
Guida alla Console di Gestione

Release 3.3.0.rc1

07 mar 2020

Indice

1 Introduzione	1
1.1 I Profili di Interoperabilità	1
1.2 Le entità di configurazione dei servizi	2
1.3 Il processo di configurazione dei servizi	3
2 Profilo “API Gateway”	7
2.1 Definizione delle API	7
2.2 Registrazione dell’erogazione	10
2.3 Registrazione della fruizione	16
2.4 Versionamento delle API	18
2.5 Configurazione Specifica	23
2.6 Gestione CORS	25
2.7 Differenziare le configurazioni specifiche per risorsa/azione	25
2.8 Controllo degli Accessi	27
2.9 Rate Limiting	44
2.10 Validazione dei messaggi	50
2.11 Caching Risposta	51
2.12 Sicurezza a livello del messaggio	51
2.13 Trasformazioni	53
2.14 Tracciamento	61
2.15 Correlazione Applicativa	63
2.16 MTOM	66
2.17 Registrazione Messaggi	67
2.18 Connettore	67
3 Profilo “ModI PA”	69
3.1 Concetti Preliminari	69
3.2 Sicurezza Canale	70
3.3 Sicurezza Messaggio	72
3.4 Profili di Interazione	88
4 Profilo “eDelivery”	113
4.1 Passi preliminari di configurazione	113
4.2 Erogazione di servizi in modalità eDelivery	114
4.3 Fruizione di servizi in modalità eDelivery	117
4.4 Generazione del PMODE Domibus	117

5 Profilo “SPCoop”	119
5.1 Configurazione di un servizio SPCoop	119
5.2 Profili Asincroni	122
5.3 Interfacce WSDL (concettuale, logico ed implementativo)	125
5.4 Profili di gestione della busta eGov	125
6 Profilo “Fatturazione Elettronica”	129
6.1 Fatturazione Passiva	129
6.2 Fatturazione Attiva	133
7 Strumenti	137
7.1 Runtime	137
7.2 Auditing	138
8 Configurazione	143
8.1 Generale	143
8.2 Tracciamento	151
8.3 Controllo del Traffico	153
8.4 Rate Limiting	158
8.5 Token Policy	170
8.6 Tags	181
8.7 Utenti	183
8.8 Importa	184
8.9 Esporta	186
8.10 Auditing	189
9 Funzionalità Avanzate	193
9.1 Modalità Avanzata	193
9.2 Configurazione manuale delle interfacce	194
9.3 Versionamento delle API e delle Erogazioni/Fruizioni	197
9.4 Modalità di identificazione dell’azione	199
9.5 Multi-Tenant	199
9.6 Header di Integrazione	200
9.7 Errori Generati dal Gateway	206
9.8 Connettori	214
9.9 Correlazione tra transazioni differenti	225
9.10 Autenticazione e Autorizzazione Principal (Security Constraint)	225
9.11 Espressioni XPath su messaggi JSON	226

CAPITOLO 1

Introduzione

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

Nota: Oltre alla console di Gestione, GovWay 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 *Utenti*.

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 di interoperabilità di base che consente di supportare qualunque generica API basata su scambio di messaggi SOAP e REST.

- *Modi PA*: è il profilo che consente di supportare gli scenari di comunicazione basati sul Modello di Interoperabilità rilasciato da AGID nel 2018, che fornisce i requisiti per l'integrazione tra il sistema informativo complessivo della Pubblica Amministrazione, Cittadini e Imprese.
- *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.
- *Fatturazione Elettronica*: questo profilo supporta le modalità di scambio delle fatture elettroniche, nel formato FatturaPA, veicolate tramite il Sistema di Interscambio.

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 (Fig. 1.1), comporta la visualizzazione dei soli elementi dell'interfaccia, e relativi dati, attinenti con tale profilo.

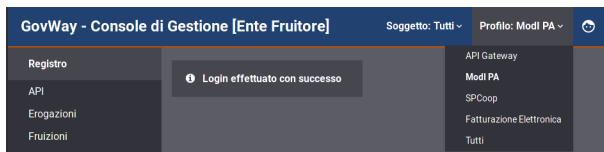


Fig. 1.1: Selezione del profilo di interoperabilità

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:

- *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.

- *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.

- *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.

- *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.

- *Scope*

Entità per censire gli scope che possono essere utilizzati nell'ambito del controllo degli accessi per costruire specifici criteri di autorizzazione basato sui token.

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'Intercambio (SDI).
- *FatturaPA - Fatturazione Passiva*: configurazione del servizio per la ricezione di fatture elettroniche dal Sistema d'Intercambio (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 *Importa*.

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 dettagli 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 Fig. 1.2 descrive lo scenario generale in cui opera GovWay.

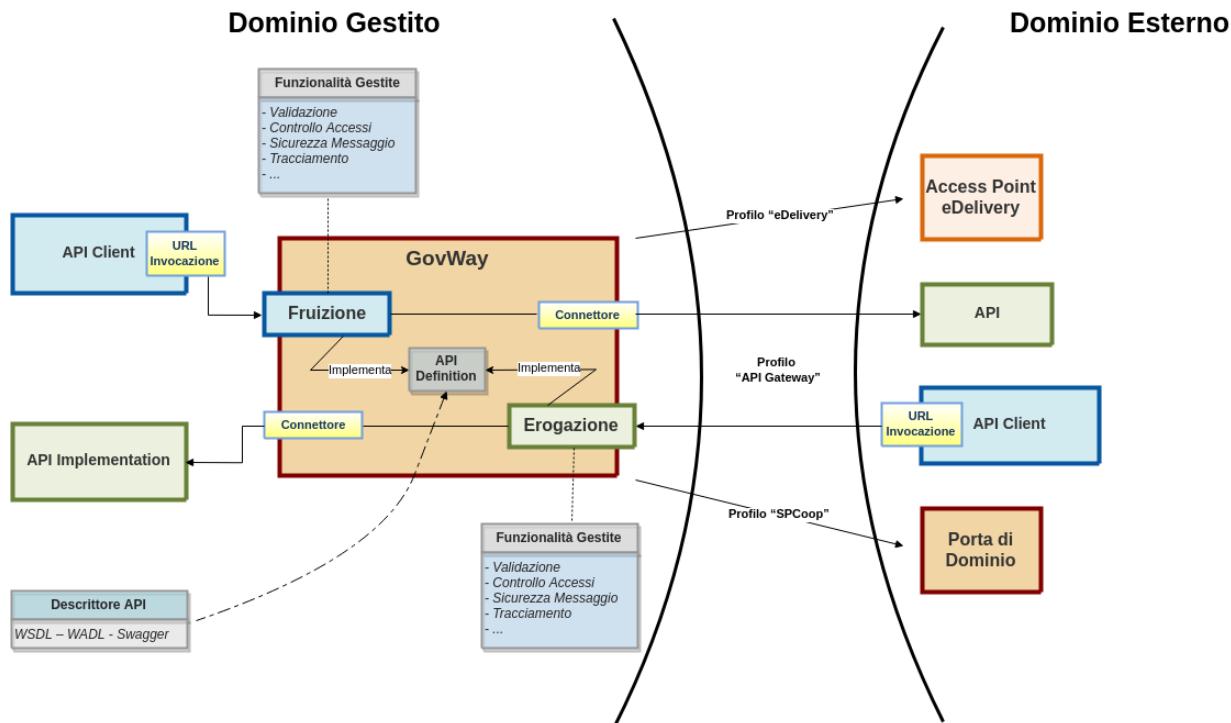


Fig. 1.2: Scenario Generale

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

CAPITOLO 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 selettori 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*.

La pagina di ingresso mostra l'elenco delle API eventualmente già presenti in configurazione. Ciascun elemento dell'elenco riporta l'identificativo, il tipo SOAP o REST e il formato del descrittore fornito in configurazione (Fig. 2.1).

Gli elementi dell'elenco possono essere selezionati per l'eliminazione, con il pulsante Elimina, e per l'esportazione, con il pulsante Esporta. La funzione di esportazione è descritta nella sezione *Esporta*.

Si crea una nuova API premendo il pulsante *Aggiungi*.

Compilare il form (Fig. 2.2) 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.
- *Tags*: un elenco di tag da associare all'API per classificarla. Iniziando a scrivere, vengono proposti i tag già esistenti compatibili.
- *Versione*: progressivo numerico che identifica l'indice di revisione.

The screenshot shows a list of APIs in a management interface. The top bar is dark grey with the word "API" in white. Below it, a header bar has a central section labeled "Visualizzati record [1-5] su 5". The main area contains five API entries, each with a checkbox and a green circular status indicator:

- api-config v1**
API Rest Open API 3.0
- api-monitor v1**
API Rest Open API 3.0
- PROVA v1** tagTest tagTest1 tagTest2
API Rest Open API 3.0
- PROVA v2**
API Rest Open API 3.0
- VariazioneAnagrafica v1** Anagrafica
API Rest Open API 3.0

At the bottom right are three buttons: "ESPORTA" (dark grey background), "ELIMINA" (white background), and "AGGIUNGI" (dark grey background).

Fig. 2.1: Elenco delle API

API > Aggiungi

Note: (*) Campi obbligatori

API

Tipo: Rest

Nome *: HelloAPI

Descrizione:

Tags: tagTest x tag2Test x

Versione: 1

Specifiche delle interfacce

Formato Specifica: Open API 3.0

Open API 3.0: Browse... No file selected.

SALVA

The screenshot shows the 'API > Aggiungi' (Add API) page. At the top, there's a note about mandatory fields. The main section is titled 'API' and contains fields for 'Tipo' (set to 'Rest'), 'Nome' (set to 'HelloAPI'), 'Descrizione' (empty), 'Tags' (containing 'tagTest' and 'tag2Test'), and 'Versione' (set to '1'). Below this is a 'Specifiche delle interfacce' (Interface Specifications) section for 'Open API 3.0', which includes a dropdown menu set to 'Open API 3.0' and a 'Browse...' button next to a message 'No file selected.'. At the bottom is a large 'SALVA' (Save) button.

Fig. 2.2: Definizione di una API

- *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 *Configurazione manuale delle interfacce*.

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 Fig. 2.3 è illustrato graficamente il caso dell’erogazione.

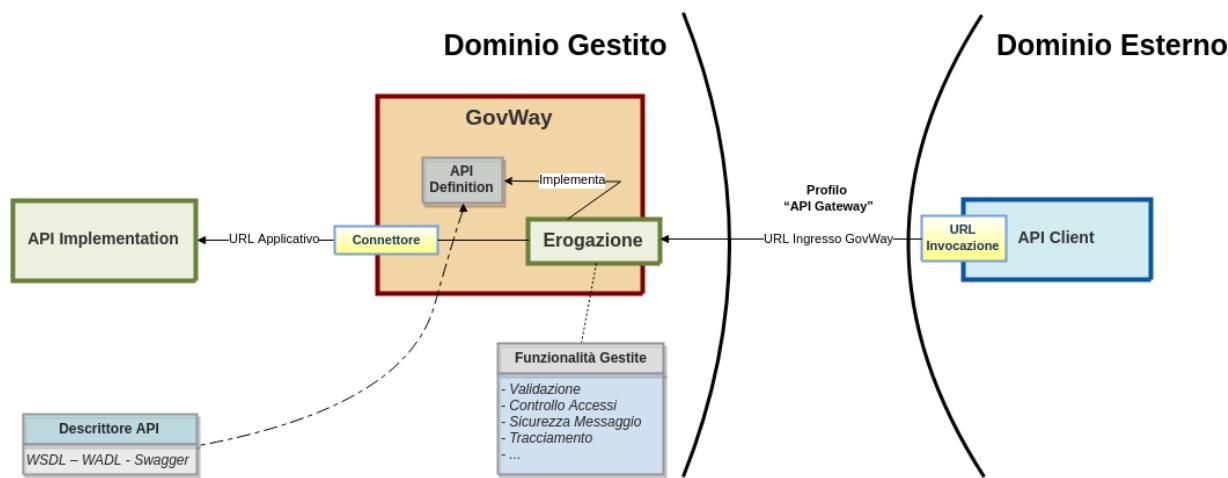


Fig. 2.3: Scenario di riferimento per l’erogazione

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

Compilare il form (Fig. 2.4) 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.
- **Controllo degli Accessi**: In questa sezione è possibile stabilire l’eventuale controllo degli accessi all’erogazione:

- *Pubblico*: non sono richieste credenziali per l’accesso.
- *Autenticato*: l’accesso è ammesso solo previa verifica dei criteri di autenticazione e autorizzazione previsti in configurazione.

Selezionando l’opzione *Autenticato*, dopo la creazione dell’erogazione, sarà necessario completare la configurazione del controllo degli accessi come descritto nella sezione *Autenticazione Trasporto*.

- **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:

Erogazioni > Aggiungi

Note: (*) Campi obbligatori

Informazioni Generali

API

Nome: API_SOAP_1 v1

Tipo: Soap

Servizio: * Esitolidentificazione

Controllo degli Accessi

Accesso API: autenticato

Connettore

Endpoint: * http://10.114.87.21:8180/openspcoop/PD/SPCCentroAnagrafico /SPCComune/SPCEsitoidentificazione/Risultato

Autenticazione Http:

AutenticazioneHttps:

Proxy:

Ridefinisci Tempi Risposta:

SALVA

Fig. 2.4: Registrazione di una Erogazione

- *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 [Tempi Risposta](#))

Nota: Se l'API riferita dall'erogazione possiede un descrittore (WSDL, OpenAPI, ecc.) l'interfaccia propone come valore di default per il connettore l'endpoint del servizio.

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 ([Fig. 2.5](#)).

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 ([Fig. 2.6](#)).

Il dettaglio dell'erogazione mostra i dati principali e con le icone «matita» è possibile entrare sulle maschere di editing per effettuare delle modifiche. In corrispondenza del connettore è disponibile anche un pulsante che consente di verificare la raggiungibilità dell'indirizzo impostato. In corrispondenza della API riferita, è possibile accedere al relativo dettaglio aprendo un nuovo tab del browser ([Fig. 2.7](#)).

La pagina di dettaglio dell'erogazione visualizza i principali elementi di configurazione, che sono:

- **Nome**: nome dell'erogazione. Accanto al valore è presente l'icona a matita che consente di modificare tale valore. In assenza di configurazioni specifiche per risorsa/azione (sezione [Differenziare le configurazioni specifiche per risorsa/azione](#)) è presente anche un'icona che permette di disattivare/riattivare l'erogazione. Lo stato di attivazione dell'erogazione è segnalato tramite l'icona colorata presente accanto al nome.
- **API**: API cui fa riferimento l'erogazione con evidenza degli eventuali tags. È presente un'icona che apre in una nuova finestra l'interfaccia per la gestione della configurazione della specifica API.
- **URL Invocazione**: URL che deve utilizzare il mittente per accedere al servizio erogato tramite il gateway. Questo dato rappresenta:
 - *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.

Erogazioni

Visualizzati record [1-4] su 4

	Erogazioni
<input type="checkbox"/>	api-config v1 API Rest: api-config v1
<input type="checkbox"/>	api-monitor v1 API Rest: api-monitor v1
<input type="checkbox"/>	PROVA v1 tagTest tagTest1 tagTest2 API Rest: PROVA v1
<input type="checkbox"/>	PROVA v2 API Rest: PROVA v2

ESPORTA ELIMINA AGGIUNGI

Fig. 2.5: Elenco Erogazioni presenti nel registro

Erogazioni

Tipo API	Qualsiasi
Tag	Qualsiasi
API / Soggetto Erogatore	

FILTRA RIPULISCI

Fig. 2.6: Filtro delle Erogazioni presenti nel registro

PROVA v1

Nome	● PROVA v1	
API	PROVA v1 (Rest)	
URL Invocazione	http://localhost:8080/govway/ENTE/PROVA/v1	
Connettore	http://127.0.0.1:8080/TestService/echo	
Gestione CORS	Abilitato	

CONFIGURA

Fig. 2.7: Dettaglio dell’erogazione

- *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>/<Azione>

Sono disponibili ulteriori metodi per l'identificazione dell'operation nel caso SOAP, per i cui dettagli si rimanda alla sezione *Modalità di identificazione dell'azione*.

- **Connettore**: Endpoint del servizio acceduto dal gateway, cui verranno consegnate le richieste pervenute. È presente l'icona a matita per aggiornare il valore del connettore. È inoltre presente un'icona che consente di testare la raggiungibilità del servizio tramite il connettore fornito.
- **Gestione CORS**: stato abilitazione della funzione CORS. L'icona a matita consente di modificare l'impostazione corrente.

Ulteriori elementi possono essere indicati per specificare il funzionamento dell'erogazione. Si tratta degli elementi di configurazione specifica, per i cui dettagli si rimanda alla sezione *Configurazione Specifica*.

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 *Header di Integrazione*.
- 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 *Header di Integrazione*) sono:
 - *GovWay-Message-ID*
 - *GovWay-Relates-To*
 - *GovWay-Conversation-ID*
 - *GovWay-Transaction-ID*

2.2.3 Errori Generati dal Gateway

La gestione dei casi di errore nelle comunicazioni mediate da un Gateway devono tenere conto di ulteriori situazioni che possono presentarsi rispetto alla situazione di dialogo diretto tra gli applicativi. Oltre agli errori conosciuti dagli applicativi, e quindi previsti nei descrittori del servizio, gli applicativi client possono ricevere ulteriori errori generati dal gateway.

Govway genera differenti errori a seconda se l'erogazione o la fruizione riguarda una API di tipologia SOAP o REST.

- *REST*: viene generato un oggetto *Problem Details* come definito nella specifica *RFC 7807* (<https://tools.ietf.org/html/rfc7807>). Ulteriori dettagli vengono descritti nella sezione *REST Problem Details (RFC 7807)*.
- *SOAP*: viene generato un *SOAPFault* contenente un *actor* (o *role* in SOAP 1.2) valorizzato con <http://govway.org/integration>. Nell'elemento *fault string* è presente il dettaglio dell'errore mentre nell'elemento *fault code* una codifica di tale errore. Ulteriori dettagli vengono descritti nella sezione *SOAP Fault*.

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 Fig. 2.8 è illustrato graficamente il caso della fruizione.

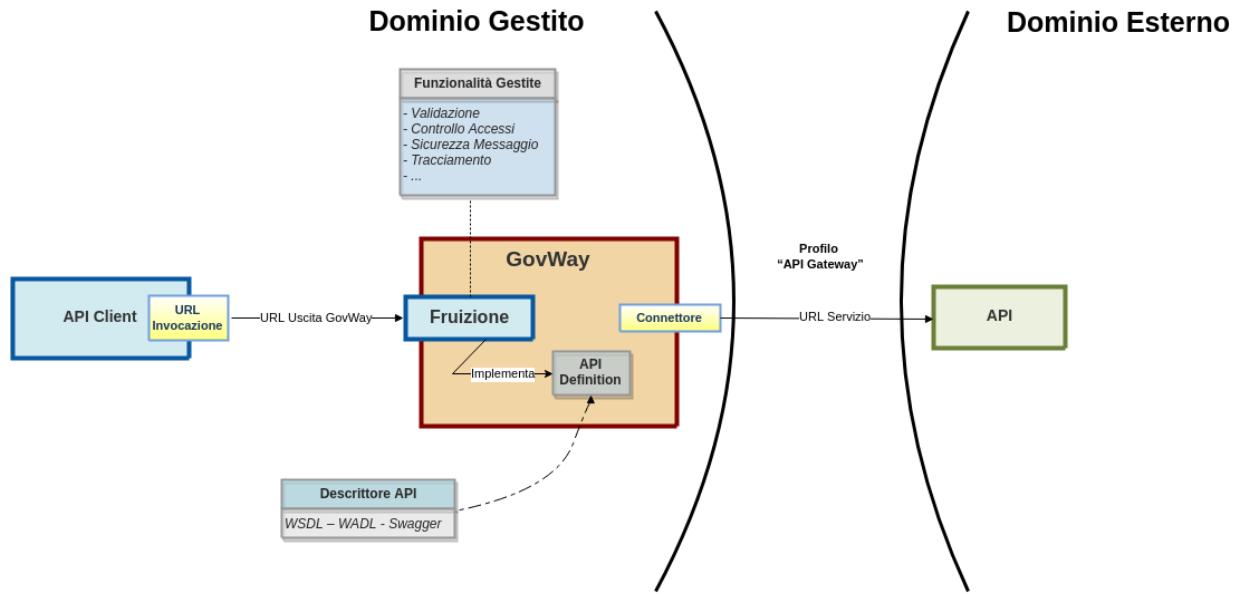


Fig. 2.8: Scenario di riferimento per la fruizione

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 (Fig. 2.9).

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:

- *GovWay-Message-ID*

Fruizioni > Aggiungi

Note: (*) Campi obbligatori

Informazioni Generali

API

Nome	API_SOAP_1 v1
Tipo	Soap
Servizio *	Esitolidentificazione

Soggetto Erogatore

Nome	Piffero
------	---------

Controllo degli Accessi

Accesso API	autenticato
-------------	-------------

Connettore

Endpoint *

Autenticazione Http

AutenticazioneHttps

Proxy

Ridefinisci Tempi Risposta

SALVA

Fig. 2.9: Registrazione di una Fruizione

- *GovWay-Relates-To*
- *GovWay-Conversation-ID*
- *GovWay-Transaction-ID*

Per ulteriori dettagli si consiglia di consultare la sezione *Header di Integrazione*.

2.3.2 Errori Generati dal Gateway

Analogamente a quanto descritto per le erogazioni, la gestione dei casi di errore nelle comunicazioni mediate da un Gateway devono tenere conto di ulteriori situazioni che possono presentarsi rispetto alla situazione di dialogo diretto tra gli applicativi. Oltre agli errori conosciuti dagli applicativi, e quindi previsti nei descrittori del servizio, gli applicativi client possono ricevere ulteriori errori generati dal gateway.

Govway genera differenti errori a seconda se l'erogazione o la fruizione riguarda una API di tipologia SOAP o REST.

- **REST:** viene generato un oggetto *Problem Details* come definito nella specifica *RFC 7807* (<https://tools.ietf.org/html/rfc7807>). Ulteriori dettagli vengono descritti nella sezione *REST Problem Details (RFC 7807)*.
- **SOAP:** viene generato un *SOAPFault* contenente un *actor* (o *role* in SOAP 1.2) valorizzato con <http://govway.org/integration>. Nell'elemento *fault string* è presente il dettaglio dell'errore mentre nell'elemento *fault code* una codifica di tale errore. Ulteriori dettagli vengono descritti nella sezione *SOAP Fault*.

2.4 Versionamento delle API

Come descritto nelle precedenti sezioni, ogni API possiede una versione. È possibile registrare una nuova versione dell'API cliccando sul pulsante “Nuova Versione” presente nel dettaglio di una API (Fig. 2.10).

La maschera di creazione della nuova versione non permette né di modificare il nome dell'API né di scendere di versione. Vengono ereditati dall'API precedente le altre caratteristiche quali il tipo di API tra SOAP e REST, i tags, la descrizione, il soggetto referente etc.

Se l'opzione “Ridefinisci Interfaccia” è abilitata, viene richiesta una nuova specifica dell'interfaccia dell'API. Terminando la creazione della nuova API verranno creati automaticamente i servizi e le azioni su SOAP o le risorse su REST definiti nella nuova interfaccia (Fig. 2.11).

In alternativa, se l'opzione “Ridefinisci Interfaccia” viene disabilitata, non viene richiesta una nuova specifica di interfaccia e la nuova versione dell'API conterrà la medesima specifica della precedente versione con i medesimi servizi e azioni su SOAP o risorse su REST (Fig. 2.12).

Una volta creata una nuova versione dell'API, è possibile effettuare l'upgrade verso la nuova versione direttamente nell'erogazione e/o nella fruizione che implementa l'API. Infatti se esiste più di una versione di una medesima API è possibile modificarne la versione implementata nell'erogazione o nella fruizione tramite il bottone “modifica” evidenziato nella figura Fig. 2.13.

Accedendo alla modifica è possibile scegliere la versione implementata dell'API, tra le versioni disponibili, come mostrato nella figura Fig. 2.14.

La modifica della versione dell'API implementata dall'erogazione, comporta automaticamente anche la modifica della versione dell'erogazione stessa. Questo si riflette nell'url di invocazione che viene automaticamente aggiornata rispetto alla nuova versione come evidenziato nella figura Fig. 2.15.

Nota: Se viene scelta una versione dell'API per la quale esiste già una medesima versione dell'erogazione, il cambio di versione dell'API non si rifletterà sulla versione dell'erogazione e sulla url di invocazione ma solamente sui messaggi scambiati e sulle azioni (soap) o risorse (rest) che l'erogazione espone.

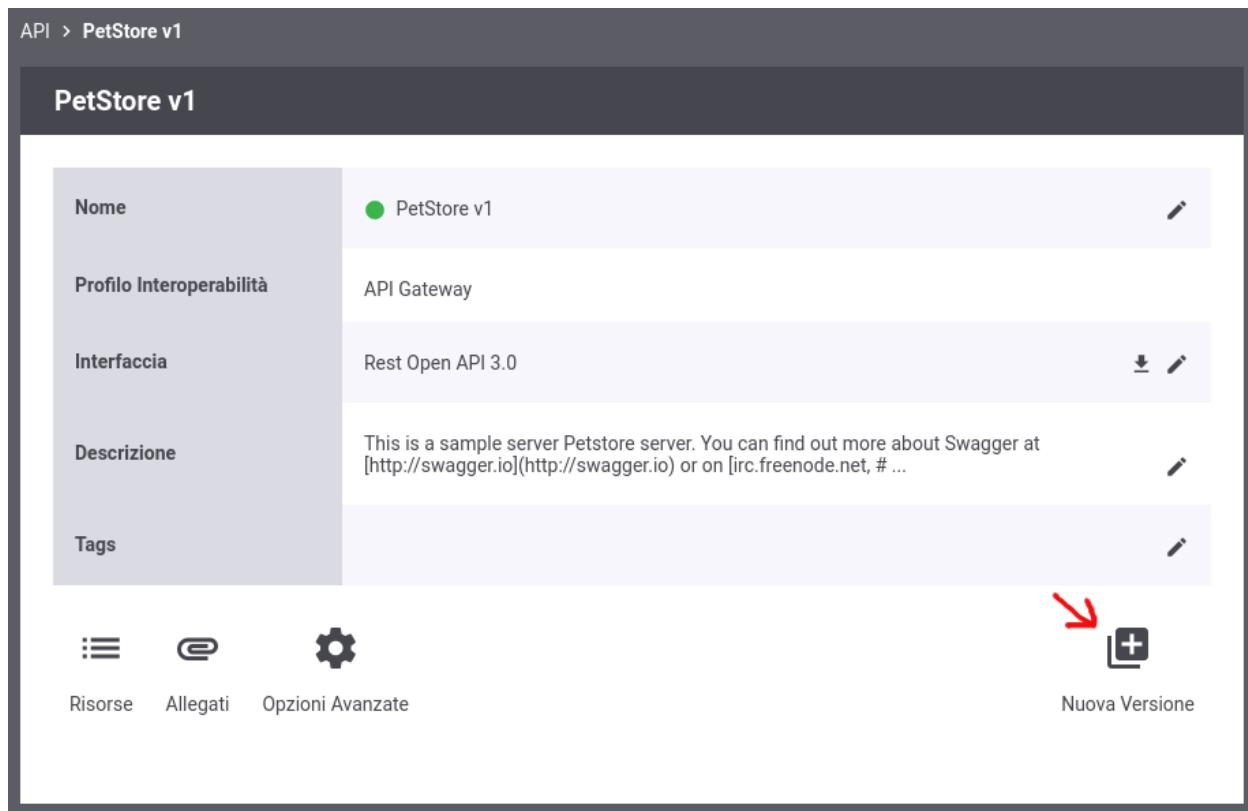


Fig. 2.10: Nuova Versione di una API

The screenshot shows the 'API > Aggiungi' (Add API) screen. The main section is titled 'API' and contains the following fields:

- Nome:** PetStore
- Descrizione:** This is a sample server Petstore server.
- Tags:** (empty input field)
- Versione:** 2

Below this is a section titled 'Specifiche delle interfacce' (Interface Specifications) with the following options:

- Ridefinisci Interfaccia:**
- Formato Specifica:** Open API 3.0
- Open API 3.0:** Choose File | No file chosen

At the bottom center is a large 'SALVA' (Save) button.

Fig. 2.11: Nuova Versione di una API tramite ridefinizione dell'intervaccia

The screenshot shows the 'API > Aggiungi' (Add API) screen. The main section is titled 'API' and contains the following fields:

- Nome:** PetStore
- Descrizione:** This is a sample server Petstore server.
- Tags:** (empty input field)
- Versione:** 2

Below this, under the heading 'Specifiche delle interfacce' (Interface Specifications), there is a checkbox labeled 'Ridefinisci Interfaccia' (Override Interface). At the bottom right of the form is a large 'SALVA' (Save) button.

Fig. 2.12: Nuova API che eredita la specifica di interfaccia dalla versione precedente

Erogazioni > PetStore@ENTE v2

PetStore@ENTE v2

Nome	PetStore v2	
Soggetto Erogatore	ENTE	
API	PetStore v2 (Rest)	
URL Invocazione	http://localhost:8080/goway/ENTE/PetStore/v2	
Connettore	http://petstore.swagger.io/v2	
Gestione CORS	Abilitato	

Fig. 2.13: Upgrade di versione dell'API implementata in una erogazione

Erogazioni > PetStore@ENTE v1 > Informazioni Generali

Informazioni Generali

API

Nome	PetStore
Versione	1
Tipo	2

Fig. 2.14: Scelta della versione dell'API implementata in una erogazione

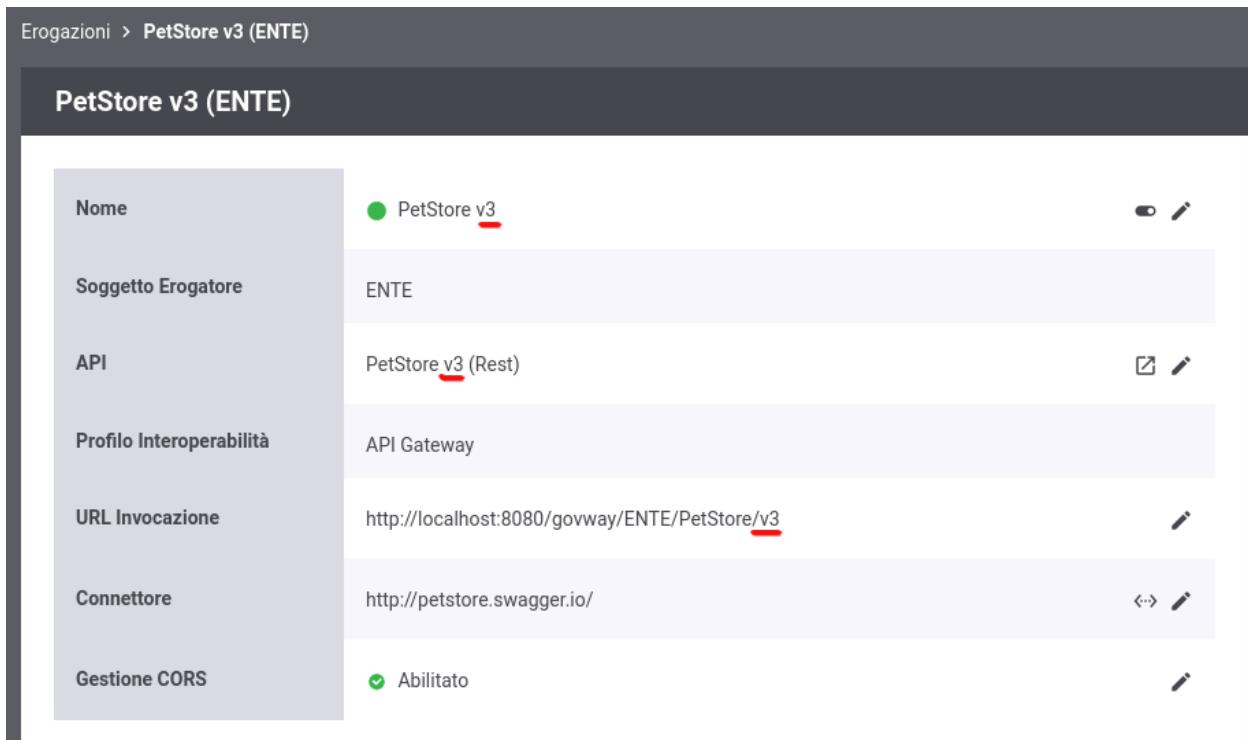


Fig. 2.15: Modifica della versione si riflette sia sull'erogazione che sulla url di invocazione

Per maggiori dettagli sul versionamento differente tra erogazione/fruizione ed API e di conseguenza su come questo si riflette nella url di invocazione si rimanda alla sezione *Versionamento delle API e delle Erogazioni/Fruizioni*

2.5 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 *Configura* presente nel dettaglio dell'erogazione/fruizione. Si accede quindi alla sezione di configurazione specifica (Fig. 2.16).

Le voci di configurazione che possono essere accedute sono:

- Controllo Accessi
- Rate Limiting
- Validazione
- Caching Risposta
- Sicurezza Messaggio
- MTOM (solo SOAP)
- Trasformazioni

The screenshot shows the 'Configurazione' (Configuration) screen in the Management Console. The top navigation bar includes 'Erogazioni > EsitoIdentificazione v1 (Ente) > Configurazione'. The main area is titled 'Configurazione' and contains a table with the following data:

Opzione	Stato	Azione
Controllo Accessi	Autenticazione Trasporto [https]	<input type="button" value="Edit"/>
Rate Limiting	Disabilitato	<input type="button" value="Edit"/>
Validazione	Disabilitato	<input type="button" value="Edit"/>
Caching Risposta	Disabilitato	<input type="button" value="Edit"/>
Sicurezza Messaggio	Disabilitato	<input type="button" value="Edit"/>
MTOM	Disabilitato	<input type="button" value="Edit"/>
Trasformazioni	Disabilitato	<input type="button" value="Edit"/>
Tracciamento	Transazioni, Diagnostici	<input type="button" value="Edit"/>
Registrazione Messaggi	Disabilitato	<input type="button" value="Edit"/>

At the bottom right of the configuration table is a dark button labeled 'CREA NUOVA'.

Fig. 2.16: Configurazione Specifica di una erogazione

- Tracciamento
- Registrazione Messaggi

Accanto a ciascuna delle voci in elenco è presente un'icona che in base al colore assume i seguenti significati:

- **Grigio:** funzionalità non attiva
- **Rosso:** funzionalità attivata ma configurata in maniera incompleta o errata, quindi non funzionante
- **Giallo:** funzionalità attivata in modalità opzionale o «non bloccante» e quindi in sola notifica
- **Verde:** funzionalità attiva

Le funzionalità specifiche possono essere configurate in maniera differenziata per gruppi di risorse/azioni relative alla API erogata/fruita. Una nuova configurazione specifica può essere creata tramite il pulsante *Crea Nuova*. Il passaggio tra una configurazione e l'altra sarà possibile tramite i tab che risulteranno visibili nell'interfaccia. Questa funzionalità è descritta in dettaglio nella sezione *Differenziare le configurazioni specifiche per risorsa/azione*.

Le sezioni successive descrivono in dettaglio le configurazioni sopraelencate e i relativi contesti di utilizzo. Tranne dove esplicitamente dichiarato, gli schemi di configurazione descritti in seguito possono essere attuati sia sulle erogazioni che sulle fruizioni.

2.6 Gestione CORS

Quando un'applicazione client in esecuzione su un browser (es. codice javascript) richiede l'accesso ad una risorsa di un differente dominio, protocollo o porta tale richiesta viene gestita dal browser tramite una politica di *cross-origin HTTP request (CORS)*. Il CORS definisce un modo nel quale un browser ed un server (o il gateway) possono interagire per abilitare interazioni attraverso differenti domini.

In GovWay è possibile abilitare la gestione del CORS sia globalmente, in modo che sia valida per tutte le APIs, che singolarmente sulla singola erogazione o fruizione.

È possibile modificare le impostazioni CORS seguendo il collegamento presente nella riga *Gestione CORS* del dettaglio di una erogazione o fruizione. L'impostazione permette di ridefinire la configurazione globale; i campi del form sono i medesimi descritti nella configurazione globale (sezione *Gestione CORS*).

2.7 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.
- *Rate Limiting:* per configurare i meccanismi di controllo del traffico a salvaguardia delle prestazioni.
- *Validazione:* per configurare i criteri di validazione dei messaggi in transito sul gateway.
- *Caching Risposta:* per configurare l'utilizzo della cache per i messaggi di risposta.
- *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.
- *Trasformazioni:* per configurare le operazioni di trasformazione attivabili sui flussi in entrata ed uscita.

- *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 [Tracciamento](#)).

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

The screenshot shows a web-based configuration form titled 'Aggiungi' (Add) under the path 'Erogazioni > API_REST_1:1 (ENTE) > Gestione Gruppi Risorse'. The form is divided into sections:

- Note: (*) Campi obbligatori** (Note: (*) Required fields)
- Configurazione** (Configuration):
 - Nome Gruppo *** (Group Name *): Input field containing 'Gruppo2'.
 - Risorse *** (Resources *): Input field containing 'POST /store/pdf'.
 - Mode**: A dropdown menu showing 'Eredita Da' (Inherits From).
 - Gruppo**: A dropdown menu showing "'Predefinito'" (Default).
- SALVA** (Save) button at the bottom.

Fig. 2.17: Aggiunta di un gruppo di configurazioni

Compilare il form di creazione della nuova configurazione (Fig. 2.17):

- *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 Connnettore.

Nota: 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: 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.

2.8 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 (Fig. 2.18).

Erogazioni > api-config v1 (ENTE) > Configurazione > **Controllo Accessi**

Controllo Accessi

Autenticazione Token

Stato: disabilitato

Autenticazione Trasporto

Stato: disabilitato

Autorizzazione

Stato: disabilitato

Autorizzazione Contenuti

Stato: disabilitato

SALVA

Fig. 2.18: Controllo degli Accessi

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

2.8.1 Autenticazione 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 autenticazione token che si vuole applicare. In questa lista a discesa saranno visualizzate tutte le *Token Policy* di tipo *Validazione* che sono state registrate in precedenza. Per le istruzioni sulla registrazione delle Token Policy si faccia riferimento alla sezione *Token Policy*.

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 (Fig. 2.8.1).

The screenshot shows the 'Autenticazione Token' configuration interface. At the top, there's a section for selecting a policy, with 'Google' chosen. Below this, several dropdown menus allow setting the status for different operations: 'Validazione JWT' is set to 'disabilitato', while others like 'Introspection', 'User Info', and 'Token Forward' are set to 'abilitato'. A large section titled 'Required Claims' contains checkboxes for 'Issuer', 'ClientId' (which is checked), 'Subject', 'Username', and 'eMail'. The entire interface is contained within a light gray rounded rectangle.

Fig. 2.19: 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* (<https://www.googleapis.com/oauth2/v3/certs>)
 - Il servizio di token introspection basato su *Google - TokenInfo* (<https://www.googleapis.com/oauth2/v3/tokeninfo>)
 - Il servizio di User Info basato su *Google - UserInfo* (<https://www.googleapis.com/oauth2/v3/userinfo>)
-

È possibile inoltre far verificare la presenza obbligatoria delle seguenti metainformazioni all'interno del token:

- Issuer
- ClientId
- Subject
- Username
- Email

2.8.2 Autenticazione Trasporto

In questa sezione è possibile configurare il meccanismo di autenticazione richiesto per l'accesso al servizio. Come mostrato in Fig. 2.20, si possono specificare:

- Il tipo di autenticazione, distinto in base al protocollo di trasporto, selezionando uno tra i valori disponibili:
 - **disabilitato** nessuna autenticazione
 - **https** La richiesta deve possedere un certificato client X509. La presenza del certificato client nella richiesta è obbligatoria a meno che non sia abilitato il flag *Opcionale*. Se è presente un certificato client, il gateway cercherà inoltre di identificare un applicativo o un soggetto a cui è stato associato il certificato come credenziale di accesso (per ulteriori dettagli si rimanda alle sezioni *Creazione di un soggetto* e *Creazione di un applicativo*); l'identificazione non è obbligatoria ma nel caso avvenga con successo l'applicativo o il soggetto verrà registrato nei log e potrà essere utilizzato anche ai fini di autorizzazione puntuale e per ruoli (*Autorizzazione*).
 - **http-basic** La richiesta deve possedere un header «Authorization» che veicola credenziali Basic (username e password) come indicato in “<https://tools.ietf.org/html/rfc2617#section-2>”. Le credenziali devono corrispondere ad un applicativo o un soggetto registrato nel gateway. Abilitando l'ulteriore opzione *Forward Authorization* è possibile propagare all'endpoint di destinazione l'header http «Authorization» che altrimenti verrà consumata.

– **principal** La richiesta deve possedere il «principal» che identifica il chiamante. La modalità con cui il gateway può ottenere il principale deve essere scelta tra le seguenti opzioni:

- * *Container*: il principal viene fornito direttamente dal container sul quale è in esecuzione il gateway.
- * *Header HTTP*: il principal viene estratto dallo specifico header http che viene indicato successivamente. È inoltre possibile attivare l’opzione *Forward Header* per far sì che il gateway propaghi il dato di autenticazione.
- * *Parametro della Url*: il principal viene estratto da un parametro della query string il cui nome viene indicato successivamente. È inoltre possibile attivare l’opzione *Forward Parametro Url* per far sì che il gateway propaghi il dato di autenticazione.
- * *Url di Invocazione*: il principal viene estratto direttamente dalla URL di invocazione tramite l’espressione regolare che viene fornita successivamente.
- * *Client IP*: il principal utilizzato è l’indirizzo IP di provenienza.
- * *X-Forwarded-For*: il principal viene estratto dall’header http utilizzato per il mantenimento dell’IP di origine nel caso di nodi intermedi (es. X-Forwarded-For).
- * *Token*: opzione presente solamente se è stata attivata, al passo precedente, l’autenticazione del token. Il principal viene letto da uno dei claim presenti nel token.

Il flag *Opzionale* consente di non rendere bloccante il superamento dell’autenticazione nel caso la richiesta non possiede il principal atteso.

– **custom**: metodo di autenticazione fornito tramite personalizzazioni di GovWay

Autenticazione Trasporto

Stato	principal
Tipo	Container
Opzionale	<input checked="" type="checkbox"/>

Fig. 2.20: Configurazione dell’autenticazione del servizio

2.8.3 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:

- *Autorizzazione per Richiedente*: superato il processo di autenticazione, saranno accettate le sole richieste provenienti dai mittenti indicati singolarmente nella lista fornita con il criterio. Dopo aver abilitato questa opzione, ed aver confermato tramite il pulsante Invia, sarà possibile fornire la lista dei mittenti autorizzati ad accedere al servizio.

I mittenti che possono essere indicati sono Soggetti (solo nel caso delle erogazioni) e Applicativi. Tali entità dovranno essere precedentemente registrate sulla govwayConsole seguendo le indicazioni fornite in sezione *Creazione di un soggetto* e *Creazione di un applicativo*.

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

Nota: L'opzione di autorizzazione sugli applicativi, nel caso di una erogazione, viene utilizzata per gestire l'accesso al servizio da parte di applicativi interni al dominio di GovWay.

- **Autorizzazione per 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 [Creazione di un ruolo](#).

- **Autorizzazione per 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.

- **Autorizzazione per Token Claims:** 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.

Per le indicazioni di dettaglio sui possibili controlli effettuabili su ogni claim si faccia riferimento alla sezione [Autorizzazione per Token Claims](#).

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

- **XACML-Policy:** È possibile basare il meccanismo di autorizzazione sulla valutazione di una policy xacml selezionando la relativa opzione sulla lista «Stato».

Per le indicazioni di dettaglio sulla configurazione delle xacml-Policy si faccia riferimento alla sezione [XACML-Policy](#).

- **Custom:** Sulla lista «Stato», è possibile selezionare questo metodo di autorizzazione eventualmente fornito tramite estensione di GovWay.

2.8.4 Autorizzazione Contenuti

L'autorizzazione dei contenuti è un ulteriore meccanismo per il controllo degli accessi tramite il quale è possibile specificare regole di autorizzazione che verificano aspetti della richiesta quali ad esempio gli header http, l'url di invocazione, parti del messaggio etc.

Una volta abilitata l'autorizzazione per contenuto si possono configuire una serie di controlli di autorizzazione nella forma (risorsa=valore).

