
Scenari Applicativi

Release 3.3.8

Link.it

11 ott 2022

1	Ambiente di esecuzione	1
1.1	Prerequisiti	1
1.2	Avvio Ambiente	2
1.3	Progetto Postman	4
2	Erogazione pubblica	11
2.1	Obiettivo	11
2.2	Sintesi	11
2.3	Esecuzione	11
2.4	Configurazione	12
3	Erogazione OAuth	17
3.1	Obiettivo	17
3.2	Sintesi	17
3.3	Esecuzione	18
3.4	Configurazione	21
4	Erogazione REST ModI	27
4.1	Obiettivo	27
4.2	Sintesi	27
4.3	Esecuzione	29
4.4	Configurazione	34
5	Fruizione REST ModI	41
5.1	Obiettivo	41
5.2	Sintesi	41
5.3	Esecuzione	43
5.4	Configurazione	46
6	Erogazione SOAP ModI	49
6.1	Obiettivo	49
6.2	Sintesi	49
6.3	Esecuzione	50
7	Fruizione SOAP ModI	55
7.1	Obiettivo	55
7.2	Sintesi	55

7.3	Esecuzione	57
8	Monitoraggio	61
8.1	Transazione in errore	61
8.2	Transazione con esito corretto	65

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

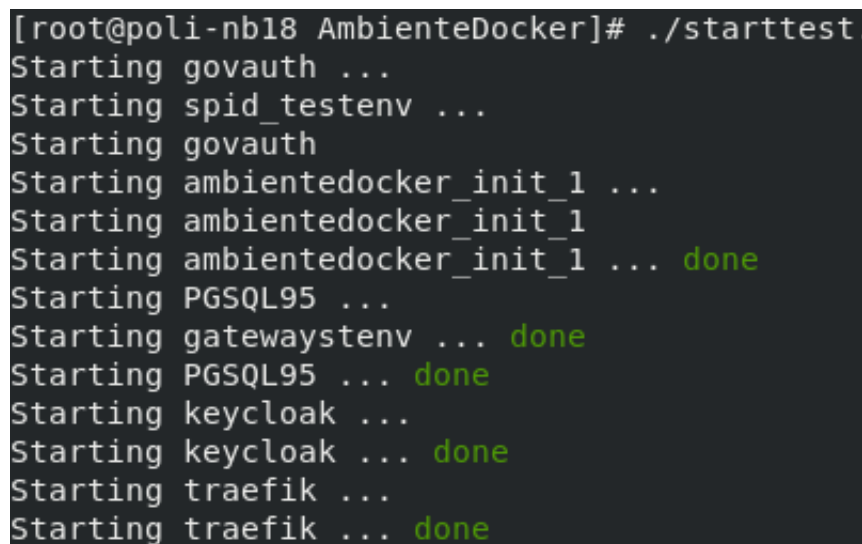
1.2 Avvio Ambiente

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.sh
Starting govauth ...
Starting spid_testenv ...
Starting govauth
Starting ambienedocker_init_1 ...
Starting ambienedocker_init_1
Starting ambienedocker_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
```



Fig. 1.2: Accesso alla console di gestione

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

