



REGIONE BASILICATA

**DIPARTIMENTO PRESIDENZA  
DELLA GIUNTA REGIONALE**  
**UFFICIO RAGIONERIA GENERALE E FISCALITA'  
REGIONALE**

Via V. Verrastro, n. 4  
85100 Potenza  
tel 0971/668271  
fax 0971/668302  
[ufficio.ragioneria@cert.regione.basilicata.it](mailto:ufficio.ragioneria@cert.regione.basilicata.it)

**Allegato tecnico**

---

# **Ordinativo Informativo – Gateway su Web Services**





## Sommario

<b>1. OBIETTIVO</b>		<b>4</b>
<b>2. PREMESSA &amp; REQUISITI</b>	ERRORE. IL SEGNALIBRO NON È DEFINITO.	
<b>3. INFRASTRUTTURA DI BASE</b>		<b>4</b>
<b>3.1. Architettura Applicativa</b>		<b>4</b>
<b>3.2. Standard di colloquio</b>		<b>4</b>
3.2.1 Server Enti – Gateway Tesoreria		4
3.2.2 Sicurezza		4
3.2.3 Retry su comunicazioni errate		5
<b>3.3. Messaggi</b>		<b>5</b>
<b>3.4. Comunicazione dei documenti</b>		<b>5</b>
<b>3.5. Definizione delle entry</b>		<b>6</b>
3.5.1 Flussi di ordinativi spediti dall'Ente		6
3.5.2 Identificativo dei flussi e nomi delle entry		6
3.5.3 Ricevute spedite dalla Tesoreria		6
3.5.4 Nomi delle ricevute		6
<b>3.6. Modalità di comunicazione</b>		<b>7</b>
3.6.1 La request https		7
3.6.2 Descrizione dei parametri della request		7
3.6.3 La response https		8
3.6.4 Descrizione della Response		8
3.6.5 Retry su comunicazioni errate		9
<b>3.7. Regole per processare gli invii</b>		<b>9</b>
3.7.1 Ordinamento delle entry in un invio		9
3.7.2 Appendice: elenco dei codici response https		9



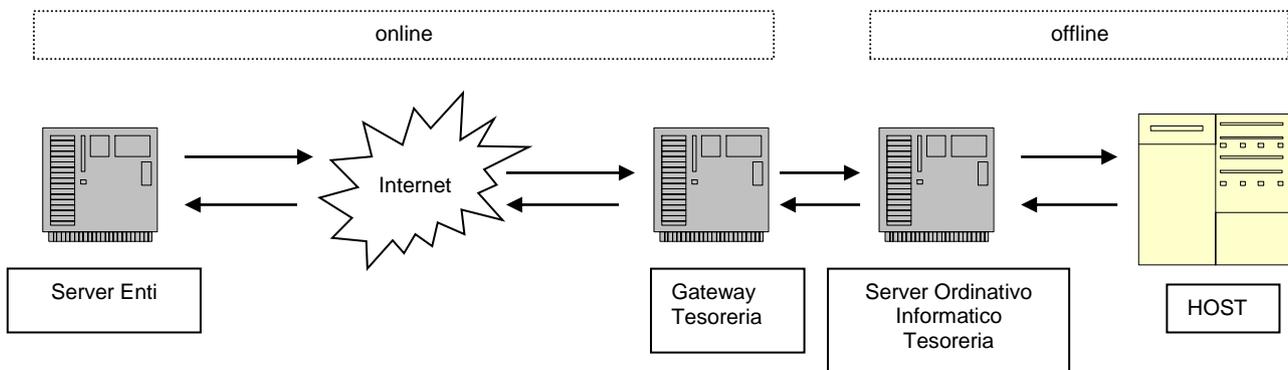
## 1. OBIETTIVO

Obiettivo: **Descrizione infrastruttura tecnica di dialogo tramite Web Services per l'Ordinativo Informatico tra Regione Basilicata (Ente) e Tesoreria**

Di seguito si descrivono sinteticamente le attuali modalità di colloquio tra Ente e Tesoreria per la gestione dell'Ordinativo Informatico.

## 2. INFRASTRUTTURA DI BASE

### 2.1. ARCHITETTURA APPLICATIVA



### 2.2. STANDARD DI COLLOQUIO

#### 2.2.1 Server Enti – Gateway Tesoreria

Il dialogo tra i due sistemi avviene tramite chiamate HTTPS in modalità XML/SOAP. In questa fase sono gestiti eventuali errori trasmissivi che comportano la mancata acquisizione del flusso (corruzione, errori http, ecc.). Gli esiti negativi previsti in questo protocollo sono limitati strettamente ai casi in cui l'errore sia imputabile al sistema di comunicazione.