Una risorsa identifica un header, una parte dell'url o del messaggio, un claim del token o un principal etc. Per identificare una risorsa sono utilizzabili le seguenti espressioni dinamiche:

- \${header:NAME}: valore presente nell'header http che possiede il nome “NAME”
- \${query:NAME}: valore associato al parametro della url con nome “NAME”
- \${urlRegExp:EXPR}: espressione regolare applicata sulla url di invocazione
- \${xPath:EXPR}: espressione XPath applicata su un messaggio XML
- \${jsonPath:EXPR}: espressione JSONPath applicata su un messaggio JSON
- \${tokenInfo:FIELD}: permette di accedere ai claim di un token; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.pdd.core.token.InformazioniToken” (es. per ottenere il valore del claim “sub” usare \${tokenInfo:sub})
- \${transportContext:FIELD}: permette di accedere ai dati della richiesta http; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.utils.transport.http.HttpServletTransportRequestContext” (es. per il principal usare \${transportContext:credential.principal})

Ogni valore atteso per una risorsa può essere fornito in una delle seguenti modalità:

- \${anyValue} : indica qualsiasi valore non nullo
- \${regExpMatch:EXPR} : la regola è soddisfatta se il valore della risorsa ha un match completo rispetto all'espressione regolare EXPR indicata
- \${regExpFind:EXPR} : simile alla precedente regola, il match dell'espressione regolare può avvenire anche su una sottostringa del valore della risorsa
- valore : indica esattamente il valore (case sensitive) che deve possedere la risorsa; il valore può essere definito come costante o contenere parti dinamiche risolte a runtime dal Gateway nella forma descritta precedentemente per le risorse
- valore1,...,valoreN : è possibile elencare differenti valori ammissibili; come per la precedente opzione il valore può contenere parti dinamiche

Di seguito alcuni esempi:

- \${header:X-Prova}=test : viene verificato che l'header “X-Prova” possiede il valore “test”
- \${header:X-Prova}=test,test2,test3 : viene verificato che l'header “X-Prova” possiede il valore “test” o “test2” o “test3”
- \${transportContext:credential.principal}=\${header:X-SSO} : viene verificato che l'identità principal del chiamante corrisponda al valore fornito nell'header “X-SSO”
- \${transportContext:credential.principal}=prefix\${header:X-SSO}suffix : simile alla precedente regola, dove l'identità principal viene confrontata con il valore presente nell'header concatenato da un prefisso e da un suffisso statico.
- \${xPath:EXPR}=\${regExpMatch:[0-9]} : viene estratto il contenuto dalla richiesta xml tramite l'espressione XPath EXPR e verificato che sia corrispondente ad una cifra decimale attraverso l'espressione regolare “[0-9]”
- \${jsonPath:EXPR}=\${transportContext:credential.principal} : viene estratto il contenuto dalla richiesta json tramite l'espressione jsonPath EXPR e verificato che sia uguale all'identità principal del chiamante

2.8.5 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».

The screenshot shows a web-based form for adding a subject. At the top, it says "Soggetti > Aggiungi". Below that, a note says "Note: (*) Campi obbligatori". The form itself is titled "Soggetto". It has four input fields: "Profilo Interoperabilità" (set to "API Gateway"), "Nome *" (marked with a red asterisk), "Tipologia" (set to "Erogatore"), and "Descrizione". At the bottom of the form is a large, dark blue "SALVA" button.

Fig. 2.21: Creazione di un soggetto

Per creare il soggetto posizionarsi nella sezione *Registro > Soggetti*, quindi premere il pulsante *Aggiungi*. Compilare il form come segue (Fig. 2.21):

- *Profilo Interoperabilità*: La scelta del profilo di interoperabilità sarà richiesta solo nel caso in cui non sia stata effettuata la relativa scelta dal menu in testata.
- *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*: Sezione presente solo nel caso in cui 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. Per i dettagli sulla configurazione della modalità di accesso si faccia riferimento alla sezione *Modalità di Accesso*.

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 (Fig. 2.22) è presente una lista dalla quale è possibile selezionare un ruolo alla volta, che viene aggiunto confermando con il tasto *Invia*.

The screenshot shows a user interface for managing roles. At the top, there is a breadcrumb navigation: "Soggetti > Ruoli di EnteEsterno2". Below this, a form titled "Ruolo" is displayed. The "Nome" (Name) field contains the value "Ticket". At the bottom of the form are two buttons: "Invia" (Send) on the left and "Cancella" (Delete) on the right.

Fig. 2.22: Assegnazione di ruoli ad un soggetto

2.8.6 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 assegnergli delle credenziali che lo identificano ed eventuali ruoli provenienti dalla fonte «Registro».

Per registrare l'applicativo posizionarsi nella sezione *Registro > Applicativi*, quindi premere il pulsante *Aggiungi*. Compilare il form come segue (Fig. 2.23):

- *Profilo Interoperabilità*: Opzione visibile solo nel caso in cui non sia stata effettuata la relativa scelta sul menu della testata.
- *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).
- *Modalità di Accesso*: 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. Per i dettagli sulla configurazione della modalità di accesso si faccia riferimento alla sezione *Modalità di Accesso*.

Dopo aver creato l'applicativo è opzionalmente possibile assegnergli 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*.

2.8.7 Modalità di Accesso

Quando il gateway richiede l'autenticazione per l'accesso è possibile selezionare la relativa modalità e quindi il tipo di credenziali che dovranno essere fornite.

Le modalità per l'accesso autenticato supportate sono le seguenti:

Applicativi > Aggiungi

Note: (*) Campi obbligatori

Applicativo

Nome * Applicativo1

Modalità di Accesso

Tipo http-basic

Utente * app1

Password * 123456

SALVA

The screenshot shows a web-based application creation interface. At the top, there's a breadcrumb navigation "Applicativi > Aggiungi". Below it, a note says "Note: (*) Campi obbligatori". The main area is divided into two sections: "Applicativo" and "Modalità di Accesso". In the "Applicativo" section, there's a field labeled "Nome *" with the value "Applicativo1". In the "Modalità di Accesso" section, there are three fields: "Tipo" set to "http-basic", "Utente *" with the value "app1", and "Password *" with the value "123456". At the bottom right of the form is a large "SALVA" button.

Fig. 2.23: Creazione di un applicativo

- **http-basic** Se il tipo selezionato è *http-basic* sarà necessario fornire l'identificativo utente e la relativa password (Fig. 2.24).

The screenshot shows a configuration interface for 'Modalità di Accesso'. At the top, there is a dropdown menu labeled 'Tipo' with 'http-basic' selected. Below it are two input fields, both marked with a red asterisk indicating they are required: 'Utente' (User) and 'Password'.

Fig. 2.24: Credenziali di tipo HTTP-Basic

- **https** Se il tipo selezionato è *https* si procede con la configurazione del certificato che sarà fornito durante l'autenticazione (Fig. 2.25). Per la configurazione si procede selezionando dall'elemento *Modalità* una tra le seguenti opzioni:

- **Upload Archivio:** con questa modalità di configurazione si procede con il caricamento del certificato che sarà utilizzato per l'autenticazione. È necessario indicare il formato del certificato fornito specificando tra le seguenti opzioni supportate:
 - * *CER*: il certificato da caricare è in formato *DER* o *PEM*.
 - * *JKS*: il certificato da caricare è contenuto in un keystore *JKS*.
 - * *PKCS12*: il certificato da caricare è contenuto in un keystore *PKCS12*.
- **Password:** campo visibile nel caso in cui il certificato da caricare è contenuto in un keystore. Rappresenta la password per l'accesso al keystore.
- **Certificato:** selezionare dal proprio filesystem il file che contiene il certificato.
- **Alias:** nel caso in cui il keystore contenga più di un certificato, questa lista consente di selezionare l'alias che riferisce l'elemento corretto. Dopo aver selezionato un alias verranno mostrati a video i dettagli del certificato selezionato, al fine di poterli verificare prima di confermare l'inserimento.
- **Verifica tutti i campi:** questa opzione, se attivata, comporta il confronto di tutti i campi del certificato fornito per l'autenticazione con quelli presenti nel certificato fornito come campione in configurazione. Il fallimento di tale verifica (ad esempio anche il caso di superamento della data di scadenza) causeranno il fallimento dell'autenticazione.
- **Configurazione Manuale:** con questa modalità di configurazione si procede con l'inserimento dei seguenti dati:
 - * *Self Signed*: opzione per indicare se il certificato è self-signed oppure rilasciato da una CA.
 - * *Subject*: il subject del certificato.
 - * *Issuer*: l'issuer del certificato, nel caso in cui non sia self-signed.

- **principal** Se il tipo selezionato è *principal* sarà necessario fornire lo UserId (Fig. 2.26).

Modalità di Accesso

Tipo	<input type="text" value="https"/>
Configurazione	
Modalità	<input type="text" value="Upload Archivio"/>
Tipo	<input type="text" value="CER"/>
Certificato *	<input type="button" value="Browse..."/> No file selected.

Fig. 2.25: Credenziali di tipo HTTPS

Modalità di Accesso

Tipo	<input type="text" value="principal"/>
UserId *	<input type="text"/>

Fig. 2.26: Credenziali di tipo Principal

2.8.8 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*.

The screenshot shows a modal dialog box titled "Ruolo". Inside the dialog, there is a note: "Note: (*) Campi obbligatori". Below this, there are five input fields:

- Nome**: Sanzioni (marked with a red asterisk)
- Descrizione**: descrizione del ruolo
- Fonte**: Esterna (with a dropdown arrow)
- Identificativo Esterno**: Multe
- Contesto**: Erogazione (with a dropdown arrow)

At the bottom of the dialog are two buttons: "Invia" and "Cancella".

Fig. 2.27: Registrazione di un ruolo

Compilare il form (Fig. 2.27) 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.

2.8.9 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.

Soggetti > Elenco > Ruoli di PROXY/ENTE

Ruolo

Nome: ruoloEsempio

Invia **Cancella**

Fig. 2.28: 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.

Servizio Applicativo > Elenco > Ruoli di SA1

Ruolo

Nome: ruoloEsempio

Invia **Cancella**

Fig. 2.29: Attribuzione di un ruolo ad un applicativo

2.8.10 Autorizzazione per Token Claims

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.

L'autorizzazione per token claims permette di effettuare dei semplici controlli sui valori dei claim presenti nel token, una volta verificato che il token sia valido. La funzionalità è utilizzabile nei contesti in cui il controllo di autorizzazione possiede una logica semplice che si basa sulla verifica del valore di uno o più claim. Dove serve una logica più complessa (ad es. con rami “if-else”) il controllo deve essere effettuato utilizzando una XACMLPolicy ([XACML-Policy](#)).

La configurazione viene effettuata inserendo nel campo di testo un claim da verificare per ogni riga, facendo seguire dopo l'uguale un valore fornito in una delle seguenti modalità:

- \${anyValue} : indica qualsiasi valore non nullo
- \${regExpMatch:EXPR} : la regola è soddisfatta se l'intero valore del claim ha un match rispetto all'espressione regolare EXPR indicata
- \${regExpFind:EXPR} : simile alla precedente regola, il match dell'espressione regolare può avvenire anche su una sottostringa del valore del claim
- valore : indica esattamente il valore (case sensitive) che deve possedere il claim; il valore può essere definito come costante o contenere parti dinamiche risolte a runtime dal Gateway descritte di seguito
- valore1,...,valoreN : è possibile elencare differenti valori ammissibili; come per la precedente opzione il valore può contenere parti dinamiche

Le espressioni utilizzabili come parti dinamiche, risolte a runtime dal gateway, sono:

- \${header:NAME}: valore presente nell'header http che possiede il nome “NAME”
- \${query:NAME}: valore associato al parametro della url con nome “NAME”
- \${urlRegExp:EXPR}: espressione regolare applicata sulla url di invocazione
- \${xpath:EXPR}: espressione XPath applicata su un messaggio XML
- \${jsonPath:EXPR}: espressione JSONPath applicata su un messaggio JSON
- \${transportContext:FIELD}: permette di accedere ai dati della richiesta http; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.utils.transport.http.HttpServletTransportRequestContext” (es. per il principal usare \${transportContext:credential.principal})

Di seguito alcuni esempi:

- client_id=3 : viene verificato che il claim “client_id” possieda il valore 3
- client_id=3,5,6 : viene verificato che il claim “client_id” possieda il valore 3 o 5 o 6
- client_id=\${anyValue} : viene verificato che il claim “client_id” possieda un valore (not null e not empty)
- client_id=\${regExpMatch:[0-9]} : viene verificato che il claim “client_id” possieda esattamente una cifra decimale attraverso la verifica di un match con l'espressione regolare “[0-9]”
- client_id=\${regExpFind:[0-9]} : viene verificato che il claim “client_id” contenga una cifra decimale attraverso l'espressione regolare “[0-9]”
- client_id=\${header:X-Prova} : viene verificato che il claim “client_id” possieda lo stesso valore presente nell'header http “X-Prova” presente nella richiesta
- client_id=cl-\${header:X-Prova} : viene verificato che il claim “client_id” possieda il valore presente nell'header http “X-Prova” arricchito del prefisso “cl-“
- client_id=\${query:prova} : viene verificato che il claim “client_id” possieda lo stesso valore presente nel parametro “prova” della url di invocazione
- client_id=\${urlRegExp:EXPR} : viene verificato che il claim “client_id” possieda lo stesso valore estratto dalla url di invocazione attraverso l'applicazione dell'espressione regolare EXPR

- `client_id=${xpath(EXPR)}` : viene verificato che il claim “`client_id`” possieda lo stesso valore estratto dalla richiesta xml tramite l’espressione XPath EXPR.
- `client_id=${jsonPath(EXPR)}` : viene verificato che il claim “`client_id`” possieda lo stesso valore estratto dalla richiesta json tramite l’espressione jsonPath EXPR.

2.8.11 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 Fig. 2.30.

Fig. 2.30: 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:

Tabella 2.1: Parametri inseriti in una XACMLRequest

Nome	Descrizione
<i>Sezione “Action”</i>	
<code>org:govway:action:provider</code>	Indica il soggetto erogatore del servizio
<code>org:govway:action:service</code>	Indica il servizio nel formato tipo/nome
<code>org:govway:action:action</code>	Nome dell’operazione del servizio invocata
<code>org:govway:action:url</code>	Url di invocazione utilizzata dal mittente
<code>org:govway:action:url:parameter:NOME_PARAM</code>	Tutti i parametri presenti nell’url di invocazione saranno inseriti nella XACMLRequest con questo formato
<code>org:govway:action:transport:header:NOME_HDR</code>	Tutti gli header http presenti nell’url di invocazione saranno inseriti nella XACMLRequest con questo formato
<code>org:govway:action:soapAction</code>	Valore della SOAPAction
<code>org:govway:action:gwService</code>	Ruolo della transazione (inbound/outbound)
<code>org:govway:action:protocol</code>	Modalità associata al servizio richiesto (es. spcoop)
<code>org:govway:action:token:audience</code>	Destinatario del token
<code>org:govway:action:token:scope</code>	Lista di scopes
<code>org:govway:action:token:jwt:claim:<nome>=<valore></code>	Tutti i claims presenti nel jwt validato

Continued on next page

Tabella 2.1 – continued from previous page

Nome	Descrizione
org:govway:action:token:introspection:claim:<nome>=<valore>	Tutti i claims presenti nella risposta del servizio di introspection
<i>Sezione “Subject”</i>	
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

Di seguito un esempio di XACMLPolicy che autorizza le richieste dei chiamanti che possiedono il ruolo “Amministratore” ed uno tra i due ruoli “Operatore1” e “Operatore2”:

```

<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" PolicyId="Policy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides" 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>
                    </Apply>
                </Apply>
            </Apply>
        </Condition>
    </Rule>
</Policy>

```

```

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
    ↳ Operatore2 </AttributeValue>
        </Apply>
        </Apply>
        </Apply>
    </Condition>
</Rule>
<Rule Effect="Deny" RuleId="ko" />
</Policy>

```

Un altro esempio di policy che verifica l'uguaglianza tra il valore del claim “sub” presente nel token e quello fornito nel query parameter “sub” è la seguente:

```

<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:or">

                <Apply FunctionId="urn:oasis:names:tc:xacml:1.
                ↳ 0:function:any-of-any">
                    <Function FunctionId="urn:oasis:names:tc:xacml:1.
                    ↳ 0:function:string-equal"/>
                    <ActionAttributeDesignator
                        AttributeId=
                            "org:govway:action:url:parameter:sub"
                            DataType="http://www.w3.org/2001/XMLSchema
                            ↳ #string"
                            MustBePresent="false"
                    />
                    <ActionAttributeDesignator
                        AttributeId=
                            "org:govway:action:token:introspection:claim:sub"
                            DataType="http://www.w3.org/2001/XMLSchema
                            ↳ #string"
                            MustBePresent="false"
                    />
                </Apply>
            </Condition>
        </Rule>
        <Rule Effect="Deny" RuleId="ko" />
    </Policy>

```

2.8.12 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 Fig. 2.31.

Note: (*) Campi obbligatori

Scope

Nome *	<input type="text"/>
Descrizione	<input type="text"/>
Identificativo Esterno	<input type="text"/>
Contesto	<input type="text"/> Qualsiasi

Invia **Cancella**

Fig. 2.31: 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.

2.9 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 *Controllo del Traffico*, dove viene illustrato il meccanismo per configurare le policy e più in dettaglio nella sezione *Policy Globali* riguardo l’attivazione di policy a valenza globale.

Una policy di rate limiting si compone concettualmente dei seguenti elementi:

- *Criterio di Misurazione*: elemento che consente di calcolare un valore utile per la valutazione della policy. Il valore calcolato dipende dalla **metrica** scelta. La metrica viene scelta in fase di configurazione tra quelle disponibili, che sono:
 - *Numero Richieste*: consente di limitare il numero totale massimo di richieste consentite.
 - *Numero Richieste Simultanee*: limita il numero totale massimo di richieste simultanee consentite.
 - *Occupazione Banda*: limita il numero totale massimo di KB consentiti.

- *Tempo Medio Risposta*: la policy blocca ogni successiva richiesta se viene rilevato un tempo medio di risposta elevato.
- *Tempo Complessivo Risposta*: la policy limita il numero totale massimo di secondi consentiti.
- *Numero Richieste Completate con Successo*: vengono conteggiate solamente il numero di richieste completate con successo; raggiunto il limite, ogni successiva richiesta viene bloccata.
- *Numero Richieste Fallite*: vengono conteggiate il numero di richieste fallite; raggiunto il limite, ogni successiva richiesta viene bloccata.
- *Numero Fault Applicativi*: vengono conteggiate il numero di richieste che veicolano un fault applicativo; raggiunto il limite, ogni successiva richiesta viene bloccata.
- *Numero Richieste Fallite o Fault Applicativi*: vengono conteggiate il numero di richieste fallite o che veicolano un fault applicativo; raggiunto il limite, ogni successiva richiesta viene bloccata.

Per ottenere un valore di confronto, alla metrica è necessario associare un intervallo di osservazione che consente di stabilire univocamente il conteggio risultante (fa eccezione “Numero Richieste Simultanee”). L’intervallo di osservazione può essere espresso scegliendone uno tra i seguenti:

- *Minuti*
 - *Orario*
 - *Giornaliero*
- *Soglia di Confronto*: elemento della policy che fornisce il valore di soglia da confrontare con il valore ottenuto dalla metrica impostata.
 - *Filtro di Applicabilità*: elemento della policy che stabilisce i criteri per i quali è applicabile la policy sui flussi in elaborazione sul Gateway (filtro su mittente, api, applicativo, ecc.).

Per ogni singola erogazione o fruizione di API è possibile definire più politiche di Rate Limiting, anche con medesima metrica. Per ogni richiesta viene applicato un algoritmo di valutazione delle policy che è il seguente (una descrizione di dettaglio viene fornita nelle sezioni successive):

- le policy vengono raggruppate «per metrica» e per ogni metrica vengono valutate nell’ordine di elenco.
- per ogni metrica vengono valutate le policy applicabili, cioè per le quali risultano soddisfatti il filtro e le condizioni di applicabilità.
- se la policy viola i livelli di soglia previsti, la transazione viene bloccata (o segnalata se configurata come «warning only») e la valutazione delle policy viene terminata.
- se la policy non viola invece i livelli di soglia previsti, si prosegue nella valutazione di ulteriori policy per quella metrica, solo se la policy è marcata come «proseguì».

2.9.1 Registrazione di una policy

Per attivare una nuova policy dalla sezione di rate limiting si procede utilizzando il pulsante *Aggiungi* che apre il form di Fig. 2.32.

Si compilano i campi seguenti:

- *Policy*: la policy da attivare. Si compone di:
 - *Nome*: Identificativo univoco della policy.
 - *Stato*: Lo stato della policy. Sono disponibili le seguenti opzioni:
 - * *Abilitato*: le violazioni rilevate saranno gestite in maniera restrittiva (negazione del servizio).

Erogazioni > api-monitor v1 (Ente) > Configurazione > Rate Limiting > Aggiungi

Note: (*) Campi obbligatori

Policy

Nome *

Stato ⓘ

Elaborazione ⓘ

Identificazione Policy ⓘ

Criteri

Metrica ⓘ

Intervallo Osservazione ⓘ

Applicata solo in presenza di Congestione del Traffico ⓘ

Applicata solo in presenza di Degrado Prestazionale ⓘ

Valori di Soglia

Ridefinisci Valori di Soglia

Num. Massimo Richieste

Raggruppamento

Se abilitato, il calcolo del valore della soglia avviene raggruppando le richieste in funzione dei criteri selezionati

Stato ⓘ

Filtro

Stato ⓘ

SALVA

Fig. 2.32: Attivazione di una policy di Rate Limiting

- * *WarningOnly*: la 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*: La policy è disabilitata.
- *Elaborazione*: Indica quale azione attuare per la policy, nell'ambito del flusso di elaborazione delle policy di eguale metrica, nel caso in cui venga superato il controllo (maggiori dettagli sull'algoritmo di valutazione delle policy sono disponibili nella sezione *Criteri di valutazione delle policy*):
 - * *Interrompi*: non verranno valutate ulteriori policy che seguono nell'ordine tra quelle di eguale metrica.
 - * *Proseguì*: si procede con la valutazione della successiva policy nell'ordine tra quelle di eguale metrica.
- *Identificazione Policy*: Scelta tra due opzioni:
 - * *Scegli Criteri*: permette di indicare direttamente i criteri che la politica deve garantire; tra i criteri utilizzabili: la metrica (numero richieste, occupazione banda, tempi medi, ...), l'intervallo temporale (minuto, ora, giorno) e le condizioni di applicabilità (congestione, degrado prestazionale).
 - * *Selezione dal Registro*: permette di utilizzare una politica arbitraria, precedentemente definita dall'utente.

Nota: La descrizione che segue assume che venga attuata una identificazione della policy per criteri. Per i dettagli sulla configurazione di policy personalizzate dall'utente si faccia riferimento alla sezione *Rate Limiting*.

- *Criteri*: devono essere forniti la metrica e l'intervallo di osservazione scelti tra i valori descritti in precedenza (*Rate Limiting*). Possono inoltre essere indicate le seguenti opzioni:
 - * *Applicata solo in presenza di Congestione del Traffico*: attivando questa opzione la policy risulta applicabile solo nel caso in cui il gateway sia entrato in modalità «Congestione», sulla base di quanto descritto nella sezione *Controllo del Traffico*.
 - * *Applicata solo in presenza di Degrado Prestazionale*: attivando questa opzione la policy risulta applicabile solo nel caso in cui il gateway abbia rilevato un degrado prestazionale e cioè un tempo medio di risposta del servizio superiore alla soglia configurata.
- *Valori di Soglia*: Le soglie per la valutazione della policy:
 - *Ridefinisci Valori di Soglia*: Opzione che consente di variare la soglia predefinita.
 - *Soglia*: Questo campo riporta, in base alla metrica selezionata sopra, il valore di riferimento. Tale valore risultà modificabile attivando l'opzione al punto precedente.
 - *Raggruppamento*: In questa sezione è possibile attivare optionalmente alcuni criteri per il raggruppamento dei dati utilizzati come soglie di confronto. Ad esempio se la policy limita a 20 il numero di richieste su base per minuti, significa che al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, si otterrà una violazione della policy. Aggiungendo un raggruppamento per risorsa, saranno conteggiate separatamente le richieste in base alla specifica risorsa invocata. In questo caso la policy risulterà violata solo al raggiungimento della ventunesima richiesta, nella stessa finestra temporale, relativa alla medesima risorsa. 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:
 - * *Risorsa/Azione*: il valore di soglia rappresenta il totale per ciascuna azione/risorsa
 - * *Richiedente*: il valore di soglia rappresenta il totale ripartito per ciascun mittente
 - * *Token*: il valore di soglia rappresenta il totale ripartito tra le richieste in base al token di provenienza. Si possono specificare i «claims» da prendere in considerazione per distinguere i token.

- * *Chiave*: il valore di soglia rappresente il totale ripartito tra le richieste raggruppate in base ad una chiave personalizzata il cui valore viene fornito secondo uno dei metodi selezionati tra i seguenti:
 - *Header HTTP*: La chiave è presente nell'header di trasporto indicato nella proprietà «Nome».
 - *Url di Invocazione*: La chiave è presente nella URL ricavabile tramite l'espressione regolare fornita nell'elemento seguente.
 - *Parametro della Url*: La chiave viene fornita in modalità Form Encoded con il parametro indicato nell'elemento «Nome».
 - *SOAPAction*: La chiave corrisponde al valore della SoapAction.
 - *Contenuto*: La chiave è presente nel body del messaggio e viene ricavata tramite una espressione XPath o JsonPath fornito nell'elemento seguente.
 - *Client IP*: La chiave corrisponde all'indirizzo IP del client.
 - *X-Forwarded-For*: La chiave corrisponde all'indirizzo IP del client presente negli header http utilizzati per il mantenimento dell'IP di origine nel caso di nodi intermedi (es. X-Forwarded-For).
 - *Plugin Personalizzato*: La chiave viene restituita tramite l'esecuzione di una classe il cui nome viene fornito con il campo «Tipo». Per maggiori dettagli si rimanda alla sezione *Filtro o Raggruppamento Personalizzato*
- *Filtro*: Abilitando questa sezione è possibile indicare i criteri affinché la policy sia applicabile in base alle caratteristiche di ciascuna richiesta in ingresso. In assenza di filtro, la policy sarà valutata su tutte le richieste in ingresso che riguardano l'erogazione/fruizione che si sta configurando. Per la creazione del filtro sono disponibili i seguenti campi:
 - *Risorsa/Azione*: Opzione per filtrare le richieste in base all'azione/risorsa invocata.
 - *Ruolo Richiedente*: Opzione per filtrare le richieste in base al ruolo posseduto dal richiedente (sia che si tratti di un soggetto che di un applicativo).
 - *Soggetto o Applicativo Fruitore*: In alternativa al filtro per ruolo, è possibile specificare un soggetto fruitore ed eventualmente uno dei suoi applicativi.
 - *Chiave*: Si tratta di un'opzione avanzata che consente di filtrare le richieste in ingresso sul gateway in base ad una chiave che può essere specificata in maniera personalizzata effettuando una delle seguenti scelte per il campo *Tipologia*:
 - * *Header HTTP*: Occorre fornire i dati “Nome” e “Valore”. La policy si applicherà soltanto alle richieste che hanno un header http che corrisponde.
 - * *Url di Invocazione*: 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.
 - * *Parametro della Url*: Occorre fornire i dati “Nome” e “Valore”. La policy si applicherà soltanto alle richieste che contengono nella url di invocazione un parametro corrispondente ai dati forniti.
 - * *SOAPAction*: Occorre fornire il dato “Valore”. La policy si applicherà soltanto alle richieste che si presentano con una SOAPAction avente il valore fornito.
 - * *Contenuto*: Occorre fornire i dati “Pattern” e “Valore”. La policy si applicherà soltanto alle richieste dove, applicando l'espressione XPath o JsonPath al messaggio di richiesta, si ottiene un valore identico a quello fornito.
 - * *Client IP*: La policy si applicherà soltanto alle richieste che provengono dall'indirizzo IP indicato.
 - * *X-Forwarded-For*: La policy si applicherà soltanto alle richieste che provengono dall'indirizzo IP indicato presente negli header http utilizzati per il mantenimento dell'IP di origine nel caso di nodi intermedi (es. X-Forwarded-For).

- * *Plugin Personalizzato*: Permette di definire un criterio di filtro personalizzato. Per maggiori dettagli si rimanda alla sezione *Filtro o Raggruppamento Personalizzato*

2.9.2 Criteri di valutazione delle policy

Le policy di rate limiting create, per la data erogazione/fruizione, sono visualizzate in un elenco che filtra automaticamente su una singola metrica (ad esempio «Numero Richieste» o «Occupazione Banda»). L'elenco delle policy visualizzato è analogo a quello riportato in Fig. 2.33.

Rate Limiting							
	Ordine	Stato	Nome	Soglia	Runtime	Elaborazione	
■	▼	✓	numeroMax	100	Visualizza	↓	
■	^ ▼	✓	limiteMaxGiornaliero	1000	Visualizza	×	
■	^	✓	sogliaMinuto	10	Visualizza	×	

[ELIMINA](#) [AGGIUNGI](#)

Fig. 2.33: Elenco delle policy di Rate Limiting

Ciascun elemento in elenco riporta le seguenti informazioni:

- *Ordine*: pulsanti per variare la posizione della policy nell'elenco per la data metrica.
- *Stato*: lo stato di abilitazione della policy, sulla base di quanto descritto in precedenza (*Registrazione di una policy*).
- *Nome*: il nome della policy.
- *Soglia*: il valore di soglia impostato per la policy.
- *Runtime*: permette di effettuare una verifica in tempo reale della metrica interrogando il runtime del gateway. Maggiori dettagli sono presenti nella sezione *Visualizzazione Statistiche Policy*.
- *Elaborazione*: flusso di elaborazione (proseguì, interrompi) nel caso di superamento del controllo relativo alla policy.

L'elenco delle policy può essere aggiornato utilizzando il meccanismo di filtro presente nell'intestazione della tabella. Sono disponibili le seguenti opzioni:

- *Metrica*: permette di stabilire le policy da visualizzare in base alla rispettiva metrica.
- *Ricerca*: permette di visualizzare le policy in base alla presenza di un pattern nel nome.

Per ogni richiesta relativa alla specifica erogazione/fruizione viene applicato l'algoritmo di valutazione delle policy che è il seguente:

- le policy vengono raggruppate «per metrica» e per ogni metrica vengono valutate nell’ordine di elenco prima utilizzando le politiche di Rate Limiting definite sull’API e poi, se esistenti, le politiche a valenza globale (*Policy Globali*).
- per ogni metrica vengono valutate le policy applicabili, cioè per le quali risultano soddisfatti il filtro e le condizioni di applicabilità.
- se la policy viola i livelli di soglia previsti, la transazione viene bloccata (o segnalata se configurata come «warning only») e la valutazione delle policy viene terminata.
- se la policy non viola invece i livelli di soglia previsti, si prosegue nella valutazione di ulteriori policy per quella metrica, solo se la policy è marcata come «proseguì».

2.10 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.

Erogazioni > Configurazioni di PetstoreAPI:1 (EnteInterno) > **Validazione di Default**

Validazione

Stato	abilitato
Tipo	Schemi XSD

Invia **Cancella**

Fig. 2.34: Validazione dei messaggi

Compilare il form di configurazione (Fig. 2.34):

- *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 transitano 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.

2.11 Caching Risposta

In GovWay è possibile abilitare il salvataggio delle risposte in una cache sia globalmente, in modo che sia attivo per tutte le APIs, che singolarmente sulla singola erogazione o fruizione. Questa funzionalità permette ad un backend server di non dover riprocessare le stesse richieste più volte.

Tramite il collegamento *Caching Risposta*, presente nella sezione di configurazione della specifica erogazione/fruizione, è possibile agire sulla configurazione di tale funzionalità. L’impostazione permette di ridefinire la configurazione globale; i campi del form sono i medesimi descritti nella configurazione globale (sezione *Caching Risposta*).

2.12 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.

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

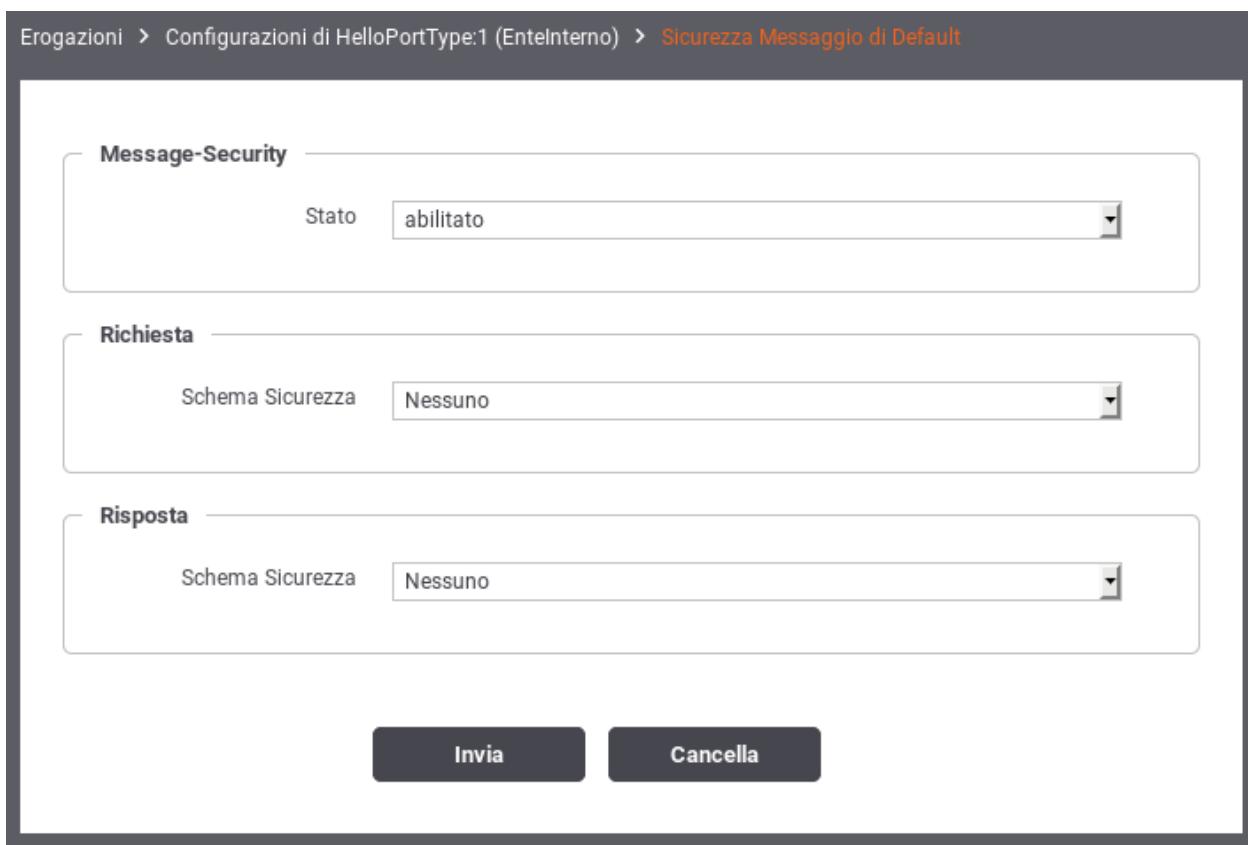


Fig. 2.35: Abilitazione Sicurezza Messaggio

- *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.

2.13 Trasformazioni

Tra le attività di elaborazione, svolte dal gateway sui flussi di comunicazione in ingresso e uscita, vi è la possibilità di applicare delle *Regole di Trasformazione* che consentono di modificare dinamicamente i contenuti in transito prima che vengano instradati alla relativa destinazione.

2.13.1 Valori dinamici

Le regole di trasformazione possono avvalersi di un contesto di risorse, con valori aggiornati dinamicamente dal gateway, cui attingere per le trasformazioni da attuare. Tali risorse sono utilizzabili quando si procede con la definizione di una regola di trasformazione. Elenchiamo le risorse disponibili:

- header.NAME: valore dell'header http, corrispondente all'identificativo NAME, della richiesta e/o della risposta.
- query.NAME: valore di un parametro della url di invocazione, corrispondente all'identificativo NAME.

- urlRegExp:EXPR: applicazione di un'espressione regolare, rappresentata dal valore EXPR, alla url di invocazione.
- xPath:EXPR: applicazione di un'espressione XPath, rappresentata dal valore EXPR, al messaggio xml o in alternativa un'espressione JsonPath se si tratta di un messaggio Json.
- transaction.id: l'identificativo UUID della transazione corrente.
- date:FORMAT: la data di elaborazione del messaggio; il formato fornito deve essere conforme a quanto richiesto dalla classe java “java.text.SimpleDateFormat” (es. \${date:yyyyMMdd_HHmmssSSS})
- busta:FIELD: accesso alle informazioni proprie del profilo di interoperabilità utilizzato; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.protocol.sdk.Busta” (ad es. per il mittente usare *busta.mittente*)
- property:NAME: accesso alle proprietà contenute nella traccia (ad esempio l'identificativo SDI); Il valore “NAME” indica il nome della proprietà da utilizzare.
- tokenInfo:FIELD: accesso ai claim di un token precedentemente validato; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.pdd.core.token.InformazioniToken” (es. per ottenere il valore del claim “sub” usare \${tokenInfo:sub})
- transportContext:FIELD: accesso ai dati della richiesta http; il valore “FIELD” fornito deve rappresentare un field valido all'interno della classe “org.openscoop2.utils.transport.http.HttpServletTransportRequestContext” (es. per il principal usare \${transportContext:credential.principal})

L'utilizzo dei suddetti elementi, come placeholder all'interno di template, comporta l'automatica sostituzione con il valore attuale a runtime da parte del gateway.

La sintassi per accedere le proprietà dinamiche sopraelencate è differente in base allo specifico contesto di utilizzo. Se si tratta di un testo interpretato direttamente da GovWay le proprietà saranno direttamente accessibili utilizzando il seguente formato:

- \${header:NAME}
- \${query:NAME}
- \${xPath:EXPR}
- \${jsonPath:EXPR}
- \${urlRegExp:EXPR}
- \${transaction:id}
- \${date:FORMAT}
- \${busta:FIELD}
- \${property:NAME}
- \${tokenInfo:FIELD}
- \${transportContext:FIELD}

Nei casi in cui il testo della trasformazione è interpretato da framework esterni (quali Freemarker o Velocity) le proprietà vengono rese disponibili da Govway inizializzando una mappa contenente i valori come oggetti. In questo caso le chiavi della mappa sono le seguenti (tra parentesi sono indicati i tipi di dato corrispondenti):

- header (java.util.Properties)
- query (java.util.Properties)
- xPath (org.openscoop2.pdd.core.dynamic.PatternExtractor)
- jsonPath (org.openscoop2.pdd.core.dynamic.PatternExtractor)

- urlRegExp (org.openscoop2.pdd.core.dynamic.URLRegExpExtractor)
- transactionId (java.lang.String)
- date (java.util.Date)
- busta (org.openscoop2.protocol.sdk.Busta)
- property (java.util.Properties)
- tokenInfo (org.openscoop2.pdd.core.token.InformazioniToken)
- transportContext (org.openscoop2.utils.transport.http.HttpServletTransportRequestContext)

Nel caso di utilizzo di template “Freemarker” o “Velocity” sono disponibili i seguenti ulteriori oggetti:

- class; permette di definire classi. L'utilizzo varia a seconda del tipo di template engine:
 - velocity: class.forName(«my.package.name»)
 - freemarker: class[«my.package.name»]
- new; permette di istanziare una classe. L'utilizzo varia a seconda del tipo di template engine:
 - velocity: new.instance(«my.package.name», »Parametro1», »ParametroN»)
 - freemarker: new(«my.package.name», »Parametro1», »ParametroN»)
- transportContext (org.openscoop2.utils.transport.http.HttpServletTransportRequestContext); permette di accedere ai dati della richiesta http (servlet request, principal ...)
- request/response: permette di accedere al contenuto della richiesta/risposta (org.openscoop2.pdd.core.dynamic.ContentExtractor)
- context (java.util.Map<String, Object>); permette di accedere al contesto della richiesta.
- errorHandler (org.openscoop2.pdd.core.dynamic.ErrorHandler); permette di generare risposte personalizzate che segnalano l'impossibilità di proseguire la trasformazione.

Nel caso di utilizzo di template “ZIP”, “TGZ” o “TAR” sono disponibili le seguenti le proprietà dinamiche, interpretate direttamente da GovWay, utilizzabili per accedere a parti della richiesta o della risposta:

- \${content} : payload http del messaggio
- \${soapEnvelope} : soap envelope del messaggio
- \${soapBody} : contenuto del soap body
- \${attachment[index]} : attachment presente in un messaggio multipart alla posizione indicata dall'intero “index”
- \${attachmentId[id]} : attachment presente in un messaggio multipart che possiede il Content-ID indicato

2.13.2 Trasformazione

Nel contesto della configurazione specifica di una erogazione o di una fruizione si può accedere alla funzionalità «Trasformazioni» per inserire una lista di definizioni che applicano trasformazioni ai flussi in entrata e/o uscita. Le trasformazioni create hanno la struttura di una lista ordinata e a ciascun elemento della lista è associato un insieme di criteri di applicabilità. La logica del gateway è quella di analizzare le trasformazioni nell'ordine della lista, selezionando la prima di esse i cui criteri di applicabilità sono tutti soddisfatti.

Tramite il pulsante *Aggiungi* è possibile inserire una nuova trasformazione (Fig. 2.36).

La creazione di una trasformazione richiede che vengano inseriti i seguenti dati:

- Nome: identificativo che rappresenta il nome assegnato alla trasformazione

The screenshot shows a web-based configuration interface for creating a new transformation. At the top, a breadcrumb navigation path is visible: Erogazioni > api-config v1 (Ente) > Configurazione > Trasformazioni > Aggiungi. Below this, a note states "Note: (*) Campi obbligatori". The main section is titled "Trasformazione" and contains the following fields:

- Nome ***: A text input field.
- Applicabilità**: A group of three dropdown menus:
 - Risorse**: Set to "Qualsiasi".
 - Content Type**: An empty input field with an information icon (i).
 - Pattern**: An empty input field with an information icon (i).
- SALVA**: A dark blue rectangular button at the bottom left.

Fig. 2.36: Nuova Trasformazione

- **Applicabilità**: sono i campi che vanno a comporre il criterio di applicabilità della trasformazione:
 - **Risorse/Azioni**: le operazioni sulle quali è applicabile la trasformazione.
 - **Content-Type**: i content-type sui quali è applicabile la trasformazione.
 - **Pattern**: il pattern inserito viene confrontato con il messaggio di richiesta del flusso di comunicazione al fine di verificare l'eventuale match. Il pattern può essere espresso nella sintassi «XPath», nel caso di messaggi XML, o JSONPath, nel caso di messaggi JSON.

Le trasformazioni create sono visualizzate nella forma di elenco ordinato (Fig. 2.37). L'icona iniziale di ciascun elemento consente di modificarne la posizione.

Ciascuna regola elencata visualizza i dati che sono stati forniti come criterio di applicabilità. A quelli inseriti in fase di creazione si aggiungono i Soggetti e gli Applicativi, che possono essere forniti accedendo i rispettivi collegamenti. I soggetti/applicativi associati ad una regola saranno confrontati con l'identità del soggetto/applicativo mittente di ciascuna richiesta.

Accedendo il dettaglio di una regola di trasformazione vengono presentate le due sezioni:

- **Trasformazione**: per aggiornare il nome o i criteri di applicabilità.
- **Regole di Trasformazione**: per aggiornare le regole di trasformazione attuate sulla richiesta e sulla risposta.

Regole di Trasformazione della Richiesta

Selezionando il collegamento «Richiesta», nel riquadro delle Regole di Trasformazione, si procede con la definizione formale della trasformazione attuata sulle richieste in ingresso sulle quali è applicabile la trasformazione corrente. Le trasformazioni possono essere applicate sia a livello del trasporto che del contenuto, come mostrano le sezioni visualizzate in Fig. 2.38.

Trasformazioni							
		Nome	Risorse	Content Type	Pattern	Soggetti	Applicativi
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trasformazione Delete	DELETE /api/{nome}/{versione}, DELETE /api/{nome}/{versione}/allegati/{nome_allegato}, DELETE /api/{nome}/{versione}/risorse/{nome_risorsa}, DELETE /api/{nome}/{versione}/servizi/{nome_servizio}, DELETE ...	application/json		Soggetti (0)	Applicativi (0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trasformazione Standard	Qualsiasi	application/json		Soggetti (0)	Applicativi (0)

[ELIMINA](#) [AGGIUNGI](#)

Fig. 2.37: Lista regole di trasformazione

Trasformazione

Trasporto

[HTTP Headers \(0\)](#)
[URL Parameters \(0\)](#)

Contenuto

Abilitato

[SALVA](#)

Fig. 2.38: Regola di trasformazione della richiesta

A livello del trasporto è possibile applicare trasformazioni sugli «HTTP Headers», selezionando l'omonimo collegamento e quindi aggiungendo le operazioni da effettuare ([Fig. 2.39](#)).