```
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
```



Fig. 1.3: Accesso alla console di monitoraggio

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).

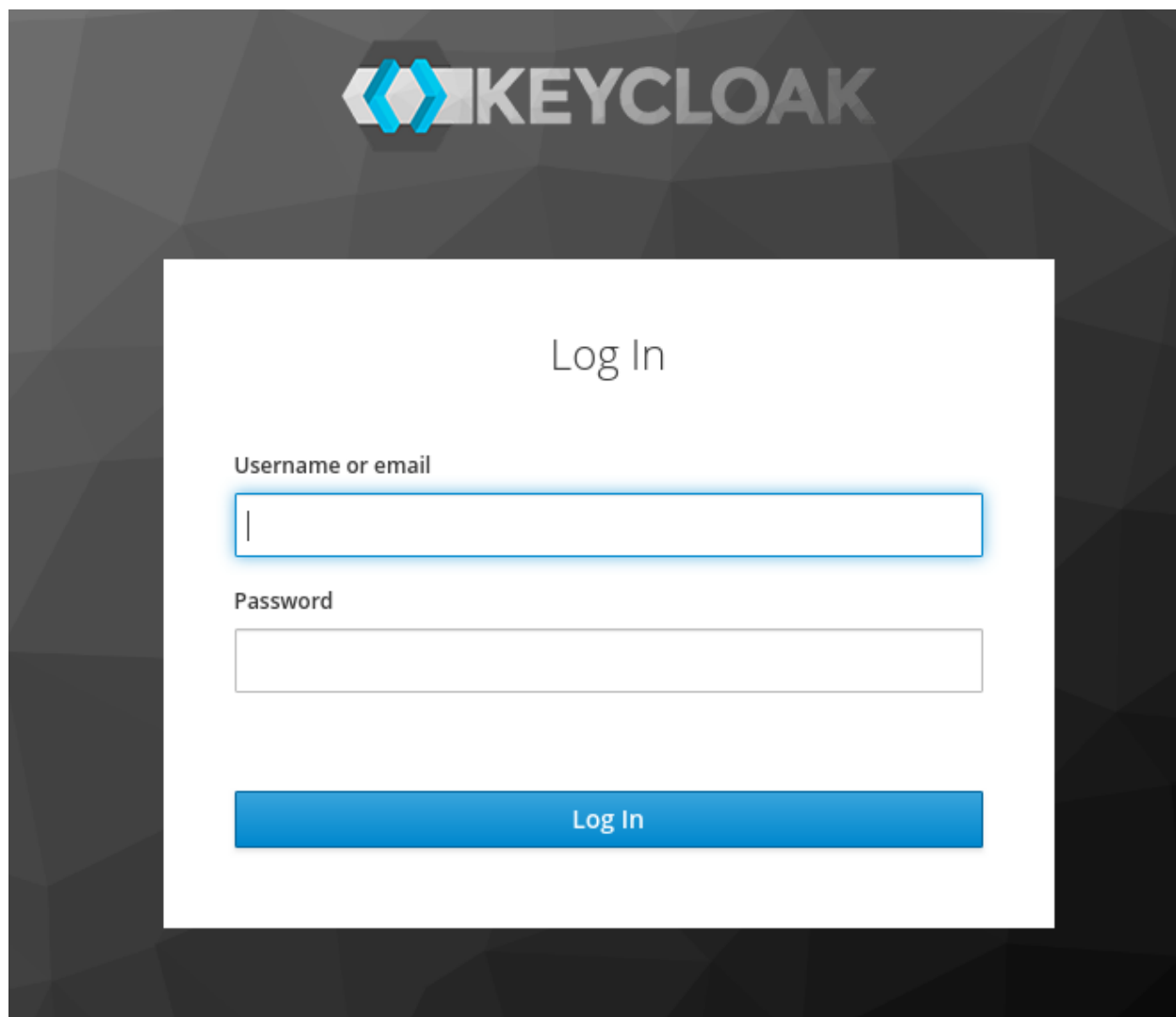


Fig. 1.4: Accesso alla console dell'authorization server

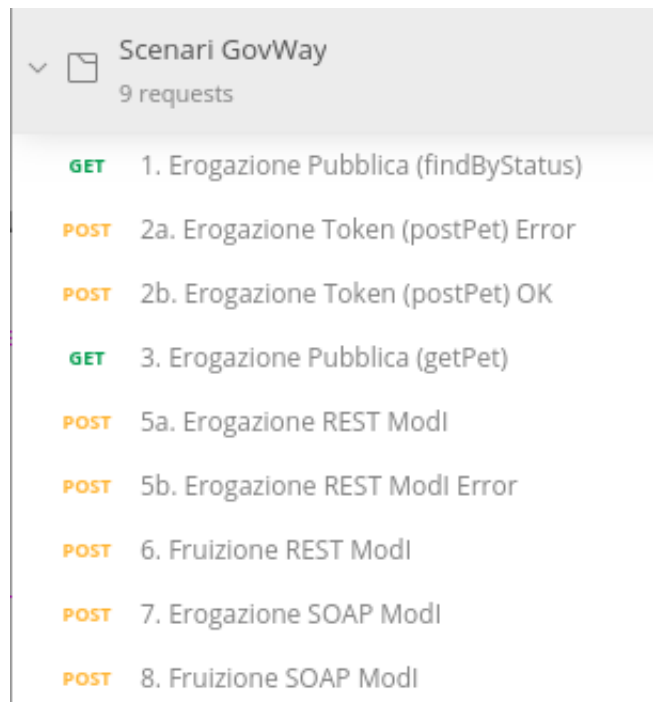


Fig. 1.5: Indice della collection Postman

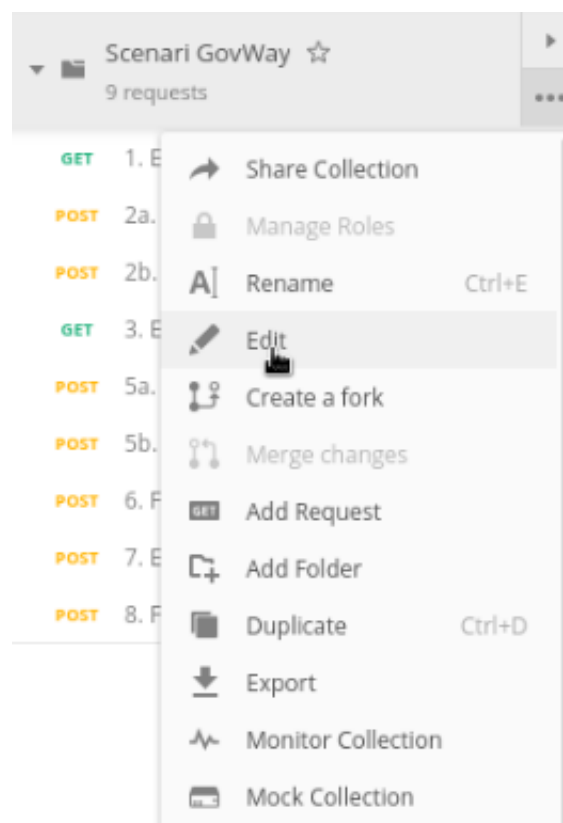


Fig. 1.6: Configurazione Collection Postman

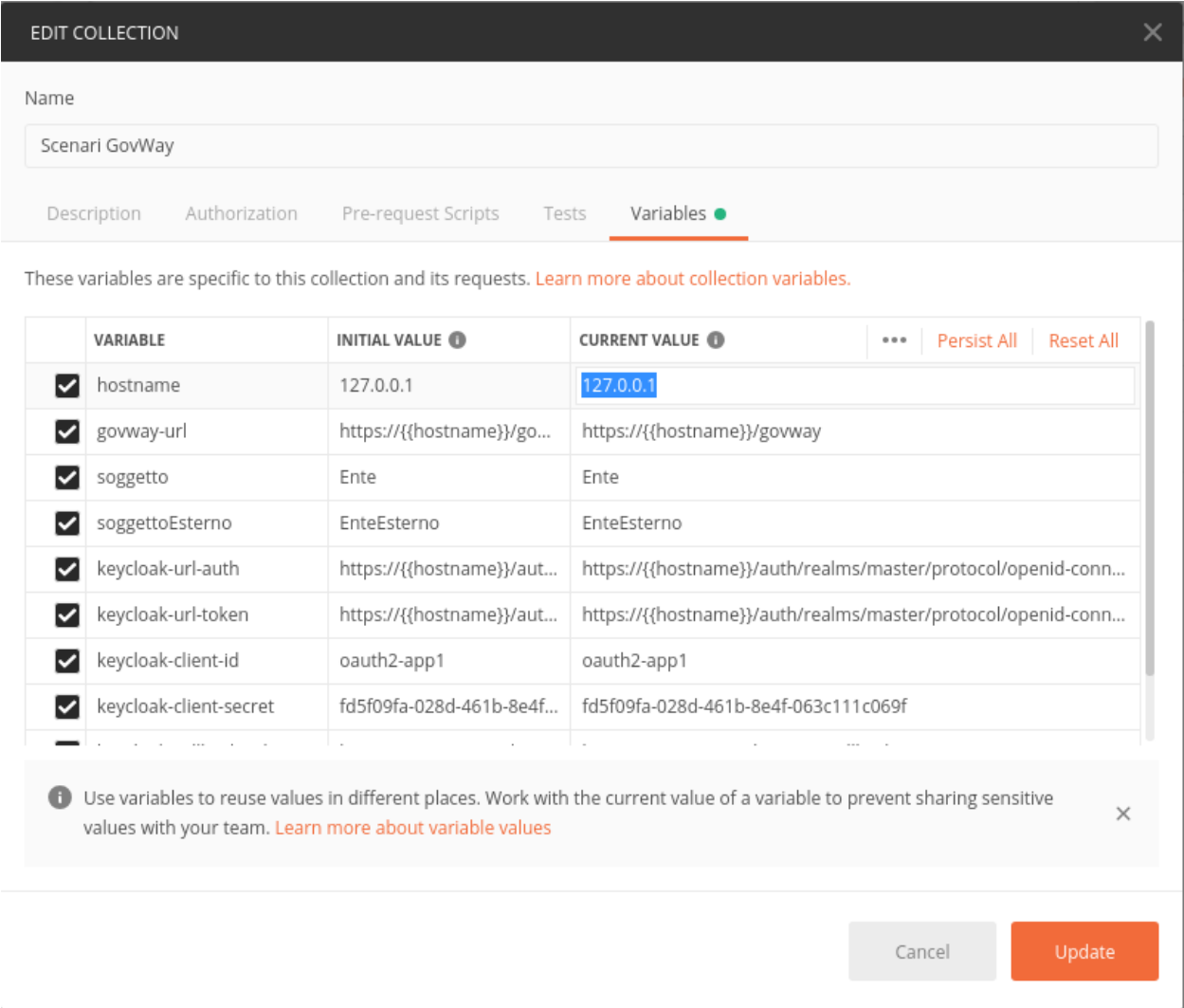


Fig. 1.7: Configurazione Hostname nella Collection Postman

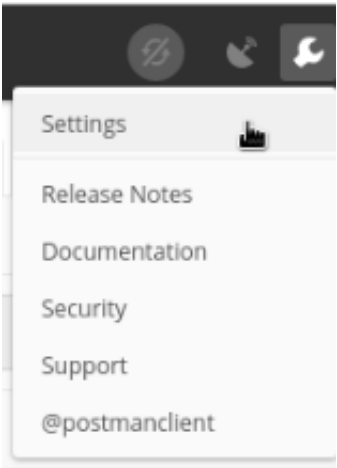


Fig. 1.8: Configurazione Generale Postman

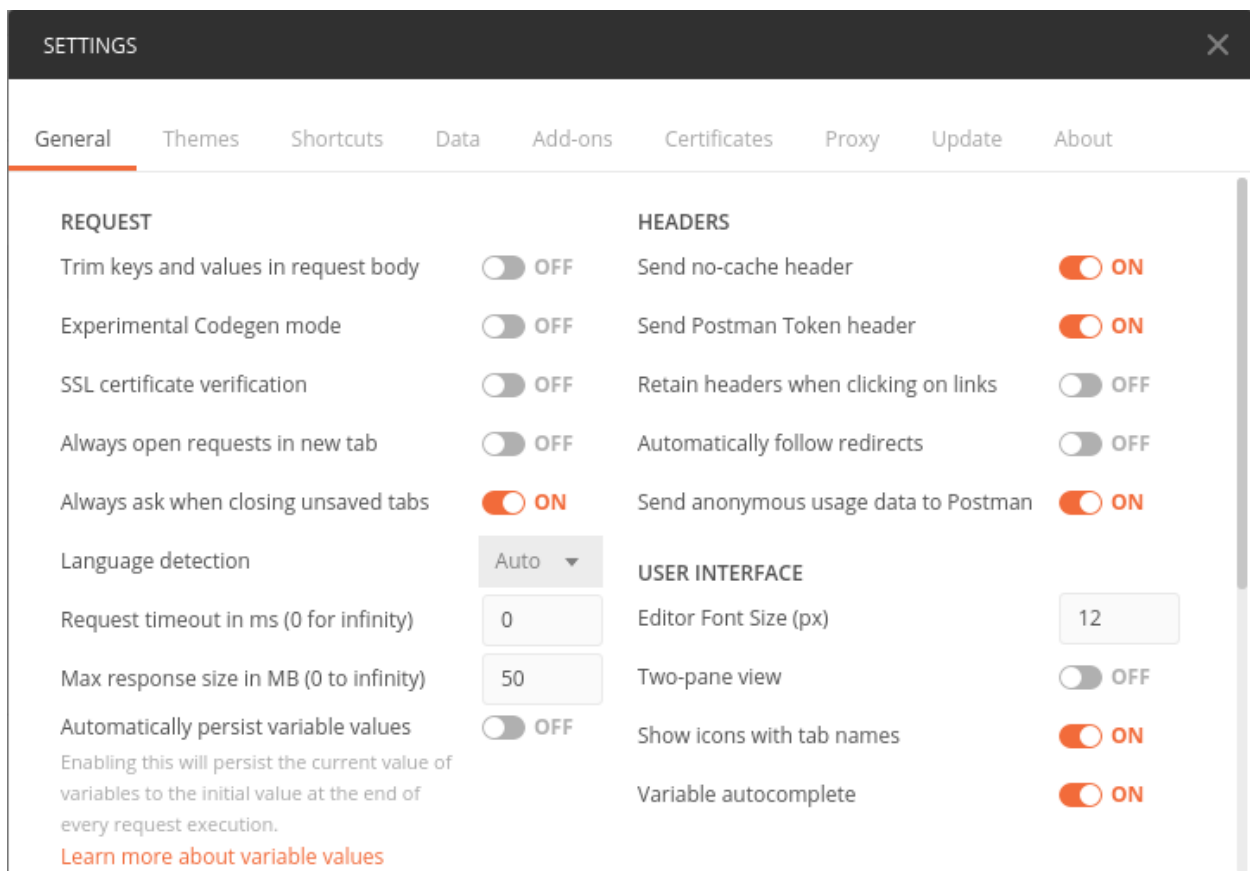


Fig. 1.9: Configurazione SSL Postman

SETTINGS

General

Themes

Shortcuts

Data

Add-ons

Certificates

Proxy

Update

About

Global Proxy Configuration

OFF

Specify a global proxy setting to act as an intermediary for requests sent to the server.

[Learn more about using a global proxy](#)

Proxy Type

☒

HTTP

☐

HTTPS

Proxy Server

proxy

:

8080

Proxy Auth

☐

OFF

Username

Username

Password

Password

Use System Proxy

OFF

Enable this option to allow Postman to use the system's default proxy configurations.

Fig. 1.10: Configurazione Proxy Postman

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.

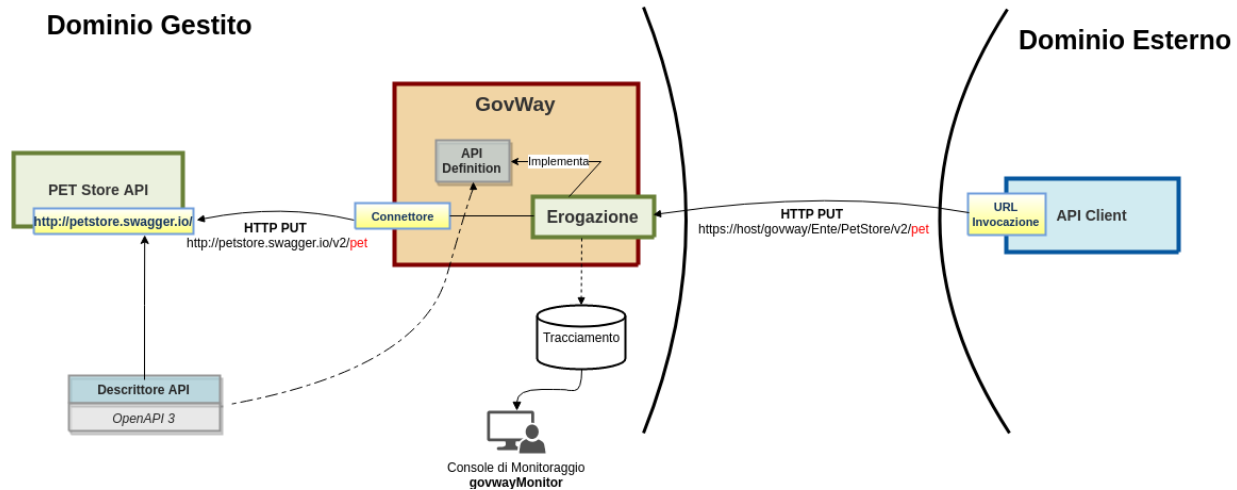


Fig. 2.1: Erogazione ad accesso pubblico

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 (descrittore scaricabile al seguente indirizzo: <https://raw.githubusercontent.com/link-it/govway/master/resources/openapi/3.0/openapi.yaml>).

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.

Nota: Verifica del certificato server

Poichè il servizio PetStore è disponibile solamente in https, modificare il prefisso dell'endpoint fornito. Inoltre per validare il certificato ritornato dal server “petstore.swagger.io” deve essere effettuata una opportuna configurazione del trustStore tls come descritto nella sezione avanzate_connettori_https. Poichè non è obiettivo di questo scenario si suggerisce di disabilitare la validazione del certificato server.

