
Scenari Applicativi

Release 3.4.2

Link.it

13 feb 2026

Contents

1	Ambiente di esecuzione	1
1.1	Prerequisiti	1
1.2	Avvio Ambiente	2
1.3	Progetto Postman	3
2	Profilo “API Gateway”	11
2.1	Erogazione pubblica	11
2.2	Erogazione OAuth	15
3	Profilo “ModI”	25
3.1	Pattern “ID_AUTH”	26
3.2	Pattern “INTEGRITY_01”	54
3.3	Pattern “ID_AUTH” via PDND	86
3.4	Pattern “ID_AUTH” via PDND + “INTEGRITY_01”	118
3.5	Pattern “ID_AUTH” via PDND + “INTEGRITY_REST_02”	150
3.6	Pattern “AUDIT_REST_01”	170
3.7	Pattern “AUDIT_REST_02”	202
4	Monitoraggio	217
4.1	Transazione in errore	217
4.2	Transazione con esito corretto	221

Ambiente di esecuzione

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

Nella sezione *Prerequisiti* vengono indicati i software di base richiesti per poter avviare l'ambiente e verificare gli scenari.

Indicazioni su come ottenere un ambiente, preconfigurato per verificare gli scenari, sono presenti nella sezione *Avvio Ambiente*.

Infine nella sezione *Progetto Postman* vengono fornite indicazioni su come ottenere un progetto Postman che contenga i client preconfigurati per attuare le richieste descritte in ogni scenario.

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** preconfigurato per verificare gli scenari:
 - invocazione pubblica o OAuth su profilo “API Gateway”;
 - profilo “ModI” su API REST;
 - profilo “ModI” su API SOAP.

Gli scenari configurati sull'ambiente docker devono poter accedere alle seguenti API pubbliche disponibili su internet:

- (API REST) Petstore: <https://petstore.swagger.io/>
- (API SOAP) Temperature Conversion: <https://www.w3schools.com/xml/tempconvert.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](#)).

```
[poli@polo2024 scenari]$ ./starttest.sh
[+] Running 4/0
  ✓ Container PGSQ16  Created
  ✓ Container keycloak Created
  ✓ Container gateway  Created
  ✓ Container nginx    Created
```

Figure1.1: Schermata di avvio «docker-compose up»

I componenti avviati sono i seguenti:

- gateway: l’istanza di Govway
- PGSQ16: il database Postgres
- keycloak: l’authorization server
- nginx: il server web

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](#)).



