-04-
08T13:04:21.852&IDNEGOZIO=123456789012345&
OPERATORE=KR839H&IDTRANS=CC842&REQREFNUM=200305014962046909345843058345 64&NUMORD=A4845b2&IMP
ORTO=100&VALUTA=978&TCONTAB=I&FINEORDINE=S&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D2 Generazione del MAC per il messaggio CHIUSURADIFFERITA

Il MAC che deve essere trasmesso allegato ai messaggi di tipo CHIUSURADIFFERITA viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di CHIUSURADIFFERITA il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD

Il MAC sarà:

MAC=Hash(OPERAZIONE=CHIUSURADIFFERITA&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numerorichiesta>&IDTRANS=<idtransazione>&NUMORD=<numero d'ordine>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=CHIUSURAAUTORIZZAZIONE&TIMESTAMP=2002-04-08T13:04:21.852
&IDNEGOZIO=123456789012345&OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&
IDTRANS=CC84HL2G&NUMORD=A4845b2&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D3 Generazione del MAC per il messaggio di STORNO

Il MAC che deve essere trasmesso allegato ai messaggi di STORNO viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di STORNO il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD
- IMPORTO
- VALUTA
- DESCROP (se presente)

Il MAC sarà:

MAC=Hash(OPERAZIONE=STORNO&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numerorichiesta>&IDTRANS=<idtransazione>&NUMORD=<numerod'ordine>&IMPORTO=<importo>&VALUTA=<valuta>&DESCROP=<descrop>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=STORNO&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=12345678901&
OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&IDTRANS=HK84HL2G&NUMORD=A4845b2&
IMPORTO=100&VALUTA=978&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D4 Generazione del MAC per il messaggio CONTABILIZZAZIONE

Il MAC che deve essere trasmesso allegato ai messaggi CONTABILIZZAZIONE viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi CONTABILIZZAZIONE il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD
- IMPORTO
- VALUTA
- DESCROP (se presente)

Il MAC sarà:

MAC=Hash (OPERAZIONE=CONTABILIZZAZIONE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numerorichiesta>&IDTRANS=<idtransazione>&NUMORD=<numerod'ordine>&IMPORTO=<importo>&VALUTA=<valuta>&DESCROP=<descrop>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=CONTABILIZZAZIONE&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=1234567890123456&
OPERATORE=KR839H&REQREFNUM=200305014962046909345843058345645&IDTRANS=HK84HL2G&NUMORD=A4845b2&
IMPORTO=100&VALUTA=978&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D5 Generazione del MAC per il messaggio ANNULLAMENTOCONTABILIZZAZIONE

Il MAC che deve essere trasmesso allegato ai messaggi ANNULLAMENTOCONTABILIZZAZIONE viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi ANNULLAMENTOCONTABILIZZAZIONE il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD

Il MAC sarà:

MAC=Hash(OPERAZIONE=ANNULLAMENTOCONTABILIZZAZIONE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numerorichiesta>&IDTRANS=<idtransazione>&NUMORD=<numerod'ordine>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=ANNULLAMENTOCONTABILIZZAZIONE&TIMESTAMP=2002-04-8T13:04:21.852
&IDNEGOZIO=123456789012345&OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&IDTRA
NS=HK84HL2G&NUMORD=A4845b2&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D6 Generazione del MAC per il messaggio SPLIT (divisione e/o riduzione)

Il MAC che deve essere trasmesso allegato ai messaggi di tipo SPLIT viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di SPLIT (divisione e/o riduzione) il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDTRANS
- NUMORD

Il MAC sarà:

MAC=Hash(OPERAZIONE=SPLIT&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numero richiesta>&IDTRANS=<id transazione>&NUMORD=<numero d'ordine>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=SPLIT&TIMESTAMP=2002-04-08T13:04:21.852&
IDNEGOZIO=123456789012345&OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&
IDTRANS=HK84HL2G&NUMORD=A4845b2&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D7 Generazione del MAC per il messaggio VERIFICA