Note: (*) Campi obbligatori

HTTP Header

Operazione *

Nome *

Valore * ⓘ

SALVA

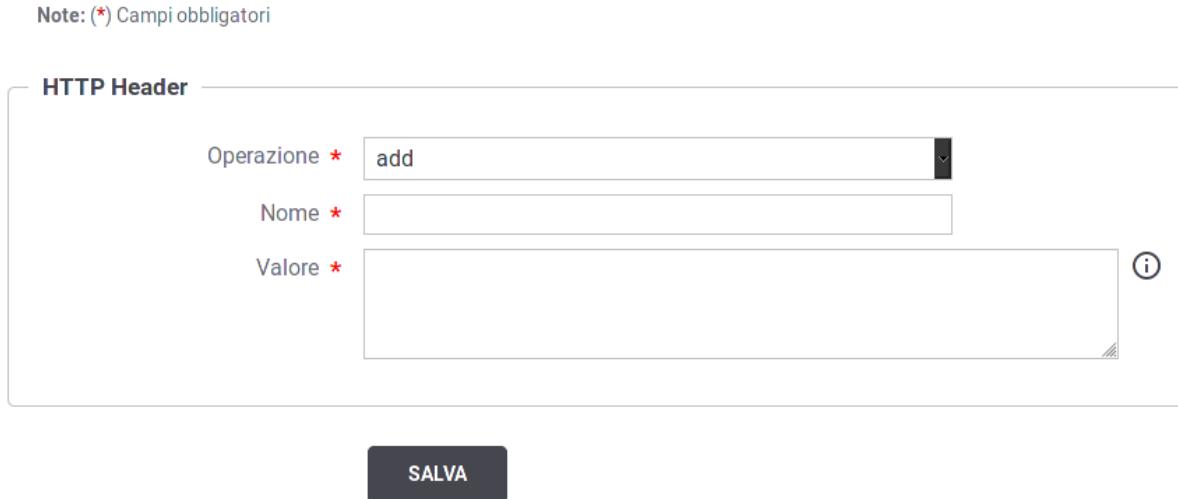


Fig. 2.39: Operazioni sugli Header HTTP

Ciascuna operazione può essere selezionata tra le seguenti:

- add: per aggiungere un nuovo header specificando successivamente nome e valore
- delete: per eliminare un header indicandone successivamente il nome
- update: per modificare un header indicandone successivamente il nome ed il nuovo valore
- updateOrAdd: per modificare un header indicandone successivamente il nome ed il nuovo valore. Nel caso l'header non si presente, verrà aggiunto.

Nota: i valori specificati per gli header http possono contenere le proprietà dinamiche descritte nella sezione [Valori dinamici](#).

Sempre a livello del trasporto è possibile applicare trasformazioni anche sui parametri presenti nella Query String, selezionando il collegamento «URL Parameters». La modalità di configurazione è del tutto analoga a quanto appena descritto per gli Header HTTP.

Abilitando l'opzione sul Contenuto è possibile procedere con la definizione di operazioni sul contenuto della richiesta ([Fig. 2.40](#)).

Per la modifica del contenuto della richiesta devono essere forniti i seguenti dati:

- Tipo Conversione: indica il tipo di trasformazione da applicare al contenuto. Si può scegliere una tra le seguenti opzioni:
 - HTTP Payload Vuoto: opzione presente nel caso REST. Il contenuto della richiesta diventa un payload http vuoto.

Contenuto

Abilitato	<input checked="" type="checkbox"/>
Tipo Conversione	Template ▼ ⓘ
Template *	<input type="button" value="Browse..."/> No file selected.
Content Type	<input type="text"/>

Fig. 2.40: Modifica del Contenuto della Richiesta

- SOAP Body Vuoto: opzione presente nel caso SOAP. Il contenuto della richiesta diventa un messaggio SOAP con SoapBody vuoto.
- Template: il contenuto della richiesta viene assegnato utilizzando il template fornito in configurazione.
- Freemaker Template: il contenuto della richiesta viene assegnato utilizzando il template «Freemaker» (<https://freemarker.apache.org/>) fornito in configurazione.
- Freemaker Template (Archivio Zip): il file fornito deve essere un archivio zip contenenti dei files che rispettano la sintassi del template engine “Freemaker”. Viene richiesta la presenza, all’interno dell’archivio zip, di un file indice che possieda il nome “index.ftl”.
- Velocity Template: il contenuto della richiesta viene assegnato utilizzando il template «Velocity» (<http://velocity.apache.org/>) fornito in configurazione.
- Velocity Template (Archivio Zip): il file fornito deve essere un archivio zip contenenti dei files che rispettano la sintassi del template engine “Velocity”. Viene richiesta la presenza, all’interno dell’archivio zip, di un file indice che possieda il nome “index.vm”.
- XSLT: il contenuto della richiesta viene modificato applicando la trasformazione XSLT fornita in configurazione. Questo metodo è applicabile nel caso di messaggi XML o SOAP.
- ZIP Compressor: il contenuto della richiesta verrà trasformato in un archivio zip il cui contenuto viene definito dal file fornito che deve contenere proprietà indicate come nome=valore in ogni linea. Il nome della proprietà corrisponde all’entry name all’interno dell’archivio (es. dir/subDir/entryName1). Il valore della proprietà corrisponde al contenuto dell’entry. È possibile selezionare parti del messaggio, per associarle come contenuto dell’entry, utilizzando le espressioni dinamiche risolte a runtime dal Gateway (sezione *Valori dinamici*).
- TGZ Compressor: il contenuto della richiesta verrà trasformato in un archivio tgz il cui contenuto è definito tramite il file fornito che deve possedere la medesima struttura descritta per il tipo “ZIP”.
- TAR Compressor: il contenuto della richiesta verrà trasformato in un archivio tar il cui contenuto è definito tramite il file fornito che deve possedere la medesima struttura descritta per il tipo “ZIP”.
- Template: nei casi che lo prevedono, con questo elemento si fornisce il template da utilizzare per ottenere il nuovo contenuto della richiesta.
- Content-Type: optionalmente, tramite questo elemento, è possibile assegnare un content-type alla richiesta modificata.

Nota: i template possono contenere le proprietà dinamiche descritte nella sezione *Valori dinamici*. La sintassi adottata dipende dal template. Una finestra di help contestuale, presente nell’interfaccia, guiderà l’utente nell’applicazione della sintassi corretta.

Conversione da REST a SOAP

Una particolare trasformazione del contenuto della richiesta è quella di convertire il formato da REST a SOAP. Questa funzionalità si ottiene abilitando la sezione «Trasformazione SOAP», presente nel caso di servizi REST. I dati da fornire per la configurazione sono (Fig. 2.41):

- Versione: selezione della versione del protocollo SOAP
- SOAP Action: indicazione della SOAP Action da utilizzare
- Imbustamento SOAP: se il messaggio ottenuto con le operazioni di trasformazione applicate non è in formato SOAP è possibile decidere di far generare al gateway gli elementi di imbustamento. Le opzioni possibili sono:
 - Disabilitato: nessun imbustamento.
 - Utilizza contenuto come SOAP Body: il contenuto attuale viene utilizzato come SOAP Body nel contesto dell’envelope creato.
 - Utilizza contenuto come Attachment: il contenuto attuale viene inserito come attachment relativo al messaggio SOAP generato. Se viene selezionata questa opzione dovranno essere forniti ulteriori dati, quali:
 - * Content Type Attachment: è possibile specificare un Content-Type per l’attachment.
 - * SOAP Body: stabilire quale deve essere il contenuto del SOAP Body. Per questo punto si procede analogamente a quanto già descritto per la trasformazione del contenuto principale della richiesta.

Trasformazione SOAP

Abilitato	<input checked="" type="checkbox"/>
Versione	SOAP 1.1
SOAP Action	test
Imbustamento SOAP	Utilizza contenuto come SOAP Body

Fig. 2.41: Conversione da REST a SOAP

Conversione da SOAP a REST

Una particolare trasformazione del contenuto della richiesta è quella di convertire il formato da SOAP a REST. Questa funzionalità si ottiene abilitando la sezione «Trasformazione REST», presente nel caso di servizi SOAP. I dati da fornire per la configurazione sono (Fig. 2.42):

- Path: path della risorsa cui deve fare riferimento il nuovo messaggio di richiesta REST-

- HTTP Method: il metodo HTTP utilizzato.

Trasformazione Rest

Abilitato	<input checked="" type="checkbox"/>
Path *	<input type="text"/> (i)
HTTP Method	<input type="text" value="GET"/> ▼

Fig. 2.42: Conversione da SOAP a REST

Regole di Trasformazione della Risposta

Analogamente a quanto visto per la richiesta è possibile utilizzare il link «Risposte», nell'area «Regole di Trasformazione», per procedere con l'impostazione di regole per trasformare le risposte. A differenza del caso della richiesta, dove si può definire un unico meccanismo di trasformazione, in questo caso è possibile definire diverse regole di trasformazione basate sulla casistica delle risposte che si può presentare.

Quando si aggiunge una nuova regola di trasformazione della risposta si procede inserendo le seguenti informazioni (Fig. 2.43):

- Nome: nome assegnato alla regola di trasformazione
- Codice Risposta: Come criterio di applicabilità della regola, è possibile indicare il codice di risposta con le seguenti opzioni:
 - Qualsiasi: qualunque codice di risposta ottenuto
 - Singolo: si inserisce un specifico codice di risposta per il quale è applicabile la regola
 - Intervallo: si inseriscono gli estremi dell'intervallo di codici di risposta per il quale è applicabile la regola
- Content-Type: criterio di corrispondenza con uno dei content-type indicati
- Pattern: espressione XPath o JsonPath da confrontare con il contenuto della risposta per un eventuale match

Le operazioni di trasformazione sulla risposta sono attuabili in maniera del tutto analoga a quanto già descritto per la richiesta. Diversamente dal caso della richiesta, al posto delle modifiche sui parametri della URL (non presenti nella risposta) è possibile modificare il Codice Risposta restituito.

Nota: Se sulla richiesta si è scelto di attuare la conversione da SOAP a REST, o viceversa, la trasformazione complementare risulterà disponibile anche nella configurazione della risposta.

2.14 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 sin-

Erogazioni > api-config v1 (Ente) > Configurazione > Trasformazioni > Trasformazione Standard > Risposte > Aggiungi

Note: (*) Campi obbligatori

Trasformazione

Nome *

Applicabilità

Codice Risposta *

Content Type ⓘ

Pattern ⓘ

SALVA

The screenshot shows a web-based configuration interface for creating a response transformation rule. At the top, a breadcrumb navigation path is visible: Erogazioni > api-config v1 (Ente) > Configurazione > Trasformazioni > Trasformazione Standard > Risposte > Aggiungi. Below the path, a note indicates that certain fields are mandatory (marked with a red asterisk). The main section is titled 'Trasformazione' and contains several input fields: 'Nome' (Name) with a mandatory field indicator (*), 'Applicabilità' (Applicability) set to 'Intervallo' (Interval), 'Content Type' (Content Type) with an information icon (ⓘ), and 'Pattern' (Pattern) with an information icon (ⓘ). A large 'SALVA' (Save) button is located at the bottom of the form.

Fig. 2.43: Creazione regola di trasformazione della risposta

gola 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 cronologicamente, 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 *Tracciamento*. Le personalizzazioni inserite in questo contesto avranno validità per le sole comunicazioni riguardanti la specifica erogazione/fruizione (Fig. 2.44).

Le sezioni presenti nella pagina sono:

- *Transazioni Registrate:* l'utente ha l'opzione per mantenere il default definito nella sezione di configurazione generale (sezione *Tracciamento*) oppure ridefinirlo.
- *Messaggi Diagnostici:* l'utente ha l'opzione per mantenere il default definito nella sezione di configurazione generale (sezione *Tracciamento*) 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 *Correlazione Applicativa*).

2.15 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.

Per accedere alla configurazione della correlazione applicativa, per una data erogazione/fruizione, si utilizza la sezione «Correlazione Applicativa» presente nell'ambito della configurazione del tracciamento di una fruizione/erogazione (sezione *Tracciamento*).

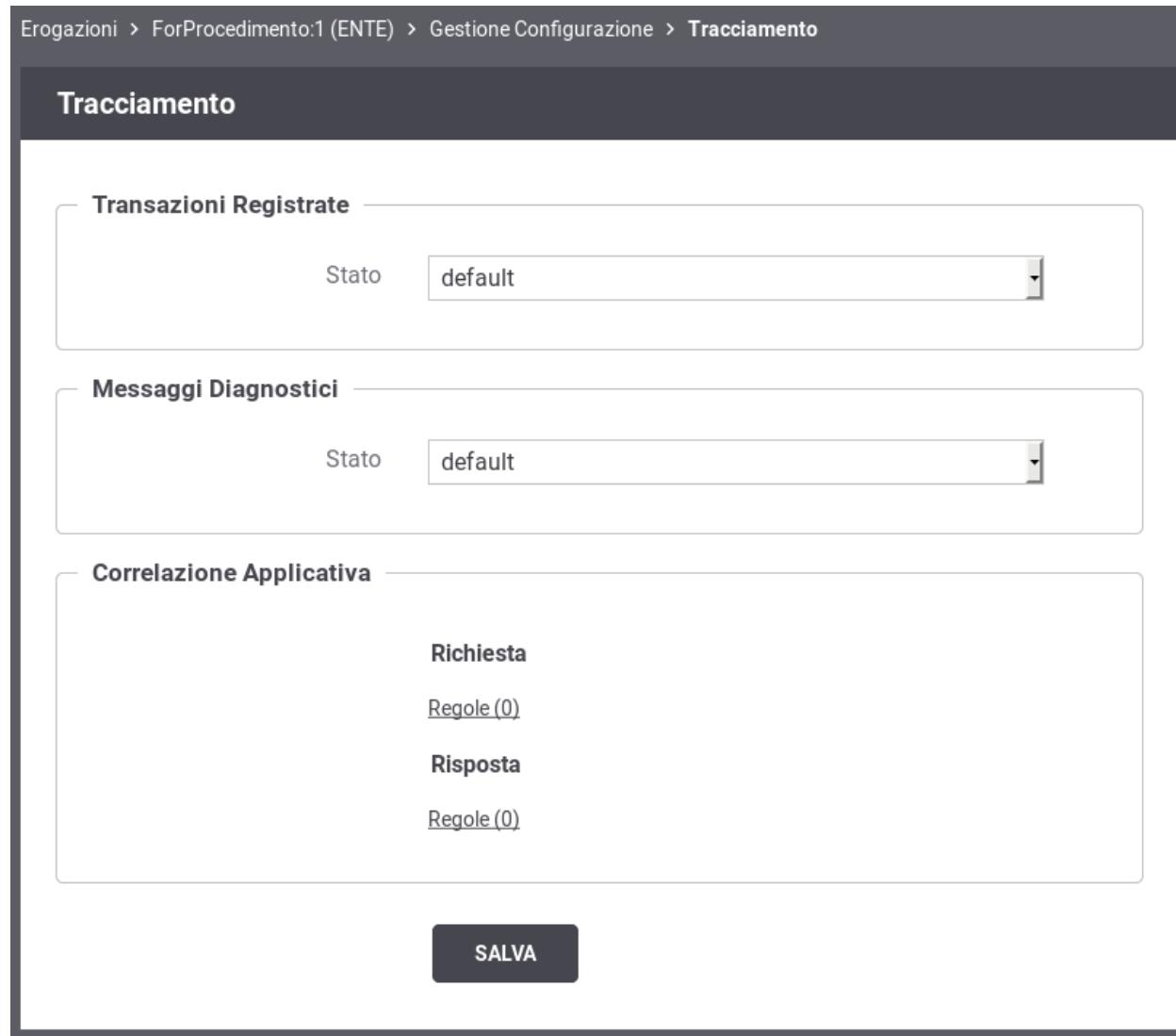


Fig. 2.44: Tracciamento per la singola erogazione/fruizione

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 (Fig. 2.45)

Note: (*) Campi obbligatori

Elemento xml	<input type="text"/>
Il campo vuoto indica qualsiasi elemento	
Modalità identificazione	contentBased
Pattern *	<input type="text"/>
Identificazione fallita	blocca
Riuso ID	disabilitato

Invia **Cancella**

Fig. 2.45: 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:
 - *Url di Invocazione*: 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.
 - *Contenuto*: 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;
 - *Header HTTP*: Il valore viene estratto dall'header di trasporto avente il nome indicato nel campo successivo.
 - *Header di Integrazione*: il valore viene estratto dall'header di integrazione GovWay presente nel valore della proprietà *IDApplicativo*.

- *Disabilitata*: 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.

2.16 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.

2.17 Registrazione Messaggi

Nella sezione *Tracciamento* sono descritte 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.

2.18 Connettore

È possibile modificare le impostazioni del connettore (ad esempio per modificare l'endpoint o aggiungere il proxy) seguendo il collegamento presente nella riga *Connettore* del dettaglio di una erogazione o fruizione. I campi del form sono uguali a quelli già descritti per la fase di creazione dell'erogazione (sezione *Registrazione dell'erogazione*). Ulteriori dettagli di configurazione e tipi di connettore diversi da HTTP e HTTPS sono descritti nella sezione *Connettori*. I contesti in cui l'interfaccia visualizza il valore di un connettore comprendono anche uno strumento per verificare la raggiungibilità dell'indirizzo impostato (Fig. 2.46).

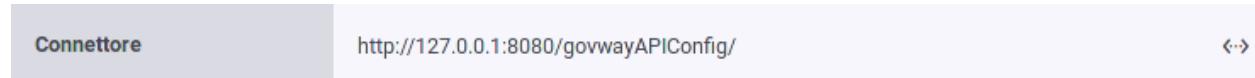


Fig. 2.46: Pulsante per la verifica del connettore

Dopo aver premuto il pulsante si accede ad una schermata che riepiloga le proprietà del connettore e comprende il pulsante *Verifica* per procedere con la verifica (Fig. 2.47).

 A screenshot of a verification page titled 'Verifica Connettività Connettore'. The page shows the configuration details of a connector: 'Connettore' set to 'http://127.0.0.1:8080/govwayAPIConfig/' and 'Autenticazione Http' with 'Utente' as 'amministratore' and 'Password' as '123456'. At the bottom is a large blue button labeled 'VERIFICA'.

Fig. 2.47: Verifica del connettore

Dopo aver premuto il pulsante *Verifica* viene presentato l'esito della verifica di raggiungibilità (Fig. 2.48).

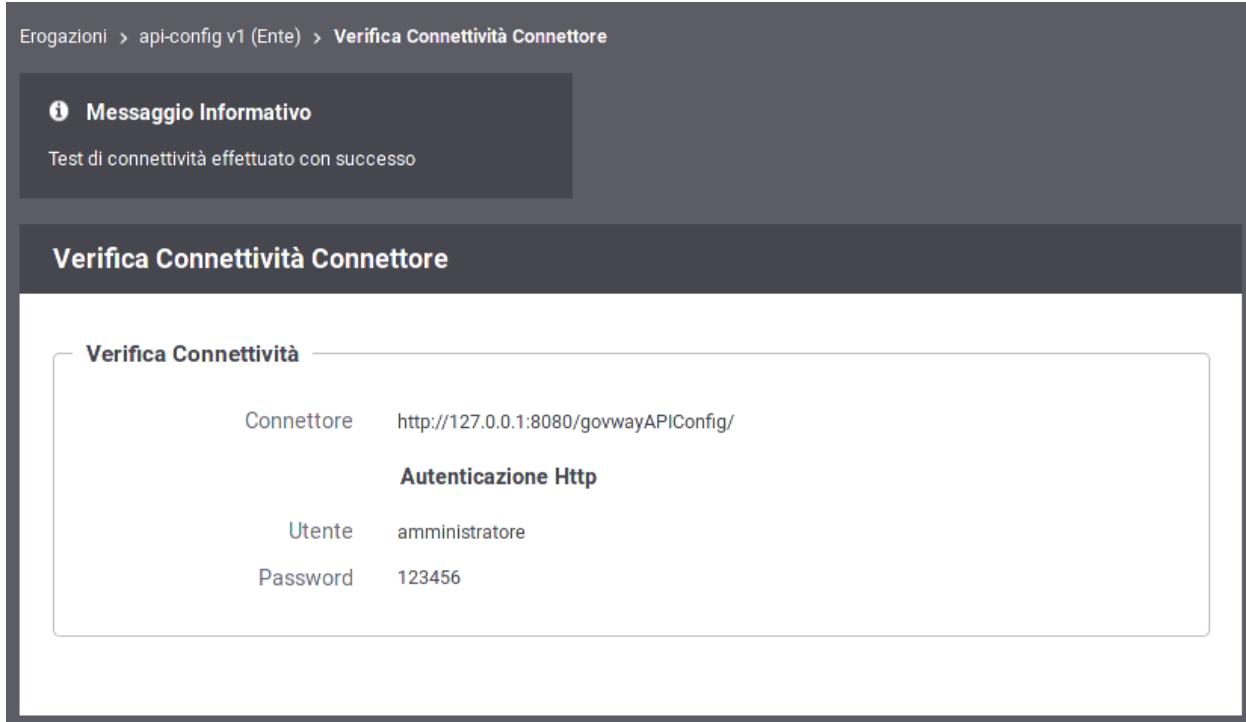


Fig. 2.48: Esito Verifica del connettore

CAPITOLO 3

Profilo “ModI PA”

Il profilo “ModI PA” consente in maniera del tutto trasparente alle applicazioni interne al dominio, la conformità delle API (sia in fruizione che in erogazione) alle nuove *Linee Guida AGID di Interoperabilità* (<https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/bozza/>).

La struttura complessiva del processo di configurazione si mantiene analoga a quanto già descritto per il profilo API Gateway. Le differenze, con rispetto al profilo API Gateway, presentate in questa sezione, riguardano vincoli sulle scelte operabili dalla console e le informazioni di configurazione aggiuntive specifiche per la realizzazione degli scenari in accordo al Modello di Interoperabilità.

3.1 Concetti Preliminari

Il Modello di Interoperabilità mantiene sostanzialmente invariato il concetto di *dominio* di un’amministrazione rispetto a quanto prevedeva il precedente modello SPCoop. Resta quindi fondamentale individuare il perimetro d’azione delle interfacce dei servizi rispetto al sistema informativo dell’ente e i propri interlocutori.

Il concetto di dominio, che riveste particolare importanza nella gestione degli aspetti di sicurezza, si sposa perfettamente con i modelli di configurazione di GovWay dove è possibile attivare:

- *erogazioni di API*: richieste che provengono da amministrazioni esterne al dominio e sono dirette ad applicativi interni.
- *fruizioni di API*: richieste che provengono dagli applicativi interni del dominio e sono dirette verso altre amministrazioni.

La govwayConsole, all’atto della registrazione di Soggetti (Enti/Organizzazioni) e Applicativi (Sistemi/Applicazioni di un ente), consente di specificarne il *Dominio*, interno o esterno, al fine della corretta rappresentazione degli scenari di configurazione dei servizi.

Il profilo ModI PA prevede che i servizi siano basati su SOAP o REST fornendo sempre un descrittore formale delle interfacce basato su uno specifico IDL (Interface Description Language):

- WSDL 1.1 e successivi, per la descrizione delle interfacce SOAP
- OpenAPI 3.0 e successivi, per la descrizione delle interfacce REST

Nel processo di configurazione, tramite la govwayConsole, sono inoltre tenuti in considerazione tutti gli aspetti previsti dalle Linee Guida:

- *URL di Invocazione API*: le linee guida richiedono che deve essere indicato in modo esplicito la tecnologia utilizzata (REST o SOAP) e la versione. Le url con cui vengono esposte le API su GovWay soddisfano entrambi i requisiti.
- *Profili di Interazione*: definiscono la modalità con cui fruitore ed erogatore di un servizio interagiscono. Sono previsti i seguenti due profili:
 - *Bloccante*: il fruitore invia la richiesta e resta bloccato in attesa di ricevere la risposta, completa dei dati attesi, dall'erogatore
 - *Non Bloccante*: il fruitore non resta bloccato dopo aver inviato la richiesta, se non per ricevere una notifica di presa in carico. Per ottenere la risposta sarà necessario effettuare una distinta interazione, prevista nello scenario del servizio.
- *Sicurezza Canale*: gestione della sicurezza inherente il canale di comunicazione tra i domini fruitore ed erogatore. La specifica prevede i seguenti due profili:
 - *[IDAC01] Direct Trust Transport-Level Security*: comunicazione basata sul canale SSL dopo aver effettuato il trust del certificato X509 fornito dal dominio erogatore.
 - *[IDAC02] Direct Trust mutual Transport-Level Security*: comunicazione basata sul canale SSL dopo aver effettuato il trust dei certificati X509, del fruitore e dell'erogatore, nella modalità di mutua autenticazione.
- *Sicurezza Messaggio*: gestione della sicurezza inherente lo scambio di informazioni tra le applicazioni agli estremi del flusso di comunicazione. I profili di sicurezza previsti si distinguono per il caso SOAP e per quello REST:
 - *[IDAS01 o IDAR01] Direct Trust con certificato X.509 su SOAP o REST*: Tramite la validazione del certificato X509, inserito dall'applicazione mittente nel token di sicurezza della richiesta, l'applicativo destinatario verifica la corrispondenza delle identità e la validità del messaggio, prima di procedere con la produzione della risposta.
 - *[IDAS02 o IDAR02] Direct Trust con certificato X.509 su SOAP o REST con unicità del token/messaggio*: estensione del profilo precedente con l'aggiunta di un meccanismo di filtro che impedisce il processamento di un messaggio di richiesta duplicato.
 - *[IDAS03 o IDAR03] Integrità del payload del messaggio SOAP o REST*: profilo che estende i profili precedenti aggiungendo la gestione della firma del payload come verifica di integrità del messaggio ricevuto.
- *URL di Invocazione API*: le linee guida richiedono una indicazione esplicita della tecnologia utilizzata (REST o SOAP) e la versione. Le url con cui vengono esposte le API su GovWay soddisfano entrambi i requisiti.

Tutti questi concetti sono stati recepiti e gestiti nelle maschere di configurazione della govwayConsole, adottando il profilo ModI PA. Le sezioni seguenti illustrano in dettaglio gli elementi di configurazione integrativi rispetto al profilo API Gateway.

3.2 Sicurezza Canale

I profili di sicurezza a livello del canale riguardano le modalità di trasporto dei messaggi tra il dominio fruitore e quello erogatore. La specifica tecnica del Modello di Interoperabilità prevede, per questa tipologia, i seguenti due profili:

- *[IDAC01] Direct Trust Transport-Level Security*: comunicazione basata sul canale SSL dopo aver effettuato il trust del certificato X509 fornito dal dominio erogatore.
- *[IDAC02] Direct Trust mutual Transport-Level Security*: comunicazione basata sul canale SSL dopo aver effettuato il trust dei certificati X509, del fruitore e dell'erogatore, nella modalità di mutua autenticazione.

Il concetto di ente/dominio, previsto dalle specifiche del Modello di Interoperabilità, viene riportato su quello di Soggetto nell'ambito delle entità di configurazione di GovWay.

Vediamo nelle sezioni seguenti come si possono effettuare le configurazioni per i profili di sicurezza canale.

3.2.1 [IDAC01] Direct Trust Transport-Level Security

Questo profilo di sicurezza prevede l'utilizzo del canale HTTPS, per le comunicazioni sul confine tra i due domini, con validazione del certificato dell'ente destinatario della comunicazione.

Descriviamo di seguito i passi di configurazione da effettuare:

- La creazione della relativa API prevede che nella sezione «ModI PA», elemento «Profilo Sicurezza Canale», venga selezionato il profilo «IDAC01» come indicato in Fig. 3.1.

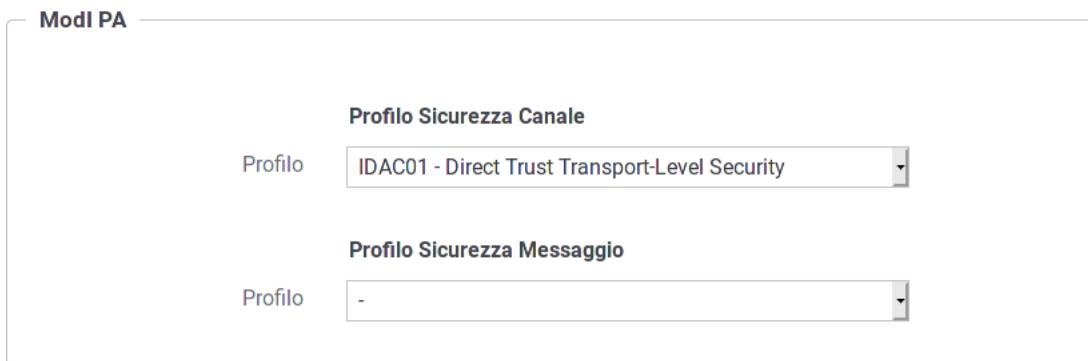


Fig. 3.1: Selezione del profilo IDAC01 per l'API

- Nel caso si voglia configurare una fruizione, le maschere di configurazione terranno conto degli aspetti di sicurezza sul canale garantendo che l'endpoint specificato nel connettore di uscita sia di tipo HTTPS, indipendentemente dal profilo adottato nella API (SSL sempre obbligatorio). L'autenticazione HTTPS può essere gestita opzionalmente da GovWay o, in alternativa, delegata alla configurazione della JVM sull'application server. Per la gestione in GovWay sono disponibili i campi per la configurazione HTTPS, lasciando opzionalmente la possibilità di impostare l'autenticazione client (vedi sez. *Autenticazione Https*).
- Nel caso si voglia configurare una erogazione, il profilo di sicurezza IDAC01 impatta sulla configurazione del Controllo Accessi, previsto nella configurazione specifica dell'erogazione:
 - La sezione «Autenticazione Canale» è impostata a «HTTPS» ammettendo il flag «Opzionale» (Fig. 3.2).

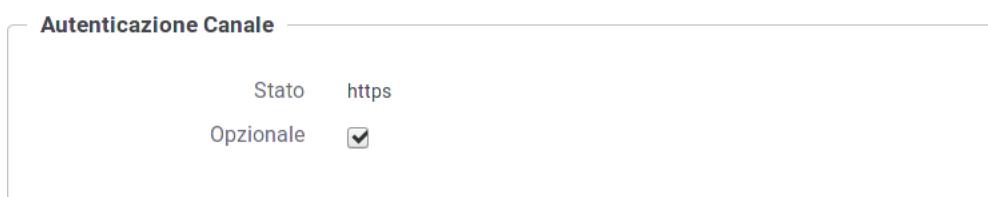


Fig. 3.2: Autenticazione Canale HTTPS con flag opzionale

- La sezione «Autorizzazione Canale» è per default disabilitata (Fig. 3.3). Abilitando tale sezione sarà possibile inserire i criteri di autorizzazione, come descritto nella sez. *Autorizzazione*, con la differenza che in questo caso le politiche saranno riferite esclusivamente ai soggetti censiti in configurazione (e non gli applicativi, per i quali si rimanda alla sez. *Sicurezza Messaggio*).



Fig. 3.3: Autorizzazione Canale Disabilitata

3.2.2 [IDAC02] Direct Trust mutual Transport-Level Security

Questo profilo di sicurezza prevede l'utilizzo del canale HTTPS con autenticazione client, per le comunicazioni sul confine tra i due domini, con reciproca validazione dei certificati degli enti in gioco.

Descriviamo di seguito i passi di configurazione da effettuare:

- La creazione della relativa API prevede che nella sezione «ModI PA», elemento «Profilo Sicurezza Canale», venga selezionato il profilo «IDAC02» come indicato in Fig. 3.4.

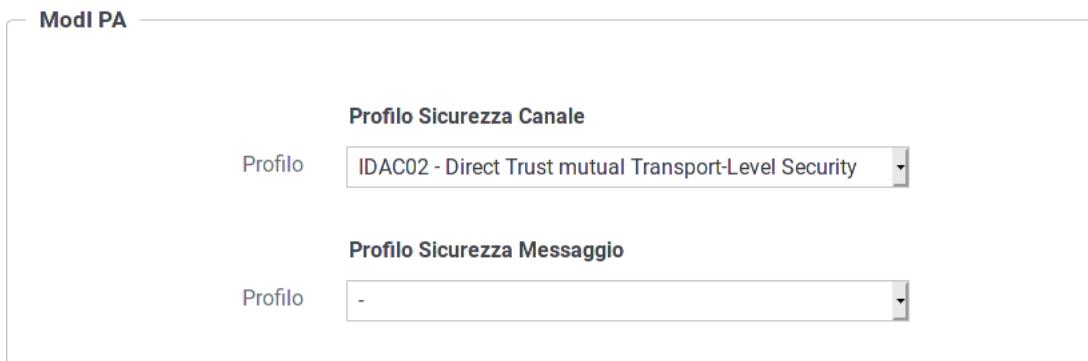


Fig. 3.4: Selezione del profilo IDAC02 per l'API

- Nel caso si voglia configurare una fruizione, le maschere di configurazione terranno conto degli aspetti di sicurezza sul canale garantendo che l'endpoint specificato nel connettore di uscita sia di tipo HTTPS, indipendentemente dal profilo adottato nella API (SSL sempre obbligatorio). L'autenticazione HTTPS può essere gestita optionalmente da GovWay o, in alternativa, delegata alla configurazione della JVM sull'application server. Per la gestione in GovWay sono disponibili i campi per la configurazione HTTPS, con l'obbligo di impostare l'autenticazione client (vedi sez. *Autenticazione Https*).
- Nel caso si voglia configurare una erogazione, il profilo di sicurezza IDAC02 impatta sulla configurazione del Controllo Accessi, previsto nella configurazione specifica dell'erogazione:
 - La sezione «Autenticazione Canale» è impostata forzatamente a «HTTPS» (Fig. 3.5).

3.3 Sicurezza Messaggio

Il profilo di sicurezza sul messaggio definisce le modalità di comunicazione dei messaggi tra componenti interne ai domini delle entità coinvolte. Tali profili sono distinti per il caso SOAP e per quello REST:

- *[IDAS01 o IDAR01] Direct Trust con certificato X.509 su SOAP o REST*: Tramite la validazione del certificato X509, inserito dall'applicazione mittente nel token di sicurezza, l'applicativo destinatario verifica la corrispondenza delle identità e la validità del messaggio, prima di procedere con il processamento del messaggio.

Autenticazione Canale

Stato	https
-------	-------

Fig. 3.5: Autenticazione Canale HTTPS

- Nella sezione «Autenticazione Canale» è possibile attivare l'autorizzazione per richiedente inserendo gli identificativi dei soggetti autorizzati tra quelli identificati tramite il certificato SSL (Fig. 3.6). Abilitando tale sezione sarà possibile inserire i criteri di autorizzazione, come descritto nella sez. *Autorizzazione*, con la differenza che in questo caso le politiche saranno riferite esclusivamente ai soggetti censiti in configurazione (e non gli applicativi, per i quali si rimanda alla sez. *Sicurezza Messaggio*).

Autorizzazione Canale

Stato	abilitato
-------	-----------

Autorizzazione per Richiedente

Abilitato	<input checked="" type="checkbox"/>
Soggetti (1)	

Autorizzazione per Ruoli

Abilitato	<input type="checkbox"/>
-----------	--------------------------

Fig. 3.6: Autorizzazione Canale su soggetti

- [IDAS02 o IDAR02] Direct Trust con certificato X.509 su SOAP o REST con unicità del token/messaggio: estensione del profilo precedente con l'aggiunta di un meccanismo di filtro che impedisce il processamento di un messaggio duplicato.
- [IDAS03 o IDAR03] Integrità del payload del messaggio SOAP o REST: profilo che estende i profili precedenti aggiungendo la gestione della firma del payload come verifica di integrità del messaggio ricevuto.

Le applicazioni di un dominio interno o esterno, descritte negli scenari del Modello di Interoperabilità, vengono rappresentate in GovWay tramite la registrazione di Applicativi come entità di configurazione. In accordo al modello di GovWay, ciascun applicativo è associato al soggetto di riferimento che, nell'ottica ModI PA, rappresenta il dominio di appartenenza.

Per quanto concerne le fruizioni, le richieste che provengono dagli applicativi interni del dominio e sono dirette verso altre amministrazioni vengono arricchite del token di sicurezza ModIPA associato all'operazione invocata. Gli applicativi vengono identificati attraverso una delle modalità di autenticazione previste da GovWay (vedi sez. [Autenticazione Trasporto](#)) ed una volta identificato viene utilizzato il certificato X509 associatogli in fase di registrazione da utilizzare per effettuare la firma del token di sicurezza ModIPA (Fig. 3.7).

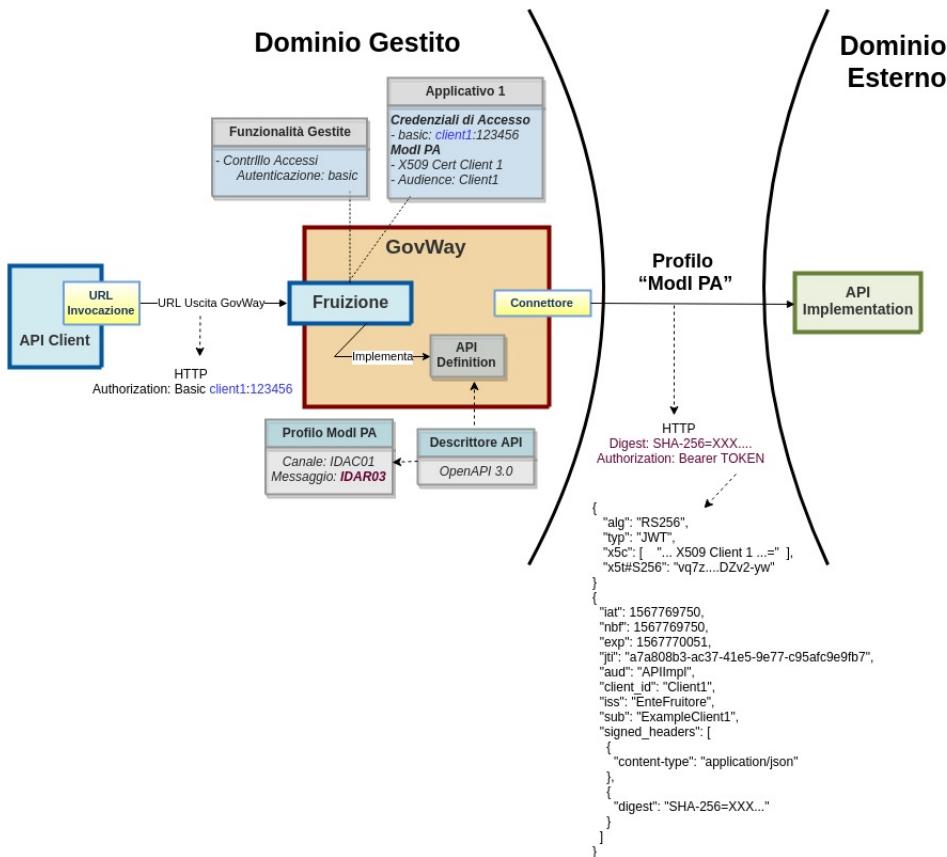


Fig. 3.7: Fruizione con Profilo di Interoperabilità ‘ModI PA’

Nelle erogazioni invece, le richieste provengono da amministrazioni esterne al dominio e sono dirette ad applicativi interni. Prima di procedere con l'inoltro della richiesta verso il backend interno, GovWay valida il token di sicurezza ricevuto rispetto al profilo associato all'operazione invocata: verifica firma, validazione temporale, filtro duplicati, verifica integrità del messaggio ... (Fig. 3.8)

Vediamo nelle sezioni seguenti come si possono effettuare le configurazioni relative ai profili di sicurezza messaggio.

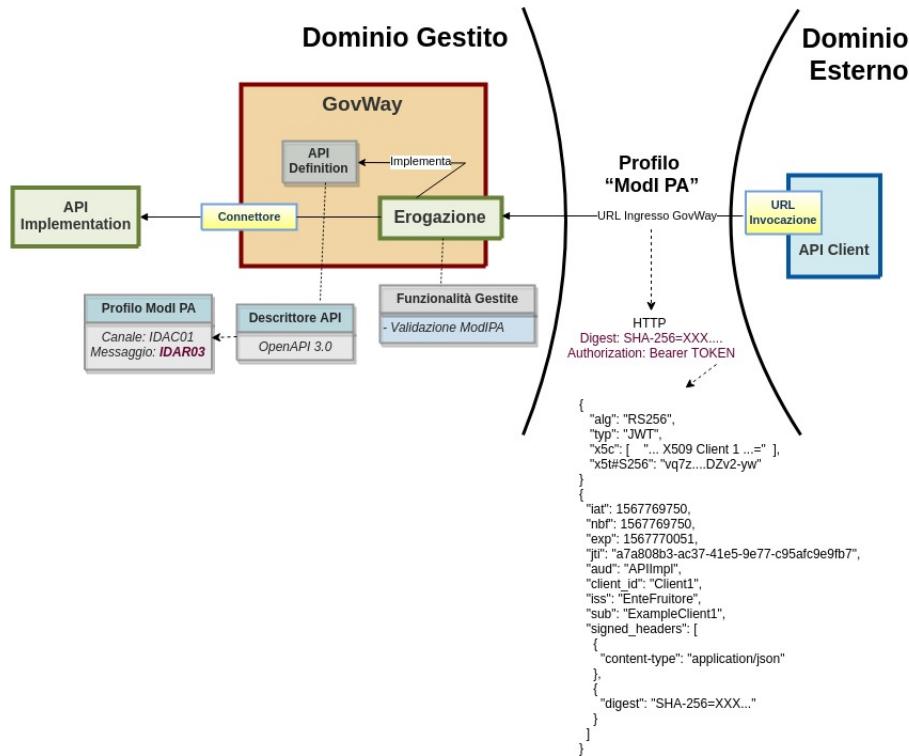


Fig. 3.8: Erogazione con Profilo di Interoperabilità “ModI PA”

3.3.1 Passi preliminari di configurazione

In questa sezione viene indicato come effettuare una configurazione iniziale dei seguenti aspetti di gestione dei certificati X509 utilizzati all'interno dei token di sicurezza “ModI PA”.

TrustStore per la validazione dei Certificati

Per le richieste, provenienti da amministrazioni esterne, GovWay deve validare il certificato presente all'interno del token di sicurezza al fine di verificare che sia rilasciato da una della CA conosciute, che non sia scaduto e che non sia stato eventualmente revocato. Per poter effettuare la validazione, deve essere configurato opportunamente GovWay per quanto riguarda le seguenti proprietà presenti nel file “/etc/govway/modipa_local.properties” (dove si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione) tutte con prefisso “org.openspcoop2.protocol.modipa.sicurezzaMessaggio.certificati.”:

- *trustStore.path* (obbligatorio): indica il path su file system di un trustStore contenente le CA conosciute.
- *trustStore.tipo* (obbligatorio): indica il tipo di trustStore (JKS)
- *trustStore.password* (obbligatorio): password per accedere al trustStore
- *trustStore.crls* (opzionale): permette di indicare un elenco, separato da virgola, di file CRL.

La configurazione sopra indicata rappresenta la configurazione di default che verrà proposta durante la gestione di una erogazione o di una fruizione. È sempre possibile ridefinire per ogni singola API tale configurazione

Nota: TrustStore delle comunicazioni HTTPS

Nei profili di sicurezza per API REST, dove il riferimento al certificato utilizzato viaggia tramite il claim “x5u”, è possibile che GovWay debba effettuare il download del certificato tramite url https che espongono certificati server non validabili tramite le CA note. In tale contesto è possibile configurare un trustStore personalizzato agendo sulle

proprietà presenti nel file “/etc/govway/modipa_local.properties” in maniera simile al trustStore dei certificati. Tali proprietà possiedono il prefisso “org.openspcoop2.protocol.modipa.sicurezzaMessaggio.ssl.”.

KeyStore per la firma della Risposte

Nella figura Fig. 3.7 della sezione *Sicurezza Messaggio* è stato descritto come GovWay utilizzerà la chiave privata associata all’applicativo interno che ha scaturito la richiesta per firmare il token di sicurezza aggiunto al messaggio in uscita dal dominio di gestione. Per quanto concerne invece le risposte che GovWay processa in una erogazione, la chiave privata utilizzata per firmare il token di sicurezza aggiunto alla risposta viene preso da una configurazione di default descritta di seguito. È sempre possibile ridefinire per ogni singola API tale configurazione.

Per poter firmare i token di sicurezza delle risposte, deve essere configurato opportunamente GovWay per quanto riguarda le seguenti proprietà presenti nel file “/etc/govway/modipa_local.properties” tutte con prefisso “org.openspcoop2.protocol.modipa.sicurezzaMessaggio.certificati.”:

- *keyStore.path* (obbligatorio): indica il path su file system di un keyStore contenente la chiave privata.
- *keyStore.tipo* (obbligatorio): indica il tipo di trustStore (JKS)
- *keyStore.password* (obbligatorio): password per accedere al keyStore
- *key.alias* (obbligatorio): alias della chiave privata all’interno del keyStore.
- *key.password* (obbligatorio): password della chiave privata all’interno del keyStore.

3.3.2 [IDAS01 / IDAR01] Direct Trust con certificato X.509

Nota: La sigla che identifica il profilo di sicurezza messaggio varia a seconda se l’API sia di tipo REST, per cui la sigla corrisponde a *IDAR01*, o SOAP dove viene utilizzata la sigla *IDAS01*.

L’adozione di questo profilo consente, alla ricezione di un messaggio, di validare il certificato fornito dall’applicativo mittente, la porzione di messaggio firmata, la validità temporale nonché la corrispondenza del destinatario della comunicazione.