Figure 1.2: Accesso alla console di gestione

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

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

```
endpoint: https://govway.localedomain/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 (alcuni esempi a seconda della versione utilizzata in Fig. 1.8 e Fig. 1.9) ed assicurarsi che la voce “*SSL Certificate Verification*” nella maschera “*General*” sia disabilitata (Fig. 1.10, Fig. 1.11) e che non vi sia impostato un proxy nella maschera “*Proxy*” (Fig. 1.12, Fig. 1.13).



Figure1.3: Accesso alla console di monitoraggio

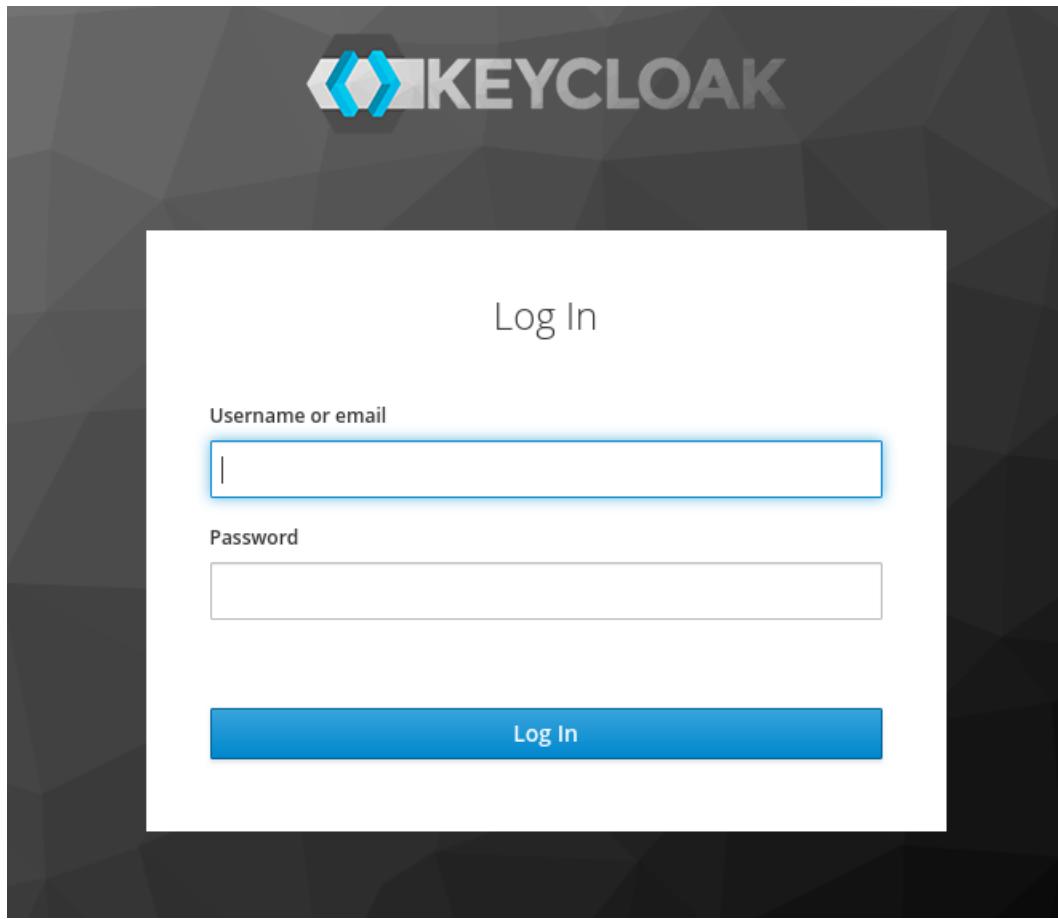


Figure1.4: Accesso alla console dell'authorization server

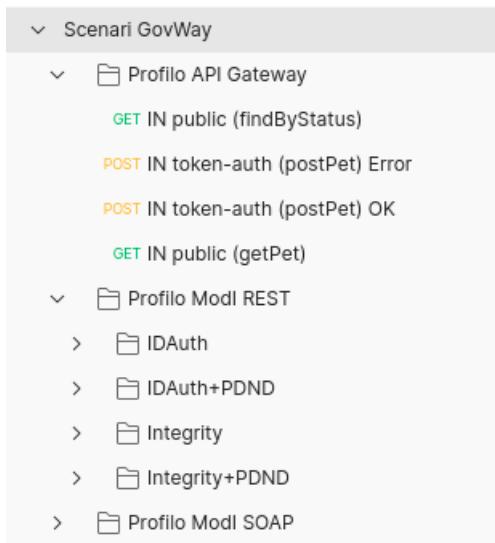


