

---

# **Scenari Applicativi**

***Release 3.3.0.rc1***

**07 mar 2020**



---

## Indice

---

|                                  |           |
|----------------------------------|-----------|
| <b>1 Ambiente di esecuzione</b>  | <b>1</b>  |
| 1.1 Prerequisiti . . . . .       | 1         |
| 1.2 Avvio Ambiente . . . . .     | 1         |
| 1.3 Progetto Postman . . . . .   | 3         |
| <b>2 Erogazione pubblica</b>     | <b>11</b> |
| 2.1 Obiettivo . . . . .          | 11        |
| 2.2 Sintesi . . . . .            | 11        |
| 2.3 Esecuzione . . . . .         | 11        |
| 2.4 Configurazione . . . . .     | 11        |
| <b>3 Erogazione OAuth</b>        | <b>17</b> |
| 3.1 Obiettivo . . . . .          | 17        |
| 3.2 Sintesi . . . . .            | 17        |
| 3.3 Esecuzione . . . . .         | 17        |
| 3.4 Configurazione . . . . .     | 21        |
| <b>4 Erogazione REST ModI PA</b> | <b>27</b> |
| 4.1 Obiettivo . . . . .          | 27        |
| 4.2 Sintesi . . . . .            | 27        |
| 4.3 Esecuzione . . . . .         | 29        |
| 4.4 Configurazione . . . . .     | 33        |
| <b>5 Fruizione REST ModI PA</b>  | <b>39</b> |
| 5.1 Obiettivo . . . . .          | 39        |
| 5.2 Sintesi . . . . .            | 39        |
| 5.3 Esecuzione . . . . .         | 41        |
| 5.4 Configurazione . . . . .     | 44        |
| <b>6 Erogazione SOAP ModI PA</b> | <b>47</b> |
| 6.1 Obiettivo . . . . .          | 47        |
| 6.2 Sintesi . . . . .            | 47        |
| 6.3 Esecuzione . . . . .         | 48        |
| <b>7 Fruizione SOAP ModI PA</b>  | <b>53</b> |
| 7.1 Obiettivo . . . . .          | 53        |
| 7.2 Sintesi . . . . .            | 53        |

|          |                                |           |
|----------|--------------------------------|-----------|
| 7.3      | Esecuzione                     | 55        |
| <b>8</b> | <b>Monitoraggio</b>            | <b>57</b> |
| 8.1      | Transazione in errore          | 58        |
| 8.2      | Transazione con esito corretto | 58        |

# CAPITOLO 1

---

## Ambiente di esecuzione

---

Per semplificare la realizzazione e verifica degli scenari d'uso, descritti in questa sezione della documentazione di Govway, è possibile dotarsi dell'ambiente di esecuzione appositamente predisposto.

### 1.1 Prerequisiti

Per l'avvio dell'ambiente di esecuzione degli scenari è necessario disporre del seguente software di base:

- Dotarsi di una installazione **Docker** che gestirà l'intero contesto di esecuzione degli scenari
- Dotarsi dell'applicativo **Postman** utilizzato come client per l'invio delle richieste a Govway

L'ambiente di esecuzione è composto da:

- Ambiente Docker Compose preinizializzato con gli scenari descritti in questo manuale.
- Progetto Postman configurato per verificare gli scenari.

---

**Nota:** Gli scenari configurati sull'ambiente docker devono poter accedere ai seguenti servizi su internet:

- Petstore: <http://petstore.swagger.io/>
  - Credit Card Verification: <http://ws.cdyne.com/creditcardverify/luhnchecker.asmx>
- 

### 1.2 Avvio Ambiente

Dopo aver scompattato l'"archivio, indicato nei prerequisiti, sarà possibile avviare un ambiente tramite docker compose preinizializzato per gli scenari descritti nel manuale. Di seguito vengono forniti tutti i passaggi da effettuare per ottenere un ambiente funzionante:

- **Archivio:** scompattare l'"archivio nella cartella di destinazione scelta per ospitare l'ambiente di esecuzione degli scenari.

- *Hostname*: l’ambiente è configurato per utilizzare l’hostname “govway.localdomain”. Configurare una risoluzione dell’hostname ad esempio registrando nel file /etc/hosts l’entry:

```
127.0.0.1      govway.localdomain
```

- *Ambiente Docker*: avviare l’ambiente docker compose utilizzando lo script “starttest.sh” presente all’interno della cartella di destinazione dell’ambiente (Fig. 1.1).

```
[root@poli-nb18 AmbienteDocker]# ./starttest
Starting goauth ...
Starting spid_testenv ...
Starting goauth
Starting ambientedocker_init_1 ...
Starting ambientedocker_init_1
Starting ambientedocker_init_1 ... done
Starting PGSQL95 ...
Starting gatewaystenv ... done
Starting PGSQL95 ... done
Starting keycloak ...
Starting keycloak ... done
Starting traefik ...
Starting traefik ... done
```

Fig. 1.1: Schermata di avvio «docker-compose up»

I componenti avviati sono i seguenti:

- gateway: l’istanza di Govway
- PGSQL95: il database Postgres
- keycloak: l’authorization server
- traefik: il load balancer

---

**Nota:** Lo script “starttest.sh” si occupa di inizializzare due variabili di ambiente prima di avviare l’ambiente tramite il comando “*docker-compose up*”:

- SERVER\_FQDN: definisce l’hostname dell’ambiente (negli esempi govway.localdomain)
  - LOCAL\_DATA: directory contenente gli storage locali utilizzate dalle immagini docker avviate dal compose (l’archivio fornisce già la directory ./data)
- 

Dopo aver avviato l’ambiente è possibile verificare l’accesso alle seguenti console:

- *GovWay - Console di Gestione*: permette di visualizzare le configurazioni realizzate su Govway (Fig. 1.2).

```
endpoint: https://govway.localdomain/govwayConsole/
username: amministratore
password: 123456
```

- *GovWay - Console di Monitoraggio*: permette di consultare le transazioni gestite da Govway (Fig. 1.3).



Fig. 1.2: Accesso alla console di gestione

```
endpoint: https://govway.localdomain/govwayMonitor/
username: operatore
password: 123456
```

- *Keycloak - Authorization Server*: permette di consultare le configurazioni realizzate sull'Authorization Server Keycloak (Fig. 1.4).

```
endpoint: https://govway.localdomain/auth/
username: admin
password: admin
```

## 1.3 Progetto Postman

La collezione Postman comprende tutte le configurazioni utilizzate nei vari scenari presentati (Fig. 1.5). La collection deve essere caricata sul proprio Postman tramite la funzionalità di import.

Una volta effettuato il caricamento della collezione, modificare i parametri della collezione (Fig. 1.6) al fine di indicare nella variabile “*hostname*” (Fig. 1.7) l’indirizzo ip su cui è stato attivato l’immagine docker compose (per default è presente 127.0.0.1).

Infine accedere alla configurazione generale di Postman (Fig. 1.8) ed assicurarsi che la voce “*SSL Certificate Verification*” nella maschera “*General*” sia disabilitata (Fig. 1.9) e che non vi sia impostato un proxy nella maschera “*Proxy*” (Fig. 1.10).



Fig. 1.3: Accesso alla console di monitoraggio

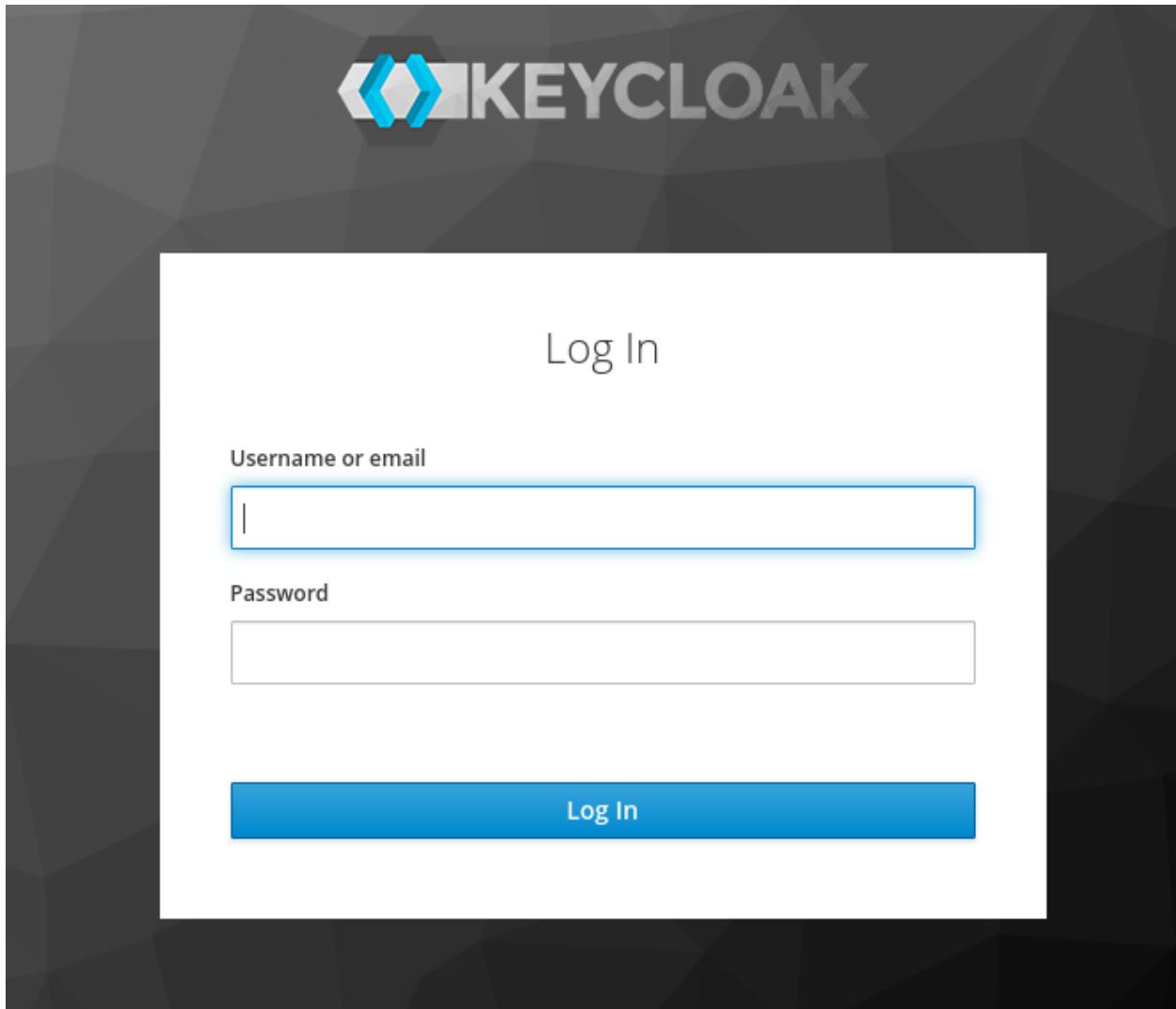


Fig. 1.4: Accesso alla console dell'authorization server

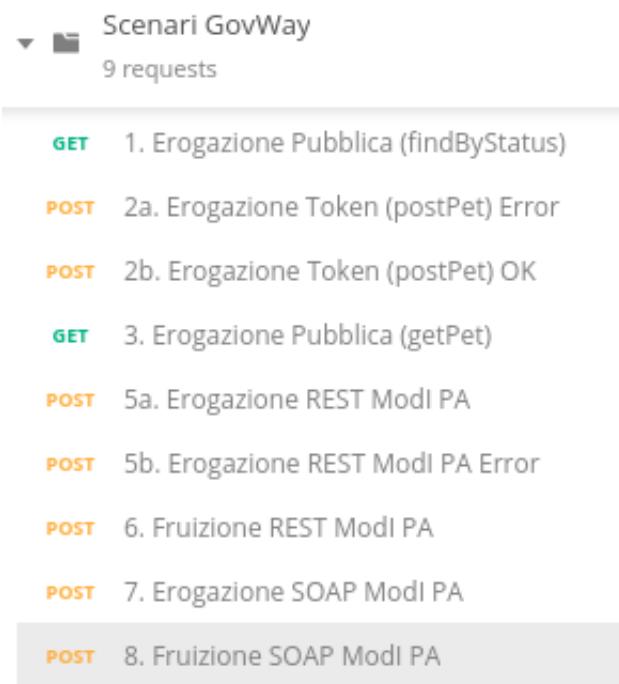


Fig. 1.5: Indice della collection Postman

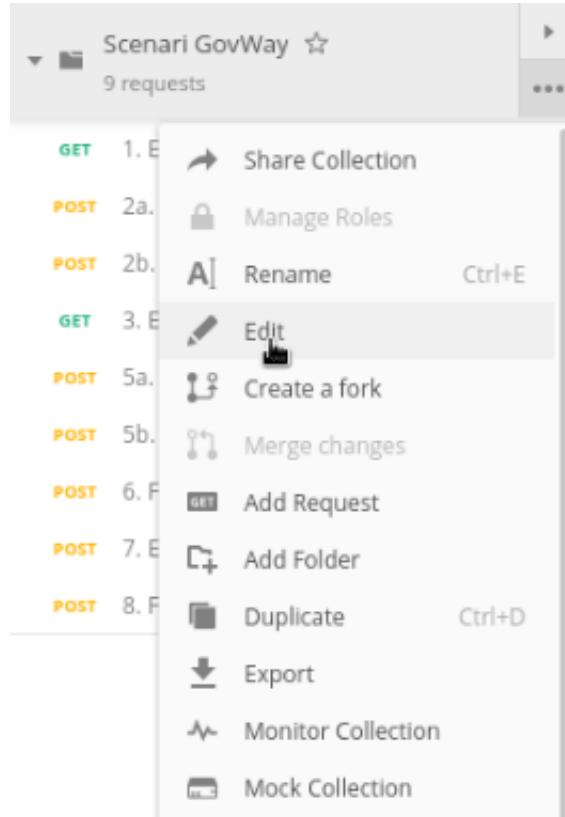


Fig. 1.6: Configurazione Collection Postman

EDIT COLLECTION X

Name  
Scenari GovWay

Description    Authorization    Pre-request Scripts    Tests    **Variables** ●

These variables are specific to this collection and its requests. [Learn more about collection variables.](#)

|                                     | VARIABLE               | INITIAL VALUE <span style="color: blue;">i</span> | CURRENT VALUE <span style="color: blue;">i</span> | ... | Persist All | Reset All |
|-------------------------------------|------------------------|---|---|-----|-------------|-----------|
| <input checked="" type="checkbox"/> | hostname               | 127.0.0.1   | 127.0.0.1   |     |             |           |
| <input checked="" type="checkbox"/> | govway-url             | https://{{hostname}}/go...                        | https://{{hostname}}/govway                       |     |             |           |
| <input checked="" type="checkbox"/> | soggetto               | Ente  | Ente  |     |             |           |
| <input checked="" type="checkbox"/> | soggettoEsterno        | EnteEsterno                                       | EnteEsterno                                       |     |             |           |
| <input checked="" type="checkbox"/> | keycloak-url-auth      | https://{{hostname}}/aut...                       | https://{{hostname}}/auth/realm...                |     |             |           |
| <input checked="" type="checkbox"/> | keycloak-url-token     | https://{{hostname}}/aut...                       | https://{{hostname}}/auth/realm...                |     |             |           |
| <input checked="" type="checkbox"/> | keycloak-client-id     | oauth2-app1                                       | oauth2-app1                                       |     |             |           |
| <input checked="" type="checkbox"/> | keycloak-client-secret | fd5f09fa-028d-461b-8e4f...                        | fd5f09fa-028d-461b-8e4f-063c111c069f              |     |             |           |

i Use variables to reuse values in different places. Work with the current value of a variable to prevent sharing sensitive values with your team. [Learn more about variable values](#) X