Nel processo di configurazione, per i servizi con questo profilo, la registrazione delle API prevede che nella sezione «ModIPA», elemento «Profilo Sicurezza Messaggio», venga selezionato il profilo «IDAR01» (o IDAS01 per SOAP) come indicato in Fig. 3.9.



Fig. 3.9: Profilo di sicurezza messaggio IDAR01 per l’API

Nel contesto della configurazione della specifica operation/risorsa è presente anche la sezione «Profilo Sicurezza Messaggio» che consente di intervenire sul profilo di sicurezza messaggio in modo puntuale. È quindi possibile lasciare l'impostazione del profilo al valore già stabilito a livello della API, oppure decidere di ridefinirlo andando a fornire una configurazione specifica per la singola operation/risorsa come indicato in Fig. 3.9.



Fig. 3.10: Profilo di sicurezza messaggio ridefinito per una risorsa dell'API

Il processo prosegue con alcune differenze in base al tipo di servizio che si vuole configurare.

Fruizione

Le richieste che provengono dagli applicativi interni del dominio e sono dirette verso altre amministrazioni verranno arricchite del token di sicurezza ModIPA previsto dall'operazione invocata, come indicato precedentemente nella sezione [\[IDAS01 / IDAR01\] Direct Trust con certificato X.509](#).

Per la configurazione delle fruizioni con i profili di sicurezza messaggio è necessario registrare ciascun applicativo interno coinvolto al fine principale di associargli una chiave privata e un certificato X509 che GovWay utilizza per firmare il token di sicurezza ModIPA prodotto. Gli applicativi vengono identificati da GovWay tramite una delle modalità di autenticazione descritte nella sezione [Autenticazione Trasporto](#) (Fig. 3.11).

La registrazione dell'applicativo avviene come già descritto nella sez. [Creazione di un applicativo](#). In questo contesto sarà necessario specificare il dominio «Interno» dell'applicativo e procedere all'inserimento dei dati nel form «ModI PA» (Fig. 3.12).

I dati da inserire sono:

- *Archivio*: il file che corrisponde al keystore contenente la chiave privata utilizzata per la firma dei messaggi
- *Tipo*: il formato del keystore (jks, pkcs12)
- *Password*: la password per l'accesso al keystore
- *Alias Chiave Privata*: l'alias con cui è riferita la chiave privata nel keystore
- *Password Chiave Privata*: la password della chiave privata
- *Reply Audience/WSA-To*: identificativo dell'applicativo, utilizzato come clientId in uscita, e verificato con il valore «Audience» eventualmente presente nelle risposte.

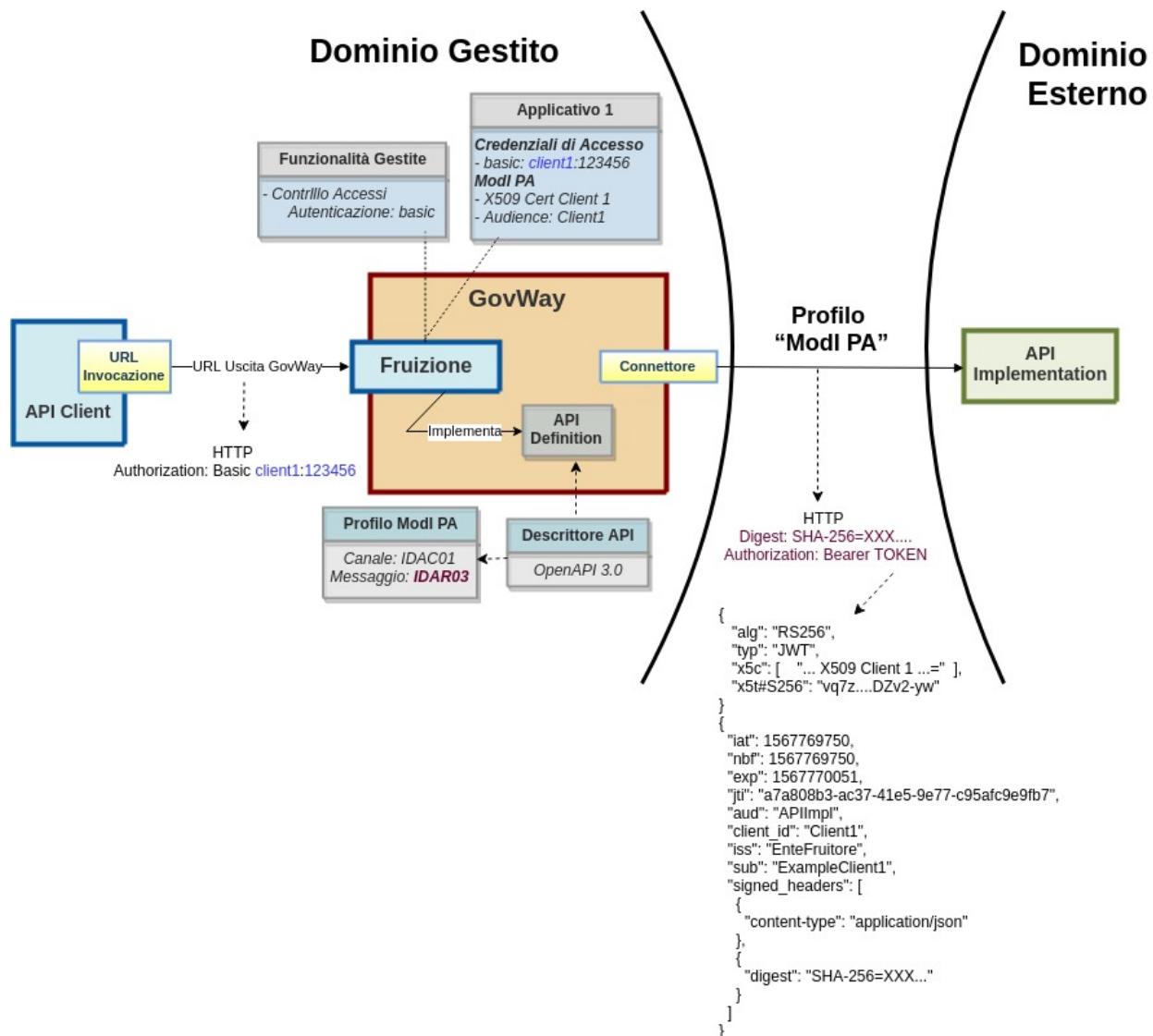


Fig. 3.11: Fruizione con Profilo di Interoperabilità “ModI PA”

Sicurezza Messaggio

Abilitato

Archivio * No file selected.

Tipo

Password *

Alias Chiave Privata *

Password Chiave Privata *

Reply Audience/WSA-To

Identificativo dell'applicativo scambiato nei token di sicurezza delle risposte

Fig. 3.12: Dati ModI PA relativi ad un applicativo interno

L’interfaccia per la creazione della fruizione, basata su una API con profilo IDAR01 (o IDAS01), presenta le sezioni «ModI PA - Richiesta» e «ModI PA - Risposta»:

- ModI PA - Richiesta (Fig. 3.13): la maschera relativa alla richiesta prevede la configurazione del meccanismo di firma digitale del messaggio, ad opera dell’applicativo mittente, e la produzione del relativo token di sicurezza:
 - Algoritmo: l’algoritmo che si vuole utilizzare per la firma digitale del messaggio
 - Riferimento X.509: il metodo da utilizzare per l’inserimento del certificato dell’applicativo nel token di sicurezza. I valori possibili sono (differenziati per il caso REST e SOAP) quelli previsti nelle Linee Guida di Interoperabilità:
 - Time to Live: tempo di validità del token prodotto (in secondi)
 - Audience: identificativo dell’applicativo destinatario da indicare come audience nel token di sicurezza; se non viene indicato alcun valore verrà utilizzato la url del connettore.
- ModI PA - Risposta (Fig. 3.14): la maschera relativa alla risposta prevede la configurazione del meccanismo di validazione del token ricevuto da parte dell’applicativo destinatario:
 - Riferimento X.509: il metodo per la localizzazione del certificato del destinatario nel messaggio di risposta. Si può mantenere la medesima impostazione prevista per il messaggio di richiesta o ridefinirla.
 - TrustStore Certificati: Riferimento al truststore che contiene le CA, i certificati e le CRL da utilizzare per poter verificare i token di sicurezza ricevuti nelle risposte. È possibile mantenere l’impostazione di default che è stata fornita al momento dell’installazione del prodotto, oppure definire un diverso riferimento (opzione «Ridefinito») fornendo Path, Tipo, Password del TrustStore e CRL.
 - Verifica Audience: Se abilitata questa opzione, viene effettuata la verifica che il campo Audience, presente nel token di sicurezza della risposta, corrisponda a quello indicato per l’applicativo mittente.

Erogazione

Nelle erogazioni, le richieste provengono da amministrazioni esterne al dominio e sono dirette ad applicativi interni. Prima di procedere con l’inoltro della richiesta verso il backend interno, GovWay valida il token di sicurezza ricevuto

Modi PA - Richiesta

Profilo Sicurezza Messaggio

Algoritmo: RS256

Riferimento X.509:
x5c (Certificate Chain)
x5t#256 (Certificate SHA-256 Thumbprint)
x5u (URL)

Time to Live (secondi) *: 300

Indica la validità temporale, in secondi, a partire dalla data di creazione del security token

Audience:

Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore



Fig. 3.13: Dati per la configurazione della sicurezza messaggio sulla richiesta di una fruizione

Modi PA - Risposta

Profilo Sicurezza Messaggio

Riferimento X.509: Utilizza impostazioni della Richiesta

TrustStore Certificati: Default

Verifica Audience:

Se abilitato viene verificato che il valore corrisponde a quello indicato nella configurazione dell'applicativo

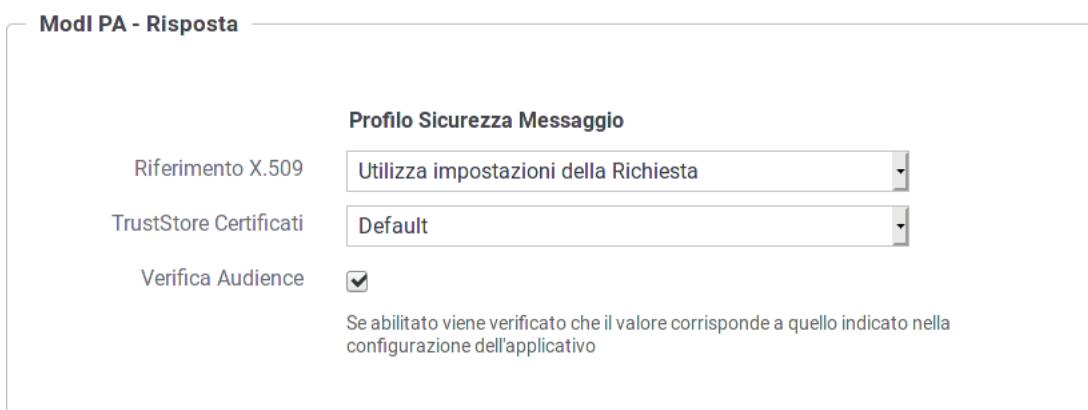


Fig. 3.14: Dati per la configurazione della sicurezza messaggio sulla risposta di una fruizione

rispetto al profilo associato all'operazione invocata (come descritto nella sezione [\[IDAS01 / IDAR01\] Direct Trust con certificato X.509](#)): verifica firma, validazione temporale, filtro duplicati, verifica integrità del messaggio ... (Fig. 3.15)

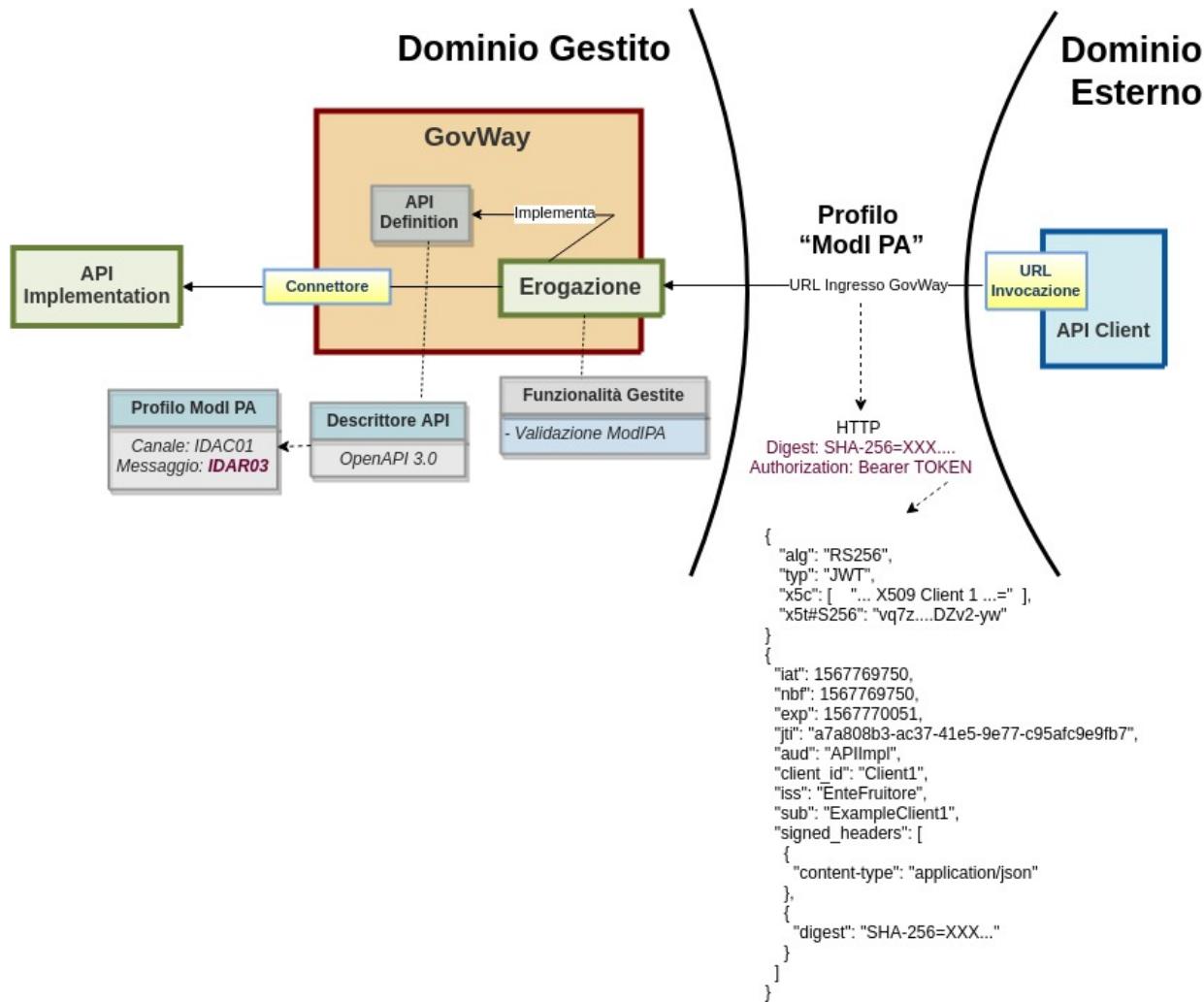


Fig. 3.15: Erogazione con Profilo di Interoperabilità ‘ModI PA’

Per la configurazione di erogazioni basate su una API con profilo IDAR01 (o IDAS01), nella relativa maschera della govwayConsole saranno presenti le sezioni «ModI PA - Richiesta» e «ModI PA - Risposta»:

- **ModI PA - Richiesta** (Fig. 3.16): la maschera relativa alla richiesta prevede la configurazione del meccanismo di validazione del token ricevuto sul messaggio di richiesta:
 - **Riferimento X.509:** il metodo per la localizzazione del certificato dell'applicativo mittente nel messaggio di richiesta. Il valore fornito deve corrispondere alla scelta operata dai mittenti. I valori possibili (differenziati per il caso REST e SOAP) sono quelli previsti nella specifica AGID.
 - **TrustStore Certificati:** Riferimento al truststore che contiene le CA, i certificati e le CRL da utilizzare per poter verificare i token di sicurezza ricevuti nelle richieste. È possibile mantenere l'impostazione di default che è stata fornita al momento dell'installazione del prodotto, oppure definire un diverso riferimento (opzione «Ridefinito») fornendo Path, Tipo, Password del TrustStore e CRL.
 - **Audience:** valore del campo Audience atteso nel token di sicurezza della richiesta.

Modi PA - Richiesta

Profilo Sicurezza Messaggio	
Riferimento X.509	x5c (Certificate Chain) x5t#256 (Certificate SHA-256 Thumbprint) x5u (URL)
TrustStore Certificati	Default
Audience	
Se non viene fornito un valore, il valore atteso all'interno del security token corrisponderà all'url di invocazione	

Fig. 3.16: Dati per la configurazione della sicurezza messaggio sulla richiesta di una erogazione

- Modi PA - Risposta (Fig. 3.17): la maschera prevede la configurazione del meccanismo di firma digitale del messaggio di risposta, e la produzione del relativo token di sicurezza, da inviare all'applicativo mittente:
 - Algoritmo: l'algoritmo che si vuole utilizzare per la firma digitale del messaggio di risposta
 - Riferimento X.509: il metodo da utilizzare per l'inserimento del certificato nel messaggio di risposta. Si può mantenere la medesima impostazione prevista per il messaggio di richiesta o ridefinirla.
 - Keystore: il keystore da utilizzare per la firma del messaggio di risposta. È possibile mantenere il riferimento al keystore di default, fornito in fase di installazione del prodotto, oppure indicare un diverso riferimento (opzione «Ridefinito») fornendo il path sul filesystem, o in alternativa direttamente l'archivio, unitamente a Tipo, Password, Alias Chiave Privata e Password Chiave Privata.
 - Time to Live (secondi): validità temporale del token prodotto.

Modi PA - Risposta

Profilo Sicurezza Messaggio	
Algoritmo	RS256
Riferimento X.509	Utilizza impostazioni della Richiesta
KeyStore	Default
Time to Live (secondi) *	300
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token della risposta	

Fig. 3.17: Dati per la configurazione della sicurezza messaggio sulla risposta di una erogazione

Nel contesto dei profili di sicurezza messaggio è possibile registrare anche gli applicativi dei domini esterni al fine di:

1. identificare puntualmente le componenti esterne coinvolte nella comunicazione abilitando le funzionalità di tracciamento e statistica per tali elementi.

2. abilitare le funzionalità di autorizzazione sugli applicativi identificando puntualmente chi autorizzare dopo il superamento del processo di autenticazione/autorizzazione canale e validazione del token di sicurezza (Fig. 3.18).

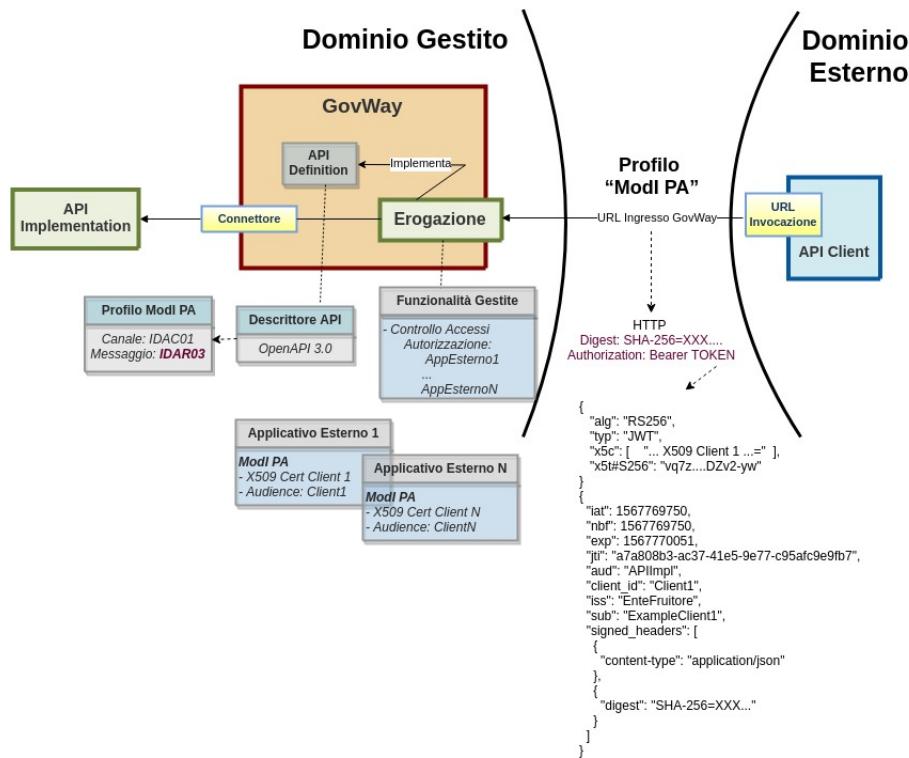


Fig. 3.18: Erogazione con Profilo di Interoperabilità “ModI PA” e criteri di autorizzazione puntuali

Per abilitare quanto al punto 1 è sufficiente la sola registrazione degli applicativi esterni coinvolti (Fig. 3.19).

Il form 'Applicativo' permette di registrare un'applicazione esterna. I campi sono:

- Dominio:** Esterno (selezionato)
- Soggetto:** (campo a dropdown vuoto)
- Nome ***: (campo input vuoto)

Fig. 3.19: Registrazione di un applicativo esterno

Dopo aver indicato il dominio «Esterno» per l'applicativo, sarà necessario selezionare il soggetto che identifica il dominio esterno di riferimento.

La registrazione dell'applicativo esterno comprende anche la sezione con i dati relativi alla sicurezza messaggio (Fig. 3.20).

I dati da fornire sono:

- **Modalità:** si seleziona tra il caricamento del certificato e la configurazione manuale

Sicurezza Messaggio

Modalità: Upload Archivio

Formato: CER

Certificato *: Browse... No file selected.

Reply Audience/WSA-To

Identificativo dell'applicativo scambiato nei token di sicurezza delle risposte

Fig. 3.20: Dati ModI PA relativi ad un applicativo esterno con upload del certificato

- Caso *Upload Archivio*:
 - *Formato*: formato dell’archivio fornito (CER, JKS; PKCS12)
 - *Certificato*: elemento per l’upload dell’archivio che contiene il certificato
 - *Reply Audience/WSA-To*: identificativo dell’applicativo da confrontare con il valore «Audience» eventualmente presente nelle richieste.
- Caso *Configurazione Manuale* (Fig. 3.21):
 - *Self Signed*: opzione per indicare se il certificato è self-signed oppure rilasciato da una CA
 - *Subject*: il subject del certificato
 - *Issuer*: l’issuer del certificato, nel caso in cui non sia self-signed
 - *Reply Audience/WSA-To*: identificativo dell’applicativo da confrontare con il valore «Audience» eventualmente presente nelle richieste.

Per abilitare le funzionalità di autorizzazione dei singoli applicativi (punto 2 del precedente elenco) si deve procedere alla configurazione della sezione «Controllo Accessi» relativa all’erogazione. Quando attiva la sicurezza messaggio, questa sezione conterrà il form «Autorizzazione ModI PA» (Fig. 3.22). Qui è possibile specificare un elenco di applicativi (esterni) autorizzati, ad accedere all’erogazione, tra quelli identificati nella fase di verifica del relativo certificato. Gli applicativi esterni saranno selezionabili tra quelli censiti nella sezione «Applicativi» (Fig. 3.22).

Nota: L’autorizzazione basata sugli identificativi degli applicativi mittenti del dominio fruitore esterno, è possibile soltanto se è stata effettuata la registrazione degli applicativi interessati, in associazione al soggetto esterno di riferimento.

3.3.3 [IDAS02 / IDAR02] Direct Trust con certificato X.509 con unicità del token/messaggio

Modi PA

Sicurezza Messaggio

Modalità

Self Signed

Subject *

Issuer

Reply Audience/WSA-To

Identificativo dell'Applicativo scambiato nei token di sicurezza delle risposte

This screenshot shows the 'Modi PA' configuration page. It includes fields for 'Sicurezza Messaggio' (Security Message) such as 'Modalità' (Manual Configuration), 'Self Signed' (Self-Signed), 'Subject' (Subject), 'Issuer' (Issuer), and 'Reply Audience/WSA-To' (Reply Audience/WSA-To). A note at the bottom indicates it's for identifying the application exchanged in response tokens.

Fig. 3.21: Dati ModI PA relativi ad un applicativo esterno con configurazione manuale dei dati di sicurezza

Autorizzazione ModI PA

Sicurezza Messaggio

[Applicativi \(2\)](#)

This screenshot shows the 'Autorizzazione ModI PA' (Authorization ModI PA) page. It displays the 'Sicurezza Messaggio' (Security Message) section and a link to 'Applicativi (2)' (Applications (2)).

Fig. 3.22: Autorizzazione di singoli applicativi per l'accesso all'erogazione

Nota: La sigla che identifica il profilo di sicurezza messaggio varia a seconda se l'API sia di tipo REST, per cui la sigla corrisponde a *IDAR02*, o SOAP dove viene utilizzata la sigla *IDAS02*.

Questo profilo di sicurezza presenta le medesime caratteristiche di *[IDAS01 / IDAR01] Direct Trust con certificato X.509*, con l'unica differenza di prevedere un meccanismo di filtro che impedisce la ricezione di messaggi duplicati da parte di ciascun ricevente.

L'attivazione di questo profilo avviene a livello della relativa API, nella sezione «ModIPA», elemento «Profilo Sicurezza Messaggio», selezionando il profilo «IDAR02» (o IDAS02 per SOAP) come indicato in Fig. 3.23.



Fig. 3.23: Profilo di sicurezza messaggio IDAR02 per l'API

Per le configurazioni successive procedere come già descritto in precedenza per il profilo *[IDAS01 / IDAR01] Direct Trust con certificato X.509*.

3.3.4 [IDAS03 / IDAR03] Integrità della payload del messaggio

Nota: La sigla che identifica il profilo di sicurezza messaggio varia a seconda se l'API sia di tipo REST, per cui la sigla corrisponde a *IDAR03*, o SOAP dove viene utilizzata la sigla *IDAS03*.

Questo profilo di sicurezza consente di estendere IDAR01 e IDAR02 aggiungendo un meccanismo che garantisce l'integrità del messaggio scambiato grazie all'invio, nel token di sicurezza, della firma digitale del payload.

L'attivazione di questo profilo avviene a livello della relativa API, nella sezione «ModIPA», elemento «Profilo Sicurezza Messaggio», selezionando il profilo «IDAR03 (IDAR01)» nel caso si voglia estendere IDAR01, oppure il profilo «IDAR03 (IDAR02)» nel caso si voglia estendere IDAR02 con il meccanismo di garanzia dell'integrità del payload (Fig. 3.24).

Per le configurazioni successive procedere come già descritto in precedenza per il profilo *[IDAS01 / IDAR01] Direct Trust con certificato X.509*.

Occorre solo tenere presente che per questo profilo di sicurezza sono presenti le seguenti differenze sulle maschere di configurazione delle API di tipo REST:

- Nel contesto della configurazione di una fruizione, relativamente alla sezione «ModI PA - Richiesta», oltre ai dati da fornire per la produzione della firma digitale deve essere aggiunta anche l'indicazione degli eventuali Header HTTP da firmare. Tale indicazione viene fornita con il campo «HTTP Headers da firmare» (Fig. 3.25).

Modi PA

Profilo Sicurezza Canale

Profilo ▾

Profilo Sicurezza Messaggio

Profilo ▾

Fig. 3.24: Profilo di sicurezza messaggio IDAR03 per l'API

Modi PA - Richiesta

Profilo Sicurezza Messaggio

Algoritmo ▾

HTTP Headers da firmare *

Riferimento X.509

Time to Live (secondi) * ▾
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token

Audience

Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore

Fig. 3.25: Fruizione IDAR03 - Configurazione richiesta con indicazione HTTP Headers da firmare

- Nel contesto della configurazione di una erogazione, relativamente alla sezione «ModI PA - Risposta», oltre ai dati da fornire per la produzione della firma digitale deve essere aggiunta anche l'indicazione degli eventuali Header HTTP da firmare. Tale indicazione viene fornita con il campo «HTTP Headers da firmare» (Fig. 3.26).

ModI PA - Risposta

Profilo Sicurezza Messaggio

Algoritmo: RS256

HTTP Headers da firmare *

Digest x Content-Type x Content-Encoding x

Riferimento X.509: Utilizza impostazioni della Richiesta

KeyStore: Default

Time to Live (secondi) *: 300

Indica la validità temporale, in secondi, a partire dalla data di creazione del security token della risposta

Fig. 3.26: Erogazione IDAR03 - Configurazione risposta con indicazione HTTP Headers da firmare

3.3.5 Funzionalità Avanzate

I Token di sicurezza, dopo essere stati validati da GovWay, vengono eliminati dai messaggi in modo da rendere trasparente agli applicativi la gestione della sicurezza che è stata effettuata sul Gateway.

È possibile, se necessario, configurare GovWay al fine di non fargli eliminare il token di sicurezza dai messaggi dopo averli validati. Per farlo si deve utilizzare la govwayConsole in modalità avanzata (vedi sezione [Modalità Avanzata](#)).

Per quanto concerne le richieste inoltrate ad un backend, durante la gestione di una erogazione, è possibile disabilitare l'eliminazione del token di sicurezza intervenendo sul connettore dell'erogazione e disabilitando la voce “Sbustamento ModI PA” all'interno della sezione “Trattamento Messaggio” come mostrato nella figura Fig. 3.27.

Sulle risposte ritornate all'applicativo mittente, durante la gestione di una fruizione, è possibile disabilitare l'eliminazione del token di sicurezza intervenendo sull'applicativo e disabilitando la voce “Sbustamento ModI PA” all'interno della sezione “Trattamento Messaggio” come mostrato nella figura Fig. 3.28.

3.4 Profili di Interazione

Le specifiche del Modello di Interoperabilità definiscono i Profili di Interazione come le modalità secondo le quali un erogatore e un fruitore possono interagire. La distinzione operata a livello della specifica è quella tra il profilo «Bloccante» e quello «Non Bloccante». Per le differenze di dettaglio tra i due profili si rimanda al testo della specifica.

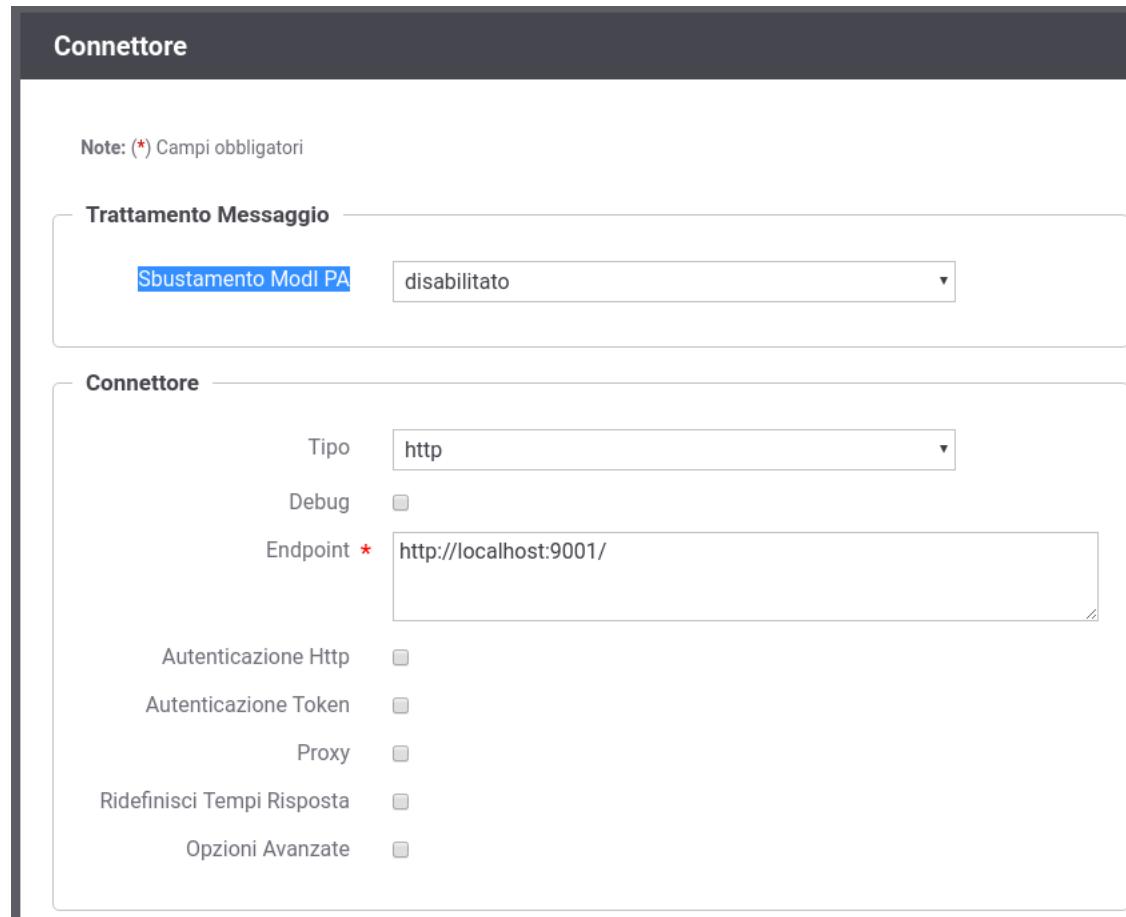


Fig. 3.27: Funzionalità “Sbustamento ModI PA” disabilitata per la Richiesta

Applicativi > ExampleClient1

ExampleClient1

Note: (*) Campi obbligatori

Applicativo

Dominio	Interno
Soggetto	EnteFruitore
Nome	ExampleClient1

Modalità di Accesso

Tipo	http-basic
Utente *	ExampleClient1
Password *	123456

Ruoli

[visualizza\(0\)](#)

Trattamento Messaggio

Sbustamento Modi PA	disabilitato
---------------------	--------------

Modi PA

Sicurezza Messaggio

Abilitato	<input checked="" type="checkbox"/>
-----------	-------------------------------------

Fig. 3.28: Funzionalità “Sbustamento Modi PA” disabilitata per la Risposta

Il profilo di interazione viene definito nell’interfaccia del servizio e conseguentemente GovWay recepisce tale informazioni nell’ambito della configurazione di una API nel contesto del profilo ModI PA.

La configurazione di API con il profilo ModI PA produce per default servizi con profilo di interazione «Bloccante». Se si desidera, è possibile modificare questa impostazione intervenendo puntualmente sulle singole operation/risorse della API.

La maschera di editing della singola operation/risorsa possiede la sezione ModI PA per consentire di specificare le seguenti informazioni (Fig. 3.29):

- *Profilo di Interazione*: specifica il profilo di interazione che si vuole associare alla specifica operation/risorsa
 - *Profilo*: indica il nome del profilo di interazione, a scelta tra Bloccante e Non Bloccante
 - *Interazione*: (solo per il profilo non bloccante) indica se l’interazione prevista è di tipo PUSH (iniziativa del mittente) o PULL (iniziativa del destinatario)
 - *Funzione*: (solo per il profilo non bloccante) indica se l’operation/risorsa ha la funzione di inviare una richiesta, chiedere lo stato di avanzamento dell’elaborazione della risposta o inviare una risposta.
 - *Richiesta Correlata*: (solo per la funzione Richiesta Stato e Risposta) indica l’operation/risorsa correlata che corrisponde all’invio della richiesta.

ModI PA	
Profilo Interazione	
Profilo	Non Bloccante
Interazione	PULL
Funzione	Richiesta
Profilo Sicurezza Messaggio	
Profilo	Usa profilo API

Fig. 3.29: Profili di interazione ModI PA per operation/risorse dell’API

Nelle sezioni seguenti vengono forniti maggiori dettagli su come siano gestiti i profili non bloccanti.

3.4.1 Profilo di Interazione PUSH per API SOAP

Il profilo di interazione, denominato PUSH, è utilizzabile nel caso in cui il fruitore abbia a sua volta la possibilità di esporre una interfaccia di servizio per la ricezione delle risposte (Fig. 3.30).

Come riportato dalle Linee Guida di Interoperabilità ModI PA:

- Al passo (1), il fruitore DEVE indicare l’endpoint della callback utilizzando l’header SOAP custom “X-ReplyTo”;
- Al passo (2), l’erogatore DEVE fornire insieme all’acknowledgement della richiesta nel body, il correlation ID utilizzando l’header SOAP custom X-Correlation-ID;

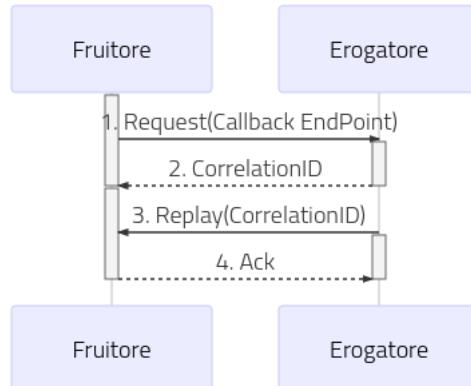


Fig. 3.30: Flusso previsto in un Profilo di Interazione PUSH

- Al passo (3), l'erogatore DEVE riutilizzare lo stesso correlation ID fornito al passo (2) sempre utilizzando l'header SOAP custom X-Correlation-ID;
- Al passo (4), il fruitore DEVE riconoscere tramite un messaggio di acknowledgement il ricevimento della risposta.

Configurazione delle API

Per attuare la configurazione su GovWay si deve procedere con la registrazione delle due API che definiscono il servizio di ricezione della richiesta e il servizio di Callback dove l'erogatore deve inoltrare la risposta.

- Richiesta

Effettuata la registrazione delle API, accedere al dettaglio dell'azione relativa al servizio di richiesta ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PUSH” con ruolo “Richiesta” come mostrato nella figura Fig. 3.31:

- Risposta

Successivamente, accedere al dettaglio dell'azione relativa al servizio di callback ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PUSH” con ruolo “Risposta”. Definire anche la correlazione verso il servizio e l'azione relativa alla richiesta come mostrato nella figura Fig. 3.32:

Configurazione dell'Erogazione

Sul dominio dell'erogatore deve essere definita sia un'erogazione dell'API relativa al servizio di richiesta che una fruizione del servizio di callback.

- Erogazione del Servizio di Richiesta

Le richieste ricevute sull'erogazione vengono validate da GovWay verificando la presenza dell'header SOAP custom “X-ReplyTo” come previsto dal profilo “ModI PA”. Effettuata la validazione del messaggio di richiesta, eventualmente gestendo anche gli aspetti di sicurezza descritti nella sezione *Sicurezza Messaggio*, GovWay inoltra il messaggio al backend e rimane in attesa dell'acknowledgement.

Ricevuto il messaggio di acknowledgement GovWay verifica la presenza dell'header SOAP custom “X-Correlation-ID”. Se tale header non risulta presente viene generato da GovWay impostando come valore l'identificativo della transazione, che è stato inoltrato con la richiesta al backend tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Transaction-ID”).

The screenshot shows the configuration of an MRequest (SOAP Blocking PUSH Request) in the GovWay Management Console. The interface is divided into sections:

- Azione**: Nome is set to MRequest.
- Informazioni Protocollo**: Profilo is set to "usa profilo servizio".
- Modi PA**:
 - Profilo Interazione**: Profilo is set to "Non Bloccante".
 - Interazione**: Profilo is set to "PUSH".
 - Funzione**: Profilo is set to "Richiesta".
 - Profilo Sicurezza Messaggio**: Profilo is set to "Usa profilo API".

Fig. 3.31: Configurazione della richiesta dell'API SOAP (PUSH)

Nota: Header “X-Correlation-ID” generato da GovWay

La generazione dell’header soap “X-Correlation-ID”, se non presente, è disabilitabile intervenendo sulla proprietà «org.openscoop2.protocol.modipa.soap.push.request.correlationId.header.useTransactionIdIfNotExists» presente nel file “/etc/govway/modipa_local.properties” (si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione). Se si disabilita la proprietà, GovWay termina con errore la transazione se rileva l’assenza dell’header soap “X-Correlation-ID” nel messaggio di acknowledgement ricevuto dal backend.

- Fruizione del Servizio di Callback per la Risposta

Le risposte devono essere inoltrate dall’applicativo mittente utilizzando la fruizione del servizio di Callback configurata su GovWay. Le risposte vengono validate da GovWay verificando la presenza dell’header SOAP custom “X-Correlation-ID”. GovWay permette di fornire l’informazione sull’identificativo di correlazione anche tramite modalità alternative all’header soap (header http, parametri della url...) per poi generare un header soap “X-Correlation-ID” come previsto dalla specifica “ModI PA” valorizzato con il valore fornito. Le modalità alternative sono le seguenti:

- Header HTTP “X-Correlation-ID”
- Header HTTP “GovWay-Conversation-ID” o parametro della url “govway_conversation_id” previsto per la correlazione tramite identificativo di collaborazione descritta nella sezione *Correlazione tra transazioni differenti*. Questa modalità richiede che sia abilitata l’indicazione dell’identificativo di collaborazione nell’API o sulla singola azione come mostrato nella seguente Fig. 3.33:
- Header HTTP “GovWay-Relates-To” o parametro della url “govway_relates_to” previsto per la correlazione tramite riferimento della richiesta descritta nella sezione *Correlazione tra transazioni differenti*. Questa modalità

API > SOAPBlockingPUSHResponse v1 > Servizi > Azioni di SOAPCallbackClient > **MRequestResponse**

MRequestResponse

Azione

Nome MRequestResponse

Informazioni Protocollo

Profilo usa profilo servizio

Modi PA

Profilo Interazione

Profilo Non Bloccante

Interazione PUSH

Funzione Risposta

API Richiesta Correlata SOAPBlockingPUSHRequest v1

Servizio SOAPCallback

Azione MRequest

Profilo Sicurezza Messaggio

Profilo Usa profilo API

Fig. 3.32: Configurazione della risposta dell'API SOAP (PUSH)

API > SOAPBlockingPUSHRequest v1 > Servizi > Azioni di SOAPCallback > **MRequest**

MRequest

Azione

Nome MRequest

Informazioni Protocollo

Profilo ridefinisci

Profilo di collaborazione sincrono

ID Collaborazione

Riferimento ID Richiesta

Fig. 3.33: Abilitazione funzionalità di correlazione govway tramite identificativo di collaborazione

richiede che sia abilitata l'indicazione dell'identificativo di riferimento alla richiesta nell'API o sulla singola azione come mostrato nella figura Fig. 3.34:

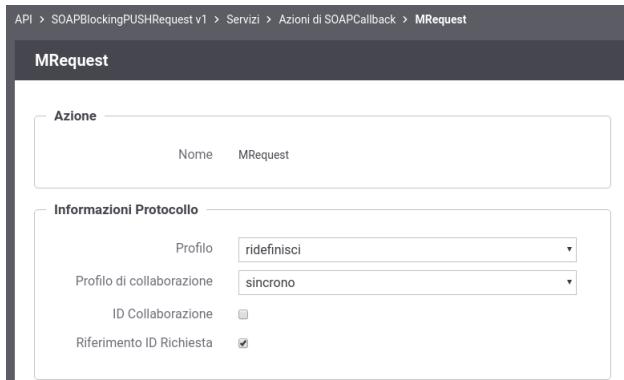


Fig. 3.34: Abilitazione funzionalità di correlazione govway tramite identificativo della richiesta

Configurazione della Fruizione

Sul dominio del fruitore deve essere definita sia una fruizione dell'API relativa al servizio di richiesta che un'erogazione del servizio di callback.

- Fruizione del Servizio di Richiesta

Le richieste devono essere inoltrate dall'applicativo mittente utilizzando la fruizione del servizio di richiesta configurata su GovWay. Su ogni richiesta GovWay crea, o ne modifica il valore se già presente, dell'header soap “X-ReplyTo” previsto dal profilo “ModI PA”. L'header viene valorizzato con l'url di invocazione utilizzabile dalla controparte per invocare il servizio di callback configurato su GovWay.

Nota: Header “X-ReplyTo” generato da GovWay

La valorizzazione dell'header soap “X-ReplyTo” da parte di GovWay è disabilitabile intervenendo sulla proprietà «org.openspcoop2.protocol.modipa.soap.push.replyTo.header.updateOrCreate» presente nel file “/etc/govway/modipa_local.properties” (si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione). Se si disabilita la proprietà, GovWay termina con errore la transazione se rileva l'assenza dell'header soap “X-ReplyTo” nel messaggio di richiesta ricevuto dal backend.

Il messaggio di acknowledgement ricevuto viene anch'esso validato al fine di verificare la presenza dell'header soap “X-Correlation-ID” come previsto dalla specifica “ModI PA”. L'informazione sull'id di correlazione è ottenibile dall'applicativo mittente sulla risposta, oltre che tramite l'header soap “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione [Scambio di informazioni nella richiesta inoltrata dal gateway al server](#) e [Altri header di Integrazione](#) (per default tramite l'header http “GovWay-Conversation-ID”).