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).

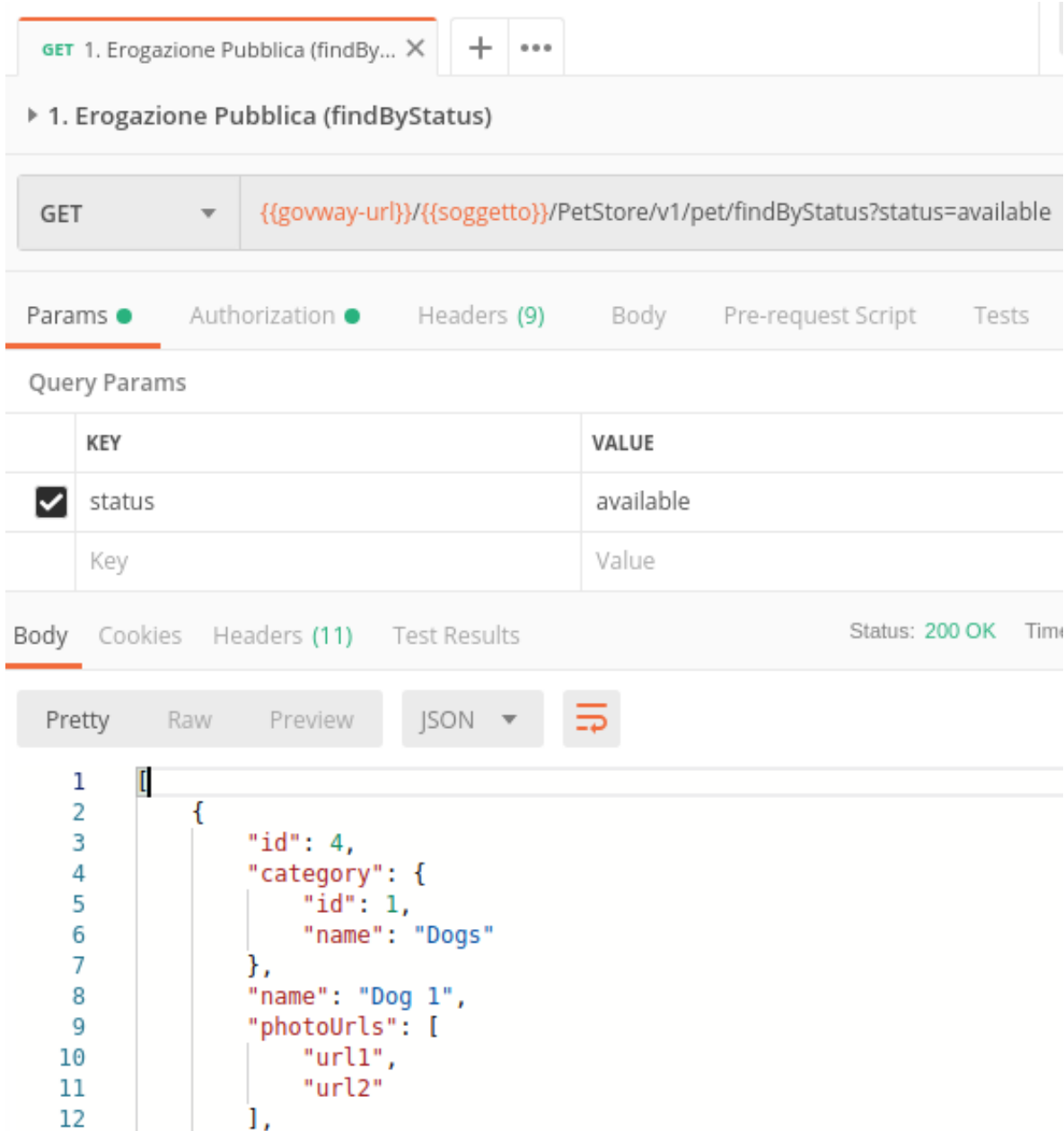


Fig. 2.2: Erogazione pubblica, esecuzione da Postman

Erogazioni > Aggiungi

Note: (*) Campi obbligatori

Informazioni Generali

API

Nome
PetStore v1

Tipo
Rest

Controllo degli Accessi

Accesso API
pubblico

Connettore

Endpoint *
https://petstore.swagger.io/v2

Autenticazione Http
☐

Autenticazione Token
☐

Autenticazione Https
☒

Proxy
☐

Ridefinisci Tempi Risposta
☐

Autenticazione Https

Tipologia
TLSv1.3

Verifica Hostname
☒

Autenticazione Server

Verifica
☐

Autenticazione Client

Abilitato
☐

SALVA

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

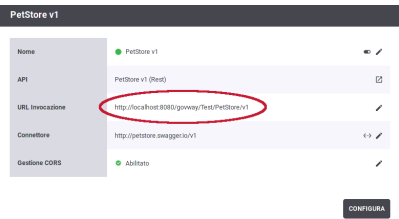


Fig. 2.4: Dettaglio dell'erogazione

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.

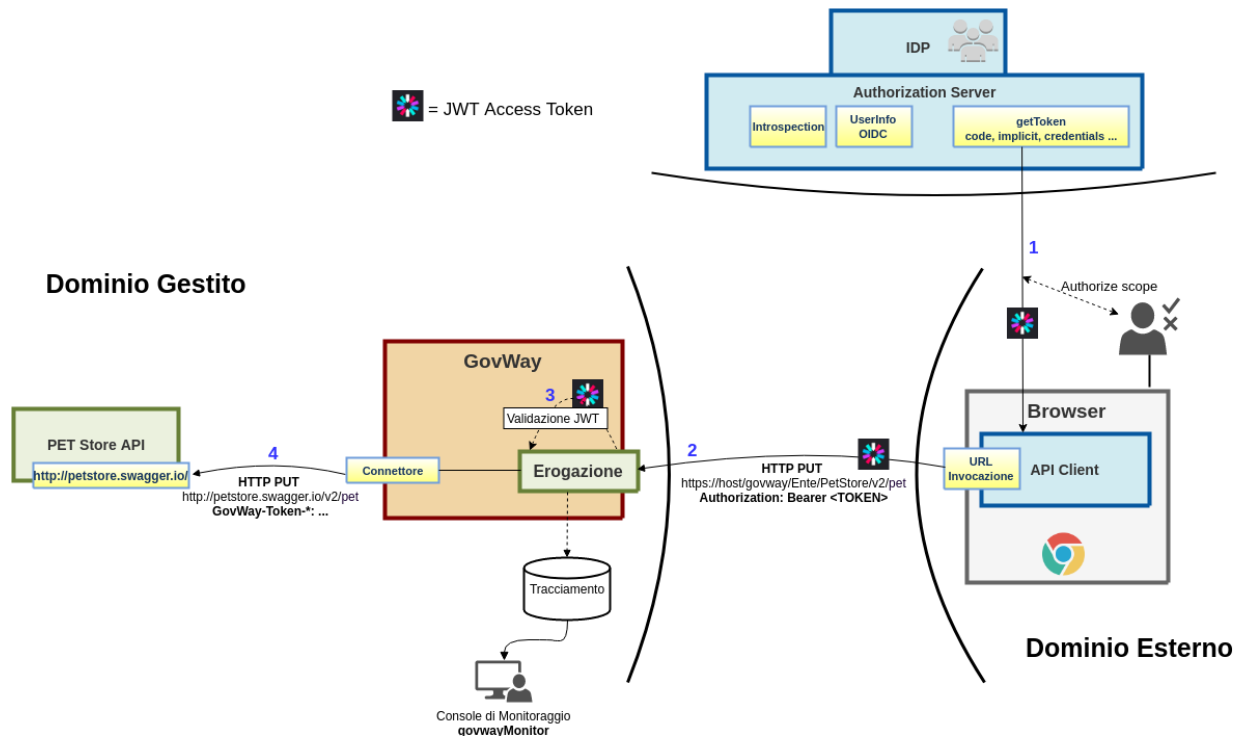


Fig. 3.1: Erogazione OAuth

3.3 Esecuzione

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

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»

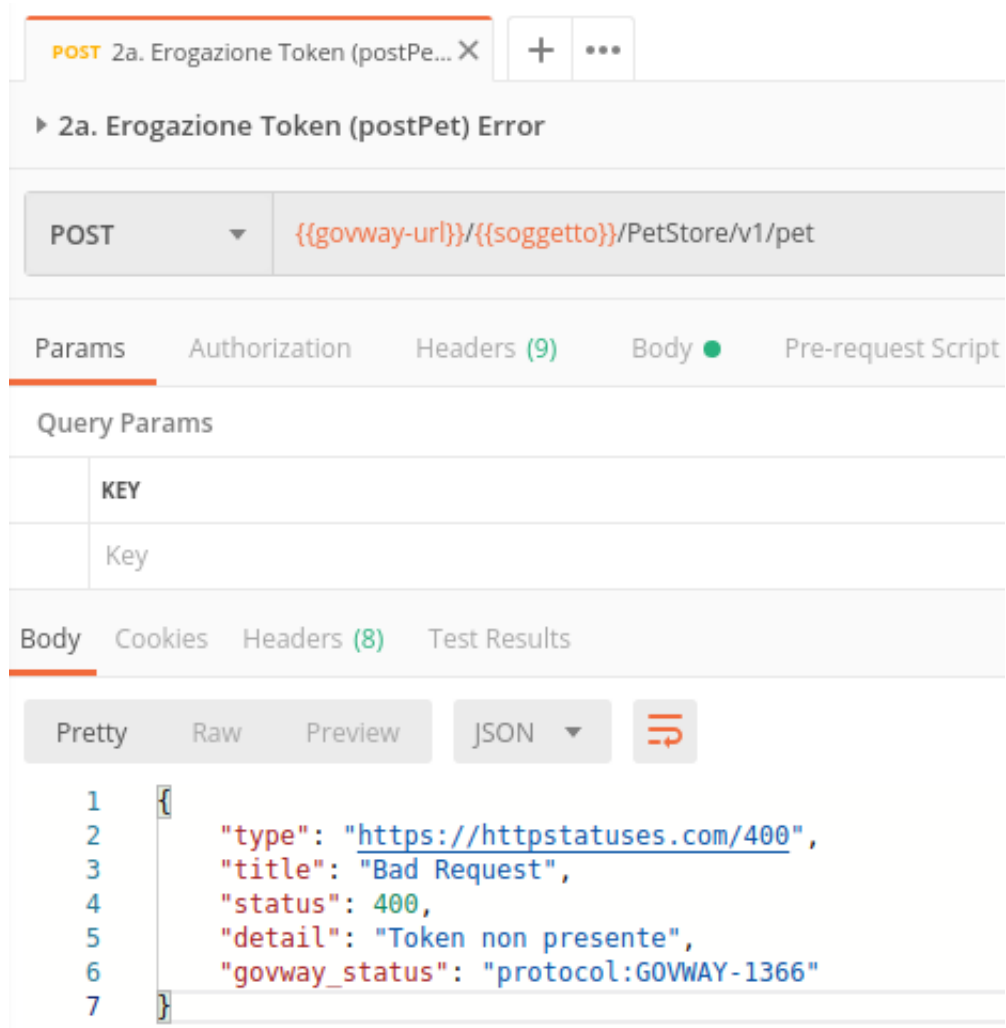


Fig. 3.2: Invocazione della POST /pet senza token

GET NEW ACCESS TOKEN
✕

Token Name	<input type="text" value="Token Name"/>
Grant Type	Authorization Code ▼
Callback URL ⓘ	<input type="text" value="{{keycloak-callback-url}}"/>
Auth URL ⓘ	<input type="text" value="{{keycloak-url-auth}}"/>
Access Token URL ⓘ	<input type="text" value="{{keycloak-url-token}}"/>
Client ID ⓘ	<input type="text" value="{{keycloak-client-id}}"/>
Client Secret ⓘ	<input type="text" value="{{keycloak-client-secret}}"/>
Scope ⓘ	<input type="text" value="e.g. read:org"/>
State ⓘ	<input type="text" value="State"/>
Client Authentication	Send as Basic Auth header ▼

Request Token

Fig. 3.3: Ottenimento nuovo 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
```