Cancel Update

Fig. 1.7: Configurazione Hostname nella Collection Postman

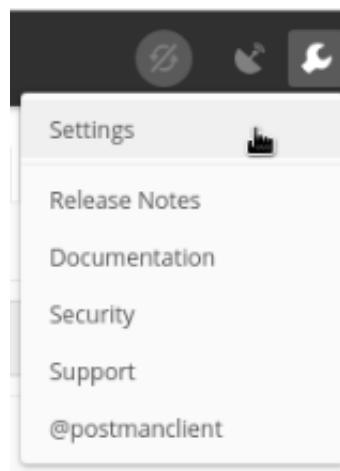


Fig. 1.8: Configurazione Generale Postman

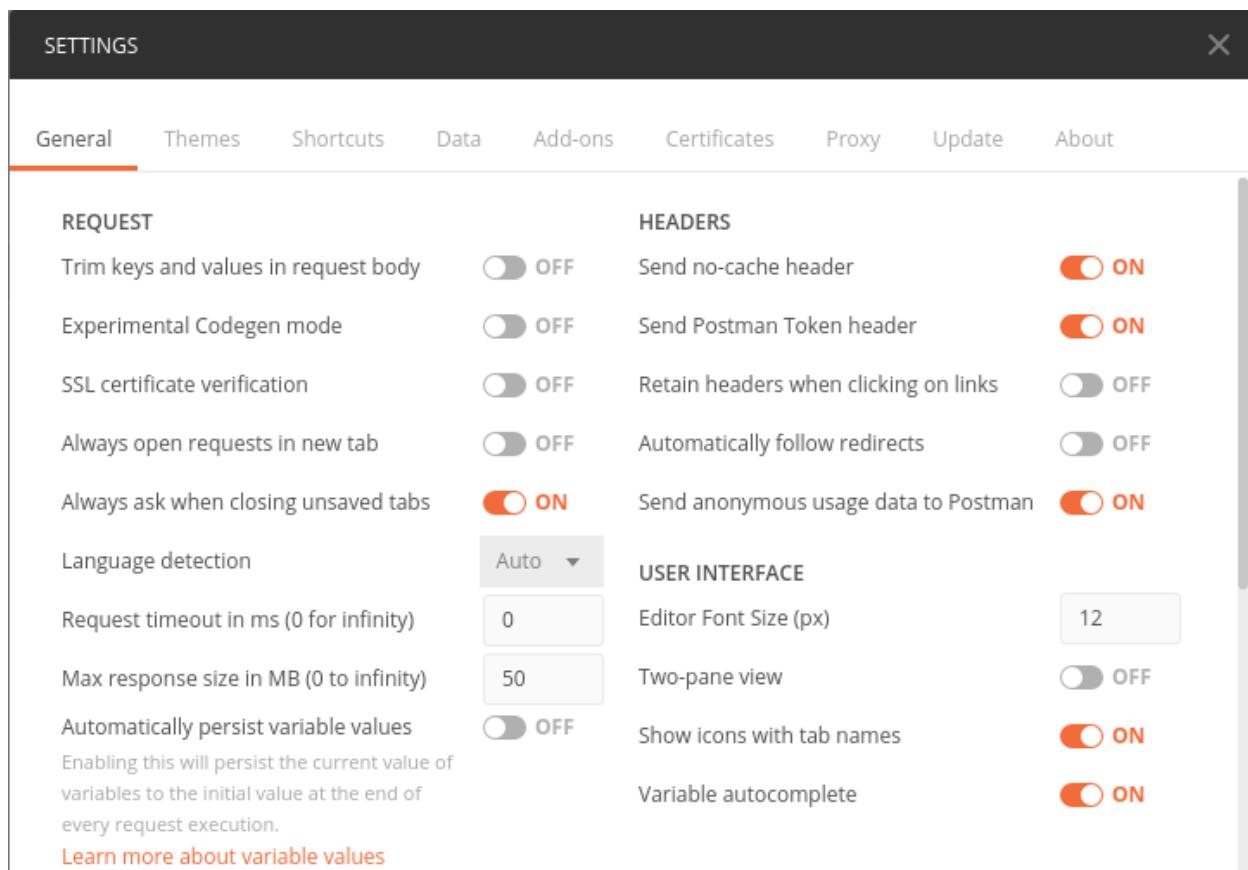


Fig. 1.9: Configurazione SSL Postman

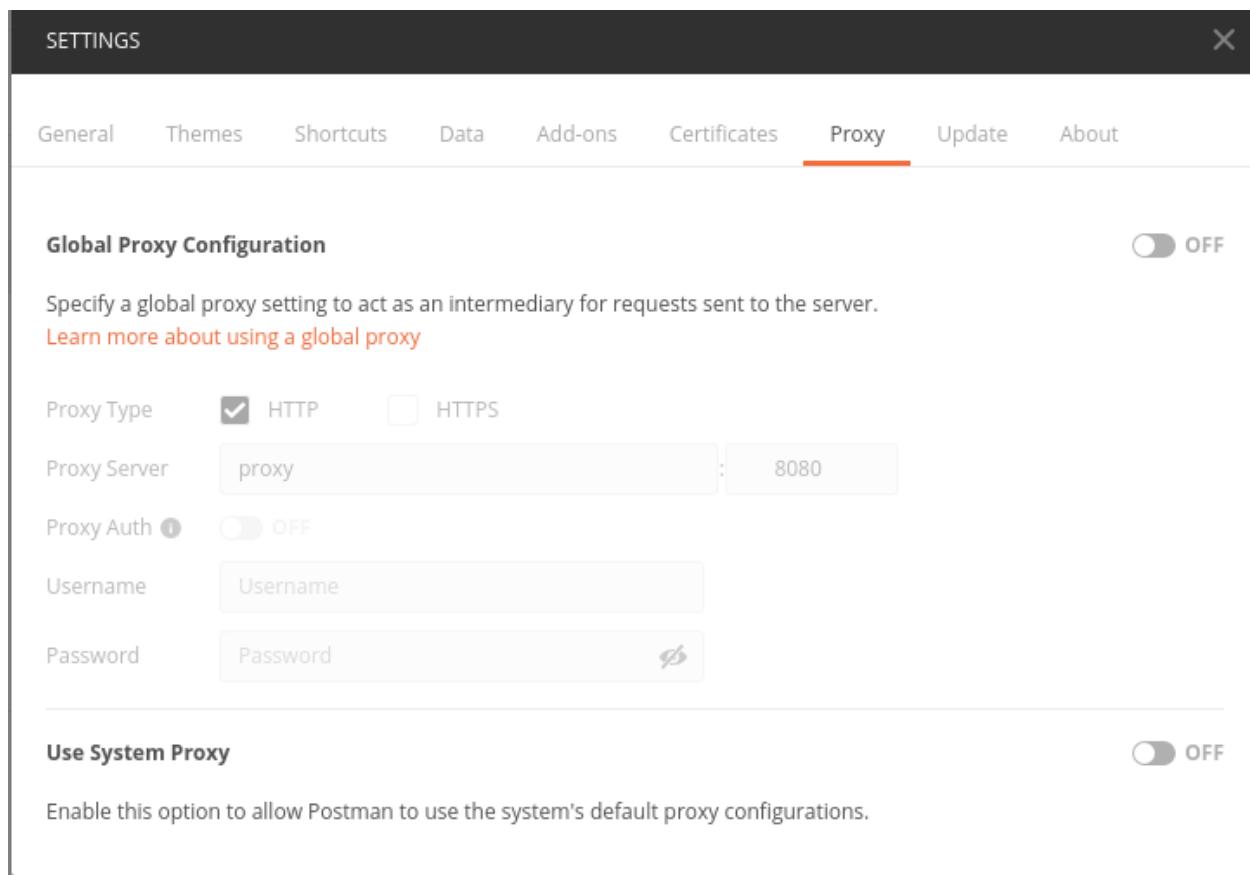


Fig. 1.10: Configurazione Proxy Postman



# CAPITOLO 2

---

## Erogazione pubblica

---

### 2.1 Obiettivo

Esporre tramite Govway un servizio con accesso pubblico (forma anonima).

### 2.2 Sintesi

In questo scenario è richiesta l'esposizione tramite gateway di un servizio da erogare, consentendo il libero accesso ai fruitori, che potranno invocare la relativa interfaccia senza presentare alcuna credenziale.

Per illustrare questo scenario, abbiamo scelto il servizio «PetStore», che sarà reso accessibile da Govway tramite l'interfaccia REST in versione OpenAPI 3.

La figura seguente descrive graficamente questo scenario.

### 2.3 Esecuzione

I fruitori del servizio «PetStore» invocano le operazioni disponibili tramite i propri client senza utilizzare alcuna forma di autenticazione. Avvalendosi eventualmente del progetto Postman a corredo, eseguire «*1. Erogazione Pubblica (findByStatus)*» per verificare l'esecuzione dell'erogazione del servizio PetStore con libero accesso.

### 2.4 Configurazione

Procediamo con la configurazione dell'erogazione del servizio «PetStore», pubblicamente accessibile, assumendo che la relativa API sia stata precedentemente configurata con il proprio descrittore OpenAPI 3 (descrit-

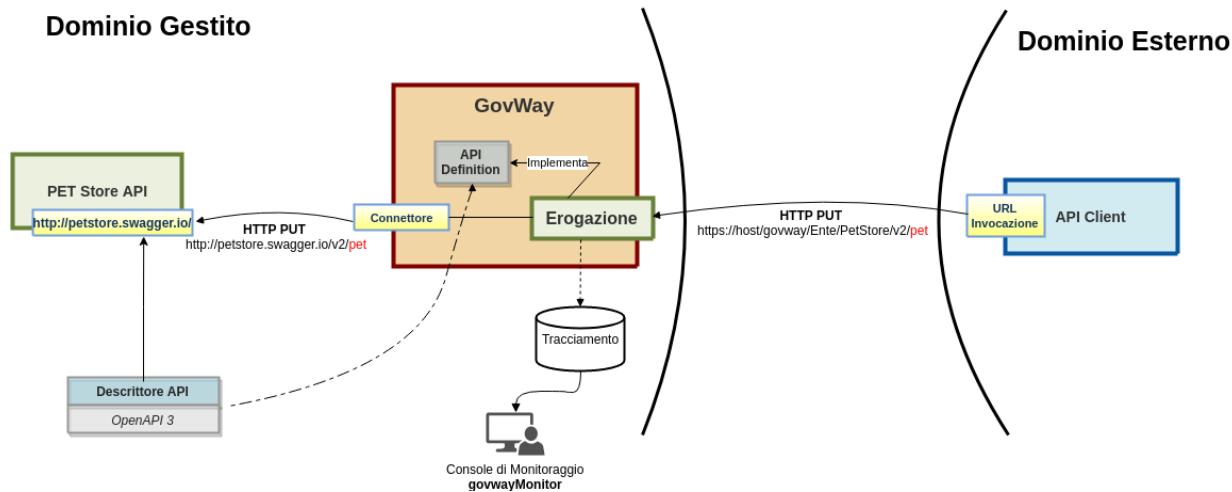


Fig. 2.1: Erogazione ad accesso pubblico

tore scaricabile al seguente indirizzo: <https://raw.githubusercontent.com/Mermade/openapi3-examples/master/fail/apimatic-converted-petstore.json>.

La configurazione si effettua dalla govwayConsole, nella sezione «Erogazione > Aggiungi» (Fig. 2.3):

1. Selezionare l'API «PetStore v1» nel riquadro delle Informazioni Generali.
2. Selezionare l'accesso API «pubblico» nel riquadro Controllo dei Accessi.
3. Verificare che il campo «Endpoint», nel riquadro Connettore, sia stato correttamente inizializzato sulla base del valore di default presente nel descritto della API.
4. Salvare la configurazione dell'erogazione.
5. Nel dettaglio dell'erogazione appena creata è possibile visualizzare la URL di invocazione che deve essere comunicata ai fruitori affinché possano invocare il servizio (Fig. 2.4).

The screenshot shows the Postman application interface. At the top, there is a header bar with the title "Scenari Applicativi, Release 3.3.0.rc1". Below the header, a navigation bar includes links for "Home", "Scenari", "Progetti", "Analisi", "Report", "Configurazione", and "Help". A search bar is also present.

The main workspace displays a collection named "1. Erogazione Pubblica (findBy...)" with one item: "1. Erogazione Pubblica (findByStatus)".

The request details are as follows:

- Method:** GET
- URL:** {{govway-url}}/{{soggetto}}/PetStore/v1/pet/findByStatus?status=available
- Params:** status = available
- Headers:** (9)
- Body:** (empty)
- Cookies:** (empty)
- Headers (11):** (empty)
- Test Results:** (empty)

The status bar at the bottom indicates "Status: 200 OK" and "Time: 0ms".

The response body is displayed in a JSON editor:

```
1
2 {
3     "id": 4,
4     "category": {
5         "id": 1,
6         "name": "Dogs"
7     },
8     "name": "Dog 1",
9     "photoUrls": [
10        "url1",
11        "url2"
12    ],
13 }
```

Fig. 2.2: Erogazione pubblica, esecuzione da Postman

Erogazioni > Aggiungi

Note: (\*) Campi obbligatori

**Informazioni Generali**

**API**

Nome: PetStore v1

Tipo: Rest

**Controllo degli Accessi**

Accesso API: pubblico

**Connettore**

Endpoint \*: http://petstore.swagger.io/v2

Autenticazione Http:

Autenticazione Token:

AutenticazioneHttps:

Proxy:

Ridefinisci Tempi Risposta:

**SALVA**

Fig. 2.3: Creazione di un'erogazione ad accesso pubblico

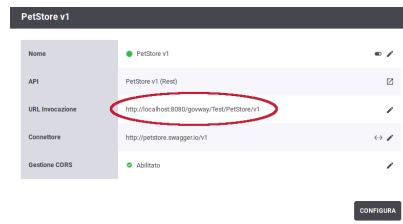


Fig. 2.4: Dettaglio dell'erogazione



# CAPITOLO 3

---

## Erogazione OAuth

---

### 3.1 Obiettivo

Esporre un servizio accessibile tramite protocollo OAuth2 (Authorization Code).

