GovWay

Dall'esperienza della Porta di Dominio italiana, l'**API Gateway** conforme alle normative della **Pubblica Amministrazione**

Console di gestione

Indice

Elenco delle figure

Elenco delle tabelle

1 Introduzione

Questo manuale documenta le funzionalità e le modalità d'uso della *Console di Gestione* del prodotto *GovWay* (http://gowway.org).

Nota
Oltre alla console di Gestione, GowWay mette a disposizione dei gestori una seconda console utilizzata per il monitoraggio delle richieste applicative gestite dal gateway. Per informazioni sulle modalità di utilizzo della Console di Monitoraggio si rimanda alla relativa manualistica distribuita con il prodotto.

Nel prosieguo si assume che il prodotto GovWay sia già correttamente installato e la console di gestione sia accessibile via browser dai Gestori del Sistema.

L'indirizzo standard della Console di Gestione è *http://ip:porta/govwayConsole*, che dovrà essere correttamente perfezionato con ip e porta del proprio ambiente di installazione. Per informazioni sulle modalità di installazione si rimanda alla relativa manualistica distribuita con il prodotto.

Nota
L'accesso alle diverse funzionalità della console è sempre mediato da un sistema di autorizzazione che verifica che l'utente sia in possesso dei dovuti permessi. Le istruzioni operative sulla gestione degli utenti e la configurazione dei permessi sono descritte nella Sezione 7.5.

1.1 I Profili di Interoperabilità

GovWay si differenzia dagli API Gateway tradizionali per essere progettato in conformità con i principali profili di interoperabilità in uso nella Pubblica Amministrazione italiana ed europea. Per tale motivo, le modalità di configurazione del prodotto si differenziano in funzione dello specifico profilo a cui le API debbano conformarsi. I profili di interoperabilità supportati dalla distribuzione standard del prodotto sono i seguenti:

- *API Gateway*: è il profilo più generico e permette di supportare, in accordo alle linee guida di interoperabilità di AGID, qualunque generica API basata su scambio di messaggi SOAP e REST.
- *eDelivery*: è il profilo standard adottato a livello europeo nell'ambito del progetto *CEF*, e basato sul protocollo AS4.
- *SPCoop*: il profilo SPCoop è il profilo basato sull'uso della busta eGov e sulla Porta di Dominio, recentemente deprecato da AGID, ma ancora in uso per la quasi totalità dei servizi centrali erogati dalla Pubblica Amministrazione italiana.
- *FatturaPA*: questo profilo supporta le modalità di scambio delle fatture elettroniche veicolate tramite il Sistema di Interscambio della Fatturazione Elettronica.

In fase di installazione possono essere scelti i profili di proprio interesse (per default viene proposto il solo profilo di API Gateway).

Durante l'utilizzo della Console di Gestione è preferibile selezionare il profilo di interoperabilità adeguato in base al tipo di configurazioni sui quali si lavora. La selezione del profilo di interoperabilità, tramite il menu presente in testata (Figura 1), comporta la visualizzazione dei soli elementi dell'interfaccia, e relativi dati, attinenti con tale profilo.

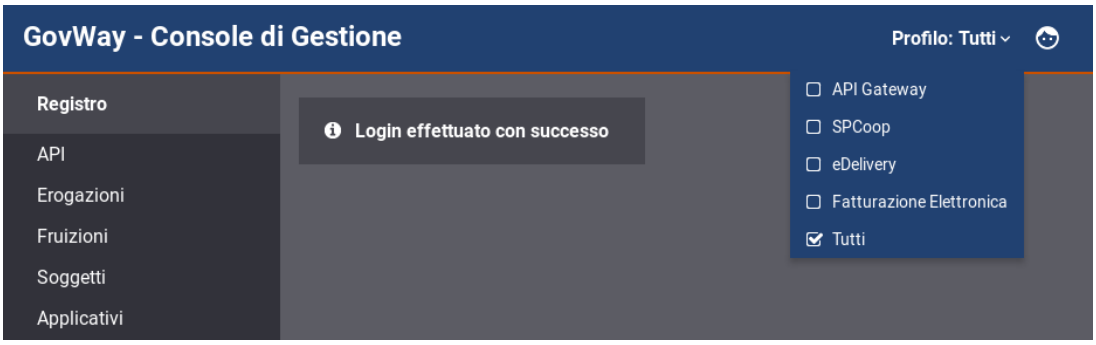


Figura 1: Selezione del profilo di interoperabilità

Esiste la possibilità (non consigliata) di operare sulla console selezionando il profilo *Tutti*. In tal caso non saranno applicati filtri sui contenuti e le maschere di visualizzazione e di configurazione potranno apparire più complesse di quanto avviene selezionando lo specifico profilo su cui si sta lavorando.

Nota

Ulteriori profili sono programmabili in GovWay ed alcuni di questi sono in uso in importanti progetti della pubblica amministrazione, come la Porta di Comunicazione del Sistema di Interscambio del Mercato dell'Energia.

1.2 Le entità di configurazione dei servizi

Prima di descrivere le entità di configurazione presenti nel registro è importante chiarire il concetto di *Dominio* cui alcuni elementi di configurazione fanno riferimento. Il dominio rappresenta il confine logico (tipicamente un ente amministrativo) entro il quale sono racchiuse le risorse applicative da condividere con l'esterno. Nel seguito si fa distinzione tra i seguenti:

- *Dominio Gestito*: l'insieme delle risorse applicative i cui flussi di comunicazione sono sotto il controllo del GovWay di propria gestione.
- *Dominio Esterno*: Insieme di risorse applicative esterne al dominio gestito.

Le principali entità di configurazione del Registro sono:

- *Soggetto*

  Entità che rappresenta la singola organizzazione, o ente amministrativo, coinvolto nei flussi di comunicazione. Ciascun soggetto censito nel registro può appartenere al dominio interno o esterno e può avere associata un'unica modalità operativa.

- *API*

  Descrizione formale dei flussi di comunicazione previsti da un dato servizio, erogato o fruito nel proprio dominio. Ad ogni API è assegnata una singola modalità operativa e, in base ad essa, sarà fornita una descrizione formale delle interfacce di dialogo supportate. Ad esempio saranno forniti WSDL/XSD per le interfacce Soap o un file YAML in formato Swagger per quelle Rest.

- *Erogazione*

  Registrazione di una specifica istanza di servizio che un soggetto del dominio interno eroga in accordo alle interfacce applicative descritte da un set di API censito nel registro.

- *Fruizione*

  Registrazione di una specifica istanza di servizio che un soggetto del dominio interno fruisce in accordo alle interfacce applicative descritte da un set di API censito nel registro.

- *Ruolo*

  Entità per censire i ruoli che possono essere utilizzati nell'ambito del controllo degli accessi per costruire specifici criteri di autorizzazione. I ruoli possono avere origine interna al registro oppure essere passati da un sistema esterno, sia in contesti fruizione che di erogazione.

- *Applicativo*

  Entità per censire i client, riferiti ad uno specifico soggetto (e quindi modalità), che fruiscono di servizi. Censire un applicativo è indispensabile nei casi in cui l'identificazione è necessaria per poter superare i criteri di autenticazione autorizzazione specificati nella configurazione del *Controllo degli Accessi* per ciascun servizio fruito.

1.3 Il processo di configurazione dei servizi

Le sezioni successive del documento illustrano i passi necessari per realizzare le configurazioni necessarie per rendere operativi i flussi di erogazione/fruizione dei servizi nei diversi profili di interoperabilità supportati.

Per semplificare il processo di configurazione, nel caso di configurazioni per l'interoperabilità con le note piattaforme di erogazione di servizi centralizzate, GovWay mette a disposizione specifici package, denominati *Govlet*. Il Govlet, attraverso un modello di tipo wizard, consente all'utente di fornire i dati necessari a produrre le entità di configurazione per uno specifico servizio. I Govlet disponibili possono essere acquisiti dal sito di Govway al seguente indirizzo http://www.govway.org/govlets. Alcuni esempi di Govlet:

- *FatturaPA - Fatturazione Attiva*: configurazione del servizio per l'invio di fatture elettroniche al Sistema d'Interscambio (SDI).
- *FatturaPA - Fatturazione Passiva*: configurazione del servizio per la ricezione di fatture elettroniche dal Sistema d'Interscambio (SDI).
- *SIOPE+*: configurazione del servizio per l'invio degli ordinativi di pagamento alla piattaforma SIOPE+ e ricezione delle relative notifiche e giornale di cassa.
- *pagoPA*: configurazione del servizio per l'accesso alla piattaforma dei pagamenti elettronici pagoPA.

Una volta entrati in possesso del Govlet è necessario eseguirlo sulla govwayConsole tramite la funzione *Importa* descritta nella Sezione 7.6.

Per procedere manualmente alla produzione delle configurazioni per i servizi, si utilizzano le funzionalità presenti nella sezione *Registro* della GovWayConsole. Il processo manuale di configurazione può essere schematizzato nei passi seguenti:

1. *Definizione delle API*. Il primo passo prevede la definizione delle API relative ai servizi che si vogliono utilizzare. In questa fase tipicamente si provvede al caricamento del descrittore formale delle interfacce (WSDL, WADL, ...).
2. *Registrazione dell'erogazione o fruizione*. Il secondo passo, dopo aver registrato l'API del servizio, prevede la creazione di una Erogazione, o di una Fruizione, a seconda del ruolo previsto nell'interazione col servizio.
3. *Configurazione Specifica*. Le interfacce della GovWayConsole sono state progettate in modo che, il completamento dei primi due passi di configurazione, sia sufficiente a disporre di una configurazione funzionante del servizio. Il terzo, e quindi opzionale passo, consiste nella produzione di tutti i dettaglio aggiuntivi di configurazione che sono necessari alla particolare situazione.

   In questo passo si forniscono i dettagli delle funzionalità aggiuntive, che riguardano:

   - *Controllo degli Accessi*: indicazione dei criteri di autenticazione e autorizzazione necessari per l'accesso al servizio.
   - *Validazione*: processo di validazione dei messaggi in transito sul gateway.
   - *Sicurezza Messaggio*: misure di sicurezza al livello del messaggio richieste.
   - *Tracciamento*: personalizzazione delle tracce prodotte nel corso dell'elaborazione delle richieste di servizio.
   - *Registrazione Messaggi*: indicazione dei criteri di salvataggio degli elementi che compongono le richieste di servizio (payload, header, allegati, ...).

La Figura 2 descrive lo scenario generale in cui opera GovWay

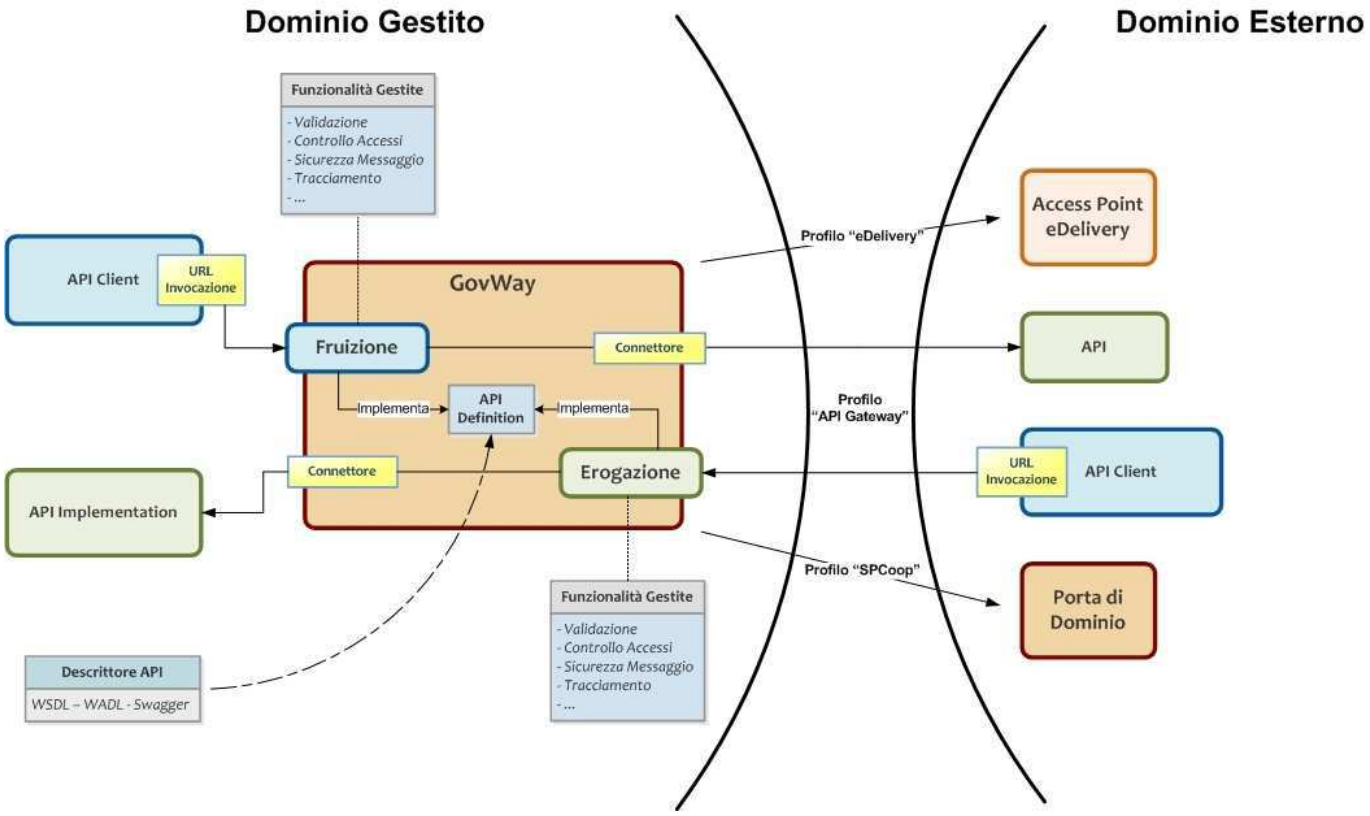


Figura 2: Fasi dell'elaborazione di una richiesta

La sezioni successive descrivono in dettaglio il processo di configurazione di cui sopra, fornendo i dettagli specifici per ciascun profilo di interoperabilità.

2 Profilo "API Gateway"

In questa sezione descriviamo le fasi di configurazione di GovWay al fine di attivare l'erogazione o la fruizione di servizi che rispettano lo standard Soap o Rest. Per semplificare l'utilizzo della console grafica govwayConsole, è consigliabile effettuare la selezione del profilo *API Gateway* tramite l'apposito selettore posto nell'intestazione della pagina.

2.1 Definizione delle API

Indipendentemente che si voglia erogare o fruire un servizio, è necessario iniziare il processo di configurazione con il censimento delle relative API. Questa operazione si effettua sulla govwayConsole posizionandosi nella sezione *Registro* > *API*, premendo quindi il pulsante *Aggiungi*.

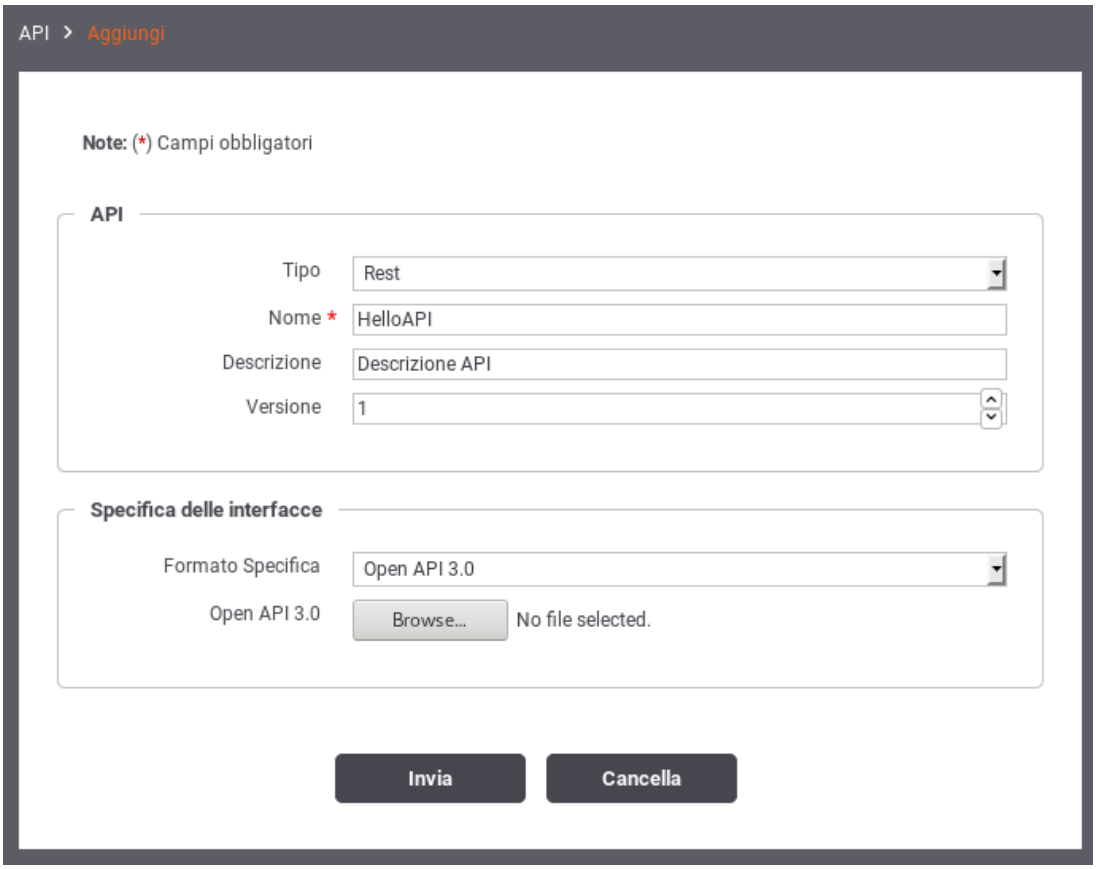


Figura 3: Definizione di una API

Compilare il form (Figura 3) inserendo i seguenti dati:

- *Tipo*: Selezionare il tipo delle API a scelta tra "Soap" e "Rest".
- *Nome*: Assegnare un nome che identifichi le API.
- *Descrizione*: un testo opzionale di descrizione.
- *Versione*: progressivo numerico che identifica l'indice di revisione.
- *Specifica delle Interfacce*: In questa sezione è possibile caricare il descrittore formale dell'interfaccia, analizzando il quale, il gateway produce la corrispondente configurazione. Nel caso di interfacce Soap si potrà caricare il relativo WSDL. Nel caso di interfacce Rest si potrà scegliere tra i formati: WADL, Swagger 2.0 e OpenAPI 3.0.

  Nel caso non si disponga del descrittore dell'interfaccia è sempre possibile inserire manualmente la relativa configurazione seguendo le modalità descritte alla Sezione 8.1.

2.2 Registrazione dell'erogazione

Una volta disponibile la definizione delle API, si passa alla registrazione dell'erogazione fornendo i dati di base per l'esposizione del servizio erogato tramite GovWay. In Figura 4 è illustrato graficamente il caso dell'erogazione.

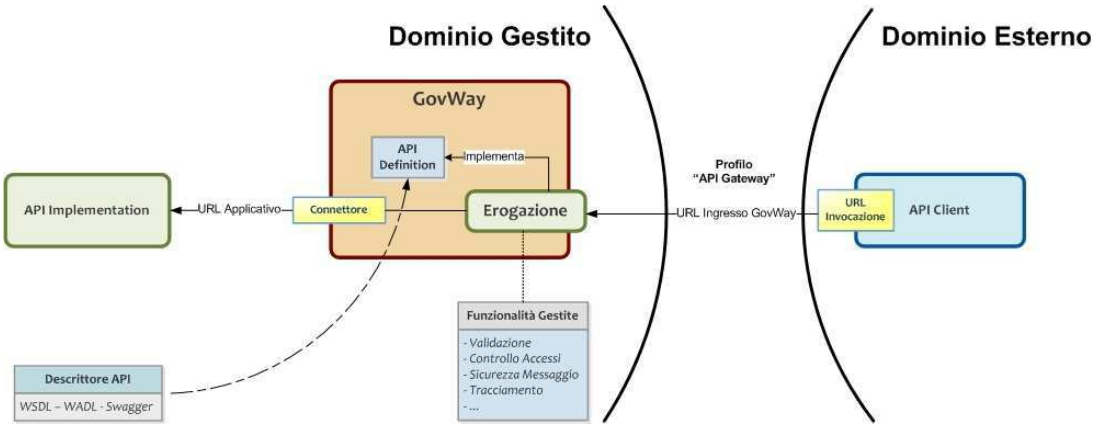


Figura 4: Scenario di riferimento per l'erogazione

Per registrare l'erogazione del servizio ci si posiziona nella sezione *Registro* > *Erogazioni* e si preme il pulsante *Aggiungi*.

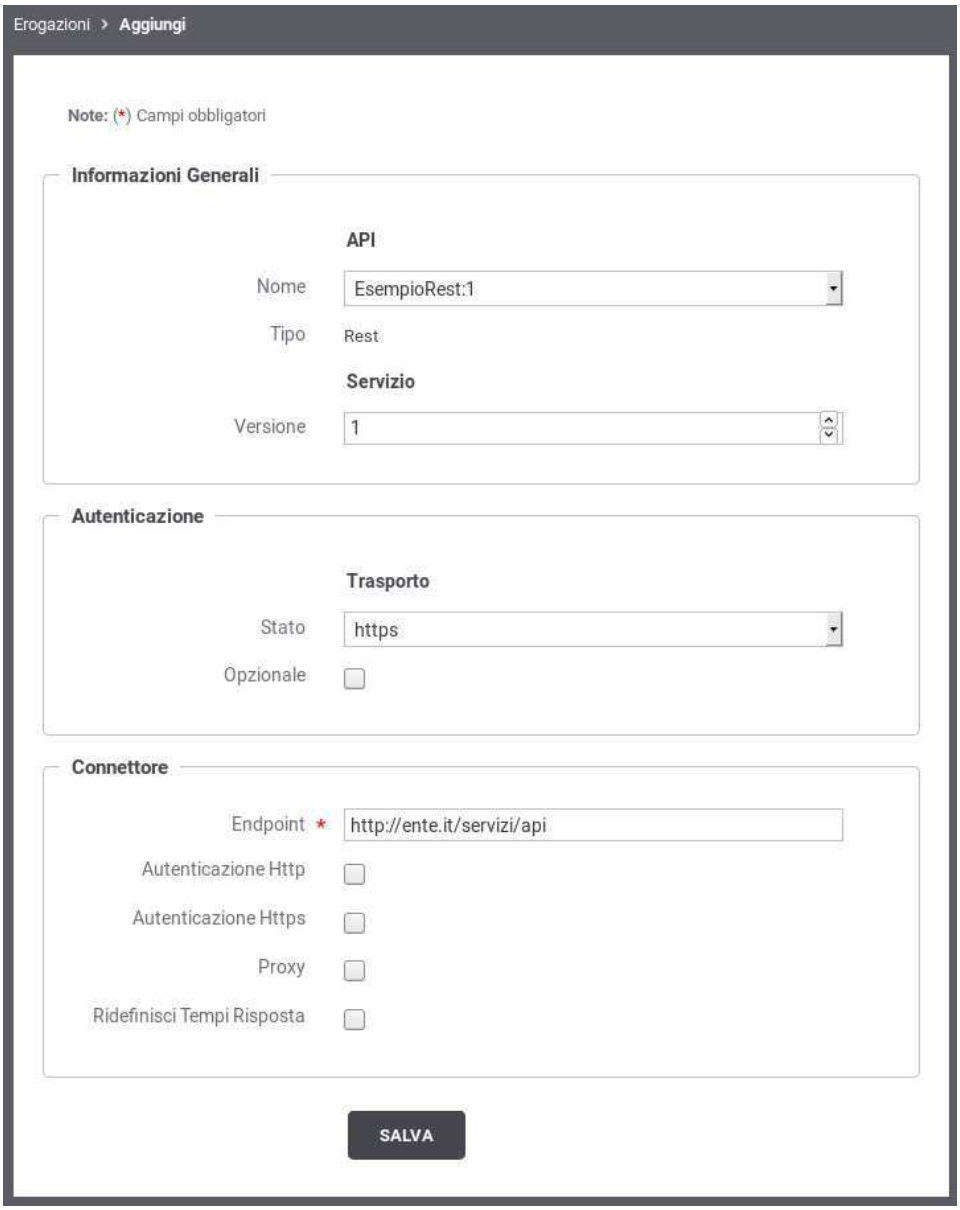


Figura 5: Registrazione di una Erogazione

Compilare il form (Figura 5) inserendo i seguenti dati:

- *API - Nome:* Selezionare dall'elenco il nome e la versione relativa alla API cui l'erogazione fa riferimento. Se la API selezionata è di tipo Soap, sarà necessario selezionare anche il Servizio che si vuole erogare.
- *Servizio - Versione:* Fornire l'indice di versione.
- *Autenticazione:* In questa sezione è possibile configurare il meccanismo di autenticazione richiesto per l'accesso al servizio da parte dei fruitori. Il valore di default proposto prevede l'autenticazione di tipo *https*.

  Come mostrato in Figura 5, è possibile selezionare il tipo di autenticazione a livello del trasporto, selezionando uno tra i valori disponibili:

  – *disabilitato*: nessuna autenticazione
  – *ssl*: autenticazione ssl
  – *basic*: autenticazione http-basic

- *principal*: autenticazione sull'application server con identificazione tramite principal
- *custom*: metodo di autenticazione fornito tramite estensione di GovWay

Il flag *Opzionale* consente di non rendere bloccante il superamento dell'autenticazione per l'accesso al servizio.

- *Connettore:* In questa sezione devono essere specificati i riferimenti al servizio, al fine di rendere possibile il corretto instradamento delle richieste inviate dai soggetti fruitori. Questo connettore riferisce il servizio del dominio interno che si sta erogando.

  Le informazioni da fornire sono:

  - *Endpoint:* la url per la consegna delle richieste al servizio.
  - *Autenticazione Http:* credenziali da fornire nel caso in cui il servizio richieda autenticazione di tipo HTTP-BASIC.
  - *Autenticazione Https:* credenziali da fornire nel caso in cui il servizio richieda autenticazione di tipo HTTPS.
  - *Proxy:* nel caso in cui l'endpoint del servizio sia raggiungibile solo attraverso un proxy, possono essere indicati qui i relativi riferimenti.
  - *Ridefinisci Tempi Risposta:* permette di ridefinire i tempi di risposta che sono stati configurati a livello generale, nell'ambito del controllo del traffico (vedi Sezione 7.3.4)

2.2.1 Completamento configurazione e indirizzamento del servizio

Dopo aver definito le API e registrato la relativa erogazione, come descritto nelle sezioni precedenti, si dispone della configurazione di un servizio erogato i cui riferimenti possono essere comunicati ai fruitori.

Per aggiungere ulteriori dettagli di configurazione, o semplicemente per conoscere il giusto endpoint cui il fruitore deve indirizzare le richieste, si procede dalla pagina di dettaglio dell'erogazione già creata. Il dettaglio dell'erogazione si raggiunge andando alla sezione del menu *Registro* > *Erogazioni*, cliccando sull'elemento visualizzato nell'elenco delle erogazioni presenti nel registro (Figura 6).

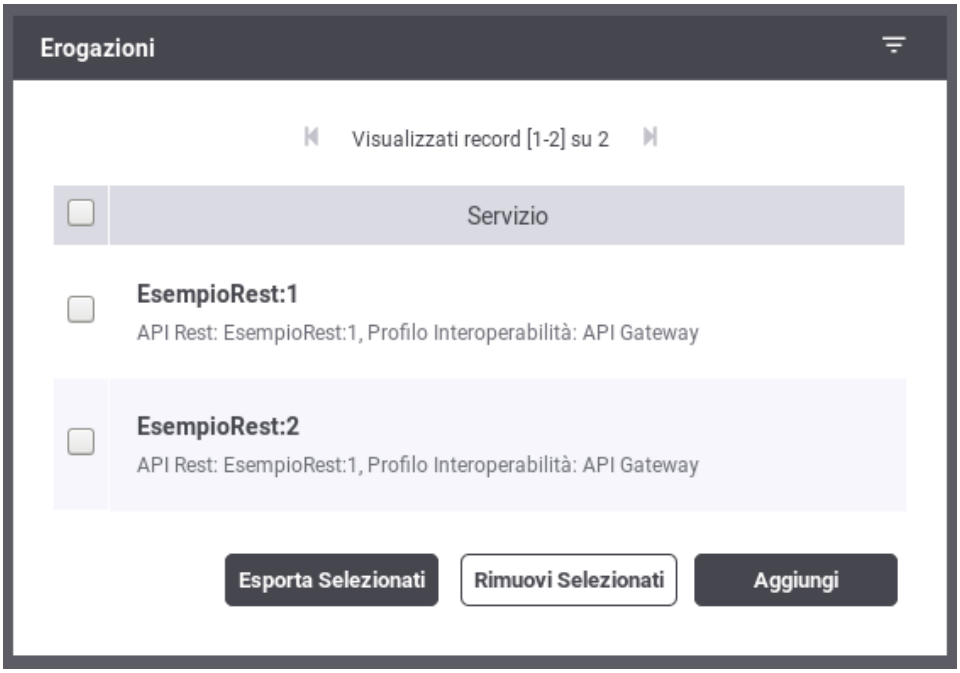


Figura 6: Elenco Erogazioni presenti nel registro

Per la ricerca dell'elemento nell'elenco delle erogazioni è possibile filtrare i dati visualizzati tramite la maschera di filtro che compare cliccando sulla voce *Erogazioni* nell'intestazione dell'elenco (Figura 7).

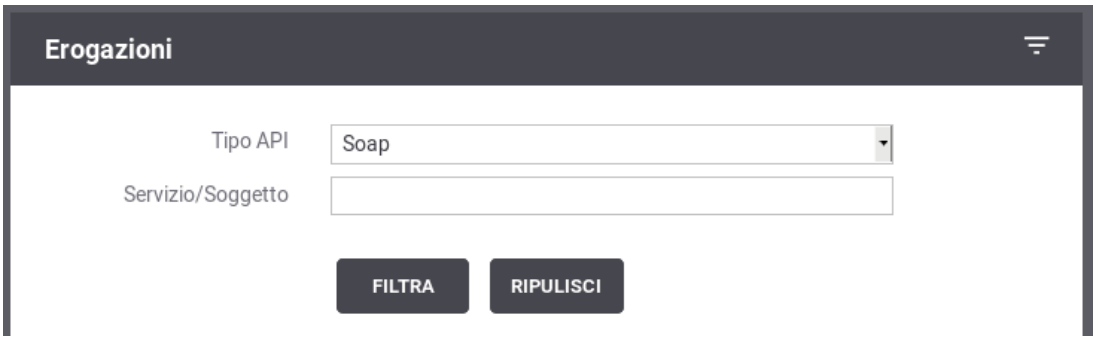


Figura 7: Filtro delle Erogazioni presenti nel registro

Il dettaglio dell'erogazione mostra i dati principali e con le icone "matita" è possibile entrare sulle maschere di editing per effettuare delle modifiche (Figura 8)

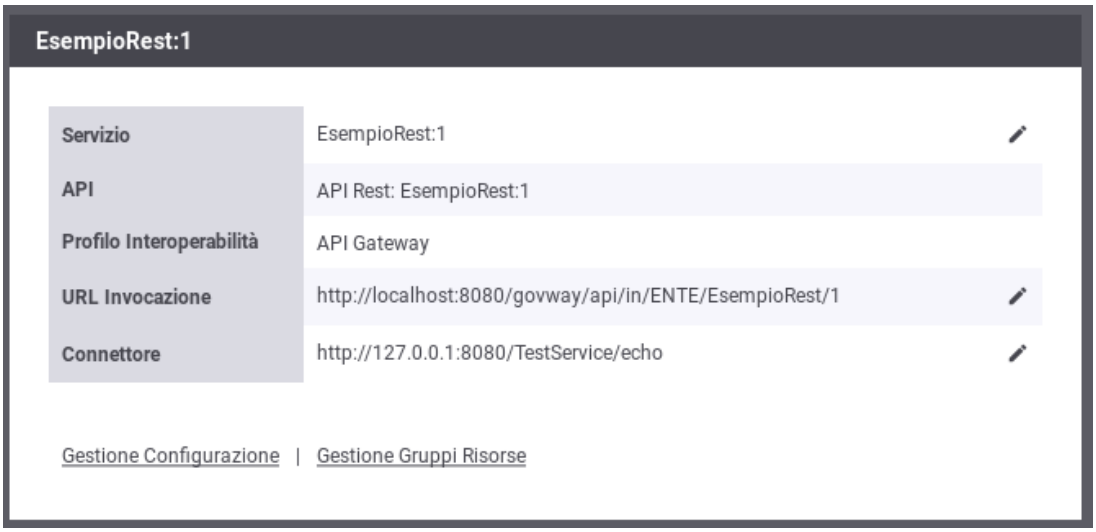


Figura 8: Dettaglio dell'erogazione

La pagina di dettaglio dell'erogazione comprende inoltre i seguenti elementi:

- *Gestione Configurazione*: link per accedere alla configurazione specifica per l'aggiunta di ulteriori funzionalità all'erogazione (vedi Sezione 2.4).
- *Gestione Gruppi Risorse/Azioni*: link per differenziare la configurazione specifica sulla base di diversi gruppi di azioni/risorse, come meglio spiegato alla Sezione 2.4.2.

Dal dettaglio dell'erogazione si ricava il valore *URL Invocazione* che rappresenta l'endpoint da comunicare ai fruitori per contattare il servizio. Questo dato rappresenta la *URL* del servizio nel caso Soap o la *Base URL* nel caso Rest.

Per la selezione dell'operazione da invocare si distinguono i seguenti casi:

- *REST*: Indipendentemente che l'API sia stata configurata fornendo il relativo descrittore, WADL o OpenAPI, l'identificazione dell'operation sarà sempre effettuata in automatico dal contesto di invocazione. Non è quindi necessario fornire ulteriori indicazioni.
- *SOAP*

- *API con WSDL*: l'operation viene automaticamente identificata dal contesto di invocazione grazie alle informazioni presenti nel descrittore.
- *API senza WSDL*: l'operation viene identificata inserendo il relativo identificativo nella URL di invocazione (<URL_Invocazione>/<
  Sono disponibili ulteriori metodi per l'identificazione dell'operation nel caso SOAP, per i cui dettagli si rimanda alla Sezione 8.2.

2.2.2 Condivisione dei dati di integrazione

Le richieste di erogazione, pervenute a GovWay, vengono elaborate e, nel corso dell'operazione, vengono creati i riferimenti alle entità di configurazione presenti nel registro.

GovWay comunica i dati di contesto ricavati, ai sistemi interlocutori, ed in particolare:

- Tutti i dati dell'header di integrazione, relativi al messaggio di richiesta, vengono inviati all'applicativo destinatario (erogatore). I dati che compongono l'header di integrazione sono quelli descritti nelle tabelle presenti alla Sezione 8.5.
- Un sottoinsieme dell'header di integrazione, relativo al messaggio di risposta, viene inviato al soggetto mittente (fruitore). I dati inviati (sempre in riferimento alle tabelle della Sezione 8.5) sono:
  - *GovWay-Message-ID*
  - *GovWay-Relates-To*
  - *GovWay-Conversation-ID*
  - *GovWay-Transaction-ID*

2.3 Registrazione della fruizione

Nel processo di fruizione sono coinvolti i client (o applicativi) interni al dominio che richiedono, tramite accesso sul gateway, un servizio erogato da un soggetto di un dominio esterno.

In Figura 9 è illustrato graficamente il caso della fruizione.

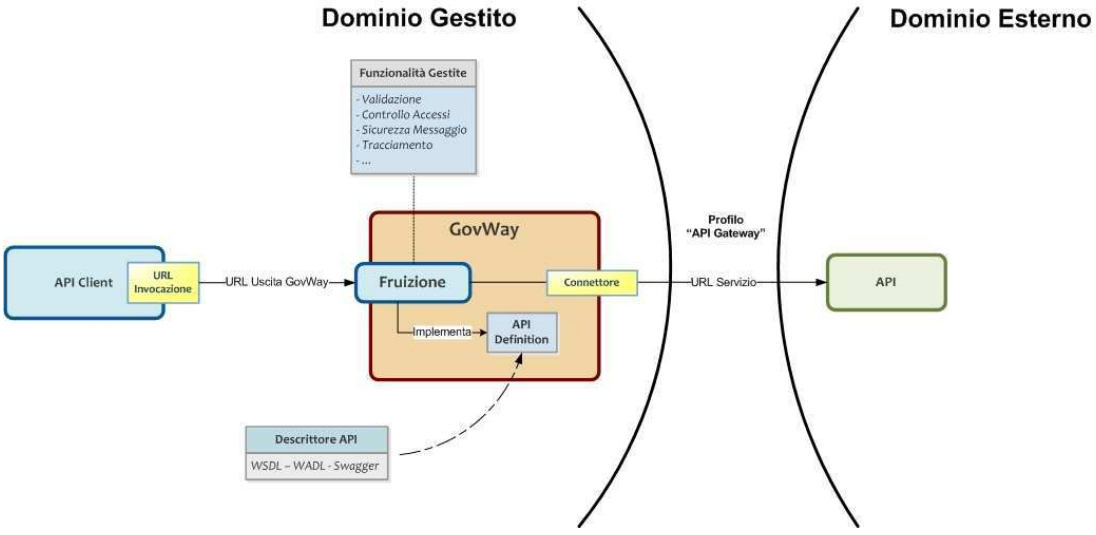


Figura 9: Scenario di riferimento per la fruizione

Analogamente a quanto descritto per le erogazioni, è possibile procedere con la configurazione delle fruizioni accedendo alla sezione di menu *Registro* > *Fruizioni*.

La configurazione delle fruizioni presenta maschere della GovWayConsole del tutto analoghe al caso dell'erogazione. È quindi possibile seguire il processo di configurazione attuando i medesimi passi, illustrati per le erogazioni, calandole sul contesto delle fruizioni.

L'unica differenza, rispetto al processo di configurazione delle erogazioni, è rappresentata dalla presenza del campo *Soggetto Erogatore*, da selezionare come soggetto che eroga il servizio (Figura 10).

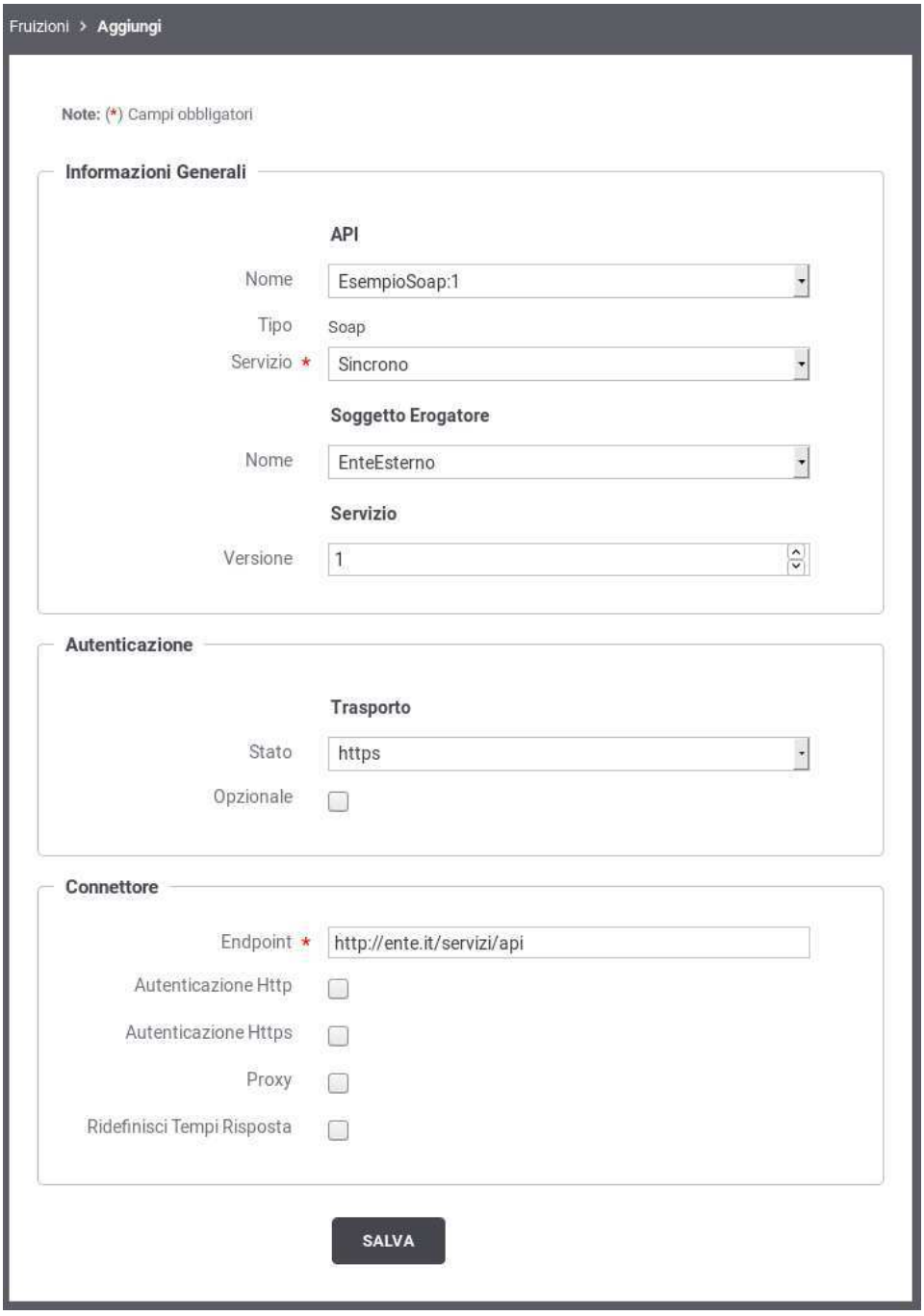


Figura 10: Registrazione di una Fruizione

Nota
Benché non vi siano differenze nelle modalità di configurazione del *Connettore*, nel caso della fruizione questi consiste nei dati di puntamento al servizio erogato sul dominio esterno.