- Erogazione del Servizio di Callback per la Risposta

Le risposte ricevute sull'erogazione del servizio di Callback vengono validate da GovWay verificando la presenza dell'header SOAP custom “X-Correlation-ID” come previsto dal profilo “ModI PA”. Effettuata la validazione del messaggio di risposta, eventualmente gestendo anche gli aspetti di sicurezza descritti nella sezione [Sicurezza Messaggio](#), GovWay inoltra il messaggio al backend e rimane in attesa dell'acknowledgement. L'informazione sull'id di correlazione è inoltrato al backend, oltre che tramite l'header soap “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione [Scambio di informazioni nella richiesta inoltrata dal gateway al server](#) e [Altri header di Integrazione](#) (per default tramite l'header http “GovWay-Conversation-ID”).

3.4.2 Profilo di Interazione PUSH per API REST

Il profilo di interazione, denominato PUSH, è utilizzabile nel caso in cui il fruitore abbia a sua volta la possibilità di esporre una interfaccia di servizio per la ricezione delle risposte (Fig. 3.35).

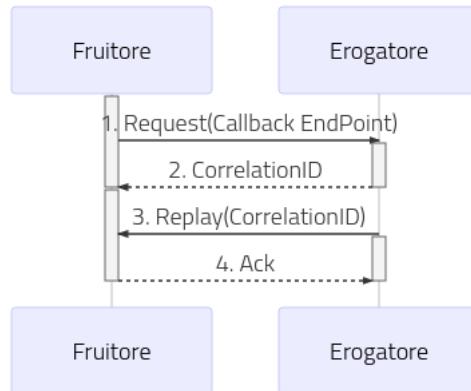


Fig. 3.35: Flusso previsto in un Profilo di Interazione PUSH

Come riportato dalle Linee Guida di Interoperabilità ModI PA:

- Al passo (1), il fruitore DEVE indicare l'endpoint della callback utilizzando l'header HTTP custom X-ReplyTo ed usando HTTP method POST;
- Al passo (2), l'erogatore DEVE fornire insieme all'acknowledgement della richiesta nel body, il correlation ID utilizzando l'header HTTP custom X-Correlation-ID; Il codice HTTP di stato DEVE essere HTTP status 202 Accepted a meno che non si verifichino errori;
- Al passo (3), l'erogatore DEVE riutilizzare lo stesso correlation ID fornito al passo (2) sempre utilizzando l'header HTTP custom X-Correlation-ID; Il verbo HTTP utilizzato deve essere POST;
- Al passo (4), il fruitore DEVE riconoscere tramite un messaggio di acknowledgement il ricevimento della risposta; Il codice HTTP di stato DEVE essere HTTP status 200 OK a meno che non si verifichino errori.

Configurazione delle API

Per attuare la configurazione su GovWay si deve procedere con la registrazione delle due API che definiscono il servizio di ricezione della richiesta e il servizio di Callback dove l'erogatore deve inoltrare la risposta.

- Richiesta

Effettuata la registrazione delle API, accedere al dettaglio della risorsa relativa al servizio di richiesta ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PUSH” con ruolo “Richiesta” come mostrato nella figura Fig. 3.36:

- Risposta

Successivamente, accedere al dettaglio della risorsa relativa al servizio di callback ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PUSH” con ruolo “Risposta”. Definire anche la correlazione verso l'API e l'azione relativa alla richiesta come mostrato nella figura Fig. 3.37:

Configurazione dell'Erogazione

API > RESTBlockingPUSHRequest v1 > Risorse > **POST /resources/{id_resource}/M**

POST /resources/{id_resource}/M

Note: (*) Campi obbligatori

Risorsa

HTTP Method	POST
Path *	/resources/{id_resource}/M
Nome	POST_resources.id_resource.M
Se non definito verrà automaticamente generato un identificativo univoco	
Descrizione	

Informazioni Protocollo

ID Collaborazione	
Riferimento ID Richiesta	

Modi PA

Profilo Interazione	
Profilo	Non Bloccante
Interazione	PUSH
Funzione	Richiesta
Profilo Sicurezza Messaggio	
Profilo	Usa profilo API

Fig. 3.36: Configurazione della richiesta dell'API REST (PUSH)

API > RESTBlockingPUSHResponse v1 > Risorse > **POST /MResponse**

POST /MResponse

Note: (*) Campi obbligatori

Risorsa

HTTP Method	POST
Path *	/MResponse
Nome	POST_MResponse
Se non definito verrà automaticamente generato un identificativo univoco	
Descrizione	

Informazioni Protocollo

ID Collaborazione	
Riferimento ID Richiesta	

Modi PA

Profilo Interazione

Profilo	Non Bloccante
Interazione	PUSH
Funzione	Risposta
API Richiesta Correlata	RESTBlockingPUSHRequest v1
Risorsa	POST /resources/{id_resource}/M

Profilo Sicurezza Messaggio

Profilo	Usa profilo API
---------	-----------------

Fig. 3.37: Configurazione della risposta dell'API REST (PUSH)

Sul dominio dell'erogatore deve essere definita sia un'erogazione dell'API relativa al servizio di richiesta che una fruizione del servizio di callback.

- Erogazione del Servizio di Richiesta

Le richieste ricevute sull'erogazione vengono validate da GovWay verificando la presenza dell'header HTTP custom “X-ReplyTo” come previsto dal profilo “ModI PA”. Effettuata la validazione del messaggio di richiesta, eventualmente gestendo anche gli aspetti di sicurezza descritti nella sezione *Sicurezza Messaggio*, GovWay inoltra il messaggio al backend e rimane in attesa dell'acknowledgement.

Ricevuto il messaggio di acknowledgement GovWay verifica che il codice HTTP di stato sia 202 e verifica la presenza dell'header HTTP custom “X-Correlation-ID”. Se tale header non risulta presente viene generato da GovWay impostando come valore l'identificativo della transazione, che è stato inoltrato con la richiesta al backend tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Transaction-ID”).

Nota: Header “X-Correlation-ID” generato da GovWay

La generazione dell'header HTTP “X-Correlation-ID”, se non presente, è disabilitabile intervenendo sulla proprietà «org.openscoop2.protocol.modipa.rest.push.request.correlationId.header.useTransactionIdIfNotExist» presente nel file “/etc/govway/modipa_local.properties” (si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione). Se si disabilita la proprietà, GovWay termina con errore la transazione se rileva l'assenza dell'header HTTP “X-Correlation-ID” nel messaggio di acknowledgement ricevuto dal backend.

- Fruizione del Servizio di Callback per la Risposta

Le risposte devono essere inoltrate dall'applicativo mittente utilizzando la fruizione del servizio di Callback configurata su GovWay. Le risposte vengono validate da GovWay verificando la presenza dell'header HTTP custom “X-Correlation-ID”. GovWay permette di fornire l'informazione sull'identificativo di correlazione anche tramite modalità alternative all'header HTTP custom per poi generarla come previsto dalla specifica “ModI PA” valorizzato con il valore fornito. Le modalità alternative sono le seguenti:

- Header HTTP “GovWay-Conversation-ID” o parametro della url “govway_conversation_id” previsto per la correlazione tramite identificativo di collaborazione descritta nella sezione *Correlazione tra transazioni differenti*. Questa modalità richiede che sia abilitata l'indicazione dell'identificativo di collaborazione nell'API o sulla singola azione come mostrato nella figura Fig. 3.38:

Fig. 3.38: Abilitazione funzionalità di correlazione govway tramite identificativo di collaborazione

- Header HTTP “GovWay-Relates-To” o parametro della url “govway_relates_to” previsto per la correlazione tramite riferimento della richiesta descritta nella sezione *Correlazione tra transazioni differenti*. Questa modalità richiede che sia abilitata l’indicazione dell’identificativo di riferimento alla richiesta nell’API o sulla singola azione come mostrato nella figura Fig. 3.39:

The screenshot shows a configuration interface for a resource. At the top, it says "API > RESTBlockingPUSHRequest v1 > Risorse > POST /resources/{id_resource}/M". Below this, a title bar says "POST /resources/{id_resource}/M". A note says "Note: (*) Campi obbligatori". The main area is divided into sections: "Risorsa" and "Informazioni Protocollo". In the "Risorsa" section, there are fields for "HTTP Method" (set to "POST"), "Path" (set to "/resources/{id_resource}/M"), and "Nome" (set to "POST_resources.id_resource.M"). A note below says "Se non definito verrà automaticamente generato un identificativo univoco". In the "Informazioni Protocollo" section, there are two checkboxes: "ID Collaborazione" (unchecked) and "Riferimento ID Richiesta" (checked).

Fig. 3.39: Abilitazione funzionalità di correlazione govway tramite identificativo della richiesta

Configurazione della Fruizione

Sul dominio del fruitore deve essere definita sia una fruizione dell’API relativa al servizio di richiesta che un’erogazione del servizio di callback.

- Fruizione del Servizio di Richiesta

Le richieste devono essere inoltrate dall’applicativo mittente utilizzando la fruizione del servizio di richiesta configurata su GovWay. Su ogni richiesta GovWay crea, o ne modifica il valore se già presente, dell’header HTTP “X-ReplyTo” previsto dal profilo “ModI PA”. L’header viene valorizzato con l’url di invocazione utilizzabile dalla controparte per invocare il servizio di callback configurato su GovWay.

Nota: Header “X-ReplyTo” generato da GovWay

La valorizzazione dell’header HTTP “X-ReplyTo” da parte di GovWay è disabilitabile intervenendo sulla proprietà «org.openspcoop2.protocol.modipa.rest.push.replyTo.header.updateOrCreate» presente nel file “/etc/govway/modipa_local.properties” (si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione). Se si disabilita la proprietà, GovWay termina con errore la transazione se rileva l’assenza dell’header HTTP “X-ReplyTo” nel messaggio di richiesta ricevuto dal backend.

Il messaggio di acknowledgement ricevuto viene anch’esso validato al fine di verificare la presenza dell’header HTTP “X-Correlation-ID” come previsto dalla specifica “ModI PA”. L’informazione sull’id di correlazione è ottenibile dall’applicativo mittente sulla risposta, oltre che tramite l’header HTTP “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l’header http “GovWay-Conversation-ID”).

- Erogazione del Servizio di Callback per la Risposta

Le risposte ricevute sull'erogazione del servizio di Callback vengono validate da GovWay verificando la presenza dell'header HTTP custom “X-Correlation-ID” come previsto dal profilo “ModI PA”. Effettuata la validazione del messaggio di risposta, eventualmente gestendo anche gli aspetti di sicurezza descritti nella sezione *Sicurezza Messaggio*, GovWay inoltra il messaggio al backend e rimane in attesa dell'acknowledgement. L'informazione sull'id di correlazione è inoltrato al backend, oltre che tramite l'header HTTP “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Conversation-ID”).

3.4.3 Profilo di Interazione PULL per API SOAP

Il profilo di interazione, denominato PULL, prevede che il fruitore non fornisca un indirizzo di callback, mentre l'erogatore fornisce un indirizzo interrogabile per verificare lo stato di processamento di una richiesta e, al fine dell'elaborazione della stessa, il risultato (Fig. 3.40).

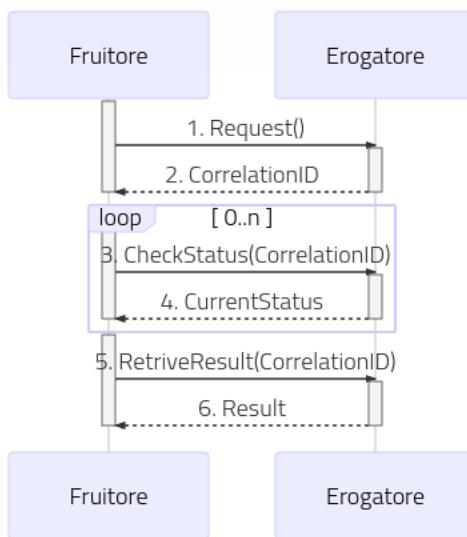


Fig. 3.40: Flusso previsto in un Profilo di Interazione PULL per API SOAP

Come riportato dalle Linee Guida di Interoperabilità ModI PA:

- L'interfaccia di servizio dell'erogatore fornisce tre metodi differenti al fine di inoltrare una richiesta, controllarne lo stato ed ottenerne il risultato
- Al passo (1), il fruitore effettua una richiesta;
- Al passo (2), l'erogatore DEVE fornire insieme all'acknowledgement della richiesta nel body, un correlation ID riportato nel header custom SOAP X-Correlation-ID;
- Al passo (3), il fruitore DEVE utilizzare i 1 correlation ID ottenuto al passo (2) per richiedere lo stato di processamento di una specifica richiesta;
- Al passo (4) l'erogatore, quando il processamento non si è ancora concluso fornisce informazioni circa lo stato della lavorazione della richiesta, quando invece il processamento si è concluso risponde indicando in maniera esplicita il completamento;
- Al passo (5), il fruitore utilizza il correlation ID di cui al passo (2) al fine di richiedere il risultato della richiesta;
- Al passo (6), l'erogatore fornisce il risultato del processamento.

Configurazione delle API

Per attuare la configurazione su GovWay si deve procedere con la registrazione dell'API che deve contenere i tre metodi differenti descritti precedentemente.

- Richiesta

Effettuata la registrazione delle API, accedere al dettaglio dell'azione corrispondente alla richiesta ed impostare nella sezione "Modi PA" un profilo di interazione non bloccante "PULL" con ruolo "Richiesta" come mostrato nella figura Fig. 3.41:

The screenshot shows the configuration interface for an MRequest API action. The top navigation bar indicates the path: API > SOAPBlockingPULL v1 > Servizi > Azioni di SOAPPull > MRequest. The main form is titled 'MRequest'. It contains three main sections: 'Azione' (Action), 'Informazioni Protocollo' (Protocol Information), and 'Modi PA' (PA Modes). In the 'Azione' section, the name is set to 'MRequest'. In the 'Informazioni Protocollo' section, the profile is set to 'usa profilo servizio'. In the 'Modi PA' section, under 'Profilo Interazione', the interaction profile is set to 'Non Bloccante'. Under 'Interazione', it is set to 'PULL'. Under 'Funzione', it is set to 'Richiesta'. In the 'Profilo Sicurezza Messaggio' section, the message security profile is set to 'Usa profilo API'.

Fig. 3.41: Configurazione della richiesta dell'API SOAP (PULL)

- Richiesta Stato

Successivamente, accedere al dettaglio dell'azione che consente di richiedere lo stato di processamento ed impostare nella sezione "Modi PA" un profilo di interazione non bloccante "PULL" con ruolo "Richiesta Stato". Definire anche la correlazione verso l'azione relativa alla richiesta come mostrato nella figura Fig. 3.42:

- Risposta

Accedere al dettaglio dell'azione corrispondente alla risposta ed impostare nella sezione "Modi PA" un profilo di interazione non bloccante "PULL" con ruolo "Risposta". Definire anche la correlazione verso l'azione relativa alla richiesta come mostrato nella figura Fig. 3.43:

Configurazione dell'Erogazione

Sul dominio dell'erogatore deve essere definita l'erogazione dell'API.

API > SOAPBlockingPULL v1 > Servizi > Azioni di SOAPPull > **MProcessingStatus**

MProcessingStatus

Azione

Nome MProcessingStatus

Informazioni Protocollo

Profilo usa profilo servizio

Modi PA

Profilo Interazione

Profilo	Non Bloccante
Interazione	PULL
Funzione	Richiesta Stato
Richiesta Correlata	MRequest

Profilo Sicurezza Messaggio

Profilo Usa profilo API

Fig. 3.42: Configurazione della richiesta stato di processamento dell'API SOAP (PULL)

API > SOAPBlockingPULL v1 > Servizi > Azioni di SOAPPull > **MResponse**

MResponse

Azione

Nome MResponse

Informazioni Protocollo

Profilo usa profilo servizio

Modi PA

Profilo Interazione

Profilo Non Bloccante

Interazione PULL

Funzione Risposta

Richiesta Correlata MRequest

Profilo Sicurezza Messaggio

Profilo Usa profilo API

Fig. 3.43: Configurazione della risposta dell'API SOAP (PUSH)

- Richiesta

Le richieste ricevute sull'erogazione vengono inoltrate al backend da GovWay rimanendo poi in attesa dell'acknowledgement.

Ricevuto il messaggio di acknowledgement GovWay verifica la presenza dell'header SOAP custom “X-Correlation-ID”. Se tale header non risulta presente viene generato da GovWay impostando come valore l'identificativo della transazione, che è stato inoltrato con la richiesta al backend tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Transaction-ID”).

Nota: Header “X-Correlation-ID” generato da GovWay

La generazione dell'header soap “X-Correlation-ID”, se non presente, è disabilitabile intervenendo sulla proprietà «org.openspcoop2.protocol.modipa.soap.pull.request.correlationId.header.useTransactionIdIfNotExists» presente nel file “/etc/govway/modipa_local.properties” (si assume che “/etc/govway” sia la directory di configurazione indicata in fase di installazione). Se si disabilita la proprietà, GovWay termina con errore la transazione se rileva l'assenza dell'header soap “X-Correlation-ID” nel messaggio di acknowledgement ricevuto dal backend.

- Richiesta Stato di Processamento

Le richieste che richiedono uno stato del processamento vengono validate da GovWay verificando la presenza dell'header soap “X-Correlation-ID” come previsto dal profilo “ModI PA”. Effettuata la validazione del messaggio di richiesta, eventualmente gestendo anche gli aspetti di sicurezza descritti nella sezione *Sicurezza Messaggio*, GovWay inoltra il messaggio al backend e rimane in attesa dell'acknowledgement. L'informazione sull'id di correlazione è inoltrato al backend, oltre che tramite l'header soap “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Conversation-ID”).

- Risposta

Le risposte vengono gestite da GovWay in maniera simile a quanto indicato per le richieste di stato del processamento.

Configurazione della Fruizione

Sul dominio del fruitore deve essere definita una fruizione dell'API.

- Richiesta

Le richieste devono essere inoltrate dall'applicativo mittente utilizzando la fruizione dell'API configurata su GovWay.

Il messaggio di acknowledgement ricevuto viene validato al fine di verificare la presenza dell'header soap “X-Correlation-ID” come previsto dalla specifica “ModI PA”. L'informazione sull'id di correlazione è ottenibile dall'applicativo mittente sulla risposta, oltre che tramite l'header soap “X-Correlation-ID”, anche tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Conversation-ID”).

- Richiesta Stato di Processamento

Le richieste che richiedono uno stato del processamento devono essere inoltrate dall'applicativo mittente utilizzando la fruizione dell'API configurata su GovWay. Le richieste vengono validate da GovWay verificando la presenza dell'header soap “X-Correlation-ID”. GovWay permette di fornire l'informazione sull'identificativo di correlazione anche tramite modalità alternative all'header soap per poi generarlo come previsto dalla specifica “ModI PA” valorizzato con il valore fornito. Le modalità alternative sono le seguenti:

- Header HTTP “X-Correlation-ID”
- Header HTTP “GovWay-Conversation-ID” o parametro della url “govway_conversation_id” previsto per la correlazione tramite identificativo di collaborazione descritta nella sezione *Correlazione tra transazioni differenti*.

Questa modalità richiede che sia abilitata l'indicazione dell'identificativo di collaborazione nell'API o sulla singola azione come mostrato nella figura Fig. 3.44:

The screenshot shows the 'MRequest' configuration page. In the 'Azione' section, the action name is 'MRequest'. In the 'Informazioni Protocollo' section, the 'ID Collaborazione' checkbox is checked, while 'Riferimento ID Richiesta' is unchecked.

Fig. 3.44: Abilitazione funzionalità di correlazione govway tramite identificativo di collaborazione

- Header HTTP “GovWay-Relates-To” o parametro della url “govway_relates_to” previsto per la correlazione tramite riferimento della richiesta descritta nella sezione *Correlazione tra transazioni differenti*. Questa modalità richiede che sia abilitata l'indicazione dell'identificativo di riferimento alla richiesta nell'API o sulla singola azione come mostrato nella figura Fig. 3.45:

The screenshot shows the 'MRequest' configuration page. In the 'Azione' section, the action name is 'MRequest'. In the 'Informazioni Protocollo' section, the 'Riferimento ID Richiesta' checkbox is checked, while 'ID Collaborazione' is unchecked.

Fig. 3.45: Abilitazione funzionalità di correlazione govway tramite identificativo della richiesta

- Risposta

Le risposte vengono gestite da GovWay in maniera simile a quanto indicato per le richieste di stato del processamento.

3.4.4 Profilo di Interazione PULL per API REST

Il profilo di interazione, denominato PULL, prevede che il fruitore non fornisca un indirizzo di callback, mentre l'erogatore fornisce un indirizzo interrogabile per verificare lo stato di processamento di una richiesta e, al fine dell'elaborazione della stessa, il risultato (Fig. 3.46).

Come riportato dalle Linee Guida di Interoperabilità ModI PA:

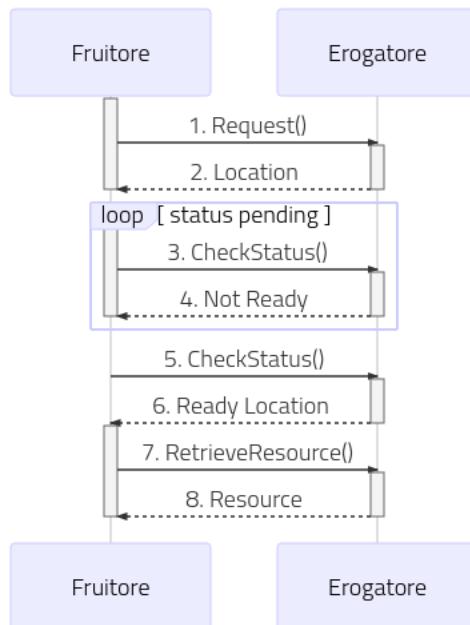


Fig. 3.46: Flusso previsto in un Profilo di Interazione PULL per API REST

- L’interfaccia di servizio dell’erogatore fornisce tre metodi differenti al fine di inoltrare una richiesta, controllarne lo stato ed ottenerne il risultato
- Al passo (1), il fruitore DEVE utilizzare il verbo HTTP POST;
- Al passo (2), l’erogatore DEVE fornire insieme all’acknowledgement della richiesta, un percorso di risorsa per interrogare lo stato di processamento utilizzando HTTP header Location ; Il codice HTTP di stato DEVE essere HTTP status 202 Accepted a meno che non si verifichino errori;
- Al passo (3), il fruitore DEVE utilizzare il percorso di cui al passo (2) per richiedere lo stato della risorsa; Il verbo HTTP utilizzato deve essere GET;
- Al passo (4) l’erogatore indica che la risorsa non è ancora pronta, fornendo informazioni circa lo stato della lavorazione della richiesta; il codice HTTP restituito è HTTP status 200 OK;
- Al passo (6) l’erogatore indica che la risorsa è pronta, utilizzando HTTP header Location ; per indicare il percorso dove recuperare la risorsa, il codice HTTP restituito è HTTP status 303 See Other;
- Al passo (8) l’erogatore risponde con la rappresentazione della risorsa,Il codice HTTP restituito è HTTP status 200 OK;

Configurazione delle API

Per attuare la configurazione su GovWay si deve procedere con la registrazione dell’API che deve contenere le tre risorse differenti descritti precedentemente.

- Richiesta

Effettuata la registrazione delle API, accedere al dettaglio della risorsa corrispondente alla richiesta ed impostare nella sezione “Modi PA” un profilo di interazione non bloccante “PULL” con ruolo “Richiesta” come mostrato nella figura Fig. 3.47:

- Richiesta Stato

API > RESTBlockingPULL v1 > Risorse > **POST /tasks/queue**

POST /tasks/queue

Note: (*) Campi obbligatori

Risorsa

HTTP Method: POST
Path: * /tasks/queue
Nome: POST_tasks.queue
Se non definito verrà automaticamente generato un identificativo univoco
Descrizione:

Informazioni Protocollo

ID Collaborazione:
Riferimento ID Richiesta:

Modi PA

Profilo Interazione
Profilo: Non Bloccante
Interazione: PULL
Funzione: Richiesta

Profilo Sicurezza Messaggio
Profilo: Usa profilo API

Fig. 3.47: Configurazione della richiesta dell'API REST (PULL)

Successivamente, accedere al dettaglio dell’azione che consente di richiedere lo stato di processamento ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PULL” con ruolo “Richiesta Stato”. Definire anche la correlazione verso la risorsa relativa alla richiesta come mostrato nella figura Fig. 3.48:

The screenshot shows the configuration interface for a REST API resource. The URL is `GET /tasks/queue/{id_task}/`. The 'Risorsa' section includes fields for HTTP Method (GET), Path (marked as required with a red asterisk), and Name (GET_tasks.queue.id_task). A note states: "Se non definito verrà automaticamente generato un identificativo univoco". The 'Informazioni Protocollo' section contains fields for ID Collaborazione and Riferimento ID Richiesta. The 'Modi PA' section includes a 'Profilo Interazione' group with dropdowns for Profilo (Non Bloccante), Interazione (PULL), Funzione (Richiesta Stato), and Richiesta Correlata (POST /tasks/queue). Below this is a 'Profilo Sicurezza Messaggio' group with a dropdown for Profilo (Usa profilo API).

Fig. 3.48: Configurazione della richiesta stato di processamento dell’API REST (PULL)

- Risposta

Accedere al dettaglio dell’azione corrispondente alla risposta ed impostare nella sezione “ModI PA” un profilo di interazione non bloccante “PULL” con ruolo “Risposta”. Definire anche la correlazione verso la risorsa relativa alla richiesta come mostrato nella figura Fig. 3.49:

Configurazione dell’Erogazione

Sul dominio dell’erogatore deve essere definita l’erogazione dell’API.

- Richiesta

Le richieste ricevute sull’erogazione vengono inoltrate al backend da GovWay rimanendo poi in attesa dell’acknowledgement.

API > RESTBlockingPULL v1 > Risorse > **GET /tasks/result/{id_task}/**

GET /tasks/result/{id_task}/

Note: (*) Campi obbligatori

Risorsa

HTTP Method	GET
Path *	/tasks/result/{id_task}/
Nome	GET_tasks.result.id_task
Se non definito verrà automaticamente generato un identificativo univoco	
Descrizione	

Informazioni Protocollo

ID Collaborazione	
Riferimento ID Richiesta	

Modi PA

Profilo Interazione	
Profilo	Non Bloccante
Interazione	PULL
Funzione	Risposta
Richiesta Correlata	POST /tasks/queue
Profilo Sicurezza Messaggio	
Profilo	Usa profilo API

Fig. 3.49: Configurazione della risposta dell'API REST (PUSH)

Ricevuto il messaggio di acknowledgement GovWay verifica che il codice HTTP di stato sia 202 e verifica la presenza dell'header HTTP “Location”.

- Richiesta Stato di Processamento

Le richieste che richiedono uno stato del processamento vengono validate da GovWay verificando che il codice HTTP di stato sia 200 (risposta non ancora pronta) o 303 (risposta pronta ad essere recuperata). Nel caso il codice HTTP sia 303 viene anche verificata la presenza dell'header HTTP “Location”.

- Risposta

Le risposte vengono gestite da GovWay vengono validate da GovWay verificando che il codice HTTP di stato sia 200.

Nota: Id Correlazione

GovWay estrae dal valore presente nell'header “Location” (per la richiesta e la richiesta stato) e dall'endpoint (per la risposta) l'identificativo di correlazione al fine di correlare la richiesta con le successive operazioni.

Configurazione della Fruizione

Sul dominio del fruitore deve essere definita una fruizione dell'API.

- Richiesta

Le richieste devono essere inoltrate dall'applicativo mittente utilizzando la fruizione dell'API configurata su GovWay.

Il messaggio di acknowledgement ricevuto viene validato al fine di verificare la presenza dell'header http “Location” come previsto dalla specifica “ModI PA”. L'informazione sull'id di correlazione è ottenibile dall'applicativo mittente sulla risposta tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta inoltrata dal gateway al server* e *Altri header di Integrazione* (per default tramite l'header http “GovWay-Conversation-ID”).

- Richiesta Stato di Processamento e Risposta

Le successive operazioni devono essere inoltrate dall'applicativo mittente utilizzando la fruizione dell'API configurata su GovWay.

Nota: Id Correlazione

GovWay estrae dal valore presente nell'header “Location” (per la richiesta) e dall'endpoint (per la richiesta stato e per la risposta) l'identificativo di correlazione al fine di correlare la richiesta con le successive operazioni.

CAPITOLO 4

Profilo “eDelivery”

Il profilo eDelivery 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 forinati 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.

4.1 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 selettori 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* (Fig. 4.1).

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 (Fig. 4.2).

eDelivery	
Base URL Erogazione	<input type="text" value="http://localhost:8080/domibus/services/msh"/>
Base URL Fruizione	<input type="text" value="http://localhost:8080/openspcoop2/as4/PD/"/>
Soggetto	EntelInterno
Visualizza Dati Soggetto	

Fig. 4.1: Configurazione delle Base URL 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.

4.2 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 Fig. 4.3.

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.

Soggetti > EntelInterno

Note: (*) Campi obbligatori

Soggetto

Nome *

Descrizione

eDelivery

Party Info

Id *

Type Name *

Type Value *

Party Endpoint

URL *

Common Name *

Invia **Cancella**

Fig. 4.2: Configurazione delle proprietà eDelivery per il soggetto interno

The screenshot shows the 'eDelivery' configuration interface. It includes sections for 'Service Info' (Type and Name fields), 'Payload Profiles' (Browse... button and 'No file selected.' message), and 'Properties' (Browse... button and 'No file selected.' message).

Fig. 4.3: Registrazione API eDelivery - Proprietà specifiche

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 property eDelivery (Fig. 4.4).

The screenshot shows the 'eDelivery' configuration interface for actions. It includes sections for 'Action Info' (Name field set to 'POST_store.pdf'), 'Payload' (Profile dropdown set to 'DefaultBinaryProfile' and Compress checkbox checked), and other configuration options.

Fig. 4.4: 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 (Fig. 4.5).



Fig. 4.5: 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. È 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 *Generazione del PMODE Domibus*.

4.3 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 nella sezione *Erogazione di servizi in modalità eDelivery*. 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 *Generazione del PMODE Domibus*.

4.4 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 (Fig. 4.6):

- 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.

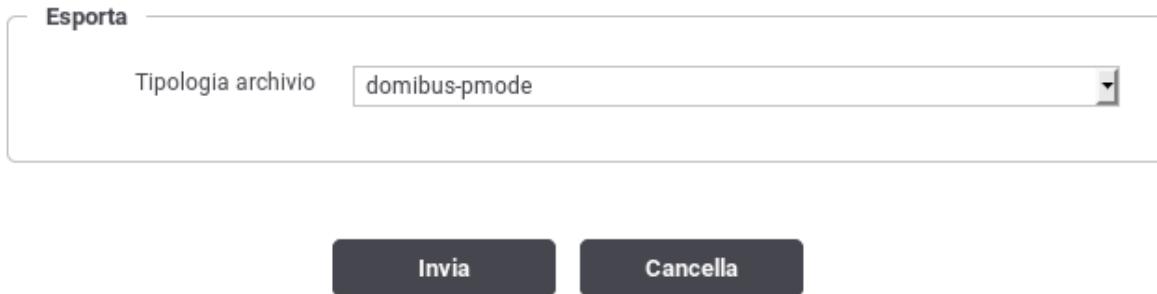


Fig. 4.6: Esportazione del PMODE

CAPITOLO 5

Profilo “SPCoop”

Il profilo SPCoop consente di produrre le configurazioni per i servizi, in accordo alla omonima 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.

5.1 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 figure seguenti, 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.

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 *Configurazione manuale delle interfacce*. In questo caso, l'aggiunta del servizio, comprende i profili di collaborazione asincroni oltre alle caratteristiche aggiuntive specifiche del protocollo SPCoop (vedi sezione *Profili di gestione della busta eGov*). La figura seguente mostra i dettagli di questo caso.

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.

The screenshot shows a web-based form for creating a new API. At the top left, there is a breadcrumb navigation: "API > Aggiungi". Below it, a note says "Note: (*) Campi obbligatori". The form is divided into two main sections: "API" and "Specifiche delle interfacce".

API

- Soggetto referente *: EnteInterno
- Nome *: Accordo1
- Descrizione: (empty input field)
- Versione: 1

Specifiche delle interfacce

- WSDL: A "Browse..." button with the message "No file selected."

At the bottom right of the form are two buttons: "Invia" and "Cancella".

Fig. 5.1: Creazione Accordo di Servizio SPCoop

API > Servizi di AccordoServizio:1 (EnteInterno) > Aggiungi

Note: (*) Campi obbligatori

Servizio

Nome *

Descrizione

Informazioni Protocollo

Profilo di collaborazione

Filtro duplicati

Conferma ricezione

ID Collaborazione

Consegna in ordine

Scadenza

Invia **Cancella**

Fig. 5.2: Aggiunta Servizio SPCoop

Informazioni Generali

API

Nome	AccordoServizio:1 (EnteInterno)
Tipo	Soap
Servizio *	servizio

Servizio

Tipo	spc
Tipologia Servizio	normale
Versione Protocollo	eGov1.1-lineeGuida1.1

Fig. 5.3: Creazione erogazione SPCoop

5.2 Profili Asincroni

5.2.1 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.

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.

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.

5.2.2 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.

API > Servizi di aaaa:1 (INPS) > Azioni di serviziocorrelato > Aggiungi

Note: (*) Campi obbligatori

Azione

Nome * azioneconrelata

Informazioni Protocollo

Profilo usa profilo servizio

Correlazione asincrona

Correlata al servizio servizio

Correlata all'azione * azione1

SALVA

The screenshot shows a web-based configuration interface for adding a new correlated action. At the top, the path is indicated: API > Servizi di aaaa:1 (INPS) > Azioni di serviziocorrelato > Aggiungi. Below this, a note states "Note: (*) Campi obbligatori". The main area is divided into three sections: "Azione" (Action), "Informazioni Protocollo" (Protocol Information), and "Correlazione asincrona" (Asynchronous Correlation). In the "Azione" section, the name "azioneconrelata" is entered into the required field. In the "Informazioni Protocollo" section, the profile "usa profilo servizio" is selected. In the "Correlazione asincrona" section, both "Correlata al servizio" and "Correlata all'azione" fields are populated with "servizio" and "azione1" respectively. A large "SALVA" (Save) button is located at the bottom of the form.

Fig. 5.4: Correlazione Asincrona Simmetrica

Note: (*) Campi obbligatori

Azione

Nome * azioneCorrelata

Informazioni Protocollo

Profilo ridefinisci

Profilo di collaborazione asincronoAsimmetrico

Filtro duplicati

Conferma ricezione

ID Collaborazione

Consegna in ordine

Scadenza

Correlazione asincrona

Correlata al servizio -

Correlata all'azione azione

SALVA

Fig. 5.5: Correlazione Asincrona Asimmetrica

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.

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.

5.3 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 5.1 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

Tabella 5.1: Descrizione di un accordo di servizio

Nome Documento	Accordo
<i>Specifiche delle Interfacce</i>	
WSDL Definitorio	Parte Comune
WSDL Concettuale	Parte Comune
WSDL Logico Erogatore	Parte Comune
WSDL Logico Fruitore	Parte Comune
<i>Specifiche delle Implementazioni</i>	
WSDL Implementativo Erogatore	Parte Specifica
WSDL Implementativo Fruitore	Parte Specifica

5.4 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 modalità (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 specifiche e-Gov1.1, per altri secondo le Linee Guida 1.1
- Uno o più fruitori accedono al un servizio erogato secondo le specifiche e-Gov1.1, altri secondo le Linee Guida 1.1

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

5.4.1 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 compatibilità 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*.

Tabella 5.2: Opzioni della busta eGov

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

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.

Informazioni Protocollo

Profilo di collaborazione	<input type="text" value="sincrono"/>	<input type="button" value="▼"/>
Filtro duplicati	<input checked="" type="checkbox"/>	
Conferma ricezione	<input checked="" type="checkbox"/>	
ID Collaborazione	<input checked="" type="checkbox"/>	
Consegna in ordine	<input checked="" type="checkbox"/>	
Scadenza	<input type="text"/>	

Fig. 5.6: Controlli avanzati sulle informazioni eGov relative all'accordo di servizio

CAPITOLO 6

Profilo “Fatturazione Elettronica”

Il profilo «Fatturazione Elettronica» 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 (http://www.fatturapa.gov.it/export/fatturazione/sdi/Specifiche_tecniche_SdI_v1.6.pdf).

Il profilo «Fatturazione Elettronica» 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*.

6.1 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 Fig. 6.1.

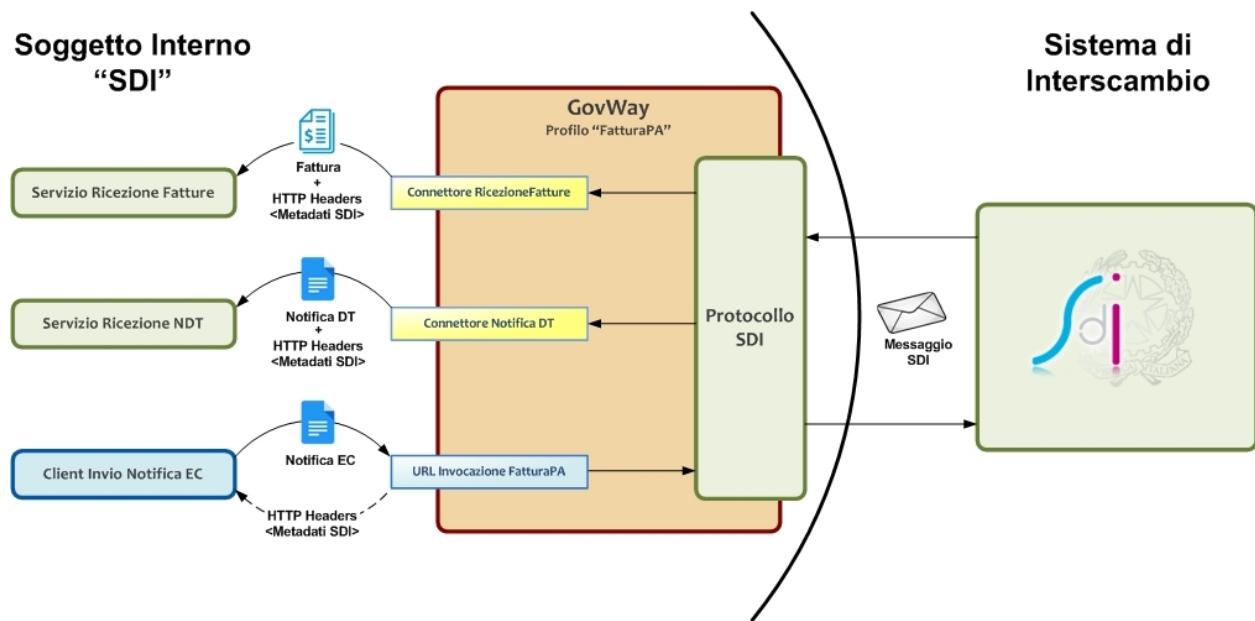


Fig. 6.1: Scenario di interoperabilità relativo alla Fatturazione Passiva

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 6.1).

Nota: Nella configurazione di default GovWay non consegna il file Metadati all'applicativo. È possibile attivare la consegna abilitando la proprietà “org.openscoop2.protocol.sdi.fatturazionePassiva.consegnaFileMetadati” all'interno del file /etc/govway/sdi_local.properties. Il file Metadati verrà consegnato, codificato in base64, nell'header HTTP “GovWay-SDI-FileMetadati”.

- *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 6.2).
- *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 6.3).

Tabella 6.1: Header di Integrazione Ricezione Fattura

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 6.2: Header di Integrazione Invio Notifica EC

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

Tabella 6.3: Header di Integrazione Ricezione Notifica DT

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

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-passiva.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.

6.1.1 Ricezione Fatture e Notifiche di Decorrenza Termini

Allo SdI, per raggiungere il servizio di RicezioneFatture su Govway, dovrà essere comunicata la seguente URL:

```
https://<host-govway>/govway/sdi/<SoggettoSDI>/RicezioneFatture/v1
```

Le fatture e le notifiche saranno consegnati all'applicativo dell'ente secondo le modalità specificate durante l'esecuzione del Govlet. In fase di consegna delle fatture e delle notifiche verranno generati rispettivamente gli header descritti nelle tabelle precedenti.

6.1.2 Invio della Notifica di Esito Committente

Per l'invio della Notifica di Esito Committente l'applicativo deve utilizzare:

- Una URL così composta:

```
http://<host-govway>/govway/sdi/out/xml2soap/<SoggettoSDI>/CentroServiziFatturaPA/
  ↵SdIRiceviNotifica/v1?NomeFile=<NomeFileFattura>&IdentificativoSdI=
  ↵<identificativoSDI>
```

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.

- L'invocazione deve essere corredata dalle credenziali che sono state indicate durante la configurazione tramite il relativo govlet.

- Utilizzare l'header http *Content-Type* valorizzato con *text/xml* o *application/xml*

Un esempio di invio di una fattura viene fornito tramite il seguente comando curl:

Soggetto Interno al Dominio

In questo esempio si suppone che il nome del soggetto (riferito precedentemente come *SoggettoSDI*) fornito durante la fase di installazione di GovWay sia *Ente*.

```
curl -X POST --basic --user SdIRiceviNotifica:123456 \
--data-binary @IT01234567890_11111_EC_001.xml \
-H "Content-Type: application/xml" \
"http://127.0.0.1:8080/govway/sdi/out/xml2soap/Ente/CentroServiziFatturaPA/
  ↵SdIRiceviNotifica/v1?NomeFile=IT01234567890_11111.xml&IdentificativoSdI=345"
```

Nota: La generazione di un nome di file univoco da associare alla notifica di esito committente viene gestita da GovWay.

È possibile disabilitare tale gestione disabilitando la proprietà “org.openscoop2.protocol.sdi.fatturazionePassiva.nomeFile.gestione” nel file “/etc/govway/sdi_local.properties”. Se viene disabilitata la funzionalità (attiva per default), la gestione dei nomi dei file (correttezza sintattica, univocità, ...) è demandata all’Applicativo Client che deve obbligatoriamente fornire il nome da associare alla notifica di esito committente del file attraverso uno dei seguenti modi:

- query parameter “NomeFile”
- header http “SDI-NomeFile”
- header http “GovWay-SDI-NomeFile”

6.2 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 Fig. 6.2.

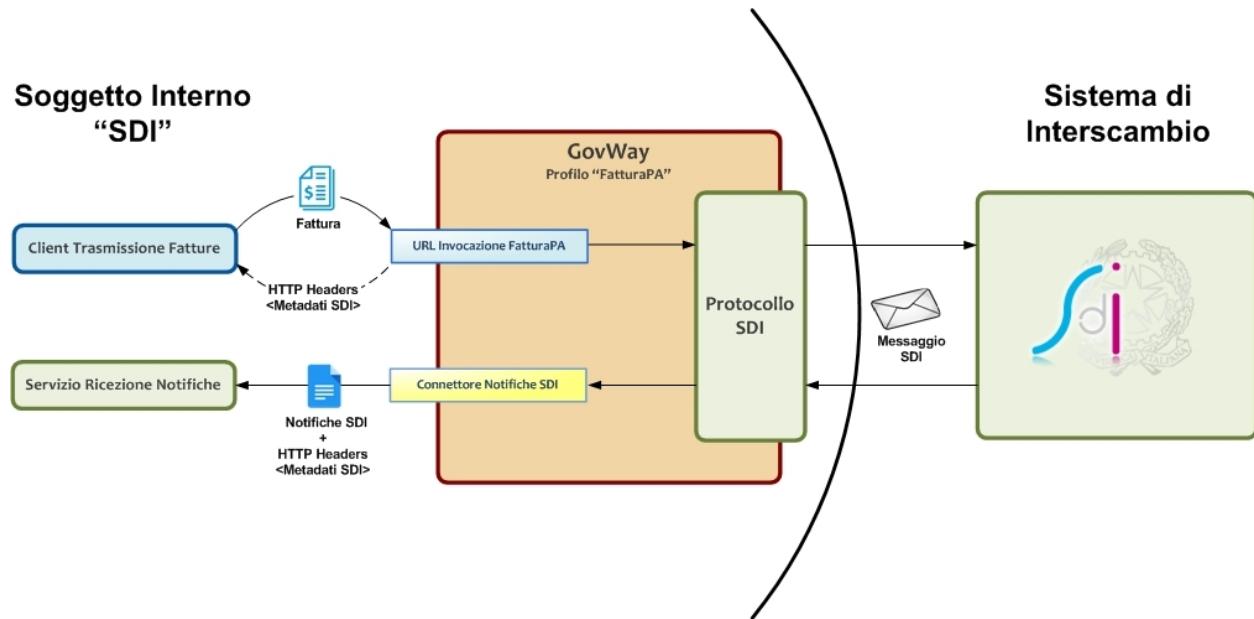


Fig. 6.2: Scenario di interoperabilità relativo alla Fatturazione Attiva

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 6.4).
- *Servizio Ricezione Notifiche*. I sistemi dell’ente devono esporre un servizio adibito 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 6.5).

Tabella 6.4: 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 6.5: Header di Integrazione “Ricezione Notifiche”

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

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-attiva.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.