- 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 a REST client interface with the following components:

- Request Bar:** Method **POST**, URL `{{govway-url}}/{{soggetto}}/PetStore/v1/pet`, and a **Send** button.
- Params Tab:** Contains a **TYPE** dropdown set to **OAuth 2.0**. Below it, text explains that authorization data is generated automatically. There is a section to "Add authorization data to" with a dropdown set to **Request Headers**, and a **Preview Request** button.
- Authorization Tab:** Shows an **Access Token** field with the value `eyJhbGciOiJSUzI1NiIsInR5cCIgOiA...` and a **Get New Access Token** button.
- Body Tab:** Shows the request body in **JSON** format, pretty-printed. The JSON is:


```

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 }
```
- Test Results Bar:** Shows **Status: 200 OK**, **Time: 734ms**, **Size: 593 B**, and a **Save** button.

Fig. 3.4: Invocazione della POST /pet con token

Erogazioni > PetStore v1 (Test) > Configurazione > **Aggiungi**

Note: (*) Campi obbligatori

Configurazione

Nome Gruppo * Scritture

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 Nuova

Controllo degli Accessi

Accesso API autenticato

SALVA

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

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

Controllo Accessi del gruppo 'Scritture'

Note: (*) Campi obbligatori

Autenticazione Token

Stato

abilitato

Policy *

KeyCloak

Token Opzionale

☐

Validazione JWT

abilitato

Token Forward

abilitato

Required Claims

Issuer

☐

ClientId

☐

Subject

☐

Username

☐

eMail

☐

Autenticazione Trasporto

Stato

disabilitato

Autorizzazione

Stato

disabilitato

Autorizzazione Contenuti

Stato

disabilitato

SALVA

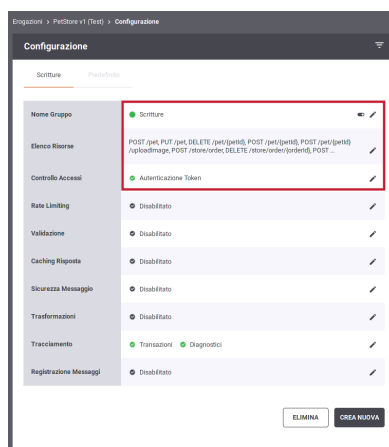


Fig. 3.7: Riepilogo della configurazione effettuata

Erogazione REST ModI

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 pattern di sicurezza canale «ID_AUTH_CHANNEL_02»
3. La confidenzialità e autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_02»
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva previsto nel pattern «INTEGRITY_REST_01»
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

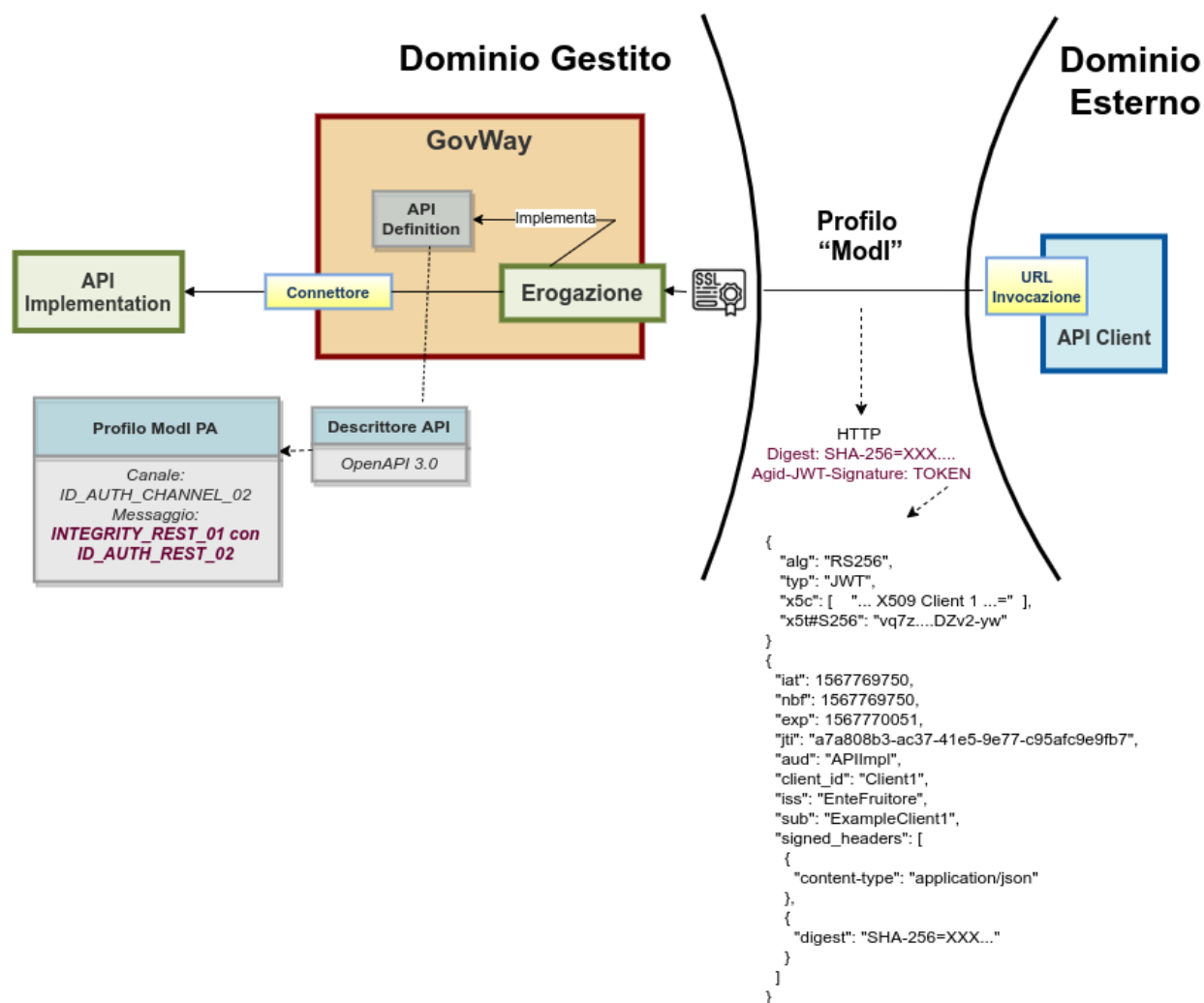


Fig. 4.1: Erogazione ModI

4.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API «PetStore», basata su REST, pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «INTEGRITY_REST_01 con ID_AUTH_REST_02».
- un'istanza Govway per la gestione del profilo ModI 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 "<https://petstore.swagger.io/>".