2.3.1 Condivisione dei dati di integrazione

Le richieste di fruizione, pervenute a GovWay, vengono elaborate e, nel corso dell'operazione, vengono creati i riferimenti alle entità di configurazione presenti nel registro.

GovWay comunica i dati di contesto ricavati, ai sistemi interlocutori, ed in particolare:

- Un sottoinsieme dell'header di integrazione, relativo al messaggio di richiesta, viene inviato al soggetto destinatario (erogatore). I dati inviati, descritti nelle tabelle della Sezione 8.5), sono:
  - *GovWay-Message-ID*
  - *GovWay-Relates-To*
  - *GovWay-Conversation-ID*
  - *GovWay-Transaction-ID*
- Tutti i dati dell'header di integrazione, relativi al messaggio di risposta, vengono inviati all'applicativo mittente (fruitore). I dati che compongono l'header di integrazione sono quelli descritti nelle tabelle presenti alla Sezione 8.5.

2.4 Configurazione Specifica

I passi di configurazione fin qui descritti, per la registrazione di erogazioni e fruizioni, consentono di ottenere uno stato delle entità del registro pronto all'utilizzo in numerose situazioni.

Nei casi in cui si abbia l'esigenza di aggiungere ulteriori elementi di configurazione, sfruttando le ulteriori funzionalità messe a disposizione da GovWay, si procede con le ulteriori configurazioni, disponibili a partire dall'erogazione o fruizione già creata in precedenza accedendo tramite il link *Gestione Configurazione* presente nel dettaglio dell'erogazione/fruizione. Le sezioni successive descrivono le configurazioni specifiche attuabili nei vari contesti. Tranne dove esplicitamente dichiarato, gli schemi di configurazione descritti in seguito possono essere attuati sia sulle erogazioni che sulle fruizioni.

2.4.1 Connettore

È possibile modificare le impostazioni del connettore al servizio erogato/fruito (ad esempio per modificare l'endpoint o aggiungere il proxy) seguendo il collegamento presente nella colonna *Connettore* in corrispondenza della voce di erogazione/fruizione presente in elenco. I campi del form sono uguali a quelli già descritti per la fase di creazione dell'erogazione (Sezione 2.2).

2.4.2 Differenziare le configurazioni specifiche per risorsa/azione

Le configurazioni specifiche che andiamo a descrivere si possono differenziare per sottoinsiemi delle azioni/risorse presenti nel servizio erogato/fruito. Il sistema crea automaticamente una configurazione unica, valida per tutte le azioni/risorse del servizio. Per intervenire su tale configurazione, o crearne di nuove, sia accede al collegamento presente nella colonna *Configurazione*, in corrispondenza della voce di erogazione/fruizione in elenco. Le funzionalità di configurazione disponibili per ciascun sottoinsieme di azioni/risorse sono raggruppabili in:

- *Controllo Accessi*: per configurare i criteri di autenticazione, autorizzazione e gestione token delle richieste.
- *Validazione*: per configurare i criteri di validazione dei messaggi in transito sul gateway.
- *Sicurezza Messaggio*: per configurare le misure di sicurezza applicate a livello del messaggio.
- *Tracciamento*: per configurare specifiche modalità di estrazione dati, dalle comunicazioni in transito, per l'arricchimento della traccia prodotta.
- *MTOM*: per configurare l'utilizzo del protocollo ottimizzato per l'invio di attachment tra nodi SOAP.
- *Registrazione Messaggi*: consente di ridefinire le politiche di archiviazione dei payload rispetto a quanto previsto dalla configurazione di default (vedi Sezione 7.2).

Per creare un nuovo gruppo di configurazione, dopo aver seguito il collegamento *visualizza* relativo all'erogazione/fruizione selezionata, si preme il pulsante *Aggiungi*

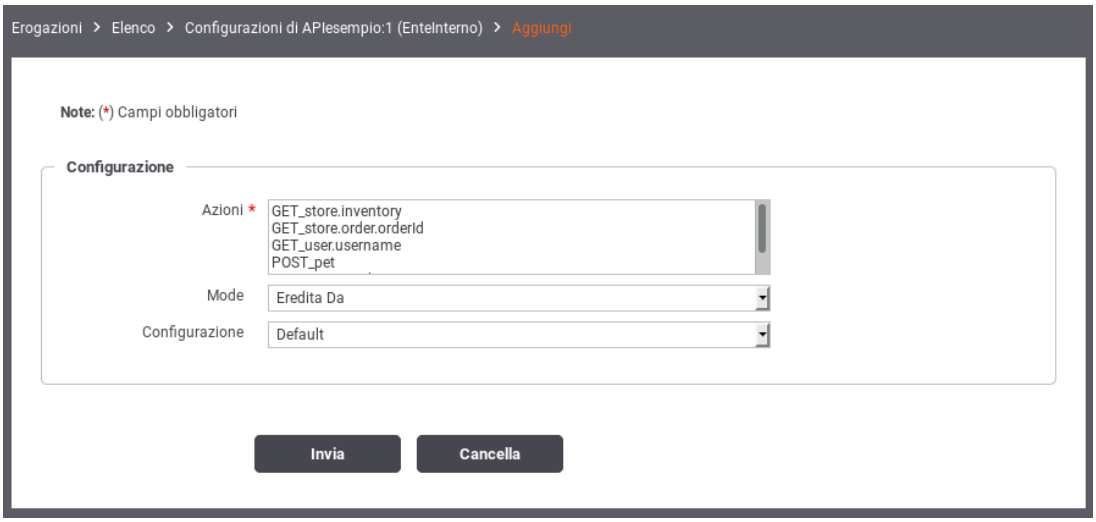


Figura 11: Aggiunta di un gruppo di configurazioni

Compilare il form di creazione della nuova configurazione (Figura 11):

- *Azioni:* selezionare dall'elenco le azioni sulle quali si vuole abbia effetto la nuova configurazione.
- *Mode:* effettuare la scelta tra *Eredita Da* e *Nuova*. Scegliendo la prima opzione, verrà creata una configurazione clone di quella selezionata nell'elemento del form subito successivo (Configurazione). Scegliendo la seconda opzione, si procederà alla creazione di una nuova configurazione, specificando subito le informazioni di Controllo degli Accessi e Connettore.

Nota
Dopo aver creato ulteriori configurazioni, si tenga presente che la configurazione di default verrà applicata alle sole azioni per le quali non è presente una regola di configurazione specifica.

Nota
È possibile disabilitare un'intera configurazione, senza la necessità di eliminarla, utilizzando il collegamento presente nella colonna "Abilitato" in corrispondenza dell'elemento di configurazione. Un successivo clic farà tornare la configurazione nello stato abilitato.

2.4.3 Controllo degli Accessi

Tramite questa funzionalità è possibile configurare i criteri di gestione token, autenticazione e autorizzazione delle richieste in ingresso sul gateway. Per aggiungere questa funzionalità si procede selezionando prima il collegamento, presente nella colonna "Configurazione", relativo all'erogazione/fruizione presente nell'elenco. Successivamente si utilizza il collegamento, presente nella colonna "Controllo Accessi", relativamente alla configurazione che si vuole modificare (Figura 12).

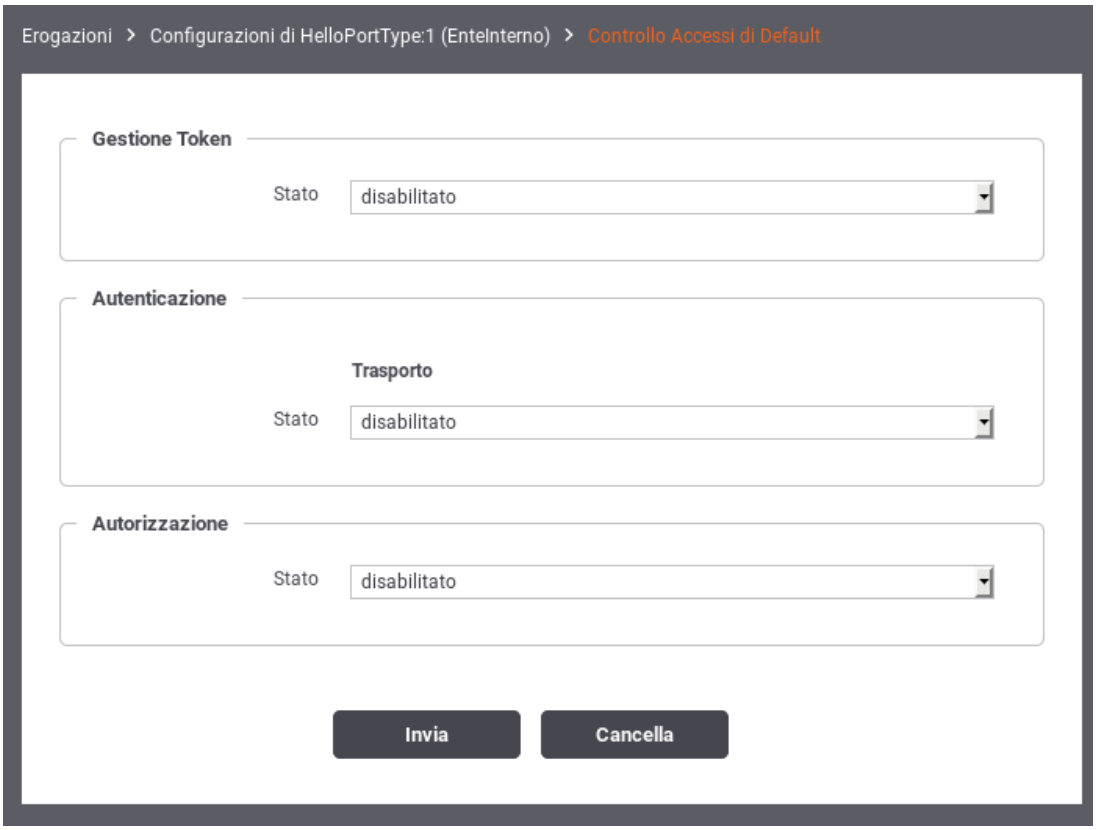


Figura 12: Controllo degli Accessi

Le tre sezioni seguenti descrivono le modalità per configurare i tre aspetti che compongono il controllo degli accessi.

2.4.3.1 Gestione Token

Questa sezione consente di configurare il controllo degli accessi basato su Bearer Token OAuth2. Facendo transitare lo stato su "abilitato" compare l'elemento *Policy* (obbligatorio) per la selezione della policy di gestione token che si vuole applicare. In questa lista a discesa saranno visualizzate tutte le *Token Policy* che sono state registrate in precedenza. Per le istruzioni sulla registrazione delle Token Policy si faccia riferimento alla Sezione 7.4.

Una volta selezionata la policy compariranno sotto gli elementi per stabilire le specifiche azioni da abilitare rispetto al totale di quelle previste nella policy stessa (Figura 13).

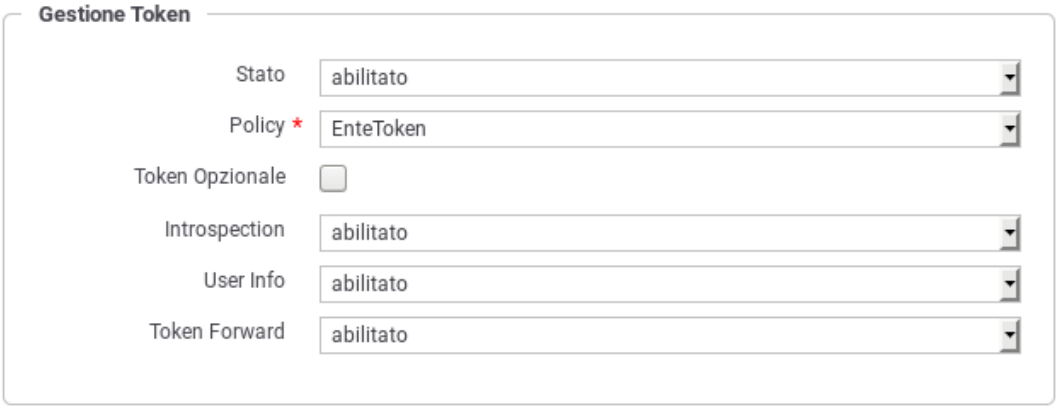


Figura 13: Configurazione della gestione token

Supponendo che la policy copra tutti gli aspetti disponibili, le opzioni configurabili sono le seguenti:

- *Token Opzionale*: consente di non forzare i richiedenti al passaggio del token, che rimane quindi un'operazione opzionale.
- *Introspection*: consente di abilitare/disabilitare l'operazione di Token Introspection, al fine di validare il token ricevuto ed ottenere le metainformazioni associate (ad esempio scope e riferimento al possessore del token). Selezionando l'opzione *WarningOnly* è possibile non rendere bloccante l'evento di fallimento della validazione, ottenendo come unico effetto l'emissione di un messaggio diagnostico di segnalazione.
- *User Info*: consente di abilitare/disabilitare l'operazione UserInfo al fine di ottenere le informazioni di dettaglio dell'utente possessore del token. Selezionando l'opzione *WarningOnly* è possibile non rendere bloccante l'evento di fallimento della validazione, ottenendo come unico effetto l'emissione di un messaggio diagnostico di segnalazione.
- *Token Forward*: consente di abilitare/disabilitare l'operazione di inoltro, al servizio destinatario, del token ricevuto dal mittente.

Le azioni che sono state abilitate saranno effettuate in accordo a quanto configurato nella relativa Token Policy selezionata.

Nota
È disponibile la Token Policy *Google* preconfigurata in modo da utilizzare i servizi di elaborazione token esposti pubblicamente da Google e quindi:

- La Validazione JWT basata su *Google - ID Token*
- Il servizio di token introspection basato su *Google - TokenInfo*
- Il servizio di User Info basato su *Google - UserInfo*

2.4.3.2 Autenticazione

In questa sezione è possibile configurare il meccanismo di autenticazione richiesto per l'accesso al servizio. Come mostrato in Figura 14, si possono specificare:

- Il tipo di autenticazione, per il quale si procede come già descritto per l'attività di creazione dell'erogazione nella Sezione 2.2.
- Se è stata attivata, al passo precedente, la gestione del token sarà possibile aggiungere ulteriori criteri di autenticazione basati sul contenuto del token ricevuto. In tal caso è possibile autenticare la richiesta sulla base delle seguenti metainformazioni presenti nel token: Issuer, ClientId, Subject, Username, Email.

i criteri di autenticazione possono essere attuati sia a livello del trasporto che del token (se abilitata la gestione del token al passo precedente).

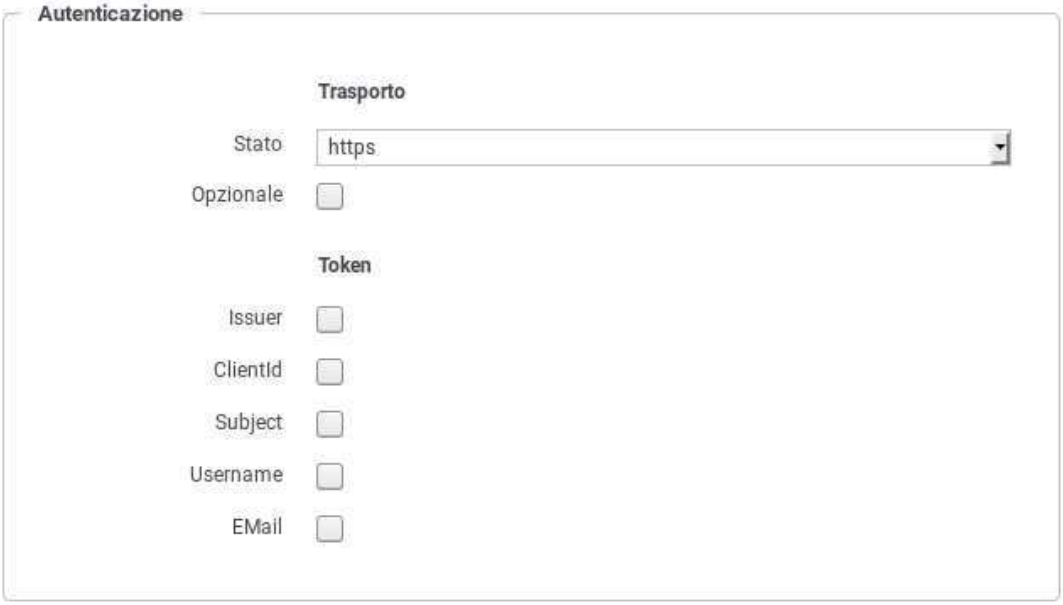


Figura 14: Configurazione dell'autenticazione del servizio

2.4.3.3 Autorizzazione

L'autorizzazione è un ulteriore meccanismo per il controllo degli accessi tramite il quale è possibile specificare con maggior dettaglio le richieste che sono in grado di essere accettate per l'accesso al servizio.

I meccanismi supportati, per specificare i criteri di autorizzazione, sono i seguenti:

- *Soggetti autenticati (solo per le erogazioni)*: superato il processo di autenticazione, saranno accettate le sole richieste provenienti dai soggetti indicati in lista. Dopo aver barrato questa opzione, ed aver confermato tramite il pulsante Invia, sarà possibile fornire la lista dei soggetti autorizzati ad accedere al servizio.

  I soggetti dovranno essere precedentemente registrati sulla govwayConsole seguendo le indicazioni fornite in Sezione 2.4.3.4.

  Nota
  L'opzione di autorizzazione sui soggetti è disponibile solo se è stata attivata l'autenticazione.

- *Applicativi autenticati (solo per le fruizioni)*: superato il processo di autenticazione, saranno accettate le sole richieste provenienti dagli applicativi indicati in lista. Dopo aver barrato questa opzione, ed aver confermato tramite il pulsante Invia, sarà possibile fornire la lista degli applicativi autorizzati ad accedere al servizio.

- *Ruoli*: consente di concedere l'autorizzazione per il servizio solo ai richiedenti in possesso di determinati ruoli nel proprio profilo. Dopo aver barrato questa opzione, ed aver confermato tramite il pulsante Invia, sarà possibile fornire una lista dei ruoli che devono essere posseduti dal chiamante per poter accedere al servizio. In particolare si dovrà anche specificare la *fonte* di provenienza dei ruoli, che può essere *esterna*, cioè proveniente dal sistema che ha autenticato il chiamante, oppure *registro*, cioè i ruoli che sono stati censiti nel registro di GovWay e assegnati al soggetto chiamante. Inoltre si deve scegliere l'opzione *Ruoli Richiesti* per indicare se, in presenza di più di un ruolo come criterio, il chiamante deve possedere "tutti" i ruoli indicati o "almeno uno".

  Per le indicazioni sul censimento dei ruoli fare riferimento alla Sezione 2.4.3.6.

- *XACML-Policy*: in alternativa alle due modalità precedenti, è possibile basare il meccanismo di autorizzazione sulla valutazione di una policy xacml.

  Per le indicazioni di dettaglio sulla configurazione delle xacml-Policy si faccia riferimento alla Sezione 2.4.3.8

- *Custom*: metodo di autorizzazione fornito tramite estensione di GovWay.

- *Scope*: criterio di autorizzazione che verifica la corrispondenza tra gli scope indicati e quelli estratti dal token presente nella richiesta ricevuta. Una volta attivata l'opzione si deve effettuare una scelta per l'elemento *Scope Richiesti*, tra i valori "tutti" (tutti gli scope indicati devono essere presenti nel token per superare l'autorizzazione) e "almeno uno" (è richiesta la presenza di almeno uno scope tra quelli indicati nella policy di autorizzazione). Dopo aver confermato la scelta con il pulsante "Invia" verrà richiesto di inserire gli scope tra quelli già censiti ed abilitati per l'uso nei contesti di erogazione (o qualsiasi contesto).

  Nota
  L'opzione di autorizzazione basata sugli scope è disponibile solo se è stata preventivamente attivata la Gestione Token e selezionata la relativa policy.

- *Token*: Se è stata abilitata la gestione del token si ha la possibilità di autorizzare le richieste inserendo i valori ammessi per i claims contenuti nel token. La configurazione viene effettuata inserendo nel campo di testo ciascun claim in una riga, facendo seguire dopo l'uguale i valori ammessi separati da virgola.

  Nota
  L'opzione di autorizzazione basata sui token è disponibile solo se è stata preventivamente attivata la Gestione Token e selezionata la relativa policy.

2.4.3.4 Creazione di un soggetto

Affinché possano essere utilizzate le funzionalità di autenticazione ed autorizzazione, associate alle erogazioni, è necessario che vengano censiti i soggetti fruitori che inviano le richieste di servizio. La registrazione di un soggetto consente di assegnargli delle credenziali che lo identificano ed eventuali ruoli provenienti dalla fonte "Registro".

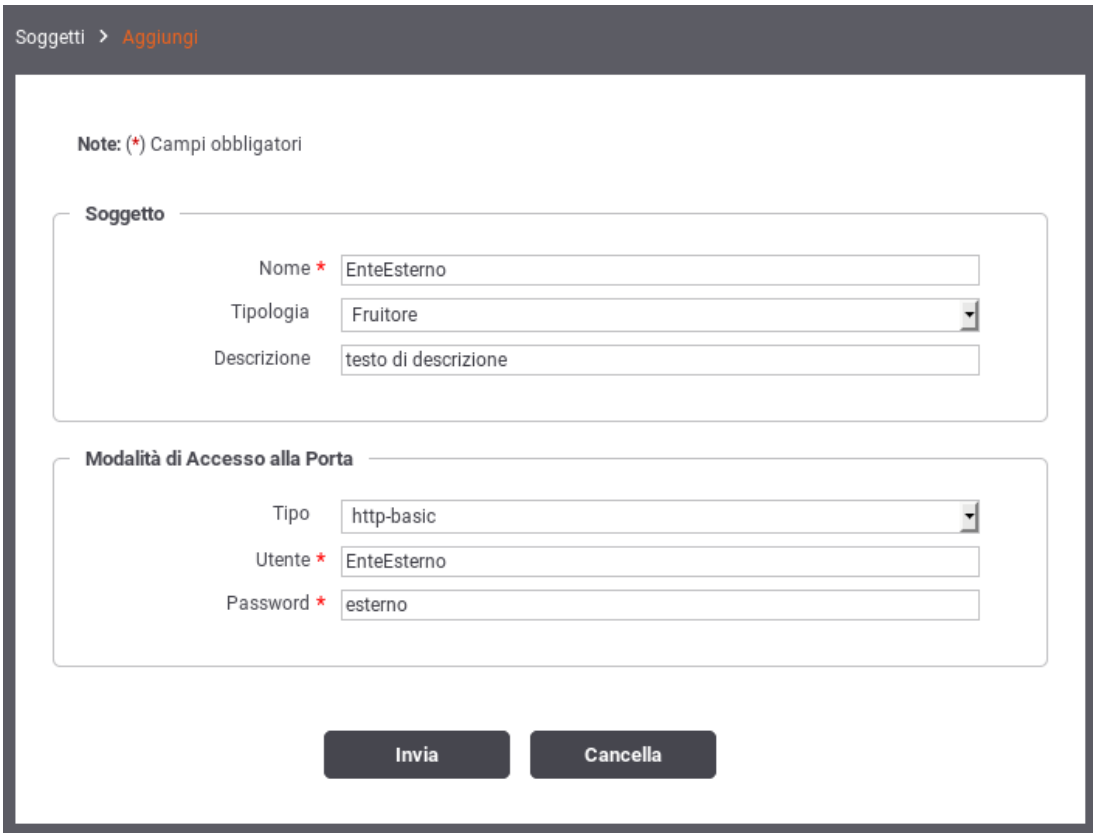


Figura 15: Creazione di un soggetto

Per creare il soggetto posizionarsi nella sezione *Registro* > *Soggetti*, quindi premere il pulsante *Aggiungi*. Compilare il form come segue (Figura 15):

- *Nome*: Il nome del soggetto. È necessario che il nome indicato risulti univoco rispetto ai nomi già presenti per la modalità operativa selezionata (in questo caso API Gateway).
- *Tipologia*: Indicare se si tratta di un soggetto esclusivamente erogatore, esclusivamente fruitore o con entrambi i ruoli.
- *Descrizione*: Un testo di descrizione per il soggetto.
- *Modalità di Accesso alla Porta*: Sezione presente solo nel caso il soggetto ricopra il ruolo di fruitore. Tramite il campo *Tipo* si seleziona il tipo di credenziali richieste per l'autenticazione del soggetto. In base alla scelta effettuata saranno mostrati i campi per consentire l'inserimento delle credenziali richieste.

Dopo aver creato il soggetto è opzionalmente possibile assegnargli dei ruoli, tra quelli che sono presenti nel registro e contrassegnati come *fonte registro*. Per associare ruoli ad un soggetto seguire il collegamento presente nella colonna *Ruoli*, in corrispondenza del soggetto scelto. Premere quindi il pulsante *Aggiungi*. Nel form che si apre (Figura 16) è presente una lista dalla quale è possibile selezionare un ruolo alla volta, che viene aggiunto confermando con il tasto *Invia*.

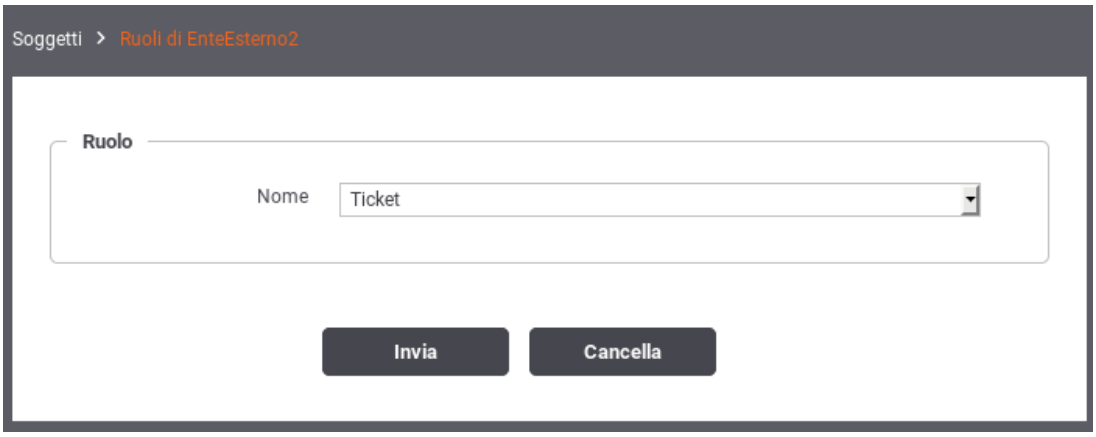


Figura 16: Assegnazione di ruoli ad un soggetto

2.4.3.5 Creazione di un applicativo

Affinché possano essere utilizzate le funzionalità di autenticazione ed autorizzazione, associate alle fruizioni, è necessario che vengano censiti gli applicativi, interni al dominio, che inviano le richieste di servizio. La registrazione di un applicativo consente di assegnargli delle credenziali che lo identificano ed eventuali ruoli provenienti dalla fonte "Registro".

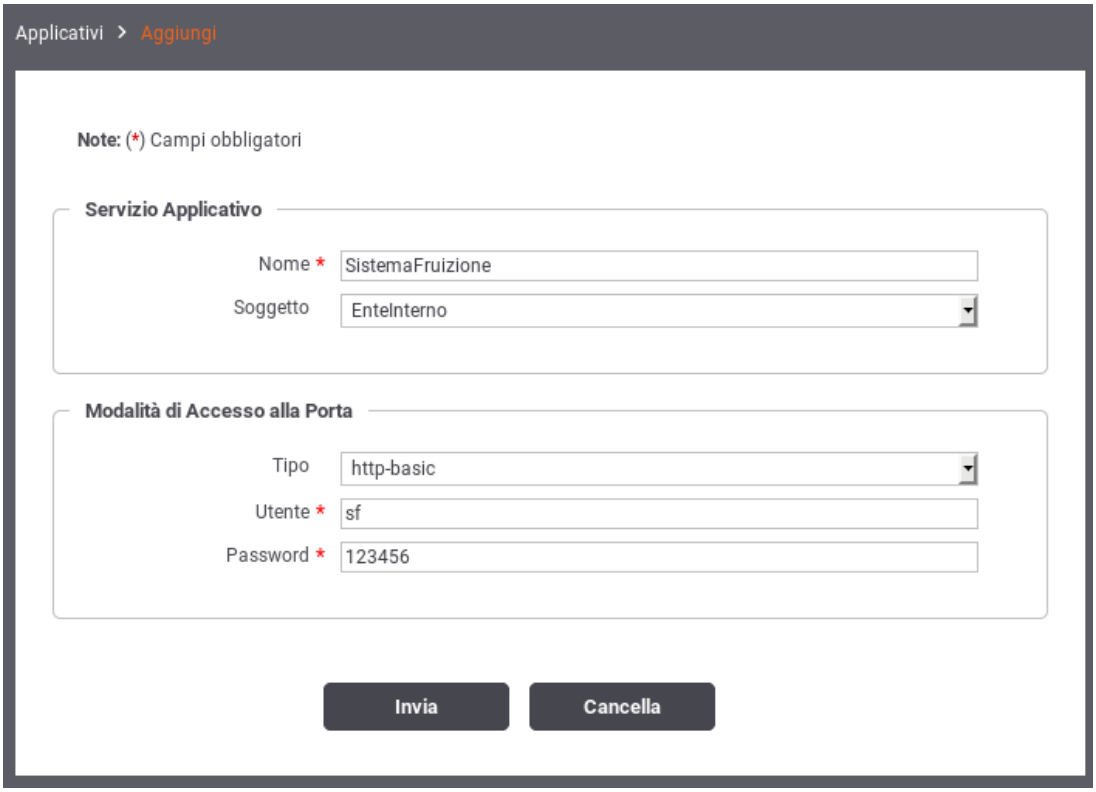


Figura 17: Creazione di un applicativo

Per registrare l'applicativo posizionarsi nella sezione *Registro* > *Applicativi*, quindi premere il pulsante *Aggiungi*. Compilare il form come segue (Figura 17):

- *Nome*: Assegnare un nome all'applicativo. È necessario che il nome indicato risulti univoco rispetto ai nomi già presenti per la modalità operativa selezionata (in questo caso API Gateway).

- *Soggetto*: Selezionare il soggetto interno cui fa riferimento l'applicativo.
- *Modalità di Accesso alla Porta*: Tramite il campo *Tipo* si seleziona il tipo di credenziali richieste per l'autenticazione dell'applicativo. In base alla scelta effettuata saranno mostrati i campi per consentire l'inserimento delle credenziali richieste.

Dopo aver creato l'applicativo è opzionalmente possibile assegnargli dei ruoli, tra quelli che sono presenti nel registro e contrassegnati come *fonte registro*. Per associare ruoli ad un applicativo seguire il collegamento presente nella colonna *Ruoli*, in corrispondenza dell'applicativo scelto. Premere quindi il pulsante *Aggiungi*. Nel form che si apre è presente una lista dalla quale è possibile selezionare un ruolo alla volta, che viene aggiunto confermando con il tasto *Invia*.

2.4.3.6 Creazione di un ruolo

È possibile censire i ruoli che potranno essere utilizzati come criterio di autorizzazione. Quelli contrassegnati come *fonte registro* potranno essere associandoli ai soggetti. Quelli invece contrassegnati come *fonte esterna* verranno assegnati dinamicamente ai soggetti che si autenticano, sulla base di quanto comunicato dal container dopo che l'utente ha effettuato l'autenticazione esternamente.

Per creare un nuovo ruolo ci si posiziona nella sezione *Registro* > *Ruoli* e si preme il pulsante *Aggiungi*.

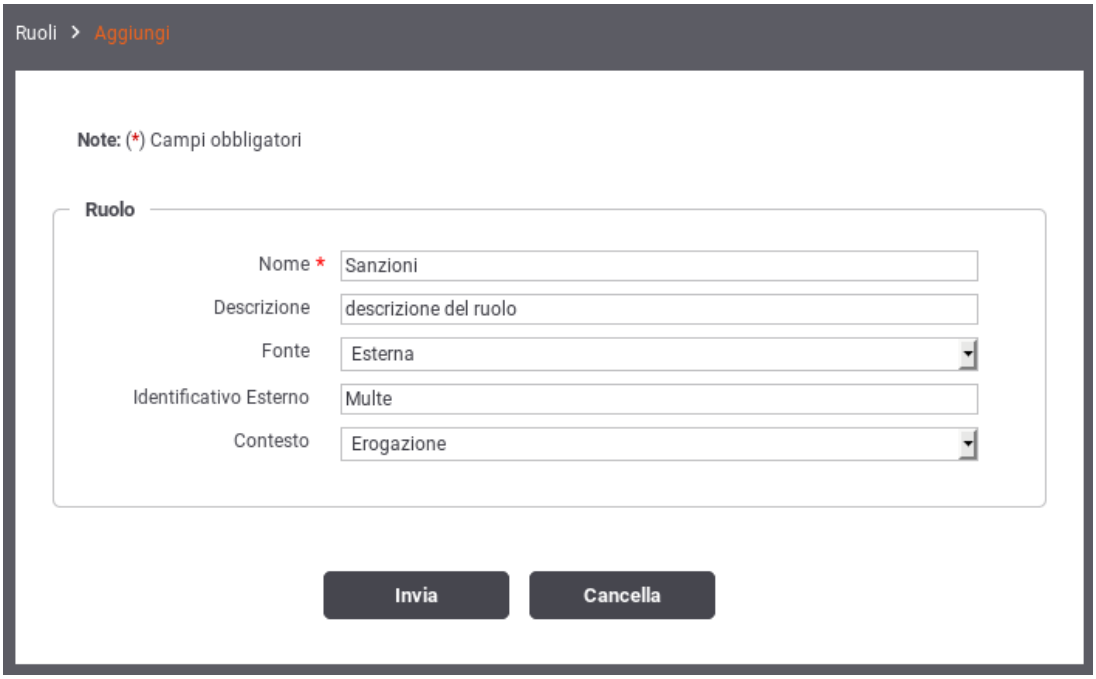


Figura 18: Registrazione di un ruolo

Compilare il form (Figura 18) nel seguente modo:

- *Nome*: identifica univocamente il ruolo.
- *Descrizione*: rappresenta una descrizione generica del ruolo.
- *Fonte*: la gestione del ruolo può essere effettuata direttamente su GovWay (fonte: registro) dove può essere assegnato ad un soggetto o applicativo. In alternativa (fonte: esterna) la gestione può essere delegata all'Application Server o a qualunque altra modalità che permetta al gateway di accedere ai ruoli tramite la api *HttpServletRequest.isUserInRole()*. In questo caso il nome del ruolo deve corrispondere allo stesso identificativo utilizzato nella configurazione esterna.

  Se non viene specificata alcuna fonte il ruolo potrà essere utilizzato per entrambe le modalità.
- *Contesto*: l'utilizzo del ruolo può essere limitato ad un contesto di erogazione o fruizione di servizio attraverso questa opzione.
- *Identificativo Esterno*: Nei casi in cui il ruolo provenga da un sistema esterno, è possibile che il suo identificativo sia differente rispetto a quello indicato nel contesto del Registro. In tal caso inserire in questo campo tale identificativo esterno.

2.4.3.7 Attribuzione dei Ruoli a Soggetti ed Applicativi

È possibile attribuire un ruolo ad un soggetto cliccando sulla voce 'Ruoli' presente sia nell'elenco dei soggetti che nel dettaglio di un singolo soggetto. L'attribuzione consiste nello scegliere uno dei ruoli selezionabili per il soggetto tra quelli compatibili con il contesto di erogazione di servizio e che prevedono una fonte di registrazione interna al registro.

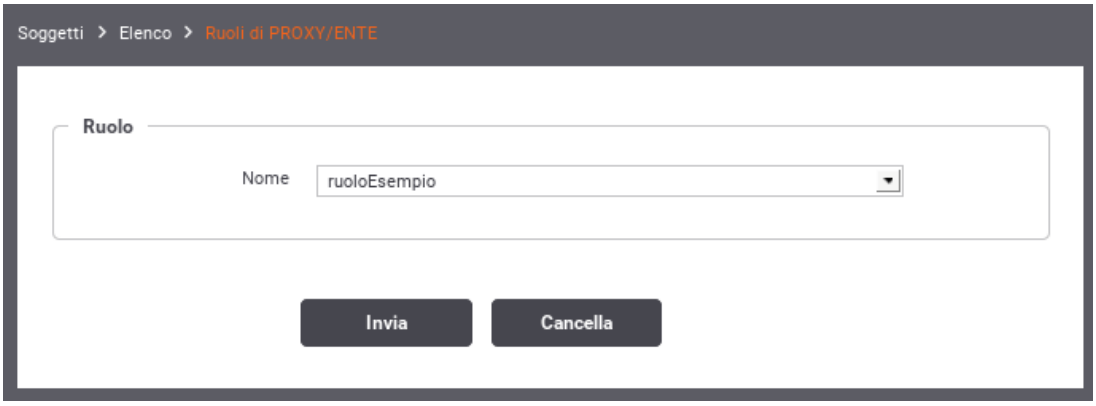


Figura 19: Attribuzione di un ruolo ad un soggetto

In uguale maniera è possibile attribuire un ruolo ad un applicativo di tipologia *Frutore* cliccando sulla voce 'Ruoli' presente nel dettaglio dell'applicativo. L'attribuzione consiste nello scegliere uno dei ruoli selezionabili per il servizio applicativo tra quelli compatibili con il contesto di fruizione di servizio e che prevedono una fonte di registrazione interna al registro.

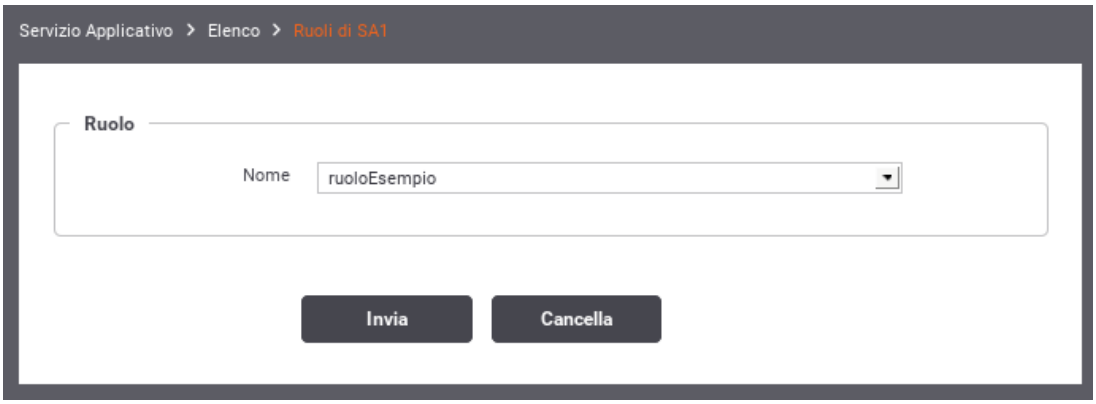


Figura 20: Attribuzione di un ruolo ad un applicativo

2.4.3.8 XACML-Policy

Questa tipologia di autorizzazione prevede di limitare l'accesso ai soli applicativi o soggetti fruitori che soddisfino una determinata policy XACML. La policy deve essere caricata nel contesto dell'autorizzazione sul controllo degli accessi, come mostrato in Figura 21.