6.2.1 Invio della fattura

Per l’invio della fattura l’applicativo mittente deve utilizzare:

- Una URL così composta:

```
http://<host-govway>/govway/sdi/out/xml2soap/<SoggettoSDI>/CentroServiziFatturaPA/
  ↵SdIRiceviFile/v1?Versione=<VersioneFatturaPA>&TipoFile=<TipoFile>&IdPaese=
  ↵<IdPaese>&IdCodice=<IdCodice>
```

dove:

- *host-govway*: è l'hostname con cui è raggiungibile l'istanza di Govway.
- *SoggettoSDI*: il soggetto interno al dominio 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: XML (Fattura firmata XADES), P7M (Fattura firmata CADES) o ZIP (archivio di fatture).
- *IdPaese e IdCodice*: dati del trasmittente della fattura.
- L'invocazione deve essere corredata dalle credenziali che sono state indicate durante la configurazione tramite il relativo govlet.
- A seconda del tipo di fattura deve essere utilizzato il corretto header http *Content-Type*:
 - XML: è possibile utilizzare *text/xml* o *application/xml*
 - P7M: *application/pkcs7-mime*
 - XML: *application/zip*

Un esempio di invio di una fattura viene fornito tramite il seguente comando curl:

Soggetto Interno al Dominio

In questo esempio si suppone che il nome del soggetto (riferito precedentemente come *SoggettoSDI*) fornito durante la fase di installazione di GovWay sia *Ente*.

```
curl -X POST -basic --user SdIRiceviFile:123456 \
--data-binary @IT01234567890_11111.xml.p7m \
-H "Content-Type: application/pkcs7-mime" \
"http://127.0.0.1:8080/govway/sdi/out/xml2soap/Ente/CentroServiziFatturaPA/
↪SdIRiceviFile/v1?Versione=SDI10&TipoFile=P7M&IdPaese=IT&IdCodice=01629370097"
```

Nota: La generazione di un nome di file univoco da associare alla fattura viene gestita da GovWay.

È possibile disabilitare tale gestione disabilitando la proprietà “org.openspcoop2.protocol.sdi.fatturazioneAttiva.nomeFile.gestione” nel file “/etc/govway/sdi_local.properties”. Se viene disabilitata la funzionalità (attiva per default), la gestione dei nomi dei file (correttezza sintattica, univocità, ...) è demandata all'Applicativo Client che deve obbligatoriamente fornire il nome del file da associare alla fattura attraverso uno dei seguenti modi:

- query parameter “NomeFile”
 - header http “SDI-NomeFile”
 - header http “GovWay-SDI-NomeFile”
-

6.2.2 Ricezione delle Notifiche dallo Sdi

Allo Sdi dovrà essere comunicata la seguente url che utilizzerà per inoltrare le notifiche:

```
https://<host-govway>/govway/sdi/<SoggettoSDI>/TrasmissioneFatture/v1
```

Le notifiche ricevute verranno consegnate secondo le modalità specificate durante l'esecuzione del Govlet. In fase di consegna verranno generati gli header descritti nella [Tabella 6.5](#)

Strumenti

7.1 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.

7.2 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 [Auditing](#).

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 [Utenti](#)) 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 Fig. 7.1.

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 *qualsiasi 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*

The screenshot shows a search form for auditing data. At the top left, it says "Reportistica > Auditing". The form is divided into three main sections: "Criteri di Ricerca", "Operazione", and "Oggetto".

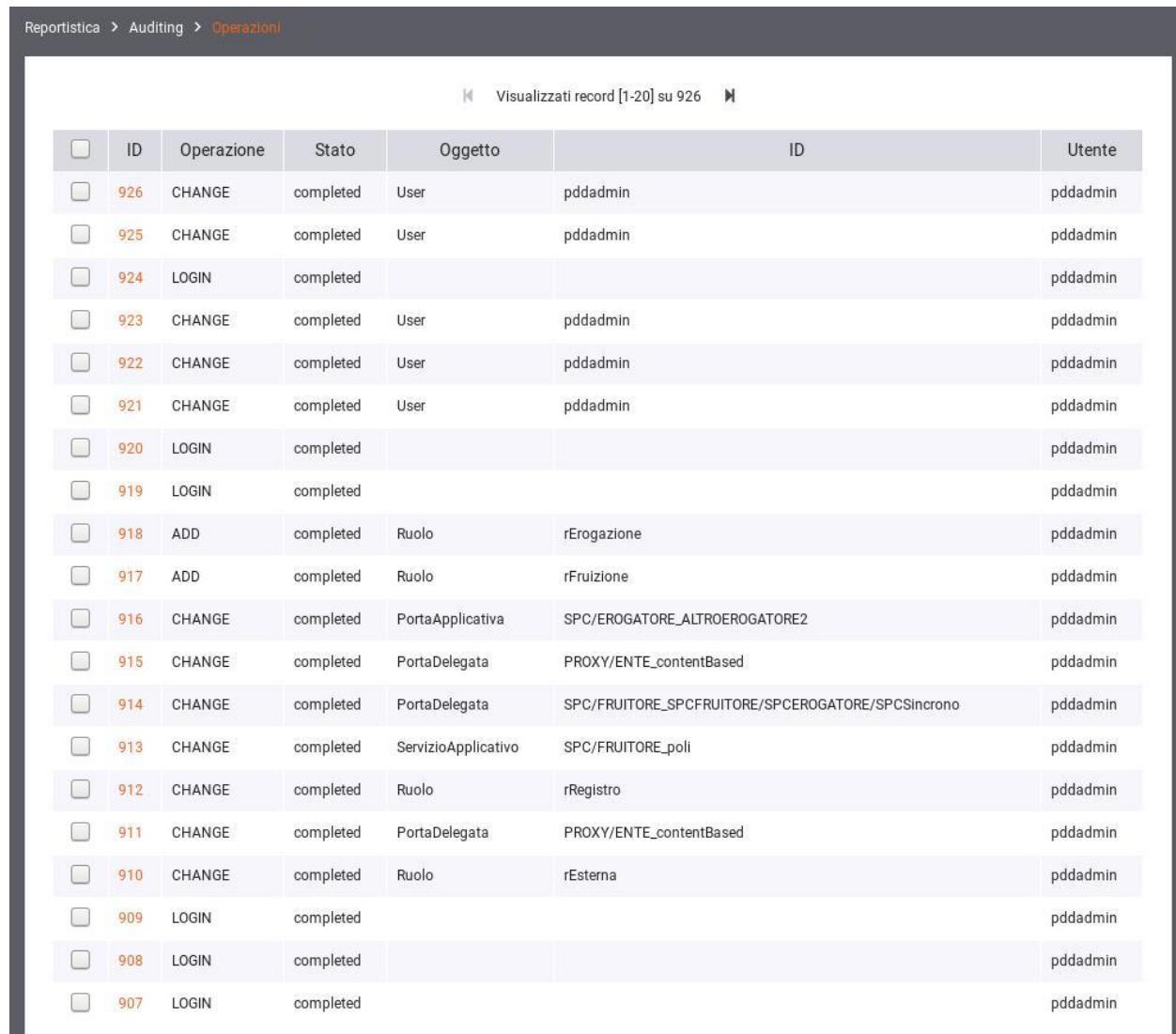
- Criteri di Ricerca:** Contains fields for "Inizio intervallo" (Start date) and "Fine intervallo" (End date), both with placeholder text "Indicare una data nel formato 'yyyy-MM-dd'". It also has a field for "Utente" (User).
- Operazione:** Contains dropdown fields for "Tipo" (Type) and "Stato" (State).
- Oggetto:** Contains dropdown fields for "Tipo" (Type), and text input fields for "Identificativo" (Identifier), "Id precedente alla modifica" (Previous ID before modification), and "Contenuto" (Content).

At the bottom right of the form are two buttons: "Invia" (Send) and "Cancella" (Delete).

Fig. 7.1: Maschera di ricerca dei dati di auditing

- **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 Fig. 7.2).



The screenshot shows a table titled "Operazioni" under the "Auditing" section of the "Reportistica" menu. The table lists 926 audit records, with 20 displayed on the current page. The columns are: ID, Operazione, Stato, Oggetto, ID, and Utente. The data includes various operations like CHANGE, LOGIN, and ADD, performed by users like pddadmin on objects such as User, Ruolo, and PortaApplicativa.

	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

Fig. 7.2: 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 Fig. 7.3). 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).

The screenshot shows a user interface for auditing. At the top, a breadcrumb navigation path is visible: Reportistica > Auditing > Operazioni > Dettaglio di 916. Below this, a section titled "Dettaglio Operazione" displays various parameters of an audit trace:

Time request	2017-08-11 11:12:34.834
Time execute	2017-08-11 11:12:34.917
Tipo operazione	CHANGE
Tipo oggetto	PortaApplicativa
Identificativo	SPC/EROGATORE_ALTROEROGATORE2
Utente	pddadmin
Stato	completed

Below the table, a link labeled "Documenti Binari (0)" is present.

Fig. 7.3: Dettaglio di una traccia di auditing

CAPITOLO 8

Configurazione

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

8.1 Generale

La sezione *Configurazione > Generale* consente di impostare i parametri generali per le funzionalità di base del gateway ([Fig. 8.1](#)). In particolare è possibile:

- Attivare e configurare la modalità Multi-Tenant. Abilitando questa modalità sarà ammessa la creazione di ulteriori soggetti interni al dominio GovWay.
- Configurare le Base URL utilizzate per visualizzare le URL di invocazione delle API
- Configurare la gestione del CORS (*cross-origin HTTP request (CORS)*) a livello globale valido per tutte le APIs
- Configurare il Caching Risposta a livello globale valido per tutte le APIs
- Configurare i profili fornendo i riferimenti ai servizi di base per l'elaborazione dei messaggi ed al soggetto interno

8.1.1 Multi-Tenant

Per abilitare la modalità multi-tenant è sufficiente selezionare il valore «abilitato» sull'elemento Stato.

Dopo aver abilitato l'opzione multi-tenant è possibile creare nuovi soggetti interni al dominio, come indicato alla sezione [Creazione di un soggetto](#). In questo contesto, i soggetti avranno come elemento distintivo il dominio, che può essere *Interno* o *Esterno*.

I dettagli sulla configurazione dell'opzione multi-tenant sono riportati nella sezione [Multi-Tenant](#).

Configurazione Generale

Note: (*) Campi obbligatori

Multi-Tenant

Stato: disabilitato

URL di Invocazione API

Base URL *: http://localhost:8080/govway/
 Base URL Fruizione:
[Regole Proxy Pass \(3\)](#)

Gestione CORS

Stato: abilitato

Access Control

All Allow Origins:
 Allow Credentials:
 Allow Methods *: GET x, PUT x, POST x, DELETE x, PATCH x
 Allow Request Headers *: Authorization x, Content-Type x, SOAPAction x, Cache-Control x
 Expose Response Headers:

Caching Risposta

Stato: disabilitato

Gestione Profilo

API Gateway

Soggetto: ENTE

8.1.2 URL di Invocazione API

Questa sezione visualizza:

- *Base URL*: Indica il prefisso utilizzato per visualizzare le URL di Invocazione delle API.
- *Base URL Fruizione*: permette di differenziare il prefisso utilizzato per visualizzare le URL di Invocazione delle fruizioni dalle erogazioni.
- *Regole Proxy Pass*: tramite questa voce è possibile ridefinire le URL di Invocazioni, per specifiche fruizioni e/o erogazioni, allineandole a regole configurate su un reverse proxy che media le comunicazioni http con GovWay.

Regole Proxy Pass

Questa sezione permette di ridefinire la modalità di visualizzazione delle Url di Invocazione delle API esposte da GovWay per assicurare che, in presenza di un reverse proxy che media le comunicazioni http con GovWay, sia possibile configurare opportunamente le url di invocazione delle API esposte da GovWay allineandole con le eventuali configurazioni specifiche realizzate sul reverse proxy.

Nota: La funzionalità permette di configurare come vengono visualizzate le URL di Invocazione sulla govwayConsole, per allinearsi ad un eventuale reverse proxy che media le comunicazioni http con GovWay. Le API, su GovWay, rimangono raggiungibili solamente sulle url originali e dovrà essere il reverse proxy ad effettuare la conversione rispetto a quella esposta.

Le regole create sono visualizzate nella forma di elenco ordinato (Fig. 8.2). L'icona iniziale di ciascun elemento consente di modificarne la posizione. Per ogni regola viene visualizzato il suo stato, il nome e la descrizione.

The screenshot shows a table titled "Regole di Proxy Pass" with the following data:

	Ordine	Stato	Nome	Descrizione
<input type="checkbox"/>	▼	<input checked="" type="checkbox"/>	<u>Domibus</u>	Servizio di ricezione dei messaggi AS4 dell'Access Point Domibus
<input type="checkbox"/>	^ ▼	<input checked="" type="checkbox"/>	<u>ServizioAnagrafica</u>	Ridefinisce le url di invocazione per l'Anagrafica
<input type="checkbox"/>	^	<input checked="" type="checkbox"/>	<u>HostProduzioneErogazioniModIPa</u>	Ridefinisce l'hostname utilizzato per le erogazioni ModI PA

At the bottom right of the table are two buttons: "ELIMINA" (Delete) and "AGGIUNGI" (Add).

Fig. 8.2: Lista Regole Proxy Pass

Per ogni regola (Fig. 8.3) deve essere obbligatoriamente definita una stringa libera o una espressione regolare utilizzata per individuare l'applicabilità della regola attraverso un confronto con il contesto dell'API. Il contesto è l'URL di Invocazione dell'API senza il prefisso Base URL. Inoltre per ogni regola è possibile indicare altri criteri di applicabilità

opzionali quali eventuali profilo di interoperabilità, un soggetto, una tipologia (fruizione/erogazione) o un tipo di api (soap/rest).

Il dettaglio dei campi associati ad una regola sono raggruppati in tre sottosezioni:

Informazioni generiche:

- *Nome*: Identificativo della regola
- *Stato*: Indica se la regola è abilitata o meno.
- *Descrizione*: (Opzionale) Descrizione generica della regola

Le regole di applicabilità vengono definite dai seguenti campi:

- *Espressione Regolare*: Indica se la regola sottostante è una espressione regolare o una stringa libera.
- *Regola*: Stringa libera o espressione regolare.
 - L'espressione regolare viene utilizzata per verificarne il match sull'contesto dell'API (url di invocazione senza la Base URL)
 - Nel caso di stringa libera si ha un'applicabilità se il contesto dell'API (url di invocazione senza la Base URL) inizia con la stringa fornita.
- *Profilo*: (Opzionale) Profilo di Interoperabilità per il quale si applica la regola
- *Soggetto*: (Opzionale) Soggetto interno per il quale si applica la regola
- *Ruolo*: (Opzionale) Tipologia di API (Erogazione/Fruizione) per il quale si applica la regola
- *Tipo API*: (Opzionale) Tipo di API (REST/SOAP) per il quale si applica la regola

La nuova url di invocazione viene definita attraverso i campi “Base URL” e “Contesto”. Se è stata fornita una espressione regolare nei due campi possono essere utilizzati le keyword “\${posizione}” per impostare un valore dinamico individuato tramite l'espressione regolare fornita. Il primo match, all'interno dell'espressione regolare, è rappresentata da “\${0}” (Ad esempio: [http://server:8080/\\${0}/altro/\\${1}](http://server:8080/${0}/altro/${1}))

- *Base URL*: Permette di ridefinire la Base URL utilizzata rispetto a quanto definito nella configurazione generale
- *Contesto*: Indica il contesto da utilizzare dopo la Base URL

Esempio 1

Tutte le API REST erogate dal Soggetto “ENTE” tramite il profilo “ModI PA” possiedono nell'installazione di default la seguente URL di Invocazione:

- <http://localhost:8080/rest/in/ENTE/NomeAPI/v1>

Per modificare la url di invocazione in modo da spostare il nome del soggetto come hostname, e rimodulare il contesto in modo da visualizzare prima la versione, è possibile utilizzare la seguente configurazione di proxy pass:

Criteri di Applicabilità:

- Espressione Regolare: true
- Regola: .+/in/(.+)/(.+)/v(.+)
- Profilo: ModI PA
- Soggetto: ENTE
- Ruolo: Erogazione
- Tipo API: REST

Nuova URL di Invocazione

Configurazione Generale > Regole di Proxy Pass > **HostProduzioneErogazioniModIPA**

HostProduzioneErogazioniModIPA

Note: (*) Campi obbligatori

Regola

Nome *	HostProduzioneErogazioniModIPA
Stato	abilitato
Descrizione	Ridefinisce l'hostname utilizzato per le erogazioni Mod IPA

Criteri di Applicabilità

Espressione Regolare	<input checked="" type="checkbox"/>
Regola *	.+/in/(.+)/(.+)/v(.+)
Profilo	Modi PA
Ruolo	Erogazione
Tipo API	Rest

Nuova URL di Invocazione

Base URL	http://\${0}/
Contesto	v\${2}/api/\${1}

SALVA

Fig. 8.3: Creazione Regola Proxy Pass

- Base URL: `http://${0}/`
- Contesto: `v${2}/api/${1}`

L'url di invocazione prodotta sarà:

- `http://ENTE/v1/api/NomeAPI`

Esempio 2

Supponiamo di voler modificare l'url di invocazione dell'API "PetStore" versione 1 erogata dal soggetto "ENTE" tramite il profilo di interoperabilità "ModI PA". Nell'installazione di default viene fornita la seguente URL di Invocazione:

- `http://localhost:8080/rest/in/ENTE/PetStore/v1`

Lo scopo è quello di eliminare il nome del soggetto e di togliere la "v" dalla versione. Per farlo è possibile utilizzare la seguente configurazione di proxy pass:

Criteri di Applicabilità:

- Espressione Regolare: false
- Regola: /rest/in/ENTE/PetStore/v1
- Profilo: ModI PA
- Soggetto: Qualsiasi
- Ruolo: Qualsiasi
- Tipo API: Qualsiasi

Nuova URL di Invocazione

- Base URL:
- Contesto: /rest/in/PetStore/1

L'url di invocazione prodotta sarà:

- `http://localhost:8080/rest/in/PetStore/1`

8.1.3 Gestione CORS

In GovWay è possibile abilitare la gestione del CORS (*cross-origin HTTP request (CORS)*) globalmente in modo che sia valido per tutte le APIs.

La configurazione permette di specificare i seguenti parametri:

- *Stato*: Indicazione se la gestione del CORS è abilitata o meno globalmente su GovWay.
- *Access Control*: tutti i parametri seguenti permettono di configurare il CORS. Per il dettaglio su cosa significa ogni singola voce si rimanda alla specifica CORS <https://www.w3.org/TR/cors/>.
 - *All Allow Origins*: se abilitato viene impostato nell'header http "Access-Control-Allow-Origin" il valore "`*`"
 - *Allow Origins*: nel caso non venga abilitato il parametro precedente, in questo campo è possibile indicare una lista di origin che vengono impostate nell'header http "Access-Control-Allow-Origin"
 - *Allow Credentials*: se abilitato o disabilitato viene impostato relativamente il valore true o false nell'header "Access-Control-Allow-Credentials"
 - *Allow Methods*: metodi inseriti nell'header http "Access-Control-Allow-Methods"
 - *Allow Request Headers*: nomi di header inseriti nell'header http "Access-Control-Allow-Headers"

- *Expose Response Headers*: abilita l’accesso a specifici headers, presenti nella risposta, da parte dei client.

Gestione CORS

Stato	abilitato
Access Control	
All Allow Origins	<input checked="" type="checkbox"/>
Allow Origins *	<input type="text"/>
Allow Credentials	<input checked="" type="checkbox"/>
Allow Methods *	<input type="button" value="GET"/> <input type="button" value="PUT"/> <input type="button" value="POST"/> <input type="button" value="DELETE"/> <input type="button" value="PATCH"/>
Allow Request Headers *	<input type="button" value="Authorization"/> <input type="button" value="Content-Type"/> <input type="button" value="SOAPAction"/> <input type="button" value="Cache-Control"/>
Expose Response Headers	<input type="text"/>

Fig. 8.4: Maschera di configurazione generale del CORS

8.1.4 Caching Risposta

In GovWay è possibile abilitare il salvataggio delle risposte in una cache globalmente in modo che sia attivo per tutte le APIs. Questa funzionalità permette ad un backend server di non dover riprocessare le stesse richieste più volte.

La configurazione permette di specificare i seguenti parametri:

- *Stato*: Indicazione se il salvataggio delle risposte in cache è abilitata o meno globalmente su GovWay.
- *Cache Timeout (secondi)*: intervallo di tempo, definito in secondi, per il quale la risposta salvata in cache viene utilizzata come risposte a successive richieste di un client.
- *Dimensione Max Risposta*: se abilitato deve essere definita la dimensione massima (in kb) che una risposta può avere per essere salvata in cache.
- *Generazione Hash*: ad ogni risposta salvata in cache viene associato un valore hash calcolato rispetto ai dati della richiesta che risultano abilitati tra le opzioni seguenti:
 - *URL di Richiesta*: viene utilizzata la URL della richiesta per il calcolo dell’hash.
 - *Payload*: viene utilizzato il payload della richiesta per il calcolo dell’hash.
 - *Headers*: vengono utilizzati gli header della richiesta indicati per il calcolo dell’hash. L’abilitazione di questa opzione comporta l’aggiunta di un elemento per consentire di specificare gli headers da selezionare.
- *Cache Control*: opzioni aggiuntive per la gestione della cache basate sul header HTTP «Cache-Control»:
 - *No Cache*: consente di attivare l’utilizzo della direttiva «no-cache» al fine di effettuare una richiesta evitando di ottenere una risposta dalla cache.

- *Max Age*: consente di attivare l'utilizzo della direttiva «max-age» che consente di forzare il tempo di vita, al valore fornito, della risposta inserita in cache.
- *No Store*: consente di attivare l'utilizzo della direttiva «no-store» che consente di impedire l'inserimento in cache della risposta generata dalla richiesta corrente.

Caching Risposta

Stato	<input type="checkbox"/> abilitato
Cache Timeout (secondi)	300
Dimensione Max Risposta	<input checked="" type="checkbox"/>
Dimensione Max (kb)	1
Generazione Hash	
URL di Richiesta	<input type="checkbox"/> abilitato
Payload	<input type="checkbox"/> abilitato
Headers	<input type="checkbox"/> disabilitato
Cache Control	
No Cache	<input checked="" type="checkbox"/>
Max Age	<input checked="" type="checkbox"/>
No Store	<input checked="" type="checkbox"/>

Fig. 8.5: Maschera di configurazione per il Caching della Risposta

Dopo aver salvato la configurazione fornita per il caching della risposta, appare la sezione *Configurazione Avanzata* che comprende il link *Regole*. Seguendo tale link è possibile inserire ulteriori criteri avanzati per la gestione della cache. Come si vede in Fig. 8.6 ciascuna regola è composta dai seguenti campi:

- *Codice Risposta*: codice HTTP ottenuto in risposta. Sono disponibili per la scelta le seguenti opzioni:
 - *Qualsiasi*: indica qualunque valore del codice HTTP restituito
 - *Singolo*: consente di specificare un singolo valore del codice HTTP restituito
 - *Intervallo*: consente di fornire l'intervallo dei valori ammessi per il codice HTTP restituito
- *Cache Timeout (Secondi)*: indica in secondi il timeout applicato agli elementi in cache relativamente ai codici HTTP che soddisfano la regola.
- *Fault*: opzione per specificare se anche i messaggi di fault devono essere inseriti in cache.

The screenshot shows a configuration form titled 'Regola'. It contains three input fields: 'Codice Risposta' with the value 'Qualsiasi', 'Cache Timeout (Secondi)' with a dropdown menu, and 'Fault' with a checked checkbox. Below the form is a large 'SALVA' button.

Fig. 8.6: Inserimento di una regola per il Caching della Risposta

8.1.5 Profili

Questa sezione viene visualizzata solamente se non è attiva la modalità Multi-tenant. Per ciascun Profilo di Interoperabilità, attivo sul gateway, viene visualizzato il nome del Soggetto interno che eroga/fruisce. Subito sotto il soggetto è presente un collegamento che porta al form di editing del soggetto visualizzato.

8.2 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 Fig. 8.7 è mostrata la pagina di 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.

Tracciamento

Transazioni Registrate

Selezionare gli esiti che verranno registrati nello storico

Completate con successo

Stato: abilitato

Fault applicativo

Stato: abilitato

Fallite

Stato: abilitato

Superamento Limite Richieste

Stato: disabilitato

Messaggi Diagnostici

Livello di Log su DB: infoIntegration

Livello di Log su File: infoIntegration

Registrazione Messaggi

Stato: abilitato

Configurazione

Invia **Cancella**

Fig. 8.7: Configurazione del servizio di tracciamento

- *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.

8.3 Controllo del Traffico

Accedendo la sezione *Configurazione > Controllo del Traffico* si possono impostare i parametri di configurazione relativamente alla funzionalità 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.

La configurazione della funzionalità di controllo del traffico (Fig. 8.8) 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 congestimento 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.

Controllo del Traffico

Note: (*) Campi obbligatori

Limitazione Numero di Richieste Complessive

Stato: abilitato

Max Richieste Simultanee *: 200

[Visualizza Informazioni Runtime](#)

Controllo della Congestione

Stato: disabilitato

Rate Limiting

[Registro Policy \(6\)](#)
[Policy Globali \(0\)](#)

Tempi Risposta

Fruizioni

Connection Timeout *: 10000
Indicazione in millisecondi (ms)

Read Timeout *: 150000
Indicazione in millisecondi (ms)

Tempo Medio di Risposta *: 10000
Indicazione in millisecondi (ms)

Erogazioni

Connection Timeout *: 10000
Indicazione in millisecondi (ms)

Read Timeout *: 120000
Indicazione in millisecondi (ms)

Tempo Medio di Risposta *: 10000
Indicazione in millisecondi (ms)

SALVA

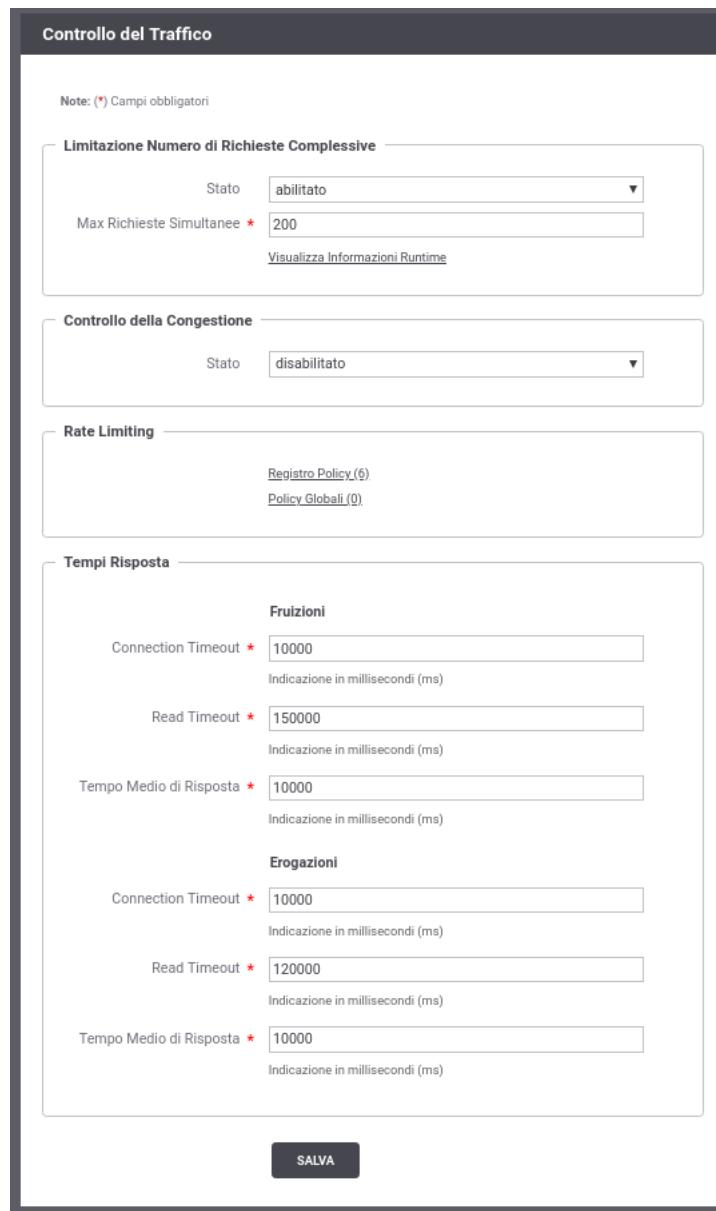


Fig. 8.8: Maschera per l'impostazione dei parametri di controllo del traffico

8.3.1 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 la sezione [Tracciamento](#).

- *Tipo Errore per API SOAP* e *Includi Descrizione Errore* (Opzioni presenti solo con console in modalità avanzata): 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 (Fig. 8.9) 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 congestimento, 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.
-

8.3.2 Controllo della Congestione

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



Fig. 8.9: Dati di congestimento in tempo reale

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

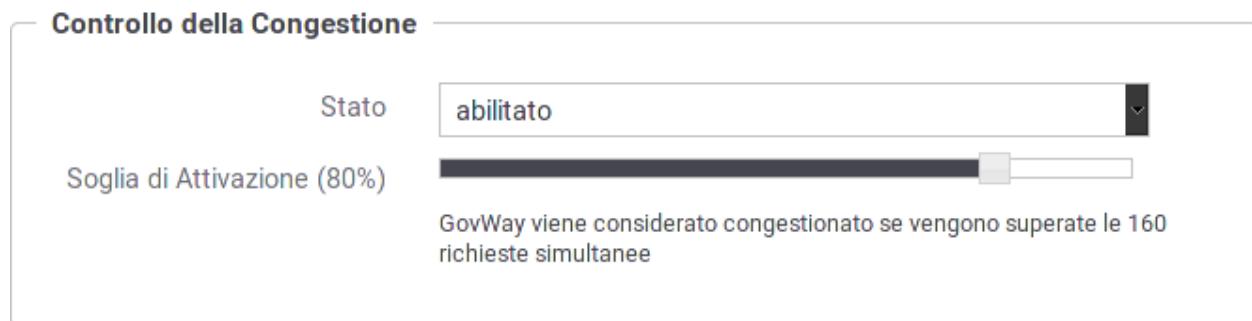


Fig. 8.10: Configurazione della soglia di congestimento

8.3.3 Rate Limiting

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

- *Tipo Errore per API SOAP e Includi Descrizione Errore* (Opzioni presenti solo con console in modalità avanzata): 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 *Registro Policy*.
- *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 *Policy Globali*.

8.3.4 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.

8.4 Rate Limiting

Questa sezione descrive come creare e attivare le policy di controllo del traffico:

- *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 [Registro Policy](#).
- *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. Questa funzionalità è descritta nella sezione [Policy Globali](#).

8.4.1 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 ([Fig. 8.11](#)).

Tramite il pulsante “Aggiungi” è possibile aprire la pagina di creazione di una policy di Rate Limiting ([Fig. 8.12](#)).

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 presenti 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.

Controllo del Traffico > Registro Policy

Registro Policy

Tipo: Built-in

Ricerca:

FILTRA RIPULISCI

Visualizzati record [1-20] su 100

	Nome	Tipo
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeGiornaliero	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeGiornaliero-Congestione	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeGiornaliero-Congestione-Degrado	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeGiornaliero-Degrado	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeMinuti	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeMinuti-Congestione	Built-in
<input type="checkbox"/>	_built-in_NumerofaultApplicativi-ControlloRealtimeMinuti-Congestione-Degrado	Built-in

Fig. 8.11: Elenco delle Policy di Rate Limiting presenti nel registro

Controllo del Traffico > Registro Policy > Aggiungi

Note: (*) Campi obbligatori

Policy

Nome * NumeroRichieste-ControlloRealtimeOrario

Descrizione * La policy limita il numero totale massimo di richieste consentite durante l'intervallo di tempo specificato in ore (campionamento real-time, finestra corrente).

Metrica Numero Richieste

Valori di Soglia

Modalità di Controllo Realtime

Num. Massimo Richieste *

Intervallo Osservazione

Frequenza Orario

Ore *

Finestra Corrente

Applicabilità

Condizionale

SALVA

Fig. 8.12: Maschera per la creazione di una policy di Rate Limiting

– *Metrica*: Si seleziona la metrica che la policy deve monitorare al fine di attuare le eventuali restrizioni. Sono disponibili le seguenti risorse:

- * *NumerRichieste*: 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:

- *Modalità di Controllo*
- *Numero Massimo di Richieste*
- *Frequenza Intervallo Osservazione*
- *Intervallo Osservazione*
- *Finestra Osservazione*

- * *NumerRichiesteSimultanee*: La policy effettua il controllo sul numero di richieste simultanee gestite. Selezionando questa metrica si attiveranno i seguenti elementi per la configurazione dei valori di soglia:

- *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*

- * *TempoComplessivRisposta*: La policy controlla la quantità di tempo complessivamente impiegata dal gateway per la ricezione delle risposte dai servizi invocati. Selezionando questa metrica 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 metrica 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*
- * *NumerRichiesteCompletateConSuccesso*
NumerRichiesteFallite
NumerFaultApplicativi

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 metrica 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 “NumerRichieste”. 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. Inoltre tale modalità richiede il tracciamento delle transazioni sulle quali viene poi calcolata la statistica (vedi sezione *Tracciamento*). 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 metrica “NumerRichieste”. 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 metrica “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 metrica “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 metriche “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 metrica “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 metrica “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» 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 Fig. 8.13 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.

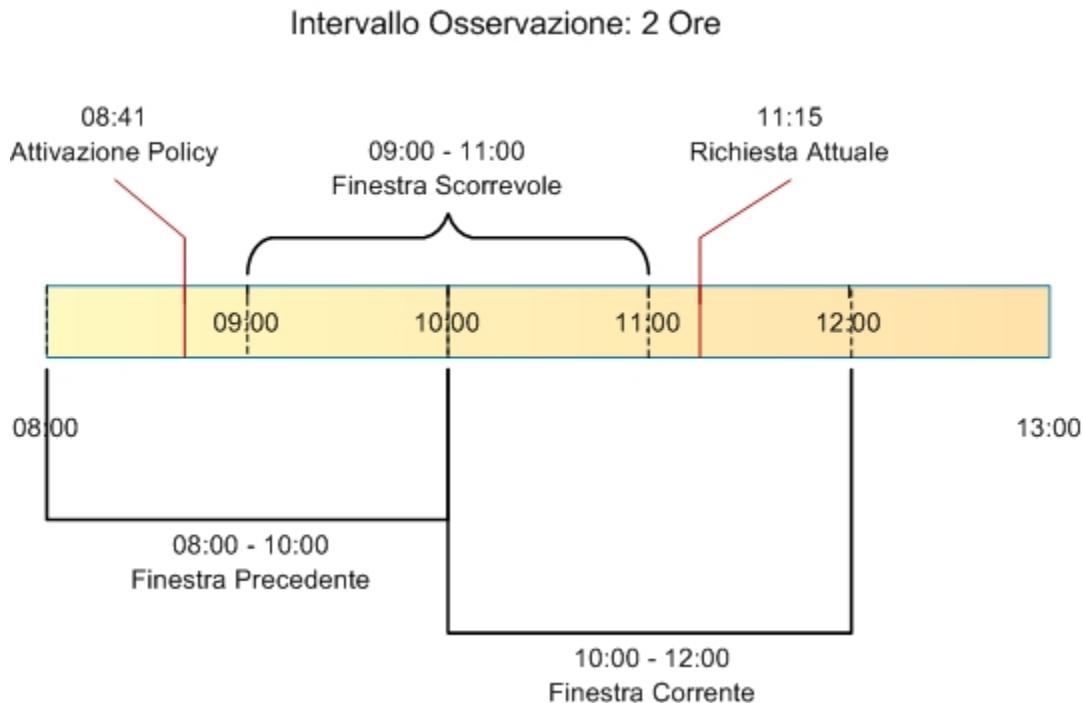


Fig. 8.13: Finestre di osservazione su un campionamento di 2 ore

- *Applicabilità*: Questa sezione della policy consente di restringere l'applicabilità della policy sulla base di alcuni criteri (Fig. 8.14). 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 congestimento. 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”.

Applicabilità

Condizionale	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Applicata solo in presenza di Congestione del Traffico i	
<input checked="" type="checkbox"/> Applicata solo in presenza di Degrado Prestazionale i	

Degrado Prestazionale

Modalità di Controllo	<input type="text" value="Realtime"/>
Tempo Medio Risposta	<input type="text" value="Latenza Servizio"/>
Intervallo Osservazione	
Frequenza	<input type="text" value="Orario"/>
Ore *	<input type="text"/>
Finestra	<input type="text" value="Precedente"/>

Fig. 8.14: 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.

8.4.2 Policy Globali

Questa sezione consente di definire le policy di rate limiting che hanno un raggio d'azione che supera la singola erogazione/fruizione ed effettua quindi valutazioni su un campo più ampio.

L'attivazione di una Policy Globale segue in prevalenza il medesimo criterio già descritto nella sezione *Registrazione di una policy* riguardo il caso della configurazione di una singola erogazione/fruizione. Vi sono però alcune differenze che riguardano i criteri di raggruppamento, per il calcolo dei valori di soglia, e i criteri di filtro per l'applicabilità della policy.

Raggruppamento

Come descritto nella sezione *Registrazione di una policy* è possibile definire dei criteri di raggruppamento che consentono di verificare i valori di soglia. La logica è del tutto analoga a quella dell'operatore GROUP BY del linguaggio SQL.

I criteri di raggruppamento, per una policy a livello globale, sono maggiori rispetto a quelli descritti in precedenza (Fig. 8.15):

- *Fruizione/Erogazione*
- *Soggetto Erogatore*
- *API*
- *Azione/Risorsa*
- *Soggetto Fruitore*
- *Applicativo Fruitore*
- *Token*
- *Raggruppamento per Chiave*

Valori di Soglia

Ridefinisci Valori di Soglia

Num. Massimo Richieste 100

Raggruppamento

Se abilitato, il calcolo del valore della soglia avviene raggruppando le richieste in funzione dei criteri selezionati

Stato	abilitato
-------	-----------

Fruizione / Erogazione

Soggetto Erogatore

API

Soggetto Fruitore

Applicativo Fruitore

Token

Chiave

Fig. 8.15: Definizione criteri di raggruppamento per la policy di rate limiting

Filtro

Abilitando questa sezione è possibile indicare i criteri affinché la policy sia applicabile in base alle caratteristiche di ciascuna richiesta in ingresso. In assenza di filtro, la policy sarà valutata su tutte le richieste in ingresso che riguardano l'erogazione/fruizione che si sta configurando. I criteri di filtro, per una policy a livello globale, sono maggiori rispetto a quelli descritti in precedenza nella sezione [Registrazione di una policy](#) (Fig. 8.16):

- *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.
- *Profilo*: Opzione per filtrare le richieste di servizio in base al profilo di utilizzo del Gateway. Nel caso si sia selezionata un singolo profilo (o se il gateway ne supporta uno solo) 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.
- *API*: Opzione per filtrare le richieste in base alla API invocata. Tramite la lista è possibile selezionare una tra le API censite nel registro. Se è stato selezionato un soggetto erogatore, saranno elencati solo le API da esso erogate. Analogamente, se è stato selezionato un profilo, saranno elencate solo API relative a tale profilo.
- *Azione/Risorsa*: Opzione per filtrare le richieste di servizio in base all'azione/risorsa invocata. Tramite la lista è possibile selezionare una tra le azioni/risorse censite nel registro. Se è stato selezionato una API, saranno elencati solo le azioni ad essa appartenenti.
- *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 in base ad una chiave che può essere specificata in maniera personalizzata. Questa parte è già stata descritta in maniera approfondita nella sezione [Registrazione di una policy](#).

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

8.4.3 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” (Fig. 8.17).

Filtro

Stato	abilitato
Tipologia	Qualsiasi
Profilo	API Gateway
Ruolo Erogatore	Qualsiasi
Soggetto Erogatore	Qualsiasi
API	Qualsiasi
Ruolo Richiedente	Qualsiasi
Soggetto Fruitore	Qualsiasi
Chiave	<input type="checkbox"/>

Fig. 8.16: Definizione del filtro per l'istanza della 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 Collezione 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).