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

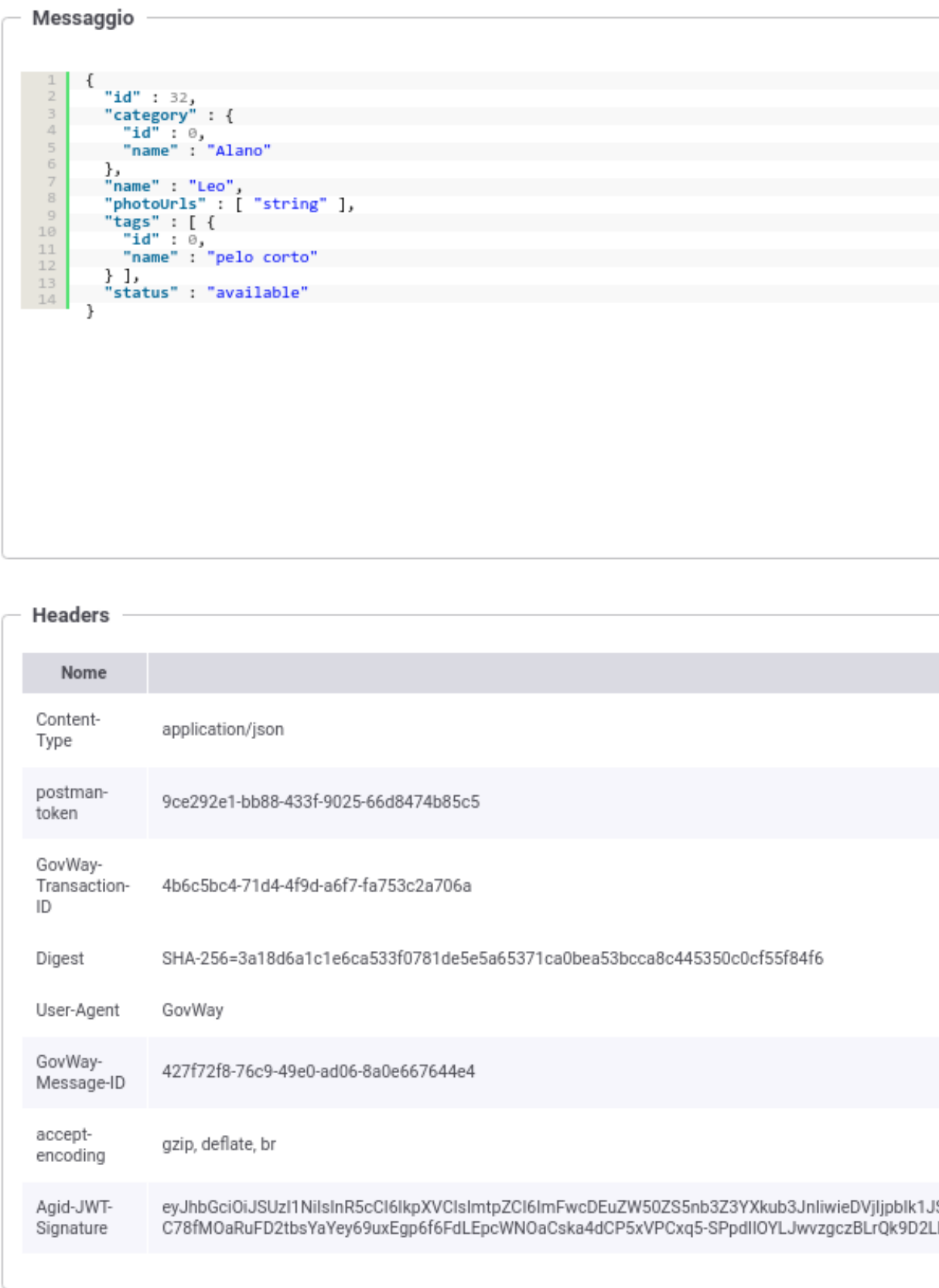
Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console govwayMonitor:

1. Lo scambio del messaggio con il dominio fruitore (comunicazione interdominio) avviene in accordo al pattern «ID_AUTH_CHANNEL_02» 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 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 14:29:03.352	infoIntegration	RicezioneBuste	Autenticazione [ssl] in corso (SSL-Subject 'CN=enteEsterno.govway.org, O=govway.org, C=it') ...
2019-10-01 14:29:03.359	infoIntegration	RicezioneBuste	Autenticazione [ssl] effettuata con successo

Fig. 4.2: Sicurezza canale «ID_AUTH_CHANNEL_02»

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 «Agit-JWT-Signature», 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 pattern 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).



HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "ExampleClient1",
  "x5c": [

    "MIIDXjCCAkagAwIBAgIBAjANBgkqhkiG9w0BAQsFADBSMQswCQYDVQ
    QGEwJjVDEOMAwGA1UECBMFSXRhbHkxDTALBgNVBACtBFBpc2ExEDA0B
    gNVBAoTB0V4YW1wbGUxEjAQBgNVBAMTCUV4YW1wbGVdQTAeFw0xOTA3
    MDkxMDI2MDBaFw00MDA3MzAxMDI2MDBaMFcxCzAJBgNVBAYTAk1UMQ4
    wDAYDVQQIEwVJdGFseTENMAAsGA1UEBxMEUGlZYTEQMA4GA1UEChMHRX
    hhbXBsZTEXMBUGA1UEAxMORXhhbXBsZUNsaWVudDEwggEiMA0GCSqGS
    Ib3DQEBAQUAA4IBDwAwggEKAoIBAQDwhiesh5jK4IJlAm92TEvlsPn6
    /4vZvACCLPhkww+paqFuCwaad7JodAgov6KGIpGBsNPTYcg0Ut4mnq5
    cLFG7oxhUReSm4jUq17bGqUbPDYX5YAs2SgWBpd4isTAi6CP156KqoF
    t5111A+vtiZceJk5L01WxBJ7JFMAEh8y2+uopRrxHhTaAUCnnCjZyAJ
    TYOTWAn8HaaIJGC97CLYRrZJK644A1OG8ATACTVzFfBlzFWo4CP0B4p
    7uQ+zv1WAKmca6i22uGqUu1PSE+mKPZPVL+vYQ1mtD17HiGQUXyrYSn
    Gq94pwXluZNo1LV70MoK2Em0arX077MQssUDHhtj
    /AgMBAAGjOjA4MAkGA1UdEwQCMAAwHQYDVR00BBYEFFfKI7UGhJZrrD
    j6KUd+IrW78z1vMAwGA1UdDwQFAwMH
    /4AwDQYJKoZIhvcNAQELBQADggEBAFZGYkr9C5Sj3rQ0I5kgnx7qLVk
    8hj++uMBIEuhAnte9bzZ4pG1Ba1R4oPnIjExgzuz1PxM90G00EDQ7J9
    ibKNui90AASo2TCeJ95/7rwK3TnryL6yCZ+UGNE0y8ICxJ6Csd2Pac8
    /vrZB30NzbnNGj4AhttpGEow0oscYw5NEe809VyC3tfZNPYHZ4fa1A7
    /0SugmyY8HR0
    /R2VyvoMi7oy7s16WcwR6n5cG1xucDTh1VociU9brKvZXG8hovBLnRb
    w9RX4B8CXei8sZ6i1D14DZD9EQxKb23yWQB1pnFXe5PUMTNpLJW4ign
    KI2oIkGPxByMeIIH8LKP+779BM4S0I="
  ]
}
```

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=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcca8
c445350c0cf55f84f6"
    },
    {
      "content-type": "application/json"
    }
  ]
}
```

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

Informazioni Modì PA

ProfiloSicurezzaMessaggio INTEGRITY_REST_01 con ID_AUTH_REST_02

ProfiloSicurezzaCanale ID_AUTH_CHANNEL_02

ProfiloInterazione Accesso CRUD

Sicurezza Messaggio

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

X509-Subject CN=app1.ente.govway.org, O=govway.org, C=it

Digest SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcca8c445350c0cf55f84f6

Subject App1

Issuer Ente

ClientId app1.ente.govway.org

Audience petstore.enteEsterno.govway.org

MessageId 427f72f8-76c9-49e0-ad06-8a0e667644e4

Expiration 2020-11-16_16:25:13.000

NotBefore 2020-11-16_16:24:13.000

IssuedAt 2020-11-16_16:24:13.000

Headers HTTP Firmati

content-type application/json

digest SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcca8c445350c0cf55f84f6

Fig. 4.6: Traccia della richiesta elaborata dall'erogatore

4.3.1 Conformità ai requisiti ModI

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

1. La trasmissione è basata sul pattern «ID_AUTH_CHANNEL_02», 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 pattern «ID_AUTH_REST_02» e «INTEGRITY_REST_01», 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 pattern 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 previsto dalla specifica del Modello di Interoperabilità si deve attivare, nella testata dell'interfaccia, il Profilo di Interoperabilità "ModI" (Fig. 4.7).



Fig. 4.7: Profilo ModI 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 prevedendo la persistenza quanto meno delle comunicazioni scambiate tra i due gateway (Fig. 4.8 e Fig. 4.9).

Si procede quindi con i passi di configurazione del servizio.

Richiesta

Stato	abilitato
Ingresso	
Headers	disabilitato
Body	disabilitato
Attachments	disabilitato
Uscita	
Headers	abilitato
Body	abilitato
Attachments	abilitato

Fig. 4.8: Abilitazione del salvataggio delle richieste in uscita

4.4.2 Registrazione API

Si registra l'API «PetStore», fornendo il relativo descrittore OpenAPI 3, selezionando i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_REST_01 con ID_AUTH_REST_02» (sicurezza messaggio) nella sezione «ModI» (Fig. 4.10).

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 omissso. 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).