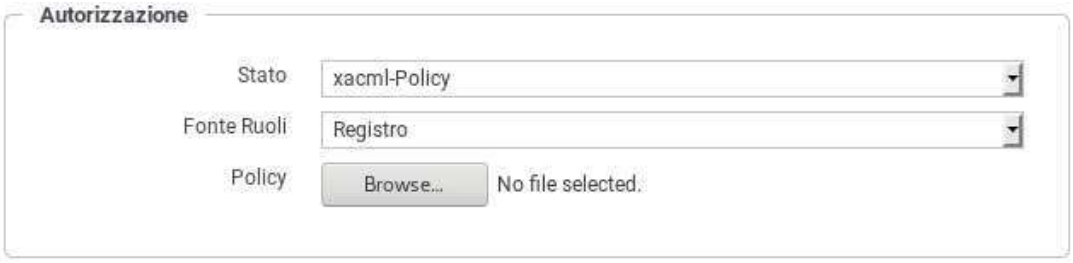


Figura 21: Registrazione di una XACML-Policy per l'erogazione

In fase di autorizzazione, il gateway costruisce una XACMLRequest contenente tutti i parametri della richiesta, comprese le informazioni relative al chiamante (credenziali ed eventuali ruoli), e la valida rispetto alla XACML-Policy associata all'erogazione. I parametri inseriti nella XACMLRequest, che possono essere utilizzati per effettuare la verifica all'interno di una XACML-Policy, sono i seguenti: Di seguito un esempio di XACMLPolicy che autorizza le richieste dei chiamanti che possiedono il ruolo

Nome	**Descrizione**
Sezione 'Action'	
org:govway:action:provider	Indica il soggetto erogatore del servizio
org:govway:action:service	Indica il servizio nel formato tipo/nome
org:govway:action:action	Nome dell'operazione del servizio invocata
org:govway:action:url	Url di invocazione utilizzata dal mittente
org:govway:action:url:parameter:NOME_PARAM	Tutti i parametri presenti nell'url di invocazione saranno inseriti nella XACMLRequest con questo formato
org:govway:action:transport:header:NOME_HDR	Tutti gli header http presenti nell'url di invocazione saranno inseriti nella XACMLRequest con questo formato
org:govway:action:soapAction	Valore della SOAPAction
org:govway:action:gwService	Ruolo della transazione (inbound/outbound)
org:govway:action:protocol	Modalità associata al servizio richiesto (es. spcoop)
org:govway:action:token:audience	Destinatario del token
org:govway:action:token:scope	Lista di scopes
org:govway:action:token:jwt:claim:<nome>=<valore>	Tutti i claims presenti nel jwt validato
org:govway:action:token:introspection:claim:<nome>=<valore>	Tutti i claims presenti nella risposta del servizio di introspection
Sezione 'Subject'	
org:govway:subject:organization	Indica il soggetto fruitore
org:govway:subject:client	Identificativo del servizio applicativo client
org:govway:subject:credential	Rappresenta la credenziale di accesso (username, subject o il principal) utilizzata dal client per richiedere il servizio
org:govway:subject:role	Elenco dei ruoli che possiede il client che ha richiesto il servizio
org:govway:subject:token:issuer	Issuer del token
org:govway:subject:token:subject	Subject del token
org:govway:subject:token:username	Username dell'utente cui è associato il token
org:govway:subject:token:clientId	Identificativo del client che ha negoziato il token
org:govway:subject:token:userInfo:fullName	Nome completo dell'utente cui è associato il token
org:govway:subject:token:userInfo:firstName	Nome dell'utente cui è associato il token
org:govway:subject:token:userInfo:middleName	Secondo nome (o nomi aggiuntivi) dell'utente cui è associato il token
org:govway:subject:token:userInfo:familyName	Cognome dell'utente cui è associato il token
org:govway:subject:token:userInfo:eMail	Email dell'utente cui è associato il token
org:govway:subject:token:userInfo:claim:<nome>=<valore>	Tutti i claims presenti nella risposta del servizio di UserInfo

Tabella 1: Parametri inseriti in una XACMLRequest

'Amministratore' ed uno tra i due ruoli 'Operatore1' e 'Operatore2':

```
<Policy PolicyId="Policy"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit- ↩
      overrides"
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi="http://www.w3.org ↩
      /2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os http://docs.oasis- ↩
      open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd">
  <Target />
  <Rule Effect="Permit" RuleId="ok">
    <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

        <Apply
          FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member- ↩
              of">
          <SubjectAttributeDesignator
            AttributeId="org:govway:subject:role"
            DataType="http://www.w3.org/2001/XMLSchema#string" />
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> ↩
                Amministratore</AttributeValue>
          </Apply>
        </Apply>

        <Apply
          FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member- ↩
              of">
          <SubjectAttributeDesignator
            AttributeId="org:govway:subject:role"
            DataType="http://www.w3.org/2001/XMLSchema#string" />
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> ↩
                Operatore1</AttributeValue>
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> ↩
                Operatore2</AttributeValue>
          </Apply>
        </Apply>

      </Apply>
    </Condition>
  </Rule>
  <Rule Effect="Deny" RuleId="ko" />
</Policy>
```

2.4.3.9 Scope

Nella sezione *Registro* > *Scope* è possibile gestire il censimento degli scope da utilizzare successivamente per le politiche di autorizzazione nell'ambito del controllo degli accessi.

La maschera di creazione di uno scope è quella mostrata in Figura 22.

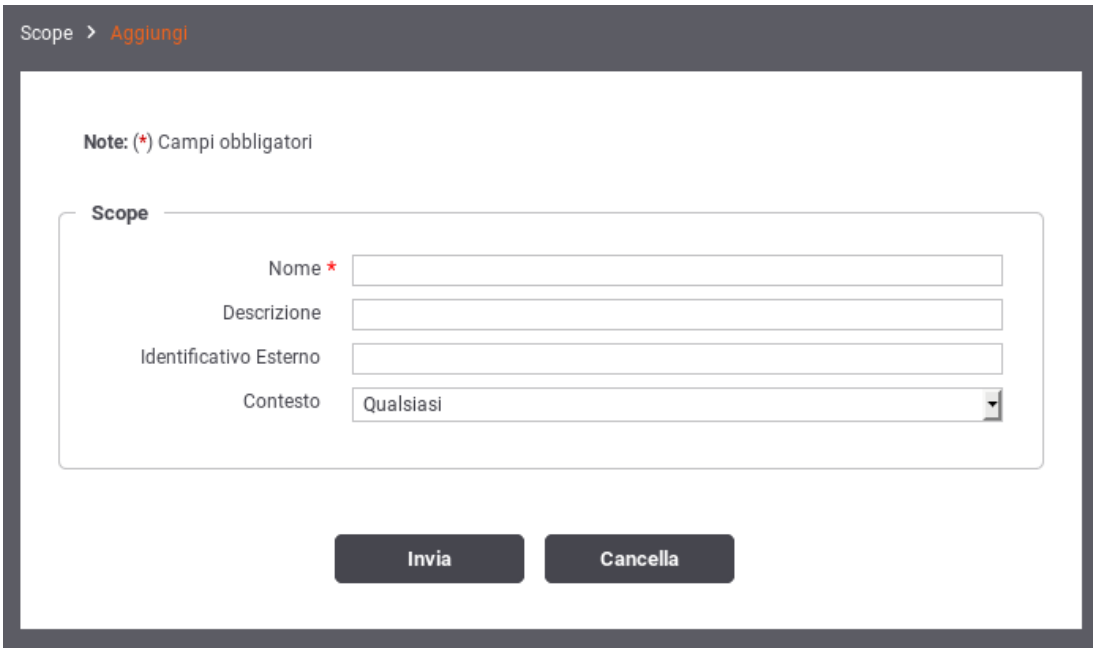


Figura 22: Creazione di uno Scope

I dati da fornire sono:

- *Nome*: nome assegnato internamente allo scope
- *Descrizione*: un testo di descrizione
- *Identificativo Esterno*: nome originale dello scope presente nel token
- *Contesto*: specifica se lo scope si utilizza solo nei contesti di erogazione, fruizione o entrambe le possibilità.

2.4.4 Validazione dei messaggi

Per attivare la validazione dei messaggi in transito sul gateway si accede al collegamento presente nella colonna *Validazione* presente tra gli elementi di configurazione della specifica erogazione/fruizione.

Figura 23: Validazione dei messaggi

Compilare il form di configurazione (Figura 23):

- *Stato*: Consente di abilitare/disabilitare la funzionalità di validazione sulla voce di configurazione scelta. L'opzione *warnignOnly* consente di attivare la funzionalità di validazione evitando però che, se tale fase non viene superata, venga bloccato il messaggio e restituito un errore. In quest'ultimo caso, gli errori di validazione verranno segnalati solo tramite l'emissione di opportuni messaggi diagnostici dal servizio di tracciamento.
- *Tipo*: Nel caso si sia abilitato il servizio di validazione, questo campo consente di selezionare la metodologia che si vuole utilizzare. I valori selezionabili da questo elenco cambiano in base alla tipologia delle API cui fa riferimento l'erogazione/fruizione.

I tipi di validazione previsti sono:

- *Schemi XSD*, la validazione si basa sugli schemi xsd allegati alle API. Utilizzato per la validazione sintattica dei messaggi XML sia nel caso Soap che Rest.
- *Wsdl*, la validazione si basa sull'interfaccia wsdl fornita con la API. Questo tipo di validazione è più rigorosa in quanto controlla non solo la conformità sintattica ma viene validato il messaggio in transito verificando che sia idoneo al PortType e Operation in uso. Questo tipo di validazione è applicabile solo al caso Soap.

  Swagger 2.0 o OpenAPI 3.0, nei casi in cui si è fornito un descrittore formale per una API Rest, la validazione sarà effettuata utilizzando gli strumenti associati allo specifico formato.

Nel caso di servizi Soap, se i messaggi che transitanto sulla porta di dominio possiedono il formato MTOM, per poterli validare è necessario attivare l'opzione *Accetta MTOM*. Tale opzione normalizza i messaggi prima di effettuarne la validazione e ripristina il formato originale una volta completato il processo di validazione.

Nota
Si tenga presente che attivando la validazione dei messaggi, questa riguarderà sia le richieste, inviate al servizio, che le conseguenti risposte.

2.4.5 Rate Limiting

Questa sezione di configurazione, specifica per erogazioni e fruizioni (o specifico gruppo di configurazione nell'ambito di un'erogazione/fruizione), consente di attivare delle policy di rate limiting specifiche per l'istanza configurata.

L'attivazione di policy di rate limiting rientra nell'ambito degli strumenti per il controllo del traffico. La descrizione di dettaglio di questi strumenti è presente nella Sezione 7.3, dove viene illustrato il meccanismo per configurare le policy e più in dettaglio nella Sezione 7.3.3.2 riguardo l'attivazione di policy a valenza globale.

Sono presenti alcune policy di rate limiting preconfigurate e pronte all'uso. L'utente può crearne di nuove seguendo le indicazioni presenti nella Sezione 7.3. Le policy preconfigurate sono le seguenti:

- *NumeroRichieste-ControlloRealtimeGiornaliero*: La policy confronta il numero di richieste, sulla finestra giornaliera corrente, della specifica istanza di servizio, con la soglia stabilita.
- *NumeroRichieste-ControlloRealtimeMinuti*: La policy confronta il numero di richieste, sulla finestra del minuto corrente, della specifica istanza di servizio, con la soglia stabilita.
- *NumeroRichieste-ControlloRealtimeOrario*: La policy confronta il numero di richieste, sulla finestra oraria corrente, della specifica istanza di servizio, con la soglia stabilita.
- *NumeroRichieste-RichiesteSimultanee*: La policy confronta il numero di richieste simultaneamente attive della specifica istanza di servizio, con la soglia stabilita.
- *OccupazioneBanda-ControlloRealtimeOrario*: La policy confronta l'occupazione di banda della specifica istanza di servizio, sulla finestra oraria corrente, con la soglia stabilita.
- *TempoMedioRisposta-ControlloRealtimeOrario*: La policy confronta il tempo medio di risposta della specifica istanza di servizio, sulla finestra oraria corrente, con la soglia stabilita.

Per attivare una nuova policy dalla sezione di rate limiting si procede utilizzando il pulsante *Aggiungi* che apre il form di Figura 24.

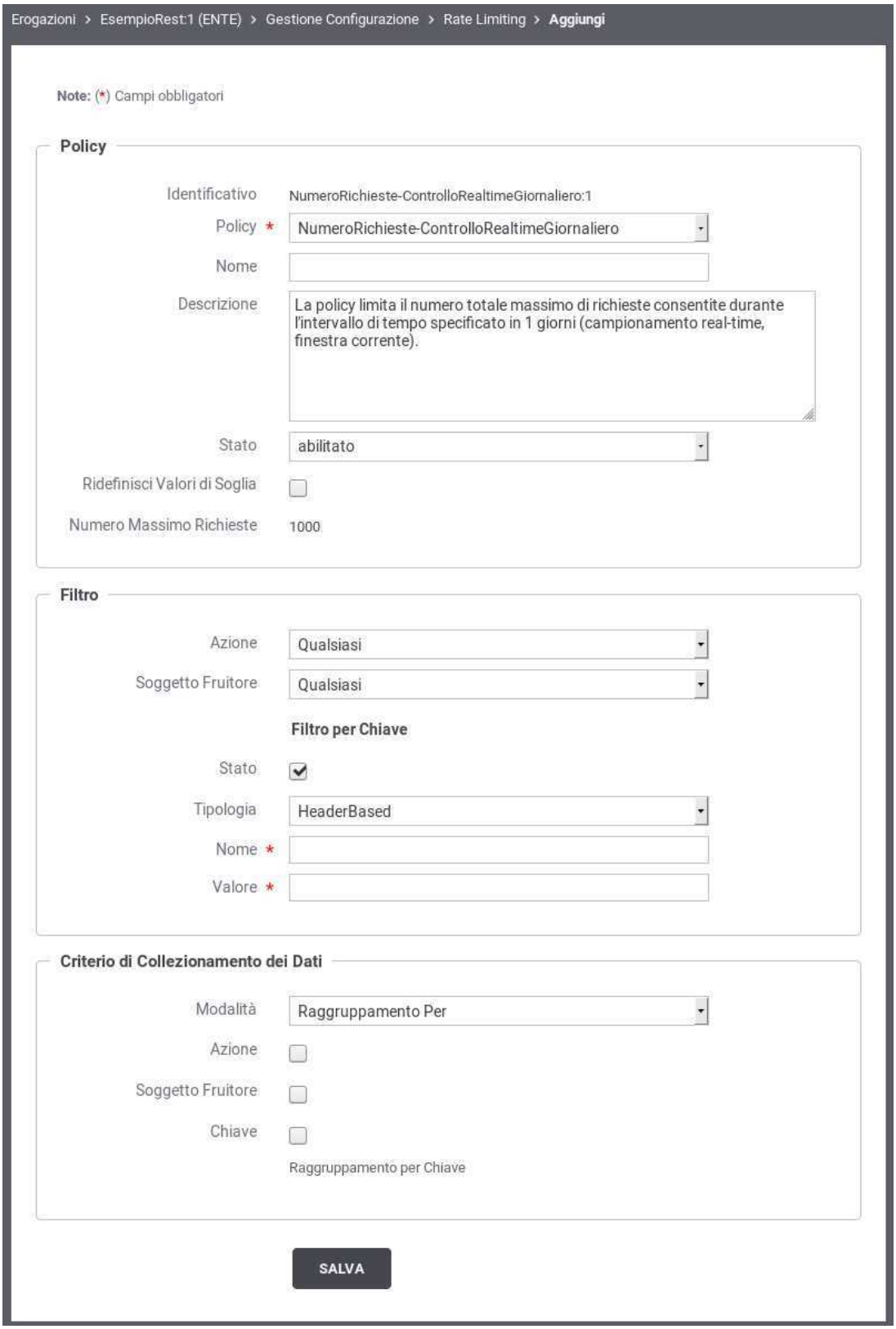


Figura 24: Attivazione di una policy di Rate Limiting

Si compilano i campi seguenti:

- *Policy*: la policy da attivare. Si compone di:
  - *Identificativo*: Identificativo univoco assegnato automaticamente all'istanza di policy.
  - *Policy*: L'elemento del registro delle policy che si vuole attivare. Inizialmente saranno presenti solo le policy preconfigurate. Eventualmente saranno presenti in seguito le policy definite dall'utente
  - *Nome*: Opzionale. Permette di identificare l'istanza della policy tramite un nome alternativo all'identificativo assegnato automaticamente dal sistema.
  - *Descrizione*: Il testo di descrizione della policy.
  - *Stato*: Lo stato dell'istanza di policy una volta creata. Sono disponibili le seguenti opzioni:
    - *Abilitato*: L'istanza di policy è abilitata. Questo significa che le violazioni rilevate saranno gestite in maniera restrittiva (negazione del servizio).
    - *WarningOnly*: L'istanza di policy è abilitata in modalità WarningOnly. Questo significa che le violazioni rilevate saranno solo segnalate tramite messaggi diagnostici ma non ci saranno ripercussioni sull'elaborazione della richiesta.
    - *Disabilitato*: L'istanza di policy è disabilitata.
  - *Ridefinisci Valori di Soglia*: Attivando questa opzione sarà possibile utilizzare una soglia per l'istanza di policy differente rispetto al valore di default previsto dalla policy d'origine.
- *Filtro*: Abilitando questa sezione dell'istanza di policy è possibile indicare i criteri per stabilire quali richieste, nell'ambito della istanza in fase di configurazione, sono soggette alla policy che si sta istanziando. In assenza di filtro, l'istanza della policy sarà valutata su tutte le richieste in ingresso per la specifica istanza di servizio che si sta configurando.

  Per la creazione del filtro sono disponibili i seguenti campi:
  - *Azione*: Opzione per filtrare le richieste in base all'azione invocata.
  - *Soggetto Fruitore*: Opzione disponibile per le erogazioni al fine di filtrare le richieste di servizio in base al soggetto fruitore.
  - *Applicativo Fruitore*: Opzione disponibile per le fruizioni al fine di filtrare le richieste di servizio in base all'applicativo fruitore
  - *Filtro per Chiave*: Si tratta di un'opzione avanzata che consente di filtrare le richieste in ingresso sul gateway base ad una chiave che può essere specificata in maniera personalizzata effettuando una delle seguenti scelte per il campo *Tipologia*:
    - *HeaderBased*: Occorre fornire i dati "Nome" e "Valore". La policy si applicherà soltanto alle richieste che hanno, nell'header di trasporto, una proprietà che corrisponde.
    - *URLBased*: Occorre fornire i dati "Espressione Regolare" e "Valore". La policy si applicherà soltanto alle richieste ove, applicando l'espressione regolare alla URL di invocazione, si ottiene un valore identico a quello fornito.
    - *FormBased*: Occorre fornire i dati "Nome" e "Valore". La policy si applicherà soltanto alle richieste che contengono nella query string un parametro corrispondente ai dati forniti.
    - *SOAPActionBased*: Occorre fornire il dato "Valore". + La policy si applicherà soltanto alle richieste che si presentano con una SOAPAction avente il valore fornito.
    - *ContentBased*: Occorre fornire i dati "Espressione XPath" e "Valore". La policy si applicherà soltanto alle richieste dove, applicando l'espressione XPath al messaggio di richiesta, si ottiene un valore identico a quello fornito.
    - *PluginBased*: Occorre fonire i dati "Tipo Personalizzato" e "Valore". Il parametro "Tipo Personalizzato" è una chiave, registrata nella configurazione, cui corrisponde una classe java che restituisce un valore da confrontare con quello fornito. Per realizzare un plugin con una logica di filtro personalizzata è necessario fornire un'implementazione della seguente interfaccia:

      ```
      package org.openspcoop2.pdd.core.controllo_traffico.plugins;
      public interface IRateLimiting {
        public String estraiValoreFiltro(Logger log,Dati datiRichiesta) throws ↩
            PluginsException;
        public String estraiValoreCollezionamentoDati(Logger log,Dati datiRichiesta) throws ↩
            PluginsException;
      }
      ```

      La classe realizzata viene successivamente registrata tramite una entry nel file *className.properties* di GovWay:

```
org.openspcoop2.pdd.controlloTraffico.rateLimiting.test=<fully qualified class name>
```

La stringa <nome>, fornita in configurazione, diventa utilizzabile come “Tipo Personalizzato”.

- *Criterio di Collezionamento dei Dati*: In questa sezione è possibile attivare opzionalmente alcuni criteri per il raggruppamento dei dati utilizzati come indicatori di confronto per l’applicabilità della policy. Ad esempio se si è attivata una policy che limita a 20 il numero di richieste su una finestra di 5 minuti, significa che al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, si otterrà una violazione della policy.

  Aggiungendo un criterio di collezionamento per Azione, saranno conteggiate separatamente le richieste in base alla specifica azione invocata. In questo caso la policy risulterà violata solo al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, relativa alla medesima azione.

  È ammesso anche il raggruppamento su criteri multipli. La logica è del tutto analoga a quella dell’operatore GROUP BY del linguaggio SQL.

  I criteri di raggruppamento selezionabili sono:

  – *Azione*
  – *Soggetto Fruitore* (caso erogazioni)
  – *Applicativo Fruitore* (caso fruizioni)
  – *Raggruppamento per Chiave*: le richieste saranno raggruppate in base al valore di una chiave personalizzata il cui valore viene fornito secondo uno dei metodi selezionati tra i seguenti:
    * *HeaderBased*: La chiave è presente nell’header di trasporto indicato nella proprietà "Nome".
    * *URLBased*: La chiave è presente nella URL ricavandola tramite l’espressione regolare fornita nell’elemento seguente.
    * *FormBased*: La chiave viene fornita in modalità Form Encoded con il parametro indicato nell’elemento "Nome".
    * *SOAPActionBased*: La chiave corrisponde al valore della SoapAction.
    * *ContentBased*: La chiave è presente nel body del messaggio e viene ricavata tramite il valore Xpath fornito nell’elemento seguente.
    * *PluginBased*: La chiave viene restituita tramite l’esecuzione di una classe il cui nome viene fornito con il campo "Tipo Personalizzato"

2.4.6 Sicurezza a livello del messaggio

Tramite il collegamento *Sicurezza Messaggio*, presente nella sezione di configurazione della specifica erogazione/fruizione, è possibile impostare criteri di elaborazione dei messaggi in transito, attuati dal gateway, al fine di gestire i meccanismi di sicurezza previsti a livello del messaggio.

Il form presenta inizialmente lo *Stato* disabilitato. Per abilitare la sicurezza, impostare il valore dello stato su abilitato e confermare con il pulsante *Invia*. Appariranno gli elementi *Richiesta* e *Risposta*, come nella figura seguente.

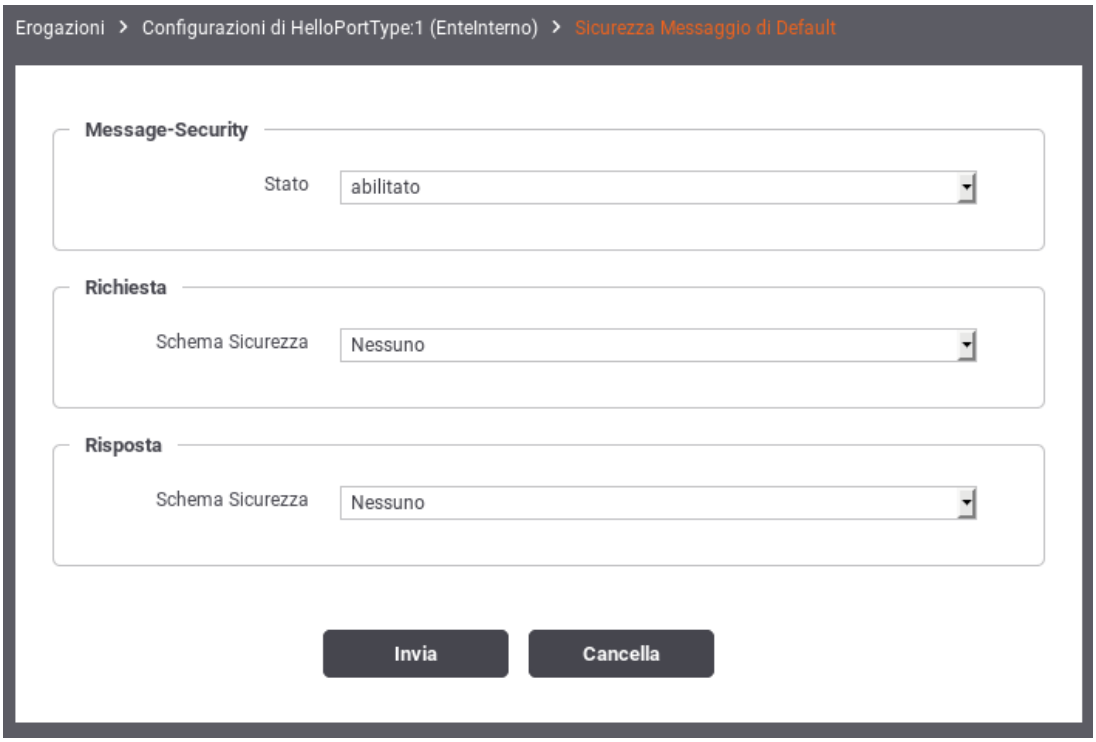


Figura 25: Abilitazione Sicurezza Messaggio

Il form consente di selezionare uno schema di sicurezza, tra quelli disponibili, da applicare al messaggio di richiesta ed a quello di risposta. Gli schemi di sicurezza applicabili cambiano in base alla tipologia del messaggio sul quale si applica.

Per la gestione della sicurezza sul messaggio di richiesta, nel caso di una erogazione, il gateway agisce con il ruolo *Receiver* che comporta la seguente casistica:

- *Nel caso del protocollo SOAP*:
  - *WSSec Signature*, in ricezione si attende un messaggio firmato; l'azione è quella di verificare la firma presente
  - *WSSec Decrypt*, il messaggio ricevuto verrà decifrato
  - *WSSec SAML Token*, si attende un messaggio contenente una asserzione SAML; viene effettuata la verifica dell'asserzione presente.
  - *WSSec Username Token*, viene effettuata la validazione del token di autenticazione
  - *WSSec Timestamp*, se è prevista una scadenza all'interno del timestamp presente nel messaggio, se ne verificherà la validità
- *Nel caso del protocollo REST*
  - *JWT Decrypt*: il messaggio JSON ricevuto viene decifrato.
  - *JWT Verifier Signature*: al messaggio JSON ricevuto viene verificata la firma.
  - *XML Decrypt*: il messaggio XML ricevuto viene decifrato.
  - *XML Verifier Signature*: al messaggio XML ricevuto viene verificata la firma.

Per la gestione della sicurezza sul messaggio di risposta, nel caso di una erogazione, il gateway agisce con il ruolo *Sender* che comporta la seguente casistica:

- *Nel caso del protocollo SOAP*:
  - *WSSec Signature*, il messaggio verrà firmato

  - *WSSec Encrypt*, il messaggio verrà cifrato
  - *WSSec SAML Token*, sul messaggio verrà inserita una asserzione SAML
  - *WSSec Username Token*, il messaggio verrà arrichito di un token di autenticazione
  - *WSSec Timestamp*, il messaggio verrà arrichito di una informazione temporale (tipicamente utilizzato insieme alla firma del messaggio)
- *Nel caso del protocollo REST*:
  - *JWT Encrypt*: il messaggio JSON di risposta viene cifrato prima dell'invio.
  - *JWT Signature*: il messaggio JSON di risposta viene firmato prima dell'invio.
  - *XML Encrypt*: il messaggio XML di risposta viene cifrato prima dell'invio.
  - *XML Signature*: il messaggio XML di risposta viene firmato prima dell'invio.

Nota

Si tenga presente che, nel caso di una fruizione, il ruolo del gateway si inverte diventando *Sender* nel caso della richiesta e *Receiver* nel caso della risposta. Gli schemi di sicurezza disponibili, nel caso della fruizione, rimangono quelli già descritti per Sender e Receiver.

2.4.7 Tracciamento

Il tracciamento è la funzionalità del gateway che comporta la registrazione dei dati relativi alle comunicazioni in transito riguardanti i servizi erogati e fruiti. Nella logica del gateway, tutte le informazioni che riguardano una singola interlocuzione, a partire dalla richiesta pervenuta fino alla conclusione con l'invio dell'eventuale risposta, sono riconducibili ad un'unica entità denominata *Transazione*.

Una transazione registrata dal gateway ha la seguente struttura:

- *Dati di Identificazione Generale*. Sono le informazioni che identificano la comunicazione specifica in termini dei soggetti coinvolti e del servizio richiesto: Soggetto Erogatore, Soggetto Fruitore, Servizio, Azione, Esito, ...
- *Dati della Richiesta*. Sono le informazioni di dettaglio relative alla richiesta: Identificativo del Messaggio, Timestamp di ingresso, Timestamp di uscita, dimensioni del messaggio, ...
- *Dati della Risposta*. Sono le medesime informazioni già citate al punto precedente, ma relative alla comunicazione di risposta.
- *Traccia Richiesta*. La traccia emessa dal gateway con i dettagli relativi alla richiesta.
- *Traccia Risposta*. La traccia emessa dal gateway con i dettagli relativi alla risposta.
- *Messaggi Diagnostici*. La sequenza dei messaggi diagnostici, ordinati cronlogicamente, emessi dal gateway nel corso dell'elaborazione dell'intera transazione.
- *Fault di Ingresso*. Viene registrato come Fault di Ingresso l'eventuale messaggio di errore ricevuto dal gateway durante l'invocazione di un servizio (interno o esterno al dominio gestito).
- *Fault di Uscita*. Viene registrato come Fault di Uscita l'eventuale messaggio di errore inoltrato dal gateway al mittente della richiesta (interno o esterno al dominio gestito), dopo aver ricevuto un fault dal servizio invocato.
- *Parametri e Misurazioni*. Sono i parametri e le misurazioni che riguardano la transazione, come ad esempio: l'identificativo della transazione, le url invocate, i tempi di latenza, ...

In questa sezione è possibile personalizzare la configurazione di default del tracciamento definita in accordo a quanto descritto in Sezione 7.2. Le personalizzazioni inserite in questo contesto avranno validità per le sole comunicazioni riguardanti la specifica erogazione/fruizione (Figura 26).

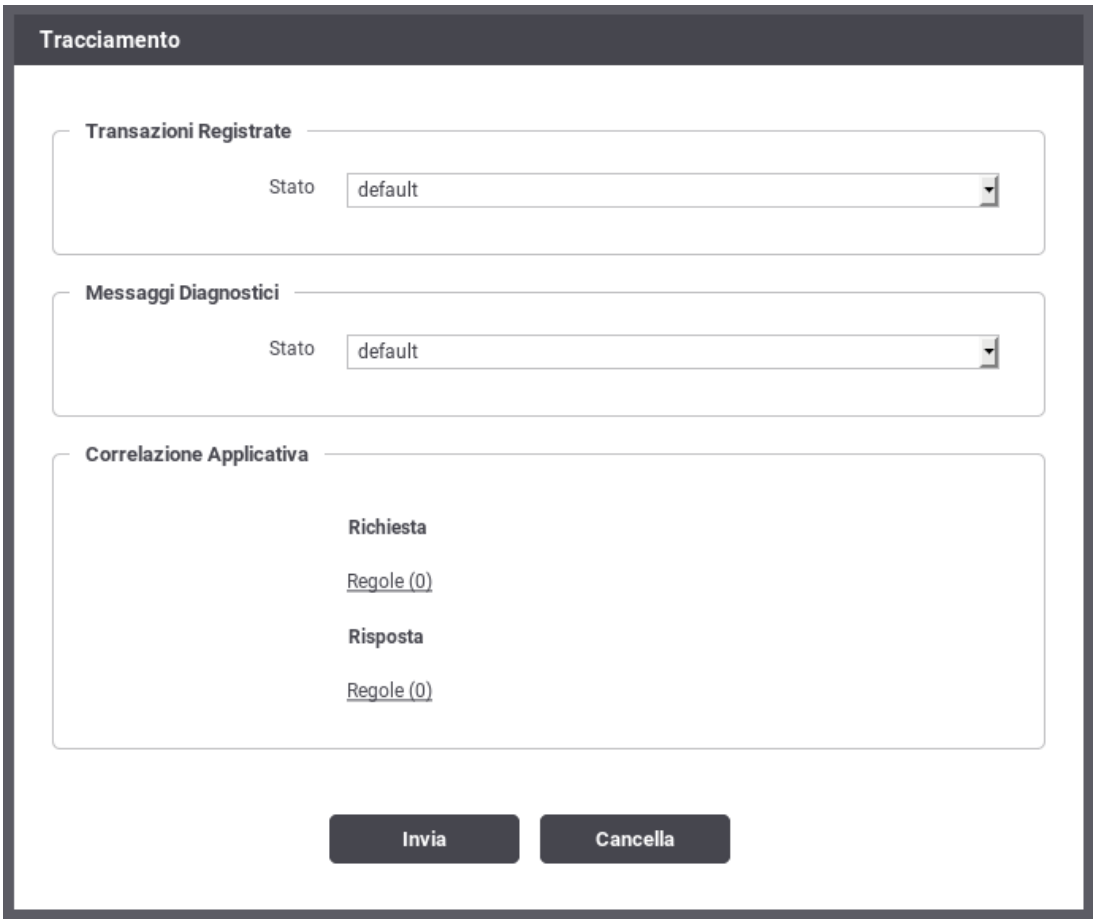


Figura 26: Tracciamento per la singola erogazione/fruizione

Le sezioni presenti nella pagina sono:

- *Transazioni Registrate*: l'utente ha l'opzione per mantenere il default definito nella sezione di configurazione generale (Sezione 7.2) oppure ridefinirlo.
- *Messaggi Diagnostici*: l'utente ha l'opzione per mantenere il default definito nella sezione di configurazione generale (Sezione 7.2) oppure ridefinire il criterio per la sola memorizzazione su Database.
- *Correlazione Applicativa*: consente di impostare delle regole per estrarre dai messaggi in transito, codici, riferimenti, o altri contenuti al fine di arricchire i dati tracciamento generati dal gateway (Sezione 2.4.7.1).

2.4.7.1 Correlazione Applicativa

La funzione di *Correlazione Applicativa* consente al gateway che elabora il messaggio di richiesta, di estrarre un identificatore relativo al contenuto applicativo. L'identificatore, se presente, finisce nei sistemi di tracciamento e diagnostici, a completamento delle informazioni già presenti. I dati per configurare la correlazione applicativa consistono in un insieme di regole per l'estrazione di tale identificatore (vedi Figura 27.

Per accedere alla configurazione della correlazione applicativa, per una data erogazione/fruizione, si utilizza il collegamento presente nella colonna *Correlazione Applicativa* in corrispondenza di una configurazione relativa all'erogazione/fruizione scelta. Si giunge alla pagina mostrata in Figura 27.

Figura 27: Regole di correlazione applicativa

Utilizzando il collegamento *Regole*, presente nel riquadro della Richiesta o Risposta, si accede all'elenco delle regole di correlazione applicativa presenti. Premere il pulsante *Aggiungi* per aggiungere una nuova regola (Figura 28)

Figura 28: Creazione di una regola di correlazione applicativa

Per la creazione di una regola di correlazione applicativa si devono indicare i seguenti dati:

- *Elemento*: Questo dato serve per capire su quali messaggi è applicabile la regola di correlazione applicativa che si sta definendo. Lasciando il campo vuoto si intende che la regola si applica a tutti i messaggi. In alternativa è possibile indicare:
  - *Nome Azione o Risorsa*: il nome esatto dell'azione o della risorsa su cui verrà applicativa la regola
  - *LocalName dell'elemento xml*: in caso il messaggio sia un xml (soap o rest), è possibile indicare il local name del root element xml su cui verrà applicativa la regola
  - *XPath o JSONPath*: Espressione che può rappresentare un XPath o JSONPath. Se l'espressione ha un match con il contenuto la regola verrà applicata
- *Modalità Identificazione*: rappresenta la modalità di acquisizione dell'identificatore applicativo. Può assumere i seguenti valori:

  - *urlBased*: il valore viene preso dalla url utilizzata dal servizio applicativo per l'invocazione. La regola per l'estrazione dalla url viene specificata tramite un'espressione regolare inserita nel campo pattern.
  - *contentBased*: Il valore viene estratto direttamente dal messaggio applicativo. La regola per l'estrazione dal messaggio è specificata tramite un'espressione XPath o JSONPath inserita nel campo pattern;
  - *headerBased*: Il valore viene estratto dall'header di trasporto avente il nome indicato nel campo successivo.
  - *inputBased*: il valore viene estratto dall'header di integrazione GovWay e presente nel valore della proprietà *IDApplicativo*.
  - *disabilitato*: l'identificatore applicativo non viene estratto. Questa opzione è utile quando si vuole disabilitare l'estrazione dell'id applicativo solo per specifici messaggi;
- *Pattern*: definisce l'espressione regolare, nel caso di identificazione urlBased, o l'espressione XPath/JSONPath, nel caso di identificazione contentBased, utilizzata per l'acquisizione dell'identificatore applicativo.
- *Identificazione Fallita*: azione da intraprendere nel caso fallisca l'estrazione dell'identificatore applicativo tramite la regola specificata. Nel caso sia stato indicato *blocca*, tali richieste non verranno accettate con restituzione di un errore al mittente;
- *Riuso ID*: opzione per abilitare/disabilitare il riuso dell'identificatore del messaggio (assegnato dal gateway) nel caso in cui vengano inviati messaggi con identificatori applicativi già processati in precedenza.

2.4.8 MTOM

Nei casi in cui il mittente e il destinatario si scambiano messaggi con allegati (nell'ambito del protocollo SOAP), utilizzando il protocollo MTOM, GovWay è in grado di gestire tali comunicazioni in modalità trasparente e quindi senza alcun intervento.

In altre situazioni è possibile sfruttare le funzionalità di GovWay per beneficiare delle ottimizzazioni del protocollo MTOM quando uno dei due interlocutori non è in grado di supportare tale protocollo, oppure per effettuare verifiche di congruità dei messaggi in transito basati su MTOM.

Nel caso di una erogazione, per il messaggio di richiesta, le opzioni disponibili sono:

- *disable*. Non viene svolta alcuna azione.
- *unpackaging*. In questo scenario il client fruitore invia dati binari nel formato MTOM ma l'erogatore non supporta tale formato. Il gateway effettua la trasformazione del messaggio inserendo i dati binari in modalità *Base64 encoded* prima che venga inviato al destinatario. Sulla risposta sarà effettuato il processo inverso.
- *verify*. Sia il fruitore che l'erogatore utilizzano MTOM ma si vogliono validare i messaggi. Il gateway effettua, tramite opportuni pattern xpath forniti, la validazione dei messaggi al fine di verificare la conformità del formato del messaggio rispetto a quanto atteso dall'erogatore.

Sempre nel caso di una erogazione, per il messaggio di risposta, le opzioni disponibili sono:

- *disable*. Non viene svolta alcuna azione.
- *packaging*. In questo scenario il client fruitore invia dati binari nella modalità Base64 encoded ma l'erogatore richiede il formato MTOM. Il gateway effettua la trasformazione del messaggio secondo il protocollo MTOM prima che venga inviato al destinatario. Sulla risposta sarà effettuato il processo inverso.
- *verify*. Analogo a quanto descritto per il messaggio di richiesta.

Nota: Nel caso si utilizzi la validazione dei contenuti, basata su xsd o wsdl, è possibile che la struttura MTOM non sia stata prevista negli schemi e quindi faccia fallire l'esito della stessa. In questo caso, quando si attiva la validazione è necessario abilitare l'opzione *Accetta MTOM/XOP-Message* affinché il processo di validazione tenga conto del formato MTOM.

Nota

Nel caso di una fruizione, le opzioni di configurazione disponibili per la richiesta diventano quelle per la risposta e viceversa.

2.4.9 Registrazione Messaggi

Nella Sezione 7.2 è possibile fornire le configurazioni per attivare il salvataggio dei messaggi in transito sul gateway. In questa sezione si ha la possibilità di ridefinire le opzioni di configurazione, stabilite a livello generale, al fine di personalizzare il servizio di registrazione dei messaggi per la specifica configurazione dell'erogazione/fruizione.

Per la descrizione delle opzioni di configurazione si faccia riferimento alla sezione generale precedentemente indicata.

3 Il Profilo "eDelivery"

In questa modalità operativa la govwayConsole consente di produrre configurazioni di scenari di interoperabilità che si basano sullo standard europeo eDelivery. Per rendere il trattamento dei messaggi conforme a tale standard, GovWay si interfaccia ad una installazione del software Domibus (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus).

Il processo di configurazione rimane strutturalmente analogo a quanto già descritto per la modalità API Gateway. Sono però presenti proprietà specifiche del contesto eDelivery i cui valori devono essere foriniti affinché il dialogo con l'access point Domibus possa essere realizzato correttamente.

Nel seguito andiamo a descrivere i passi di configurazione evidenziando, per differenza con il caso API Gateway, gli elementi di eDelivery che dovranno essere gestiti. Al termine della configurazione è necessario procedere con l'export dei dati in formato *PMODE*. Il file prodotto è quello necessario per permettere la configurazione dell'access point Domibus.

3.1 Passi preliminari di configurazione

Per gestire in maniera più semplice i passi di configurazione dei servizi eDelivery è consigliabile impostare l'opportuna modalità operativa della govwayConsole selezionando la voce *eDelivery* sul selettore di modalità presente nella testata dell'applicazione.

Prima di procedere con la configurazione dei servizi si devono verificare i dati relativi ai soggetti interlocutori. Nel caso del soggetto interno al proprio dominio, i dati di configurazione possono essere gestiti alla sezione *Configurazione* > *Generale* (Figura 29).

Figura 29: Configurazione delle Base URL eDelivery per il soggetto interno

Sono presenti valori iniziali, inseriti dal processo di installazione, che devono essere verificati ed eventualmente aggiornati:

- *Base URL Erogazione*: Indirizzo pubblico del Domibus per la ricezione dei messaggi sul canale eDelivery.
- *Base URL Fruizione*: Indirizzo del servizio di GovWay riservato ai client per l'invio di messaggi sul canale eDelivery.

Tramite il collegamento *Visualizza Dati Soggetto* è possibile accedere alla conffigurazione del soggetto interno (Figura 30).