### 3.2 Sintesi

Assumendo che sia stata effettuata la configurazione di un’erogazione ad accesso pubblico (vedi scenario *Erogazione pubblica*), verifichiamo in questo scenario come impostare il sistema di controllo degli accessi affinché il servizio richieda un token di sicurezza, come previsto dal protocollo OAuth2. In particolare la limitazione dell’accesso sarà configurata solo per le operazioni di scrittura, lasciando libero accesso per le letture.

La figura seguente descrive graficamente questo scenario.

I passi previsti sono i seguenti:

1. Il client entra in possesso del token, previa autenticazione e consenso dell’utente richiedente.
2. Il client utilizza il token per l’invio della richiesta.
3. Govway valida il token ricevuto e verifica i criteri di controllo degli accessi.
4. Se la validazione è superata, Govway inoltra la richiesta al servizio erogatore.

### 3.3 Esecuzione

Facendo riferimento al progetto Postman è possibile verificare direttamente l’esecuzione dei passi di questo scenario. Passi da eseguire:

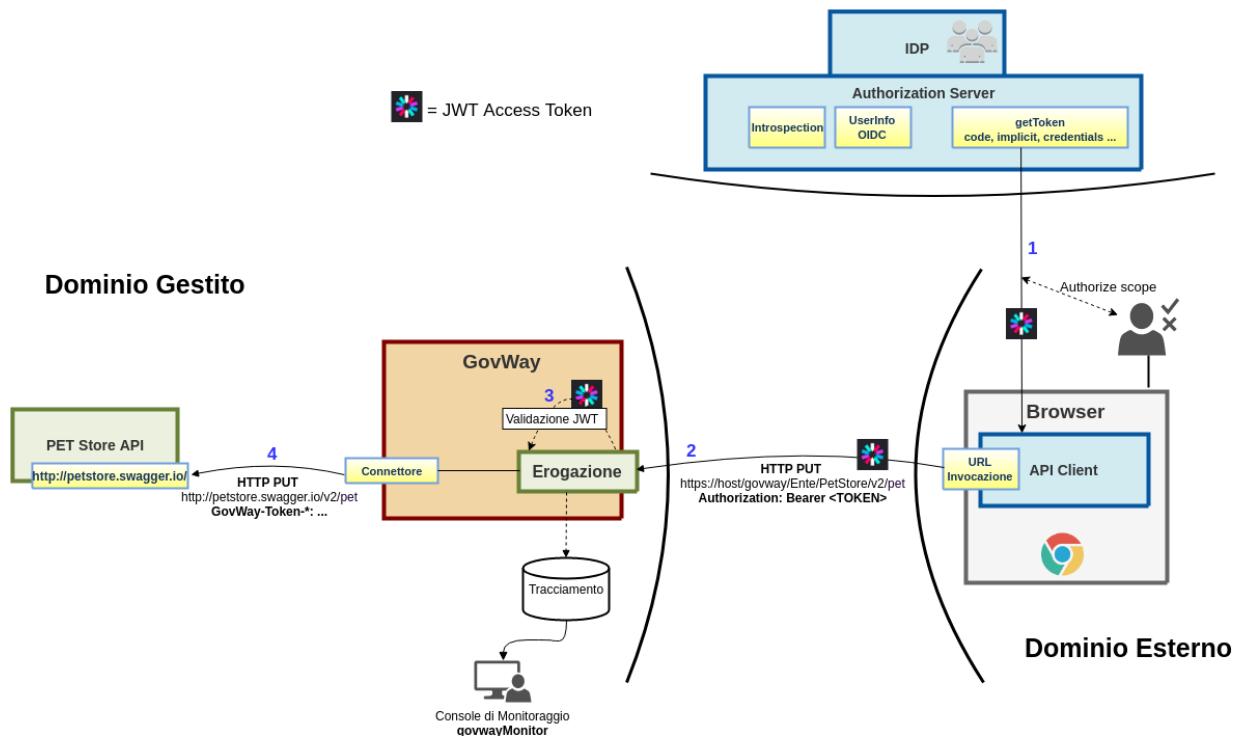


Fig. 3.1: Erogazione OAuth

1. All'inizio possiamo verificare come il client non riesca ad accedere al servizio senza l'utilizzo del token. La request «2a. Erogazione Token (postPet) Error» effettua una chiamata alla risorsa «POST /pet» in assenza del token richiesto. Govway respinge la richiesta con la restituzione dell'errore mostrato in Fig. 3.2.
2. Successivamente si passa alla chiamata della «POST /pet» seguendo il flusso OAuth2 richiesto per l'approvvigionamento del token di autorizzazione. Posizionarsi sulla request «2b. Erogazione Token (postPet) OK»:
  - Nella sezione «Authorization» selezionare il Type «OAuth 2.0» e premere il pulsante «Get New Access Token»
  - La maschera fornita (Fig. 3.3) deve essere compilata con i parametri necessari ad richiedere un token all'authorization server. Utilizzare i seguenti parametri che permettono di richiedere un token all'authorization server preconfigurato per lo scenario:

```

Callback URL: {{keycloak-callback-url}}
Auth URL: {{keycloak-url-auth}}
Access Token URL: {{keycloak-url-token}}
Client ID: {{keycloak-client-id}}
Client Secret: {{keycloak-client-secret}}

```

- Compilati correttamente i campi per ottenere un token cliccare sul pulsante «Request Token»
- Completare il processo di autenticazione dell'utente seguendo il flusso proposto ed utilizzando le credenziali dell'utente preconfigurato sull'authorization server per lo scenario di test:

```

username: paolorossi
password: 123456

```

The screenshot shows the Postman application interface. At the top, there is a header bar with the text "POST 2a. Erogazione Token (postPe... X)" and three buttons: a plus sign (+), a three-dot menu (•••), and a close button (X). Below the header, a section titled "▶ 2a. Erogazione Token (postPet) Error" is expanded. The main request configuration area shows a "POST" method selected from a dropdown and the URL template "{{govway-url}}/{{soggetto}}/PetStore/v1/pet". Below this, a tab bar has "Params" selected, followed by "Authorization", "Headers (9)", "Body ●", and "Pre-request Script". Under the "Params" tab, there is a table with one row labeled "Key" and "Key". In the "Body" tab, which is currently active, there are four sub-options: "Pretty", "Raw", "Preview", and "JSON". The "JSON" option is selected and has a dropdown arrow. Below these options, a JSON response is displayed with line numbers 1 through 7:

```
1 {  
2   "type": "https://httpstatuses.com/400",  
3   "title": "Bad Request",  
4   "status": 400,  
5   "detail": "Token non presente",  
6   "govway_status": "protocol:GOVWAY-1366"  
7 }
```

Fig. 3.2: Invocazione della POST /pet senza token

GET NEW ACCESS TOKEN X

|   |  |
|---|--|
| Token Name  | <input type="text"/>   |
| Grant Type  | Authorization Code <span style="float: right;">▼</span>        |
| Callback URL <span style="color: red;">!</span>     | <input type="text"/> {{keycloak-callback-url}}                 |
| Auth URL <span style="color: red;">!</span>         | <input type="text"/> {{keycloak-url-auth}}                     |
| Access Token URL <span style="color: red;">!</span> | <input type="text"/> {{keycloak-url-token}}                    |
| Client ID <span style="color: red;">!</span>        | <input type="text"/> {{keycloak-client-id}}                    |
| Client Secret <span style="color: red;">!</span>    | <input type="text"/> {{keycloak-client-secret}}                |
| Scope <span style="color: red;">!</span>            | <input type="text"/> e.g. read:org                             |
| State <span style="color: red;">!</span>            | <input type="text"/> State                                     |
| Client Authentication                               | Send as Basic Auth header <span style="float: right;">▼</span> |
| <input type="button" value="Request Token"/>        |  |

Fig. 3.3: Ottenimento nuovo token

- Superata l'autenticazione, viene restituito l'access token (mostrato a video sulla finestra popup).
  - Inserire il token nella richiesta premendo il pulsante «Use Token».
  - Eseguire la richiesta tramite il pulsante «Send».
  - L'operazione viene eseguita con successo e restituito l'esito ([Fig. 3.4](#)).
3. Possiamo verificare che le limitazioni sull'accesso non sono efficaci nel caso di invocazione di operazioni di lettura. Il passo «3. Erogazione Pubblica (getPet)» esegue una GET. Si noti come la sezione Authorization abbia l'impostazione del Type su «No Auth». Questa request legge il dato creato con la POST precedente e, come è possibile riscontrare al termine dell'esecuzione, viene correttamente eseguita in assenza di credenziali.

## 3.4 Configurazione

Per effettuare le configurazioni necessarie al funzionamento dello scenario partiamo dall'erogazione già configurata con accesso pubblico. Si procede quindi con i passi di configurazione finalizzati a limitare l'accesso alle sole operazioni di scrittura. Per fare questo si eseguono i seguenti passi sulla govwayConsole:

1. Dal dettaglio dell'erogazione, si procede con la creazione di una nuova configurazione, cui diamo il nome «Scritture» ([Fig. 3.5](#)).
  - Selezionare dall'elenco delle risorse quelle che riguardano operazioni di scrittura (POST, PUT, DELETE)
  - Indicare per la *Modalità* il valore «Nuova» e quindi selezionare «autenticato» nel campo *Accesso API*
2. Nella nuova configurazione «Scritture» si va ad aggiornare la sezione «Controllo Accessi» effettuando le seguenti azioni ([Fig. 3.6](#)):
  - Abilitare l'autenticazione token selezionando la policy «KeyCloak» (configurazione preesistente per l'integrazione all'authorization server), lasciando invariate le altre opzioni del medesimo riquadro.
  - Disabilitare le altre funzionalità di controllo degli accessi: Autenticazione Trasporto, Autorizzazione e Autorizzazione Contenuti.
3. Dopo aver salvato la nuova configurazione, verificare il riepilogo delle informazioni, che devono corrispondere a quanto riportato in [Fig. 3.7](#).

The screenshot shows the Postman application interface. At the top, there is a header bar with a red button labeled "POST 2b. Erogazione Token (postPet...)" and a "Test" button. Below the header, the main interface has a "POST" method selected and the URL "{{govway-url}}/{{soggetto}}/PetStore/v1/pet". A "Send" button is on the right.

The "Authorization" tab is active, showing "OAuth 2.0" selected. To the right, there is a box containing an access token: "eyJhbGciOiJSUzI1NiIsInR5cIgOIA...". A "Get New Access Token" button is available. Below this, a note says: "The authorization data will be automatically generated when you send the request. [Learn more about authorization](#)".

The "Body" tab is active at the bottom, showing a JSON response:

```

1   [
2     "id": 32,
3     "category": {
4       "id": 0,
5       "name": "Alano"
6     },
7     "name": "Leo",
8     "photoUrls": [
9       "string"
10    ],
11    "tags": [
12      {
13        "id": 0,
14        "name": "pelo corto"
15      }
16    ],
17    "status": "available"
18  ]

```

The status bar at the bottom indicates: Status: 200 OK Time: 734ms Size: 593 B Save.

Fig. 3.4: Invocazione della POST /pet con token

Erogazioni > PetStore v1 (Test) > Configurazione > Aggiungi

Note: (\*) Campi obbligatori

**Configurazione**

Nome Gruppo \*

Risorse \*  POST /pet  
 PUT /pet  
 GET /pet/findByStatus  
 GET /pet/findByTags  
 DELETE /pet/{petId}  
 GET /pet/{petId}  
 POST /pet/{petId}  
 POST /pet/{petId}/uploadImage  
 GET /store/inventory  
 POST /store/order

Modalità

**Controllo degli Accessi**

Accesso API

**SALVA**

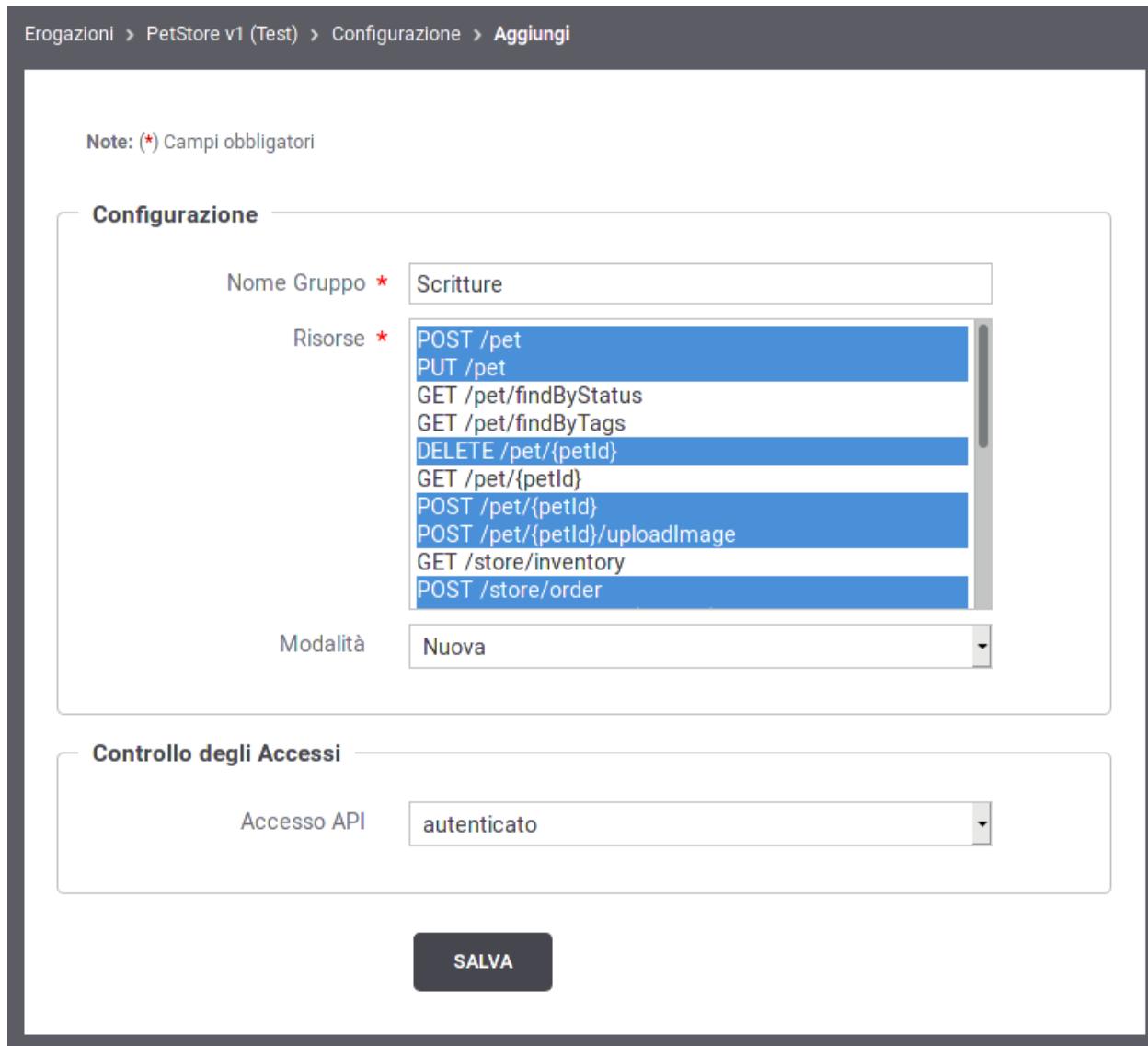


Fig. 3.5: Creazione di una configurazione specifica per le operazioni di scrittura