Risposta

Stato

abilitato

Ingresso

Headers

abilitato

Body

abilitato

Attachments

abilitato

Uscita

Headers

disabilitato

Body

disabilitato

Attachments

disabilitato

Fig. 4.9: Abilitazione del salvataggio delle risposte in ingresso

4.4.4 Erogazione

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

La sezione «ModI 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

Profilo Sicurezza Canale

Profilo
ID_AUTH_CHANNEL_02

Direct Trust mutual Transport-Level Security

Profilo Sicurezza Messaggio

Profilo
INTEGRITY_REST_01 con ID_AUTH_REST_02

Integrità payload del messaggio + unicità del token

Header HTTP del Token
Agid-JWT-Signature

Applicabilità
Richiesta e Risposta

Informazioni Utente
☐ Dati dell'utente che effettua la richiesta ⓘ

Digest Richiesta
☐ Non ripudiabilità della trasmissione ⓘ

Fig. 4.10: Configurazione Profilo ModI sulla API

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)

Modi PA - Richiesta

Profilo Sicurezza Messaggio

Riferimento X.509

x5c (Certificate Chain)
x5t#256 (Certificate SHA-256 Thumbprint)
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

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

```

graph TD
    A[Autorizzazione Modi PA] --> B[Sicurezza Messaggio  
Applicativo (2)]
    B --> C[Applicativo (2)]
  
```

Fig. 4.14: Controllo accessi con autorizzazione degli applicativi esterni

4.4. Configurazione

39

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 in accordo ad una API condivisa
2. La comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»
3. La confidenzialità e autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_02»
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva previsto nel pattern «INTEGRITY_REST_01»
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

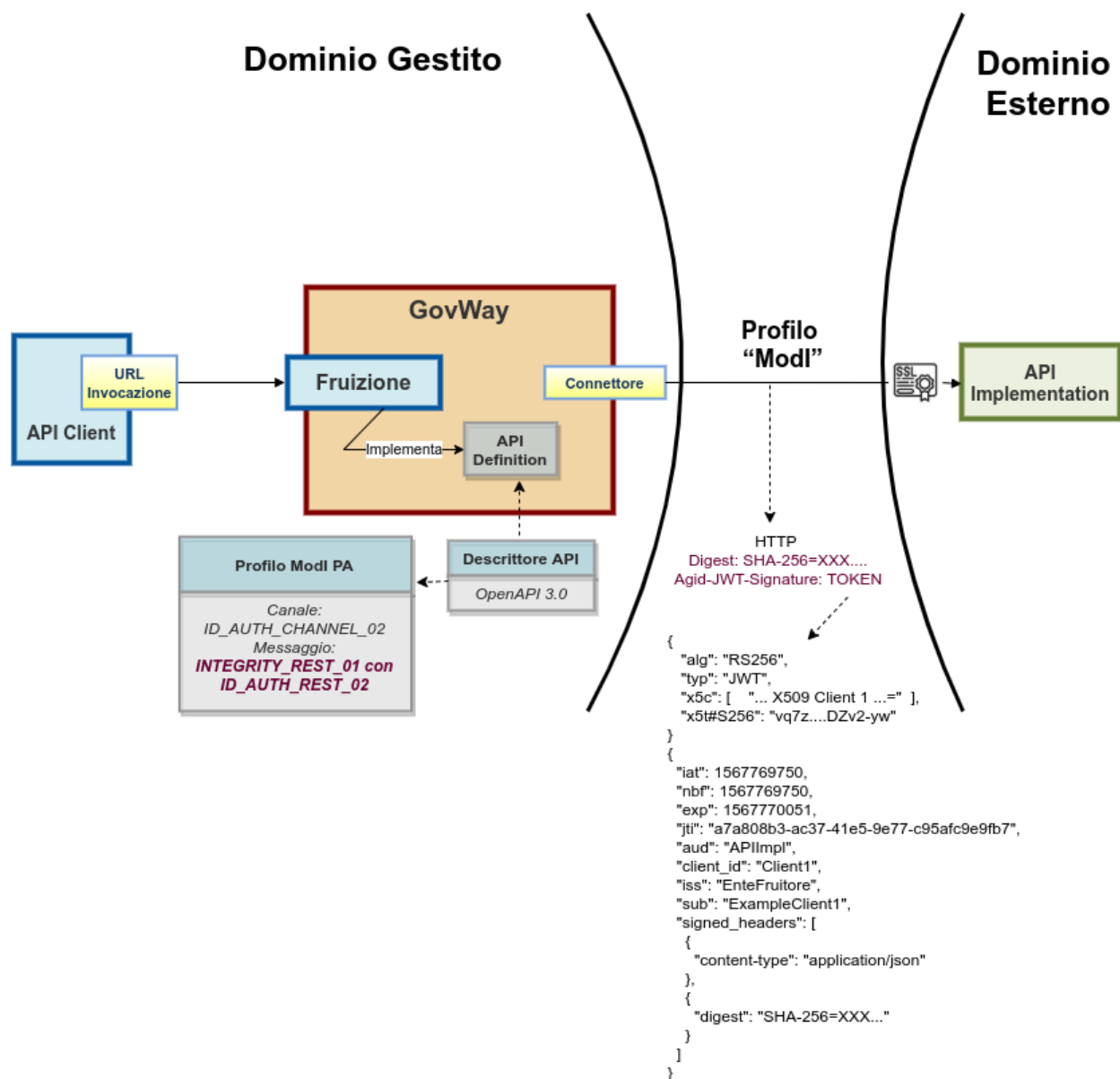


Fig. 5.1: Fruizione ModI

5.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API «PetStore», basata su REST, pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «INTEGRITY_REST_01 con ID_AUTH_REST_02».
- Un'istanza Govway per la gestione del profilo ModI 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», 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 pattern «ID_AUTH_CHANNEL_02» 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

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

1. La trasmissione è basata sul pattern «ID_AUTH_CHANNEL_02», 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 pattern «ID_AUTH_REST_02» e «INTEGRITY_REST_01», 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 pattern 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.

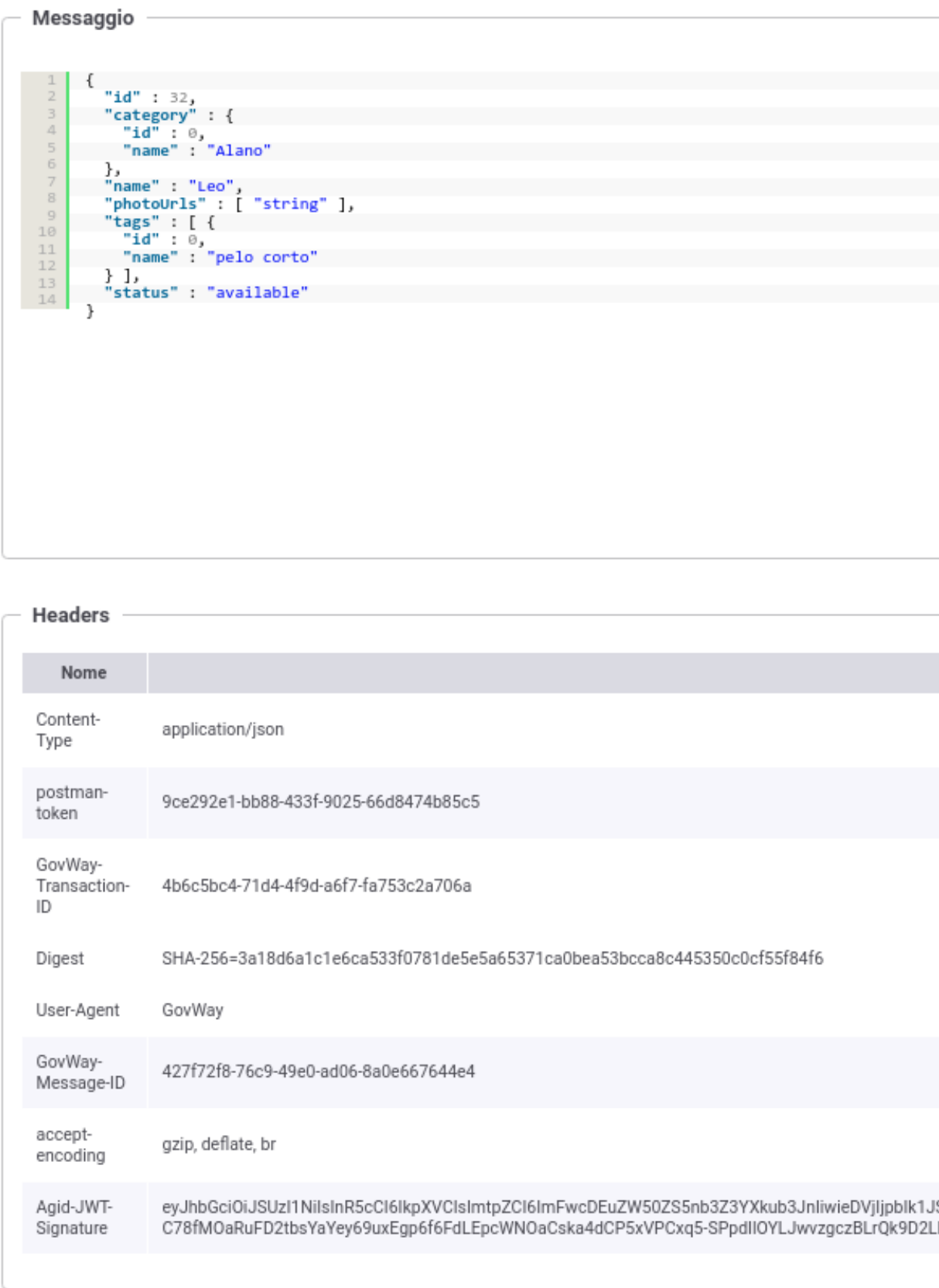


Fig. 5.2: Messaggio di richiesta in uscita (con token di sicurezza inserito nell'header HTTP)

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

Fig. 5.3: Sicurezza canale «ID_AUTH_CHANNEL_02» sulla fruizione

Informazioni Modl PA

ProfiloSicurezzaMessaggio	INTEGRITY_REST_01 con ID_AUTH_REST_02
ProfiloSicurezzaCanale	ID_AUTH_CHANNEL_02
ProfiloInterazione	Accesso CRUD

Sicurezza Messaggio

Digest	SHA-256=ec2592738426e38b9e61f4d00507f11ba362ed4335babe912ee222bc937616ff
ClientId	PetStore/v1
Subject	PetStore/v1
Issuer	EnteEsterno
MessageId	2d3bd9e2-ff0d-46ba-879c-92df6a1a2f60
Audience	app1.ente.govway.org
NotBefore	2020-11-16_16:24:14.000
Expiration	2020-11-16_16:25:14.000
IssuedAt	2020-11-16_16:24:14.000
X509-Issuer	CN=GovWay CA, O=govway.org, C=it
X509-Subject	CN=app1.enteEsterno.govway.org, O=govway.org, C=it

Headers HTTP Firmati

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

Fig. 5.4: Traccia della risposta

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 si deve attivare, nella testata dell'interfaccia, il Profilo di Interoperabilità «ModI» (Fig. 5.5).