Il MAC che deve essere trasmesso allegato ai messaggi VERIFICA viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi VERIFICA il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- REQREFNUMORIG

Il MAC sarà:

MAC=Hash(OPERAZIONE=VERIFICA&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid> &OPERATORE=<operatore>&REQREFNUM=<numero richiesta>&REQREFNUMORIG=<numero precedente richiesta>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=VERIFICA&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=123456789012345
&OPERATORE=KR839H& REQREFNUM=20030501496204690934584305834564&
REQREFNUMORIG=20030501496204690934584305834579&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D8 Generazione del MAC per il messaggio ELENCOCONTABILE

Il MAC che deve essere trasmesso allegato ai messaggi ELENCOCONTABILE viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi ELENCOCONTABILE il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- DATAINIZIO
- DATAFINE
- DESCROP (se presente)

Il MAC sarà:

MAC=Hash(OPERAZIONE=ELENCOCONTABILE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numero richiesta>&DATAINIZIO=<data inizio>&DATAFINE=<data fine>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=ELENCOCONTABILE&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=1234567890123456&
OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&DATAINIZIO=2001-04-
04&DATAFINE=2001-04-04&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D9 Generazione del MAC per il messaggio ELENCOAUTORIZZAZIONI

Il MAC che deve essere trasmesso allegato ai messaggi ELENCOAUTORIZZAZIONI viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi ELENCOAUTORIZZAZIONI il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- DATAINIZIO (se presente)
- DATAFINE (se presente)
- FILTRO
- IDTRANS (se presente)
- ORAINIZIO (se presente)
- ORAFINE (se presente)

Il MAC sarà:

MAC=Hash(OPERAZIONE= ELENCOAUTORIZZAZIONI
&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numero richiesta>&DATAINIZIO=<data inizio>&DATAFINE=<data fine>&FILTRO=1&IDTRANS=<id transazione>[*&ORAINIZIO=<ora inizio>&ORAFINE=<ora fine>*]&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

Nel caso in cui la ricerca non venga fatta per IDTRANS, tale campo deve comunque essere inserito nel calcolo del MAC come: IDTRANS=. Nel caso la ricerca venga effettuata per data ma non per ora, i campi ORAINIZIO e ORAFINE non devono essere inseriti nel calcolo del MAC.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=ELENCOAUTORIZZAZIONI&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=123456789012345&
OPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&DATAINIZIO=2001-04-04&DATAFINE=2001-04-
04&FILTRO=1&IDTRANS=HK84HL2G&ORAINIZIO=10.00&ORAFINE=18.30&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D10 Generazione del MAC per il messaggio SITUAZIONEORDINE

Il MAC che deve essere trasmesso allegato ai messaggi SITUAZIONEORDINE viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi SITUAZIONEORDINE il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- NUMORD

Il MAC sarà:

MAC=Hash(OPERAZIONE=SITUAZIONEORDINE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numero richiesta>&NUMORD=<numord>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=SITUAZIONEORDINE&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=123456789012345&
OPERATORE=KR839H&NUMORD=A4845b2&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D11 Generazione del MAC per l'elemento XML <BPWXmlRisposta>

Il MAC che @POS allega agli elementi XML BPWXmlRisposta contenuti nei messaggi di risposta spediti verso il merchant system viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di richiesta. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di richiesta, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di richiesta è calcolato con MD5, anche il MAC della risposta sarà calcolato con MD5. Viceversa se il MAC del messaggio di richiesta è calcolato con SHA-1, anche il MAC della risposta sarà calcolato con SHA-1.

Per l'elemento BPWXmlRisposta il testo firmato contiene il valore dei sottoelementi:

- Timestamp
- Esito

Il MAC sarà:

MAC = Hash ("<timestamp>&<esito>&<stringa segreta >**")**

Le scritte fra < > indicano i valori dei campi.

NOTA BENE: Si noti che i nomi degli elementi XML non vengono utilizzati per calcolare il MAC. Si utilizzano solo i valori.