Figure1.5: Indice della collection Postman

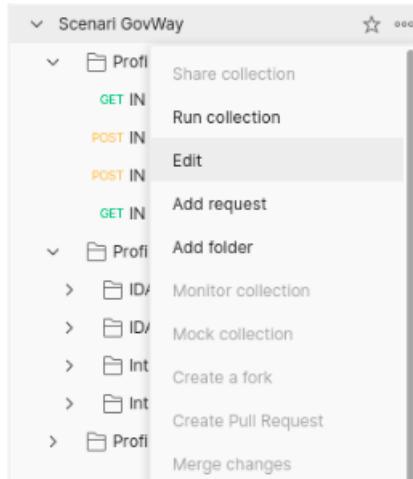


Figure1.6: Configurazione Collection Postman

EDIT COLLECTION

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	CURRENT VALUE	...	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/realms/master/protocol/openid-conn...			
<input checked="" type="checkbox"/>	keycloak-url-token	https://{{hostname}}/aut...	https://{{hostname}}/auth/realms/master/protocol/openid-conn...			
<input checked="" type="checkbox"/>	keycloak-client-id	oauth2-app1	oauth2-app1			
<input checked="" type="checkbox"/>	keycloak-client-secret	fd5f09fa-028d-461b-8e4f-063c111c069f	fd5f09fa-028d-461b-8e4f-063c111c069f			

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](#)