Fig. 5.5: Profilo ModI 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 pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_REST_01 con ID_AUTH_REST_02» (sicurezza messaggio) nella sezione «ModI» (vedi [Registrazione API](#)).

5.4.3 Applicativo

Si configura l'applicativo mittente indicando, nella sezione ModI, 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 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 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 ☒

Archivio

Tipo

Password *

Alias Chiave Privata *

Password Chiave Privata *

Reply Audience/WSA-To

Identificativo dell'Applicativo scambiato nei token di sicurezza delle risposte

Fig. 5.6: Configurazione applicativo fruitore

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. 5.7: Configurazione richiesta della 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. 5.8: Configurazione risposta della fruizione

Erogazione SOAP ModI

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»
3. La confidenzialità e autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_02»
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva previsto nel pattern «INTEGRITY_SOAP_01»
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

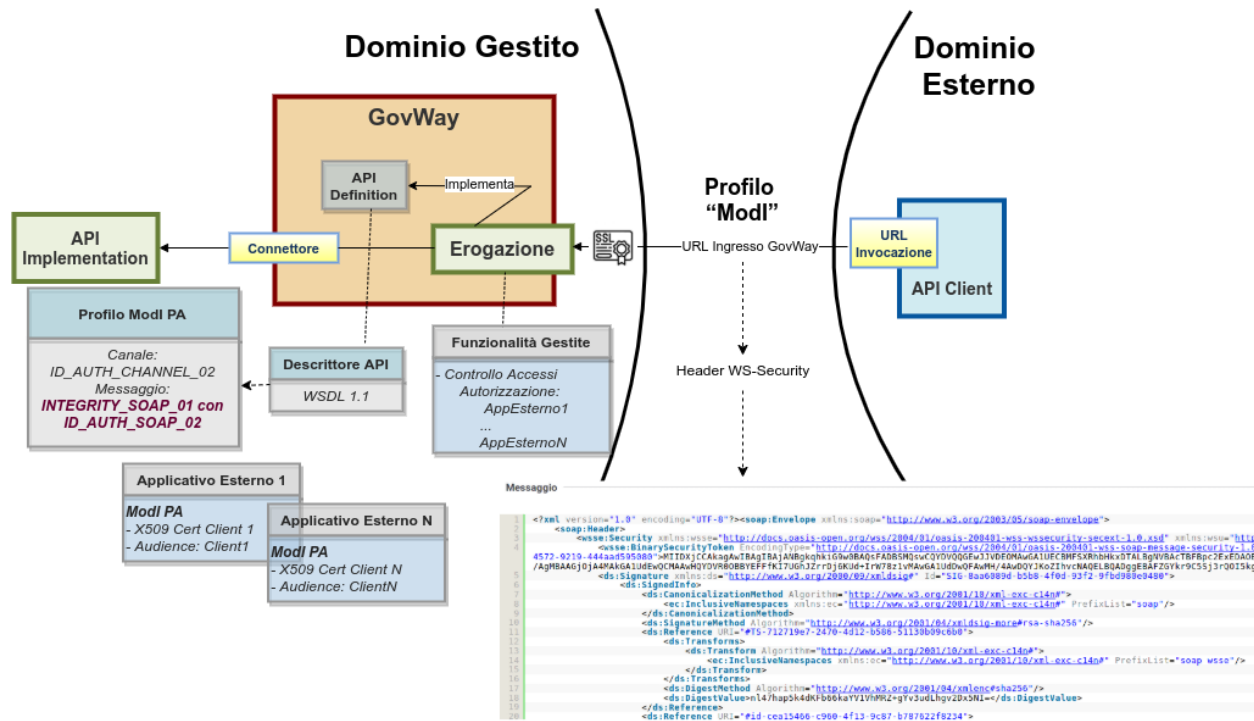


Fig. 6.1: Erogazione SOAP ModI

6.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API di esempio (Credit Card Verification), basata su SOAP, pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02», «ID_AUTH_SOAP_02» e «INTEGRITY_SOAP_01».
- un'istanza Govway per la gestione del profilo ModI 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 “<https://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», 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 pattern «ID_AUTH_CHANNEL_02», si procede come già illustrato per *Erogazione REST ModI*
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 pattern 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://
4       <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#
c7761d94d64f">MIE/zCCAuegAwIBAgICAN4wDQYJKoZIhvcNAQELBQAwNjELMAkGA1UEBhMCaXQxEzARBgNVBAoMCmdvdndheS5vcmcxEjAQBGNVBAAMCudvdldheSBDQTAef
/Wudo6/rYXIVIDHLYMjybp/fL0SL8SKA6uW9swPXcoGJPk9aqw0ivQ/8w2Lpvi1657H+BtNie8FhSmUnL7C25HBa/WivKh782i3F5LYc4sY8H9nfc/fa6QUouiDLTXwOhKwzNl
/zAJBgNVHRMEAjAAMBEGCWCAGSAGG+EIBAQQEAWIHgDAzBgLghkgBhvCAQ0EJhYkT3BlbLNTTCBHZW5lcmF0ZWQgQ2xpZW50IENlcnRpZmljYXRlMB0GA1UdDgQWBBRUAiCyENl
/JIBWmVuatppwNcJRTZi06qmIElqmo8TWLZj0VMxI/+zSwVQUTWNGNs0zziTDS11rmeEldiRcbKVvNcxt rPHH4Ysh5JdIp1fN7G3L4CaTjJHBHo2Ufua0eb03dFqgRc6QzmEr
/OFgpiDpcA7fXITXDgDoKm+WaqMAZ7s6DEmgW+h7KLk6ub0hVewzukaSdpYbqycioVDaomD4yWvaI5csmubwSRIAlRH80uew0JcyeJSfEY8f5LFud0B1G934DtI4HnT2CBM8
/NKL76fLQPRGAcHtEV4x0nvCe8Nwm28oAPi0hYpPutv5YIP5Y=</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 fruitore

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.

4. 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

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

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario *Erogazione REST ModI*. 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 pattern:

- «ID_AUTH_CHANNEL_02» per la sicurezza canale
- «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_02» per la sicurezza messaggio

Informazioni ModI PA

ProfiloSicurezzaMessaggio INTEGRITY_SOAP_01 con ID_AUTH_SOAP_02

ProfiloSicurezzaCanale ID_AUTH_CHANNEL_02

ProfiloInterazione Bloccante

Sicurezza Messaggio

MessageId f7ddaa57-c3c3-4a13-91fb-feadc664c961

WSA-From app1.enteesterno.govway.org

WSA-To luhnCheckerSoap.ente.govway.org

Digest SHA256=ABI8LEJJU5n4C7Cacet046YoHG3huXPt8psR JW2hwg=

Expiration 2020-11-16_16:26:24.780

IssuedAt 2020-11-16_16:25:24.780

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

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

Fig. 6.3: Traccia della richiesta elaborata dall'erogatore

6.3.3 Erogazione

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

ModI PA - Richiesta

TrustStore Certificati

WSAddressing To

Profilo Sicurezza Messaggio

Default

soapblocking.ente.govcloud.it

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 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

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 in accordo ad una API condivisa
2. La comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»
3. La confidenzialità e autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_02»
4. L'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva previsto nel pattern «INTEGRITY_SOAP_01»
5. L'applicativo fruitore ottiene e conserva la conferma di ricezione del messaggio da parte dell'erogatore