L'ordine con il quale appaiono i valori è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
2001-07-04T12:02:55&00&Absd830923fk32h7de23r..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo viene utilizzata dal server SIA una conversione in esadecimale. Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non deve essere trattato come case sensitive. Il server SIA utilizza lettere maiuscole.

N.B. Se l'esito della richiesta è un errore di autenticazione il MAC non sarà calcolato e verrà valorizzato a "NULL".

D12 Generazione del MAC per l'elemento XML <OperazioneContabile>

Il MAC che viene trasmesso allegato agli elementi XML di tipo OperazioneContabile viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di richiesta. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di richiesta, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di richiesta è calcolato con MD5, anche il MAC della risposta sarà calcolato con MD5. Viceversa se il MAC del messaggio di richiesta è calcolato con SHA-1, anche il MAC della risposta sarà calcolato con SHA-1.

Per gli elementi XML OperazioneContabile il testo firmato contiene i valori dei seguenti sottoelementi:

- IDtran
- TimestampRic
- TimestampElab
- TipoOp
- Importo
- Esito
- Stato
- DescrOp (se presente)

Il MAC sarà:

MAC = Hash (<id transazione>&<timestamp richiesta>&<timestamp elaborazione>&<tipo operazione>&<importo>&<esito>&<stato>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

NOTA BENE: Si noti che i nomi degli elementi XML non vengono utilizzati per calcolare il MAC. Si utilizzano solo i valori.

L'ordine con il quale appaiono i valori è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
CC8424&2001-07-04T12:02:54&2001-07-07T12:03:02&CTO05&100&00&SGN03&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

N.B. Se l'esito della richiesta è un errore di autenticazione il MAC non sarà calcolato e verrà valorizzato a "NULL".

D13 Generazione del MAC per l'elemento XML <Autorizzazione>

Il MAC che viene trasmesso da @POS allegato agli elementi XML Autorizzazione viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di richiesta. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di richiesta, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di richiesta è calcolato con MD5, anche il MAC della risposta sarà calcolato con MD5. Viceversa se il MAC del messaggio di richiesta è calcolato con SHA-1, anche il MAC della risposta sarà calcolato con SHA-1.

Per gli elementi XML Autorizzazione il testo firmato contiene i valori dei seguenti sottoelementi:

- Tautor
- IDtrans
- Circuito
- NunOrd
- ImportoTrans
- ImportoAutor
- Valuta
- ImportoContab
- ImportoStornato (*solo se nella richiesta viene specificato il parametro **RELEASE=02)***
- EsitoTrans
- Timestamp
- NumAut
- AcqBIN
- CodiceEsercente
- Stato
- ResponseCodeISO (se presente)

Il MAC sarà:

MAC=Hash(<tipoautorizzazione>&<idtransazione>&<circuito>&<numeroordine>&<importotransazione>&<importoautorizzato>&<valuta>&<importocontabilizzato>&<importostornato>&<esitotransazione>&<timestamp>&<numeroautorizzazione>&<aquirer bin>&<codice esercente>&<stato>&<responsecodeiso>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

<u>NOTA BENE:</u> Si noti che i nomi degli elementi XML non vengono utilizzati per calcolare il MAC. Si utilizzano solo i valori.

L'ordine con il quale appaiono i valori è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
I&8032180310wieeuejjwerrrrr&01&ordine1&10000&10000&978&10000&0&00&2001-07-
06T13:04:34&123456&234569&05423956754389&02&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.

Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

N.B. Se l'esito della richiesta è un errore di autenticazione il MAC non sarà calcolato e verrà valorizzato a "NULL".

D14 Generazione del MAC per l'elemento XML <Verifica>

Il MAC che @POS allega agli elementi XML di tipo <Verifica> spediti verso il merchant system viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di avvio. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di avvio, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di avvio è calcolato con MD5, anche il MAC dell'esito sarà calcolato con MD5. Viceversa se il MAC del messaggio di avvio è calcolato con SHA-1, anche il MAC dell'esito sarà calcolato con SHA-1.