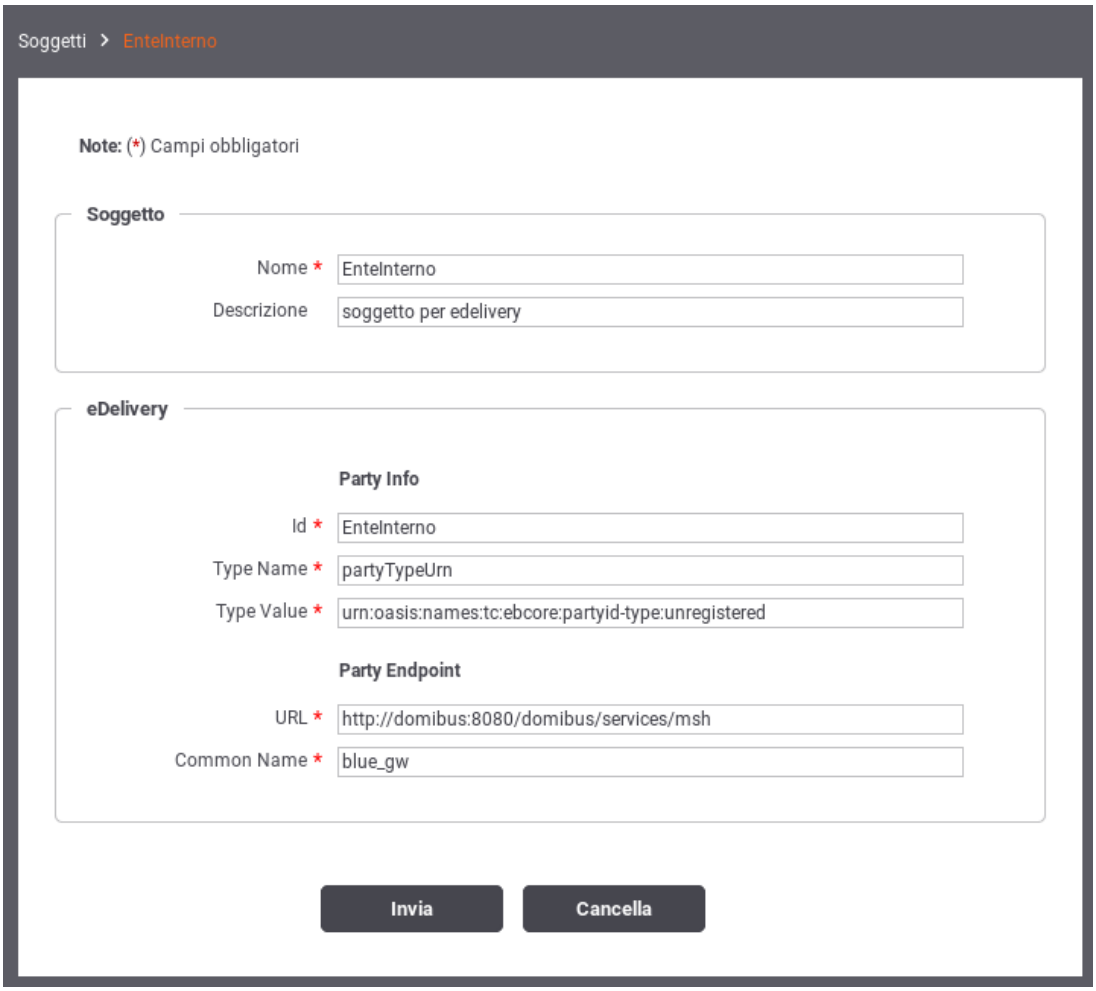


Figura 30: Configurazione delle proprietà eDelivery per il soggetto interno

Le proprietà eDelivery da fornire sono le seguenti:

- *Party Info - Id*: Identificativo del soggetto utilizzato nel canale eDelivery.
- *Party Info - Type Name*: Nome assegnato internamente allo schema indicato nel Type Value.
- *Party Info - Type Value*: Schema di generazione riferito all'identificativo del soggetto eDelivery.
- *Party Endpoint - URL*: Indirizzo pubblico del Domibus per la ricezione dei messaggi sul canale eDelivery.
- *Party Endpoint - Common Name*: Valore della omonima proprietà del certificato utilizzato dall'access point Domibus cui afferisce. Questo nome coincide con quello dell'access point.

3.2 Erogazione di servizi in modalità eDelivery

Configurare un'erogazione eDelivery permette ad un'applicazione interna di ricevere i messaggi inviati da un generico access point eDelivery esterno.

Il primo passo di configurazione prevede che venga censito il soggetto esterno mittente dei messaggi. La creazione di tale soggetto si realizza dalla sezione *Registro* > *Soggetti* della govwayConsole, impostando le proprietà eDelivery già descritte nella sezione precedente per il soggetto interno.

Il passo successivo è quello di registrare le API corrispondenti al servizio eDelivery alla sezione *Registro* > *API*. Le proprietà eDelivery, presenti nel form di creazione, sono quelle mostrate in Figura 31.

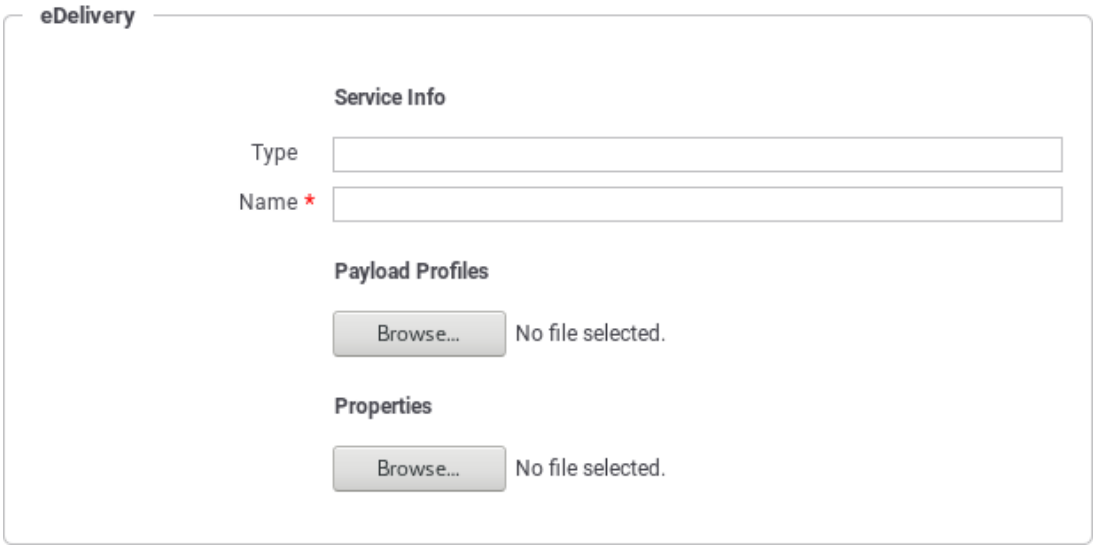


Figura 31: Registrazione API eDelivery - Proprietà specifiche

Le proprietà da specificare sono le seguenti:

- *Service Info - Type*: Identificativo assegnato come tipo del servizio (opzionale).
- *Service Info - Name*: Nome del servizio.
- *Payload Profiles - File*: Campo per l'upload del descrittore XML che rappresenta il formato dei messaggi inviati dal mittente. Campo opzionale, utilizzabile per aggiungere nuovi profili rispetto a quelli già presenti nell'installazione standard di Domibus. Per la specifica del formato XML da adottare si consulti la documentazione ufficiale di Domibus.
- *Properties - File*: Campo per l'upload del descrittore XML che definisce le proprietà custom che saranno presenti nei messaggi inviati dal mittente. Campo opzionale, utilizzabile per aggiungere nuove property rispetto a quelle già presenti nell'installazione standard di Domibus. Per la specifica del formato XML da adottare si consulti la documentazione ufficiale di Domibus.

Dopo aver effettuato il salvataggio è necessario completare la configurazione del servizio utilizzando il link presente nella colonna *Risorse* o *Servizi*, a seconda che si tratti di un servizio Rest o Soap, in corrispondenza dell'elemento presente nell'indice dei servizi. Per ciascuna delle azioni/risorse elencate per il servizio (o create, nel caso che, non disponendo del descrittore del servizio, si proceda con la configurazione manuale delle azioni), si accede al dettaglio per completare la configurazione delle proprerty eDelivery (Figura 32).

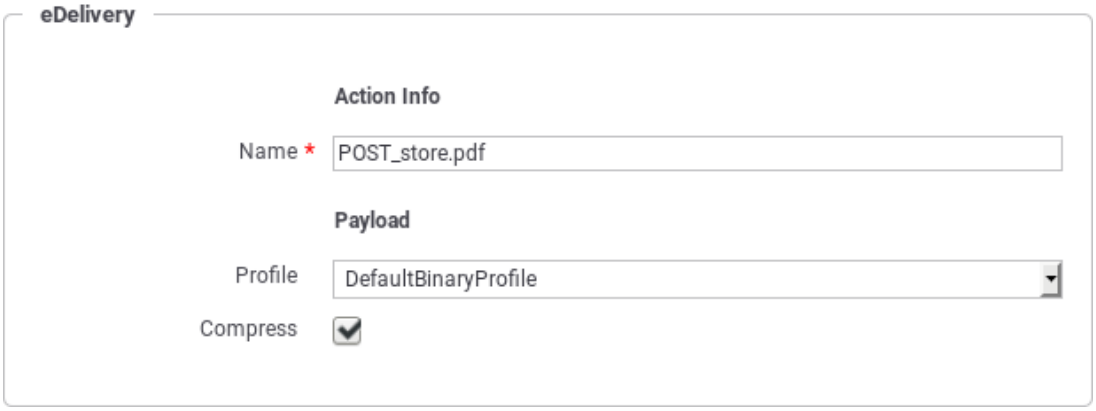


Figura 32: Proprietà eDelivery relative alle azioni delle API

I valori da impostare nel form sono:

- *Action Info - Name*: Nome dell'azione.
- *Payload - Profile*: Payload Profile, tra quelli disponibili, da utilizzare per l'azione.
- *Payload - Compress*: Indicare se l'invio del messaggio farà uso di compressione dei dati.

Dopo aver creato l'API si procede con la configurazione dell'erogazione alla sezione *Registro* > *Erogazioni* della govwayConsole (Figura 33).

Figura 33: Proprietà eDelivery relative all'erogazione del servizio

L'unica impostazione eDelivery da fornire in questo contesto è:

- *Security Profile*: profilo di sicurezza adottato dagli access point durante la comunicazione. E' necessario scegliere tra i valori presenti, che corrispondono alle policy standard, già presenti in Domibus con l'installazione.

Nota
L'endpoint fornito alla voce Connettore sarà quello utilizzato da GovWay per la consegna dei messaggi consegnati all'access point Domibus interno.

Nota
Affinché le configurazioni apportate in modalità eDelivery possano essere attuate sull'access point Domibus è necessario procedere alla generazione del PMODE nel modo descritto alla Sezione 3.4

3.3 Fruizione di servizi in modalità eDelivery

Configurare una fruizione eDelivery permette ad un'applicazione interna di inviare messaggi da veicolare verso un generico access point eDelivery esterno.

Il processo di configurazione della fruizione eDelivery prevede inizialmente i medesimi passi già descritti per l'erogazione al paragrafo Sezione 3.2. Dovranno quindi essere configurati i dati eDelivery relativi ai soggetti interlocutori, interno ed esterno, dovranno inoltre essere censite le API relative al servizio da fruire.

Dopo aver censito le API si procede con la configurazione della fruizione creando un nuovo elemento nella sezione *Registro* > *Fruizioni* della govwayConsole. Analogamente al caso dell'erogazione si dovrà selezionare la security policy necessaria per gli scambi tra gli access point.

Nota
Affinché le configurazioni apportate in modalità eDelivery possano essere attuate sull'access point Domibus è necessario procedere alla generazione del PMODE nel modo descritto alla Sezione 3.4

3.4 Generazione del PMODE Domibus

Affinché il Domibus interno al proprio dominio sia in grado di recepire tutte le configurazioni prodotte nella modalità eDelivery, è necessario che gli venga fornito il relativo file PMODE, così come prevede la configurazione dell'access point eDelivery.

Dopo aver ultimato le configurazioni dei servizi eDelivery, tramite la govwayConsole, si procede all'esportazione del PMODE effettuando i seguenti passaggi (Figura 34):

- Selezionare la voce di menu *Configurazione* > *Esporta*.
- Selezionare la tipologia archivio *domibus-pmode*.
- Premere il pulsante Invia e salvare il file XML che viene restituito.
- Effettuare l'upload del file ottenuto sulla Domibus Console.

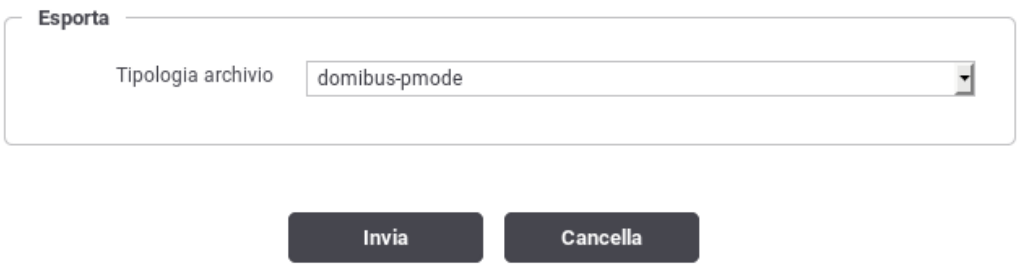


Figura 34: Esportazione del PMODE

4 Il Profilo "SPCoop"

In questa modalità operativa la govwayConsole consente di produrre le configurazioni per i servizi SPCoop, in accordo alla specifica di cooperazione applicativa della PA italiana. I passi di configurazione, per erogazioni e fruizioni, presentano minime differenze rispetto a quanto descritto per la modalità API Gateway. Nel seguito saranno descritte tali differenze.

4.1 Configurazione di un servizio SPCoop

Il primo passaggio per la configurazione di un servizio SPCoop è quello di creare il relativo Accordo di Servizio. Questi viene creato registrando una nuova API (sezione *Registro* > *API*). Come illustrato nelle figura seguente, la particolarità di questa configurazione, rispetto a quanto descritto in precedenza, risiede nella presenza del campo *Soggetto referente*, nel quale deve essere selezionato uno dei soggetti precedentemente registrati.

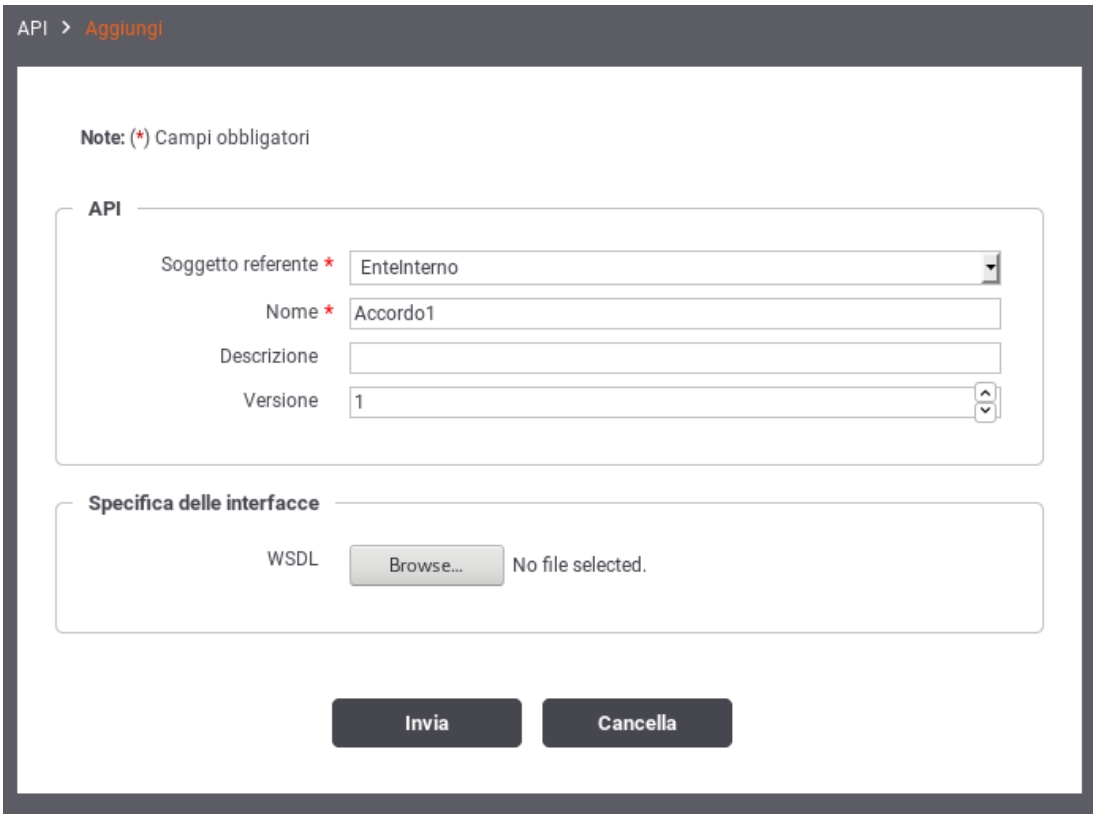


Figura 35: Creazione Accordo di Servizio SPCoop

Se non viene fornito un WSDL, relativo all'accordo di servizio, è necessario definire manualmente l'interfaccia del servizio, analogamente a quanto descritto in Sezione 8.1. In questo caso, l'aggiunta del servizio, comprende i profili di collaborazione asincroni oltre alle caratteristiche aggiuntive specifiche del protocollo SPCoop (vedi Sezione 4.4). La figura seguente mostra i dettagli di questo caso.

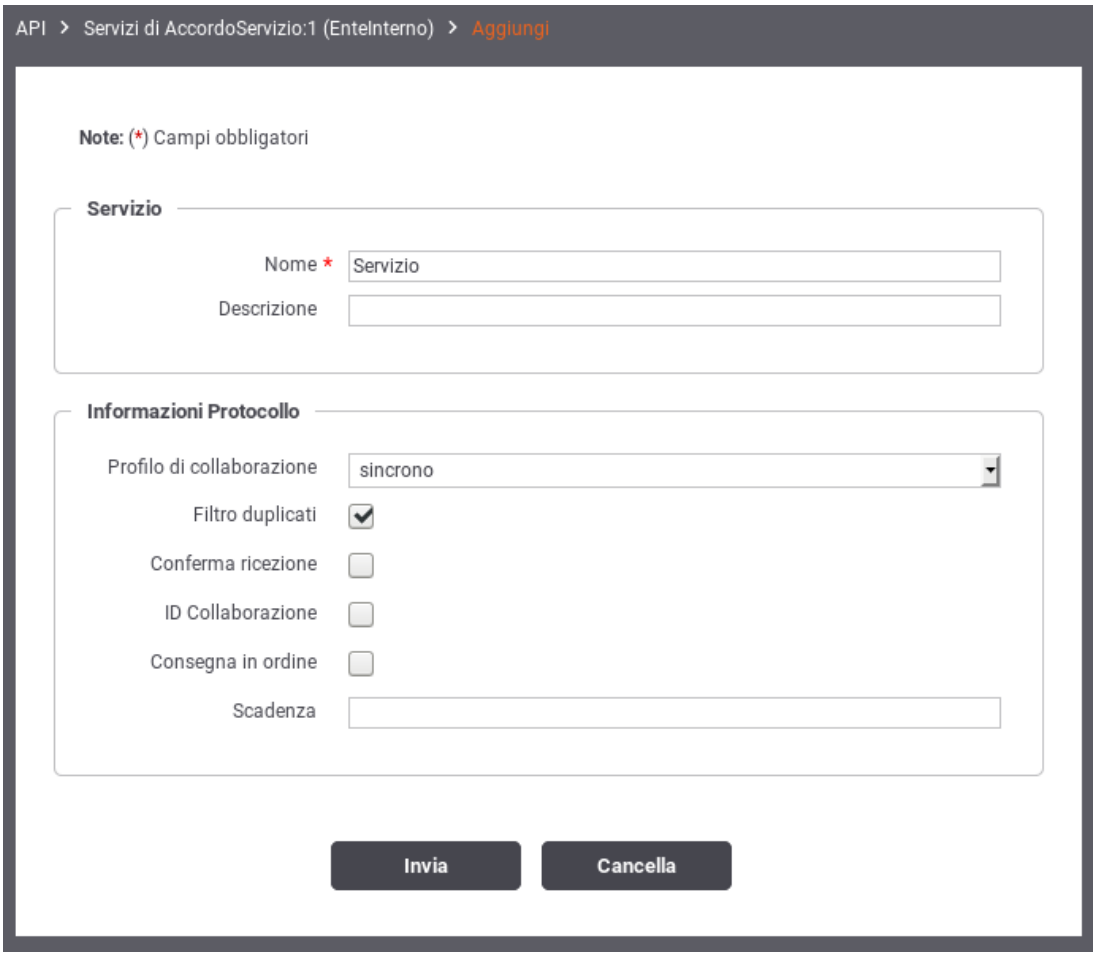


Figura 36: Aggiunta Servizio SPCoop

La registrazione di una nuova erogazione o fruizione, presenta le seguenti differenze rispetto a quanto descritto per la modalità API Gateway:

- È presente il campo *Tipo* relativamente al servizio
- È presente il campo *Versione Protocollo* per selezionare la versione della specifica SPCoop adottata.

Figura 37: Creazione erogazione SPCoop

4.2 Profili Asincroni

4.2.1 Profilo di Collaborazione Asincrono Simmetrico

La registrazione di un profilo asincrono simmetrico prevede che vengano correlati tra di loro due azioni di due servizi differenti presenti all'interno del solito accordo di servizio parte comune (API). Di seguito un esempio di tale configurazione.

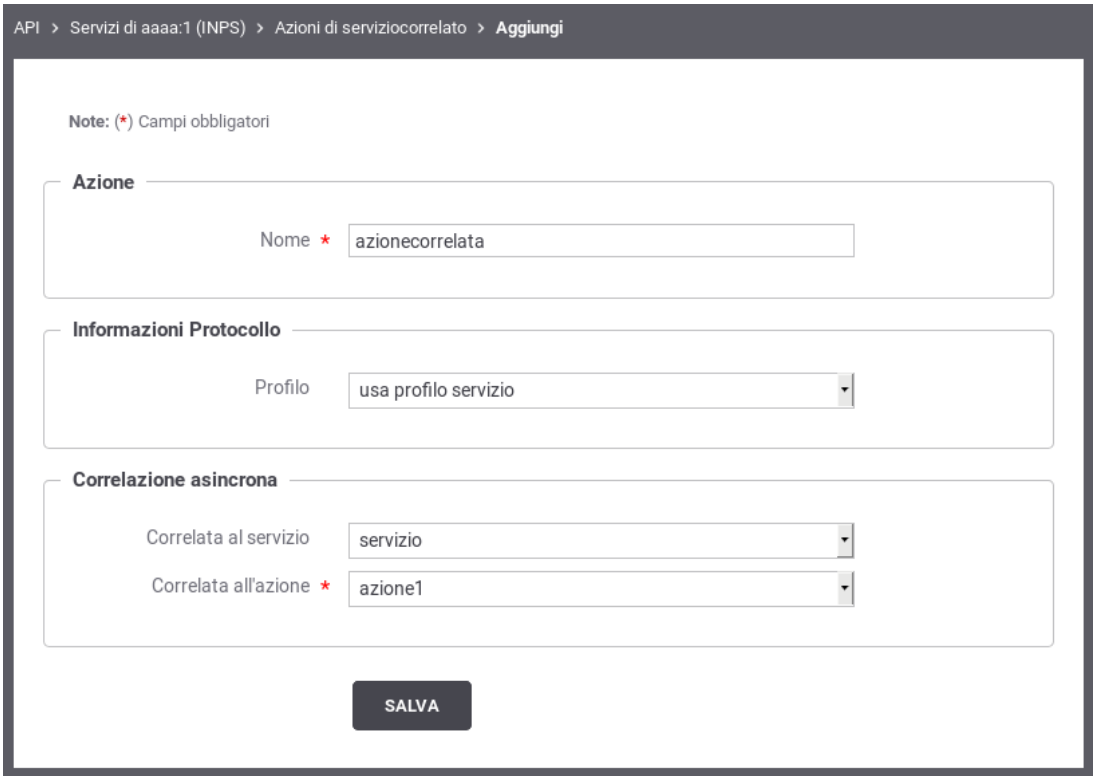


Figura 38: Correlazione Asincrona Simmetrica

4.2.1.1 Ruolo Fruitore

Per poter fruire di un servizio con il profilo asincrono simmetrico la registrazione dell'applicativo fruitore deve prevedere, oltre alle normali configurazioni, la definizione di un connettore attraverso il quale la PdD consegnerà la risposta asincrona. Per definire tale connettore utilizzare la sezione 'Risposta Asincrona' presente nell'elenco degli applicativi relativamente al servizio desiderato.

4.2.1.2 Ruolo Erogatore

Per poter erogare un servizio con il profilo asincrono simmetrico non sono richieste particolari configurazioni. Dovrà essere erogato il servizio relativo alla richiesta e fruito il servizio su cui inviare la risposta.

4.2.2 Profilo di Collaborazione Asincrono Asimmetrico

La registrazione di un profilo asincrono asimmetrico prevede che vengano correlati tra di loro due azioni, normalmente di uno stesso servizio, presenti all'interno dell'accordo di servizio parte comune (API). Di seguito un esempio di tale configurazione.

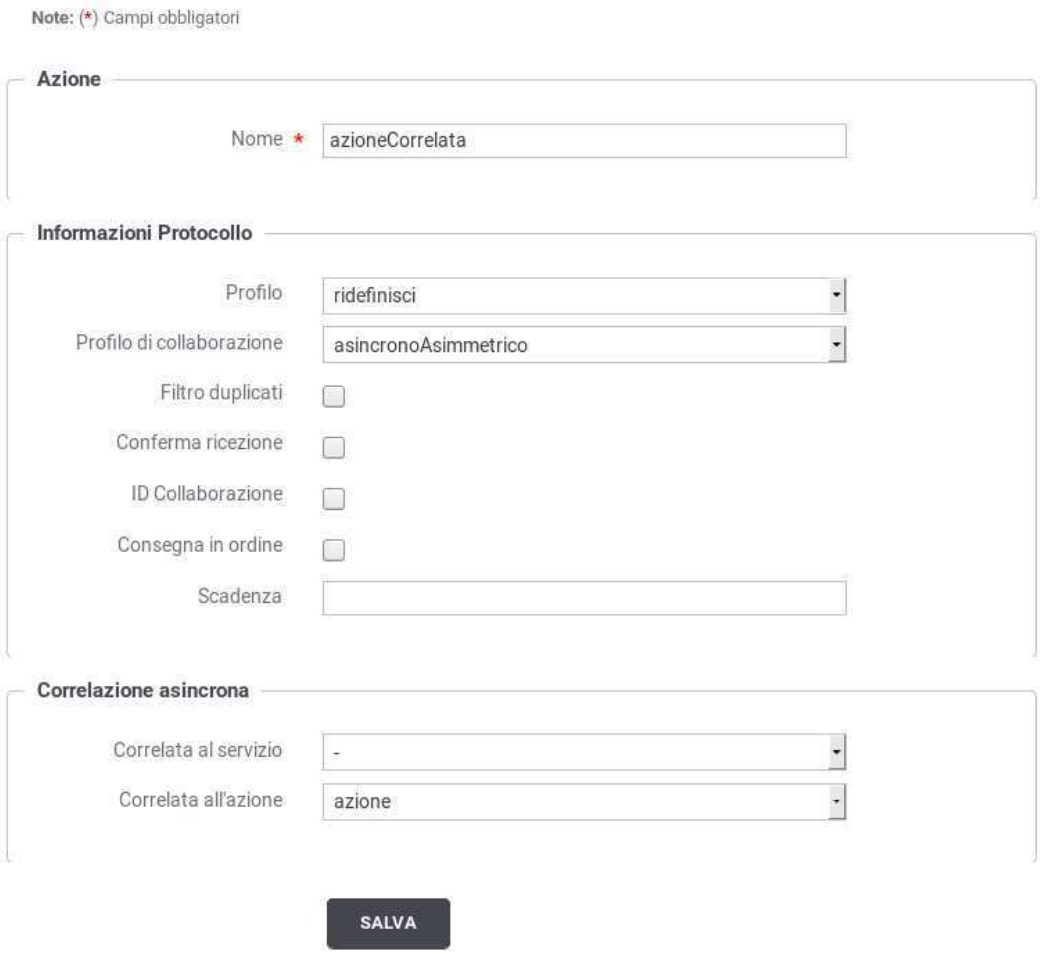


Figura 39: Correlazione Asincrona Asimmetrica

4.2.2.1 Ruolo Fruitore

Per poter fruire un servizio con il profilo asincrono asimmetrico non sono richieste particolari configurazioni. Dovrà essere fruito il servizio su cui inviare la richiesta e richiedere l'esito della risposta.

4.2.2.2 Ruolo Erogatore

Per poter erogare un servizio con il profilo asincrono asimmetrico la registrazione del servizio applicativo erogatore deve prevedere, oltre alle normali configurazioni, la definizione di un connettore attraverso il quale la PdD consegnerà il messaggio contenente la richiesta dello stato dell'operazione (seconda fase del profilo asincrono asimmetrico). Per definire tale connettore utilizzare la sezione 'Risposta Asincrona' presente nell'elenco dei servizi applicativi relativamente al servizio desiderato.

4.3 Interfacce WSDL (concettuale, logico ed implementativo)

La specifica SPCoop prevede che nell'accordo di servizio siano specificati i documenti WSDL del servizio applicativo erogatore e, nel caso di profili di collaborazione asincroni asimmetrici, anche quelli del servizio applicativo correlato erogato dal soggetto fruitore.

La Tabella 2 riepiloga i documenti necessari alla descrizione formale di un accordo di servizio che possono essere associati agli accordi parte comune e specifica se viene utilizzata la modalità avanzata della console

Nome Documento	**Accordo**
Specifica delle Interfacce	
WSDL Definitorio	Parte Comune
WSDL Concettuale	Parte Comune
WSDL Logico Erogatore	Parte Comune
WSDL Logico Fruitore	Parte Comune
Specifica delle Implementazioni	
WSDL Implementativo Erogatore	Parte Specifica
WSDL Implementativo Fruitore	Parte Specifica

Tabella 2: Descrizione di un accordo di servizio

4.4 Profili di gestione della busta eGov

L'interfaccia *completa* fornisce la possibilità di fruire/erogare di servizi SPCoop che non seguono le Linee Guida 1.1 ma si basano sul documento e-Gov 1.1. Questa funzionalità è utile sia per backward compatibility in quei domini dove i servizi non sono ancora stati adeguati al profilo descritto nelle Linee Guida 1.1, sia per usufruire di servizi infrastrutturali quali *consegna affidabile*, *consegna in ordine*, *conversazioni* che non sono presenti nel profilo Linee Guida 1.1.

Fruizione di un servizio Supponiamo di essere in un contesto dove vogliamo usufruire di un servizio erogato da un soggetto la cui PdD non è ancora stata adeguata a quanto descritto nelle Linee Guida 1.1. Per usufruire del servizio, il soggetto fruitore deve inviare buste conformi al profilo e-Gov 1.1, nonostante la propria porta di dominio sia già conforme alle Linee Guida 1.1. Per gestire tale contesto è possibile definire il soggetto erogatore con profilo *eGov1.1*. In un successivo momento, la PdD del soggetto erogatore può iniziare ad adeguarsi alle Linee Guida 1.1. Supponiamo che l'adeguamento sia incrementale, fornito per un servizio alla volta. Per usufruire dei servizi erogati da tale soggetto, con la giusta modalita (Linee Guida 1.1 o e-Gov 1.1) *è possibile ridefinire il profilo di gestione all'interno del servizio*.

Erogazione di un servizio Poniamoci in un contesto in cui la Porta di Dominio eroga dei servizi che rispettano quanto descritto nelle Linee Guida 1.1. In questo contesto, i soggetti di PdD che non si sono ancora adeguate alle linee guida, non potrebbero usufruire dei servizi. La PdD può essere configurata, in modo da erogare i servizi, per questi soggetti, secondo il profilo *eGov 1.1*. Questa configurazione richiede che al soggetto fruitore venga associato un profilo *eGov 1.1*. In un successivo momento, la PdD di un soggetto fruitore può iniziare ad adeguarsi alle Linee Guida 1.1. Si creano quindi due situazioni di transizione dove devono coesistere entrambe le specifiche:

- Un soggetto fruisce per alcuni servizi erogati secondo le specidiche e-Gov1.1, per altri secondo le Linee Guida 1.1
- Uno o più fruitori accedono al un servizio erogato secondo le specidiche e-Gov1.1, altri secondo le Linee Guida 1.1

In entrmabi i casi, per erogare il servizio con la giusta modalita (linee guida o e-gov 1.1) è *possibile ridefinire il profilo di gestione impostandolo nella lista dei fruitori del servizio*.

4.4.1 Profilo di gestione e-Gov 1.1

Il documento delle linee guida ha deprecato alcune opzioni al fine di snellire la specifica. Per mantenere la conpatibilità con la vecchia versione viene sempre offerta la possibilità di specificare tali opzioni all'interno degli accordi di servizio. Tali funzionalità vengono impostate/validate all'interno della busta e-Gov solo se il servizio viene fruito/erogato con profilo *eGov1.1*.

Nome	Default	Funzionalità
Filtro duplicati	true	Funzionalità di filtro delle buste duplicate (Imposta l'attributo inoltro del profilo di trasmissione al valore EGOV_IT_ALPIUUNAVOLTA).
Conferma Ricezione	false	Funzionalità di consegna affidabile delle buste spcoop attraverso l'utilizzo dei riscontri (Imposta l'attributo confermaRicezione del profilo di trasmissione al valore true).
ID Collaborazione	false	Aggiunge un elemento Collaborazione alla busta (Diverse istanze di cooperazione possono essere correlate in un'unica conversazione).
Consegna in ordine	false	Consegna in ordine delle buste (Richiede Filtro Duplicati e Conferma Ricezione)
Scadenza		Assegna una scadenza temporale alla busta SPCoop

Tabella 3: Funzionalita eGov 1.1

Di seguito un esempio di creazione di un accordo di servizio che richiede consegna affidabile tramite riscontri, filtro duplicati e id di collaborazione per un servizio sincrono.

Figura 40: Controlli avanzati sulle informazioni eGov relative all'accordo di servizio

5 Il Profilo "FatturaPA"

Il profilo "FatturaPA" consente di utilizzare GovWay come nodo di interconnessione al Sistema di Interscambio (SdI), responsabile della gestione dei flussi di fatturazione elettronica.

GovWay supporta la connessione al SdI attraverso lo scenario di interoperabilità su rete Internet basato sull'accesso al servizio *SdICoop*. Il servizio SdICoop prevede un protocollo di comunicazione, basato su SOAP, che veicola messaggi (fatture, archivi, notifiche e metadati) secondo la codifica dettata dalle specifiche tecniche (Per dettagli in merito si faccia riferimento alle Specifiche Tecniche SdI).

Il profilo FatturaPA di GovWay consente, ai sistemi di gestione delle fatture di un ente, di non occuparsi della gestione del formato di scambio, previsto dal SdI, mantenendo un grado di interfacciamento notevolmente semplificato. Più in dettaglio:

- I gestionali dell'ente, registrati come applicativi su GovWay, inviano/ricevono le fatture e le notifiche, previste dal colloquio, nel formato originario XML senza ulteriori complessità.
- I metadati presenti nelle comunicazioni con il SdI vengono estratti ed elaborati da GovWay e trasmessi ai gestionali dell'ente tramite appositi *Header di Integrazione SdI*.
- La produzione dei metadati SdI, nel caso delle comunicazioni in uscita (fatturazione attiva), è a carico di GovWay che provvede anche a generare gli identificativi univoci da associare ai messaggi da trasmettere al SdI.

Per la produzione delle configurazioni necessarie a rendere operativo GovWay sono stati realizzati due wizard che guidano l'utente verso il corretto inserimento dei dati necessari. Gli scenari di configurazione supportati sono due e riguardano i casi della *Fatturazione Passiva* e *Fatturazione Attiva*.

5.1 Fatturazione Passiva

Nello scenario di fatturazione passiva si utilizza GovWay per la ricezione delle fatture in arrivo dal SdI. GovWay attua la decodifica del messaggio SdI ricevuto, al fine di estrarre i file fattura in esso contenuti e trasmetterli, nel formato FatturaPA, all'applicativo registrato come destinatario.

Lo scenario complessivo, relativo alla Fatturazione Passiva, è quello illustrato in Figura 41.

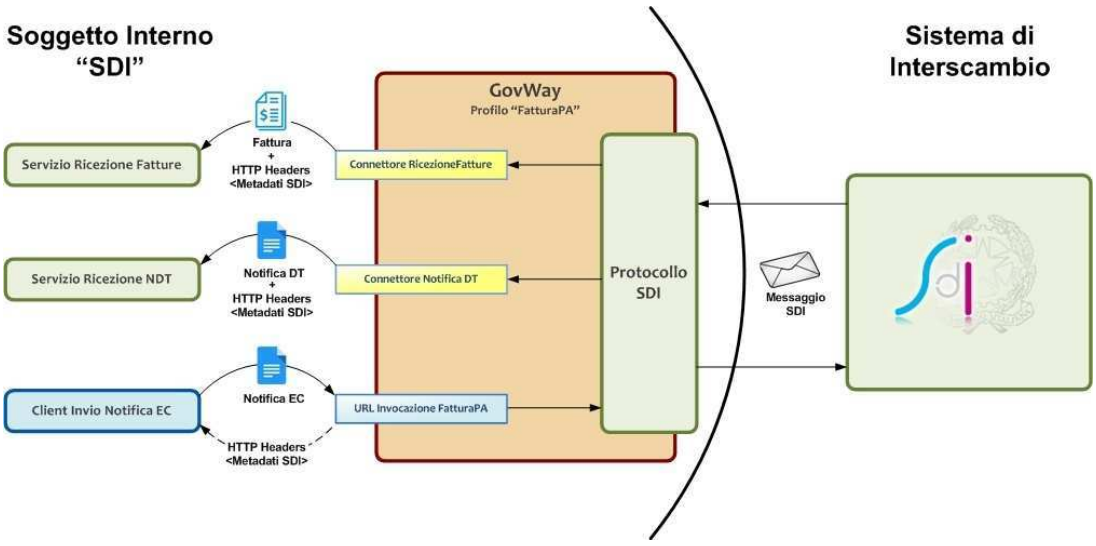


Figura 41: Scenario di interoperabilità relativo alla Fatturazione Passiva

Descriviamo per punti i passi significativi di questo scenario:

- *Servizio Ricezione Fatture*. Per consentire a GovWay di consegnare le fatture ricevute dal SdI è necessario esporre un servizio i cui riferimenti per l'accesso dovranno essere configurati nel contesto del *Connettore RicezioneFatture*, presente nella configurazione di GovWay.

  Le fatture vengono ricevute da GovWay formato codificato dal protocollo SdI, e comprendono il lotto delle fatture, con i relativi allegati, e un insieme di metadati che descrivono il contesto di invocazione. GovWay si occupa di estrarre le informazioni presenti, elaborando il messaggio SdI, provvedendo quindi a consegnare il lotto di fatture al servizio destinatario, nel formato *FatturaPA* attraverso l'invocazione di una HTTP POST. I metadati raccolti dal messaggio SdI vengono forniti, nel contesto della medesima richiesta, sotto forma di HTTP Headers (fare riferimento alla Tabella 4).

- *Client Invio Notifica EC*. I sistemi dell'ente, dopo aver ricevuto le fatture, inviano le *Notifiche di Esito Committente*, previste dal protocollo SdI, utilizzando un apposito servizio di GovWay. La URL di invocazione di tale servizio sarà disponibile al termine del processo di configurazione descritto più avanti. GovWay provvede a codificare il messaggio SdI di richiesta contenente il messaggio di notifica ricevuto dall'applicativo mittente. I metadati prodotti per il messaggio SdI, unitamente all'identificativo messaggio univoco generato, vengono restituiti all'applicativo mittente sotto forma di HTTP Headers (fare riferimento alla Tabella 5).

- *Servizio Ricezione NDT*. Per consentire a GovWay di consegnare le eventuali *Notifiche di Decorrenza Termini* è necessario esporre un servizio i cui riferimenti per l'accesso dovranno essere configurati nel contesto del *Connettore NotificaDT*, presente nella configurazione di GovWay.

  GovWay consegna le notifiche DT nel formato originale tramite una HTTP POST, includendo come HTTP Headers i metadati estratti dal messaggio SdI originariamente ricevuto (fare riferimento alla Tabella 6).

Header	**Descrizione**
GovWay-SDI-FormatoArchivioBase64	Indica se il file fattura è codificato in formato Base64
GovWay-SDI-FormatoArchivioInvioFattura	Indica se è stata utilizzata la modalità di firma CAdES o XAdES (P7M o XML)
GovWay-SDI-FormatoFatturaPA	Indice di versione del formato FatturaPA adottato
GovWay-SDI-IdentificativoSdI	Identificativo assegnato dal SdI alla fattura
GovWay-SDI-MessageId	Identificativo assegnato alla fattura dall'ente trasmittente
GovWay-SDI-NomeFile	Nome del file fattura
GovWay-SDI-NomeFileMetadati	Nome del file di metadati
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Tabella 4: Header di Integrazione "Ricezione Fattura"

Header	**Descrizione**
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Tabella 5: Header di Integrazione "Invio Notifica EC"

Header	**Descrizione**
GovWay-SDI-IdentificativoSdI	Identificativo assegnato dal SdI alla fattura
GovWay-SDI-NomeFile	Nome del file fattura
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Tabella 6: Header di Integrazione "Ricezione Notifica DT"

Per produrre le configurazioni necessarie all'utilizzo dello scenario di fatturazione passiva, è possibile utilizzare il wizard messo a disposizione per semplificare l'attività di configurazione di GovWay. I passi da eseguire sono i seguenti:

1. Scaricare il govlet per la fatturazione passiva al seguente indirizzo `http://www.govway.org/govlets/fatturazione-zip`
2. Avviare il govlet posizionandosi sulla sezione *Configurazione* > *Importa* della GovWayConsole e selezionare il file appena scaricato come oggetto da importare.