Erogazioni > PetStore v1 (Test) > Configurazione > Controllo Accessi del gruppo 'Scrittura'

## Controllo Accessi del gruppo 'Scrittura'

Note: (\*) Campi obbligatori

**Autenticazione Token**

|                 |                          |
|-----------------|--------------------------|
| Stato           | abilitato                |
| Policy *        | Keycloak                 |
| Token Opzionale | <input type="checkbox"/> |
| Validazione JWT | abilitato                |
| Token Forward   | abilitato                |

**Required Claims**

|          |                          |
|----------|--------------------------|
| Issuer   | <input type="checkbox"/> |
| ClientId | <input type="checkbox"/> |
| Subject  | <input type="checkbox"/> |
| Username | <input type="checkbox"/> |
| eMail    | <input type="checkbox"/> |

**Autenticazione Trasporto**

|       |              |
|-------|--------------|
| Stato | disabilitato |
|-------|--------------|

**Autorizzazione**

|       |              |
|-------|--------------|
| Stato | disabilitato |
|-------|--------------|

**Autorizzazione Contenuti**

|       |              |
|-------|--------------|
| Stato | disabilitato |
|-------|--------------|

**SALVA**

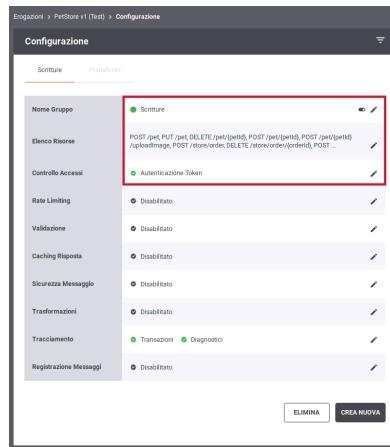


Fig. 3.7: Riepilogo della configurazione effettuata



# CAPITOLO 4

---

## Erogazione REST Modelli PA

---

### 4.1 Obiettivo

Esporre un servizio REST accessibile in accordo alla normativa prevista dal Modello di Interoperabilità.

### 4.2 Sintesi

Mostriamo in questa sezione come procedere per l'esposizione di un servizio REST da erogare nel rispetto della normativa italiana alla base dell'interoperabilità tra i sistemi della pubblica amministrazione. In particolare andiamo ad illustrare lo scenario, tra quelli prospettati nel Modello di Interoperabilità di AGID, che prevede le più ampie caratteristiche di sicurezza e affidabilità. I requisiti di riferimento sono quelli descritti nella sezione 5.4.2 del Modello di Interoperabilità che, oltre a garantire la confidenzialità della comunicazione con autenticazione dell'interlocutore, prevedono supporto a garanzia dell'integrità del messaggio e non ripudiabilità dell'avvenuta trasmissione.

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

1. Un applicativo eroga un servizio, rivolto a fruitori di domini esterni, in conformità al Modello di Interoperabilità AGID
2. La comunicazione con i domini esterni avviene su un canale gestito con sicurezza canale di profilo IDAC02
3. La confidenzialità e autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con profilo IDAR02
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva di profilo IDAR03
5. Ciascun fruitore riceve conferma di ricezione del messaggio da parte dell'erogatore
6. Garanzia di opponibilità ai terzi e non ripudio delle trasmissioni con persistenza delle prove di trasmissione

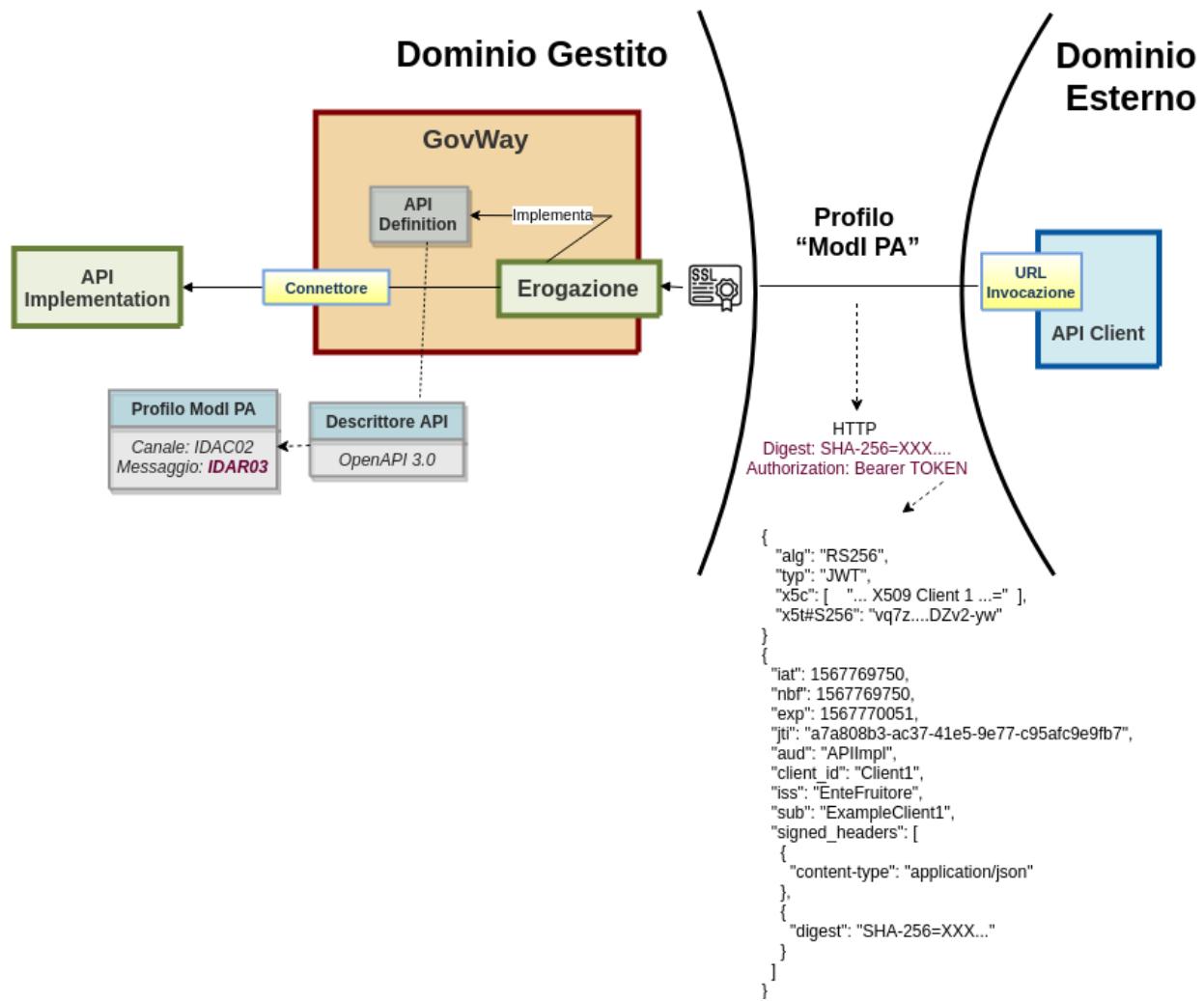


Fig. 4.1: Erogazione ModI PA

## 4.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API «PetStore», basata su REST, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAR02 e IDAR03.
- un'istanza Govway per la gestione del profilo ModI PA nel dominio dell'erogatore.
- un client del dominio esterno che invoca la «POST /pet» diretto all'erogazione esposta da Govway.
- il server PetStore di esempio che riceve le richieste inoltrate dal Govway e produce le relative risposte. Per questo scenario viene utilizzato il server disponibile on line all'indirizzo “<http://petstore.swagger.io/>”.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «5. Erogazione ModI PA», che è stato preconfigurato per il funzionamento con le caratteristiche descritte sopra.

Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console govwayMonitor:

1. Lo scambio del messaggio con il dominio fruitore (comunicazione interdominio) avviene in accordo al profilo IDAC02 e quindi con protocollo SSL e autenticazione client. Dal dettaglio della transazione si possono consultare i messaggi diagnostici dove è visibile la fase di autenticazione del client con i dati di validazione del certificato ricevuto ([Fig. 4.2](#)).

|                            |                 |                |  |
|----------------------------|-----------------|----------------|--|
| 2019-10-01<br>14:29:03.352 | infoIntegration | RicezioneBuste | Ottenute credenziali di accesso ( SSL-Subject 'CN=enteEsterno.govway.org, O=govway.org, C=it' ) fornite da Traefik |
| 2019-10-01<br>14:29:03.352 | infoIntegration | RicezioneBuste | Autenticazione [ssl] in corso ( SSL-Subject 'CN=enteEsterno.govway.org, O=govway.org, C=it' ) ...                  |
| 2019-10-01<br>14:29:03.359 | infoIntegration | RicezioneBuste | Autenticazione [ssl] effettuata con successo   |

Fig. 4.2: Sicurezza canale IDAC02

2. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in [Fig. 4.3](#). Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization», che contiene il token di sicurezza, e «Digest» che contiene il valore per la verifica dell'integrità del payload.
3. Grazie alle configurazioni presenti nell'erogazione, ed in particolare alla relazione di trust stabilita con il fruitore, Govway è in grado di validare i dati di sicurezza ricevuti andando a decodificare il token e a verificare il digest del messaggio. Nella fase di validazione del token si può notare come la sezione header ([Fig. 4.4](#)) riporti l'identità del fruitore e il suo certificato X.509, mentre la sezione payload ([Fig. 4.5](#)) contenga i riferimenti temporali (iat, nbf, exp) e le componenti firmate del messaggio (tra cui il digest).
4. Il messaggio ricevuto dal Govway viene quindi validato, sulla base dei profili di sicurezza previsti nello scambio, verificando in questo caso l'identità del fruitore, la validità temporale, la corrispondenza del digest relativo al payload. Solo in caso di superamento dell'intero processo di validazione, il messaggio viene inoltrato al servizio erogatore. Le evidenze del processo di validazione sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta ([Fig. 4.6](#)). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal token di sicurezza presente nel messaggio.
5. Dopo l'inoltro al servizio erogatore, Govway riceve la risposta e la elabora producendo il relativo token di sicurezza utilizzando le impostazioni di firma fornite nell'ambito dell'erogazione relativamente all'elaborazione della risposta. Sulla console govwayMonitor è possibile visualizzare il messaggio di risposta in uscita, dove si rileva la presenza del token prodotto nell'header HTTP «Authorization» (analogamente a [Fig. 4.3](#)).

## Messaggio

```
1  {
2      "id" : 32,
3      "category" : {
4          "id" : 0,
5          "name" : "Alano"
6      },
7      "name" : "Leo",
8      "photoUrls" : [ "string" ],
9      "tags" : [ {
10         "id" : 0,
11         "name" : "pelo corto"
12     } ],
13     "status" : "available"
14 }
```

## Headers

### Nome

|                       |                                      |
|-----------------------|--------------------------------------|
| x-forwarded-<br>proto | https                                |
| host                  | auth03.govcloud.it                   |
| content-type          | application/json                     |
| postman-<br>token     | c4e9048a-1038-4c3e-8fa5-18138099b483 |
| user-agent            | GovWay                               |

---

HEADER: ALGORITHM & TOKEN TYPE

---

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "ExampleClient1",
  "x5c": [
    "MIIDXjCCAkagAwIBAgIBAjANBgkqhkiG9w0BAQsFADBSMQswCQYDVQ
    QGEwJJVDE0MAwGA1UECBMFSXRhbHkxDTALBgNVBAcTBFBpc2ExEDA0B
    gNVBAoTB0V4YW1wbGUxEjAQBgNVBAMTCUV4YW1wbGVDQTaeFw0xOTA3
    MDkxMDI2MDBaFw00MDA3MzAxMDI2MDBaMFcxCzAJBgNVBAYTAK1UMQ4
    wDAYDVQQIEwVJdGFseTENMASGA1UEBxMEUG1zYTEQMA4GA1UEChMHRX
    hhbXBsZTEXMBUGA1UEAxMORXhhbXBsZUNsaWVudDEwggiMA0GCSqGS
    Ib3DQEBAQUAA4IBDwAwggEKAoIBAQDwhiesh5jK4IJ1Am92TEvlsPn6
    /4vZvACCLPhkwk+paqFuCwaad7JodAgov6KGIpGBsNPTYcg0Ut4mnq5
    cLFG7oxhUReSm4juq17bGqUbPDYX5YAs2SgWBpd4isTAi6CP156KqoF
    t5111A+vtiZceJk5L01WxBJ7JFMaEh8y2+uopRrxHhTaAUChnnCjZyAJ
    TYOTWAn8HaaiejGC97CLYRrZJK644A10G8ATACTVzFfB1zFWo4CP0B4p
    7uQ+zv1WAKmca6i22uGqUu1PSE+mKPZPVL+vYQ1mtD17HiGQUXyrYSn
    Gq94pwXluZNo1LV70MoK2Em0arX077MQssUDHhtj
    /AgMBAAGjOjA4MAkGA1UdEwQCMAAwHQYDVR00BBYEFFFKI7UGHJZrrD
    j6KUd+IrW78z1vMAwGA1UdDwQFAwMH
    /4AwDQYJKoZIhvcNAQELBQADggEBAFZGYkr9C5Sj3rQ0I5kgnx7qLVk
    8hj++uMBIEuhAnte9bzZ4pG1Ba1R4oPnIjExgzuZ1PxM90G00EDQ7J9
    ibKNui90AAASo2TCeJ95/7rwK3TnryL6yCZ+UGNE0y8ICxJ6Csd2Pac8
    /vrZB30NzbnNGj4AtpGEow0oscYw5NEe809VyC3tfZNPyHZ4fa1A7
    /0SugmyY8HR0
    /R2VyyoMi7oy7s16WcwR6n5cG1xucDTh1VociU9brKvZXG8hovBLnRb
    w9RX4B8CXei8sZ6iiD14DZD9EQxKb23yWQB1pnFXe5PUMTNpLJW4ign
    KI2oIkGPxByMeIIH8LKP+779BM4SOI="
  ]
}
```

Fig. 4.4: Sezione «Header» del Token di sicurezza

PAYLOAD: DATA

---