Per gli elementi XML Verifica il testo firmato contiene i valori dei seguenti sottoelementi:

- TipoRichiesta
- Esito
- IDtrans

Il MAC sarà:

MAC = Hash ("<tipo richiesta>&<esito>&<id transazione>&<stringa segreta >**")**

Le scritte fra < > indicano i valori dei campi.

NOTA BENE: Si noti che i nomi degli elementi XML non vengono utilizzati per calcolare il MAC. Si utilizzano solo i valori.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
STORNO&00&CC405594&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale. Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non deve essere trattato come case sensitive. Il server SIA utilizza lettere maiuscole.

N.B. Se l'esito della richiesta è un errore di autenticazione il MAC non sarà calcolato e verrà valorizzato a "NULL".

D15 Generazione del MAC per il messaggio AUTORIZZAZIONEONLINE

Il MAC che deve essere trasmesso allegato ai messaggi di tipo AUTORIZZAZIONEONLINE viene ottenuto con il procedimento qui descritto.
Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.
La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di AUTORIZZAZIONEONLINE, il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- IDORDINE
- IDOPERATORE
- REQREFNUM
- PAN
- CVV2 (se presente)
- DATASCAD
- IMPORTO
- VALUTA
- TCONTAB
- CODICECIRCUITO
- EMAILTIT (se presente)
- USERID (se presente)
- ACQUIRER (se presente)
- IPADDRESS (se presente)
- DESCROP (se presente)

Il MAC sarà: (MAC = Hash)

(OPERAZIONE=AUTORIZZAZIONEONLINE&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>& IDORDINE=<idordine>&IDOPERATORE=<operatore>& REQREFNUM=<numerorichiesta>& PAN=<pan>&CVV2=<cvv2> &DATASCAD=<data di scadenza>&IMPORTO=<importo> &VALUTA=<valuta>&TCONTAB=<tipo contab>& CODICECIRCUITO=<codice circuito>&EMAILTIT=<e-mail titolare>USERID=<user id>&IPADDRESS=<ipaddress>&DESCROP=<descrop>&< stringa segreta **>)**

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.
Nel caso in cui ci siano dei campi opzionali non valorizzati, essi dovranno essere omessi totalmente dalla stringa che determina il MAC

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=AUTORIZZAZIONEONLINE&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=123456789012345&
IDORDINE=ord1&IDOPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&PAN=123456781234
5678&DATASCAD=0312&IMPORTO=100&VALUTA=978&TCONTAB=I&CODICECIRCUITO=01&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.
Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D16 Generazione del MAC per il messaggio AUTORIZZAZIONEDIFFERITA

Il MAC che deve essere trasmesso allegato ai messaggi di tipo AUTORIZZAZIONEDIFFERITA viene ottenuto con il procedimento qui descritto.
Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.
La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di AUTORIZZAZIONEDIFFERITA, il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- IDORDINE
- IDOPERATORE
- REQREFNUM
- PAN
- CVV2 (se presente)
- DATASCAD
- IMPORTO
- VALUTA
- CODICECIRCUITO
- EMAILTIT (se presente)
- USERID (se presente)
- ACQUIRER (se presente)
- IPADDRESS (se presente)

Il MAC sarà: (MAC = Hash)

(OPERAZIONE=AUTORIZZAZIONEDIFFERITA&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>& IDORDINE=<idordine>&IDOPERATORE=<operatore>& REQREFNUM=<numerorichiesta>& PAN=<pan>&CVV2=<cvv2> &DATASCAD=<data di scadenza>&IMPORTO=<importo> &VALUTA=<valuta>& CODICECIRCUITO=<codice circuito>& EMAILTIT=<e-mail titolare>&USERID=<user id>& IPADDRESS=<ipaddress>&< stringa segreta **>)**

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.
Nel caso in cui ci siano dei campi opzionali non valorizzati, essi dovranno essere omessi totalmente dalla stringa che determina il MAC