3. *Soggetto SDI*: al primo step del wizard viene richiesto di indicare, tra gli elementi presenti nella lista a discesa, il soggetto interno destinatario delle fatture. Si tratta di un soggetto appartenente al profilo "FatturaPA".

4. *Servizio SdIRiceviNotifica erogato dal Sistema di Interscambio*: al secondo step viene richiesto di indicare la URL che corrisponde all'endpoint del servizio SdIRiceviNotifica, necessario per l'invio delle *Notifiche di Esito Committente*.

   Nota
   il valore suggerito dalla maschera di configurazione del govlet fa riferimento alla url del sistema di produzione SDI. Se si vuole configurare un servizio di test è necessario cambiare tale valore ed impostare il riferimento all'ambiente di test SDI. I certificati, sia per l'ambiente di test che di produzione, devono essere stati inseriti nel truststore di GovWay dopo averli prelevati all'indirizzo http://www.fatturapa.gov.it/export/fatturazione/it/normativa/f-3.htm

5. *Credenziali per accesso URL NotificaEsito*: al terzo step viene richiesto di fornire il criterio di autenticazione utilizzato dall'applicativo per inviare la notifica di esito committente.

6. *Applicativo per consegna FatturaPA*: al quarto step viene richiesto di fornire i dati di configurazione del connettore, utilizzato da GovWay per la consegna delle fatture. La configurazione del connettore comprende: endpoint, credenziali di autenticazione ed eventualmente i riferimenti del proxy.

7. *Applicativo per consegna NotificaDecorrenzaTermini*: al quinto ed ultimo step viene richiesto di fornire i dati di configurazione del connettore, utilizzato da GovWay per la consegna della notifica di decorrenza termini. La configurazione del connettore comprende: endpoint, credenziali di autenticazione ed eventualmente i riferimenti del proxy.

5.1.1 Invio della Notifica di Esito Committente

Per l'invio della Notifica di Esito Committente l'applicativo mittente utilizza una URL così composta: *http://<host-govway>/govway/sdi*
Dove:

- *host-govway*: è l'hostname con cui è raggiungibile l'istanza di Govway.
- *SoggettoSDI*: il soggetto interno destinatario delle fatture, come configurato durante l'esecuzione del govlet di fatturazione passiva.
- *NomeFileFattura*: è il nome del file che contiene la fattura cui fa riferimento la notifica EC.
- *identificativoSDI*: è l'identificativo SDI che fa riferimento al lotto della fattura ricevuta.

Nota
La chiamata deve essere corredata dalle credenziali che sono state indicate durante la configurazione tramite il relativo govlet.

5.2 Fatturazione Attiva

Nello scenario di fatturazione attiva si utilizza GovWay per l'invio delle fatture al SdI. GovWay attua la codifica dei file ricevuti al fine di produrre un messaggio valido per l'invio al SdI.

Lo scenario complessivo, relativo alla Fatturazione Attiva, è quello illustrato in Figura 42.

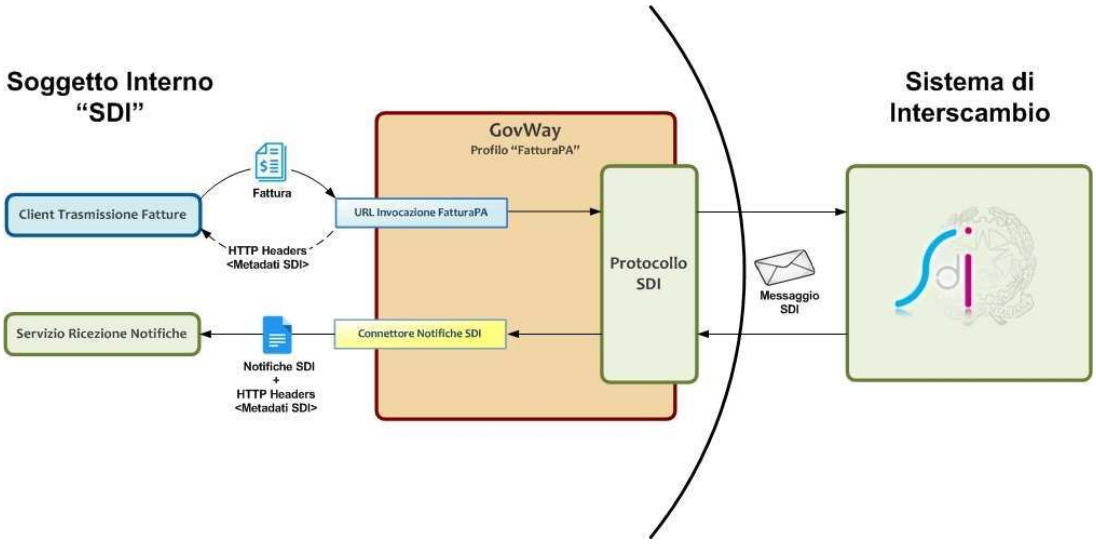


Figura 42: Scenario di interoperabilità relativo alla Fatturazione Attiva

Descriviamo per punti i passi significativi di questo scenario:

- *Client Trasmissione Fatture*. I sistemi dell'ente possono trasmettere le fatture al SdI tramite un apposito servizio di ricezione di GovWay. La URL di invocazione di tale servizio sarà disponibile al termine del processo di configurazione dello scenario di fatturazione attiva descritto più avanti. Una volta ricevuta la fattura, nel formato previsto da FatturaPA, GovWay provvede a codificare il messaggio SdI di richiesta contenente la fattura da trasmettere. I metadati prodotti per il messaggio SdI, unitamente all'identificativo SdI, vengono restituiti all'applicativo mittente sotto forma di HTTP Headers (fare riferimento alla Tabella 7).
- *Servizio Ricezione Notifiche*. I sistemi dell'ente devono esporre un servizio adibilito alla ricezione delle notifiche che il SdI invia successivamente alla trasmissione di una fattura. I riferimenti per l'accesso a tale servizio dovranno essere configurati nel contesto del *Connettore NotificheSDI*, presente nella configurazione di GovWay.

  GovWay consegna le notifiche, al servizio dell'ente, nel formato originale tramite una HTTP POST, includendo come HTTP Headers i metadati estratti dal messaggio SdI originariamente ricevuto (fare riferimento alla Tabella 8).

Header	**Descrizione**
GovWay-SDI-IdentificativoSdI	Identificativo assegnato dal SdI alla fattura
GovWay-SDI-NomeFile	Nome del file fattura
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Tabella 7: Header di Integrazione "Trasmissione Fatture"

Header	**Descrizione**
GovWay-SDI-IdentificativoSdI	Identificativo assegnato dal SdI alla fattura
GovWay-SDI-NomeFile	Nome del file fattura
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Tabella 8: Header di Integrazione "Ricezione Notifiche"

Per produrre le configurazioni necessarie all'utilizzo dello scenario di fatturazione attiva, è possibile utilizzare il wizard messo a disposizione per semplificare l'attività di configurazione di GovWay. I passi da eseguire sono i seguenti:

1. Scaricare il govlet per la fatturazione attiva al seguente indirizzo `http://www.govway.org/govlets/fatturazione-a` `zip`

2. Avviare il govlet posizionandosi sulla sezione *Configurazione* > *Importa* della GovWayConsole e selezionare il file appena scaricato come oggetto da importare.
3. *Soggetto SDI*: al primo step viene richiesto di indicare, tra gli elementi presenti nella lista a discesa, il soggetto interno mittente delle fatture. Si tratta di un soggetto appartenente al profilo "FatturaPA".
4. *Servizio SdIRiceviFile erogato dal Sistema di Interscambio*: al secondo step viene richiesto di indicare la URL che corrisponde all'endpoint del servizio SdIRiceviFile, erogato dal SdI per la trasmissione delle fatture.

   Nota
   il valore suggerito dalla maschera di configurazione del govlet fa riferimento alla url del sistema di produzione SDI. Se si vuole configurare un servizio di test è necessario cambiare tale valore ed impostare il riferimento all'ambiente di test SDI. I certificati, sia per l'ambiente di test che di produzione, devono essere stati inseriti nel truststore di GovWay dopo averli prelevati all'indirizzo http://www.fatturapa.gov.it/export/fatturazione/it/normativa/f-3.htm

5. *Credenziali per accesso URL RiceviFile*: al terzo step viene richiesto di fornire il criterio di autenticazione utilizzato dall'applicativo per invocare la url del GovWay per la trasmissione delle fatture.
6. *Applicativo per consegna Notifiche*: al quarto ed ultimo step viene richiesto di fornire i dati di configurazione del connettore, utilizzato da GovWay per la consegna delle notifiche inviate dal SdI, successivamente alla trasmissione di una determinata fattura. La configurazione del connettore comprende: endpoint, credenziali di autenticazione ed eventualmente i riferimenti del proxy.

5.2.1 Invio della fattura attiva

Per l'invio della fattura attiva l'applicativo mittente utilizza una URL così composta: *http://<host-govway>/govway/sdi/out/xml2soap/<S*
Dove:

- *host-govway*: è l'hostname con cui è raggiungibile l'istanza di Govway.
- *SoggettoSDI*: il soggetto interno destinatario delle fatture, come configurato durante l'esecuzione. del govlet di fatturazione passiva.
- *Versione*: versione della fattura che si sta inviando: FPA12 (Fattura 1.2 per Pubbliche Amministrazione), FPR12 (Fattura 1.2 per Privati), SDI11 e SDI10 (Fattura per Pubblica amministrazione versione 1.1. e 1.0).
- *TipoFile*: tipo di fattura: P7M (Fattura firmata) o ZIP (archivio di fatture).
- *IdPaese e IdCodice*: dati del trasmittente della fattura.

Nota
La chiamata deve essere corredata dalle credenziali che sono state indicate durante la configurazione tramite il relativo govlet.

6 Strumenti

6.1 Runtime

Questa sezione consente di visualizzare dati in tempo reale relativi al contesto di esecuzione del gateway, con la possibilità di effettuare alcune modifiche di stato. Le informazioni presenti sono:

- *Runtime*:
  - *Download*: consente di effettuare il download di un file di testo che contiene tutti i parametri visualizzati nella pagina.

  - *ResetAllCaches*: consente di effettuare il reset contemporaneo di tutte le cache utilizzate dal gateway.

- *Informazioni Generali*: Informazioni sul prodotto e sul software di base.
- *Stato Servizi*: Consente di abilitare/disabilitare in tempo reale i servizi per l'elaborazione delle richieste in ingresso intra ed extra dominio.
- *Informazioni Diagnostica*: Riferimenti ai file di log attivi per il prodotto, con la possibilità di modificare in tempo reale il livello di verbosità degli stessi.
- *Informazioni Tracciamento*: Riferimenti ai file contenenti il tracciamento delle richieste in elaborazione sul gateway, con la possibilità di abilitare/disabilitare le specifiche fonti.
- *Informazioni Database*: Informazioni relative la piattaforma database adottata.
- *Informazioni SSL*: Informazioni sulla configurazione SSL.
- *Informazioni Internazionalizzazione*: Informazioni sulla configurazione del servizio di internazionalizzazione.
- *Informazioni Timezone*: Timezone attivo.
- *Informazioni Java Networking*: Parametri di configurazione inerenti la configurazione del networking a livello Java.
- *Informazioni Modalità Gateway*: Contesti configurati per ciascuna specifica modalità operativa.
- *Cache*: Parametri di configurazione di tutte le cache adottate dal gateway, con la possibilità di effettuare il reset di ciascuna singolarmente.
- *Connessioni Attive*: Evidenza in tempo reale delle connessioni attive verso altri software a supporto (database, broker jms, ecc.)
- *Transazioni Attive*: Riferimenti alle transazioni in corso di elaborazione.
- *Connessioni HTTP Attive*: Evidenza in tempo reale delle connessioni HTTP, aperte in uscita, per l'elaborazione delle richieste in corso.

6.2 Auditing

La funzionalità di *auditing* consente di tracciare il comportamento degli utenti della govwayConsole, al fine di verificare le operazioni eseguite e i loro effetti.

Per gli aspetti di configurazione della funzionalità di auditing si rimanda alla Sezione 7.8.

In questa sezione descriviamo le interfacce della govwayConsole dedicate alla consultazione delle informazioni raccolte tramite il servizio di auditing.

Gli utenti della govwayConsole aventi il permesso [A] Auditing (vedi Sezione 7.5) hanno accesso alla funzionalità di consultazione dei dati presenti nel repository del servizio di auditing.

Per accedere al servizio di consultazione selezionare la voce **Auditing** nella sezione **Reportistica** del menu laterale sinistro. La consultazione dei dati di auditing avviene tramite ricerche effettuate impostando i criteri attraverso il form riportato in Figura 43.

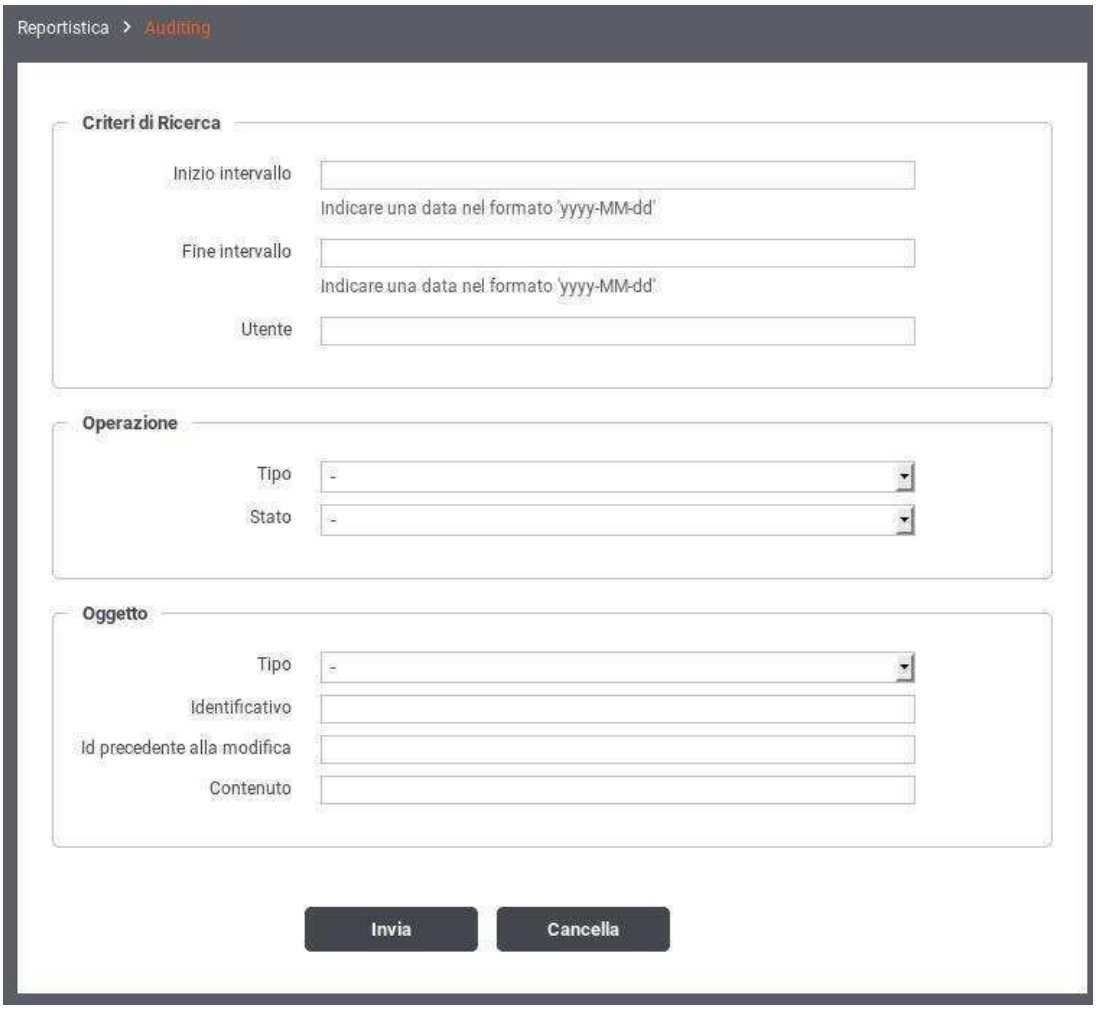


Figura 43: Maschera di ricerca dei dati di auditing

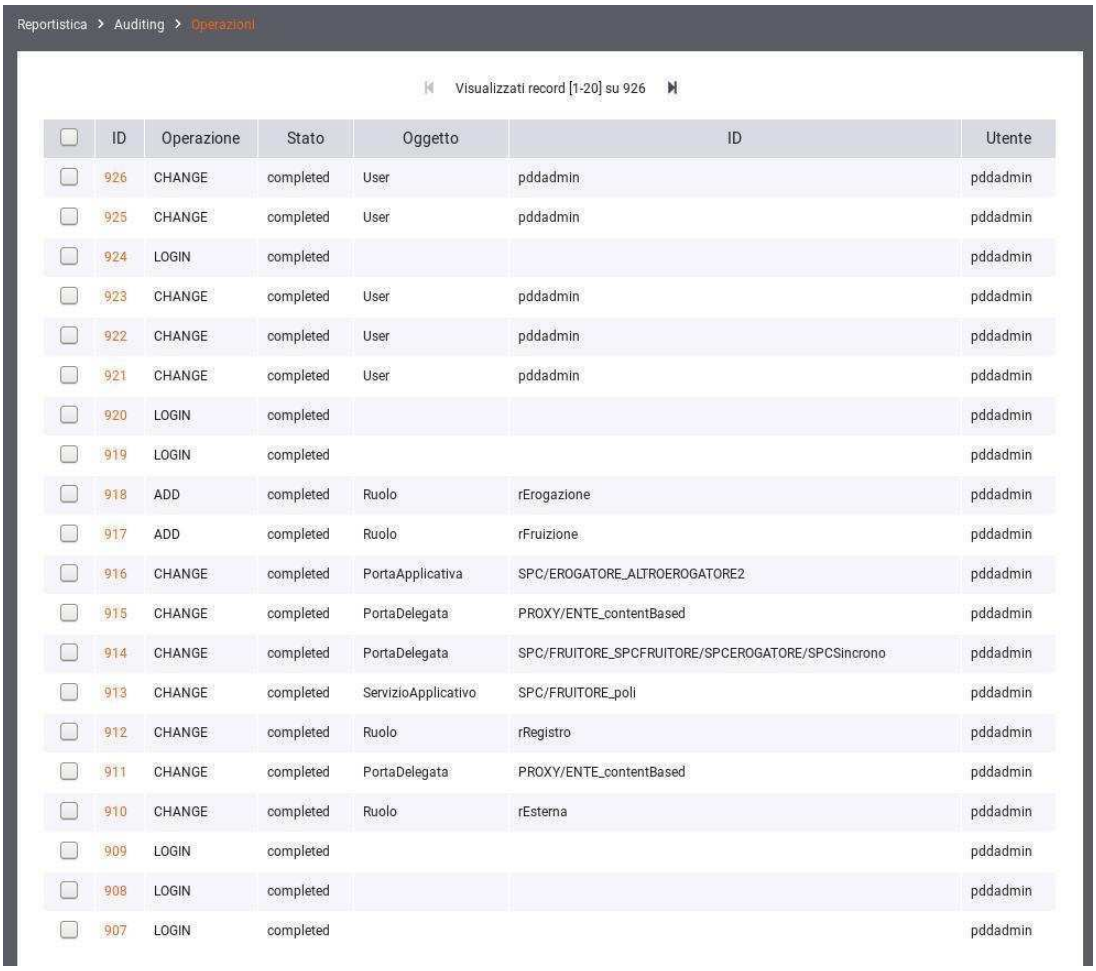
Vediamo adesso il significato dei parametri per la ricerca dei dati di auditing:

- *Criteri di Ricerca*
  - **Inizio Intervallo**: Data iniziale che serve ad impostare l'intervallo temporale su cui restringere la ricerca dei dati di auditing. Lasciare il campo vuoto equivale all'impostazione *illimitato*.
  - **Fine Intervallo**: Data finale che serve ad impostare l'intervallo temporale su cui restringere la ricerca dei dati di auditing. Lasciare il campo vuoto equivale all'impostazione *illimitato*.
  - **Utente**: Consente di restringere la ricerca alle sole operazioni effettuate da un determinato utente. Il campo lasciato vuoto equivale a *qualasiasi utente*.
- *Operazione*
  - **Tipo**: Filtro per tipo di operazione, distinguendo tra:
    - *ADD*: creazione di un'entità
    - *CHANGE*: modifica di un'entità
    - *DEL*: cancellazione di un'entità
    - *LOGIN*: accesso alla govwayConsole
    - *LOGOUT*: disconnessione dalla govwayConsole
  - **Stato**: Filtro in base allo stato dell'operazione, distinguendo tra:

  - *requesting*: in fase di richiesta
  - *error*: terminata con errore
  - *completed*: terminata correttamente

- *Oggetto*
  - **Tipo**: campo per restringere la ricerca alle sole operazioni riferite ad un determinato tipo di entità. Il campo è costituito da una lista a discesa popolata con tutte le tipologie di entità gestite dalla govwayConsole.
  - **Identificativo**: campo testuale per restringere la ricerca alle sole operazioni effettuate su una specifica entità. La composizione dell'identificativo cambia in base alla tipologia dell'entità. Ad esempio un soggetto è identificato attraverso il tipo e il nome: Tipo/NomeSoggetto.
  - **Id precedente alla modifica**: campo testuale analogo al precedente ma utile in quei casi in cui l'operazione che si sta cercando ha modificato i dati che compongono l'identificativo.
  - **Contenuto**: pattern per la ricerca sul contenuto dell'entità associata all'operazione. Per utilizzare questo criterio di filtro il servizio di auditing deve essere configurato in modo da effettuare il dump degli oggetti.

Una volta effettuata la ricerca viene mostrata una pagina con la lista dei risultati corrispondenti (vedi Figura 44).



ID	Operazione	Stato	Oggetto	ID	Utente
926	CHANGE	completed	User	pddadmin	pddadmin
925	CHANGE	completed	User	pddadmin	pddadmin
924	LOGIN	completed			pddadmin
923	CHANGE	completed	User	pddadmin	pddadmin
922	CHANGE	completed	User	pddadmin	pddadmin
921	CHANGE	completed	User	pddadmin	pddadmin
920	LOGIN	completed			pddadmin
919	LOGIN	completed			pddadmin
918	ADD	completed	Ruolo	rErogazione	pddadmin
917	ADD	completed	Ruolo	rFruizione	pddadmin
916	CHANGE	completed	PortaApplicativa	SPC/EROGATORE_ALTROEROGATORE2	pddadmin
915	CHANGE	completed	PortaDelegata	PROXY/ENTE_contentBased	pddadmin
914	CHANGE	completed	PortaDelegata	SPC/FRUITORE_SPCFRUITORE/SPCEROGATORE/SPCSincrono	pddadmin
913	CHANGE	completed	ServizioApplicativo	SPC/FRUITORE_poli	pddadmin
912	CHANGE	completed	Ruolo	rRegistro	pddadmin
911	CHANGE	completed	PortaDelegata	PROXY/ENTE_contentBased	pddadmin
910	CHANGE	completed	Ruolo	rEsterna	pddadmin
909	LOGIN	completed			pddadmin
908	LOGIN	completed			pddadmin
907	LOGIN	completed			pddadmin

Figura 44: Risultato della ricerca dei dati di auditing

Ciascun elemento della lista riporta i dati principali che identificano l'operazione. Selezionando l'identificatore dell'operazione si visualizzano i dati di dettaglio (vedi Figura 45). Dal dettaglio dell'operazione, se è attivo il dump, si può visualizzare il dettaglio dell'entità coinvolta nell'operazione e gli eventuali documenti binari (ad esempio i file WSDL associati ad un accordo di servizio).

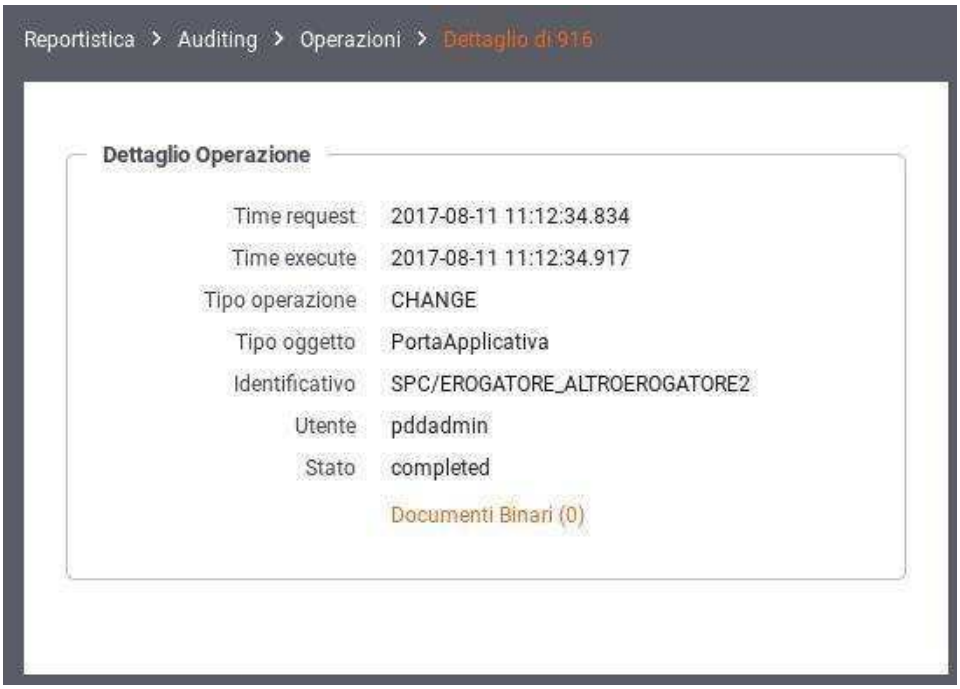


Figura 45: Dettaglio di una traccia di auditing

7 Configurazione

Nella sezione del menu *Configurazione* si raggiungono le funzionalità per modificare i parametri di configurazione del gateway.

7.1 Generale

La sezione *Configurazione* > *Generale* consente di impostare i parametri generali per le funzionalità di base del gateway. In particolare è possibile fornire i riferimenti ai servizi di base per l'elaborazione dei messaggi nelle diverse modalità supportate dal gateway (Figura 46).

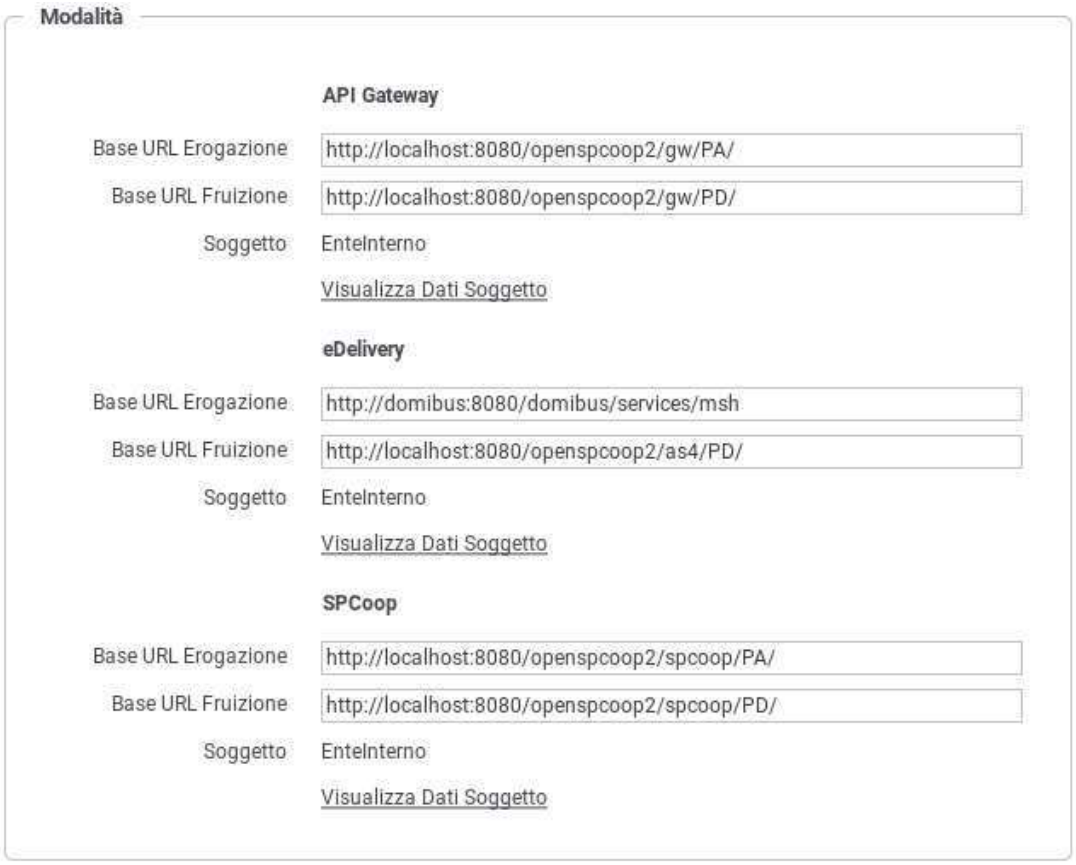


Figura 46: Maschera per l'impostazione dei parametri di configurazione generale

Per ciascuna delle modalità operative, attive sul gateway, è possibile specificare i seguenti parametri:

- *Base URL Erogazione*: Endpoint del servizio di ricezione delle richieste di erogazione supportate dal gateway.
- *Base URL Fruizione*: Endpoint del servizio di ricezione delle richieste di fruizione supportate dal gateway.
- *Soggetto*: Indicazione del soggetto interno che eroga/fruisce i servizi che fanno riferimento agli endpoint di cui sopra. Subito sotto il soggetto è presente un collegamento che porta al form di editing del soggetto visualizzato.

7.2 Tracciamento

Accedendo la sezione *Configurazione* > *Tracciamento* si possono configurare i dettagli per la registrazione delle informazioni inerenti gli scambi sui servizi gestiti dal gateway. In particolare il gateway è in grado di memorizzare le seguenti tipologie di informazioni:

- *Transazioni*: tutte le proprietà inerenti il contesto di invocazione dei servizi (dati di indirizzamento, esito, tempi di elaborazione,...)
- *Messaggi Diagnostici*: tutte le informazioni necessarie per comprendere la fase di elaborazione delle richieste e indagare sulle anomalie occorse
- *Messaggi Applicativi*: salvataggio dei messaggi in transito sulle singole comunicazioni

In Figura 47 è mostrata la pagina di configurazione del servizio di tracciamento.

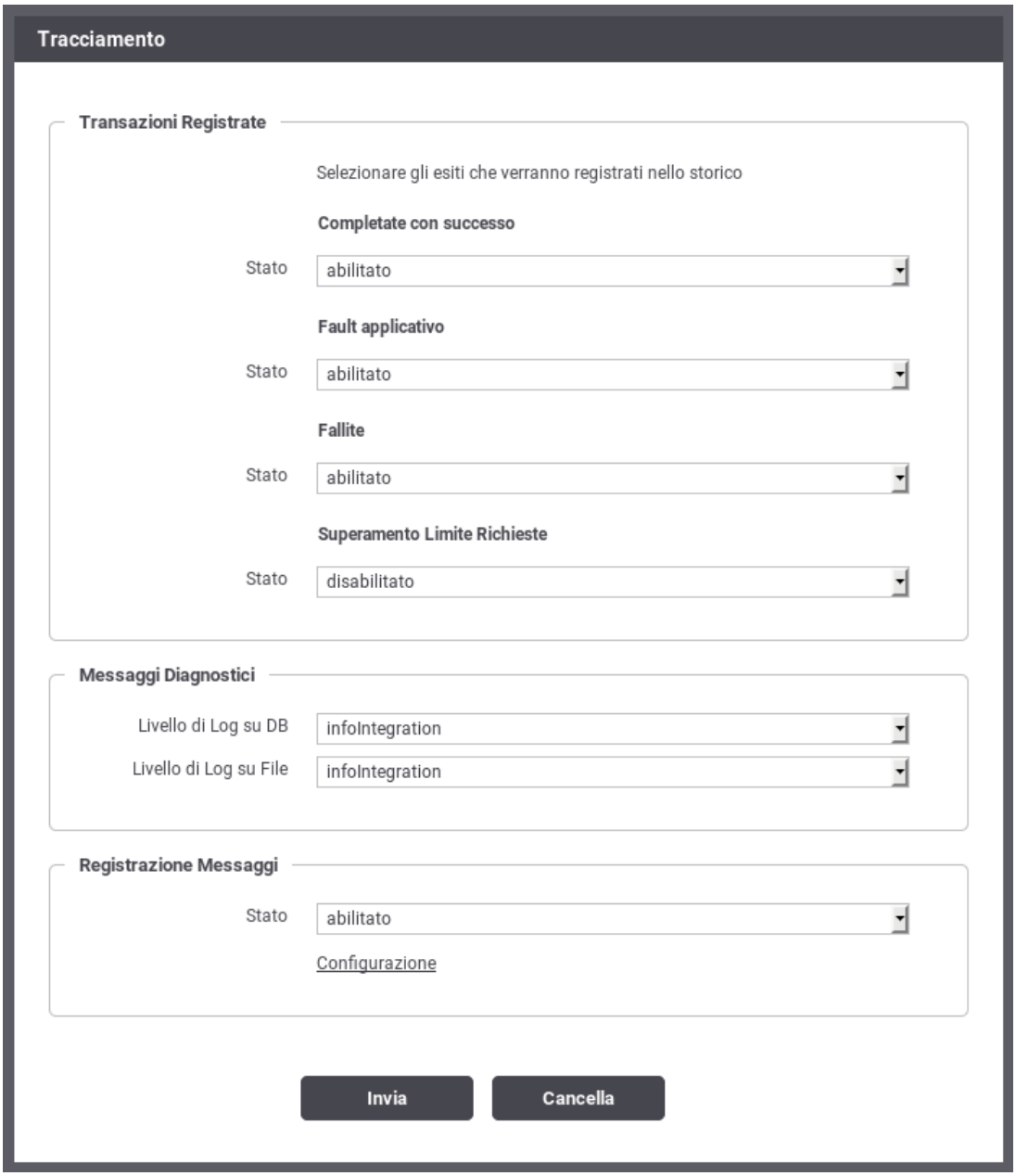


Figura 47: Configurazione del servizio di tracciamento

Vediamo il significato delle sezioni di questa pagina:

- *Transazioni Registrate*: questa sezione consente di specificare quali transazioni memorizzare nell'archivio di monitoraggio in base all'esito rilevato in fase di elaborazione. Gli esiti sono suddivisi nei seguenti gruppi: Completate con successo, Fault applicativo, Fallite e Superamento Limite Richieste. Per ciascun esito è possibile abilitare o disabilitare la registrazione. È possibile inoltre, scegliendo l'opzione *Personalizzato* specificare puntualmente quali esiti di dettaglio includere.
- *Messaggi Diagnostici*: questa sezione consente di specificare il livello di verbosità dei messaggi diagnostici da generare. Si può distinguere il livello di verbosità per il salvataggio su *Database* e su *File*.
- *Registrazione Messaggi*: questa sezione consente di abilitare e configurare la registrazione dei messaggi in transito sul gateway durante l'elaborazione delle richieste e relative risposte. Una volta abilitata l'opzione si possono configurare i dettagli della funzionalità tramite il link *Configurazione*.

Dalla sottosezione di configurazione si può distinguere il criterio di registrazione dei messaggi tra la Richiesta e la Risposta, abilitando/disabilitando solo la comunicazione desiderata. Sia per la Richiesta che per la Risposta, dopo aver optato per l'abilitazione della registrazione, si distingue tra:

- *Ingresso*: il messaggio di richiesta o risposta nel momento in cui giunge sul gateway e quindi prima che venga sottoposto al processo di elaborazione previsto.
- *Uscita*: il messaggio di richiesta o risposta nel momento in cui esce dal gateway, per raggiungere il nodo successivo del flusso, e quindi dopo che è stato sottoposto al processo di elaborazione previsto.

Per ciascuno dei messaggi, su cui è stata abilitata la registrazione, è possibile scegliere quale elemento viene registrato:

- *Headers*: vengono salvati gli header di trasporto (HTTP HEADERS) associati al messaggio.
- *Body*: viene salvato il corpo del messaggio.
- *Attachments*: vengono salvati gli eventuali attachments presenti nel messaggio.

Nota

Le configurazioni effettuate in questa sezione della console hanno valenza globale e quindi rappresentano il comportamento di default adottato dal gateway nella gestione dei diversi flussi di comunicazione. Tale comportamento può essere ridefinito puntualmente su ogni singola erogazione/fruizione agendo sulla voce di configurazione *Tracciamento* in quel contesto.

7.3 Controllo del Traffico

Accedendo la sezione *Configurazione* > *Controllo del Traffico* si possono impostare i parametri di configurazione relativamente alla fuzionalità che consente di stabilire le politiche di accesso alle risorse del gateway, nell'ottica di amministrare le risorse applicative a disposizione, ottimizzando le prestazioni e gestendo le situazioni di picco.

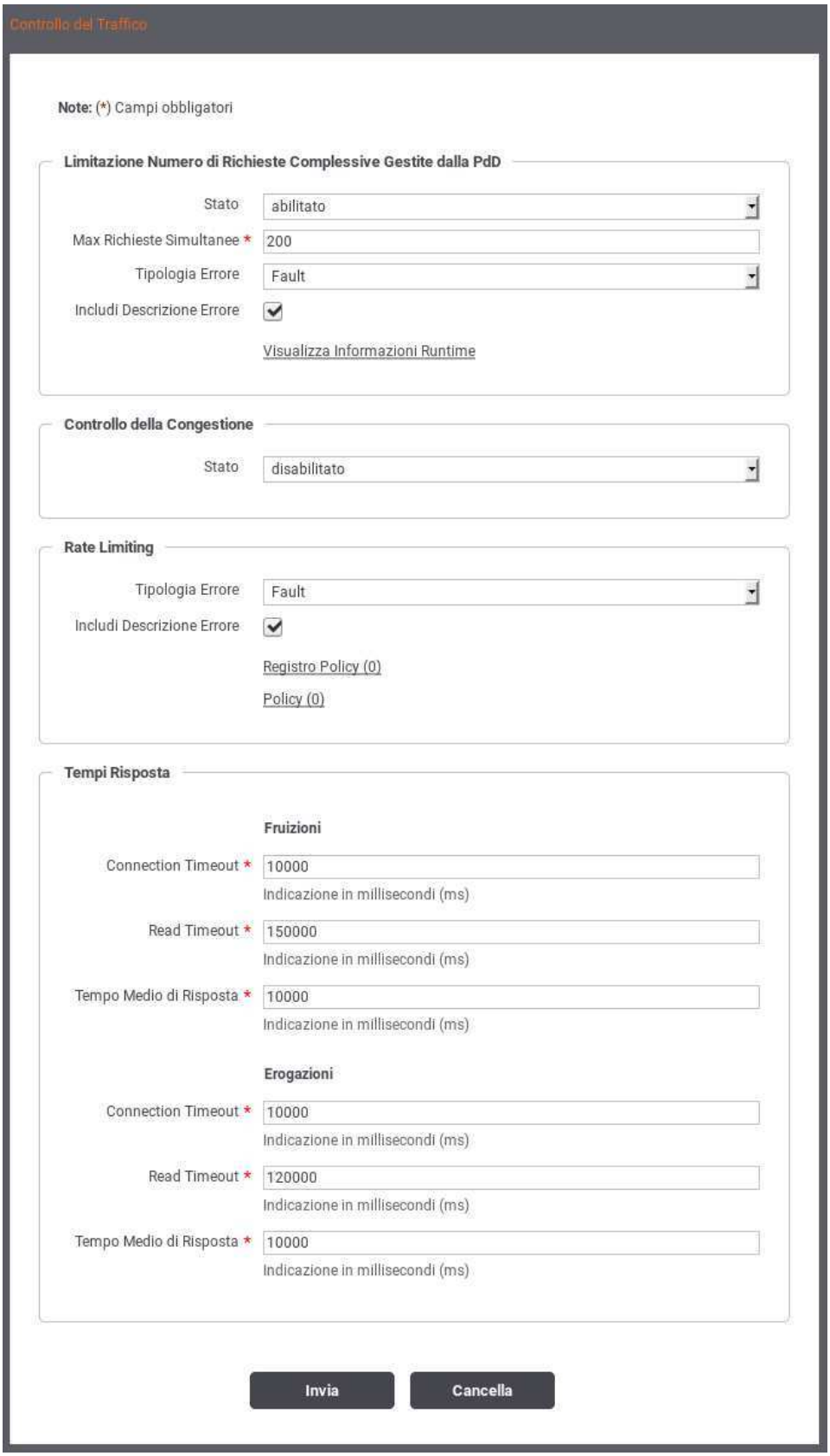


Figura 48: Maschera per l'impostazione dei parametri di controllo del traffico

La configurazione della funzionalità di controllo del traffico (Figura 48) si compone dei seguenti gruppi di configurazioni:

- *Limitazione Numero di Richieste Complessive*: consente di fissare un numero limite, riguardo le richieste gestibili simultaneamente dal gateway, bloccando le richieste in eccesso.
- *Controllo della Congestione*: consente di attivare il rilevamento dello stato di congestionamento del gateway, in seguito al superamento di una determinata soglia relativamente alle richieste simultanee.
- *Rate Limiting*: sezione per l'impostazione di policy al fine di attivare strategie di controllo del traffico con criteri di selezione specifici della singola richiesta.
- *Tempi Risposta*: sezione per l'impostazione dei valori limite relativi ai tempi di risposta dei servizi, sia nei casi di erogazione che di fruizione.