```
{  
    "iat": 1568301379,  
    "nbf": 1568301379,  
    "exp": 1568301679,  
    "jti": "0f39c183-84ca-4d33-a85c-552fa2038888",  
    "aud": "PetStore",  
    "client_id": "Client1Test",  
    "iss": "EnteFruitore",  
    "sub": "ExampleClient1",  
    "signed_headers": [  
        {  
            "digest":  
                "SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcc8  
                c445350c0cf55f84f6"  
        },  
        {  
            "content-type": "application/json"  
        }  
    ]  
}
```

Fig. 4.5: Sezione «Payload» del Token di sicurezza

### Informazioni ModI PA

**ProfiloSicurezzaMessaggio** IDAR0302  
**ProfiloSicurezzaCanale** IDAC02  
**ProfiloInterazione** bloccante

#### Sicurezza Messaggio

**Digest** SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcc8c445350c0cf55f84f6  
**ClientId** Client1Test  
**Issuer** EnteFruitore  
**Subject** ExampleClient1  
**MessageId** 4d9b84b3-80f7-4a5f-a1f7-494779bedfd3  
**Audience** PetStore  
**NotBefore** 2019-09-12\_17:21:16.000  
**Expiration** 2019-09-12\_17:26:16.000  
**IssuedAt** 2019-09-12\_17:21:16.000  
**X509-Issuer** CN=ExampleCA, O=Example, L=Pisa, ST=Italy, C=IT  
**X509-Subject** CN=ExampleClient1, O=Example, L=Pisa, ST=Italy, C=IT

#### Headers HTTP Firmati

**content-type** application/json  
**digest** SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcc8c445350c0cf55f84f6

Fig. 4.6: Traccia della richiesta elaborata dall'erogatore

### 4.3.1 Conformità ai requisiti ModI PA

I requisiti iniziali, legati alla comunicazione basata su uno scenario ModI PA, sono verificati dalle seguenti evidenze:

1. La trasmissione è basata sul profilo IDAC02, riguardo la sicurezza canale, come evidenziato nei messaggi diagnostici dalla presenza degli elementi dell'handshake SSL e relativi dati dei certificati scambiati (Fig. 4.2).
2. La sicurezza messaggio applicata è quella dei profili IDAR02 e IDAR03, come ampiamente mostrato nelle tracce dei messaggi di richiesta e risposta, dove sono presenti i certificati degli applicativi e le firme dei payload (e le relative validazioni).
3. La conferma di ricezione da parte dell'erogatore è costituita dalla risposta ottenuta dal fruitore, sul profilo di interazione bloccante, con il token di sicurezza e la firma del payload applicati sul messaggio di risposta.
4. Il non ripudio della trasmissione da parte del fruitore è garantito tramite la conservazione del messaggio ottenuto, comprensivo di riferimenti temporali, digest del payload, identità del mittente, il tutto garantito dalla firma digitale.
5. L'opponibilità verso i terzi è garantita dal mantenimento nell'archivio delle evidenze tracciate, citate ai punti precedenti, con la possibilità, offerta dalla console govwayMonitor, di effettuare successive ricerche per la consultazione delle stesse.

## 4.4 Configurazione

Per la configurazione dello scenario descritto è necessario intervenire sulla govwayConsole (lato fruitore ed erogatore in base all'ambito di propria competenza). Per operare con la govwayConsole in modo conforme a quanto pre-

visto dalla specifica del Modello di Interoperabilità 2018 si deve attivare, nella testata dell’interfaccia, il Profilo di Interoperabilità «ModI PA» (Fig. 4.7).

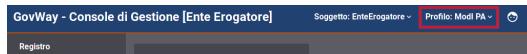


Fig. 4.7: Profilo ModI PA della govwayConsole

#### 4.4.1 Salvataggio Messaggi

Per far gestire a Govway la persistenza dei messaggi scambiati, come prova di trasmissione per l’opponibilità ai terzi, è necessario intervenire sulla configurazione della funzionalità di tracciamento (sezione del menu «Configurazione > Tracciamento», abilitando la «Registrazione Messaggi» e prevendendo la persistenza quanto meno delle comunicazioni scambiate tra i due gateway (Fig. 4.8 e Fig. 4.9).

A screenshot of the 'Richiesta' configuration page. The page has a header 'Richiesta'. Underneath, there are sections for 'Ingresso' and 'Uscita', each containing dropdown menus for 'Headers', 'Body', and 'Attachments'. The dropdowns are set to 'abilitato' (enabled) for all categories in both sections. The entire configuration area is enclosed in a light gray border.

Fig. 4.8: Abilitazione del salvataggio delle richieste in uscita

Si procede quindi con i passi di configurazione del servizio.

#### 4.4.2 Registrazione API

Si registra l’API «PetStore», fornendo il relativo descrittore OpenAPI 3, selezionando i profili IDAC02 (sicurezza canale) e IDAR02/IDAR03 (sicurezza messaggio) nella sezione «ModI PA» (Fig. 4.10).

**Risposta**

|                 |              |
|-----------------|--------------|
| Stato           | abilitato    |
| <b>Ingresso</b> |              |
| Headers         | abilitato    |
| Body            | abilitato    |
| Attachments     | abilitato    |
| <b>Uscita</b>   |              |
| Headers         | disabilitato |
| Body            | disabilitato |
| Attachments     | disabilitato |

Fig. 4.9: Abilitazione del salvataggio delle risposte in ingresso

**Modi PA**

|                                    |   |
|------------------------------------|---|
| <b>Profilo Sicurezza Canale</b>    |   |
| Profilo                            | IDAC02 - Direct Trust mutual Transport-Level Security   |
| <b>Profilo Sicurezza Messaggio</b> |   |
| Profilo                            | IDAR03 (IDAR02) - Integrità della payload del messaggio |

Fig. 4.10: Profilo ModI PA della govwayConsole

#### 4.4.3 Applicativo Esterno

È opzionalmente possibile registrare l'applicativo esterno che corrisponde al fruitore del servizio. Questa scelta può essere fatta in base al tipo di autorizzazione che si è impostata sui fruitori. Vediamo i seguenti casi:

- Se il truststore utilizzato da Govway per l'autenticazione dei fruitori (sicurezza messaggio) contiene i singoli certificati degli applicativi autorizzati, questo passo può anche essere omesso. La gestione del truststore è sufficiente a stabilire i singoli fruitori autorizzati.
- Se il truststore contiene la CA emittente dei certificati utilizzati dai fruitori, l'autorizzazione puntuale non è possibile a meno di non procedere con la registrazione puntuale degli applicativi fornendo i singoli certificati necessari per l'identificazione (Fig. 4.11).

**Applicativo**

|          |                |
|----------|----------------|
| Dominio  | Esterno        |
| Soggetto | EnteFruitore   |
| Nome *   | ExampleClient1 |

**Modi PA**

**Sicurezza Messaggio**

|               |                              |
|---------------|------------------------------|
| Modalità      | Upload Archivio              |
| Formato       | CER                          |
| Certificato * | Browse... ExampleClient1.crt |

Reply Audience/WSA-To

Identificativo dell'Applicativo scambiato nei token di sicurezza delle risposte

Fig. 4.11: Configurazione applicativo esterno (fruitore)

#### 4.4.4 Erogazione

Si registra l'erogazione «PetStore», relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «Modi PA Richiesta» (Fig. 4.12). In questo contesto vengono inseriti i dati necessari per validare le richieste in ingresso.

**Modi PA - Richiesta**

| <b>Profilo Sicurezza Messaggio</b> |  |
|------------------------------------|--|
| Riferimento X.509                  | x5c (Certificate Chain)<br>x5t#256 (Certificate SHA-256 Thumbprint)<br>x5u (URL) |
| TrustStore Certificati             | Default  |
| Audience                           | PetStore   |

Se non viene fornito un valore, il valore atteso all'interno del security token corrisponderà all'url di invocazione

Fig. 4.12: Configurazione richiesta dell'erogazione

La sezione «Modi PA Risposta» si utilizza per indicare i parametri per la produzione del token di sicurezza da inserire nel messaggio di risposta (Fig. 4.13).

Se si è scelto di registrare gli applicativi esterni, fruitori del servizio, è possibile intervenire sulla configurazione del «Controllo degli Accessi» per l'erogazione, in modo da specificare i singoli applicativi fruitori autorizzati ad effettuare richieste al servizio erogato (Fig. 4.14).

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. 4.13: Configurazione risposta dell'erogazione



Fig. 4.14: Controllo accessi con autorizzazione degli applicativi esterni

# CAPITOLO 5

---

## Fruizione REST ModI PA

---

### 5.1 Obiettivo

Fruire di un servizio REST accessibile in accordo alla normativa prevista dal Modello di Interoperabilità.

### 5.2 Sintesi

Mostriamo in questa sezione come procedere per l'integrazione di un applicativo con un servizio REST erogato nel rispetto della normativa italiana alla base dell'interoperabilità tra i sistemi della pubblica amministrazione. In particolare andiamo ad illustrare lo scenario, tra quelli prospettati nel Modello di Interoperabilità di AGID, che prevede le più ampie caratteristiche di sicurezza e affidabilità. I requisiti di riferimento sono quelli descritti nella sezione 5.4.2 del Modello di Interoperabilità che, oltre a garantire la confidenzialità della comunicazione con autenticazione dell'interlocutore, prevedono supporto a garanzia dell'integrità del messaggio e non ripudiabilità dell'avvenuta trasmissione.

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

1. Un applicativo fruitore che dialoga con il servizio erogato in modalità ModI PA in accordo ad una API condivisa
2. La comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con sicurezza canale di profilo IDAC02
3. La confidenzialità e autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con profilo IDAR02
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva di profilo IDAR03
5. L'applicativo fruitore ottiene e conserva la conferma di ricezione del messaggio da parte dell'erogatore
6. Garanzia di opponibilità ai terzi e non ripudio delle trasmissioni

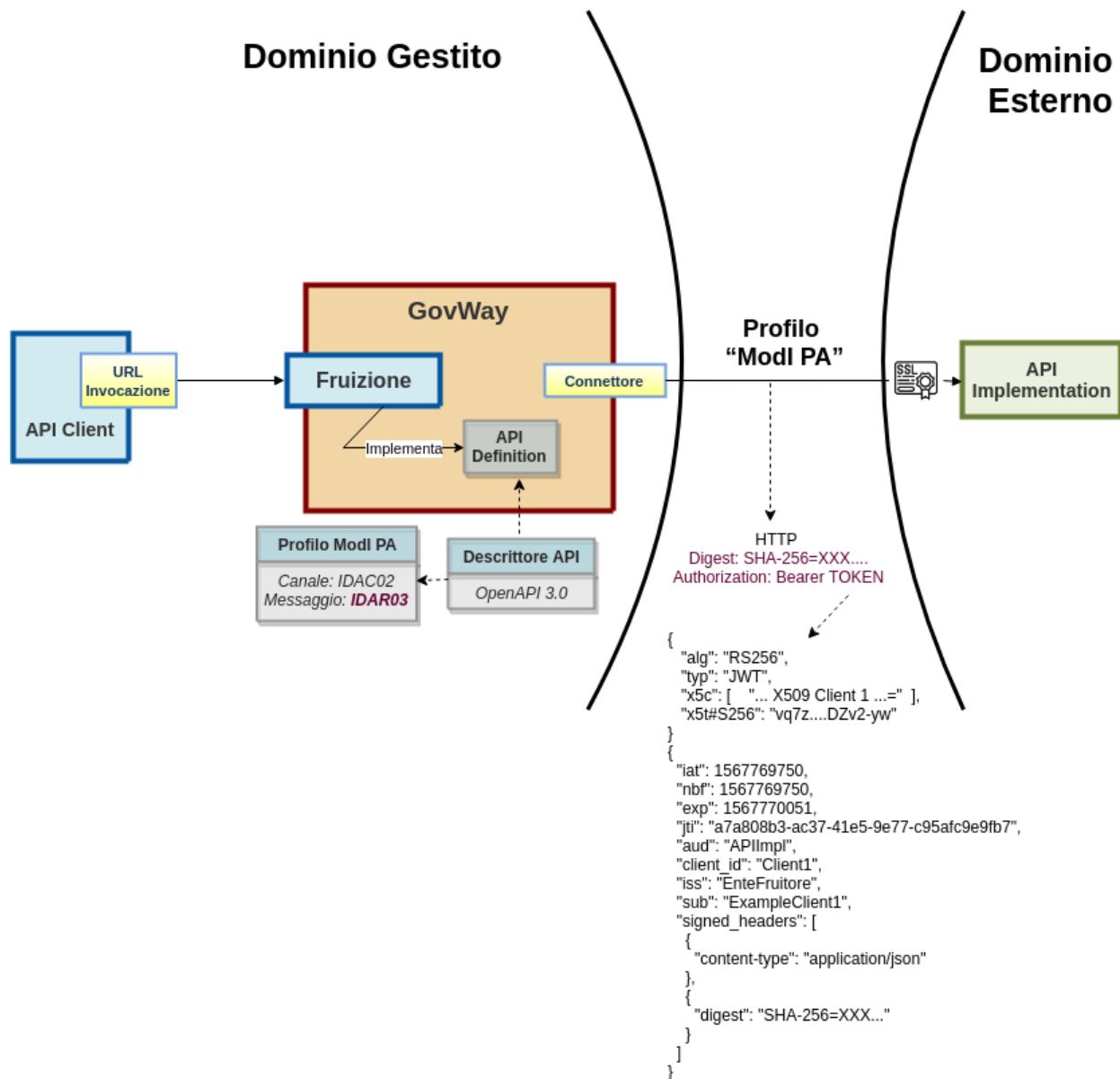


Fig. 5.1: Fruizione ModI PA

## 5.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API «PetStore», basata su REST, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAR02 e IDAR03.
- Un'istanza Govway per la gestione del profilo ModI PA nel dominio del fruitore.
- un client che invoca la «POST /pet» con un messaggio di esempio diretto al Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «6. Fruizione ModI PA», che è stato preconfigurato per il funzionamento con le caratteristiche descritte sopra.

Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto nelle diverse fasi dell'esecuzione andando a consultare le console govwayMonitor:

1. Il messaggio di richiesta inviato dal fruitore viene elaborato da Govway che, tramite la configurazione della firma digitale associata all'applicativo mittente, è in grado di produrre il token di sicurezza da inviare con la richiesta all'erogatore. Da govwayMonitor si può visualizzare il messaggio di richiesta in uscita che è il medesimo di quello in entrata con la differenza che è stato aggiunto il token di sicurezza tra gli header HTTP ([Fig. 5.2](#)).
2. Col processo di validazione del token di sicurezza, Govway estrae le informazioni in esso contenute. L'header e il payload del token sono identici a quelli visualizzati nello scenario di erogazione REST, relativamente al messaggio in uscita ([Fig. 4.4](#) e [Fig. 4.5](#)).
3. Lo scambio del messaggio con il dominio erogatore (comunicazione interdominio) avviene in accordo al profilo IDAC02 e quindi con protocollo SSL e autenticazione client. Dal dettaglio della transazione si possono consultare i messaggi diagnostici dove è visibile la fase di apertura della connessione SSL ([Fig. 5.3](#)).
4. Govway riceve la risposta dell'erogatore, dalla quale estrae il token di sicurezza al fine di effettuare i relativi controlli di validità e conservare la traccia come conferma di ricezione da parte dell'erogatore. Consultando la traccia relativa alla trasmissione della risposta ([Fig. 5.4](#)), sono visibili i dati di autenticazione dell'erogatore, i riferimenti temporali e l'identificativo del messaggio, nonché il digest del payload per la verifica di integrità.

### 5.3.1 Conformità ai requisiti ModI PA

I requisiti iniziali, legati alla comunicazione basata su uno scenario ModI PA, sono verificati dalle seguenti evidenze:

1. La trasmissione è basata sul profilo IDAC02, riguardo la sicurezza canale, come evidenziato nei messaggi diagnostici dalla presenza degli elementi dell'handshake SSL e relativi dati dei certificati scambiati ([Fig. 5.3](#)).
2. La sicurezza messaggio applicata è quella dei profili IDAR02 e IDAR03, come ampiamente mostrato nelle tracce dei messaggi di richiesta e risposta, dove sono presenti i certificati degli applicativi e le firme dei payload (e le relative validazioni).
3. La conferma di ricezione da parte dell'erogatore è costituita dalla risposta ottenuta dal fruitore, sul profilo di interazione bloccante, con il token di sicurezza e la firma del payload applicati sul messaggio di risposta.
4. Il non ripudio della trasmissione da parte del fruitore è garantito tramite la conservazione del messaggio ottenuto, comprensivo di riferimenti temporali, digest del payload, identità del mittente, il tutto garantito dalla firma digitale.
5. L'opponibilità verso i terzi è garantita dal mantenimento nell'archivio delle evidenze tracciate, citate ai punti precedenti, con la possibilità, offerta dalla console govwayMonitor, di effettuare successive ricerche per la consultazione delle stesse.

**Messaggio**