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=AUTORIZZAZIONEONLINE&TIMESTAMP=2002-04-08T13:04:21.852&IDNEGOZIO=1234567890123456&
IDORDINE=ord1&IDOPERATORE=KR839H&REQREFNUM=20030501496204690934584305834564&PAN=1234567812345678&DATASCAD=0312&IMPORTO=100&VALUTA=978&CODICECIRCUITO=01&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D17 Generazione del MAC per il messaggio AUTORIZZAZIONEONLINEVBV

Il MAC che deve essere trasmesso allegato ai messaggi di tipo AUTORIZZAZIONEONLINEVBV viene ottenuto con il procedimento qui descritto.
Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.
La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di AUTORIZZAZIONEONLINEVBV, il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- IDORDINE
- IDOPERATORE
- REQREFNUM
- PAN
- CVV2
- DATASCAD
- IMPORTO
- VALUTA
- TCONTAB
- CODICECIRCUITO
- EMAILTIT (se presente)
- USERID (se presente)
- ACQUIRER (se presente)
- IPADDRESS (se presente)
- DESCROP (se presente)
- PRESENTE (se presente)
- URLMERCHANT (se presente)
- SERVIZIO (se presente)
- XID (se presente)
- CAVV (se presente)
- ECI (se presente)
- PP_AUTHENTICATEMETHOD (se presente)
- PP_CARDENROLLMETHOD (se presente)
- PARESSTATUS (se presente)
- SCENROLLSTATUS (se presente)
- SIGNATUREVERIFICATION (se presente)

Il MAC sarà: (MAC = Hash)
(OPERAZIONE= AUTORIZZAZIONEONLINEVBV
&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&
IDORDINE=<idordine>&IDOPERATORE=<operatore>& REQREFNUM=<numerorichiesta>&
PAN=<pan>&CVV2=<cvv2> &DATASCAD=<data di scadenza>&IMPORTO=<importo>
&VALUTA=<valuta>&TCONTAB=<tipo contab>& CODICECIRCUITO=<codice
circuito>&EMAILTIT=<e-mailtitolare>USERID=<userid>&
IPADDRESS=<ipaddress>&DESCROP=<descrop>&PRESENTE=<presente>&URLMERCHANT=<url>&< stringa segreta **>)**

Le scritte fra < > indicano i valori dei campi.
L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Nel caso in cui ci siano dei campi opzionali non valorizzati, essi dovranno essere omessi totalmente dalla stringa che determina il MAC

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D18 Generazione del MAC per il messaggio AUTORIZZAZIONEONLINEVBV2

Il MAC che deve essere trasmesso allegato ai messaggi di tipo AUTORIZZAZIONEONLINEVBV2 viene ottenuto con il procedimento qui descritto.
Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.
La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di AUTORIZZAZIONEONLINEVBV2, il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- IDOPERATORE
- REQREFNUM
- REQREFNUMORIG
- PARES
- ACQUIRER (se presente)

Il MAC sarà: (MAC = Hash)

(OPERAZIONE=AUTORIZZAZIONEONLINEVBV2&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>& IDOPERATORE=<operatore>& REQREFNUM=<numerorichiesta>& REQREFNUMORIG=<numerorichiestaorig>&PARES=<pares>&< stringa segreta **>)**

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.
Nel caso in cui ci siano dei campi opzionali non valorizzati, essi dovranno essere omessi totalmente dalla stringa che determina il MAC

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

D19 Generazione del MAC per l'elemento XML <VBVRedir>

Il MAC che @POS allega agli elementi XML di tipo <VBVRedir> spediti verso il merchant system viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di avvio. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di avvio, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di avvio è calcolato con MD5, anche il MAC dell'esito sarà calcolato con MD5. Viceversa se il MAC del messaggio di avvio è calcolato con SHA-1, anche il MAC dell'esito sarà calcolato con SHA-1.

Per gli elementi XML VBVRedir il testo firmato contiene i valori dei seguenti sottoelementi:

- PaReq
- URLAcs

Il MAC sarà:

MAC = Hash ("<PaReq>&<URLAcs>&<stringa segreta >**")**

Le scritte fra < > indicano i valori dei campi.