Le sezioni seguenti dettagliano questi elementi di configurazione.

7.3.1 Limitazione Numero di Richieste Complessive

Il primo livello di configurazione, presente nella pagina di accesso, consente di impostare i seguenti parametri:

- *Stato* (abilitato | disabilitato | warningOnly): Attiva il controllo sul numero di richieste simultanee in elaborazione. Selezionando l'opzione *abilitato* le richieste simultanee ricevute, che eccedono la soglia indicata (parametro *MaxRichiesteSimultanee*) verranno rifiutate restituendo al chiamante un errore. La tipologia di errore restituita è configurabile tramite l'elemento *Tipologia Errore* che appare solamente in caso di controllo abilitato.

  Il controllo sul numero di richieste simultanee in elaborazione può anche essere attivato in modalità *WarningOnly* dove, in caso il superamento della soglia, genera solamente un messaggio diagnostico di livello *error* e un evento che segnala l'accaduto.

- *Max Richieste Simultanee*: Corrisponde al numero massimo di richieste simultanee accettate. In genere è possibile fornire un valore accurato dopo aver valutato la portata massima del prodotto installato, in base alle risorse hardware disponibili e ai parametri di dimensionamento delle risorse applicative (ad esempio: numero connessioni al database, dimensioni della memoria java, ecc).

  Al superamento di tale valore non verranno accettate ulteriori richieste concorrenti, che verranno quindi rifiutate. Al verificarsi di questa situazione il gateway emette un evento specifico. Queste transazioni vengono marcate con esito *Superamento Limite Richieste* e saranno registrate solamente se previsto dalla configurazione (per default non vengono registrate). Per i dettagli sulla configurazione delle transazioni da registrare in base all'esito consultare Sezione 7.2.

- *Tipologia Errore* e *Includi Descrizione Errore*: Imposta il tipo di errore restituito al chiamante nel caso di rifiuto dell'elaborazione per superamento della soglia del numero massimo di richieste simultanee. Le opzioni possibili sono le seguenti:

  - *Fault*: viene generato un messaggio di Fault contenente un codice ed una descrizione dell'errore rilevato nel caso l'elemento *Includi Descrizione Errore* sia abilitato, o un codice di errore generico altrimenti.
  - *Http 429 (Too Many Requests)*
    Http 503 (Service Unavailable)
    Http 500 (Internal Server Error)
    Viene generata una risposta HTTP con il codice selezionato, contenente una pagina html di errore, se l'elemento *Includi Descrizione Errore* è abilitato, o una risposta http vuota altrimenti.

- *Visualizza Informazioni Runtime*: Selezionando questo collegamento si apre una pagina (Figura 49) che mostra in real-time le seguenti informazioni:

  - *Richieste Attive*: il numero di richieste simultanee attualmente in corso di elaborazione.
  - *Stato Gateway*: indica se il gateway ha raggiunto o meno lo stato di congestionamento, e quindi superata la soglia sul numero massimo di richieste simultanee.

    Nota
    L'indicatore è attivo solo nel caso in cui lo stato della successiva opzione *Controllo della Congestione* sia abilitato.

– *Refresh*: collegamento che consente di aggiornare le informazioni presentate nello schermo.

Figura 49: Dati di congestionamento in tempo reale

7.3.2 Controllo della Congestione

Questa sezione consente di impostare i parametri relativi al controllo della congestione. Sono disponibili le seguenti opzioni:

- *Stato* (abilitato | disabilitato): Attiva il controllo sul numero di richieste simultanee al fine di individuare lo stato di congestionamento.
- *Soglia di Attivazione (%)*: Selezionando l'opzione *abilitato*, al passo precedente, questo elemento consente di indicare la soglia dello stato di congestionamento. La soglia da indicare è in percentuale rispetto al Numero Massimo Richieste Simultanee. Al superamento di tale soglia si entra nello stato di congestionamento con conseguente emissione di un evento e un messaggio diagnostico al riguardo.

Nota
Sulla base della percentuale indicata come soglia, una dicitura riporta nella pagina il valore di congestionamento calcolato in base al numero massimo di richieste simultanee.

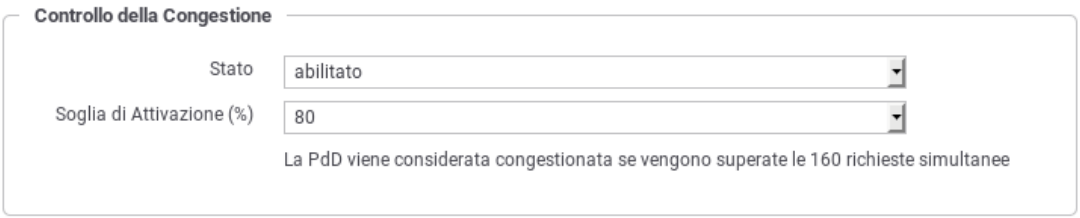


Figura 50: Configurazione della soglia di congestionamento

7.3.3 Rate Limiting

Questa sezione consente di creare e attivare le policy di controllo del traffico. Gli elementi di configurazione presenti sono:

- *Tipologia Errore* e *Includi Descrizione Errore*: Imposta il tipo di errore restituito al chiamante nel caso venga rilevata una violazione delle policy configurate:
  - *Fault*: viene generato un messaggio di Fault contenente un codice ed una descrizione dell'errore rilevato nel caso l'elemento *Includi Descrizione Errore* sia abilitato, o un codice di errore generico altrimenti.
  - *Http 429 (Too Many Requests)*
    Http 503 (Service Unavailable)
    Http 500 (Internal Server Error)
    viene generata una risposta HTTP con il codice selezionato contenente una pagina html di errore se l'elemento *Includi Descrizione Errore* è abilitato, od una risposta http vuota altrimenti.
- *Registro Policy*: Consente di accedere al Registro delle Policy per visualizzare, modificare e creare le policy di controllo istanziabili per la configurazione del rate limiting. Tra parentesi viene visualizzato il numero di policy attualmente presenti nel registro. Questa funzionalità è descritta nella Sezione 7.3.3.1.
- *Policy Globali*: Consente di accedere al Registro delle Policy Attivate in ambito globale, cioè operative sul traffico complessivo che transita sul gateway. A queste policy si aggiungono quelle eventualmente definite localmente nella configurazione specifica di ciascuna erogazione/fruizione.
  Tra parentesi viene visualizzato il numero di policy attualmente attivate. Questa funzionalità è descritta nella Sezione 7.3.3.2.

7.3.3.1 Registro Policy

Il Registro delle Policy è il repository dove si possono creare le policy di rate limiting che potranno essere successivamente istanziate. L'accesso alla sezione è possibile grazie all'omonimo collegamento presente nella sezione *Rate Limiting* della pagina principale del controllo del traffico.

La pagina indice del Registro delle Policy mostra l'elenco delle policy già presenti (Figura 51).

Figura 51: Elenco delle Policy di Rate Limiting presenti nel registro

Tramite il pulsante "Aggiungi" è possibile aprire la pagina di creazione di una policy di Rate Limiting (Figura 52).

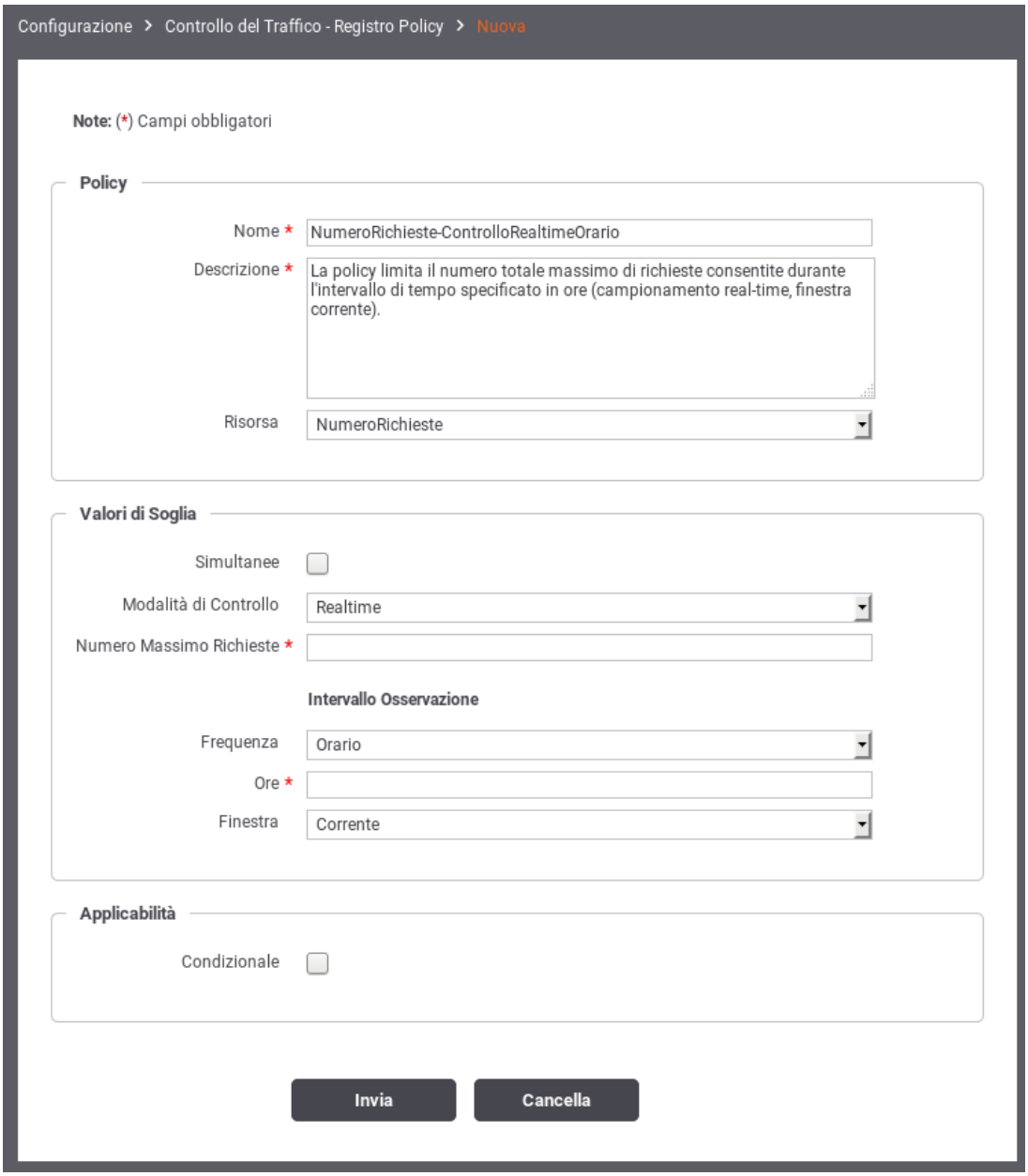


Figura 52: Maschera per la creazione di una policy di Rate Limiting

Descriviamo nel seguito i dati che è necessario inserire per la creazione di una policy. Si tenga presente che il sistema propone valori di default per alcuni campi; tali valori cambiano in base alle scelte operate sugli altri campi e possono essere considerati come "consigliati" in base alla combinazione di scelte attuate.

- *Policy*: In questa sezione sono presente i dati che identificano la policy.
  - *Nome*: Nome assegnato alla policy. Finché il campo non viene modificato dall'utente, viene proposto automaticamente un nome espressivo sulla base delle scelte operate sui rimanenti elementi del form.
  - *Descrizione*: Un testo di descrizione riferito alla policy. Finché il campo non viene modificato dall'utente, viene proposto un testo automatico di descrizione sulla base delle scelte operate sui rimanenti elementi del form.
  - *Risorsa*: Si seleziona la risorsa che la policy deve monitorare al fine di attuare le eventuali restrizioni. Sono disponibili le seguenti risorse:

  - *NumeroRichieste*: La policy effettua il controllo sul numero di richieste gestite. Selezionando questa risorsa si attiveranno i seguenti elementi per la configurazione dei valori di soglia:
    - *Simultanee*
    - *Modalità di Controllo*
    - *Numero Massimo di Richieste*
    - *Frequenza Intervallo Osservazione*
    - *Intervallo Osservazione*
    - *Finestra Osservazione*
    - Se si attiva l'opzione "Simultanee" l'unico campo visibile sarà: *Numero Massimo di Richieste*
  - *OccupazioneBanda*: La policy effettua il controllo sulla banda occupata da e verso le comunicazioni con il gateway. Selezionando questa risorsa si attiveranno i seguenti elementi per la configurazione dei valori di soglia:
    - *Modalità di Controllo*
    - *Tipo Banda*
    - *Occupazione Massima di Banda (kb)*
    - *Frequenza Intervallo Osservazione*
    - *Intervallo Osservazione*
    - *Finestra Osservazione*
  - *TempoComplessivioRisposta*: La policy controlla la quantità di tempo complessivamente impiegata dal gateway per la ricezione delle risposte dai servizi invocati. Selezionando questa risorsa si attiveranno i seguenti elementi per la configurazione dei valori di soglia:
    - *Modalità di Controllo su Realtime (non modificabile)*
    - *Tipo Latenza*
    - *Occupazione Massima di Tempo (secondi)*
    - *Frequenza Intervallo Osservazione*
    - *Intervallo Osservazione*
    - *Finestra Osservazione*
  - *TempoMedioRisposta*: La policy controlla il tempo medio impiegato dal gateway per la ricezione delle risposte dai servizi invocati. Selezionando questa risorsa si attiveranno i seguenti elementi per la configurazione dei valori di soglia:
    - *Modalità di Controllo*
    - *Tipo Latenza*
    - *Tempo Medio Risposta (ms)*
    - *Frequenza Intervallo Osservazione*
    - *Intervallo Osservazione*
    - *Finestra Osservazione*
  - *NumeroRichiesteCompletateConSuccesso*
    NumeroRichiesteFallite
    NumeroFaultApplicativi
    La policy effettua il controllo sul numero di richieste gestite dal gateway e terminate con un esito che rientra nella casistica associata alla risorsa selezionata (completate con successo, fallite o fault applicativi). Selezionando questa risorsa si attiveranno i seguenti elementi per la configurazione dei valori di soglia:
    - *Modalità di Controllo*
    - *Numero Massimo di Richieste*
    - *Frequenza Intervallo Osservazione*
    - *Intervallo Osservazione*
    - *Finestra Osservazione*

- *Valori di Soglia*: In questa sezione si specificano i valori di soglia (già anticipati al punto precedente), superati i quali, la policy risulta violata. Alcuni campi presenti in questa sezione cambiano in base alla risorsa monitorata.

  – *Simultanee*: Questa opzione è presente solo per la risorsa "NumeroRichieste". Attivandola si specifica che il criterio restrittivo entra in funzione al superamento di una soglia sul numero di richieste simultaneamente in gestione.

- *Modalità di Controllo*: Rappresenta la modalità di raccolta dei dati di traffico che saranno usati per la valutazione della policy. Si può scegliere tra le seguenti opzioni:
  - *Realtime*: L'indicatore utilizzato per valutare la policy viene calcolato sulla base di dati raccolti in tempo reale durante l'elaborazione. Questa modalità assicura la massima accuratezza ma occorre tenere presenti le seguenti restrizioni nell'uso:
    1. I dati "realtime" vengono raccolti in maniera separata sui singoli nodi del cluster. Quindi il controllo effettuato dalla policy riguarderà il traffico sul singolo nodo.
    2. Si possono impostare criteri di controllo su grana temporale piccola: secondi, minuti, orario, giornaliero.
  - *Statistica*: L'indicatore utilizzato per valutare la policy viene calcolato sulla base delle informazioni statistiche presenti nel database di monitoraggio. L'accuratezza dei dati utilizzati per la valutazione è subordinata alla frequenza di aggiornamento dei dati statistici sul database. In questa modalità:
    1. L'indicatore utilizzato per il confronto con la soglia della policy è sempre complessivo rispetto a tutti i nodi del cluster.
    2. Si possono impostare criteri di controllo con grana temporale ampia: orario, giornaliero, settimanale, mensile.
    3. Si può utilizzare la tipologia "finestra scorrevole" come valore per la "Finestra Osservazione", che descriveremo poco più avanti.
- *Numero Massimo di Richieste*: Campo visibile solo per la risorsa monitorata "NumeroRichieste". Consente di specificare la soglia per la policy. Quando il numero delle richieste, conteggiate secondo la logica specificata nella policy, supera questo valore, la policy risulta violata.
- *Tipo Banda*: Campo visibile solo per la risorsa monitorata "OccupazioneBanda". Consente di specificare la modalità di calcolo della banda occupata per il confronto con la soglia impostata nella policy. Sono disponibili le seguenti opzioni:
  - *Banda Interna*: Ai fini del conteggio dell'occupazione di banda (in KB) verrà considerato il solo traffico relativo alle comunicazioni con gli applicativi interni al dominio.
  - *Banda Esterna*: Ai fini del conteggio dell'occupazione di banda (in KB) verrà considerato il solo traffico relativo alle comunicazioni con i servizi esterni al dominio.
  - *Banda Complessiva*: Ai fini del conteggio dell'occupazione di banda (in KB) verrà considerato tutto il traffico in entrata ed uscita sul gateway.
- *Occupazione Massima di Banda (kb)*: Campo visibile solo per la risorsa monitorata "OccupazioneBanda". Consente di specificare la soglia per la policy. Quando la banda, calcolata secondo la logica specificata nella policy, supera questo valore, la policy risulta violata.
- *Tipo Latenza*: Campo visibile solo per le risorse monitorate "TempoComplessivoRisposta" e "TempoMedioRisposta". Consente di specificare la logica di calcolo del tempo di risposta sulla base delle due seguenti opzioni:
  - *Latenza Servizio*: Per il calcolo del tempo di risposta si considera unicamente il tempo di attesa del gateway dall'invio della richiesta alla ricezione della risposta.
  - *Latenza Totale*: Per il calcolo del tempo di risposta si considera, oltre alla latenza del servizio, anche il tempo di elaborazione del gateway dal momento dell'ingresso della richiesta fino all'uscita della risposta.
- *Occupazione Massima di Tempo (secondi)*: Campo visibile solo per la risorsa monitorata "TempoComplessivoRisposta". Consente di specificare la soglia per la policy. Quando la latenza complessiva, calcolata secondo la logica specificata nella policy, supera questo valore, la policy risulta violata.
- *Tempo Medio Risposta (ms)*: Campo visibile solo per la risorsa monitorata "TempoMedioRisposta". Consente di specificare la soglia per la policy. Quando la latenza media, calcolata secondo la logica specificata nella policy, supera questo valore, la policy risulta violata.
- *Frequenza Intervallo Osservazione*

  Intervallo Osservazione

  Finestra Osservazione

  La composizione di questi 3 campi specifica in quale intervallo temporale devono essere selezionati i dati da utilizzare per calcolare l'indicatore che deve essere confrontato con la soglia della policy.

  I valori di "Frequenza Intervallo Osservazione" e "Intervallo Osservazione" specificano la frequenza di campionamento dei dati utilizzati per la valutazione delle soglie. In particolare il valore da specificare come Intervallo Osservazione è sempre un numero intero (ad esempio inserendo 8 si campioneranno i dati su finestre di 8 secondi, 8 minuti, ecc, in base all'unità di misura indicata per la frequenza). Il valore selezionato come "Finestra Osservazione" individua l'esatto intervallo utilizzato nella catena temporale ogni volta che si valuta la policy per una specifica richiesta di servizio.

Per comprendere la logica con cui viene calcolata la finestra di osservazione è necessario introdurre il concetto di Data Attivazione Policy. Si tratta della data in cui la policy è stata applicata ad una richiesta in transito sul gateway. A partire da questa data vengono calcolate le finestre di osservazione in base alla frequenza di campionamento selezionata.

In Figura 8 è mostrato un confronto tra le diverse finestre di osservazione su un campionamento di 2 ore. La determinazione della finestra può essere analogamente trasposta su altre frequenze di campionamento.

Riepilogando:

* *Corrente*: Indica che per il calcolo dell'indicatore saranno utilizzati i dati che rientrano nella finestra temporale in cui ricade la richiesta in esame.
* *Precedente*: Indica che per il calcolo dell'indicatore saranno utilizzati i dati che rientrano nella finestra temporale precedente a quella in cui ricade la richiesta in esame.
* *Scorrevole (disponibile solo nella Modalità Controllo "Statistica")*: Indica che per il calcolo dell'indicatore saranno utilizzati i dati che rientrano in una finestra dinamica che ha come estremo superiore l'ora piena subito precedente all'istante della richiesta in fase di valutazione.

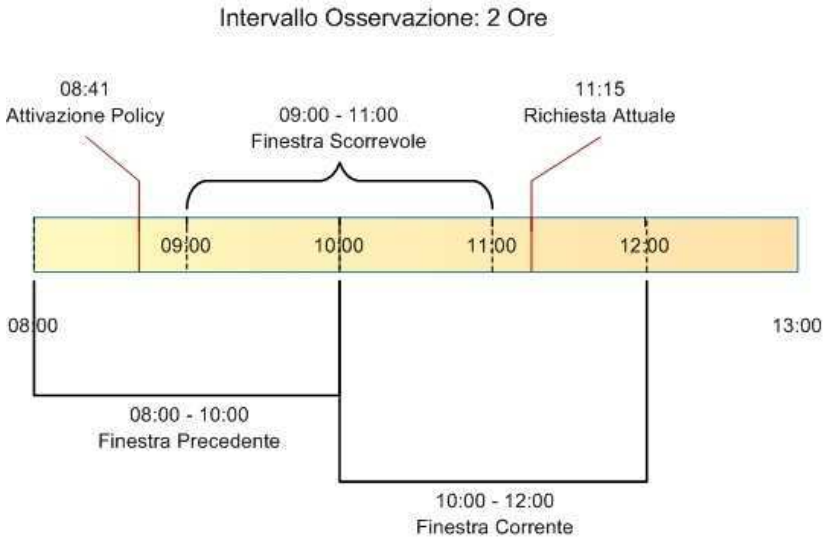


Figura 53: Finestre di osservazione su un campionamento di 2 ore

- *Applicabilità*: Questa sezione della policy consente di restringere l'applicabilità della policy sulla base di alcuni criteri (Figura 54). Sono presenti i seguenti campi:
  - *Condizionale*: Se questa opzione non è attiva, la policy si applica in maniera incondizionata. Attivando l'opzione, la policy risulterà applicabile sulla base dei criteri specificati nei campi successivi.
  - *In presenza di Congestione del Traffico*: Attivando questa opzione la policy risulta applicabile solo quando sussiste lo stato di congestionamento. Affinché questo evento venga rilevato è necessario che sia abilitato il "Controllo della Congestione", descritto in precedenza, e che risulti superata la soglia impostata sul numero di richieste simultanee.
  - *In presenza di Degrado Prestazionale*: Attivando questa opzione, la policy risulta applicabile solo in caso si rilevi un degrado prestazionale sullo specifico servizio corrispondente alla richiesta in gestione sul gateway. Per la rilevazione del degrado prestazionale si utilizzano le soglie "Tempo Medio di Risposta" impostate sia per le fruizioni che per le erogazioni. Come descritto in precedenza, tali soglie vengono definite per default nella sezione "Configurazione > Controllo del Traffico", ma possono essere ridefinite al livello del singolo connettore. Per il calcolo del tempo medio di risposta del servizio, da confrontare con la soglia impostata, si utilizza il criterio definito con i campi seguenti:
    * *Modalità di Controllo*
    * *Tempo Medio Risposta*
    * *Frequenza Intervallo Osservazione*
    * *Intervallo Osservazione*
    * *Finestra Osservazione*

    Per tutti questi campi valgono le medesime descrizioni già riportate nella sezione precedente "Valori di Soglia".

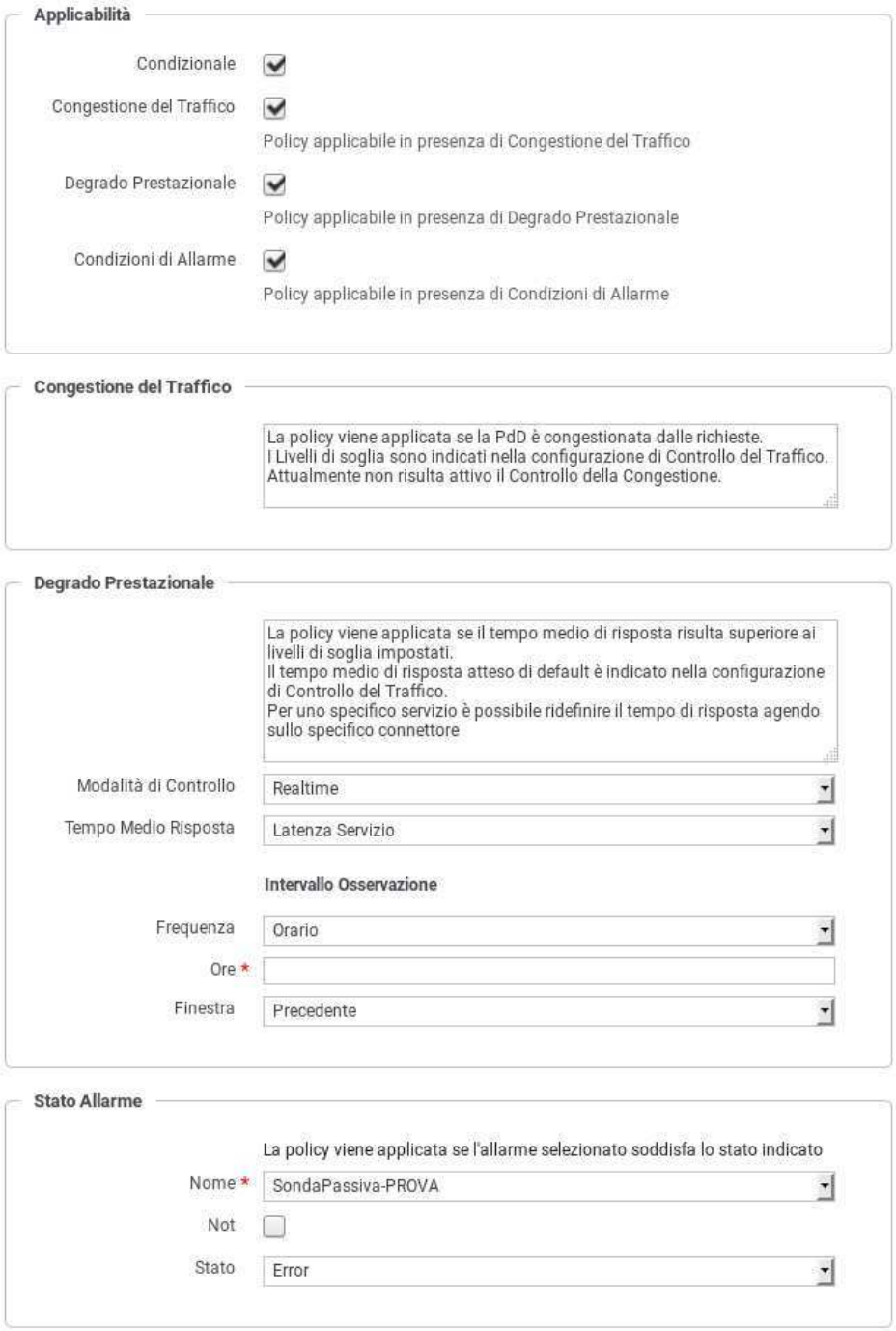


Figura 54: Opzioni per l'applicabilità di una policy di rate limiting

Nota
Se si selezionano più opzioni di applicabilità queste si considerano connesse secondo l'operatore logico AND.

7.3.3.2 Policy

Le policy di rate limiting vengono definite ed inserite nel Registro delle Policy secondo le modalità descritte nella sezione precedente. Le policy presenti nel Registro delle Policy non sono attive fino a quando non vengono istanziate.

Dalla pagina *Configurazione* > *Controllo del Traffico* selezionare il collegamento *Policy*, nella sezione *Rate Limiting*, per accedere alle policy istanziate (Figura 55).

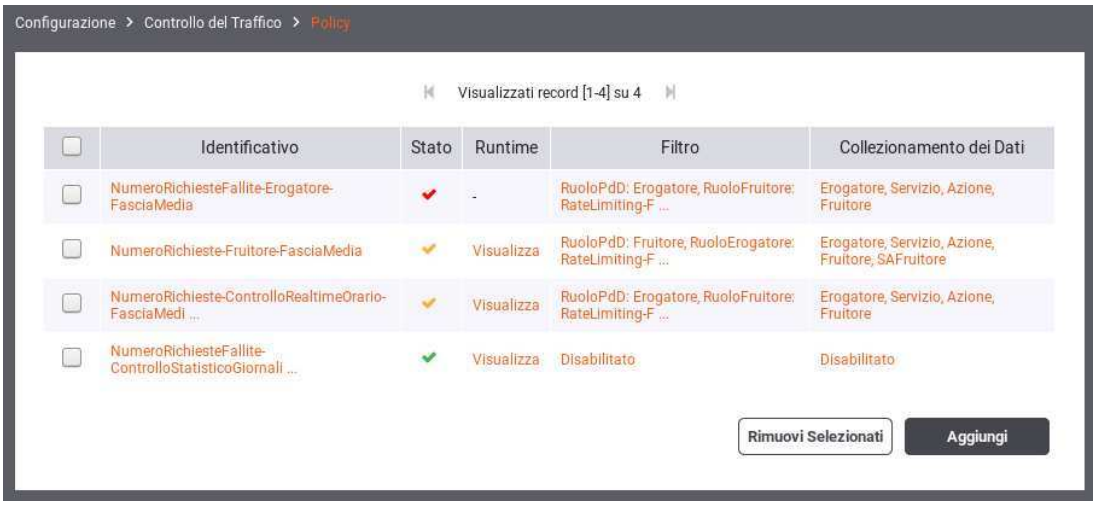


Figura 55: Elenco delle policy di Rate Limiting attivate

La pagina indice delle Policy Istanziate mostra l'elenco delle istanze già presenti e i pulsanti per le operazioni CRUD.

Tramite il pulsante *Aggiungi* è possibile aprire la pagina che contiene il form di creazione di una nuova istanza di policy (Figura 56).

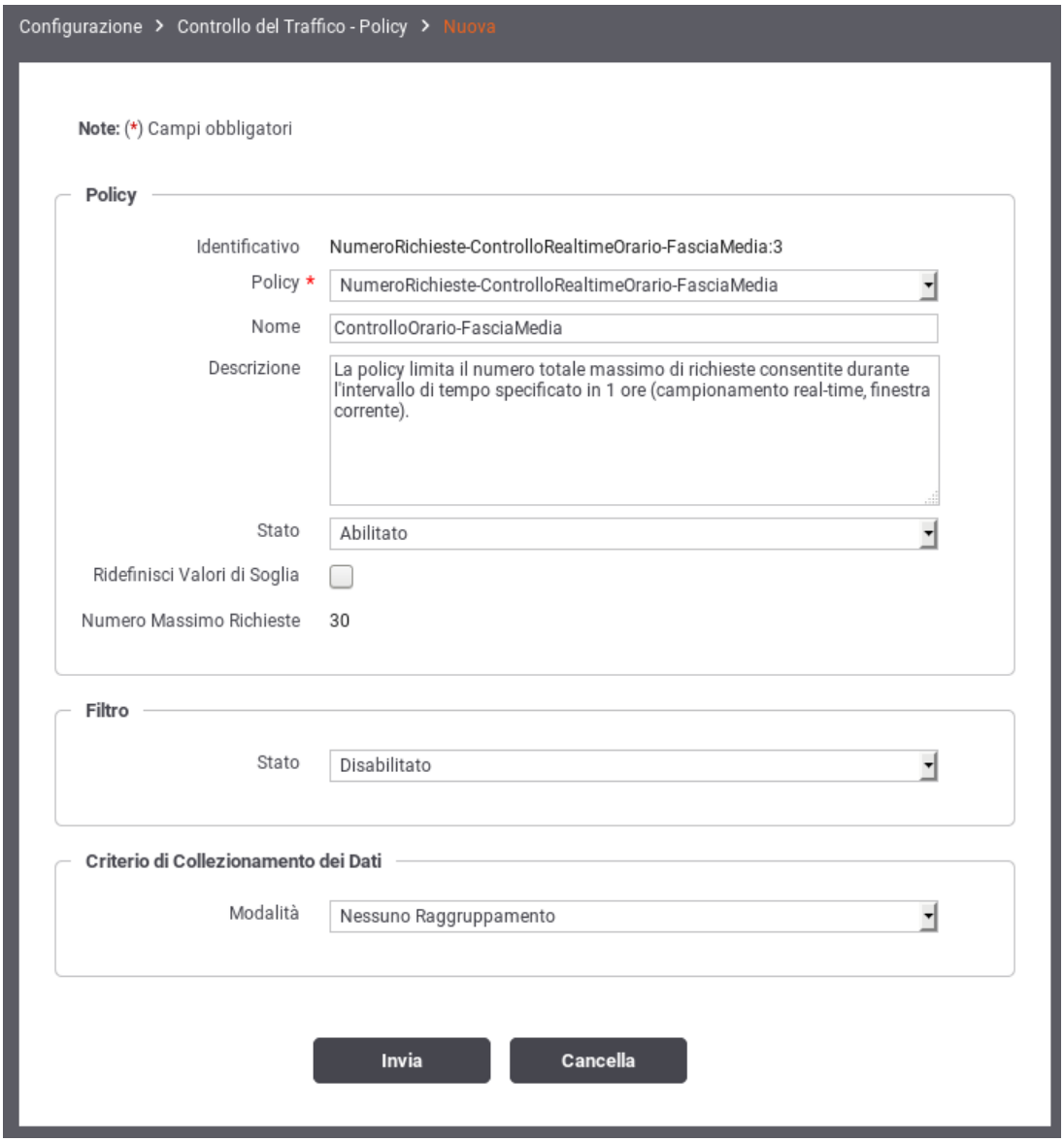


Figura 56: Creazione di una istanza relativa ad una policy di Rate Limiting

Dalla pagina di creazione dell'istanza di policy il primo passo è quello di selezionare la policy di origine tra quelle disponibili nel Registro delle Policy. Una volta selezionata la policy è visibile come il sistema assegni automaticamente un identificativo univoco per l'istanza e mostri quindi i rimanenti campi per completare la configurazione. Di seguito si descrivono in dettaglio tali sezione di configurazione.

- *Policy*: la policy da attivare. Si compone di:
  - *Identificativo*: Identificativo univoco assegnato automaticamente all'istanza di policy.
  - *Policy*: La policy su cui è basata l'istanza in fase di creazione.
  - *Nome*: Opzionale. Permette di identificare l'istanza della policy tramite un nome alternativo all'identificativo assegnato automaticamente dal sistema.
  - *Descrizione*: Il testo di descrizione della policy.
  - *Stato*: Lo stato dell'istanza di policy una volta creata. Sono disponibili le seguenti opzioni:
    - *Abilitato*: L'istanza di policy è abilitata. Questo significa che le violazioni rilevate saranno gestite in maniera restrittiva (negazione del servizio).

    - *WarningOnly*: L'istanza di policy è abilitata in modalità WarningOnly. Questo significa che le violazioni rilevate saranno solo segnalate tramite messaggi diagnostici ma non ci saranno ripercussioni sull'elaborazione della richiesta.
    - *Disabilitato*: L'istanza di policy è disabilitata.
  - *Ridefinisci Valori di Soglia*: Attivando questa opzione sarà possibile utilizzare una soglia per l'istanza di policy differente rispetto a quella prevista dalla policy d'origine.

- *Filtro*: Abilitando questa sezione dell'istanza di policy è possibile indicare i criteri per stabilire quali richieste, in entrata sul gateway, sono soggette alla policy che si sta istanziando. In assenza di filtro, l'istanza della policy sarà valutata su tutte le richieste in ingresso.

  Per la creazione del filtro sono disponibili i seguenti campi (Figura 57):

  - *Stato*: Opzione per abilitare/disabilitare il filtro.
  - *Ruolo Gateway*: Opzione per filtrare le richieste di servizio in base al ruolo ricoperto dal gateway nella specifica richiesta: Fruitore o Erogatore.
  - *Modalità*: Opzione per filtrare le richieste di servizio in base alla modalità operativa. Nel caso si sia selezionata una singola modalità (o se il gateway supporta una sola modalità) viene visualizzato il valore attuale in modo non modificabile.
  - *Ruolo Erogatore*: Opzione per filtrare le richieste di servizio in base al ruolo posseduto dal soggetto erogatore. Tramite la lista è possibile selezionare uno tra i ruoli censiti nel registro. La selezione di un ruolo esclude la possibilità di selezionare un soggetto erogatore.
  - *Soggetto Erogatore*: Opzione per filtrare le richieste di servizio in base al soggetto erogatore. Tramite la lista è possibile selezionare uno tra i soggetti censiti nel registro. La selezione di un soggetto esclude la possibilità di selezionare un ruolo erogatore.
  - *Servizio*: Opzione per filtrare le richieste di servizio in base al servizio invocato. Tramite la lista è possibile selezionare uno tra i servizi censiti nel registro. Se è stato selezionato un soggetto erogatore, saranno elencati solo i servizi da esso erogati. Analogamente, se è stata selezionata una modalità, saranno elencati solo i servizi appartenenti a quella modalità.
  - *Azione*: Opzione per filtrare le richieste di servizio in base all'azione invocata. Tramite la lista è possibile selezionare una tra le azioni censite nel registro. Se è stato selezionato un servizio, saranno elencati solo le azioni ad esso appartenenti.
  - *Applicativo Erogatore*: Opzione per filtrare le richieste di servizio in base all'applicativo erogatore (opzione non disponibile nel caso di una fruizione). Tramite la lista è possibile selezionare uno tra gli applicativi censiti nel registro. Se sono stati selezionati servizi e/o soggetti, la lista presentata sarà filtrata di conseguenza.
  - *Ruolo Fruitore*: Opzione per filtrare le richieste di servizio in base al ruolo posseduto dal soggetto fruitore. Tramite la lista è possibile selezionare uno tra i ruoli censiti nel registro. La selezione di un ruolo esclude la possibilità di selezionare un soggetto fruitore.
  - *Soggetto Fruitore*: Opzione per filtrare le richieste di servizio in base al soggetto fruitore. Tramite la lista è possibile selezionare uno tra i soggetti censiti nel registro. Se è stato selezionato un servizio, saranno elencati solo i soggetti fruitori del medesimo. La selezione di un soggetto esclude la possibilità di selezionare un ruolo fruitore.
  - *Applicativo Fruitore*: Opzione per filtrare le richieste di servizio in base all'applicativo fruitore (opzione non disponibile nel caso di una erogazione). Tramite la lista è possibile selezionare uno tra i servizi applicativi censiti nel registro. Se sono stati selezionati servizi e/o soggetti, la lista presentata sarà filtrata di conseguenza.
  - *Filtro per Chiave*: Si tratta di un'opzione avanzata che consente di filtrare le richieste in ingresso sul gateway base ad una chiave che può essere specificata in maniera personalizzata effettuando una delle seguenti scelte per il campo *Tipologia*:
    - *HeaderBased*: Occorre fornire i dati "Nome" e "Valore". La policy si applicherà soltanto alle richieste che hanno, nell'header di trasporto, una proprietà che corrisponde.
    - *URLBased*: Occorre fornire i dati "Espressione Regolare" e "Valore". La policy si applicherà soltanto alle richieste ove, applicando l'espressione regolare alla URL di invocazione, si ottiene un valore identico a quello fornito.
    - *FormBased*: Occorre fornire i dati "Nome" e "Valore". La policy si applicherà soltanto alle richieste che contengono nella query string un parametro corrispondente ai dati forniti.
    - *SOAPActionBased*: Occorre fornire il dato "Valore". + La policy si applicherà soltanto alle richieste che si presentano con una SOAPAction avente il valore fornito.
    - *ContentBased*: Occorre fornire i dati "Espressione XPath" e "Valore". La policy si applicherà soltanto alle richieste dove, applicando l'espressione XPath al messaggio di richiesta, si ottiene un valore identico a quello fornito.