```

1  {
2    "id" : 32,
3    "category" : {
4      "id" : 0,
5      "name" : "Alano"
6    },
7    "name" : "Leo",
8    "photoUrls" : [ "string" ],
9    "tags" : [ {
10      "id" : 0,
11      "name" : "pelo corto"
12    }],
13    "status" : "available"
14 }
```

**Headers**

| Nome             |   |
|------------------|---|
| Content-Type     | application/json  |
| postman-token    | a7f1c665-cf1f-488d-a07e-78e19557dd0e  |
| x-forwarded-port | 443   |
| Digest           | SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcc8c445350c0cf55f84f6   |
| x-real-ip        | 172.19.0.1  |
| cache-control    | no-cache  |
| User-Agent       | GovWay  |
| Authorization    | Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZS5nb3ZjbG91ZC5pdCIsIng1YhECvMrbrpW3fsX85SdQ7jRIH6p-FLWLyzsZ2mb2xVFw8wPZtlrOc2_P_rPvr0GDy9EZSU9Yf_5MY2 |

Fig. 5.2: Messaggio di richiesta in uscita (con token di sicurezza inserito nell'header HTTP)

|                            |                     |              |  |
|----------------------------|---------------------|--------------|--|
| 2019-09-16<br>16:36:11.209 | <b>infoProtocol</b> | InoltroBuste | Invio Messaggio di cooperazione con identificativo<br>[f26754d8-d596-476b-bc5b-5c1b2b95966b] in corso<br>(location: https://auth03.govcloud.it/govway<br>/rest/EnteEsterno/PetStore/v1/pet http-method:POST) ... |
|----------------------------|---------------------|--------------|--|

Fig. 5.3: Sicurezza canale IDAC02 sulla fruizione

**Informazioni Modelli PA**

**ProfiloSicurezzaMessaggio** IDAR0302  
**ProfiloSicurezzaCanale** IDAC02  
**ProfiloInterazione** bloccante

**Sicurezza Messaggio**

**Digest** SHA-256=ec2592738426e38b9e61f4d00507f11ba362ed4335babe912ee222bc937616ff  
**ClientId** PetStore/v1  
**Issuer** EnteErogatore  
**Subject** PetStore/v1  
**MessageId** 4a927d48-a830-4a89-93b6-4cb6b596f02e  
**Audience** Client1Test  
**NotBefore** 2019-09-12\_17:16:19.000  
**Expiration** 2019-09-12\_17:21:19.000  
**IssuedAt** 2019-09-12\_17:16:19.000  
**X509-Issuer** CN=ExampleCA, O=Example, L=Pisa, ST=Italy, C=IT  
**X509-Subject** CN=ExampleClient1, O=Example, L=Pisa, ST=Italy, C=IT

**Headers HTTP Firmati**

**content-type** application/json  
**digest** SHA-256=ec2592738426e38b9e61f4d00507f11ba362ed4335babe912ee222bc937616ff

Fig. 5.4: Traccia della richiesta elaborata dall'erogatore

## 5.4 Configurazione

Per la configurazione dello scenario descritto è necessario intervenire sulla govwayConsole (lato fruitore ed erogatore in base all'ambito di propria competenza). Per operare con la govwayConsole in modo conforme a quanto previsto dalla specifica del Modello di Interoperabilità 2018 si deve attivare, nella testata dell'interfaccia, il Profilo di Interoperabilità «ModI PA» (Fig. 5.5).

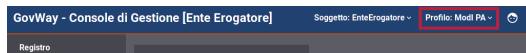


Fig. 5.5: Profilo ModI PA della govwayConsole

### 5.4.1 Salvataggio Messaggi

Per far gestire a Govway la peristenza dei messaggi scambiati, come prova di trasmissione per l'opponibilità ai terzi, è necessario intervenire sulla configurazione della funzionalità di tracciamento (vedi [Salvataggio Messaggi](#)).

Si procede quindi con i passi di configurazione del servizio.

### 5.4.2 Registrazione API

Si registra l'API «PetStore», fornendo il relativo descrittore OpenAPI 3, selezionando i profili IDAC02 (sicurezza canale) e IDAR02/IDAR03 (sicurezza messaggio) nella sezione «ModI PA» (vedi [Registrazione API](#)).

### 5.4.3 Applicativo

Si configura l'applicativo mittente indicando, nella sezione ModI PA, i parametri del keystore necessari affinché Govway possa produrre il token di sicurezza firmando per conto dell'applicativo (Fig. 5.6).

### 5.4.4 Fruizione

Si registra la fruizione «PetStore», relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI PA Richiesta» (Fig. 5.7). In particolare è possibile specificare quali header HTTP si vuole firmare, oltre al payload, e quale scadenza per il token impostare.

La sezione «ModI PA Risposta» definisce i criteri per la validazione dei messaggi di risposta, come la posizione del token di sicurezza e il truststore per l'autenticazione dell'erogatore (Fig. 5.8).

**Modi PA**

**Sicurezza Messaggio**

|                           |                                     |
|---------------------------|-------------------------------------|
| Abilitato                 | <input checked="" type="checkbox"/> |
| Archivio                  |                                     |
| Tipo                      | pkcs12                              |
| Password *                | 123456                              |
| Alias Chiave Privata *    | ExampleClient1                      |
| Password Chiave Privata * | 123456                              |
| Reply Audience/WSA-To     | Client1Test                         |

Identificativo dell'Applicativo scambiato nei token di sicurezza delle risposte

Fig. 5.6: Configurazione applicativo fruitore

**Modi PA - Richiesta**

**Profilo Sicurezza Messaggio**

|                           |  |
|---------------------------|--|
| Algoritmo                 | RS256  |
| HTTP Headers da firmare * | Digest x Content-Type x Content-Encoding x                                       |
| Riferimento X.509         | x5c (Certificate Chain)<br>x5t#256 (Certificate SHA-256 Thumbprint)<br>x5u (URL) |
| Time to Live (secondi) *  | 300  |

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

|          |          |
|----------|----------|
| Audience | PetStore |
|----------|----------|

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

Fig. 5.7: Configurazione richiesta della fruizione

**Modi PA - Risposta**

**Profilo Sicurezza Messaggio**

|                        |  |
|------------------------|--|
| Riferimento X.509      | <input type="text" value="Utilizza impostazioni della Richiesta"/>   |
| TrustStore Certificati | <input type="text" value="Default"/>   |
| Verifica Audience      | <input checked="" type="checkbox"/><br>Se abilitato viene verificato che il valore corrisponde a quello indicato nella configurazione dell'applicativo |

Fig. 5.8: Configurazione risposta della fruizione

# CAPITOLO 6

---

## Erogazione SOAP Modelli PA

---

### 6.1 Obiettivo

Esporre un servizio SOAP accessibile in accordo alla normativa prevista dal Modello di Interoperabilità.

### 6.2 Sintesi

Mostriamo in questa sezione come procedere per l'esposizione di un servizio SOAP da erogare nel rispetto della normativa italiana alla base dell'interoperabilità tra i sistemi della pubblica amministrazione. In particolare andiamo ad illustrare lo scenario, tra quelli prospettati nel Modello di Interoperabilità di AGID, che prevede le più ampie caratteristiche di sicurezza e affidabilità. I requisiti di riferimento sono quelli descritti nella sezione 5.4.2 del Modello di Interoperabilità che, oltre a garantire la confidenzialità della comunicazione con autenticazione dell'interlocutore, prevedono supporto a garanzia dell'integrità del messaggio e non ripudiabilità dell'avvenuta trasmissione.

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

1. Un applicativo eroga un servizio SOAP, rivolto a fruitori di domini esterni, in conformità al Modello di Interoperabilità AGID
2. La comunicazione con i domini esterni avviene su un canale gestito con sicurezza canale di profilo IDAC02
3. La confidenzialità e autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con profilo IDAS02
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva di profilo IDAS03
5. Ciascun fruitore riceve conferma di ricezione del messaggio da parte dell'erogatore
6. Garanzia di opponibilità ai terzi e non ripudio delle trasmissioni con persistenza delle prove di trasmissione

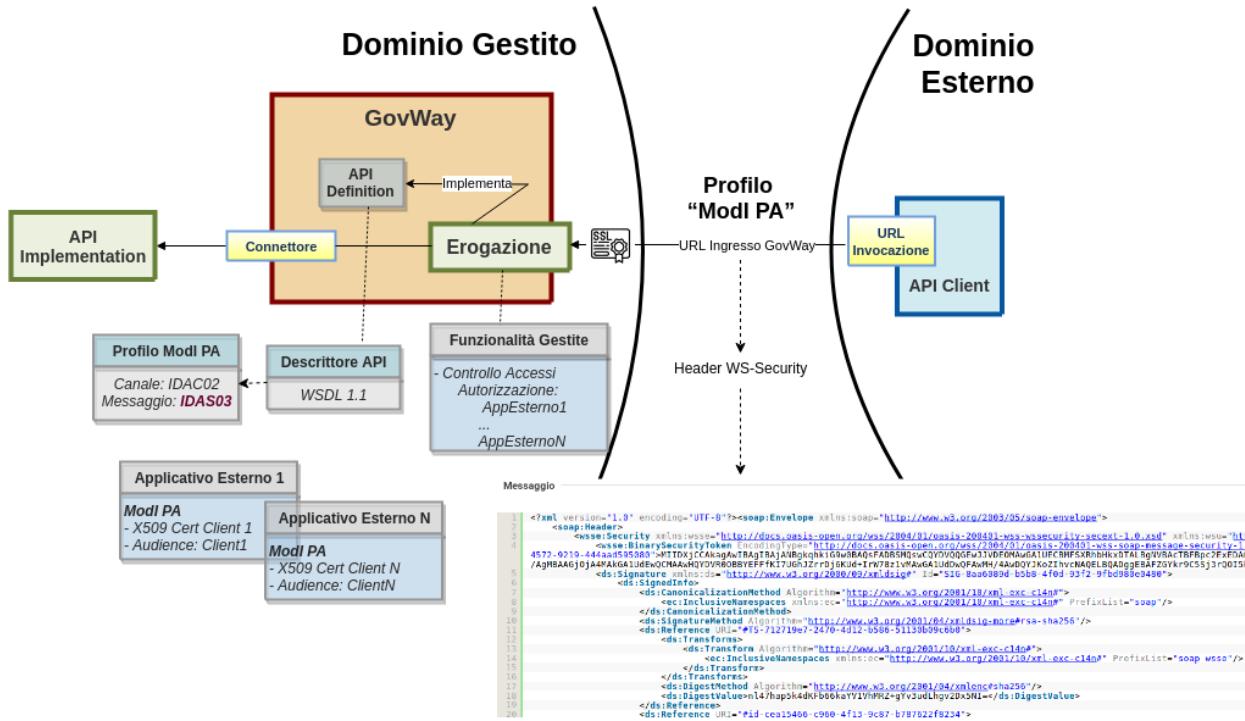


Fig. 6.1: Erogazione SOAP ModI PA

## 6.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API di esempio (Credit Card Verification), basata su SOAP, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAS02 e IDAS03.
  - un’istanza Govway per la gestione del profilo ModI PA nel dominio dell’erogatore.
  - un client del dominio esterno che invoca l’azione di esempio «CheckCC».
  - il server “Credit Card Verification” di esempio che riceve le richieste inoltrate dal Govway e produce le relative risposte. Per questo scenario viene utilizzato il server disponibile on line all’indirizzo “<http://ws.cdyne.com/creditcardverify/luhnchecker.asmx>”.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «7. Erogazione SOAP ModI PA», che è stato preconfigurato per il funzionamento con le caratteristiche descritte sopra.

Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console govwayMonitor.

1. Per verificare l'utilizzo del canale SSL, in accordo al profilo IDAC02, si procede come già illustrato per [Erogazione REST ModI PA](#)
  2. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in [Fig. 6.2](#). Come si nota, il messaggio SOAP contiene nell'header WS-Security, sia il token di sicurezza (elemento «BinarySecurityToken»), sia il digest del payload (elemento «DigestValue»), prodotti dal fruitore con la relativa firma digitale (elemento «SignatureValue»).
  3. Il messaggio ricevuto dal Govway viene quindi validato, sulla base dei profili di sicurezza previsti nello scambio, verificando in questo caso l'identità del fruitore, la validità temporale, la corrispondenza del digest relativo al payload. Solo in caso di superamento dell'intero processo di validazione, il messaggio viene inoltrato al servizio erogatore. Le

**Messaggio**