NOTA BENE: Si noti che i nomi degli elementi XML non vengono utilizzati per calcolare il MAC. Si utilizzano solo i valori.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale. Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non deve essere trattato come case sensitive. Il server SIA utilizza lettere maiuscole.

D20 Generazione del MAC per il messaggio RECUPERAALIASPAN

Il MAC che deve essere trasmesso allegato ai messaggi RECUPERAALIASPAN viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi RECUPERAALIASPAN il testo da firmare deve contenere i campi:

- OPERAZIONE
- TIMESTAMP
- IDNEGOZIO
- OPERATORE
- REQREFNUM
- IDORDINE

Il MAC sarà:

MAC=Hash(OPERAZIONE=RECUPERAALIASPAN&TIMESTAMP=<timestamp>&IDNEGOZIO=<merchantid>&OPERATORE=<operatore>&REQREFNUM=<numerorichiesta>&IDORDINE=<idordine>&<stringa segreta >)

Le scritte fra < > indicano i valori dei campi.

L'ordine con il quale appaiono i campi è ovviamente fondamentale.

Un esempio di tale stringa potrebbe essere:

```
OPERAZIONE=RECUPERAALIASPAN&TIMESTAMP=2015-04-14T12:21:56.774&IDNEGOZIO=120500000511889
&OPERATORE=AF06TSTAPI1&REQREFNUM=20150414122156000000000000000004&IDORDINE=1234567890000
&Absd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

Appendice C Generazione MAC

C1 Generazione del MAC per i messaggi di redirect

Il MAC che deve essere trasmesso allegato ai messaggi di avvio del processo di pagamento viene ottenuto con il procedimento qui descritto.

Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare e la stringa segreta.

La funzione di hash può essere scelta dall'esercente a piacere fra due algoritmi standard: SHA-1 (detto anche SHA) ed MD5. Dato che i due algoritmi producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC. Il sito del negozio può variare a proprio piacimento l'algoritmo utilizzato.

Per i messaggi di avvio transazione, il testo da firmare deve contenere i campi nel seguente ordine:

- URLMS
- URLDONE
- NUMORD
- IDNEGOZIO
- IMPORTO
- VALUTA
- TCONTAB
- TAUTOR
- OPTIONS (se presente)
- NOME (se presente per OPTIONS B)
- COGNOME (se presente per OPTIONS B)
- LOCKCARD (se presente)
- COMMIS (se presente per OPTIONS F)
- DESCRORD (se presente per OPTIONS O)
- IDVS (se presente)
- DESCROP (se presente)

Il MAC (se OPTIONS non presente) sarà:

MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&NUMORD=<idoper>&IDNEGOZIO=<merchantid>&IMPORTO=<importo>&VALUTA=<valuta>&TCONTAB=<tipocontab>&TAUTOR=<tipoautor>&**<stringasegretaavvio>**)

Il MAC con OPTIONS=B e NOME COGNOME presenti sarà:

MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&NUMORD=<idoper>&IDNEGOZIO=<merchantid>&IMPORTO=<importo>&VALUTA=<valuta>&TCONTAB=<tipocontab>&TAUTOR=<tipoautor>&OPTIONS=B&NOME=<nom>&COGNOME=<cogn>&**<stringa segreta avvio>**)

L'ordine con il quale appaiono i campi è ovviamente fondamentale. La stringa segreta da utilizzate è quella denominata "chiave di avvio".

Nel calcolo del MAC i campi URLMS ed URLDONE devono essere utilizzati nella loro forma non "encoded" anche se contengono parametri.

Un esempio di tale stringa potrebbe essere:

```
URLMS=http://www.dominio.it/ok.asp?par=45&nord=23684&URLDONE=http://www.dominio.it/negozio.asp?par=
45&nord=23684&NUMORD=A4845b2&IDNEGOZIO=123456789012345&IMPORTO=100&VALUTA=978&TCONTAB=I&TAUTOR=D&Ab
sd830923fk32..
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale.
Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non è case sensitive. Lettere maiuscole e minuscole possono essere utilizzate indistintamente.