* *PluginBased*: Occorre fonire i dati “Tipo Personalizzato” e “Valore”. Il parametro “Tipo Personalizzato” è una chiave, registrata nella configurazione, cui corrisponde una classe java che restituisce un valore da confrontare con quello fornito. Per realizzare un plugin con una logica di filtro personalizzata è necessario fornire un’implementazione della seguente interfaccia:

```
package org.openspcoop2.pdd.core.controllo_traffico.plugins;
public interface IRateLimiting {
  public String estraiValoreFiltro(Logger log,Dati datiRichiesta) throws ↩
      PluginsException;
  public String estraiValoreCollezionamentoDati(Logger log,Dati datiRichiesta) throws ↩
      PluginsException;
}
```

La classe realizzata viene successivamente registrata tramite una entry nel file *className.properties* di GovWay:

```
org.openspcoop2.pdd.controlloTraffico.rateLimiting.test=<fully qualified class name>
```

La stringa <nome>, fornita in configurazione, diventa utilizzabile come “Tipo Personalizzato”.

Nota
È possibile specificare più di un criterio di filtro; la logica applicata sarà quella dell’operatore AND.

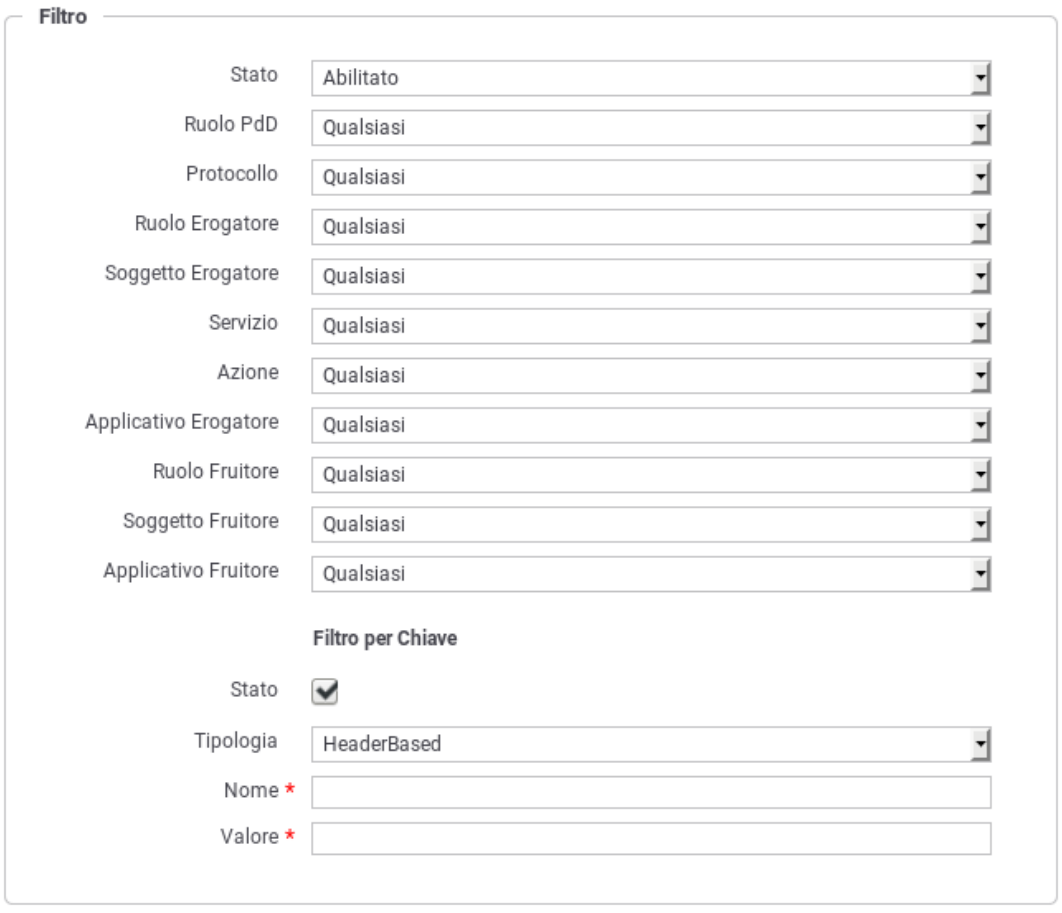


Figura 57: Definizione del filtro per l’istanza della policy di rate limiting

- *Criterio di Collezionamento dei Dati*: In questa sezione è possibile attivare opzionalmente alcuni criteri per il raggruppamento dei dati utilizzati come indicatori di confronto per l’applicabilità della policy. Ad esempio se si è attivata una policy che limita

a 20 il numero di richieste su una finestra di 5 minuti, significa che al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, si otterrà una violazione della policy.

Aggiungendo un criterio di collezionamento per Soggetto Erogatore, saranno conteggiate separatamente le richieste destinate ad ogni singolo soggetto erogatore. In questo caso la policy risulterà violata solo al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, destinata al medesimo soggetto erogatore.

È ammesso anche il raggruppamento su criteri multipli. La logica è del tutto analoga a quella dell'operatore GROUP BY del linguaggio SQL.

I criteri di raggruppamento selezionabili sono (Figura 58):

- *Ruolo (Fruitore/Erogatore)*
- *Soggetto Erogatore*
- *Servizio*
- *Azione*
- *Applicativo Erogatore*
- *Soggetto Fruitore*
- *Applicativo Fruitore*
- *Raggruppamento per Chiave*: le richieste saranno raggruppate in base al valore di una chiave personalizzata il cui valore viene fornito secondo uno dei metodi selezionati tra i seguenti:
  - *HeaderBased*: La chiave è presente nell'header di trasporto indicato nella proprietà "Nome".
  - *URLBased*: La chiave è presente nella URL ricavandola tramite l'espressione regolare fornita nell'elemento seguente.
  - *FormBased*: La chiave viene fornita in modalità Form Encoded con il parametro indicato nell'elemento "Nome".
  - *SOAPActionBased*: La chiave corrisponde al valore della SoapAction.
  - *ContentBased*: La chiave è presente nel body del messaggio e viene ricavata tramite il valore Xpath fornito nell'elemento seguente.
  - *PluginBased*: La chiave viene restituita tramite l'esecuzione di una classe il cui nome viene fornito con il campo "Tipo Personalizzato"

Figura 58: Definizione del filtro per l'istanza della policy di rate limiting

7.3.3.3 Visualizzazione Statistiche Policy

Quando una policy è attivata si ha la possibilità di accedere ad una finestra che fornisce una sintesi dei dati statistici legati all'applicazione della policy in fase di controllo del traffico.

Per visualizzare questa finestra è sufficiente accedere all'elenco delle policy attivate ed utilizzare il collegamento "Visualizza" nella colonna "Runtime" (Figura 59).

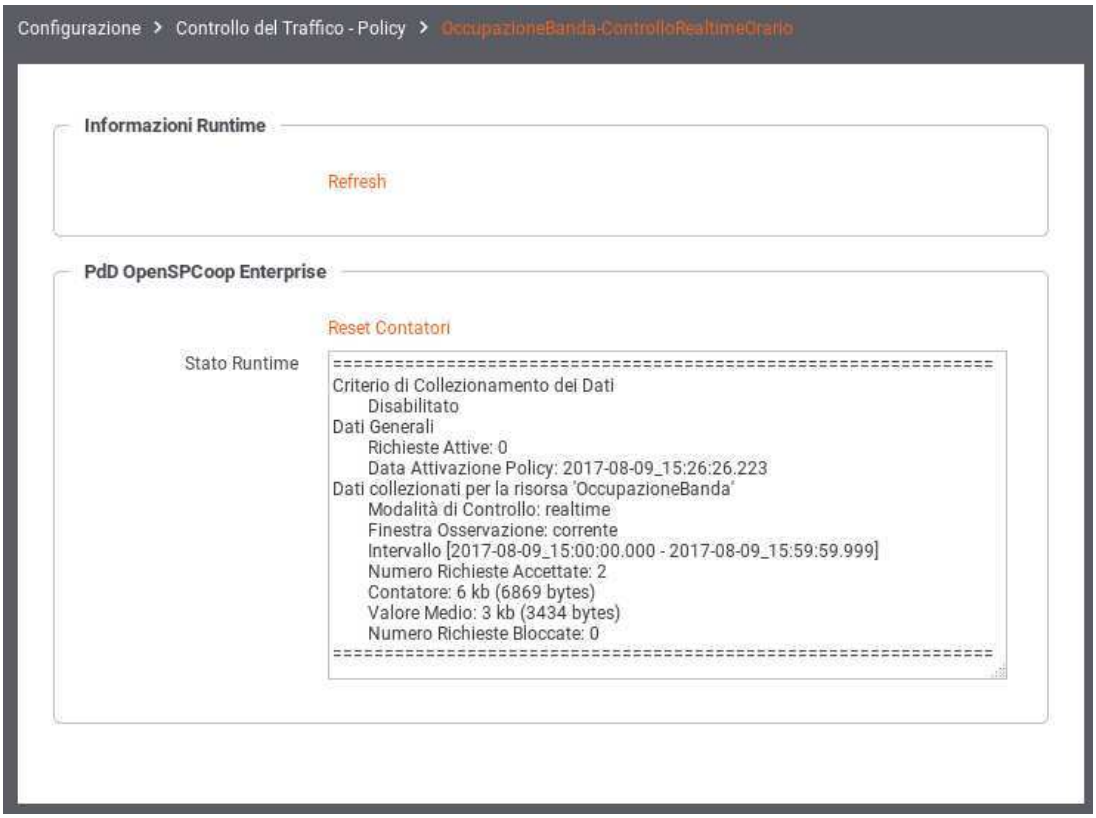


Figura 59: Dati statistici relativi ad una policy di rate limiting

Si noti che saranno visualizzati dei dati solo dopo la data di attivazione della policy e cioè dopo che è transitata la prima richiesta cui viene applicata la policy.

I dati statistici riportati sono i seguenti:

- *Criterio di Collezionamento dei dati*: I criteri di raggruppamento utilizzati dalla policy.
- *Dati Generali*:
  - *Il numero istantaneo delle richieste attive*
  - *la data di attivazione della policy (che corrisponde alla data di primo utilizzo della medesima)*
- *Dati collezionati per la risorsa <nomeRisorsa>*: dati di sintesi sulle transazioni cui è stata applicata la policy.

Sono inoltre disponibili i seguenti collegamenti:

- *Refresh*: per aggiornare i dati visualizzati.
- *Reset Contatori*: per azzerare i valori visualizzati (solo nella modalità di controllo realtime).

7.3.4 Tempi Risposta

In questa sezione vengono indicati i valori limite di default riguardo i tempi di risposta dei servizi con cui il gateway interagisce durante l'elaborazione delle richieste. Nel caso delle erogazioni, si tratta dei tempi di risposta dei servizi interni, successivamente ad una richiesta di erogazione dall'esterno. Nel caso delle fruizioni, si tratta dei tempi di risposta dei servizi esterni, successivamente ad una richiesta di fruizione da parte di un client interno al dominio. I tempi configurabili sono:

- *Connection Timeout (ms)*: Intervallo di tempo atteso, sulle comunicazioni in uscita, prima di sollevare l'errore Connection Timeout (scadenza del tempo di attesa per stabilire una connessione).
- *Read Timeout (ms)*: Intervallo di tempo atteso, dopo aver stabilito una connessione in uscita, prima di sollevare l'errore di Read Timeout (scadenza del tempo di attesa per ricevere il payload dall'interlocutore).
- *Tempo Medio di Risposta (ms)*: Valore di soglia del tempo medio di risposta al fine di valutare la situazione di *Degrado Prestazionale*, condizione per l'applicabilità di eventuali politiche restrittive come documentate più avanti.

7.4 Token Policy

Per poter definire politiche di controllo degli accessi basate sui Bearer Token è necessario creare delle Token Policy da riferire nelle configurazioni degli specifici servizi. La gestione delle Token Policy si effettua andando alla sezione *Configurazione* > *Token Policy* della govwayConsole. Per creare una nuova policy si utilizza il pulsante *Aggiungi*. Il form di creazione appare inizialmente come quello illustrato in Figura 60

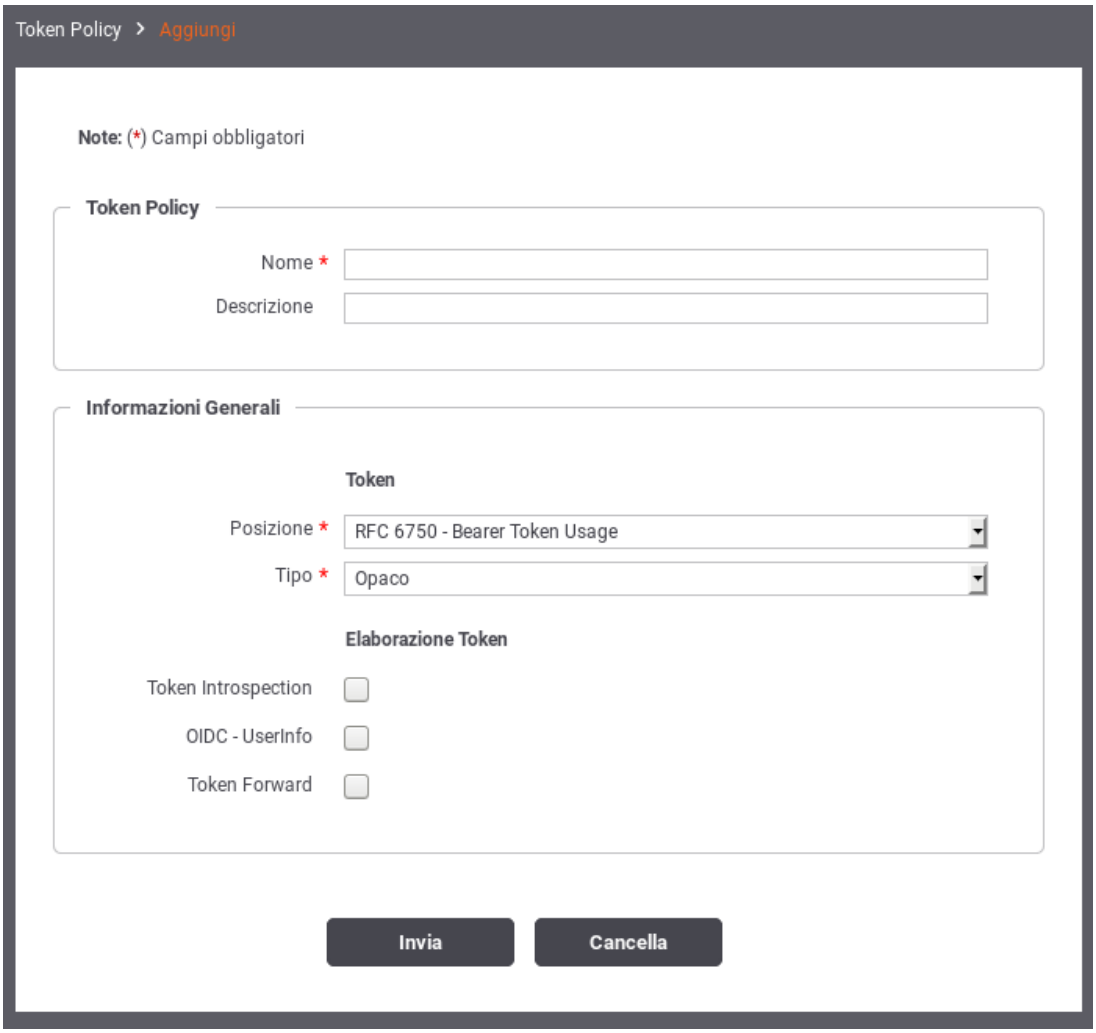


Figura 60: Informazioni generali di una Token Policy

Inizialmente si inseriscono i dati identificativi:

- *Nome*: nome univoco da assegnare alla policy
- *Descrizione*: testo di descrizione generale della policy

Al passo successivo si inseriscono le Informazioni Generali. Nella sezione *Token* si specifica il tipo di token accettato e il metodo di passaggio:

- *Posizione*: indica la modalità di passaggio del token da parte dell'applicativo richiedente. I valori possibili sono:
  - *RFC 6750 - Bearer Token Usage*: la modalità di passaggio del token è una qualsiasi delle tre previste dallo standard RFC 6750 (le tre opzioni successive a questa).
  - *RFC 6750 - Bearer Token Usage (Authorization Request Header Field)*: la modalità di passaggio del token è quella che prevede l'inserimento nell'header "Authorization" del messaggio di richiesta. Ad esempio:

    ```
    GET /resource HTTP/1.1
    Host: server.example.com
    Authorization: Bearer mF_9.B5f-4.1JqM
    ```

  - *RFC 6750 - Bearer Token Usage (Form-Encoded Body Parameter)*: la modalità di passaggio del token è quella di inserirlo nel body della richiesta, eseguita con una POST, utilizzando il parametro *access_token*, come ad esempio:

    ```
    POST /resource HTTP/1.1
    Host: server.example.com
    Content-Type: application/x-www-form-urlencoded

    access_token=mF_9.B5f-4.1JqM
    ```

  - *RFC 6750 - Bearer Token Usage (URI Query Parameter)*: la modalità di passaggio del token è quella di utilizzare il parametro *access_token* della Query String, come ad esempio:

    ```
    GET /resource?access_token=mF_9.B5f-4.1JqM HTTP/1.1
    Host: server.example.com
    ```

  - *Header HTTP*: la modalità di passaggio del token è quella di inserirlo in un header http custom, il cui nome deve essere fornito nel campo *Nome Header Http*, che appare di seguito.
  - *Parametro URL*: la modalità di passaggio del token è quella di inserirlo in un parametro custom della query string. Il nome del parametro deve essere fornito nel campo *Nome Parametro URL*, che appare di seguito.
- *Tipo*: specifica il tipo di token che il gateway attende di ricevere. I valori possibili sono:
  - *JWS*: un JSON Web Token di tipo "Signed".
  - *JWE*: un JSON Web Token di tipo "Encrypt".
  - *Opaco*: un generico token di tipo non specificato.

Nella sezione *Elaborazione Token* si specificano le azioni che si possono compiere durante la fase di elaborazione del token ricevuto. Le opzioni disponibili sono:

- Validazione JWT
- Token Introspection
- OIDC - UserInfo
- Token Forward

Le sezioni successive dettagliano questi elementi.

7.4.1 Validazione JWT

Nel caso in cui il token sia di tipo JWT (quindi JWE o JWS), questa opzione attiva la validazione basata su tale standard (Figura 61).

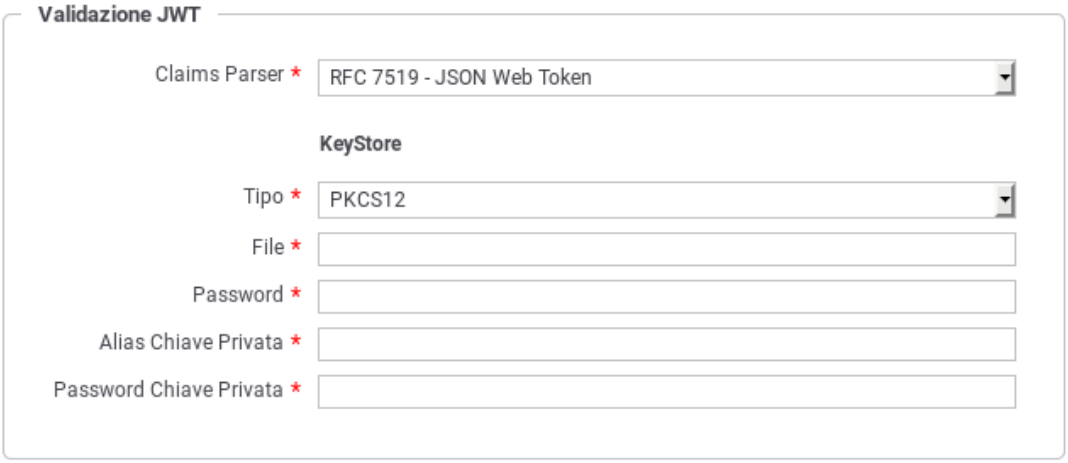


Figura 61: Dati di configurazione della validazione JWT

I dati da inserire sono:

- *Claims Parser*: indica il tipo di parser che deve essere utilizzato per la validazione del token JWT. I valori possibili sono:
  - *RFC 7519 - JSON Web Token*
  - *OpenID Connect - ID Token*
  - *Google - ID Token*
  - *Personalizzato*: nel caso del parser personalizzato occorre fornire il relativo ClassName della classe con la logica di parsing.
- *KeyStore*: I parametri di configurazione del keystore da utilizzare per il servizio di validazione.

7.4.2 Token Introspection

Questa sezione consente di attivare la validazione del token ricevuto attraverso un servizio di Token Introspection i cui dati di accesso devono essere forniti in questo contesto (Figura 62).

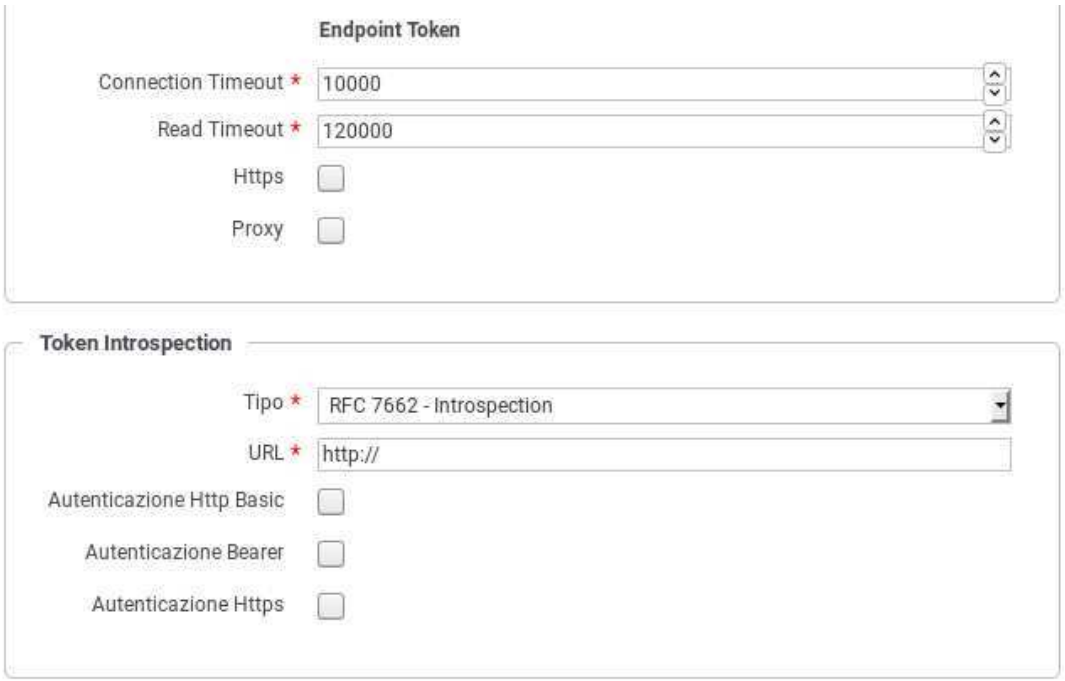


Figura 62: Dati di puntamento al servizio di Token Instrospection

Per il corretto puntamento al servizio di Token Introspection devono essere forniti in prima istanza i parametri generali legati all'endpoint riferito:

- *Connection Timeout*: Tempo massimo in millisecondi di attesa per stabilire una connessione con il server di validazione token.
- *Read Timeout*: Tempo massimo in millisecondi di attesa per la ricezione di una risposta dal server di validazione token.
- *Https*: Parametri di configurazione nel caso in cui il server di validazione token richieda un accesso Https.
- *Proxy*: Parametri di configurazione nel caso in cui il server di validazione token richieda l'uso di un proxy per l'accesso.

Successivamente devono essere forniti i dati di configurazione specifici del servizio di Token Introspection:

- *Tipo*: tipologia del servizio. A scelta tra i seguenti valori:
  - *RFC 7662 - Introspection*: Servizio di introspection conforme allo standard RFC 7662. Richiede che vengano forniti i seguenti dati:
    - *URL*: endpoint del servizio di introspection.
    - *Autenticazione Http Basic*: flag da attivare nel caso in cui il servizio di introspection richieda autenticazione di tipo HTTP-BASIC. In questo caso dovranno essere forniti Username e Password nei campi successivi.
    - *Autenticazione Bearer*: flag da attivare nel caso in cui il servizio di introspection richieda autenticazione tramite un token. Quest'ultimo dovrà essere indicato nel campo seguente.
    - *Autenticazione Https*: flag da attivare nel caso in cui il servizio di introspection richieda autenticazione di tipo Https. In questo caso dovranno essere forniti tutti i dati di configurazione nei campi seguenti.
  - *Google - TokenInfo*: Riferimento al servizio di token introspection di Google. L'unico campo da fornire in questo caso è la URL del servizio. Il sistema precompila questo campo con il valore di default *https://www.googleapis.com/oauth2/v3/tokeninfo*.
  - *Personalizzato*: Questa opzione consente di configurare un servizio di Token Introspection personalizzato (Figura 63).

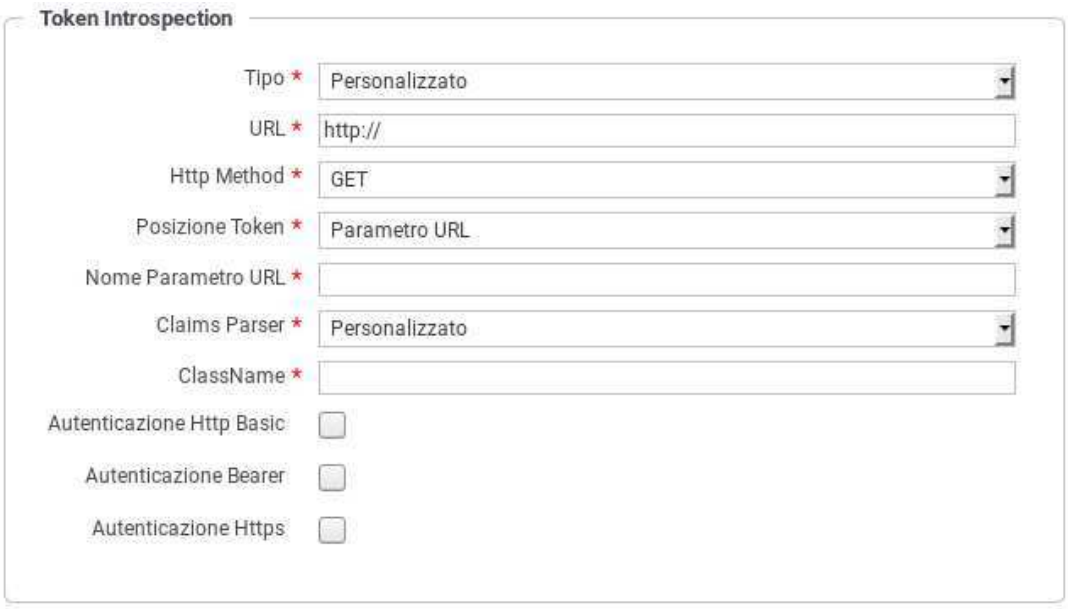


Figura 63: Configurazione personalizzata del servizio di Token Instrospection

I dati da fornire sono:

- *URL*: la URL del servizio di introspection.
- *Http Method*: Il metodo HTTP che deve essere utilizzato per la chiamata al servizio di introspection.
- *Posizione Token*: Il metodo di passaggio del token al servizio di introspection. Sono supportati i classici metodi: HTTP Authorization Bearer, Header HTTP, Parametro URL e Parametro Form-Encoded Body. Negli ultimi tre casi sarà necessario fornire il nome dell'header o del parametro.
- *Claims Parser*: Il metodo di parsing dei claims che vengono restituiti dal servizio di introspection. I valori possibili sono: RFC 7662 - Introspection, Google - TokenInfo e Personalizzato. In quest'ultimo caso si dovrà fornire il ClassName della classe contenente la logica di parsing.
- *Autenticazione*: Analogamente a quanto visto in precedenza è necessario indicare con il flag opportuno il tipo di autenticazione richiesta dal servizio di introspection personalizzato.

7.4.3 OIDC - UserInfo

Sezione per attivare la richiesta al servizio di UserInfo per ottenere i dati inerenti l'utente possessore del token ricevuto (Figura 64).

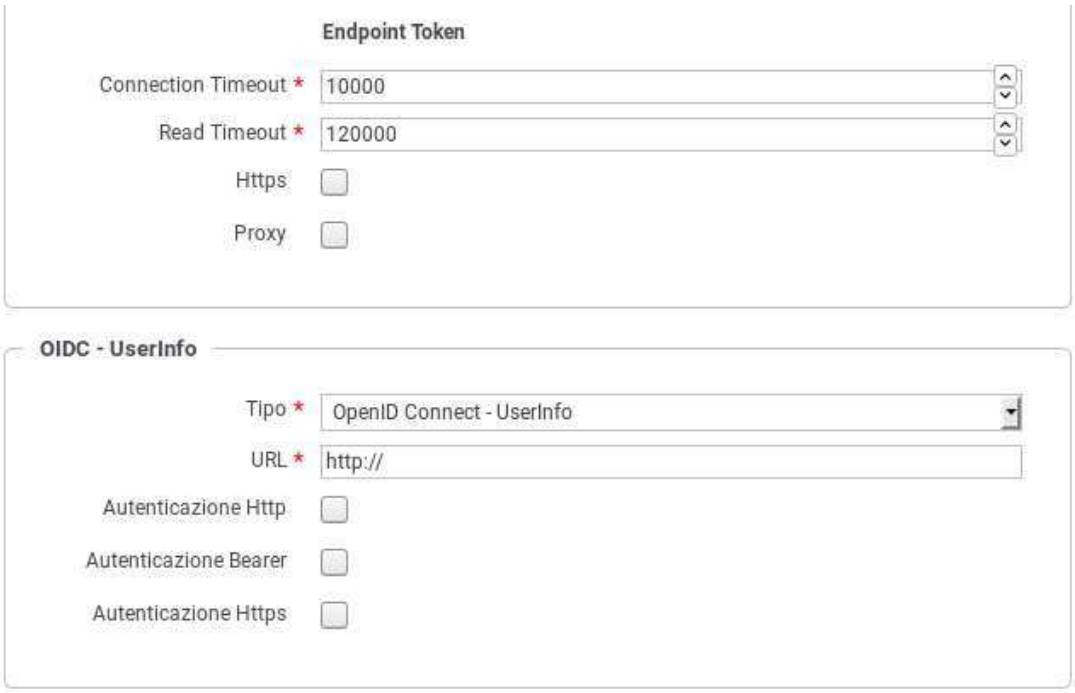


Figura 64: Dati di puntamento al servizio di UserInfo

Per il corretto puntamento al servizio di UserInfo devono essere forniti in prima istanza i parametri generali legati all'endpoint riferito, che sono in comune con quelli del servizio di Token Introspection, e quindi già descritti in precedenza.

Successivamente si dovranno fornire i dati di configurazione specifici per il servizio UserInfo, che sono:

- *Tipo*: Si seleziona il tipo di servizio UserInfo riferito. I valori possibili sono:
  - *OpenID Connect - UserInfo*: servizio di UserInfo standard OpenID Connect.
  - *Google - UserInfo*: servizio UserInfo di Google. La URL di default del servizio viene inserita automaticamente.
  - *Personalizzato*: si consente di fornire i dati di configurazione di un servizio personalizzato di UserInfo. I dati di configurazione sono gli stessi già descritti nel caso della configurazione del servizio di Token Introspection personalizzato.
- *URL*: La URL del servizio di UserInfo.
- *Autenticazione*: La configurazione del metodo di autenticazione, quando applicabile.

7.4.4 Token Forward

Azione di elaborazione che consiste nell'inoltro del token ricevuto al destinatario. Una volta attivata questa opzione, devono essere indicate le seguenti informazioni:

- *Originale*: opzione che consente di inoltrare il token originale al destinatario. Attivando questo flag è necessario specificare la modalità di inoltro a scelta tra le seguenti opzioni:
  - *Come è stato ricevuto*: Il token viene inoltrato al destinatario utilizzando lo stesso metodo con cui è stato ricevuto dal gateway.
  - *RFC 6750 - Bearer Token Usage (Authorization Request Header Field)*: Il token viene inoltrato al destinatario utilizzando l'header Authorization presente nella richiesta HTTP.
  - *RFC 6750 - Bearer Token Usage (URI Query Parameter)*: Il token viene inoltrato al destinatario tramite parametro access_token della Query String.

  - *Header HTTP*: : Il token viene inoltrato al destinatario utilizzando un header HTTP il cui nome deve essere specificato nel campo seguente.
  - *Parametro URL* Il token viene inoltrato al destinatario utilizzando un parametro della Query String il cui nome deve essere specificato nel campo seguente.

- *Informazioni Raccolte*: opzione disponibile quando è stata abilitata una delle azioni di validazione del token (introspection, user info o validazione JWT), consente di veicolare i dati ottenuti dal servizio di validazione, al destinatario. Una volta attivato il flag è necessario specificare la modalità di inoltro dei dati selezionando una tra le opzioni seguenti:

  - *GovWay Headers*: I dati raccolti dal token vengono inseriti nei seguenti header HTTP:

```
GovWay-Token-Issuer
GovWay-Token-Subject
GovWay-Token-Username
GovWay-Token-Audience
GovWay-Token-ClientId
GovWay-Token-IssuedAt
GovWay-Token-Expire
GovWay-Token-NotToBeUsedBefore
GovWay-Token-Scopes
GovWay-Token-FullName
GovWay-Token-FirstName
GovWay-Token-MiddleName
GovWay-Token-FamilyName
GovWay-Token-EMail
```

  - *GovWay JSON*: I dati raccolti dal token vengono inseriti in un oggetto JSON, il cui JsonSchema è il seguente:

```
{
    "required" : [ "id" ],
    "properties": {
        "id": {"type": "string"},
        "issuer": {"type": "string"},
  "subject": {"type": "string"},
  "username": {"type": "string"},
  "audience": {"type": "string"},
  "clientId": {"type": "string"},
  "iat": {
            "type": "string",
            "format": "date-time"
        },
  "expire": {
            "type": "string",
            "format": "date-time"
        },
  "expire": {
            "type": "string",
            "format": "date-time"
        },
        "roles": {
            "type": "array",
            "items": {"type": "string"}
        },
        "scope": {
            "type": "array",
            "items": {"type": "string"}
        },
  "userInfo": {
    "type": "object",
    "properties": {
      "fullName": {"type": "string"},
      "firstName": {"type": "string"},
```

```
      "middleName": {"type": "string"},
      "familyName": {"type": "string"},
      "email": {"type": "string"},
    },
    "additionalProperties": false
  }
    },
    "additionalProperties": false
}
```

Il JSON risultante viene inserito nell'Header HTTP *GovWay-Token*.

– *GovWay JWS*: I dati raccolti dal token vengono inseriti in un oggetto JSON, come descritto al punto precedente. In questo caso il token JSON viene inserito successivamente in un JWT e quindi firmato. Il JWS risultante viene inserito nell'Header HTTP *GovWay-JWT*.

– *JSON*: Le informazioni ottenute dai servizi di introspection, userinfo o il json estratto dal token jwt dopo la validazione, vengono inseriti negli header http o proprietà delle url indicati.

> **Nota**
> Le informazioni sono esattamente quelle recuperate dai servizi originali (o presenti nel token originale nel caso di validazione jwt).

– *JWS/JWE*: Uguale alla modalità JSON con la differenza che negli header http, o nelle proprietà delle url, vengono inseriti dei JWT firmati (caso JWS) o cifrati (caso JWE) contenenti al loro interno il JSON.

7.5 Utenti

La sezione *Configurazione* > *Utenti* è dedicata alla gestione degli utenti dei cruscotti grafici govwayConsole e govwayMonitor.

Prima di descrivere le funzionalità relative alla gestione utenti è necessario fare una premessa sull'organizzazione dei permessi che sono assegnabili ad un utente.

Le funzionalità delle console grafiche sono partizionate in gruppi cui corrispondono puntuali permessi che possono essere concessi agli utenti per limitarne l'operatività. Vediamo quali sono i gruppi funzionali, e conseguentemente i permessi associabili a ciascun utente:

- *[U]* - Possibilità di gestire gli utenti delle console. Gli utenti con questo permesso, sono di fatto dei superutenti in quanto possono assumere l'identità di un qualunque utente del sistema.
- *[S]* - Gestione delle entità di configurazione dei servizi, quali: API, Erogazioni, Fruizioni, ecc.
- *[P]* - Gestione delle entità di configurazione degli Accordi di Cooperazione e Servizi Composti.
- *[D]* - Accesso alle funzionalità della console govwayMonitor.
- *[C]* - Accesso alle funzionalità di configurazione. Queste funzionalità sono quelle presenti nel menu di navigazione nel gruppo *Configurazione* e riguardano: tracciamento, controllo del traffico, import-export, ecc.
- *[M]* - Accesso alle code messaggi sul gateway. Questa autorizzazione consente ad esempio di consultare i messaggi presenti nelle Message Box dell'Integration Manager ed eventualmente effettuare delle rimozioni.
- *[A]* - Accesso alle funzionalità di consultazione delle tracce del servizio di Auditing.

L'applicazione, al termine dell'installazione, contiene una utenza (credenziali indicate durante l'esecuzione dell'installer) che permette di effettuare tutte le principali operazioni di gestione.

Gli utenti in possesso del permesso [U] possono creare dei nuovi utenti. La maschera di creazione di un nuovo utente è quella mostrata in Figura 65.

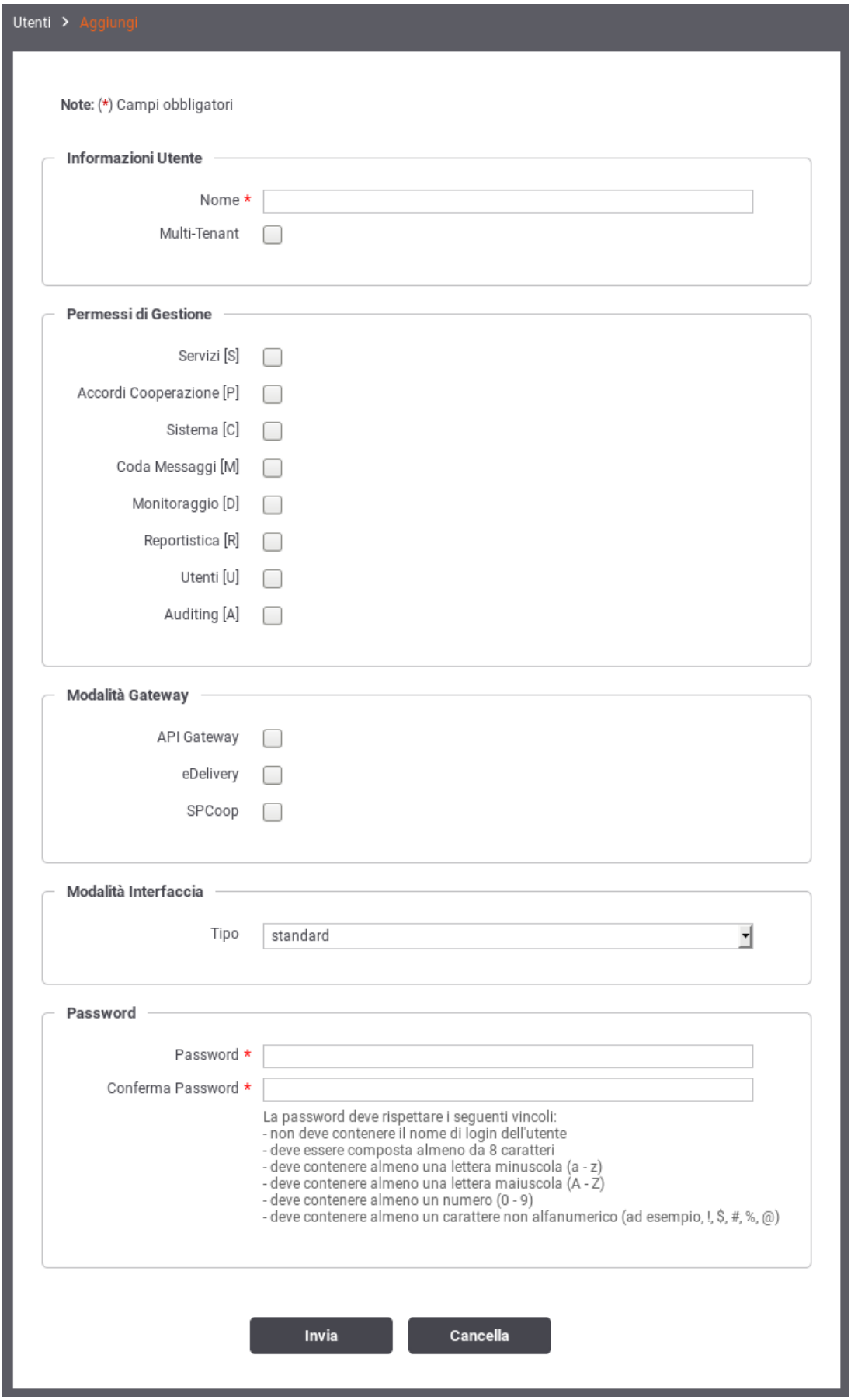


Figura 65: Creazione nuovo utente

Le informazioni da inserire sono:

- *Informazioni Utente*
  - *Nome*
  - *Multi-Tenant*: opzione per creare un utente che opera sulle console in una modalità che prevede la gestione contemporanea di più di un soggetto interno.
- *Permessi di Gestione*: sezione che consente di assegnare i permessi all'utente e quindi decidere quali funzionalità rendergli accessibili.
- *Modalità Gateway*: sezione che consente di decidere quali, tra le modalità operative disponibili, rendere accessibili all'utente.
- *Modalità Interfaccia*: opzione per decidere quale modalità, tra standard e avanzata, è quella di default per l'utente.
- *Password*: sezione per l'impostazione della password dell'utente.