#### 2.2.2 Sicurezza

Per rispettare la circolare ABI che regola la trasmissione di Ordinativi Informatici tra Pubblica Amministrazione e Banca Tesoriera, è stato implementato un meccanismo di protezione dei dati trasmessi. I Web Services del gateway Ente sono posti su un server della DMZ regionale (protetto da Firewall) e sono accessibili da tutti (link pubblico).

Il protocollo di comunicazione utilizzato si basa in ogni caso sulla trasmissione di una coppia di credenziali (utente, password) criptate dal canale di comunicazione https. Per questo motivo non è richiesta necessariamente la mutua autenticazione tra client e server ma solo l'utilizzo del protocollo https standard senza mutua autenticazione.



### 2.2.3 Retry su comunicazioni errate

Il protocollo di comunicazione prevede la garanzia nella sequenza degli invii, quindi a fronte di un esito errato la comunicazione viene tentata di nuovo dal mittente finché non verrà ottenuta una response con esito positivo sull'invio bloccato.

## 2.3. WORKFLOW MESSAGGI

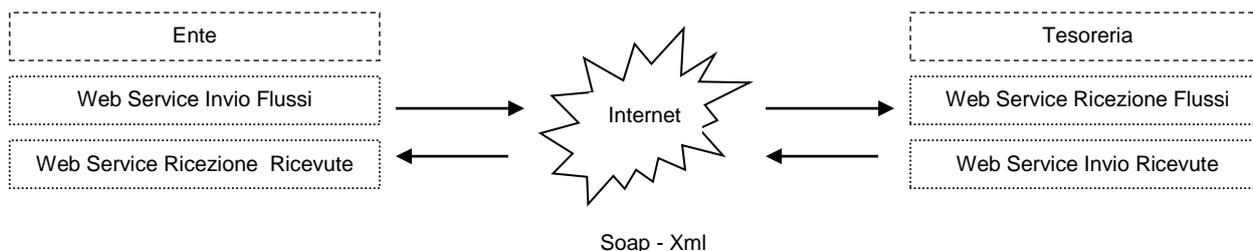
L'Ente invia:

1. i flussi contenenti gli ordinativi

verso il web service Tesoreria di ricezione dati e riceve:

2. le ricevute di trasmissione,
3. le ricevute di servizio,
4. le ricevute applicative (esito di carico e quietanza)

tramite un proprio web service. Quindi la comunicazione è accoppiata, come nello schema sottostante.



## 2.4. COMUNICAZIONE DEI DOCUMENTI

Il protocollo ha lo scopo di regolamentare due tipi di comunicazioni:

- la spedizione da Ente alla Tesoreria di gruppi di flussi, a loro volta contenenti documenti firmati relativi agli ordinativi,
- la spedizione dalla Tesoreria all'Ente di gruppi di ricevute, sia di servizio che applicative.

A causa dell'evidente analogia, il protocollo è simmetrico e specifica le regole di composizione e di trattamento delle unità di spedizione.

Ogni unità di spedizione viene denominata "Invio", ogni oggetto trasmesso (flusso o ricevuta) viene denominato "Entry".



## 2.5. DEFINIZIONE DELLE ENTRY

### 2.5.1 Flussi di ordinativi spediti dall'Ente

Ogni entry presente negli invii prodotti dall'Ente contiene una sola busta firmata PKCS#7, detta flusso di ordinativi. All'interno della busta è presente un singolo tracciato xml che rappresenta un flusso Tesoreria corrispondente ad un solo documento.

### 2.5.2 Identificativo dei flussi e nomi delle entry

Le singole entry contenenti i flussi hanno un nome (nome della entry). Il nome della entry contiene un riferimento all'identificativo del flusso presente nel tracciato. L'identificativo del flusso per i flussi prodotti dall'Ente coincide con il numero del documento (riportato anche ulteriormente all'interno del tracciato). La numerazione utilizzata per l'identificativo del flusso è univoca all'interno del codice ente dichiarato e dell'esercizio di appartenenza, ma non è compatta e non è sequenziale. La numerazione non è sequenziale, relativamente all'ordine di spedizione, perchè rispetta l'ordine di produzione/firma dei documenti. Questa operazione, che rende un documento non modificabile, può essere effettuata in un ordine diverso dalla spedizione per garantire la corretta elaborazione dei documenti stessi. L'identificativo del flusso è un numero di 7 cifre (numero documento). Gli identificativi, all'interno dei nomi delle entry, sono "paddingati" alla dimensione massima, ovvero sono preceduti da un numero di zeri tale da completare il numero di cifre massime previste. In questo modo è possibile fare anche degli ordinamenti di tipo alfabetico sui dati.