C2 Generazione del MAC per il messaggio esito

Il MAC che @POS allega ai messaggi di esito spediti verso il merchant system viene ottenuto con il procedimento qui descritto. Il merchant e SIA condividono una stringa segreta di 50 caratteri. Per produrre il MAC dei dati si esegue un hash del concatenamento tra il testo da firmare ed una stringa segreta. Si noti che SIA utilizza una stringa segreta diversa da quella di avvio per calcolare il MAC dei messaggi di esito; questa stringa viene detta chiave di "esito-API" perché viene utilizzata anche per l'accesso alle API @POS.

La funzione di hash utilizzata dal sistema per generare il MAC è la medesima che l'esercente ha adottato per la generazione del MAC del messaggio di avvio. Dato che gli algoritmi SHA-1 ed MD5 producono un diverso numeri di bit (160 il primo, 128 il secondo) il sistema è in grado di riconoscere automaticamente il tipo di funzione utilizzato per la generazione del MAC del messaggio di avvio, ed utilizzare a sua volta lo stesso algoritmo per rispondere.
In sostanza se il MAC del messaggio di avvio è calcolato con MD5, anche il MAC dell'esito sarà calcolato con MD5. Viceversa se il MAC del messaggio di avvio è calcolato con SHA-1, anche il MAC dell'esito sarà calcolato con SHA-1.

Per i messaggi conferma, il testo firmato contiene i campi:

- NUMORD
- IDNEGOZIO
- AUT (Se l'autorizzazione non è presente, il campo è valorizzato con "NULL")
- IMPORTO
- VALUTA
- IDTRANS
- TCONTAB
- TAUTOR
- ESITO
- BPW_TIPO_TRANSAZIONE
- BPW_ISSUER_COUNTRY (se richiesto tramite OPTIONS I)
- RESPONSE_CODE_AUT (se richiesto tramite OPTIONS P)
- PAYERID, PAYER, PAYERSTATUS (per pagamenti Paypal, se richiesto tramite OPTIONS Q)
- BPW_HASH_PAN (se il negozio è abilitato al servizio)

Il MAC con BPW_TIPO_TRANSAZIONE e BPW_ISSUER_COUNTRY sarà:

MAC = Hash_ (" NUMORD =<numero d'ordine>&IDNEGOZIO=<merchant id>&AUT=<numero autor>&IMPORTO=<importo> &VALUTA=<valuta>&IDTRANS=<id.transazione>&TCONTAB=<tipo contab>&TAUTOR=<tipo autor>&ESITO=<esito>&BPW_TIPO_TRANSAZIONE =<tipo trans>& BPW_ISSUER_COUNTRY=<nazione dell'issuer>&**<stringa segreta esito-API>**")

L'ordine con il quale appaiono i campi è ovviamente fondamentale. La stringa segreta da utilizzate è quella denominata "chiave di esito-API".

Un esempio di tale stringa potrebbe essere:

```
NUMORD=A4845b2&IDNEGOZIO=123456789012345&AUT=HJ89KR&IMPORTO=100&VALUTA=978&IDTRANS=HK84HL2G&TCONTAB
=I&TAUTOR=I&ESITO=00&BPW_TIPO_TRANSAZIONE=TT01&Absd830923fk32&BPW_ISSUER_COUNTRY=ITA
```

Il MAC, essendo il risultato di un hash, per essere trasmesso in HTTP deve essere codificato opportunamente. A tale scopo si deve utilizzare una conversione in esadecimale. Il risultato di tale conversione e' una stringa di 32 caratteri se la funzione di hash usata è MD5. Se invece si è utilizzato SHA-1 il risultato sarà una stringa di 40 caratteri.

Il MAC non deve essere trattato come case sensitive. Il server SIA utilizza lettere maiuscole.
N.B. Se l'esito della transazione è negativo, a meno che non sia stata richiesta la OPTION "R", il MAC non sarà calcolato e sarà valorizzato a "NULL".