```

1  <?xml version="1.0" encoding="UTF-8"?><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
2    <soap:Header>
3      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#"
4        c7761d94d64f!>MIIE/zCCAuegAwIBAgICAN4wDQYJKoZIhvcaNAQELBQAwNjELMAKGA1UEBhMCaXQxEARBnIVBaolCmvdndheS5vcmcxEjAQBgNVBAMMCUdvdlheSBDBQTaf
/Wudo6/YXIV1VDHLYMjypb/fL0SL8SKA6uW95WPXcogJPk9aqdw1V0/8w2lpv1t657H+bTNe8fhsmuN1725HBa/W1VKn78213F5LYC4SY8H9nFC/faQu0u0ld1TxohhKwZN1
/ZAJBgNVHRMEAjAAMBEGCWCGSAGG+EBAQEAwIHqDAzBg1ghkgBvhvCA0OEjhYKT3lbLNTTCBHZW5LcnF0ZWQgQ2xpZWS50IENlcnRpZmljYXRlMB0GA1UdbgQWBKRUAicYEN1
/JIBWmVuatppwNcJRTZl06qmIElqmoBTWLZj0MVxJ/+2SwV0UTWNGNsUzziTDS11rmeElidRcbKVvNcxtPHH4ysh5JdIp1fn7G3l4CaTjJHBHo2Ufu0eb03dfqqRc6QzmEr1
/OfppiOpca7fxITX0gDokm+wqgMAZ7s6DEmgW+h7KL6ub0bhewzukba5dpYbgycioDaomD4ywAi5csvmubwSRIALRH80uew0JcyeJSfEY8f5lFud0Blg934DtI4HnT2CBM8C
/NKL76fLQPRGActEV4x0nvCe8NwM28oApI8hYpPutv5YIP5Y=</wsse:BinarySecurityToken>
5    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-4bbe4224-d2df-4f57-814c-2b8a47ec328d">
6      <ds:SignedInfo>
7        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
8          <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap"/>
9        </ds:CanonicalizationMethod>
10       <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
11       <ds:Reference URI="#TS-91e2766f-c512-4440-bfa1-046bbdec9b7">
12         <ds:Transforms>
13           <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
14             <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap wsse"/>
15           </ds:Transform>
16         </ds:Transforms>

```

Fig. 6.2: Messaggio inviato dal frutto

evidenze del processo di validazione sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 6.3). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal token di sicurezza presente nell'header soap.

**– Informazioni ModI PA**

**ProfiloSicurezzaMessaggio** IDAS0302

**ProfiloSicurezzaCanale** IDAC01

**ProfiloInterazione** bloccante

**Sicurezza Messaggio**

**MessageId** e137cd92-6dcc-4afd-a502-1d4fc2da677c

**WSA-From** app1.enteesterno.govcloud.it

**WSA-To** soapblocking.ente.govcloud.it

**Digest** SHA256=fa876310714e6e2b1b51a1a0e72e545de9a59a376f8bf5f62efdb039e7955433

**Expiration** 2019-09-16\_18:45:29.899

**IssuedAt** 2019-09-16\_18:44:29.899

**X509-Issuer** CN=GovWay CA, O=govway.org, C=it

**X509-Subject** CN=app1.enteEsterno.govcloud.it, O=govway.org, C=it

Fig. 6.3: Traccia della richiesta elaborata dall'erogatore

- Dopo l'inoltro al servizio erogatore, Govway riceve la risposta e la elabora producendo il relativo header ws-security da inserire nel messaggio di risposta. Sulla console govwayMonitor è possibile visualizzare il messaggio di risposta in uscita (analogamente a Fig. 6.2).

**6.3.1 Conformità ai requisiti ModI PA**

La verifica dei requisiti ModI PA per questo scenario non differisce da quanto già descritto in *Conformità ai requisiti ModI PA*.

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario *Erogazione REST ModI PA*. Nel seguito sono evidenziate le sole differenze.

L'interfaccia wsdl del servizio soap è ottenibile all'indirizzo “<https://ws.cdyne.com/creditcardverify/luhnchecker.asmx?wsdl>”.

### **6.3.2 Registrazione API**

In fase di registrazione della relativa API, tenere presente che saranno selezionati i profili:

- IDAC02 per la sicurezza canale
- IDAS03 (IDAS02) per la sicurezza messaggio

### **6.3.3 Erogazione**

Si registra l'erogazione SOAP, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI PA Richiesta» (Fig. 6.4). In questo contesto vengono inseriti i dati necessari per validare le richieste in ingresso.

The screenshot shows the configuration interface for a service request. At the top, there is a header labeled "ModI PA - Richiesta". Below it, under the heading "Profilo Sicurezza Messaggio", there are two dropdown menus. The first dropdown is labeled "TrustStore Certificati" and has "Default" selected. The second dropdown is labeled "WSAddressing To" and has "soapblocking.ente.govcloud.it" selected. A note below the dropdowns states: "Se non viene fornito un valore, il valore atteso all'interno del security token corrisponderà all'url di invocazione".

Fig. 6.4: Configurazione richiesta dell'erogazione

La sezione «ModI PA Risposta» si utilizza per indicare i parametri per la produzione del token di sicurezza da inserire nel messaggio di risposta (Fig. 6.5).

**Modi PA - Risposta**

**Profilo Sicurezza Messaggio**

|                          |                                    |
|--------------------------|------------------------------------|
| Algoritmo                | RSA-SHA-256                        |
| Forma Canonica XML       | Exclusive XML Canonicalization 1.0 |
| Riferimento X.509        | Binary Security Token              |
| Certificate Chain        | <input type="checkbox"/>           |
| KeyStore                 | Ridefinito                         |
| Time to Live (secondi) * | 60                                 |

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

**KeyStore**

|                           |  |
|---------------------------|--|
| Modalità                  | File System                                |
| Path *                    | /var/govway/keys/keystore_app1.ente.pkcs12 |
| Tipo                      | pkcs12                                     |
| Password *                | 123456                                     |
| Alias Chiave Privata *    | app1.ente.govcloud.it                      |
| Password Chiave Privata * | 123456                                     |

Fig. 6.5: Configurazione risposta dell'erogazione



# CAPITOLO 7

## Fruizione SOAP ModI PA

### 7.1 Obiettivo

Fruire di un servizio SOAP accessibile in accordo alla normativa prevista dal Modello di Interoperabilità.

### 7.2 Sintesi

Mostriamo in questa sezione come procedere per l'integrazione di un applicativo con un servizio SOAP erogato nel rispetto della normativa italiana alla base dell'interoperabilità tra i sistemi della pubblica amministrazione. In particolare andiamo ad illustrare lo scenario, tra quelli prospettati nel Modello di Interoperabilità di AGID, che prevede le più ampie caratteristiche di sicurezza e affidabilità. I requisiti di riferimento sono quelli descritti nella sezione 5.4.2 del Modello di Interoperabilità che, oltre a garantire la confidenzialità della comunicazione con autenticazione dell'interlocutore, prevedono supporto a garanzia dell'integrità del messaggio e non ripudiabilità dell'avvenuta trasmissione.

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

1. Un applicativo fruitore che dialoga con il servizio SOAP erogato in modalità ModI PA in accordo ad una API condivisa
2. La comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con sicurezza canale di profilo IDAC02
3. La confidenzialità e autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con profilo IDAS02
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva di profilo IDAS03
5. L'applicativo fruitore ottiene e conserva la conferma di ricezione del messaggio da parte dell'erogatore
6. Garanzia di opponibilità ai terzi e non ripudio delle trasmissioni

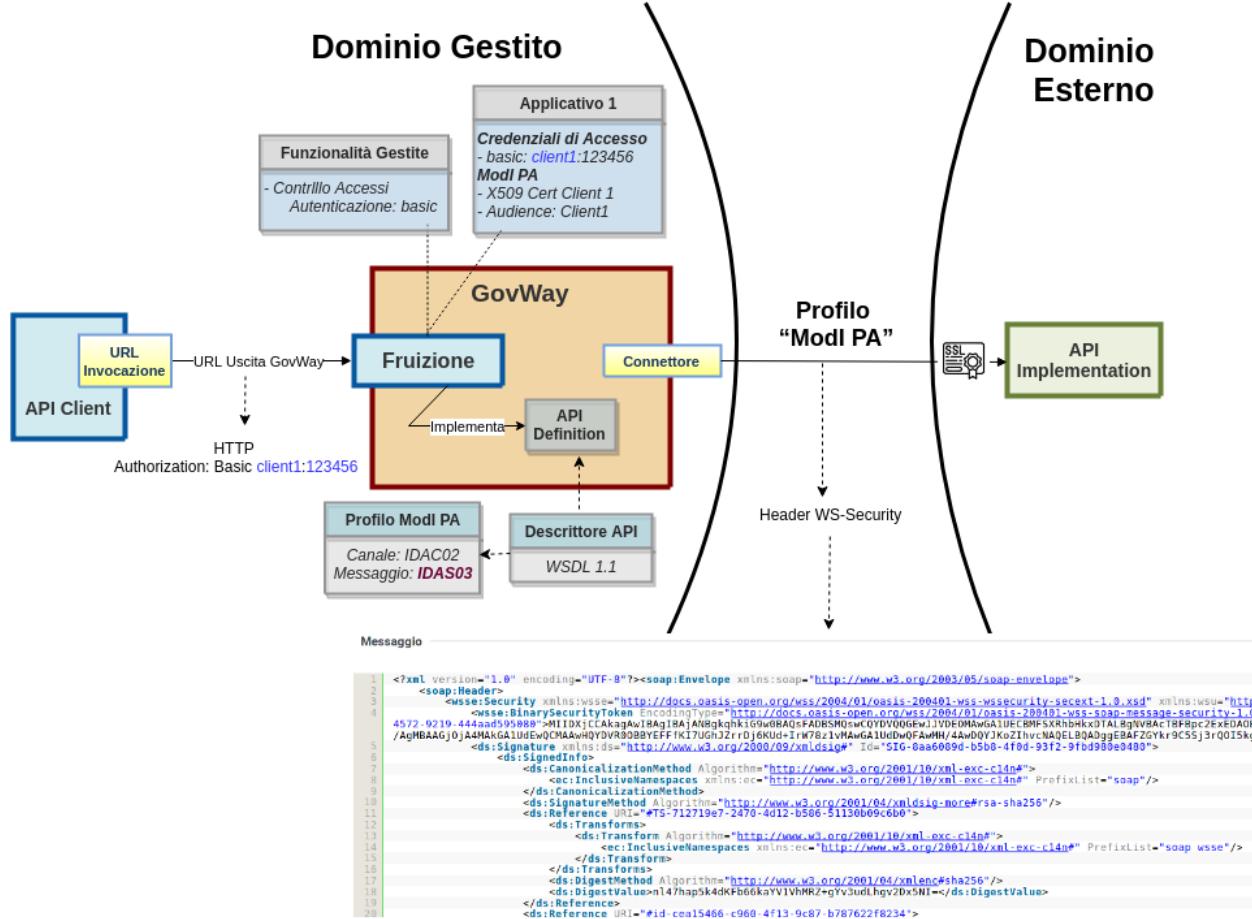


Fig. 7.1: Fruizione SOAP ModI PA

## 7.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API di esempio (Credit Card Verification), basata su SOAP, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAS02 e IDAS03.
- un'istanza Govway per la gestione del profilo ModI PA nel dominio del fruttore.
- un client del dominio gestito che invoca l'azione di esempio «CheckCC» tramite Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «8. Fruizione SOAP ModI PA», che è stato preconfigurato per il funzionamento con le caratteristiche descritte sopra.

Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console govwayMonitor.

1. Il messaggio di richiesta inviato dal fruttore viene elaborato da Govway che, tramite la configurazione della firma digitale associata all'applicativo mittente, è in grado di produrre l'header WS-Security da inserire nella richiesta inviata all'erogatore. Da govwayMonitor si può visualizzare il messaggio di richiesta in uscita, analogo a quanto già visto in [Fig. 6.2](#).
2. Per verificare l'utilizzo del canale SSL, in accordo al profilo IDAC02, si procede come già illustrato per [Erogazione REST ModI PA](#).
3. Govway riceve la risposta dell'erogatore, dalla quale estrae l'header WS-Security al fine di effettuare i relativi controlli di validità e conservare la traccia come conferma di ricezione da parte dell'erogatore. Consultando la traccia relativa alla trasmissione della risposta ([Fig. 7.2](#)), sono visibili i dati di autenticazione dell'erogatore, i riferimenti temporali e l'identificativo del messaggio, nonché il digest del payload per la verifica di integrità.

### Informazioni ModI PA

**ProfiloSicurezzaMessaggio** IDAS0302

**ProfiloSicurezzaCanale** IDAC01

**ProfiloInterazione** bloccante

#### Sicurezza Messaggio

|                     |  |
|---------------------|--|
| <b>RelatesTo</b>    | a9eb35d2-6747-4b95-b99e-b62a1c27b704                                   |
| <b>MessageId</b>    | 7bdddc0-710f-4c12-baee-16da54b98116                                    |
| <b>WSA-From</b>     | SOAPBlockingImpl/v1  |
| <b>WSA-To</b>       | app1.ente.govcloud.it  |
| <b>Digest</b>       | SHA256=3420173c4cab7606e0dc9deb98721064c756d398fb57a94eb2d790fb72cf3a1 |
| <b>Expiration</b>   | 2019-09-16_19:42:18.783  |
| <b>IssuedAt</b>     | 2019-09-16_19:37:18.783  |
| <b>X509-Issuer</b>  | CN=GovWay CA, O=govway.org, C=it                                       |
| <b>X509-Subject</b> | CN=app1.enteEsterno.govcloud.it, O=govway.org, C=it                    |

Fig. 7.2: Traccia della richiesta elaborata dall'erogatore

### 7.3.1 Conformità ai requisiti ModI PA

La verifica dei requisiti ModI PA per questo scenario non differisce da quanto già descritto in [Conformità ai requisiti ModI PA](#).

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario [Fruizione REST ModI PA](#). Nel seguito sono evidenziate le sole differenze.

### 7.3.2 Registrazione API

In fase di registrazione della relativa API, tenere presente che saranno selezionati i profili:

- IDAC02 per la sicurezza canale
- IDAS03 (IDAS02) per la sicurezza messaggio

### 7.3.3 Fruizione

Si registra la fruizione SOAP, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI PA Richiesta» (Fig. 7.3).

**ModI PA - Richiesta**

| Profilo Sicurezza Messaggio  |                                    |
|--|------------------------------------|
| Algoritmo  | RSA-SHA-256                        |
| Forma Canonica XML   | Exclusive XML Canonicalization 1.0 |
| Riferimento X.509  | Binary Security Token              |
| Certificate Chain  | <input type="checkbox"/>           |
| Time to Live (secondi) *   | 60                                 |
| Indica la validità temporale, in secondi, a partire dalla data di creazione del security token                   |                                    |
| WSAddressing To  | soapblocking.ente.govcloud.it      |
| Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore |                                    |

Fig. 7.3: Configurazione richiesta della fruizione

La sezione «ModI PA Risposta» definisce i criteri per la validazione dei messaggi di risposta (Fig. 7.4).

**ModI PA - Risposta**

| Profilo Sicurezza Messaggio   |                                     |
|---|-------------------------------------|
| TrustStore Certificati  | Default                             |
| Verifica WSAddressing To  | <input checked="" type="checkbox"/> |
| Se abilitato viene verificato che il valore corrisponde a quello indicato nella configurazione dell'applicativo |                                     |

Fig. 7.4: Configurazione risposta della fruizione

# CAPITOLO 8

## Monitoraggio

In questa sezione descriviamo alcuni tipici scenari di impiego delle funzionalità di monitoraggio offerte da Govway. Il monitoraggio consente di tenere sotto controllo il traffico gestito dal gateway al fine di verificare il regolare funzionamento dei servizi, individuare situazioni anomale ed avviare l'indagine diagnostica.

Per meglio descrivere le attività tipiche della fase di monitoraggio, supponiamo di intervenire nella fase successiva all'esecuzione dei passi dello scenario «Erogazione SPID» (*Erogazione OAuth*).

La console govwayMonitor, nella sezione Monitoraggio, prevede la consultazione del traffico gestito nelle modalità «Storico» e «Live». Ciascuna di queste sezioni mostra l'elenco delle transazioni, in ordine cronologico decrescente, che soddisfano i criteri di filtro impostati (Fig. 8.1).

|   | Data Richiesta                      | Tipologia  | API                | Operazione    | Mittente | Esito                  |
|---|-------------------------------------|------------|--------------------|---------------|----------|------------------------|
| ✓ | <a href="#">2019-09-05 11:32:00</a> | Erogazione | PetStore v1 (Test) | POST_pet      |          | Ok                     |
| ! | <a href="#">2019-09-05 10:53:01</a> | Erogazione | PetStore v1 (Test) | POST_pet      |          | Gestione Token Fallita |
| ✓ | <a href="#">2019-09-04 16:26:19</a> | Erogazione | PetStore v1 (Test) | GET_pet.petid |          | Ok                     |
| ✓ | <a href="#">2019-09-04 16:26:06</a> | Erogazione | PetStore v1 (Test) | GET_pet.petid |          | Ok                     |
| ✓ | <a href="#">2019-09-04 16:25:30</a> | Erogazione | PetStore v1 (Test) | POST_pet      |          | Ok                     |
| ! | <a href="#">2019-09-04 16:24:05</a> | Erogazione | PetStore v1 (Test) | POST_pet      |          | Gestione Token Fallita |
| ! | <a href="#">2019-09-04 16:22:30</a> | Erogazione | PetStore v1 (Test) | POST_pet      |          | Gestione Token Fallita |

Fig. 8.1: Elenco delle transazioni

Le transazioni riportate nell'elenco riportano i dati per l'identificazione delle stesse, con evidenza dell'esito riportato.

## 8.1 Transazione in errore

Se apriamo il dettaglio della transazione con esito errore, relativa all'invocazione della «POST /pet» senza token, vediamo le informazioni di Fig. 8.2.

Il dettaglio della transazione:

- Il riquadro «Informazioni Generali» riepiloga i principali dati identificativi della transazione. In questo riquadro è mostrato l'esito, in questo caso negativo. Tramite il link apposito si possono visualizzare i messaggi diagnostici, utili alla comprensione del problema occorso (Fig. 8.3).
- I riquadri «Dettagli Richiesta» e «Dettagli Risposta» forniscono informazioni specifiche relative al messaggio di richiesta e a quello di risposta. In questo caso, ad esempio, è possibile visualizzare il messaggio di fault inviato al client in risposta (Fig. 8.4).
- Il riquadro «Informazioni Mittente» fornisce dettagli sulla provenienza della richiesta.
- Il riquadro «Informazioni Avanzate» fornisce dati aggiuntivi riguardo la transazione.

## 8.2 Transazione con esito corretto

Se apriamo il dettaglio della transazione con esito positivo, relativa all'invocazione della «POST /pet», possiamo ad esempio:

- Visualizzare le informazioni generali con l'esito dell'operazione (Fig. 8.2).

Messaggi diagnostici della transazione con esito regolare

- Nel contesto delle informazioni generali si possono visualizzare i messaggi diagnostici con il dettaglio dell'elaborazione regolarmente eseguita (Fig. 8.2).

Messaggi diagnostici della transazione con esito regolare

- Nel contesto delle informazioni mittente in questo caso sarà presente la sezione «Token Info» che consente di visualizzare dati inerenti il token che è stato fornito con la richiesta del mittente. Risultano immediatamente visibili le informazioni principali (issuer, subject, ...), come mostrato in Fig. 8.2.

Informazioni mittente con presenza del token

- Dalla sezione mittente è possibile aprire una finestra per visualizzare la versione in chiaro del token ricevuto con la richiesta (Fig. 8.2).

Visualizzazione del token

Visualizza Transazioni (Live) > **Dettaglio Transazione**

## Dettagli Transazione

**Informazioni Generali**

|             |  |
|-------------|--|
| Tipologia   | Erogazione (API Gateway)                             |
| Erogatore   | Test   |
| API         | PetStore v1  |
| Azione      | POST_pet   |
| ⚠️ Esito    | Gestione Token Fallita                               |
| Diagnostici | <a href="#">Visualizza</a>   <a href="#">Esporta</a> |

**Dettagli Richiesta**

|                |                              |
|----------------|------------------------------|
| Data Ingresso  | 2019-09-04 16:24:05.876 CEST |
| Bytes Ingresso | n.d.                         |
| Bytes Uscita   | n.d.                         |

**Dettagli Risposta**

|                |                              |
|----------------|------------------------------|
| Data Uscita    | 2019-09-04 16:24:05.878 CEST |
| Bytes Ingresso | 143 B                        |
| Bytes Uscita   | 143 B                        |
| Fault Uscita   | <a href="#">Visualizza</a>   |

**Informazioni Mittente**

|                        |                                      |
|------------------------|--------------------------------------|
| Metodo HTTP            | POST                                 |
| URL Invocazione        | [in] /govway/in/Test/PetStore/v1/pet |
| Indirizzo Client       | 127.0.0.1                            |
| Codice Risposta Client | 400                                  |

**Informazioni Avanzate**

|                       |                                      |
|-----------------------|--------------------------------------|
| ID Transazione        | 5fcf5ee0-7588-4313-bcdd-3a7840289aa7 |
| Dominio (ID)          | domain/gw/GovWay                     |
| Dominio (Soggetto)    | GovWay                               |
| Latenza Totale        | 2 ms                                 |
| Latenza Servizio      | N.D.                                 |
| Latenza Gateway       | 2 ms                                 |
| Porta Inbound         | _gw_Test/PetStore/v1__Specific1      |
| Applicativo Erogatore | gw_Test/gw_PetStore/v1               |

| Visualizza Transazioni (Live) > Dettagli Transazione > Messaggi Diagnostici |                  |                |   |
|---|------------------|----------------|---|
| Lista Diagnostici: record [1 - 6] su 6                                      |                  |                |   |
| Data  | Severità         | Funzione       | Messaggio   |
| 2019-09-04<br>16:24:05.875  | infoIntegration  | RicezioneBuste | Ricevuta richiesta applicativa  |
| 2019-09-04<br>16:24:05.877  | infoIntegration  | RicezioneBuste | Gestione Token [KeyCloak] (Validazione JWT) in corso ...  |
| 2019-09-04<br>16:24:05.877  | errorIntegration | RicezioneBuste | <p>Non è stato riscontrato un token nella posizione [RFC 6750 - Bearer Token Usage];</p> <p>(Authorization Request Header) Non è stato riscontrato un header http 'Authorization' valorizzato tramite autenticazione 'Bearer ' e contenente un token</p> <p>(URI Query Parameter) Non è stato riscontrata la proprietà della URL 'access_token' contenente il token</p> <p>(Form-Encoded Body Parameter) Non è stato riscontrata la presenza di un contenuto 'Form-Encoded'</p> |
| 2019-09-04<br>16:24:05.878  | errorIntegration | RicezioneBuste | Gestione Token [KeyCloak] (Validazione JWT) fallita   |
| 2019-09-04<br>16:24:05.878  | errorProtocol    | RicezioneBuste | Generato messaggio di cooperazione di Errore con identificativo [9419b58e-7693-434f-b1df-fec9e1dda772]  |
| 2019-09-04<br>16:24:05.879  | infoIntegration  | RicezioneBuste | Risposta ({ "type": "https://httpstatuses.com/400", "title": "Bad Request", "status": 400, "detail": "Token non presente", "govway_status": "protocol:GOVWAY-1366" }) consegnata al mittente con codice di trasporto: 400   |

ESPORTA

Fig. 8.3: Messaggi diagnostici della transazione in errore

The screenshot shows a web application interface. At the top, there is a navigation bar with the text "Visualizza Transazioni (Live) > Dettagli Transazione > Fault Uscita". Below this, a dark header bar contains the title "Fault Uscita". The main content area displays a JSON object with line numbers on the left:

```
1 {  
2   "type" : "https://httpstatuses.com/400",  
3   "title" : "Bad Request",  
4   "status" : 400,  
5   "detail" : "Token non presente",  
6   "govway_status" : "protocol:GOVWAY-1366"  
7 }
```

Fig. 8.4: Fault in uscita

### Informazioni Generali

|   |  |
|---|--|
| Tipologia                                 | Erogazione (API Gateway)                             |
| Erogatore                                 | Test   |
| API                                       | PetStore v1  |
| Azione                                    | POST_pet   |
| Profilo Collaborazione                    | Sincrono   |
| <input checked="" type="checkbox"/> Esito | Ok   |
| Diagnostici                               | <a href="#">Visualizza</a>   <a href="#">Esporta</a> |

| Visualizza Transazioni (Live) > Dettagli Transazione > Messaggi Diagnostici |                 |                              |  |
|---|-----------------|------------------------------|--|
| Lista Diagnostici: record [1 - 8] su 8                                      |                 |                              |  |
| Data  | Severità        | Funzione                     | Messaggio  |
| 2019-09-05<br>11:32:00.804  | infoIntegration | RicezioneBuste               | Ricevuta richiesta applicativa   |
| 2019-09-05<br>11:32:00.806  | infoIntegration | RicezioneBuste               | Gestione Token [Keycloak] (Validazione JWT) in corso ...   |
| 2019-09-05<br>11:32:00.808  | infoIntegration | RicezioneBuste               | Gestione Token [Keycloak] (Validazione JWT) completata con successo  |
| 2019-09-05<br>11:32:01.083  | infoProtocol    | RicezioneBuste               | Ricevuto messaggio di cooperazione con identificativo [222152f4-f8a6-410c-831e-4da92b121f41]   |
| 2019-09-05<br>11:32:01.154  | infoProtocol    | ConsegnaContenutiApplicativi | Invio Messaggio di cooperazione con identificativo [222152f4-f8a6-410c-831e-4da92b121f41] in corso (location: http://petstore.swagger.io/v2/pet http-method:POST) ...  |
| 2019-09-05<br>11:32:01.521  | infoProtocol    | ConsegnaContenutiApplicativi | Messaggio applicativo con ID [222152f4-f8a6-410c-831e-4da92b121f41] consegnato al servizio applicativo [gw_Test/gw_PetStore/v1] mediante connettore [http] (location: http://petstore.swagger.io/v2/pet http-method:POST) con codice di trasporto: 200 |
| 2019-09-05<br>11:32:01.524  | infoProtocol    | RicezioneBuste               | Generato messaggio di cooperazione con identificativo [c6991eca-fde0-4065-87a0-bf78410283c8]   |
| 2019-09-05<br>11:32:01.526  | infoIntegration | RicezioneBuste               | Risposta consegnata al mittente con codice di trasporto: 200   |

ESPORTA

## Informazioni Mittente

**Metodo HTTP** POST  
**URL Invocazione** [in] /govway/in/Test/PetStore/v1/pet  
**Indirizzo Client** 127.0.0.1  
**Codice Risposta Client** 200

### Token Info

**Issuer** http://10.114.87.37:8080/auth/realm/testrealm  
**Client ID** testclient  
**Subject** 22158fb1-cea7-46c9-8180-1e30ccb4f944  
**Username** testuser  
**Token Info** [Visualizza](#)

Visualizza Transazioni (Live) > Dettagli Transazione > **Token Info**

### Token Info

```

1  {
2    "valid" : true,
3    "iss" : "http://10.114.87.37:8080/auth/realm/testrealm",
4    "sub" : "22158fb1-cea7-46c9-8180-1e30ccb4f944",
5    "username" : "testuser",
6    "aud" : [ "account" ],
7    "exp" : 1567676163000,
8    "iat" : 1567675863000,
9    "clientId" : "testclient",
10   "userInfo" : {
11     "fullName" : "Utente Test",
12     "firstName" : "Utente",
13     "familyName" : "Test"
14   },
15   "claims" : {
16     "sub" : "22158fb1-cea7-46c9-8180-1e30ccb4f944",
17     "email_verified" : "false",
18     "allowed_origins" : [ "http://servizi-clienti.link.it/*" ],
19     "iss" : "http://10.114.87.37:8080/auth/realm/testrealm",
20     "typ" : "Bearer",
21     "preferred_username" : "testuser",
22     "given_name" : "Utente".

```

[DOWNLOAD](#)