Il formato del nome del flusso è :

**"E"** seguito da **<identificativo del flusso>\_ANNO\_OIMAN per mandati**

**"E"** seguito da **<identificativo del flusso>\_ANNO\_OIREV per reversali**

esempi:

E0012340\_2015\_OIMAN

E0012345\_2015\_OIREV

### 2.5.3 Ricevute spedite dalla Tesoreria

Ogni entry presente negli invii prodotti dalla Tesoreria contiene una sola busta firmata PKCS#7, detta ricevuta. All'interno della busta è presente un singolo tracciato xml che rappresenta una delle ricevute previste dalla Tesoreria.

### 2.5.4 Nomi delle ricevute

I nomi delle ricevute sono "parlanti", ovvero permettono di avere informazioni sul tipo della ricevuta senza dover necessariamente aprire la busta PKCS#7 ; il formato del nome è:

**"E"** seguito da **<identificativo della ricevuta>\_<tipo di ricevuta>**

dove **<tipo di ricevuta>** assume i valori:

- **RSOK RSKO** per le ricevute di servizio
- **RC** per le ricevute applicative di carico
- **RAOK** per le ricevute applicative di quietanza

esempi :



E0000123\_RSOK

E0000134\_RAKO

## 2.6. MODALITÀ DI COMUNICAZIONE

### 2.6.1 La request https

Per ogni invio il mittente effettua una chiamata https al servizio esposto dal ricevente dichiarando

- il codice dominio,
- il codice operatore,
- la password,
- il codice ente,
- il codice banca,
- il tipo di messaggio
- ed il messaggio

a cui fanno riferimento i dati da elaborare come parametri della chiamata.

La request https è composta da uno stream compresso con tecnologia ZIP, a sua volta codificato in base 64, che rappresenta un invio e composto di file ognuna delle quali rappresenta una entry. Per ogni request il mittente riceve un esito che può essere una response https esplicita generata dal ricevente, oppure un generico errore di trasmissione https. La dimensione massima di un singolo invio è fissata a 5Mb.

### 2.6.2 Descrizione dei parametri della request

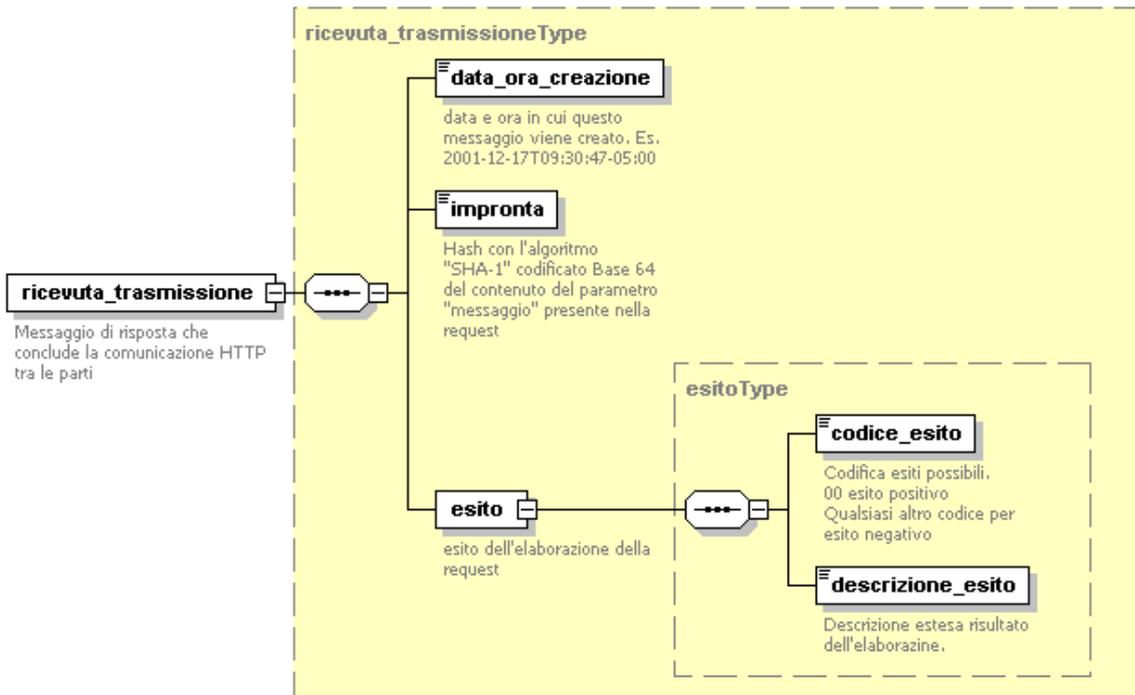
Nome parametro	Valori possibili	Descrizione
Codice_dominio	05387	05387 Cod. ABI BPER da usare in test
Codice_operatore	4161103	
Password	Tdoc2005	
codice_ente_BT	4161103	Codice di riconoscimento Ente concordato con la Tesoreria
Codice_ABI_BT	05387	Codice identificativo della Tesoreria 05387 Cod. ABI BPER da usare in test
Tipo_messaggio	ZIP	Attualmente é supportata solo la compressione zip
messaggio	Tracciato concordato con la Tesoreria	Testo del messaggio scambiato, prima compresso con algoritmo ZIP e successivamente codificato in formato Base64