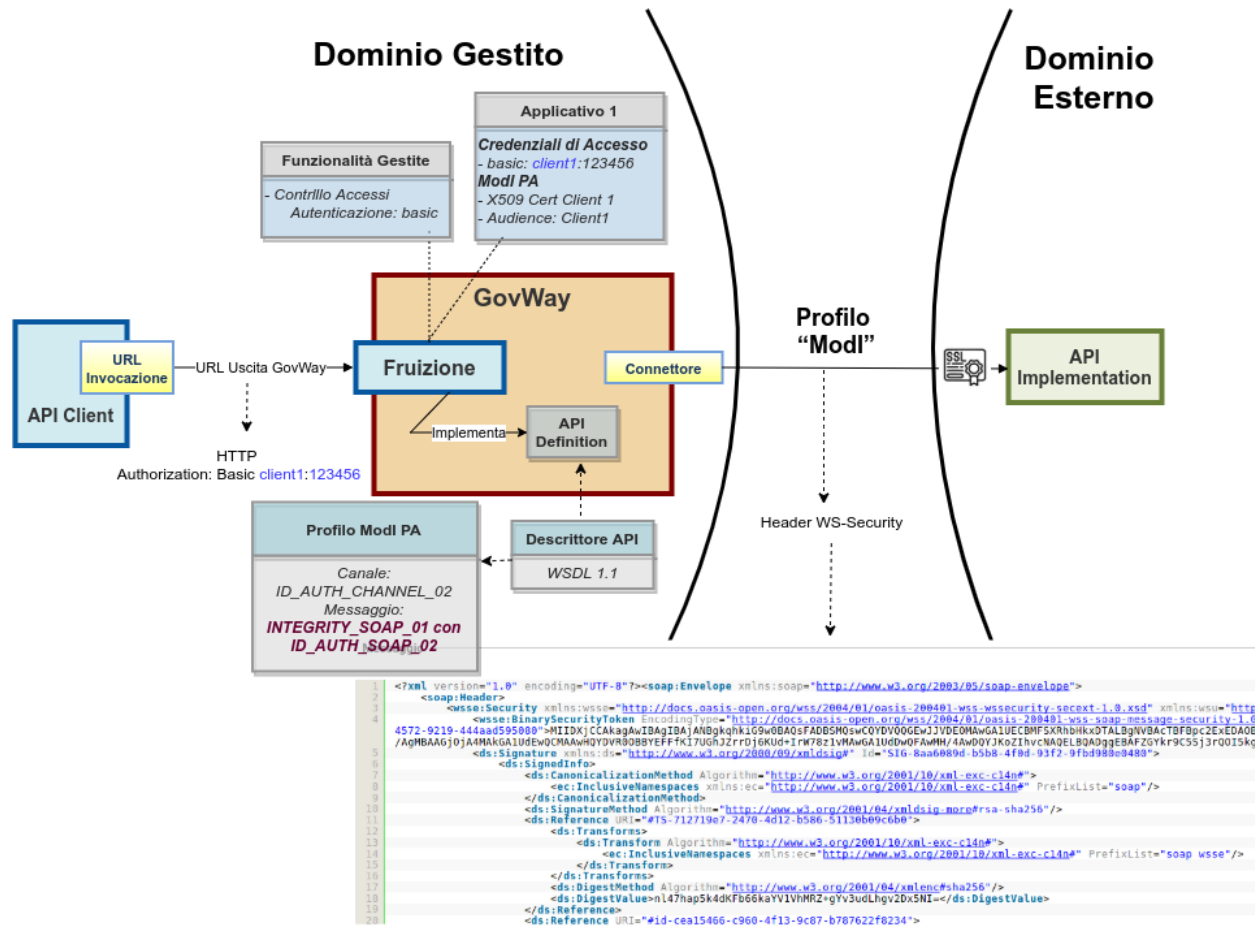


Fig. 7.1: Fruizione SOAP ModI

6. Garanzia di opponibilità ai terzi e non ripudio delle trasmissioni

7.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API di esempio (Credit Card Verification), basata su SOAP, pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02», «ID_AUTH_SOAP_02» e «INTEGRITY_SOAP_01».
- un'istanza Govway per la gestione del profilo ModI nel dominio del fruitore.
- 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», 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 fruitore 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 pattern «ID_AUTH_CHANNEL_02», si procede come già illustrato per [Erogazione REST ModI](#).
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.

7.3.1 Conformità ai requisiti ModI

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

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario [Fruizione REST ModI](#). 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 pattern:

- «ID_AUTH_CHANNEL_02» per la sicurezza canale
- «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_02» per la sicurezza messaggio

Informazioni ModI PA

ProfiloSicurezzaMessaggio INTEGRITY_SOAP_01 con ID_AUTH_SOAP_02
ProfiloSicurezzaCanale ID_AUTH_CHANNEL_02
ProfiloInterazione Bloccante

Sicurezza Messaggio

Digest SHA256=Sh0UH2m5gmLwrEfi/hrZFxhzGQn48ThAhhVLriUA3GM=
Expiration 2020-11-16_16:26:25.741
IssuedAt 2020-11-16_16:25:25.741
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app1.ente.govway.org, O=govway.org, C=it
RelatesTo f7ddaa57-c3c3-4a13-91fb-feadc664c961
WSA-From LuhnCheckerSoap/v1
WSA-To app1.enteesterno.govway.org
MessageId fa672f1a-5b72-4f48-acdf-62383904f02c

Fig. 7.2: Traccia della richiesta elaborata dall'erogatore

7.3.3 Fruizione

Si registra la fruizione SOAP, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI 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

☐

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 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

☒

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

Fig. 7.4: Configurazione risposta della fruizione

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).

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 all'identificazione 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).

Transazioni > Ricerca Base

Ricerca Base 🔍

⏮ ⏪ Lista Transazioni: record [1 - 6] ⏩ ⏭
























PetStore@Ente v1   Data: 2020-11-16 16:23:09, Risorsa API Rest: GET /pet/{petId}	 719 ms	 HTTP 200	<input type="checkbox"/>
PetStore@Ente v1  paolorossi Data: 2020-11-16 16:22:39, Risorsa API Rest: POST /pet	 722 ms	 HTTP 200	<input type="checkbox"/>
PetStore@Ente v1   Data: 2020-11-16 16:21:43, Risorsa API Rest: POST /pet	 66 ms	 Gestione Token 401	<input type="checkbox"/>
PetStore@Ente v1   Data: 2020-11-16 16:21:21, Risorsa API Rest: POST /pet	 93 ms	 Token non Presente 401	<input type="checkbox"/>
PetStore@Ente v1   Data: 2020-11-16 16:20:19, Risorsa API Rest: GET /pet/findByStatus	 783 ms	 HTTP 200	<input type="checkbox"/>
PetStore@Ente v1   Data: 2020-11-16 16:19:33, Risorsa API Rest: GET /pet/findByStatus	 599 ms	 HTTP 302	<input type="checkbox"/>

Fig. 8.1: Elenco delle transazioni

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	Visualizza Esporta

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	Visualizza

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	5cfc5ee0-7588-4313-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

Fig. 8.2: Dettaglio della transazione in errore

Visualizza Transazioni (Live) > Dettagli Transazione > **Messaggi Diagnostici**

⏮ ⏪ Lista Diagnostici: record [1 - 6] su 6 ⏩ ⏭

Data	Severita	Funzione	Messaggio
2019-09-04 16:24:05.875	infoIntegration	RicezioneBuste	Ricevuta richiesta applicativa
2019-09-04 16:24:05.877	infoIntegration	RicezioneBuste	Gestione Token [KeyCloak] (Validazione JWT) in corso ...
2019-09-04 16:24:05.877	errorIntegration	RicezioneBuste	Non è stato riscontrato un token nella posizione [RFC 6750 - Bearer Token Usage]: (Authorization Request Header) Non è stato riscontrato un header http 'Authorization' valorizzato tramite autenticazione 'Bearer ' e contenente un token (URI Query Parameter) Non è stato riscontrata la proprietà della URL 'access_token' contenente il token (Form-Encoded Body Parameter) Non è stato riscontrata la presenza di un contenuto 'Form-Encoded'
2019-09-04 16:24:05.878	errorIntegration	RicezioneBuste	Gestione Token [KeyCloak] (Validazione JWT) fallita
2019-09-04 16:24:05.878	errorProtocol	RicezioneBuste	Generato messaggio di cooperazione di Errore con identificativo [9419b58e-7693-434f-b1df-fec9e1dda772]
2019-09-04 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



Fig. 8.4: Fault in uscita

- 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. 8.5).

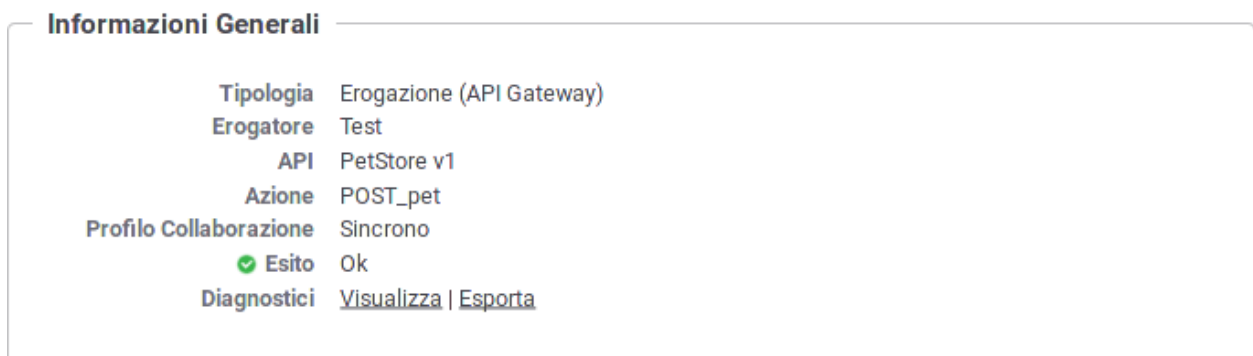


Fig. 8.5: Messaggi diagnostici della transazione con esito regolare

- Nel contesto delle informazioni generali si possono visualizzare i messaggi diagnostici con il dettaglio dell'elaborazione regolarmente eseguita (Fig. 8.6).
- 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. 8.7.

Visualizza Transazioni (Live) > Dettagli Transazione > Messaggi Diagnostici

Lista Diagnostici: record [1 - 8] su 8

Data	Severita	Funzione	Messaggio
2019-09-05 11:32:00.804	infoIntegration	RicezioneBuste	Ricevuta richiesta applicativa
2019-09-05 11:32:00.806	infoIntegration	RicezioneBuste	Gestione Token [KeyCloak] (Validazione JWT) in corso ...
2019-09-05 11:32:00.808	infoIntegration	RicezioneBuste	Gestione Token [KeyCloak] (Validazione JWT) completata con successo
2019-09-05 11:32:01.083	infoProtocol	RicezioneBuste	Ricevuto messaggio di cooperazione con identificativo [222152f4-f8a6-410c-831e-4da92b121f41]
2019-09-05 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 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 11:32:01.524	infoProtocol	RicezioneBuste	Generato messaggio di cooperazione con identificativo [c6991eca-fde0-4065-87a0-bf78410283c8]
2019-09-05 11:32:01.526	infoIntegration	RicezioneBuste	Risposta consegnata al mittente con codice di trasporto: 200

ESPORTA

Fig. 8.6: Messaggi diagnostici della transazione con esito regolare

Informazioni Mittente

Metodo HTTP

POST

URL Invocazione

[in] /gowway/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/realms/testrealm

Client ID

testclient

Subject

22158fb1-cea7-46c9-8180-1e30ccb4f944

Username

testuser

Token Info

[Visualizza](#)

Fig. 8.7: 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. 8.8).

Visualizza Transazioni (Live) > Dettagli Transazione > Token Info

Token Info

```

1  {
2    "valid" : true,
3    "iss" : "http://10.114.87.37:8080/auth/realms/testrealm",
4    "sub" : "22158fbl-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" : "22158fbl-cea7-46c9-8180-1e30ccb4f944",
17     "email_verified" : "false",
18     "allowed-origins" : [ "http://serviziclienti.link.it/" ],
19     "iss" : "http://10.114.87.37:8080/auth/realms/testrealm",
20     "typ" : "Bearer",
21     "preferred_username" : "testuser",
22     "given name" : "Utente".

```

DOWNLOAD

Fig. 8.8: Visualizzazione del token