Appendice E parametri TAUTOR, TCONTAB e scenari possibili

Di seguito viene illustrato brevemente il significato dei parametri TAUTOR e TCONTAB in relazione alle possibili modalità di utilizzo del sistema @POS.

TAUTOR

Autorizzazione immediata I

La modalità di autorizzazione immediata prevede che durante la fase di pagamento online venga immediatamente inviata la richiesta di autorizzazione ai circuiti internazionali. Una volta conclusa la transazione in modo positivo l'esercente ha la certezza che quanto dovuto dal cliente è stato "prenotato" dal suo plafond.

Autorizzazione differita D

La modalità di autorizzazione differita prevede che durante la fase di pagamento online le transazioni siano prese in carico ma non inoltrate ai circuiti (viene comunque effettuato un controllo della validità della carta presso l'issuer).
L'esercente che utilizza questa modalità di accettazione dei pagamenti è in grado, in un secondo tempo, di far elaborare le richieste di autorizzazione pendenti che lo riguardano. Le richieste di autorizzazione differita possono pervenire a PIB per un importo inferiore a quello originale; l'esercente può inoltrare una serie di autorizzazioni differite fino a coprire il totale originale.

TCONTAB

Contabilizzazione immediata I

La modalità di contabilizzazione immediata permette all'esercente di rendere automaticamente contabili tutte le transazioni autorizzate. Senza un suo intervento, la sera stessa del giorno in cui è avvenuta la transazione, il processor di front end esegue il clearing in automatico del movimento per l'intero importo autorizzato.
Questa modalità può essere ad esempio utilizzata nel caso in cui si vendano beni/servizi immediatamente fruibili da parte del compratore (software, musica, servizi online, etc.9).

Contabilizzazione differita D

La modalità di contabilizzazione differita prevede che le operazioni autorizzate debbano essere esplicitamente rese contabili dall'esercente. Per eseguire l'operazione di contabilizzazione di un movimento l'esercente ha a disposizione un predeterminato numero di giorni dal momento della autorizzazione.

Questa modalità mette a disposizione dell'esercente le seguenti operazioni:

- contabilizzazione totale: un movimento viene reso contabile per l'intero ammontare della cifra autorizzata.
- contabilizzazione parziale: un movimento viene reso contabile per un ammontare inferiore alla cifra autorizzata; una operazione di contabilizzazione parziale può far riferimento ad una autorizzazione per la quale era già stata richiesta una contabilizzazione parziale (split shipment) a patto che non sia scaduto il termine ultimo di contabilizzazione.
- annullamento: viene annullata una operazione di contabilizzazione eseguita durante la giornata, il movimento è nuovamente contabilizzabile.

Scenari possibili

Di seguito sono riportati alcun possibili scenari di utilizzo del sistema

Funzionalità	**Meccanismo utilizzabile**
Pagamento di beni immateriali (download o servizi)	Avvio pagamento con autorizzazione immediata TAUTOR=I, contabilizzazione immediata o differita
Pagamento di beni materiali inscindibili sempre disponibili	Avvio pagamento con autorizzazione immediata TAUTOR=I, contabilizzazione immediata o differita

Pagamento di beni materiali da procurare	Avvio pagamento con autorizzazione differita (TAUTOR=D) ed 1 richiesta di autorizzazioni successiva con contabilizzazione immediata
Split shipment (divisione e/o riduzione): consegna in più tempi della merce Ipotesi: • Il negozio sa a priori che consegnerà a pezzi • L'importo totale è noto a priori	Avvio pagamento con autorizzazione differita (TAUTOR=D) ed N richieste di autorizzazioni successive con contabilizzazione immediata
Split shipment (divisione e/o riduzione): consegna in più tempi della merce Ipotesi: • Il negozio non sapeva a priori di dover consegnare a rate • È stata inviata una autorizzazione online per l'intero importo	In questa situazione si deve eseguire lo split (divisione e/o riduzione) della autorizzazione: questa operazione tramuta un ordine online in uno in differito. Dopo l'operazione di split (divisione e/o riduzione) si potranno inviare N richieste di autorizzazione come per una normale autorizzazione differita