### 2.6.3 La response https

La response è un messaggio xml comprensibile che permette di stabilire se la comunicazione è avvenuta correttamente e, in caso contrario, fornisce elementi utili per conoscere l'esito dell'operazione.

### 2.6.4 Descrizione della Response



Esempio di response in caso di comunicazione corretta :

```
<ricevuta_trasmissione>
  <data_ora_creazione >2001-12-17T09:30:47-05:00</data_ora_creazione >
  <impronta>hYwxNO0ZzNG5tAsgZTfszTyzdhs=</impronta>
  <esito>
    <codice_esito>00</codice_esito>
    <descrizione_esito>Ricevuti correttamente [42] flussi</descrizione_esito>
  </esito>
</ricevuta_trasmissione>
```

Esempio di response in caso di problemi di trasmissione :

```
<ricevuta_trasmissione>
  <data_ora_creazione >2001-12-17T09:30:47-05:00</data_ora_creazione >
  <impronta>hYwxNO0ZzNG5tAsgZTfszTyzdhs=</impronta>
  <esito>
    <codice_esito>05</codice_esito>
    <descrizione_esito>Messaggio eccedente la dimensione massima</descrizione_esito>
  </esito>
</ricevuta_trasmissione>
```

I codici di errore “server error 400” o “server error 500” si limitano ad indicare le sole problematiche di errori senza risposta o non previsti.

NB: gli esiti negativi da prevedere in questo protocollo sono limitati strettamente ai casi in cui l'errore sia imputabile al sistema di comunicazione. In altre parole hanno senso esiti negativi nella response https solo dove abbia senso una politica di “retry” da parte del mittente.



### **2.6.5 Retry su comunicazioni errate**

Il protocollo garantisce la sequenza degli invii, quindi a fronte di un esito errato la comunicazione viene tentata di nuovo dal mittente finché non verrà ottenuta una response con esito positivo sull'invio bloccato.

## **2.7. REGOLE PER PROCESSARE GLI INVII**

Il ricevente elabora ogni invio singolarmente. In altre parole, anche se l'elaborazione è differita, non sono riuniti i contenuti di invii diversi.

### **2.7.1 Ordinamento delle entry in un invio**

Il criterio per decidere in che ordine processare le entry all'interno di un invio è il nome della entry. Ordinando i flussi in ordine alfabetico e processando i flussi dal primo all'ultimo si ha la garanzia di processarli nell'ordine corretto. Il mittente quindi definisce i nomi delle entry in modo da garantire che l'ordine sia quello necessario. Inoltre, per rendere più efficiente la comunicazione, le file entry sono già ordinate dal mittente all'interno dello zip per nome, in modo da poter essere processate dal ricevente anche in modalità sincrona, dalla prima all'ultima, senza bisogno di un ulteriore ordinamento. Il ricevente effettua comunque un controllo attivo dell'ordinamento alfabetico e solleva un errore nella response https qualora non vi fosse corrispondenza tra l'ordine delle entry e l'ordine alfabetico dei nomi.

### **2.7.2 Appendice: elenco dei codici response https**

codice_esito	descrizione_esito
00	Messaggio ricevuto correttamente – numero flussi [nnn]
02	Parametri del post non valorizzati correttamente
03	Tipo messaggio non gestito
04	Codice ente non gestito
05	Messaggio eccedente la dimensione massima
06	Formato zip non valido
07	Formato nome documento non valido
08	Ordine alfabetico non corretto
50	Dominio non gestito
51	Utente non gestito
52	Password non riconosciuta