La pagina indice della sezione Utenti visualizza gli utenti già presenti nel sistema con i relativi permessi e i link per modificarli o assumerne l'identità (Figura 66)

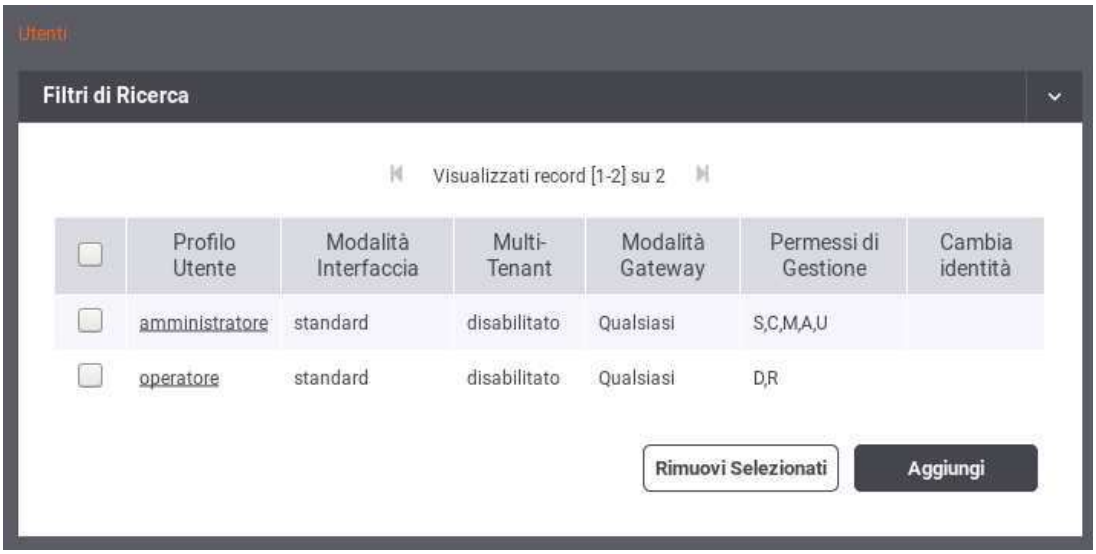


Figura 66: Lista degli utenti

7.6 Importa

L'importazione di entità nel registro può essere effettuata tramite la sezione accessibile con la voce di menu *Importa* presente nella sezione *Configurazione*.

Il form che compare per l'importazione è quello riportato in Figura 67. I passi da eseguire sono i seguenti:

- Selezionare la modalità cui fanno riferimento le entità contenute nell'archivio da importare.
- In base alla modalità selezionata potrebbero essere richieste ulteriori informazioni. Ad esempio, per il protocollo SPCoop, verrà richiesto quale tipo di archivio si vuole importare, a scelta tra:
  - *spcoop*: il formato standard basato sulle specifiche SPCoop
  - *govlet*: il formato di govway. Gli archivi con tale formato sono ottenibili o attraverso un'esportazione effettuabile tramite govwayConsole o scaricando le govlets disponibili sul sito del progetto che permettono di pre-configurare GovWay per uno specifico servizio

- *Validazione Documenti* (disponibile solamente con interfaccia in modalità avanzata, per default è abilitato): Se attivato, questo flag indica che i documenti presenti nell'archivio vengono validati prima di essere importati (es. wsdl, xsd ...).
- *Aggiornamento*: Se attivato, questo flag indica che l'archivio da importare costituisce un aggiornamento del registro attuale.
- Selezionare dal filesystem il file che corrisponde all'archivio che deve essere importato.

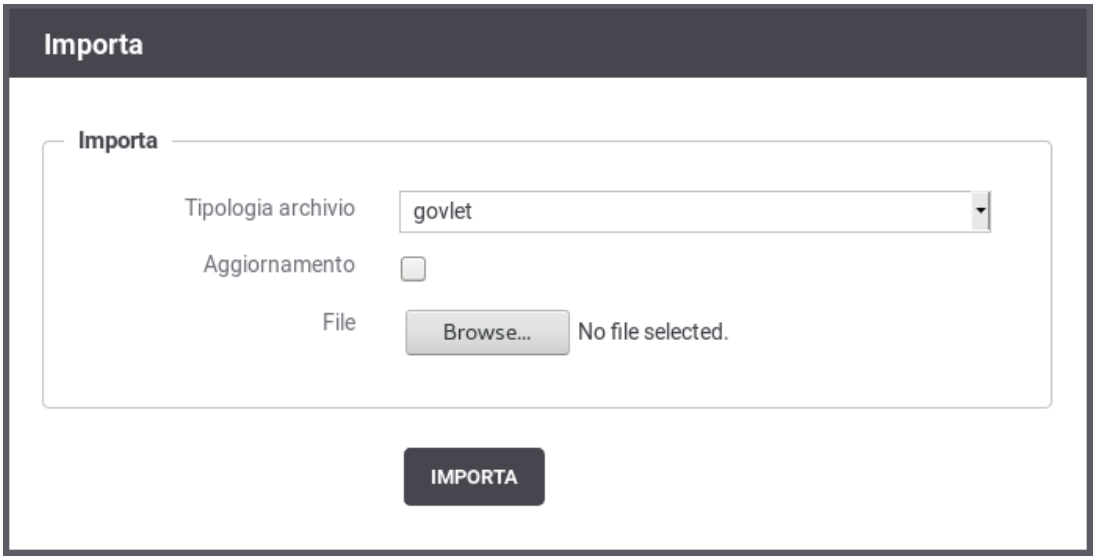


Figura 67: Importazione di entità nel registro

7.7 Esporta

L'esportazione dei dati di configurazione dalla govwayConsole è possibile nei modi seguenti:

- Selezionando singolarmente le entità di configurazione da esportare, come ad esempio "Erogazioni" o "API", e premendo il pulsante *Esporta* (Figura 68).

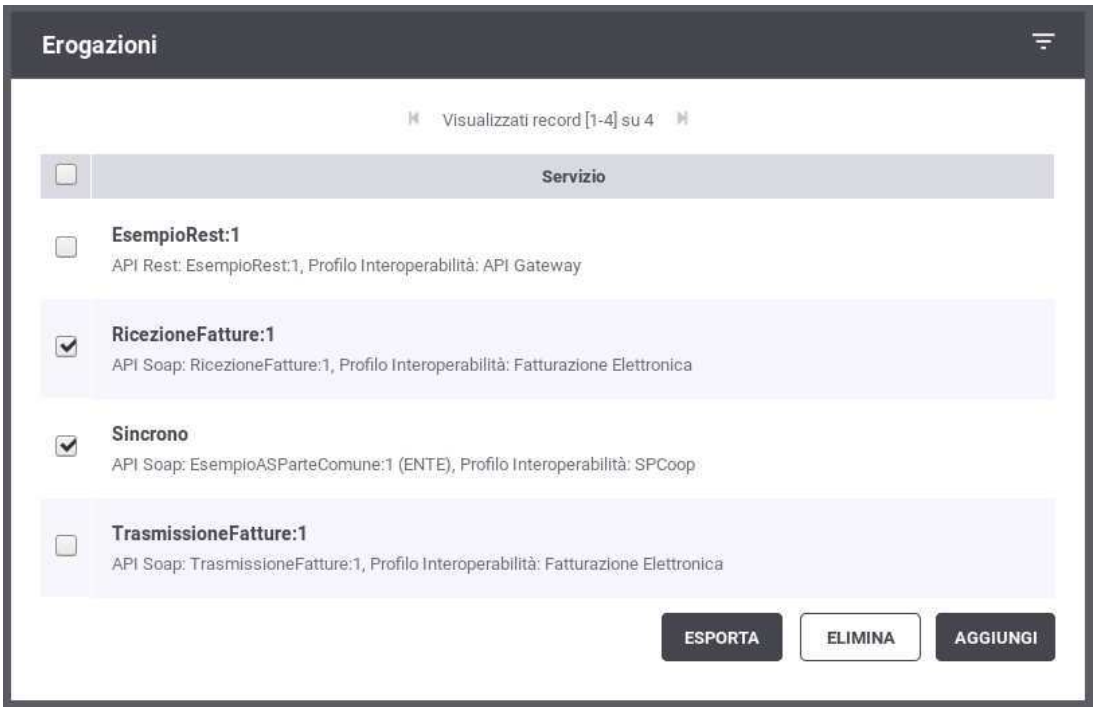


Figura 68: Esportazione di singole entità del registro

Dopo aver selezionato il pulsante "Esporta", una seconda maschera (Figura 69) riporta le seguenti informazioni:

- *Profilo Interoperabilità*: indicazione del profilo cui fa riferimento l'esportazione.
- *Tipologia archivio*: se previsto, fa selezionare la tipologia di archivio da produrre. Il default è il formato *Govlet* standard di esportazione di Govway.
- *Includi elementi riferiti*: include nell'archivio di esportazione anche gli elementi di configurazione riferiti da quelli selezionati.

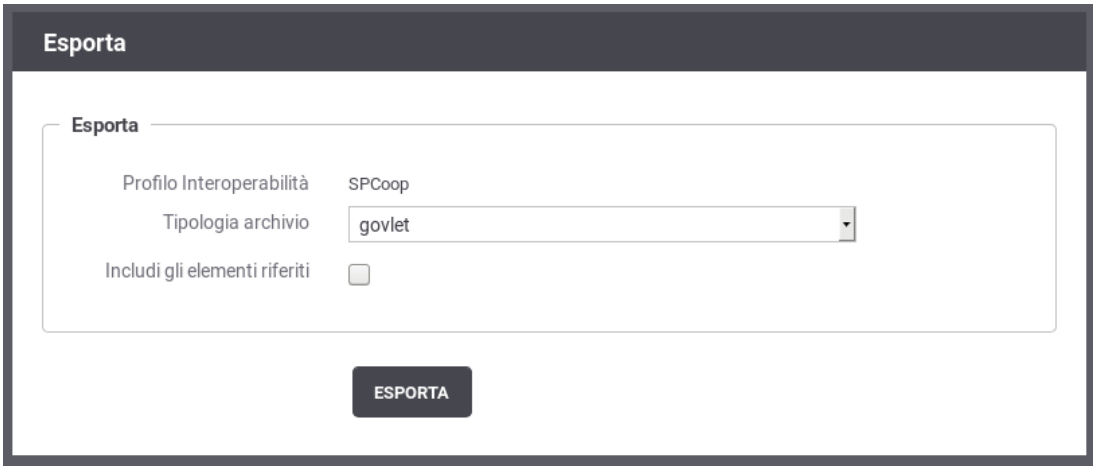


Figura 69: Esportazione di entità nel registro

- Tramite la voce di menu *Configurazione* > *Esporta* che presenta le opzioni mostrate in Figura 70.

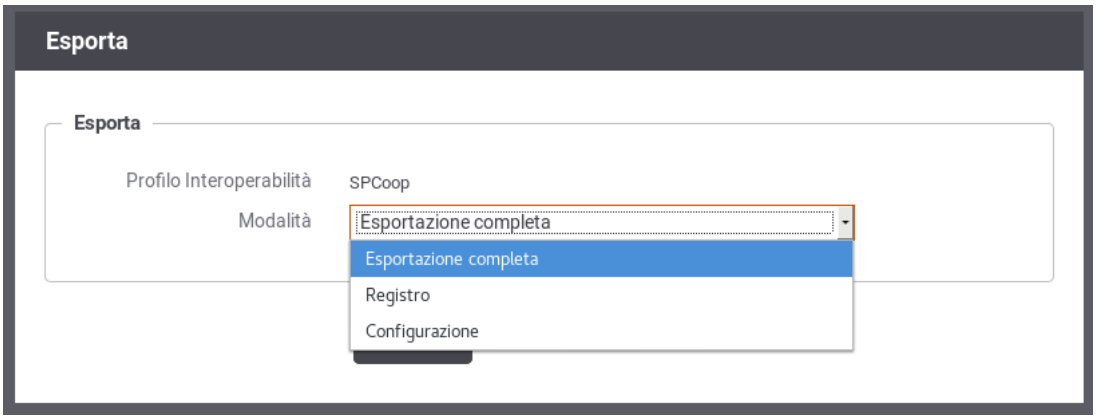


Figura 70: Esportazione di entità nel registro

Le opzioni presenti sono:

- *Profilo Interoperabilità*: indica quale profilo riguarda l'esportazione che si sta effettuando
- *Tipologia Archivio*: nei casi che lo prevedono, consente di specificare il formato dell'archivio di esportazione da produrre.
- *Modalità*: consente di specificare cosa esportare tra le seguenti possibilità:
  - *Esportazione completa*: esportazione dell'intero repository di configurazione (limitatamente al profilo di interoperabilità selezionato, se diverso da "Tutti").
  - *Registro*: esporta solo le entità del registro (erogazioni, fruizioni, api, ecc)
  - *Configurazione*: esporta solo le entità della sezione Configurazione (token policy, tracciamento, ecc).

Il formato dell'archivio prodotto come risultato dell'esportazione dipende dalla modalità cui fanno riferimento le entità selezionate.

7.8 Auditing

In questa sezione descriviamo le modalità di configurazione del servizio di auditing, al fine di definire quali informazioni devono essere tracciate, con che formato e con che livello di dettaglio.

Gli utenti con permesso [C] Configurazione (vedi Sezione 7.5) hanno la possibilità di configurare il servizio di auditing, al fine di stabilire cosa tracciare, con che formato e con che livello di dettaglio.

L'accesso alla funzionalità di configurazione del servizio di auditing avviene tramite la voce *Auditing* nella sezione *Configurazione* del menu laterale sinistro.

Se la maschera si presenta come in Figura 71 il servizio di auditing è disabilitato e quindi nessun dato verrà tracciato.

Figura 71: Servizio di auditing disabilitato

Modificando lo *Stato* del servizio di auditing in **Abilitato** appariranno ulteriori campi nel form (vedi Figura 72) per effettuare le impostazioni.

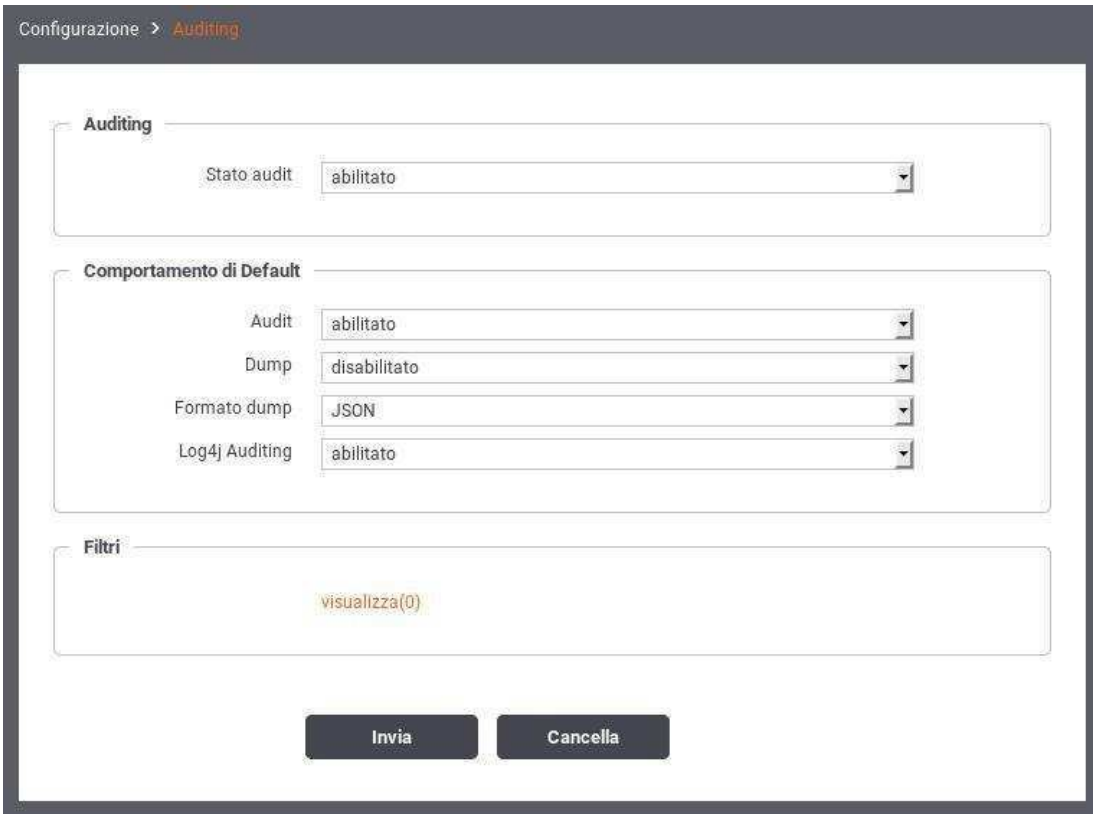


Figura 72: Servizio di auditing abilitato

La configurazione del servizio di auditing avviene tramite la creazione di una lista di **Filtri**, ciascuno dei quali stabilisce un criterio per stabilire se una data informazione deve o non deve essere tracciata. Alle informazioni cui non si applica nessuno dei filtri definiti, viene applicato il comportamento di default, i cui parametri sono presenti nella schermata principale del servizio. Facendo riferimento alla Figura 72 vediamo quali sono i parametri per specificare il comportamento di default:

- **Audit** (abilitato/disabilitato): Se abilitato, tutte le informazioni, cui non risulta applicabile nessuno dei filtri impostati, verranno tracciate dal servizio di auditing.
- **Dump** (abilitato/disabilitato): Questo campo viene preso in considerazione quando *Audit* = *abilitato*. Stabilisce, nei casi in cui non si applica nessun filtro, se oltre a tracciare i campi che descrivono l'operazione, devono essere tracciate anche le strutture dati coinvolte.
- **Formato Dump** (JSON/XML): Stabilisce il formato in cui vengono memorizzate le strutture dati di cui si è scelto di effettuare il dump. Le opzioni possibili sono tra il formato standard JSON (http://www.json.org) e la sua rappresentazione in formato XML.
- **Log4J Auditing** (abilitato/disabilitato): Questa opzione consente di abilitare/disabilitare l'appender log4j relativo ai dati tracciati dal servizio di auditing.

Una volta stabilito il comportamento di default si potranno definire i filtri specifici. Per passare alla sezione di gestione dei filtri si seleziona *Visualizza* nella sezione Filtri. Nell'area di gestione filtri viene mostrata la lista dei filtri esistenti con la possibilità di modificare/cancellare gli esistenti o inserirne di nuovi. Si può aggiungere un nuovo filtro premendo il pulsante *Aggiungi*. In Figura 73 è mostrata la maschera per la creazione di un nuovo filtro di auditing.

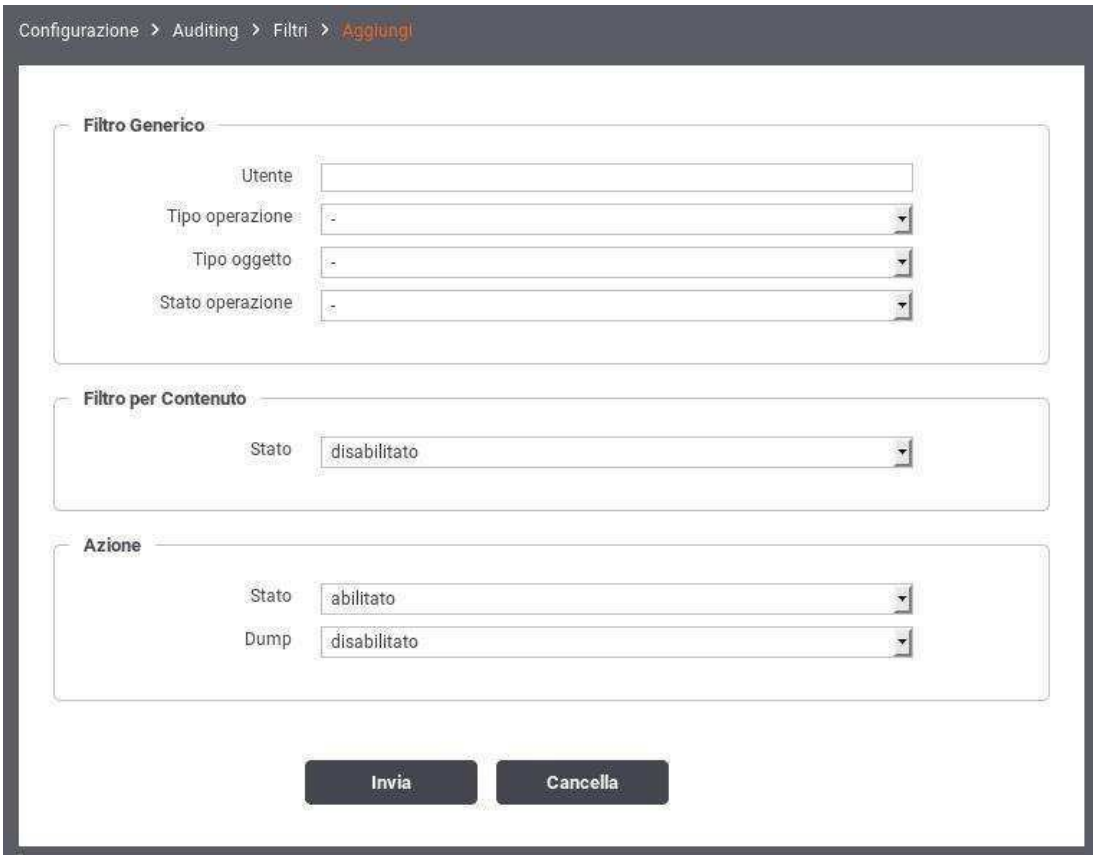


Figura 73: Creazione di un filtro per il servizio di auditing

Facendo riferimento alla Figura 73 vediamo in dettaglio il significato dei campi di un filtro:

- *Filtro Generico*
  - **Utente**: è possibile specificare in questo campo uno username relativo ad un utente della govwayConsole del quale si vogliono tracciare le operazioni effettuate. Lasciare il campo di testo vuoto equivale a *Qualsiasi Utente*
  - **Tipo Operazione** (ADD/CHANGE/DEL): Specifica il tipo di operazione che si vuole tracciare distinguendo tra operazioni di creazione, modifica e cancellazione. Lasciare il campo vuoto equivale a *Qualsiasi Tipo*.
  - **Tipo Oggetto**: Questo campo è costituito da una lista contenente tutte le entità gestibili tramite l'interfaccia govwayConsole (ad esempio: Accordo di Servizio, Porta Delegata, ecc). Consente di restringere il tracciamento alle sole operazioni riguardanti una determinata entità. Lasciare il campo vuoto equivale a *Qualsiasi Tipo Oggetto*.
  - **Stato Operazione** (requesting/error/completed): Consente di restringere le operazioni da tracciare in base al loro stato:
    - *requesting*: indica un'operazione in fase di richiesta e non ancora completata
    - *error*: Indica un'operazione completata che ha restituito un errore
    - *completed*: Indica un'operazione che è terminata correttamente

    Lasciare il campo vuoto equivale a *Qualsiasi Stato Operazione*.
- *Filtro per contenuto*
  - **Stato** (abilitato/disabilitato): Opzione che consente di abilitare il filtro basato sul contenuto degli oggetti coinvolti nell'operazione. Se l'opzione viene abilitata compariranno i 2 campi descritti ai passi successivi.
  - **Tipo** (normale/espressioneRegolare): Descrive se la stringa riportata nel campo Dump deve essere interpretata come pattern o come espressione regolare.

  - **Dump**: Campo di testo per inserire il pattern (o espressione regolare) sulla base del quale verranno filtrate le operazioni. Il sistema di auditing traccerà soltanto le operazioni che coinvolgeranno entità il cui contenuto corrisponde alla stringa specificata.

- *Azione*: indica quale azione deve essere effettuata al verificarsi delle condizioni del filtro
  - **Stato** (abilitato/disabilitato): Se abilitato, al verificarsi delle condizioni impostate nel filtro, i dati dell'operazione verranno tracciati.
  - **Dump** (abilitato/disabilitato): Se *Stato* = *abilitato* è possibile specificare se si deve effettuare anche il dump delle entità coinvolte nell'operazione. Ad esempio, se viene tracciata un'operazione di modifica di un Accordo di Servizio, si decide se si vuole effettuare anche il dump dell'Accordo di Servizio oggetto della modifica.

8 Funzionalità Avanzate

8.1 Configurazione manuale delle interfacce

Nel caso non si disponga del descrittore della API, è possibile in alternativa fornire manualmente la specifica delle interfacce. Dopo aver salvato la nuova API, senza aver fornito il descrittore delle interfacce, si procede individuando il nuovo elemento nella lista delle API presenti e cliccando sul collegamento presente nella colonna *Servizi*, nel caso SOAP, o *Risorse* nel caso REST.

Nel caso SOAP, si procede aggiungendo il nuovo servizio tramite il pulsante *Aggiungi*. Il form da compilare è quello mostrato nella figura seguente.

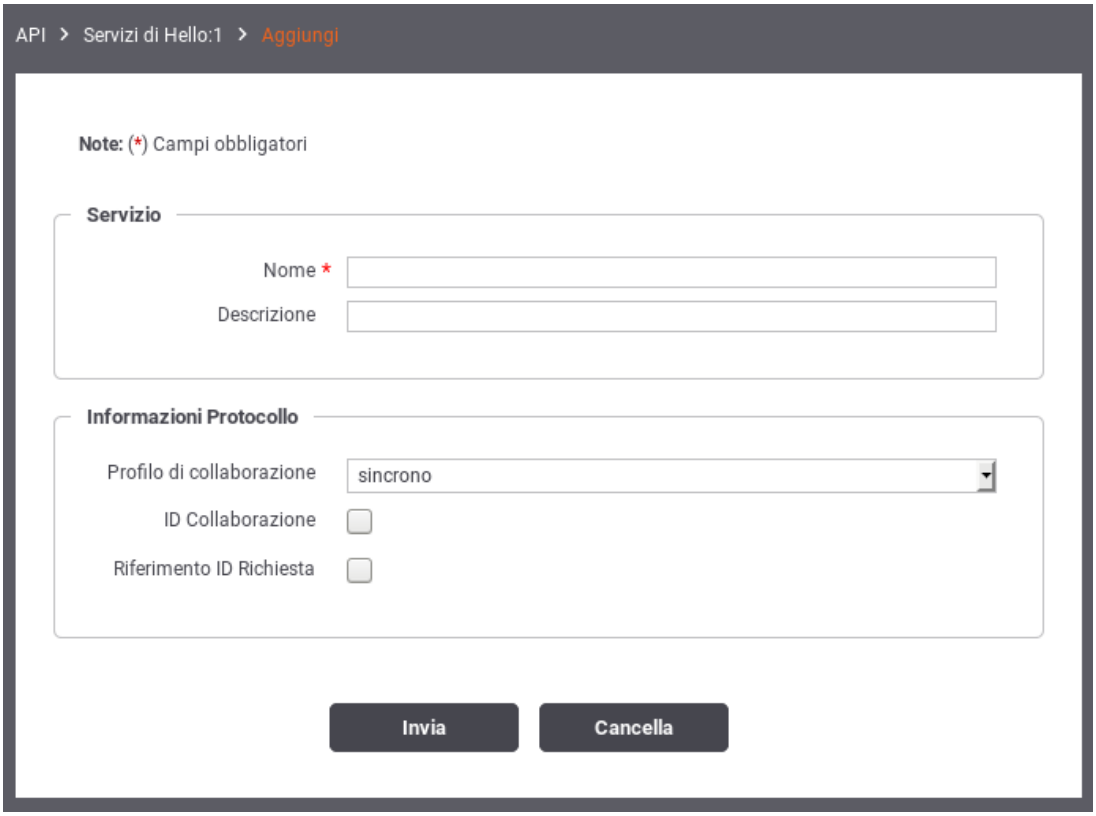


Figura 74: Aggiunta di un servizio alla API SOAP

I dati da fornire sono i seguenti:

- *Nome* del servizio

- *Descrizione* del servizio
- *Profilo di collaborazione* del servizio, a scelta tra oneway e sincrono
- *ID Collaborazione*. Flag per consentire di specificare nelle richieste un valore che identifica una conversazione.
- *Riferimento ID Richiesta*. Flag per consentire di specificare nelle richieste un identificativo relativo ad un messaggio precedente.

Al passo successivo, utilizzando il collegamento nella colonna *Azioni*, relativamente al servizio appena creato, si procede con l'aggiunta delle azioni. Il form da compilare è quello mostrato nella figura seguente.

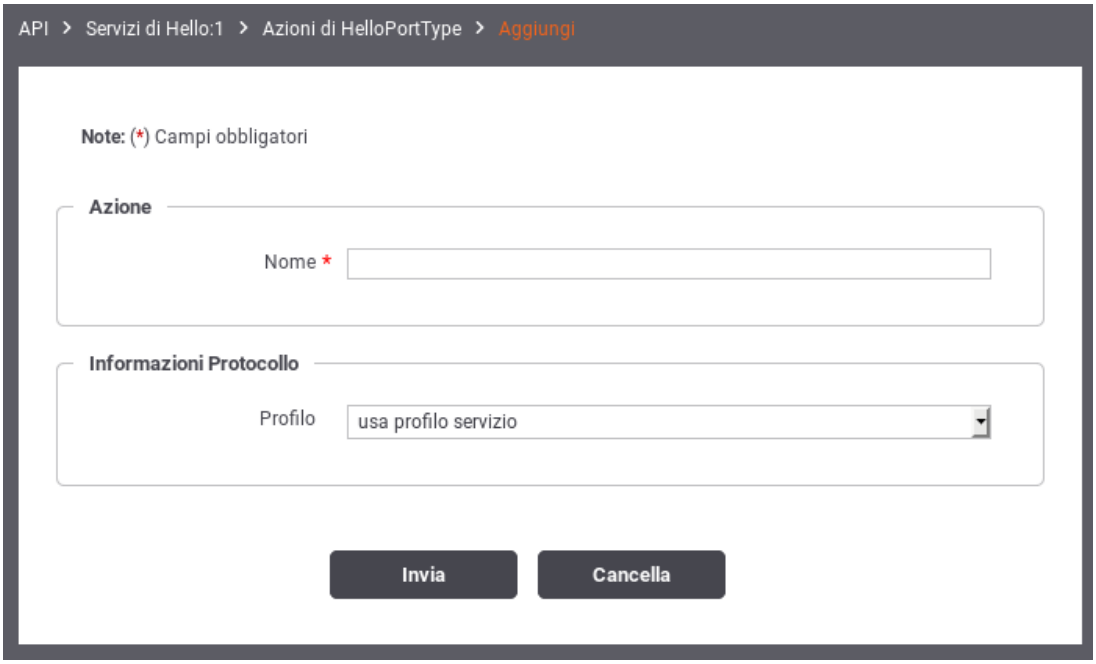


Figura 75: Aggiunta di un'azione alla API SOAP

I dati da fornire sono i seguenti:

- *Nome* dell'azione
- *Profilo*. Si può scegliere se utilizzare le impostazioni già fornite a livello del servizio, oppure ridefinirle indicando nuovamente Profilo di collaborazione, ID Collaborazione e Riferimento ID Richiesta.

Nel caso REST, si procede aggiungendo la nuova risorsa tramite il pulsante *Aggiungi*. Il form da compilare è quello mostrato nella figura seguente.

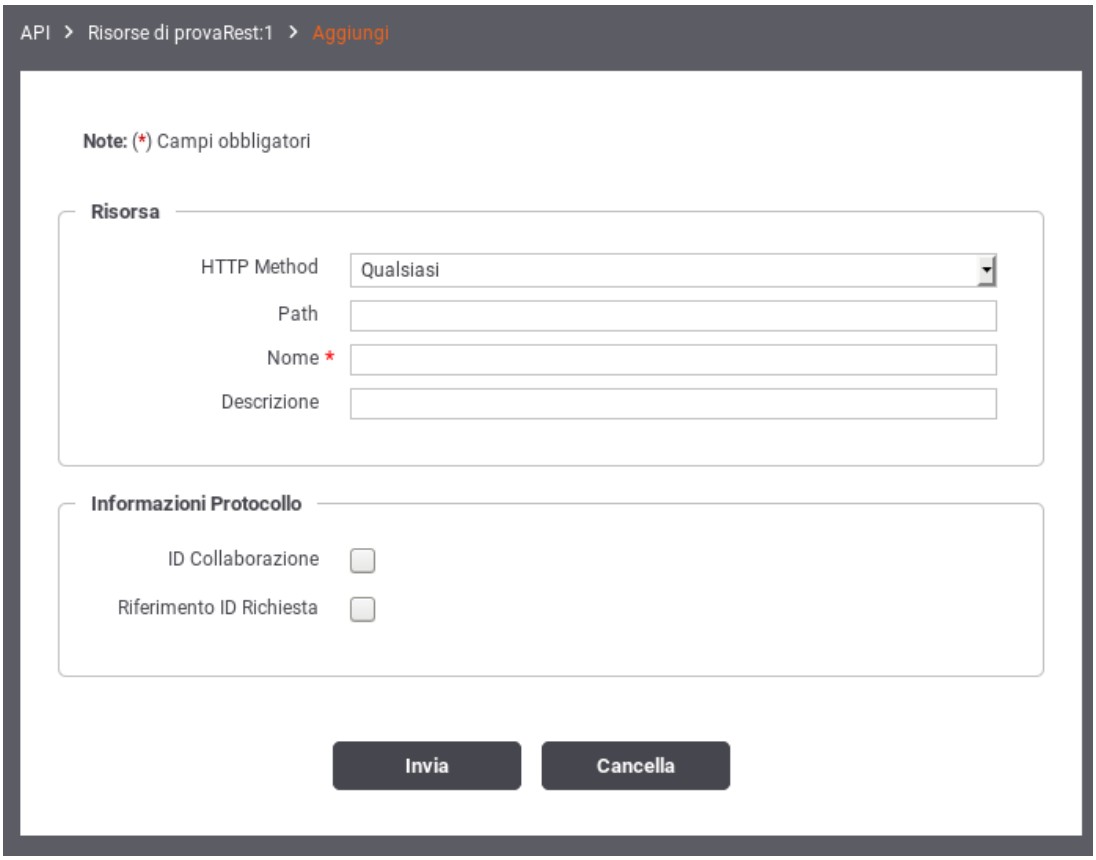


Figura 76: Aggiunta di una risorsa alla API REST

I dati da fornire sono i seguenti:

- *HTTP Method* relativo alla risorsa (GET, POST, DELETE, ecc.)
- *Path* della risorsa
- *Nome* della risorsa
- *Descrizione* della risorsa
- *ID Collaborazione*. Flag per consentire di specificare nelle richieste un valore che identifica una conversazione.
- *Riferimento ID Richiesta*. Flag per consentire di specificare nelle richieste un identificativo relativo ad un messaggio precedente.

8.2 Modalità di identificazione dell'azione

Nel contesto dei servizi Soap, sia erogazioni che fruizioni, si ha la possibilità di selezionare una tra diverse opzioni che riguardano la modalità di identificazione dell'azione. Dopo aver acceduto la sezione *URL di Invocazione*, relativamente alla fruizione o erogazione, si può selezionare una tra le seguenti opzioni:

- *content-based* (Soap e Rest): il dato viene ricavato dal messaggio di richiesta utilizzando come criterio l'espressione XPath indicata nel campo *Pattern* sottostante.
- *header-based* (Soap e Rest): il dato viene ricavato da un valore passato come Http Header. Il campo sottostante consente di specificare il nome di tale header.

- *input-based* (Soap e Rest): il dato viene ricavato dall'header di integrazione fornito con il messaggio di richiesta. Per l'utilizzo di questa modalità fare riferimento al Manuale delle Funzionalità Avanzate.
- *interface-based* (Soap e Rest): il dato viene ricavato in automatico sulla base delle informazioni fornite con la richiesta (messaggio e parametri) confrontandole con la descrizione dell'interfaccia del servizio.
- *url-based* (Soap): il dato viene ricavato dinamicamente dalla url di invocazione utilizzando come criterio l'espressione regolare inserita nel campo *Pattern* sottostante.
- *soap-action-based* (Soap): Questa opzione consente di ricavare il dato dal campo *SoapAction* presente nell'header di trasporto delle comunicazioni SOAP.

Attivando il flag *Force interface*, in caso di fallimento dell'identificazione dell'azione nella modalità prevista al passo precedente, si tenterà di utilizzare la modalità "interface-based" come seconda opzione.

Il campo *Azioni* illustra l'elenco delle azioni presenti per semplice comodità.

8.3 Modalità Avanzata

L'interfaccia della govwayConsole, fin qui descritta, fa riferimento all'operatività nella *modalità standard*. La modalità standard prevede varie semplificazioni, sulle opzioni visualizzate nelle schermate, mirate al compimento delle operazioni di uso comune.

Nel caso si avesse la necessità di ricorrere a configurazioni più specifiche, non contemplate nella modalità standard, è possibile passare alla visualizzazione dell'interfaccia nella *Modalità Avanzata* utilizzando la voce omonima del menu a discesa che compare selezionando l'icona in alto a destra (nella testata della govwayConsole).

Operando in modalità avanzata, in ciascuno dei contesti di configurazione già descritti in questo manuale, compariranno opzioni aggiuntive per le quali sono previsti valori di default nel caso della modalità standard.

Nella modalità avanzata sarà disponibile la funzionalità aggiuntiva *Elimina*, presente nel menu di Configurazione, che consente di utilizzare package di esportazione per l'eliminazione selettiva di entità dal registro.

Nota
L'utilizzo delle funzionalità dell'interfaccia in modalità avanzata non è descritto nel presente manuale.

8.4 Multi-Tenant

I processi di configurazione, descritti in questo manuale, sono ottimizzati nell'ottica di mantenere sempre sottinteso il soggetto interno al dominio. In tal senso, le fruizioni e le erogazioni si intendono sempre in soggettiva riguardo un singolo soggetto interno amministrato dall'utente in sessione.

Multi-tenant è un'opzione che consente di estendere l'ambito delle configurazioni prodotte dalla govwayConsole a più di un soggetto interno al dominio. Tale opzione si attiva nel profilo dell'utente tramite il flag omonimo (Sezione 7.5).

Nota
L'utilizzo della modalità Multi-Tenant non è descritto nel presente manuale.

8.5 Header di Integrazione

In base alle configurazioni prodotte per i servizi, è previsto in diverse situazioni che gli applicativi scambino dei dati con il gateway. Nel caso delle fruizioni si rende necessario al fine di passare al gateway specifici parametri richiesti. Nel caso delle erogazioni lo scopo è quello di consentire al gateway la comunicazione dei metadati della richiesta all'applicativo erogatore.

Per consentire lo scambio di tali informazioni, funzionali all'integrazione tra applicativi e gateway, sono previste alcune strutture dati, che indichiamo sempre con il termine *Header di Integrazione*, che possono essere trasmesse in differenti modalità. Nel

Header	Descrizione
GovWay-Message-ID	Identificativo del messaggio assegnato da GovWay
GovWay-Sender-Type	Codice che identifica il tipo del mittente
GovWay-Sender	Identificativo del mittente
GovWay-Provider-Type	Codice che identifica il tipo del destinatario
GovWay-Provider	Identificativo del destinatario
GovWay-Service-Type	Codice che identifica il tipo del servizio
GovWay-Service	Identificativo del servizio
GovWay-Service-Version	Progressivo di versione del servizio
GovWay-Action	Identificativo dell'azione
GovWay-Relates-To	Identificativo del messaggio riferito
GovWay-Conversation-ID	Identificativo della conversazione
GovWay-Application-Message-ID	Identificativo del messaggio assegnato dall'applicativo
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay
GovWay-Application	Identificativo dell'applicativo

Tabella 9: Header di Integrazione tramite Header HTTP

seguito descriviamo la struttura dell'header di integrazione previsto nelle due modalità attivate per default con l'installazione del prodotto: Header HTTP e Query String.

Se viene utilizzato l'Header HTTP le keyword che costituiscono i dati di integrazione sono quelli della Tabella 9.

Se viene utilizzata la query string (e quindi la url) le keyword che costituiscono i dati di integrazione sono:

Header	Descrizione
govway_message_id	Identificativo del messaggio assegnato da GovWay
govway_sender_type	Codice che identifica il tipo del mittente
govway_sender	Identificativo del mittente
govway_provider_type	Codice che identifica il tipo del destinatario
govway_provider	Identificativo del destinatario
govway_service_type	Codice che identifica il tipo del servizio
govway_service	Identificativo del servizio
govway_service_version	Progressivo di versione del servizio
govway_action	Identificativo dell'azione
govway_relates_to	Identificativo del messaggio riferito
govway_conversation_id	Identificativo della conversazione
govway_application_message_id	Identificativo del messaggio assegnato dall'applicativo
govway_transaction_id	Identificativo della transazione assegnato da GovWay
govway_application	Identificativo dell'applicativo

Tabella 10: Header di Integrazione tramite Query String

Nota

L'header di integrazione descritto è quello che viene trasmesso da Govway agli applicativi interni al dominio, sul messaggio di richiesta per le erogazioni, sul messaggio di risposta per le fruizioni.
L'header di integrazione trasmesso verso i domini esterni comprende esclusivamente i seguenti campi:

- govway_message_id
- govway_relates_to
- govway_conversation_id
- govway_transaction_id