8.4.4 Filtro o Raggruppamento Personalizzato

Nella sezione *Registrazione di una policy* è possibile utilizzare dei criteri di raggruppamento per il valore di soglia o un filtro di applicabilità personalizzato in modo da definire un comportamento specifico per le proprie esigenze di servizio. Una configurazione personalizzata richiede la realizzazione di un plugin che contiene la logica di filtro e/o il raggruppamento personalizzato; il plugin consiste nell'implementazione di una classe java che implementa l'interfaccia:

The screenshot shows a web-based management interface for PdD OpenSPCoop Enterprise. The top navigation bar indicates the path: Configurazione > Controllo del Traffico - Policy > OccupazioneBanda-ControlloRealtimeOrario. The main content area is divided into two sections: "Informazioni Runtime" and "PdD OpenSPCoop Enterprise". The "Informazioni Runtime" section contains a "Refresh" button. The "PdD OpenSPCoop Enterprise" section is titled "Reset Contatori" and displays runtime statistics for a specific policy. The statistics include:

```
=====
Criterio di Collezione dei Dati
  Disabilitato
Dati Generali
  Richieste Attive: 0
  Data Attivazione Policy: 2017-08-09_15:26:26.223
Dati collezionati per la risorsa 'OccupazioneBanda'
  Modalità di Controllo: realtime
  Finestra Osservazione: corrente
  Intervallo [2017-08-09_15:00:00.000 - 2017-08-09_15:59:59.999]
  Numero Richieste Accettate: 2
  Contatore: 6 kb (6869 bytes)
  Valore Medio: 3 kb (3434 bytes)
  Numero Richieste Bloccate: 0
=====
```

Fig. 8.17: Dati statistici relativi ad una policy di rate limiting

```
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 deve essere successivamente registrata tramite una entry da aggiungere all'interno del file (da creare se non esiste) `/etc/govway/govway_local.classRegistry.properties` di GovWay:

```
org.openspcoop2.pdd.controlloTrafico.rateLimiting.<tipo>=<fully qualified_
↪class name>
```

La stringa `<tipo>` diventa utilizzabile come “Tipo Personalizzato” da indicare in fase di configurazione per un criterio di filtro personalizzato (Fig. 8.18) e/o per un criterio di raggruppamento personalizzato (Fig. 8.19).

Filtro per Chiave	
Stato	<input checked="" type="checkbox"/>
Tipologia	PluginBased
Tipo Personalizzato *	
Valore *	

Fig. 8.18: Filtro Personalizzato

Raggruppamento per Chiave	
Stato	<input checked="" type="checkbox"/>
Tipologia	PluginBased
Tipo Personalizzato *	

Fig. 8.19: Raggruppamento Personalizzato

8.5 Token Policy

Per poter definire politiche di controllo degli accessi basate sui Bearer Token o per poterne spedire uno verso l'endpoint associato ad un connettore 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 Fig. 8.22.

The screenshot shows a web-based configuration interface for creating a new Token Policy. At the top, it says "Token Policy > Aggiungi". Below that, a note states "Note: (*) Campi obbligatori". The main section is titled "Token Policy" and contains three fields: "Tipo" (with a red asterisk indicating it's required) which has a dropdown menu showing a single option "-"; "Nome" (with a red asterisk) which is currently empty; and "Descrizione" which is also empty. At the bottom of the form is a large "SALVA" button.

Fig. 8.20: Creazione di una Token Policy

Inizialmente si inseriscono i dati identificativi:

- *Nome*: nome univoco da assegnare alla policy
- *Tipo*: determina il tipo di policy:
 - *Validazione*: definisce una policy utilizzabile per validare Bearer Token nel Controllo degli Accessi (*Autenticazione Token*)
 - *Negoziazione*: definisce i criteri per la negoziazione di un Bearer Token poi utilizzato sui connettori nei quali sarà associata la policy (*Autenticazione Token*)
- *Descrizione*: testo di descrizione generale della policy

I parametri richiesti differiscono a seconda del tipo selezionato. Le sezioni successive dettagliano i due tipi supportati.

8.5.1 Token Negoziazione Policy

Per poter definire politiche che consentono di spedire un Bearer Token verso l'endpoint associato ad un connettore 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 Fig. 8.22.

Inizialmente si inseriscono i dati identificativi:

- *Nome*: nome univoco da assegnare alla policy

Token Policy

Tipo *	Negoziazione
Nome *	
Descrizione	

Token Endpoint

Tipo	Client Credentials
URL *	http://
Connection Timeout *	10000
Read Timeout *	120000
Https	<input type="checkbox"/>
Proxy	<input type="checkbox"/>

Autenticazione Client

Basic	<input type="checkbox"/>
Bearer	<input type="checkbox"/>
Https	<input type="checkbox"/>

Configurazione

Scope	
Elencare più scope separandoli con la virgola	
Audience	

Token Forward

Modalità	RFC 6750 - Bearer Token Usage (Authorization Request ▾)
----------	---

Fig. 8.21: Informazioni generali di una Token Policy

- *Tipo*: deve essere selezionato il tipo *Negoziazione*
- *Descrizione*: testo di descrizione generale della policy

Al passo successivo si inseriscono le Informazioni Generali. Nella sezione *Token Endpoint* si specifica il tipo di negoziazione e i vari parametri necessari:

- *Tipo*: indica la modalità di negoziazione del token. I valori possibili sono:
 - *Client Credentials*: modalità di negoziazione “Client Credentials Grant” descritta nel RFC 6749 (<https://tools.ietf.org/html/rfc6749#page-40>).
 - *Resource Owner Password Credentials*: modalità di negoziazione “Resource Owner Password Credentials Grant” descritta nel RFC 6749 (<https://tools.ietf.org/html/rfc6749#page-37>).
- *URL*: endpoint del servizio di negoziazione token.
- *Connection Timeout*: Tempo massimo in millisecondi di attesa per stabilire una connessione con il server di negoziazione token.
- *Read Timeout*: Tempo massimo in millisecondi di attesa per la ricezione di una risposta dal server di negoziazione token.
- *Https*: Parametri di configurazione nel caso in cui il server di negoziazione token richieda un accesso Https.
- *Proxy*: Parametri di configurazione nel caso in cui il server di negoziazione token richieda l’uso di un proxy per l’accesso.

Successivamente devono essere forniti i dati di configurazione specifici dell’autenticazione utente, se il tipo di negoziazione selezionato è “Resource Owner Password Credentials”:

- *Username* e *Password*: Dovranno essere forniti Username e Password dell’utente per cui verrà effettuata la negoziazione del token.

Successivamente devono essere forniti i dati di configurazione specifici dell’autenticazione client:

- *Autenticazione Http Basic*: flag da attivare nel caso in cui il servizio di negoziazione richieda autenticazione di tipo HTTP-BASIC. In questo caso dovranno essere forniti Client-ID e Client-Secret nei campi successivi.
- *Autenticazione Bearer*: flag da attivare nel caso in cui il servizio di negoziazione richieda autenticazione tramite un bearer token. Quest’ultimo dovrà essere indicato nel campo seguente.
- *Autenticazione Https*: flag da attivare nel caso in cui il servizio di negoziazione richieda autenticazione di tipo Https. In questo caso dovranno essere forniti tutti i dati di configurazione nei campi seguenti.

Nella sezione “Configurazione” potranno invece essere definiti ulteriori criteri che riguardano la richiesta di un token:

- *Scope*: Elenco di scope utente richiesti.
- *Audience*: Audience per il quale si vorrebbe ottenere il token.

Infine nella sezione “Token Forward” si può configurare la modalità di inoltro del token verso l’endpoint del connettore a cui verrà associata la policy che stiamo definendo:

- *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.

8.5.2 Token Validazione 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 Fig. 8.22.

The screenshot shows the 'Token Policy > Aggiungi' creation form. At the top, a note says 'Note: (*) Campi obbligatori'. The 'Token Policy' section contains fields for 'Nome' (Name) and 'Descrizione' (Description). Below this is the 'Informazioni Generali' (General Information) section, which is expanded to show the 'Token' and 'Elaborazione Token' (Token Processing) sub-sections. In the 'Token' sub-section, 'Posizione' (Position) is set to 'RFC 6750 - Bearer Token Usage' and 'Tipo' (Type) is set to 'Opaco'. In the 'Elaborazione Token' sub-section, three checkboxes are present: 'Token Introspection', 'OIDC - UserInfo', and 'Token Forward', all of which are unchecked. At the bottom of the form are two buttons: 'Invia' (Send) and 'Cancella' (Cancel).

Fig. 8.22: Informazioni generali di una Token Policy

Inizialmente si inseriscono i dati identificativi:

- *Nome*: nome univoco da assegnare alla policy
- *Tipo*: deve essere selezionato il tipo *Validazione*
- *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.

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 ([Fig. 8.23](#)).

Validazione JWT

Claims Parser *

KeyStore

Tipo *

File *

Password *

Alias Chiave Privata *

Password Chiave Privata *

Fig. 8.23: 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.

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 (Fig. 8.24).

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.

Endpoint Token

Connection Timeout *

Read Timeout *

Https

Proxy

Token Introspection

Tipo *

URL *

Autenticazione Http Basic

Autenticazione Bearer

AutenticazioneHttps

Fig. 8.24: Dati di puntamento al servizio di Token Instrospection

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.
 - * *AutenticazioneHttps*: 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 (Fig. 8.5.2).

Configurazione personalizzata del servizio di Token Instrospection

I dati da fornire sono:

- *URL*: la URL del servizio di introspection.

Token Introspection

Tipo *	Personalizzato
URL *	http://
Http Method *	GET
Posizione Token *	Parametro URL
Nome Parametro URL *	
Claims Parser *	Personalizzato
ClassName *	
Autenticazione Http Basic	<input type="checkbox"/>
Autenticazione Bearer	<input type="checkbox"/>
AutenticazioneHttps	<input type="checkbox"/>

- *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.

OIDC - UserInfo

Sezione per attivare la richiesta al servizio di UserInfo per ottenere i dati inerenti l'utente possessore del token ricevuto (Fig. 8.25).

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.

Endpoint Token

- Connection Timeout * [Up/Down]
- Read Timeout * [Up/Down]
- Https
- Proxy

OIDC - UserInfo

- Tipo * [Down]
- URL * [Up/Down]
- Autenticazione Http
- Autenticazione Bearer
- AutenticazioneHttps

Fig. 8.25: Dati di puntamento al servizio di UserInfo

- *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.

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": {
                "name": {"type": "string"},
```

```

    "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.
-

8.6 Tags

La sezione *Configurazione > Tags* è dedicata alla gestione dei tags che possono essere utilizzati per la classificazione delle API presenti nel registro.

I tags possono essere creati direttamente durante la registrazione di una API, oppure da questa sezione in maniera più sistematica e assegnando loro un tipo, Soap o Rest, che indica l'ambito di utilizzo del tag stesso.

La sezione mostra l'elenco dei tags disponibili ([Fig. 8.26](#)).

L'elenco dei tag può essere filtrato impostando, nella barra dei filtri a comparsa, un pattern per il nome o un tipo. Oltre ad aggiungere ed eliminare i tag esistenti è possibile esportarli in blocco.

Col pulsante *Aggiungi* si apre il form per creare un nuovo tag ([Fig. 8.27](#)).

Per creare un tag si inseriscono i seguenti dati:

- *Nome*: il nome del tag
- *Descrizione*: descrizione del tag
- *Tipo*: serve per indicare per quali API è possibile utilizzare il tag: SOAP, REST o Qualsiasi.

Tags		
◀ Visualizzati record [1-8] su 8 ▶		
	Nome	Tipo
<input type="checkbox"/>	altroTag	Qualsiasi
<input type="checkbox"/>	Anagrafica	Qualsiasi
<input type="checkbox"/>	PagamentiTelematici	Qualsiasi
<input type="checkbox"/>	PagamentiTelematiciREST	Rest
<input type="checkbox"/>	PagamentiTelematiciSOAP	Soap
<input type="checkbox"/>	tagTest	Qualsiasi
<input type="checkbox"/>	tagTest1	Qualsiasi
<input type="checkbox"/>	tagTest2	Qualsiasi

ESPORTA **ELIMINA** **AGGIUNGI**

Fig. 8.26: Elenco dei tags

Note: (*) Campi obbligatori

Tag

Nome *	<input type="text"/>
Descrizione	<input type="text"/>
Tipo	Qualsiasi

SALVA

Fig. 8.27: Creazione di un tag

8.7 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:

- *Registro*
 - *Gestione API [S]* - Gestione delle entità di configurazione dei servizi, quali: API, Erogazioni, Fruizioni, ecc.
- *GovWay Monitor*
 - *Monitoraggio [D]* - Accesso alle funzionalità di monitoraggio della console govwayMonitor.
 - *Reportistica [R]* - Accesso alle funzionalità di reportistica della console govwayMonitor.
- *Strumenti*
 - *Auditing [A]* - Accesso alle funzionalità di consultazione delle tracce del servizio di Auditing.
- *Configurazione*
 - *[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.

- [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.
- *Altri Permessi (visibili solo configurazione specifica del prodotto)*
 - [P] - Gestione delle entità di configurazione degli Accordi di Cooperazione e Servizi Composti.
 - [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.

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 Fig. 8.28.

Le informazioni da inserire sono:

- *Informazioni Utente*
 - *Nome*
- *Permessi di Gestione*: sezione che consente di assegnare i permessi all'utente e quindi decidere quali funzionalità rendergli accessibili.
- *Profilo di Interoperabilità*: sezione che consente di decidere quali, tra i profili disponibili, rendere accessibili all'utente.
- *Visibilità dati tramite govwayMonitor*: questa sezione è visibile solo se è stato abilitato uno dei permessi «GovWay Monitor». In questo contesto è possibile stabilire la visibilità dell'utente sulla console GovWay Monitor riguardo i seguenti:
 - *Soggetti*: opzione visibile solo se attiva la modalità multi-tenant, consente di limitare la visibilità delle entità di monitoraggio ai soli soggetti interni indicati in una whitelist. Per configurare la whitelist è necessario salvare l'utente da creare e successivamente accedere in editing. In alternativa è possibile attivare il flag «Tutti» per non assegnare limitazioni.
 - *API*: consente di limitare la visibilità delle entità di monitoraggio alle sole API indicate in una whitelist. Per configurare la whitelist è necessario salvare l'utente da creare e successivamente accedere in editing. In alternativa è possibile attivare il flag «Tutti» per non assegnare limitazioni.
- *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 (Fig. 8.29)

8.8 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 Fig. 8.30. I passi da eseguire sono i seguenti:

- Selezionare la modalità cui fanno riferimento le entità contenute nell'archivio da importare.

Utenti > Aggiungi

Note: (*) Campi obbligatori

Informazioni Utente

Nome *

Permessi di Gestione

Registro

Gestione API [S]

GovWay Monitor

Monitoraggio [D]

Reportistica [R]

Strumenti

Auditing [A]

Configurazione

Configurazione Generale [C]

Utenti [U]

Profilo di Interoperabilità

API Gateway

SPCoop

eDelivery

Fatturazione Elettronica

Modalità Interfaccia

Tipo

Password

Password *

Conferma Password *

La password deve rispettare i seguenti vincoli:
 - non deve contenere il nome di login dell'utente
 - deve essere composta almeno da 8 caratteri
 - deve contenere almeno una lettera minuscola (a - z)
 - deve contenere almeno una lettera maiuscola (A - Z)
 - deve contenere almeno un numero (0 - 9)
 - deve contenere almeno un carattere non alfano numerico (ad esempio, !, \$, #, %, @)

SALVA

Fig. 8.28: Creazione nuovo utente

Utenti						
		Profilo Utente	Modalità Interfaccia	Profilo	Permessi di Gestione	Cambia identità
<input type="checkbox"/>	<input checked="" type="checkbox"/>	amministratore	avanzata	Tutti	S,C,M,A,U	Accedi
<input type="checkbox"/>	<input checked="" type="checkbox"/>	config	standard	API Gateway	C	Accedi
<input type="checkbox"/>	<input checked="" type="checkbox"/>	giuseppe	standard	Tutti	S,D,R,C,A,U	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	operatore	standard	Tutti	D,R	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	operatore2	standard	API Gateway	D,R	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	test	standard	SPCoop, API Gateway	S,C	Accedi

Fig. 8.29: Lista degli utenti

- 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.

8.9 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* (Fig. 8.31).

Dopo aver selezionato il pulsante «Esporta», una seconda maschera (Fig. 8.32) 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.

Importa

Importa

Tipologia archivio: govlet

Aggiornamento:

File: No file selected.

IMPORTA

Fig. 8.30: Importazione di entità nel registro

Erogazioni

Visualizzati record [1-4] su 4

	Servizio
<input type="checkbox"/>	EsempioRest:1 API Rest: EsempioRest:1, Profilo Interoperabilità: API Gateway
<input checked="" type="checkbox"/>	RicezioneFatture:1 API Soap: RicezioneFatture:1, Profilo Interoperabilità: Fatturazione Elettronica
<input checked="" type="checkbox"/>	Sincrono API Soap: EsempioASParteComune:1 (ENTE), Profilo Interoperabilità: SPCoop
<input type="checkbox"/>	TrasmissioneFatture:1 API Soap: TrasmissioneFatture:1, Profilo Interoperabilità: Fatturazione Elettronica

ESPORTA **ELIMINA** **AGGIUNGI**

Fig. 8.31: Esportazione di singole entità del registro

- *Includi elementi riferiti*: include nell’archivio di esportazione anche gli elementi di configurazione riferiti da quelli selezionati.

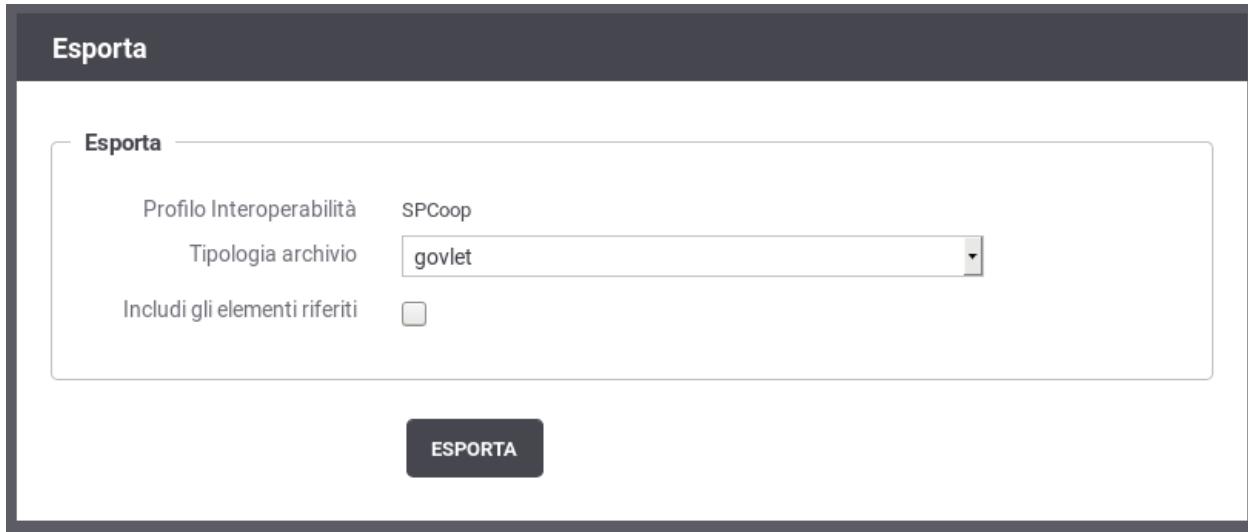


Fig. 8.32: Esportazione di entità nel registro: parametri

- Tramite la voce di menu *Configurazione > Esporta* che presenta le opzioni mostrate in Fig. 8.33.

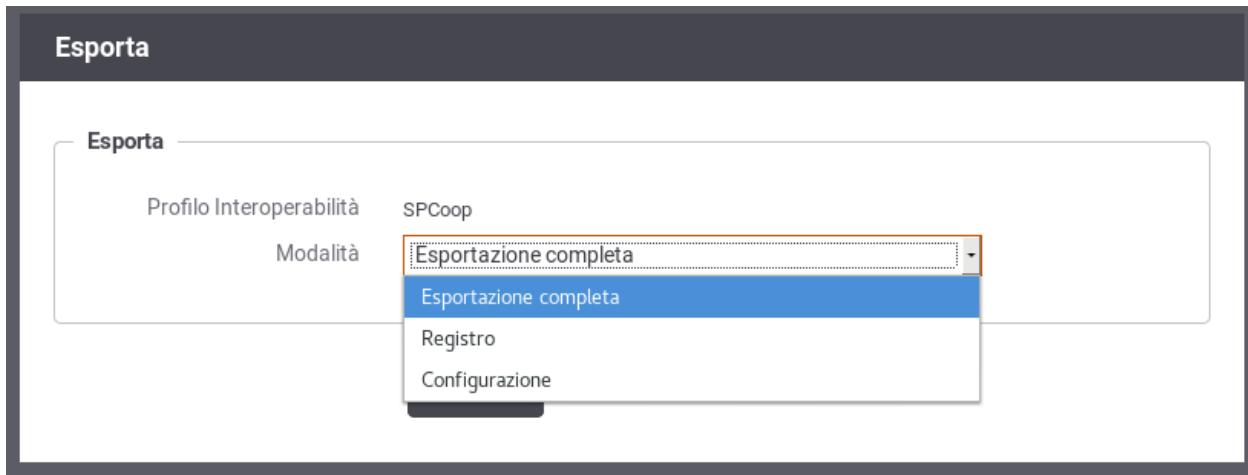


Fig. 8.33: Esportazione di entità nel registro

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.

8.10 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 [Utenti](#)) 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 Fig. 8.34 il servizio di auditing è disabilitato e quindi nessun dato verrà tracciato.

Fig. 8.34: Servizio di auditing disabilitato

Modificando lo *Stato* del servizio di auditing in **Abilitato** appariranno ulteriori campi nel form (vedi Fig. 8.35) per effettuare le impostazioni.

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 Fig. 8.35 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.

Configurazione > **Auditing**

Auditing

Stato audit: abilitato

Comportamento di Default

Audit: abilitato

Dump: disabilitato

Formato dump: JSON

Log4j Auditing: abilitato

Filtri

visualizza(0)

Invia **Cancella**

The screenshot shows the 'Auditing' configuration page. At the top, there's a breadcrumb navigation: 'Configurazione > Auditing'. The main area is divided into sections: 'Auditing' (with a dropdown menu set to 'abilitato'), 'Comportamento di Default' (with dropdowns for 'Audit' (abilitato), 'Dump' (disabilitato), 'Formato dump' (JSON), and 'Log4j Auditing' (abilitato)), and 'Filtri' (with a button 'visualizza(0)'). At the bottom, there are two buttons: 'Invia' and 'Cancella'.

Fig. 8.35: Servizio di auditing abilitato

- **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 Fig. 8.36 è mostrata la maschera per la creazione di un nuovo filtro di auditing.

Fig. 8.36: Creazione di un filtro per il servizio di auditing

Facendo riferimento alla Fig. 8.36 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 tracerà 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.

Funzionalità Avanzate

9.1 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) come mostrato nella figura Fig. 9.1.

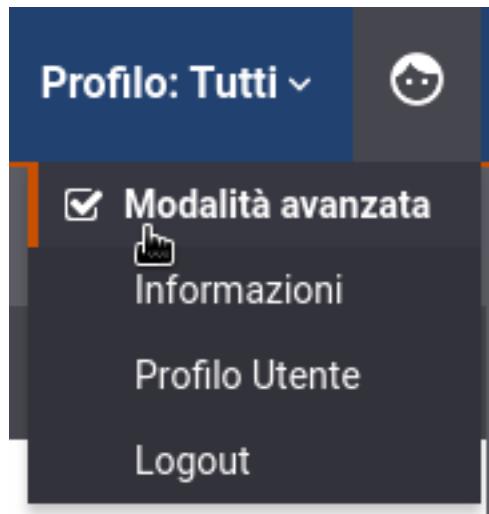


Fig. 9.1: Selezione Modalità Avanzata

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: Non tutte le funzionalità disponibili in modalità avanzata sono descritte nel presente manuale.

9.2 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.

API > Servizi di Hello:1 > Aggiungi

Note: (*) Campi obbligatori

Servizio

Nome *

Descrizione

Informazioni Protocollo

Profilo di collaborazione

ID Collaborazione

Riferimento ID Richiesta

Invia Cancella

Fig. 9.2: 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.

The screenshot shows a web-based configuration interface for adding a new action to a service. At the top, the breadcrumb navigation reads: API > Servizi di Hello:1 > Azioni di HelloPortType > Aggiungi. A note at the top left says "Note: (*) Campi obbligatori". The main form has two sections: "Azione" and "Informazioni Protocollo". The "Azione" section contains a field labeled "Nome" with a red asterisk indicating it is required, and a text input field. The "Informazioni Protocollo" section contains a dropdown menu labeled "Profilo" with the option "usa profilo servizio". At the bottom of the form are two buttons: "Invia" (Send) and "Cancella" (Cancel).

Fig. 9.3: 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.

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

API > Risorse di provaRest:1 > Aggiungi

Note: (*) Campi obbligatori

Risorsa

HTTP Method	Qualsiasi
Path	
Nome *	
Descrizione	

Informazioni Protocollo

ID Collaborazione	<input type="checkbox"/>
Riferimento ID Richiesta	<input type="checkbox"/>

Invia **Cancella**

The screenshot shows a user interface for adding a new REST resource. The top navigation bar indicates the path: API > Risorse di provaRest:1 > Aggiungi. A note at the top says "Note: (*) Campi obbligatori". The main area is divided into two sections: "Risorsa" and "Informazioni Protocollo". The "Risorsa" section contains fields for "HTTP Method" (set to "Qualsiasi"), "Path" (empty), "Nome" (marked with a red asterisk), and "Descrizione" (empty). The "Informazioni Protocollo" section contains two checkboxes: "ID Collaborazione" and "Riferimento ID Richiesta". At the bottom are two buttons: "Invia" and "Cancella".

Fig. 9.4: Aggiunta di una risorsa alla API REST

- *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.

9.3 Versionamento delle API e delle Erogazioni/Fruizioni

Su GovWay vi è una gestione del versionamento effettuato su due componenti:

- API
- Erogazione o Fruizione dell'API

Come descritto nella sezione [Versionamento delle API](#), sulla singola erogazione/fruizione è possibile modificare la versione dell'API implementata solamente se ne esiste più di una versione. Questa modifica si riflette automaticamente anche sulla versione dell'erogazione/fruizione, e sull'url di invocazione, se non esiste già una erogazione/fruizione con la nuova versione.

Utilizzando la console in modalità avanzata ([Modalità Avanzata](#)) è invece possibile modificare puntualmente la versione dell'erogazione/fruizione e di conseguenza l'url di invocazione tramite il bottone “modifica” evidenziato nella figura Fig. 9.5.

PetStore@ENTE v2	
Nome	PetStore v2
Soggetto Erogatore	ENTE
API	PetStore v2 (Rest)
URL Invocazione	http://localhost:8080/goway/ENTE/PetStore/v2
Connettore	http://petstore.swagger.io/v2
Gestione CORS	Abilitato

Fig. 9.5: Nuova Versione di una Erogazione

Accedendo alla modifica del nome dell'erogazione/fruizione con la console in modalità avanzata, è possibile modificare la versione (Fig. 9.6).

Effettuata la modifica l'erogazione possiederà una versione indipendente dalla versione dell'API implementata. L'url di invocazione riflette la versione dell'erogazione come evidenziato nella figura Fig. 9.7.

Erogazioni > PetStore@ENTE v2 > Informazioni Generali

Informazioni Generali

Note: (*) Campi obbligatori

Informazioni Generali

Nome *	PetStore
Versione	6
Allegati (0)	

Fig. 9.6: Scelta di una nuova versione per una Erogazione

Erogazioni > PetStore@ENTE v6

PetStore@ENTE v6

Nome	PetStore v6	
Soggetto Erogatore	ENTE	
API	PetStore v2 (Rest)	
<u>URL Invocazione</u>	http://localhost:8080/govway/ENTE/PetStore/v6	
Connettore	http://petstore.swagger.io/v2	
Gestione CORS	Abilitato	

Fig. 9.7: Nuova versione dell'erogazione differente dalla versione dell'API

9.4 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:

- *Contenuto* (Soap e Rest): il dato viene ricavato dal messaggio di richiesta utilizzando come criterio l'espressione XPath o JsonPath indicata nel campo *Pattern* sottostante.
- *Header HTTP* (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.
- *Header di Integrazione* (Soap e Rest): il dato viene ricavato dall'header di integrazione fornito con il messaggio di richiesta. Per conoscere come gli applicativi client forniscono tale informazione vedere la sezione *Scambio di informazioni nella richiesta del client verso il gateway*.
- *Specifiche di Interfaccia dell'API* (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 dell'API.
- *Url di Invocazione* (Soap): il dato viene ricavato dinamicamente dalla url di invocazione utilizzando come criterio l'espressione regolare inserita nel campo *Espressione Regolare* sottostante.
- *SOAPAction* (Soap): Questa opzione consente di ricavare il dato dal campo *SOAPAction* presente nell'header di trasporto delle comunicazioni SOAP.

Attivando il flag *Identificazione tramite API*, in caso di fallimento dell'identificazione dell'azione nella modalità prevista al passo precedente, si tenterà di utilizzare la modalità «*Specifiche di Interfaccia dell'API*» come seconda opzione.

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

9.5 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 nella configurazione generale (sezione *Generale*).

Per gestire la compresenza di più soggetti interni al dominio, per la configurazione di erogazioni e fruizioni, è possibile scegliere quali soggetti interni rendere ammissibili (Fig. 9.8):

- *Fruizioni (Soggetto Erogatore)*
 - *Tutti*: indica che tutti i soggetti interni, censiti nel registro di GovWay, sono selezionabili come soggetto erogatore, in una fruizione.
 - *Escludi Soggetto Fruitore*: indica che tutti i soggetti interni, tranne il soggetto fruitore, sono selezionabili come soggetto erogatore, in una fruizione.
 - *Solo Soggetti Esterni*: indica che il soggetto erogatore di una fruizione deve essere un soggetto esterno.
- *Erogazioni (Soggetti Fruitori)*
 - *Tutti*: indica che tutti i soggetti interni, censiti nel registro di GovWay, sono selezionabili come soggetti fruitori, in una erogazione.
 - *Escludi Soggetto Erogatore*: indica che tutti i soggetti interni, tranne il soggetto erogatore, sono selezionabili come soggetti fruitori, in una erogazione.

- *Solo Soggetti Esterni*: indica che i soggetti fruitori di una erogazione devono essere soggetti esterni.

Multi-Tenant

Stato	abilitato
Fruizioni	
Soggetto Erogatore	<input type="text" value="Solo Soggetti Esterni"/>
Erogazioni	
Soggetti Fruitori	<input type="text" value="Escludi Soggetto Erogatore"/>

Fig. 9.8: Elementi di configurazione della modalità multi-tenant

L’utente che ha l’opzione multi-tenant attiva, visualizza sulla testata un menu a discesa che consente di selezionare l’utente interno al dominio sul quale vuole operare (Fig. 9.9). Se viene selezionato un soggetto dalla lista, l’operatività sulla console risulterà identica alla situazione con un unico soggetto interno. Selezionando l’opzione «Tutti» sarà richiesto nei singoli contesti di specificare il soggetto interno.

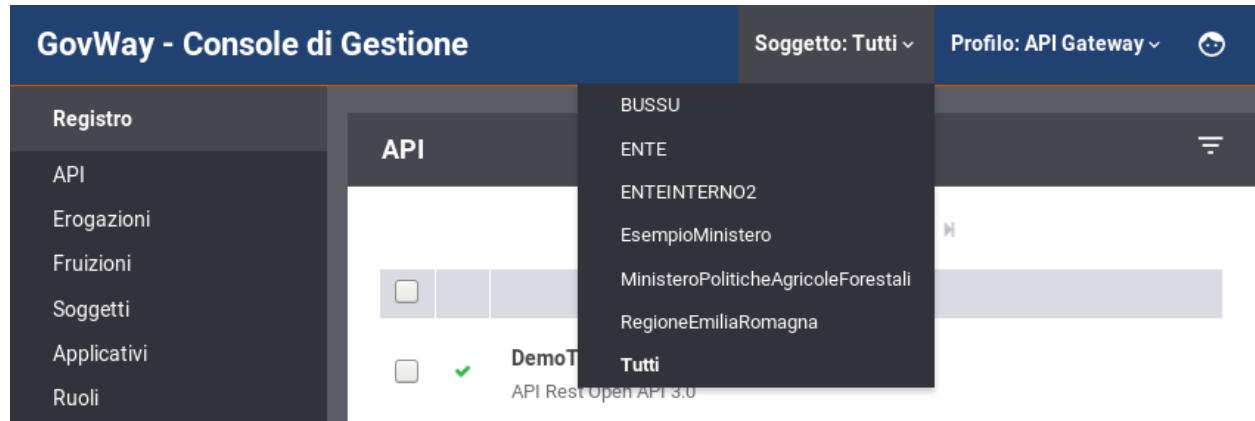


Fig. 9.9: Selezione del soggetto operativo in modalità multi-tenant

9.6 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 degli applicativi server lo scopo è quello di ricevere dal gateway i metadati che riguardano la richiesta gestita.

Per gli applicativi client tale scambio si rende necessario al fine di fornire al gateway specifici parametri necessari a elaborare la richiesta.

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

- *Trasporto*: le informazioni sono contenute nell'header di trasporto
- *Url Based*: le informazioni sono incapsulate nella url
- *SOAP*: le informazioni sono incluse in uno specifico header SOAP proprietario di GovWay
- *WS-Addressing*: le informazioni sono incluse in un header SOAP secondo il formato standard WS-Addressing

Nel seguito descriviamo le strutture degli header di integrazione attive per default con l'installazione del prodotto. Tali strutture variano in funzione del ruolo dell'applicativo. Per l'applicativo client è possibile fornire informazioni al gateway tramite le modalità *Trasporto* e *Url Based*. L'applicativo server, invece, riceve le informazioni dal gateway solamente tramite la modalità *Trasporto*.

9.6.1 Scambio di informazioni nella richiesta inoltrata dal gateway al server

Le informazioni fornite dal gateway all'applicativo erogatore, sia per quanto concerne fruizioni che per erogazioni, sono riassunte nella [Tabella 9.1](#).

Tabella 9.1: Scambio di informazioni nella richiesta inoltrata dal gateway al server

Nome Header Trasporto	Descrizione
GovWay-Message-ID	Identificativo del messaggio assegnato da GovWay
GovWay-Relates-To	Identificativo del messaggio riferito
GovWay-Conversation-ID	Identificativo della conversazione
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

Inoltre, solamente per quanto concerne le erogazioni, all'applicativo interno al dominio vengono inoltrate ulteriori meta-informationi riguardanti la transazione gestita sul gateway descritte nella [Tabella 9.2](#).

Tabella 9.2: Scambio di informazioni nella richiesta inoltrata dal gateway al server per una Erogazione

Header	Descrizione
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-Application-Message-ID	Identificativo del messaggio assegnato dall'applicativo
GovWay-Application	Identificativo dell'applicativo

9.6.2 Scambio di informazioni tra gateway e la risposta ritornata al client

Le informazioni fornite dal gateway all'applicativo fruitore, sia per quanto concerne fruizioni che per erogazioni, sono riassunte nella [Tabella 9.3](#).

Tabella 9.3: Scambio di informazioni tra gateway e la risposta ritornata al client

Nome Header Trasporto	Descrizione
GovWay-Message-ID	Identificativo del messaggio assegnato da GovWay
GovWay-Relates-To	Identificativo del messaggio riferito
GovWay-Conversation-ID	Identificativo della conversazione
GovWay-Application-Message-ID	Identificativo del messaggio assegnato dall'applicativo (solo nel caso di Fruizione)
GovWay-Transaction-ID	Identificativo della transazione assegnato da GovWay

All'applicativo client vengono inoltre forniti ulteriori header http generati se l'applicativo erogatore non è disponibile o se sono stati attivati meccanismi di Rate Limiting (sezione [Rate Limiting](#)).

Tabella 9.4: Scambio di informazioni tra gateway e la risposta ritornata al client

Nome Header Trasporto	Descrizione	Motivazione
Retry-After	Indica al client il numero di secondi dopo i quali ripresentarsi poichè il servizio contattato non è al momento disponibile.	Le principali cause della generazione di tale header sono imputabili alla non raggiungibilità un applicativo erogatore, alla violazione di politiche di RateLimiting o a quando un servizio è temporaneamente disabilitato
X-RateLimit-Limit	Indica il numero massimo di richieste effettuabili	Rate-Limiting attivato con policy di tipo "NumeroRichieste-ControlloRealtime*" (sezione Rate Limiting)
X-RateLimit-Remaining	Numero di richieste rimanenti prima del prossimo reset	Rate-Limiting attivato con policy di tipo "NumeroRichieste-ControlloRealtime*" (sezione Rate Limiting)
X-RateLimit-Reset	Numero di secondi mancante al prossimo reset	Rate-Limiting attivato con policy di tipo "NumeroRichieste-ControlloRealtime*" (sezione Rate Limiting)
GovWay-RateLimit-ConcurrentRequest-Limit	Indica il numero massimo di richieste concorrenti inviabili	Rate-Limiting attivato con policy di tipo "NumeroRichieste-RichiesteSimultanee" (sezione Rate Limiting)
GovWay-RateLimit-ConcurrentRequest-Remaining	Indica il numero massimo di richieste concorrenti ancora inviabili	Rate-Limiting attivato con policy di tipo "NumeroRichieste-RichiesteSimultanee" (sezione Rate Limiting)
GovWay-RateLimit-BandwidthQuota-Limit	Indica la massima banda occupabile	Rate-Limiting attivato con policy di tipo "OccupazioneBanda-*" (sezione Rate Limiting)
GovWay-RateLimit-BandwidthQuota-Remaining	Indica la banda ancora occupabile prima del prossimo reset	Rate-Limiting attivato con policy di tipo "OccupazioneBanda-*" (sezione Rate Limiting)
GovWay-RateLimit-BandwidthQuota-Reset	Numero di secondi mancante al prossimo reset	Rate-Limiting attivato con policy di tipo "OccupazioneBanda-*" (sezione Rate Limiting)
GovWay-RateLimit-AvgTimeResponse-Limit	Tempo medio di risposta atteso	Rate-Limiting attivato con policy di tipo "TempoMedioRisposta-*" (sezione Rate Limiting)

Continued on next page

Tabella 9.4 – continued from previous page

Nome Header Trasporto	Descrizione	Motivazione
GovWay-RateLimit-AvgTimeResponse-Reset	Numero di secondi mancante al prossimo reset	Rate-Limiting attivato con policy di tipo “TempoMedioRisposta-*” (sezione <i>Rate Limiting</i>)
GovWay-RateLimit-TimeResponseQuota-Limit	Tempo complessivo di risposta occupabile	Policy creata con risorsa di tipo “TempoComplessivioRisposta” (sezione <i>Registro Policy</i>)
GovWay-RateLimit-TimeResponseQuota-Remaining	Tempo di risposta ancora occupabile prima del prossimo reset	Policy creata con risorsa di tipo “TempoComplessivioRisposta” (sezione <i>Registro Policy</i>)
GovWay-RateLimit-TimeResponseQuota-Reset	Numero di secondi mancante al prossimo reset	Policy creata con risorsa di tipo “TempoComplessivioRisposta” (sezione <i>Registro Policy</i>)
GovWay-RateLimit-RequestSuccessful-Limit, GovWay-RateLimit-RequestFailed-Limit, GovWay-RateLimit-Fault-Limit	Indica il numero massimo di richieste effettuabili	Policy creata rispettivamente con risorsa di tipo “NumeroRichiesteCompletate-ConSuccesso”, “NumeroRichiesteFallite” e “NumeroFaultApplicativi” (sezione <i>Registro Policy</i>)
GovWay-RateLimit-RequestSuccessful-Remaining, GovWay-RateLimit-RequestFailed-Remaining, GovWay-RateLimit-Fault-Remaining	Numero di richieste rimanenti prima del prossimo reset	Policy creata rispettivamente con risorsa di tipo “NumeroRichiesteCompletate-ConSuccesso”, “NumeroRichiesteFallite” e “NumeroFaultApplicativi” (sezione <i>Registro Policy</i>)
GovWay-RateLimit-RequestSuccessful-Reset, GovWay-RateLimit-RequestFailed-Reset, GovWay-RateLimit-Fault-Reset	Numero di secondi mancante al prossimo reset	Policy creata rispettivamente con risorsa di tipo “NumeroRichiesteCompletate-ConSuccesso”, “NumeroRichiesteFallite” e “NumeroFaultApplicativi” (sezione <i>Registro Policy</i>)

9.6.3 Scambio di informazioni nella richiesta del client verso il gateway

Le informazioni che possono essere fornite dal client al gateway sono riassunte nella tabella Tabella 9.5 e riguardano le modalità *Trasporto* e *Url Based* attive di default.

Tabella 9.5: Scambio di informazioni nella richiesta del client verso il gateway

Nome Header Trasporto	Nome Url Property	Descrizione
GovWay-Action	govway_action	Identificativo dell’azione invocata. Tale informazione deve essere fornita dal client se il servizio è stato configurato in modalità di identificazione dell’azione <i>input-based</i> . (Sezione <i>Modalità di identificazione dell’azione</i>)
GovWay-Relates-To	govway_relates_to	Identificativo di un precedente messaggio a cui la richiesta in essere si riferisce. (Sezione <i>Correlazione tra transazioni differenti</i>)
GovWay-Conversation-ID	govway_conversation_id	Identificativo di una conversazione a cui la richiesta in essere si riferisce (Sezione <i>Correlazione tra transazioni differenti</i>)

9.6.4 Altri header di Integrazione

Per attivare differenti header di integrazione è richiesto l'accesso alla govwayConsole in modalità *avanzata* (Sezione [Modalità Avanzata](#)).

Nota: Gli header di trasporto relativi alle funzionalità di Rate-Limiting e Service-Unavailable, descritti nella sezione *Scambio di informazioni tra gateway e la risposta ritornata al client*, vengono generati solamente nella modalità *Header HTTP*.

A partire dall'erogazione o fruizione già creata in precedenza accedendo tramite il link Gestione Configurazione presente nel dettaglio dell'erogazione/fruizione è possibile accedere a configurazioni specifiche come descritto nella sezione [Configurazione Specifica](#). Accedendo in modalità avanzata compare una sezione precedentemente non documentata denominata *Opzioni Avanzate*. All'interno di tale sezione è possibile agire sulla configurazione della voce *Metadati* nella sezione *Integrazione*. In tale campo, per default non impostato, è possibile attivare gli header di integrazione desiderati utilizzando le seguenti keyword separate da virgola:

Nota: Per ogni tipo di header di integrazione descritto di seguito, esiste una modalità normale ed una estesa (suffisso “Ext”). Le due modalità si differenziano poichè nella modalità non estesa non vengono generati gli header nella richiesta inoltrata al server in una fruizione e quelli generati nella risposta ritornata al client in una erogazione.

- *trasporto* o *trasportoExt*: header di trasporto descritti nelle precedenti sezioni.
- *urlBased* o *urlBasedExt*: le informazioni precedentemente descritte vengono aggiunte alla url tramite i parametri descritti nella [Tabella 9.6](#).

Tabella 9.6: Informazioni generate dal gateway nella url della richiesta inoltrata al server

Nome Query URL Parameter	Descrizione
govway_message_id	Identificativo del messaggio assegnato da GovWay
govway_relates_to	Identificativo del messaggio riferito
govway_conversation_id	Identificativo della conversazione
govway_transaction_id	Identificativo della transazione 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_application_message_id	Identificativo del messaggio assegnato dall'applicativo
govway_application	Identificativo dell'applicativo

Nota: Esiste una terza versione *urlBasedOnlyRead* che permette di attivare la lettura delle informazioni impostate dall'applicativo client ma non genera header verso l'applicativo server.

- *soap* o *soapExt*: le informazioni precedentemente descritte vengono incluse come attributi in uno specifico header SOAP proprietario di GovWay che possiede il nome *integration* associato al namespace <http://govway.org/integration>. Di seguito un esempio di tale header:

```
<gw:integration
  ...
  transactionId="a2c6fd66-ec0b-407c-8a21-25b4920e7c73"
  SOAP_ENV:actor="http://govway.org/integration"
  SOAP_ENV:mustUnderstand="0"
  xmlns:SOAP_ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:gw="http://govway.org/integration"/>
```

Nella tabella [Tabella 9.7](#) vengono descritti i nome degli attributi.

Tabella 9.7: Informazioni generate dal gateway nell'header soap proprietario di GovWay

Nome Attributo	Descrizione
messageId	Identificativo del messaggio assegnato da GovWay
relatesTo	Identificativo del messaggio riferito
conversationId	Identificativo della conversazione
transactionId	Identificativo della transazione assegnato da GovWay
senderType	Codice che identifica il tipo del mittente
sender	Identificativo del mittente
providerType	Codice che identifica il tipo del destinatario
provider	Identificativo del destinatario
serviceType	Codice che identifica il tipo del servizio
service	Identificativo del servizio
serviceVersion	Progressivo di versione del servizio
action	Identificativo dell'azione
applicationMessageId	Identificativo del messaggio assegnato dall'applicativo
application	Identificativo dell'applicativo

Nota: Utilizzabile solamente con API di tipologia SOAP

- *wsa* o *wsaExt*: all'interno del messaggio Soap vengono generati gli header *To*, *From*, *Action*, *MessageID* e *RelatesTo* associati al namespace <http://www.w3.org/2005/08/addressing>. I valori utilizzati per i vari header sono i seguenti:
 - *To*, http://<providerType>_<provider>.govway.org/services/<serviceType>_<service>/<serviceVersion>
 - *From*, [http://\[<application>.\]<senderType>_<sender>.govway.org](http://[<application>.]<senderType>_<sender>.govway.org)
 - *Action*, http://<providerType>_<provider>.govway.org/services/<serviceType>_<service>/<serviceVersion>/<action>
 - *MessageID*, *uuid:<messageId>* in caso di Messaggio di Protocollo (restituzione di una risposta lato PD o in caso di consegna tramite PA), *uuid:<applicationMessageId>* in caso di Messaggio di Integrazione (invocazione lato PD o lettura risposta lato PA, es. per correlazione applicativa)
 - *RelatesTo*, *uuid:<relatesTo>*

Nota: Utilizzabile solamente con API di tipologia SOAP

- *openspcoop2-<tipo>* o *openspcoop1-<tipo>*: sono disponibili header di integrazione compatibili con le versioni di OpenSPCoop 2.x e 1.x:
 - *openspcoop2-trasporto* o *openspcoop1-trasporto*: le informazioni sono veicolate all'interno di header HTTP senza prefisso “X-“

- openspcoop2-x-trasporto o openspcoop1-x-trasporto: le informazioni sono veicolate all'interno di header HTTP con prefisso “X-“
- openspcoop2-urlBased o openspcoop1-urlBased: le informazioni sono veicolate come parametri della url
- openspcoop2-soap o openspcoop1-soap: le informazioni sono incluse in uno specifico header SOAP proprietario di OpenSPCoop 2.x o 1.x
- openspcoop2-<tipo>Ext: rispetto alla descrizione fornita precedentemente, le informazioni vengono veicolate anche fuori dal dominio di gestione

9.7 Errori Generati dal Gateway

La gestione dei casi di errore nelle comunicazioni mediate da un Gateway devono tenere conto di ulteriori situazioni che possono presentarsi rispetto alla situazione di dialogo diretto tra gli applicativi. Oltre agli errori conosciuti dagli applicativi, e quindi previsti nei descrittori del servizio, gli applicativi client possono ricevere ulteriori errori generati dal gateway.

Govway genera differenti errori a seconda se l'erogazione o la fruizione riguarda una API di tipologia SOAP (sezione *SOAP Fault*) o REST (sezione *REST Problem Details (RFC 7807)*).

Per entrambe le tipologie, all'interno dell'errore generato, viene ritornato al client un codice di errore che rappresenta una classificazione interna a GovWay dell'errore avvenuto. Nella sezione *Codici di Errore* vengono riportate due tabelle che descrivono cosa rappresentano tali codici.

9.7.1 REST Problem Details (RFC 7807)

Quando il Gateway non può completare con successo la gestione della transazione in corso genera un oggetto *Problem Details* come definito nella specifica *RFC 7807* (<https://tools.ietf.org/html/rfc7807>).

Di seguito viene riportato un esempio di tale oggetto:

```
{  
  "type": "https://httpstatuses.com/401",  
  "title": "Unauthorized",  
  "status": 401,  
  "detail": "Token non valido",  
  "govway_status": "integration:GOVWAY-444"  
}
```

L'elemento *type* presenta sempre il suffisso *https://httpstatuses.com/* seguito poi dal codice http ritornato al client, riportato anche nell'elemento *status*. L'elemento *title* contiene invece la descrizione http del codice ritornato al client.

Nell'elemento *detail* sono presenti informazioni di dettaglio sull'errore avvenuto, errore codificato dal codice presente nell'elemento *govway_status*. (Per ulteriori dettagli sul codice consultare la sezione *Codici di Errore*).

La casistica dei possibili errori generati dal gateway viene riportata nella tabella [Tabella 9.8](#).

Tabella 9.8: Casistica Problem Details per API REST

HTTP Status	Descrizione
401	Rientrano in questa casistica gli errori avvenuti durante le fasi di autenticazione degli applicativi (Sezione <i>Autenticazione Trasporto</i>) e di verifica del token OAuth (Sezione <i>Autenticazione Token</i>)
403	In questa categoria rientrano errori avvenuti durante la fase di autorizzazione descritta nella sezione <i>Autorizzazione</i>
404	Identifica la richiesta di una erogazione o fruizione inesistente
400	L'errore occorso è imputabile ai dati forniti dal client (es. messaggio non valido in caso di validazione attiva)
429	Identifica una violazione della politica di Rate Limiting (Sezione <i>Rate Limiting</i>)
503	Rientrano in questa casistica gli errori causati da una irraggiungibilità dell'applicativo indirizzato dal Gateway o una temporanea sospensione della erogazione/fruizione
500	Qualsiasi altro errore

Nota

L'oggetto *Problem Details* generato dal Gateway possiede per default il formato *json*.

Viene utilizzato il formato *xml* (Appendice "A" del RFC 7807) solamente se la richiesta presenta anch'essa tale formato.

Un applicativo client può indicare al Gateway quale formato desidera attraverso l'header http *Accept*.

9.7.2 SOAP Fault

Per le API di tipologia SOAP, sia in erogazione che in fruizione, quando il Gateway non può completare con successo la gestione della transazione in corso genera un SOAPFault contenente un actor (o role in SOAP 1.2) valorizzato con *http://govway.org/integration*.

Di seguito viene riportato un esempio di tale oggetto:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <SOAP-ENV:Fault>
            <faultcode xmlns:integration="http://govway.org/integration/fault">
                integration:GOVWAY-403
            </faultcode>
            <faultstring>Identificazione dinamica dell'azione associata alla porta delegata fallita</faultstring>
            <faultactor>http://govway.org/integration</faultactor>
            <detail>
                <problem xmlns="urn:ietf:rfc:7807">
                    <type>https://httpstatuses.com/500</type>
                    <title>Internal Server Error</title>
                    <status>500</status>
                    <detail>Identificazione dinamica dell'azione associata alla porta delegata fallita</detail>
                    <govway_status>integration:GOVWAY-403</govway_status>
                </problem>
            </detail>
        </SOAP-ENV:Fault>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

L'elemento *fault string* contiene informazioni di dettaglio sull'errore avvenuto, errore codificato dal codice presente nell'elemento *fault code*. (Per ulteriori dettagli sul codice consultare la sezione [Codici di Errore](#)).

Il SOAP Fault contiene all'interno dell'elemento *detail* un oggetto *Problem Details* simile a quanto descritto nella sezione [REST Problem Details \(RFC 7807\)](#) utile a comprendere il codice di errore ed il dettaglio attraverso una modalità alternativa alla lettura degli elementi *fault string* e *fault code* (che varia a seconda della versione SOAP utilizzata).

9.7.3 Codici di Errore

Di seguito vengono riportate le casistiche di errore che possono avvenire sul Gateway, con i relativi codici utilizzati all'interno dei formati di errore come descritto nelle sezioni [REST Problem Details \(RFC 7807\)](#) e [SOAP Fault](#).

Nota: Alcuni degli errori riportati sono scaturiti da funzionalità disponibili nel Gateway attraverso configurazioni avanzate non descritte nel presente manuale.

Tabella 9.9: Codici di Errore GovWay

Codice	Descrizione
integration:GOVWAY-401	Identifica la richiesta di una erogazione o fruizione inesistente
integration:GOVWAY-402	Rientrano in questa casistica gli errori avvenuti durante la fase di autenticazione di una fruizione (sezione Autenticazione Trasporto)
integration:GOVWAY-403	Azione non identificabile tramite i meccanismi configurati. (sezione Modalità di identificazione dell'azione)
integration:GOVWAY-404	Rientrano in questa casistica gli errori avvenuti durante la fase di autorizzazione di una fruizione (sezione Autorizzazione)
integration:GOVWAY-405	Servizio richiesto non esistente (richiede una configurazione non documentata)
integration:GOVWAY-406	Indica che non sono disponibili messaggi (richiede accesso alla MessageBox via Integration Manager, configurazione non documentata)
integration:GOVWAY-407	Il messaggio richiesto non esiste (richiede accesso alla MessageBox via Integration Manager, configurazione non documentata)
integration:GOVWAY-408	Indica che non esiste una API utilizzabile per correlare la richiesta con una precedente transazione (es. utilizzato con i profili asincroni descritti nella sezione Profili Asincroni)
integration:GOVWAY-409	Indica che non è possibile correlare la richiesta con una precedente transazione (es. utilizzato con i profili asincroni descritti nella sezione Profili Asincroni)
integration:GOVWAY-410	L'API invocata possiede il profilo <i>asincrono simmetrico</i> e la configurazione della fruizione non presenta meccanismi di autenticazione dell'applicativo client. L'identificazione di un applicativo fruitore è fondamentale nel profilo asincrono simmetrico per consegnare la risposta (Profili Asincroni)
integration:GOVWAY-411	Indica una configurazione errata dove l'applicativo mittente non possiede una configurazione per la spedizione della risposta asincrona e l'API possiede il profilo <i>asincrono simmetrico</i> (Profili Asincroni)
integration:GOVWAY-412	L'API è stata invocata senza fornire il riferimento ad un messaggio attualmente in carico sul Gateway, mentre la configurazione lo richiede. richiede una configurazione non documentata)

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
integration:GOVWAY-413	L'API è stata invocata fornendo il riferimento ad un messaggio attualmente in carico sul Gateway, mentre la configurazione non lo richiede. richiede una configurazione non documentata)
integration:GOVWAY-414	L'API invocata è stata configurata con un profilo differente da <i>oneway</i> e richiede la funzionalità di <i>consegna in ordine</i> (sezione <i>Profili di gestione della busta eGov</i>)
integration:GOVWAY-415	L'API invocata è stata configurata per utilizzare la funzionalità di <i>consegna in ordine</i> ma non presenta altre caratteristiche obbligatorie con questa funzionalità (es. confermaRicezione,filtroDuplicati,collaborazione) (sezione <i>Profili di gestione della busta eGov</i>)
integration:GOVWAY-416	Rientrano in questa casistica gli errori avvenuti durante la fase di correlazione applicativa della richiesta (sezione <i>Correlazione Applicativa</i>)
integration:GOVWAY-417	Tale errore viene sollevato se l'interfaccia API e/o gli schemi associati (xsd,json,yaml) contengono errori che non ne consentono l'utilizzo durante la validazione dei contenuti (sezione <i>Validazione dei messaggi</i>)
integration:GOVWAY-418	La validazione dei contenuti ha rilevato una richiesta non conforme all'interfaccia API (sezione <i>Validazione dei messaggi</i>)
integration:GOVWAY-419	La validazione dei contenuti ha rilevato una risposta non conforme all'interfaccia API (sezione <i>Validazione dei messaggi</i>)
integration:GOVWAY-420	Viene sollevato questo errore se un applicativo invoca una fruizione di una API fornendo un messaggio contenente già un header di protocollo. (es. se viene inviato un messaggio contenente un'header eGov (sezione <i>Profilo "SPCoop"</i>)
integration:GOVWAY-421	Indica che il messaggio di richiesta fornito via Integration Manager non è un messaggio SOAP valido (configurazione non documentata)
integration:GOVWAY-422	Il messaggio di richiesta presente nell'http body (Accesso al servizio out/xml2soap) o il messaggio indicato nella richiesta via Integration-Manager (Accesso al servizio via Integration Manager con imbustamento SOAP) non è utilizzabile, tramite la funzionalità di Imbustamento, per ottenere un messaggio SOAP valido (configurazione non documentata)
integration:GOVWAY-423	L'azione identificata tramite i meccanismi configurati non risulta esistere all'interno dell'API invocata. (sezione <i>Modalità di identificazione dell'azione</i>)
integration:GOVWAY-424	La funzionalità avanzata <i>Allega Body</i> ha generato un errore (configurazione non documentata)
integration:GOVWAY-425	La funzionalità avanzata <i>Scarta Body</i> ha generato un errore (configurazione non documentata)
integration:GOVWAY-426	Errore generico che può avvenire durante la gestione della richiesta, dovuto comunque a dati forniti nella richiesta stessa (es. Valore SOAPAction scorretto)
integration:GOVWAY-427	Indica che il Gateway ha rilevato la presenza di SOAPHeader Element che non è in grado di processare e che richiedono obbligatoriamente il processamento (mustUnderstand=1 e actor non presente)
integration:GOVWAY-428	Rientrano in questa casistica gli errori avvenuti durante la fase di autorizzazione del contenuto (configurazione non documentata)
integration:GOVWAY-429	Errore che viene ritornato dal Gateway se la richiesta presenta un header http <i>Content-Type</i> non supportato (per API SOAP)
integration:GOVWAY-430	Errore che viene ritornato dal Gateway se rileva una busta soap che possiede un namespace differente da quello atteso per la versione SOAP corrispondente al <i>Content-Type</i> (per API SOAP)

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
integration:GOVWAY-431	Rientrano in questa casistica gli errori avvenuti durante il recupero delle credenziali fornite tramite un Proxy (configurazione non documentata)
integration:GOVWAY-432	Errore che viene ritornato dal Gateway se la richiesta presenta un contenuto malformato (es. xml malformato in una API SOAP)
integration:GOVWAY-433	Indica che la richiesta non presenta un header http <i>Content-Type</i> (obbligatorio in API SOAP)
integration:GOVWAY-434	Rientrano in questa casistica gli errori avvenuti durante la fase di correlazione applicativa della risposta (sezione <i>Correlazione Applicativa</i>)
integration:GOVWAY-435	L'errore viene sollevato se viene rilevata una configurazione <i>Local Forward</i> non corretta (configurazione non documentata)
integration:GOVWAY-436	L'errore viene sollevato se viene rilevato un tipo di fruitore non supportato dalla modalità di utilizzo del Gateway fruita (configurazione non documentata)
integration:GOVWAY-437	L'errore viene sollevato se viene rilevato un tipo di erogatore non supportato dalla modalità di utilizzo del Gateway fruita (configurazione non documentata)
integration:GOVWAY-438	L'errore viene sollevato se viene rilevato un tipo di servizio non supportato dalla modalità di utilizzo del Gateway fruita (configurazione non documentata)
integration:GOVWAY-439	L'errore viene sollevato se viene rilevata una configurazione che richiede una funzionalità non supportata nella modalità di utilizzo del Gateway (configurazione non documentata)
integration:GOVWAY-440	Errore che viene ritornato dal Gateway se la risposta presenta un contenuto malformato (es. xml malformato in una API SOAP)
integration:GOVWAY-441	La richiesta indirizza una configurazione non invocabile direttamente, configurazione creata tramite le indicazioni descritte nella sezione <i>Differenziare le configurazioni specifiche per risorsa/azione</i>
integration:GOVWAY-442	La richiesta pervenuta sul Gateway non presenta un riferimento ad una precedente transazione, mentre la configurazione lo richiede (sezione <i>Correlazione tra transazioni differenti</i>). Nell'installazione di default del Gateway, l'errore indicato non viene mai sollevato poiché non è obbligatorio fornire il riferimento ad una precedente transazione.
integration:GOVWAY-443	L'errore viene ritornato dal Gateway se non viene rilevato un token durante l'invocazione di una fruizione (sezione <i>Autenticazione Token</i>)
integration:GOVWAY-444	L'errore viene ritornato dal Gateway se viene rilevato un token non valido durante l'invocazione di una fruizione (sezione <i>Autenticazione Token</i>)
integration:GOVWAY-445	Rientrano in questa casistica gli errori avvenuti durante la fase di autorizzazione di una fruizione, riguardanti la gestione di un token (sezione <i>Autorizzazione</i>)
integration:GOVWAY-446	Il Gateway ritorna tale codice se la fruizione o l'erogazione invocata risulta sospesa
integration:GOVWAY-450	La richiesta pervenuta sul Gateway non indirizza una erogazione specifica e non è utilizzabile per identificarne alcuna (configurazione non documentata)
integration:GOVWAY-451	Il soggetto invocato non esiste (configurazione non documentata)
integration:GOVWAY-452	Indica che il messaggio ricevuto è già stato gestito in precedenza (es. filtro duplicati attivo descritto nella sezione <i>Profilo “SPCoop”</i>)
integration:GOVWAY-453	L'applicativo erogatore associato all'erogazione non esiste (configurazione non documentata)

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
integration:GOVWAY-454	Viene sollevato questo errore se il messaggio ritornato come risposta dall'applicativo erogatore, in una erogazione, contiene già un header di protocollo. (es. se viene ritornato un messaggio contenente un'header eGov (sezione <i>Profilo "SPCoop"</i>)
integration:GOVWAY-455	L'errore indica che la richiesta presenta al suo interno degli identificativi di API differenti da quelli dell'erogazione invocata (es. busta eGov contiene dei dati di servizio non allineati all'erogazione invocata)
integration:GOVWAY-500	Errore generico
integration:GOVWAY-516	Errore ritornato dal gateway se non riesce ad inoltrare il messaggio all'endpoint configurato
integration:GOVWAY-517	Errore ritornato dal gateway se non viene ritornata una risposta dall'endpoint contattato e il profilo ne prevede una (es. profilo sincrono nelle API SOAP)
integration:GOVWAY-518	Indica che l'applicativo erogatore ha ritornato un SOAPFault (API SOAP)
integration:GOVWAY-537	La richiesta pervenuta è già presente in carico sul Gateway ed è attualmente in fase di processamento (configurazione non documentata)
integration:GOVWAY-538	La richiesta asincrona pervenuta è già presente in carico sul Gateway ed è attualmente in fase di processamento (configurazione non documentata)
integration:GOVWAY-539	La ricevuta della richiesta asincrona pervenuta è già presente in carico sul Gateway ed è attualmente in fase di processamento (configurazione non documentata)
integration:GOVWAY-CC00	Errore generico avvenuto durante la gestione del Controllo del Traffico (sezione <i>Controllo del Traffico</i>)
integration:GOVWAY-CC01	Il Gateway ha rilevato il superamento del massimo numero di richieste simultanee configurato (sezione <i>Limitazione Numero di Richieste Complessive</i>)
integration:GOVWAY-CP00	Indica che la funzionalità di Rate-Limiting ha rilevato una policy sconosciuta (sezione <i>Rate Limiting</i>)
integration:GOVWAY-CP01	Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo "NumeroRichieste-RichiesteSimultanee" (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP01	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo "NumeroRichieste-RichiesteSimultanee" (sezione <i>Rate Limiting</i>).
integration:GOVWAY-CP02	Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo "NumeroRichieste-ControlloRealtime*" (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado (sezione <i>Rate Limiting</i>).
integration:GOVWAY-ERR-CP02	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo "NumeroRichieste-ControlloRealtime**" (sezione <i>Rate Limiting</i>). integration:GOVWAY-CP03 Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo "OccupazioneBanda-*" (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado (sezione <i>Rate Limiting</i>).

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
integration:GOVWAY-ERR-CP03	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “OccupazioneBanda-*” (sezione <i>Rate Limiting</i>). integration:GOVWAY-CP04 Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo “TempoComplessivoRisposta” (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP04	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “TempoComplessivoRisposta” (sezione <i>Rate Limiting</i>).
integration:GOVWAY-CP05	Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo “TempoMedioRisposta-*” (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP05	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “TempoMedioRisposta-*” (sezione <i>Rate Limiting</i>). integration:GOVWAY-CP06 Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo “NumeroRichiesteCompletateConSuccesso” (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP06	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “NumeroRichiesteCompletateConSuccesso” (sezione <i>Rate Limiting</i>). integration:GOVWAY-CP07 Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo “NumeroRichiesteFallite” (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP07	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “NumeroRichiesteFallite” (sezione <i>Rate Limiting</i>).
integration:GOVWAY-CP08	Indica che la funzionalità di Rate-Limiting ha rilevato una violazione di una policy di tipo “NumeroFaultApplicativi” (sezione <i>Rate Limiting</i>). Il codice di errore può presentare il suffisso -CC se la policy è configurata insieme a controlli di congestione e/o il suffisso -DP se configurata con meccanismi di degrado.
integration:GOVWAY-ERR-CP08	Errore emerso durante la gestione da parte del Gateway della policy di Rate-Limiting di tipo “NumeroFaultApplicativi” (sezione <i>Rate Limiting</i>).
protocol:GOVWAY-109	Rientrano in questa casistica gli errori avvenuti durante la fase di autenticazione di una erogazione, se non vengono rilevate credenziali (sezione <i>Autenticazione Trasporto</i>)
protocol:GOVWAY-117	Rientrano in questa casistica gli errori avvenuti durante la fase di autenticazione di una erogazione, se vengono rilevate credenziali non corrette (sezione <i>Autenticazione Trasporto</i>)
protocol:GOVWAY-1350	Rientrano in questa casistica eventuali errori generici avvenuti durante la fase di autorizzazione di una erogazione (sezione <i>Autorizzazione</i>) o sicurezza del messaggio (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-1351	L'errore viene ritornato dal Gateway se viene rilevato che il messaggio presenta al suo interno un mittente differente da quello identificato dalle credenziali (configurazione non documentata)

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
protocol:GOVWAY-1352	Rientrano in questa casistica gli errori avvenuti durante la fase di autorizzazione di una erogazione, quando la richiesta non viene autorizzata (sezione <i>Autorizzazione</i>)
protocol:GOVWAY-[1353-1354]	L'errore viene ritornato dal Gateway se viene rilevato che la firma della busta, prevista dalla modalità utilizzata, non è rispettivamente valida o presente (configurazione non documentata)
protocol:GOVWAY-1355	L'errore viene ritornato dal Gateway se viene rilevato che la firma del messaggio non è valida (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-1356	L'errore viene ritornato dal Gateway se viene rilevato che il messaggio non è firmato (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-[1357-1360]	L'errore viene ritornato dal Gateway se viene rilevato che la firma degli allegati non sono valide o presenti (configurazione non documentata)
protocol:GOVWAY-1361	L'errore viene ritornato dal Gateway se viene rilevato che la cifratura del messaggio non è valida (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-1362	L'errore viene ritornato dal Gateway se viene rilevato che il messaggio non è cifrato (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-[1363-1364]	L'errore viene ritornato dal Gateway se viene rilevato che le cifrature degli allegati non sono valide o presenti (configurazione non documentata)
protocol:GOVWAY-1365	L'errore viene ritornato dal Gateway se viene rilevato che il messaggio non contiene l'attesa configurazione di sicurezza (sezione <i>Sicurezza a livello del messaggio</i>)
protocol:GOVWAY-1366	L'errore viene ritornato dal Gateway se non viene rilevato un token durante l'invocazione di una erogazione (sezione <i>Autenticazione Token</i>)
protocol:GOVWAY-1367	L'errore viene ritornato dal Gateway se viene rilevato un token non valido durante l'invocazione di una erogazione (sezione <i>Autenticazione Token</i>)
protocol:GOVWAY-1368	Rientrano in questa casistica gli errori avvenuti durante la fase di autorizzazione di una erogazione, riguardanti la gestione di un token (sezione <i>Autorizzazione</i>)
protocol:GOVWAY-[1-6]	Rientrano in questa casistica gli errori generici avvenuti durante il processamento e la validazione di una richiesta di erogazione
protocol:GOVWAY-[51-60]	Gli errori che rientrano in questa casistica vengono generati durante la validazione della richiesta se sono presenti informazioni non valide per quanto concerne gli attributi <i>mustUnderstand</i> e <i>actor</i> di un header SOAP (es. busta egov nella modalità descritta in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[100-120]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul mittente (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[150-170]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul destinatario (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[200-205]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul profilo di collaborazione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[250-265]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul servizio (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[300-315]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla correlazione asincrona (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[350-355]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla collaborazione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)

Continued on next page

Tabella 9.9 – continued from previous page

Codice	Descrizione
protocol:GOVWAY-[400-406]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sull'azione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[450-455]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla correlazione asincrona per quanto riguarda l'azione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[500-506]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sull'identificativo messaggio (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[550-556]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul riferimento messaggio (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[600-610]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sull'ora registrazione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[650-661]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla scadenza (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[700-717]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul filtro duplicati e sulla conferma della ricezione (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[750-766]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla consegna in ordine (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[800-817]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sul servizio applicativo
protocol:GOVWAY-[850-879]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sui riscontri (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[900-971]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla lista trasmissioni (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[1000-1035]	Errore rilevato durante la validazione della richiesta che riguarda informazioni sulla lista eccezioni (es. busta egov in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[1300-1329]	Errore rilevato durante la validazione del messaggio per quanto concerne la parte di SOAPFault previsto dal protocollo (es. busta egov errore in sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-[1400-1404]	Errore rilevato durante la validazione del messaggio per quanto concerne la parte di attachments previsto dal protocollo (es. busta egov con attachments, sezione <i>Profilo "SPCoop"</i>)
protocol:GOVWAY-2000	Errore generico rilevato durante la validazione del messaggio

9.8 Connettori

I connettori rappresentano le entità di configurazione che consentono a GovWay di indirizzare le comunicazioni verso gli attori dei flussi di erogazione/fruizione gestiti. Nel nostro contesto possiamo distinguere due tipologie di comunicazioni:

- *GovWay* —> *Applicativo Esterno*, nel caso di fruizioni
- *GovWay* —> *Applicativo Interno*, nel caso di erogazioni

I connettori di GovWay permettono di configurare differenti aspetti della comunicazione http:

- *Autenticazione http*: tale funzionalità permette di impostare delle credenziali http basic (username e password).
- *Autenticazione token*: tale funzionalità permette di inoltrare un Bearer Token.
- *Autenticazione https*: se l'utente lo desidera può personalizzare tutti gli aspetti che riguardano una comunicazione sicura su https.
- *Proxy*: è possibile configurare un proxy http che media la comunicazione.
- *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 *Tempi Risposta*).

Attivando la *modalità avanzata* dell'interfaccia saranno inoltre disponibili le seguenti opzioni:

- *Data Transfer Mode*: tramite questa configurazione è possibile indicare se la comunicazione deve avvenire in modalità transfer-encoding-chunked (streaming) o content length fisso.
- *Redirect*: tramite questa configurazione è possibile indicare se un eventuale redirect ritornato dal server contattato deve essere seguito o meno.
- *Debug*: è possibile abilitare un log verboso di tutta la comunicazione.

La govwayConsole, tramite l'interfaccia in modalità *avanzata*, consente anche di configurare le comunicazioni attraverso connettori non basati sul protocollo HTTP (o HTTPS). GovWay offre built-in i seguenti ulteriori connettori:

- *JMS*: connettore basato sul protocollo JMS
- *File*: connettore che permette di serializzare il messaggio di richiesta su FileSystem ed opzionalmente generare una risposta.
- *Null*: connettore per test. Si comporta come un servizio Oneway ricevendo richieste senza rispondere
- *NullEcho*: connettore per test. Si comporta come un servizio Sincrono rispondendo con un messaggio identico alla richiesta

Nel seguito vengono descritte alcune funzionalità specifiche dei connettori HTTP e HTTPS. Inoltre viene fornita una descrizione del connettore built-in JMS.

9.8.1 Autenticazione Http

Quando si configura l'autenticazione per un connettore è possibile scegliere la modalità di autenticazione HTTP-BASIC. Tale funzionalità permette di impostare delle credenziali (username e password) che verranno iniettate nella comunicazione http tramite header “Authorization” (“<https://tools.ietf.org/html/rfc2617#section-2>”).

9.8.2 Autenticazione Token

Quando si configura l'autenticazione per un connettore è possibile scegliere la modalità di autenticazione per token. Tale funzionalità permette di iniettare un Token Bearer nella comunicazione http tramite la modalità definita all'interno della policy selezionata (es. tramite header “Authorization”). Per ulteriori dettagli su come registrare una policy di negoziazione del Bearer Token si rimanda alla sezione *Token Negoziazione Policy*.

Connettore

Abilitato	<input checked="" type="checkbox"/>
Endpoint *	<input type="text" value="http://127.0.0.1:8080/TestService/echo"/>
Autenticazione Http	<input checked="" type="checkbox"/>
AutenticazioneHttps	<input type="checkbox"/>
Proxy	<input type="checkbox"/>
Ridefinisci Tempi Risposta	<input type="checkbox"/>

Autenticazione Http

Utente *	<input type="text"/>
Password *	<input type="password"/>

Fig. 9.10: Dati di configurazione di un'autenticazione Http

Connettore

Endpoint *	<input type="text" value="http://127.0.0.1:8080/TestService/echo"/>
Autenticazione Token	<input checked="" type="checkbox"/>
AutenticazioneHttps	<input type="checkbox"/>
Proxy	<input type="checkbox"/>
Ridefinisci Tempi Risposta	<input type="checkbox"/>

Autenticazione Token

Policy *	<input type="text" value="AuthorizationServerEnte"/>
----------	--

Fig. 9.11: Dati di configurazione di un'autenticazione Token

9.8.3 Autenticazione Https

Il connettore HTTPS permette di personalizzare i parametri SSL per ogni connessione che utilizza questo protocollo.

Il connettore HTTPS supporta:

- **Autenticazione Server**, è possibile definire le trusted keys e indicare se si desidera verificare l'hostname rispetto al certificato server contenuto nella sessione SSL.
- **Autenticazione Client**, è opzionale; se abilitata permette di definire il keystore contenente la chiave privata che si deve utilizzare durante la sessione SSL.

Facendo riferimento alla maschera raffigurata in Fig. 9.12 andiamo a descrivere il significato dei parametri:

- *Connettore*
 - **Url**: indirizzo endpoint del connettore
 - **Tipologia** (es. TLSv1.2): Tipo e versione del protocollo di trasporto. Sono selezionabili tutti i tipi supportati dalla versione della jvm utilizzata.
 - **Hostname Verifier** (true/false): Attiva la verifica in fase di autenticazione server della corrispondenza tra l'hostname indicato nella url e quello presente nel certificato server ritornato dal server (nel subject CN=hostname)
- *Autenticazione Server*
 - **Path**: Path dove è localizzato il truststore contenente i certificati server trusted.
 - **Tipo** (jks, pkcs12, jceks, bks, uber e gkr): Tipologia del TrustStore (default: jks)
 - **Password**: Password per l'accesso al TrustStore
 - **CRL File(s)**: Path dove è presente una CRL da utilizzare per validare i certificati server. L'indicazione di una CRL è opzionale e ne possono essere indicate più di una separando i path con la virgola.
- *Autenticazione Client (opzionale)*
 - **Dati di Accesso al KeyStore** (usa valori del TrustStore, Ridefinisci): Consente di riutilizzare i medesimi riferimenti del TrustStore anche per il KeyStore o in alternativa ridefinirli.
 - **Tipo (solo se Dati di Accesso ridefiniti)** (jks, pkcs12, jceks, bks, uber e gkr): Tipologia del Keystore (default: jks)
 - **Password (solo se Dati di Accesso ridefiniti)**: Password per l'accesso al Keystore
 - **Password Chiave Privata**: Password per accedere alla chiave privata presente nel keystore.
 - **Alias Chiave Privata**: Alias che individua la chiave privata, presente nel keystore, da utilizzare. L'indicazione di un alias è opzionale e se non fornito viene utilizzata la prima chiave trovata.

9.8.4 Proxy

Funzionalità che consente di configurare un proxy http che media la comunicazione. Oltre ai classici parametri hostname e porta, è possibile anche indicare delle credenziali http basic (username e password) che verranno iniettate nella comunicazione http tramite header “Proxy-Authorization”.

Connettore

Endpoint *

Autenticazione Http

Autenticazione Token

AutenticazioneHttps

Proxy

Ridefinisci Tempi Risposta

Autenticazione Https

Tipologia

HostnameVerifier

Autenticazione Server

Path *

Tipo

Password *

CRL File(s)

Elencare più file separandoli con la ";"

Autenticazione Client

Abilitato

Dati Accesso al KeyStore

Path *

Tipo

Password *

Password Chiave Privata *

Alias Chiave Privata

Connettore

- Abilitato
- Endpoint *
- Autenticazione Http
- AutenticazioneHttps
- Proxy
- Ridefinisci Tempi Risposta

Proxy

- Hostname *
- Porta *
- Username
- Password

Fig. 9.13: Dati di configurazione di un Proxy Http

9.8.5 Configurazione Http Avanzata

Richiede accesso alla govwayConsole in modalità *avanzata*

Tramite questa sezione è possibile indicare sia quale modalità di comunicazione (streaming o meno) deve essere utilizzata, sia se deve avvenire una eventuale gestione dei redirect http.

Facendo riferimento alla maschera raffigurata in Fig. 9.14 andiamo a descrivere il significato dei parametri:

- *Data Transfer Mode* tramite questa configurazione è possibile indicare se la comunicazione deve avvenire in modalità transfer-encoding-chunked (streaming) o con content length fisso.
 - **Modalità Data Transfer** (default, content-length, transfer-encoding-chunked): indica il tipo di trasferimento dati; scegliendo la voce default verrà utilizzato il comportamento configurato a livello globale nel file govway.properties tramite le opzioni:
 - * org.openspcoop2.pdd.connatori.inoltroBuste.httpTransferLength
 - * org.openspcoop2.pdd.connatori.consegnaContenutiApplicativi.httpTransferLength
 - **Chunk Length (Bytes)** (presente solamente se la modalità è transfer-encoding-chunked): indica la dimensione in bytes di ogni singolo http chunk.
- *Redirect* tramite questa configurazione è possibile indicare se un eventuale redirect ritornato dal server contattato deve essere seguito o meno.
 - **Gestione Redirect** (default, abilitato, disabilitato): consente di personalizzare il comportamento sul singolo connettore; scegliendo la voce default verrà utilizzato il comportamento configurato a livello globale nel file govway.properties tramite le opzioni:

Connettore

Tipo	<input type="text" value="http"/>
Debug	<input type="checkbox"/>
Endpoint *	<input type="text" value="http://127.0.0.1:8080/TestService/echo"/>
Autenticazione Http	<input type="checkbox"/>
Proxy	<input type="checkbox"/>
Ridefinisci Tempi Risposta	<input type="checkbox"/>
Opzioni Avanzate	<input checked="" type="checkbox"/>

Opzioni Avanzate

Modalità Data Transfer	<input type="text" value="transfer-encoding-chunked"/>
Chunk Length (Bytes)	<input type="text"/>
Gestione Redirect	<input type="text" value="abilitato"/>
Max Numero di Redirect	<input type="text"/>

Fig. 9.14: Configurazione http avanzata

- * org.openspcoop2.pdd.connettori.inoltroBuste.followRedirects
- * org.openspcoop2.pdd.connettori.consegnaContenutiApplicativi.followRedirects
- **Massimo Numero di Redirect** (presente solamente se la gestione redirect è abilitata): indica il massimo numero di redirect seguiti.

9.8.6 Debug

Richiede accesso alla govwayConsole in modalità *avanzata* (sezione *Modalità Avanzata*).

Se viene abilitato il debug, GovWay produce un log verboso di tutta la comunicazione nel file

- `/var/log/govway/govway_connatori.log`

(assumendo che `/var/log/govway` sia la directory di logging configurata)

Fig. 9.15: Debug

9.8.7 Connettore JMS

Il connettore JMS consente di configurare i parametri per abilitare la comunicazione tra GovWay e gli applicativi attraverso il protocollo JMS.

In Fig. 9.16 è mostrata la maschera di configurazione del connettore JMS.

In riferimento alla Fig. 9.16 descriviamo in dettaglio il significato dei campi per la configurazione:

- **Nome:** identificatore JNDI della risorsa queue/topic JMS
- **Tipo** (Queue/Topic): Si specifica se la risorsa JMS è di tipo queue o topic
- **Send As** (TextMessage/BytesMessage): Si sceglie la codifica del messaggio da inviare tramite broker JMS, tra TextMessage e BytesMessage.
- **Utente:** Username relativo alle credenziali per l'autenticazione e la negoziazione di una connessione sul Broker JMS

Connettore

Tipo	<input type="text" value="jms"/>
Debug	<input type="checkbox"/>
Ridefinisci Tempi Risposta	<input type="checkbox"/>

Dati Configurazione Coda

Nome *	<input type="text" value="http://127.0.0.1:8080/TestService/echo"/>
Tipo	<input type="text" value="queue"/>
Send As	<input type="text" value="TextMessage"/>

Dati Configurazione Connessione

Connection Factory *	<input type="text"/>
Utente	<input type="text"/>
Password	<input type="text"/>

Contesto JNDI

Initial Context Factory	<input type="text"/>
Url Pgk Prefixes	<input type="text"/>
Provider Url	<input type="text"/>

Fig. 9.16: Dati di configurazione di un connettore JMS

- **Password:** Password relativa alle credenziali per l'autenticazione e la negoziazione di una connessione sul Broker JMS
- **Connection Factory:** Identificatore della risorsa JNDI per la creazione di una connessione verso il broker JMS
- **Initial Context Factory:** Class Name per l'inizializzazione del server JNDI per la lookup della Connection Factory e della Coda
- **Url Pkg Prefixes:** Lista separata da ":" per specificare i prefissi dei package da utilizzare per l'inizializzazione del Context JNDI
- **Provider Url:** Indirizzo che localizza il server JNDI

9.8.8 Connettore File

Il connettore permette di serializzare la richiesta su FileSystem ed opzionalmente di generare una risposta.

Il connettore File supporta:

- **Richiesta**, è possibile serializzare il messaggio di richiesta su file-system fornendo un path che può contenere anche parti dinamiche risolte a runtime da GovWay. È permesso anche abilitare l'eventuale sovrascrittura del file, se risulta già esistente, e la creazione automatica delle directory padre, se non esistono.
- **Risposta**, è opzionale; se abilitata permette di generare una risposta costruita utilizzando il contenuto di un file indirizzabile a sua volta tramite gli stessi meccanismi dinamici della richiesta. Il file contenente la risposta può essere eliminato una volta consumato (opzione configurabile). L'utente può inoltre indicare un tempo di attesa (ms) qualora il file non sia immediatamente disponibile.

Facendo riferimento alla maschera raffigurata in Fig. 9.17 andiamo a descrivere il significato dei parametri:

- *Richiesta*
 - **File:** indirizzo su file-system (path) dove verrà serializzato il messaggio di richiesta. È possibile fornire delle macro per creare dei path dinamici (per ulteriori dettagli vedi sezione "Informazioni Dinamiche").
 - **File Headers** (opzionale): indirizzo su file-system (path) dove verranno serializzati gli header di trasporto associati alla richiesta. È possibile fornire delle macro per creare dei path dinamici (per ulteriori dettagli vedi sezione "Informazioni Dinamiche").
 - **Overwrite If Exists** (true/false): abilita l'eventuale sovrascrittura del file, se risulta già esistere.
 - **AutoCreate Parent Directory** (true/false): abilita la creazione automatica delle directory padre, se non esistono.
- *Risposta (Opzionale)*
 - **Generazione** (true/false): abilita la generazione di una risposta. Tutte le successive opzioni della sezione "Risposta" sono configurabili solamente se la generazione è abilitata.
 - **File:** indirizzo su file-system (path) dove verrà letto il messaggio di risposta. È possibile fornire delle macro per creare dei path dinamici, come descritto più avanti al punto «Informazioni Dinamiche».
 - **File Headers** (opzionale): indirizzo su file system (path) dove verranno letti gli header di trasporto da associare alla risposta. È possibile fornire delle macro per creare dei path dinamici, come descritto più avanti al punto «Informazioni Dinamiche».
 - **Delete After Read** (true/false): abilita l'eventuale eliminazione del file una volta utilizzato per la generazione della risposta.
 - **Wait Time If Not Exists (ms)** (opzionale): indica un tempo di attesa (ms) qualora il file per la generazione della risposta non sia immediatamente disponibile.

Connettore

Tipo	<input type="text" value="file"/>
Debug	<input type="checkbox"/>
Ridefinisci Tempi Risposta	<input type="checkbox"/>

Richiesta

File *	<input type="text" value="/tmp/request.xml"/>
File Headers	<input type="text" value="/tmp/request.hdr"/>
AutoCreate Parent Dir	<input type="checkbox"/>
Overwrite If Exists	<input type="checkbox"/>

Risposta

Generazione	<input type="text" value="abilitato"/>
File *	<input type="text" value="/tmp/response.xml"/>
File Headers	<input type="text" value="/tmp/response.hdr"/>
Delete After Read	<input type="checkbox"/>
WaitTime ifNotExists (ms)	<input type="text"/>

Fig. 9.17: Dati di configurazione di un connettore File

- *Informazioni Dinamiche.* Per creare dei path dinamici rispetto alla transazione in corso di elaborazione, possono essere utilizzate le seguenti macro:
 - **{date:FORMAT}** indica la data di elaborazione del messaggio. Il formato fornito deve essere conforme a quanto richiesto dalla classe java “java.text.SimpleDateFormat”. Ad esempio: {date:yyyyMMdd_HHmmssSSS}.
 - **{transaction:id}** indica l’identificativo della transazione (UUID).
 - **{busta:FIELD}** permette di utilizzare informazioni di protocollo riguardanti la transazione in corso. Il valore “FIELD” fornito deve rappresentare un field valido all’interno della classe di openscoop “org.openscoop2.protocol.sdk.Busta”. Ad esempio per ottenere il mittente della busta usare {busta:mittente}.
 - **{header:NAME}** permette di utilizzare informazioni, relative alla transazione in corso, inserite negli header http generati da GovWay (maggiori dettagli in sezione *Header di Integrazione*). Il valore “NAME” indica il nome dell’header da utilizzare. Ad esempio per utilizzare il nome del mittente è possibile usare {header:GovWay-Sender}. Un altro esempio valido nello scenario della fatturazione elettronica (sezione *Profilo “Fatturazione Elettronica”*) potrebbe essere quello di utilizzare il nome originale del file fattura utilizzando la sintassi {header:GovWay-SDI-NomeFile}
 - **{query:NAME}** permette di utilizzare informazioni, relative alla transazione in corso, inserite nei query parameter aggiunti all’endpoint da GovWay (maggiori dettagli in sezione *Header di Integrazione*). Il valore “NAME” indica il nome della proprietà da utilizzare. Ad esempio per utilizzare il nome del mittente è possibile usare {query:govway_sender}.
 - **{property:NAME}** permette di utilizzare informazioni, relative alla transazione in corso, specifiche della sezione relativa al profilo utilizzato all’interno della traccia (es. sezione “Informazioni Fatturazione Elettronica”). Il valore “NAME” indica il nome della proprietà da utilizzare. Un esempio valido nello scenario della fatturazione elettronica (sezione *Profilo “Fatturazione Elettronica”*) potrebbe essere quello di utilizzare l’identificativo sdi utilizzando la sintassi {property:IdentificativoSdI}

9.9 Correlazione tra transazioni differenti

Richiede accesso alla govwayConsole in modalità *avanzata* (sezione *Modalità Avanzata*).

Come descritto anche nella sezione *Configurazione manuale delle interfacce*, durante la configurazione di un API di tipo SOAP o REST è possibile specificare i parametri descritti di seguito rispettivamente in un servizio/azione o in una 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.

Tali parametri consentono agli applicativi client di fornire tali informazioni tramite gli header di integrazione descritti nella sezione *Scambio di informazioni nella richiesta del client verso il gateway*

Le informazioni fornite saranno associate alla traccia della transazione gestita, e quindi utilizzabili in fase di monitoraggio tramite le modalità di ricerca basate su identificativi descritte nella Guida alla Console di Monitoraggio.

9.10 Autenticazione e Autorizzazione Principal (Security Constraint)

In precedenza, relativamente alla configurazione del controllo degli accessi, ed in particolare del meccanismo di autenticazione, si è indicata anche la possibilità di utilizzare il tipo *principal*. Questa configurazione richiede che l’autenti-

cazione sia delegata all'application server o qualunque altra modalità che permetta a GovWay di accedere al principal tramite la api *HttpServletRequest.getUserPrincipal()*.

In precedenza, relativamente all'autorizzazione, si è descritta la possibilità di utilizzare ruoli con fonte *esterna*. Questa fonte richiede che la gestione dei ruoli sia delegata all'Application Server o a qualunque altra modalità che permetta a GovWay di accedere ai ruoli tramite la api *HttpServletRequest.isUserInRole()*.

Le modalità di configurazione di utenti e ruoli sull'application server variano in funzione della versione utilizzata e pertanto si rimanda alla documentazione del prodotto.

È inoltre richiesto che l'applicazione utente sia protetta tramite un *security-constraint*. A tale scopo l'installazione di GovWay dispone di un contesto built-in *govwaySec* (definito nel war *govwaySec.war/WEB-INF/web.xml*) protetto tramite security constraint con metodo di autenticazione *HTTP-BASIC*:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>AuthenticationContainer</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>*</role-name>
    </auth-constraint>
</security-constraint>

...
<security-role>
    <role-name>*</role-name>
</security-role>

<login-config>
    <auth-method>BASIC</auth-method>
</login-config>
```

Se si intende utilizzare una configurazione differente di quella built-in si deve procedere con la modifica di tale descrittore web.xml presente all'interno dell'archivio.

Nota: Con questo tipo di configurazione, le URL che gli applicativi devono invocare devono essere adeguate sostituendo il contesto *govway* con *govwaySec*.

9.11 Espressioni XPath su messaggi JSON

In diverse funzionalità (*Correlazione Applicativa*, *Registrazione di una policy*, *Modalità di identificazione dell'azione*) è stata documentato la possibilità di utilizzare espressioni jsonPath o XPath per estrarre contenuti dai messaggi JSON o XML in transito sul Gateway.

L'estrazione dei contenuti da messaggi JSON si basa su espressioni JSONPath che allo stato attuale non hanno la stessa «potenza» delle espressioni XPath. Ad esempio:

- non è possibile ottenere il nome di un claim, come invece in XPath è possibile ottenere il local-name di un elemento tramite la funzione “local-name”
- non si dispongono delle complesse funzioni per le elaborazioni sulle stringhe (ad es. in xpath è disponibile la funzione “substring-before”)
- ...

Per ovviare a tali limitazioni GovWay fornisce la possibilità di utilizzare espressioni XPath su messaggi JSON attraverso la seguente sintassi:

```
xpath [namespace(prefix1:uri1, ... ,prefixN:uriN) ] <espressioneXPathStandard>
```

Nel caso il gateway rilevi una espressione che inizi con il prefisso “xpath” da applicare su un messaggio JSON, effettua una trasformazione del messaggio in una rappresentazione xml. Ad esempio per il messaggio JSON:

```
{
    "prova": "test1",
    "prova2": 23
}
```

Per estrarre il valore del field “prova” è possibile utilizzare le seguenti espressioni, la prima jsonPath e le successive xpath:

- \$.prova
- xpath //prova/text()
- xpath /json2xml/prova/text()

Le espressioni xpath sono utilizzabili poichè il messaggio JSON viene convertito nel seguente messaggio xml (inserito all'interno dell'elemento radice “json2xml”):

```
<json2xml>
    <prova>test1</prova>
    <prova2>23</prova2>
</json2xml>
```

Mentre nell'esempio precedente sono sufficienti le funzionalità offerte dal jsonPath per estrarre il valore del field “prova”, ricorrere all'utilizzo di xPath è necessario se ad esempio vogliamo ottenere il nome di un field. Nell'esempio seguente l'espressione fornita consente di estrarre il nome dell'ultimo field presente nella struttura json “prova2”. Tale risultato è ottenibile solamente utilizzando l'espressione xPath:

```
xpath local-name(/json2xml/*[last()])
```

In alcuni contesti i servizi REST non vengono implementati a partire da interfacce progettate ad hoc (OpenAPI, Swagger...) ma sono frutto di una trasformazioni di esistenti servizi SOAP. In questi scenari, i servizi REST veicolano messaggi JSON ottenuti attraverso la trasformazione dei relativi messaggi XML utilizzati su SOAP. Per poter utilizzare espressioni xPath devono essere affrontate le problematiche di risoluzione dei prefissi e dei namespace. In questi contesti i messaggi JSON presenteranno field che possiedono nel nome il carattere “:” ereditato dalla rappresentazione xml. Di seguito un esempio di messaggio json ottenuto da una trasformazione di un messaggio xml equivalente:

```
{
    "m:NomeAzioneTestRequest": {
        "bodyWithNS" : "true",
        "xmlns:m" : "http://testNamespace",
        "prodotto" : {
            "codice" : "26",
            "altro:codice3" : "34",
            "xmlns:altro" : "http://testNamespaceAltro"
        }
    }
}
```

Supponendo di voler estrarre il nome del field “NomeAzioneTestRequest” e da questo eliminare anche il suffisso “Request” è possibile utilizzare la seguente espressione xPath:

```
xpath namespace(m:http://testNamespace, altro:http://altro) substring-before(local-
˓→name(//json2xml/*), \"Request\")
```

Si può notare come tra il prefisso “xpath” e l'espressione xpath vera e propria (`substring-before(...)`) siano stati definiti i namespace che coinvolgono i field presenti nella struttura json che avevano il carattere “:”.

La struttura xml, ottenuta dalla conversione del messaggio json, su cui viene applicata l'espressione xpath è la seguente:

```
<json2xml xmlns:m="http://testNamespace" xmlns:altro="http://altro" xmlns:__xmlns=
˓→"http://govway.org/utils/json2xml/xmlns">
    <m:NomeAzioneTestRequest>
        <bodyWithNS>true</bodyWithNS>
        <__xmlns:m>http://testNamespace</__xmlns:m>
        <prodotto>
            <codice>26</codice>
            <altro:codice3>34</altro:codice3>
            <__xmlns:altro>http://testNamespaceAltro</__xmlns:altro>
        </prodotto>
    </m:NomeAzioneTestRequest>
</json2xml>
```

Nota: Il prefisso “`xmlns:`” viene gestito automaticamente da GovWay, il quale gli associa un namespace di default “<http://govway.org/utils/json2xml/xmlns>”. Tale namespace è possibile ridefinirlo aggiungendo all'elenco dei namespace anche un mapping per “`xmlns`”.