Cancel **Update**

Figure1.7: Configurazione Hostname nella Collection Postman

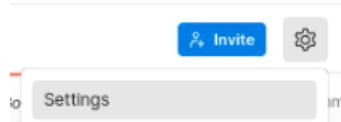


Figure1.8: Configurazione Generale Postman (versioni più recenti)

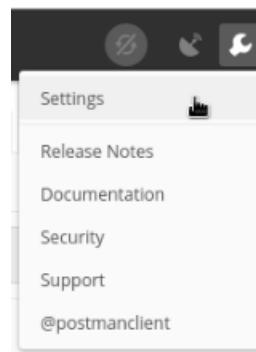


Figure1.9: Configurazione Generale Postman

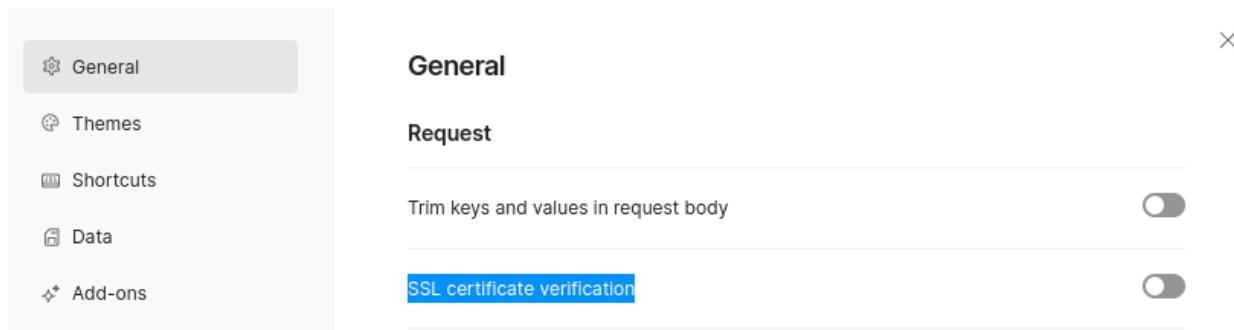


Figure1.10: Configurazione SSL Postman (versioni più recenti)

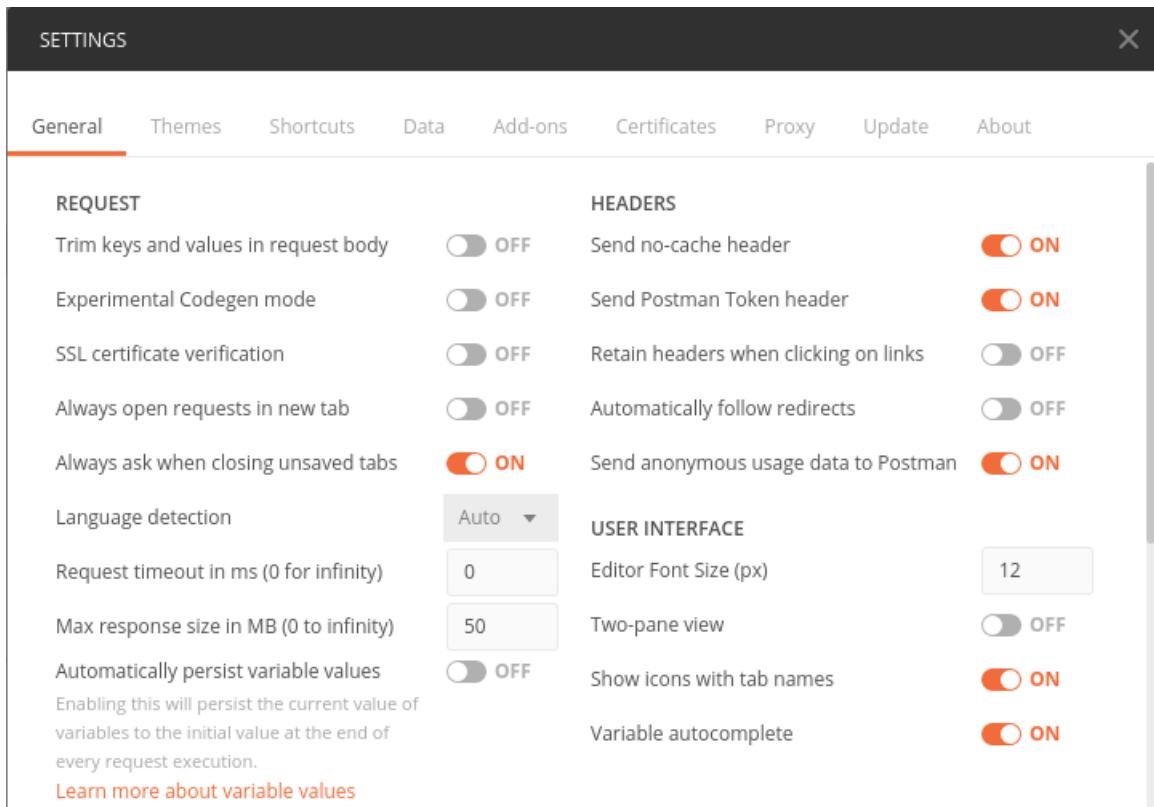


Figure1.11: Configurazione SSL Postman

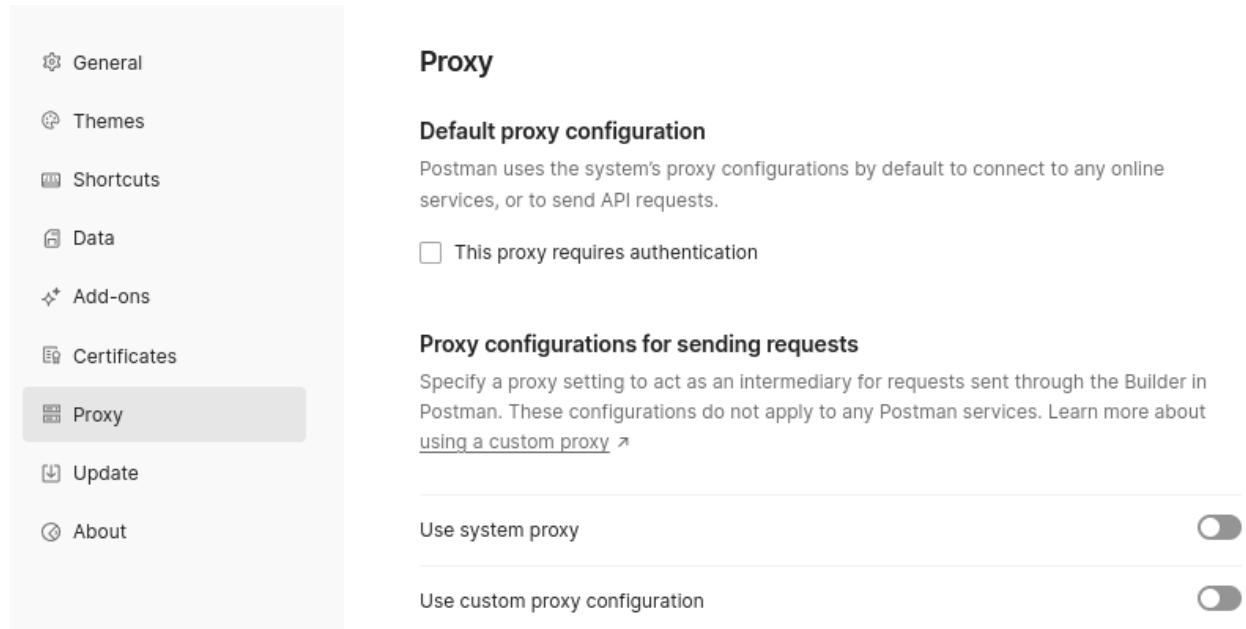


Figure1.12: Configurazione Proxy Postman (versioni più recenti)

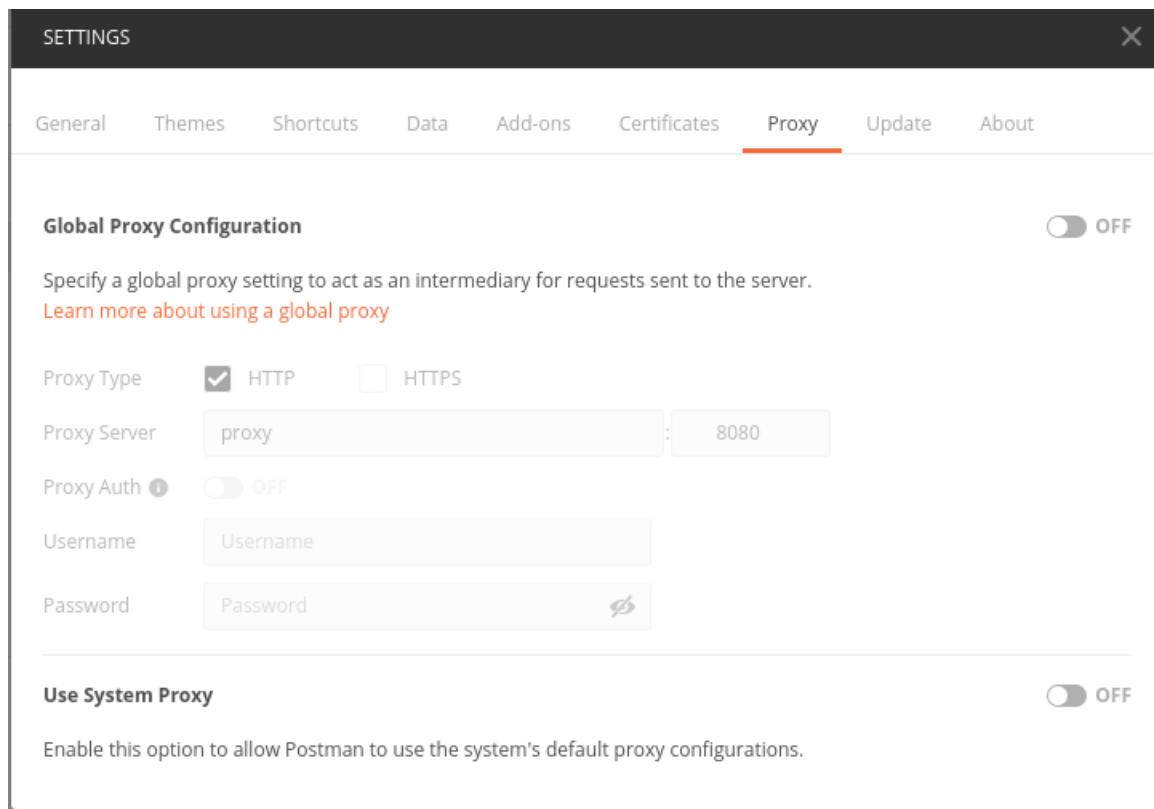


Figure1.13: Configurazione Proxy Postman

CHAPTER 2

Profilo “API Gateway”

Nelle sezioni successive verranno mostrati degli scenari di esempio di una API Rest erogata con profilo “API Gateway”.

Nel primo scenario descritto la sua fruizione è a disposizione di qualsiasi client poiché non vi sono meccanismi di autenticazione/autorizzazione configurati.

Nel secondo scenario viene invece richiesto un token OAuth.

Nota

Per una consultazione mirata alle informazioni di interesse per lo scenario si consiglia di impostare nel menù in alto a destra il profilo “API Gateway” come mostrato nella figura Fig. 2.1.



Soggetto: Ente Profilo: API Gateway ▾

Figure2.1: Selezione del profilo “API Gateway”

2.1 Erogazione pubblica

Obiettivo

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

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.

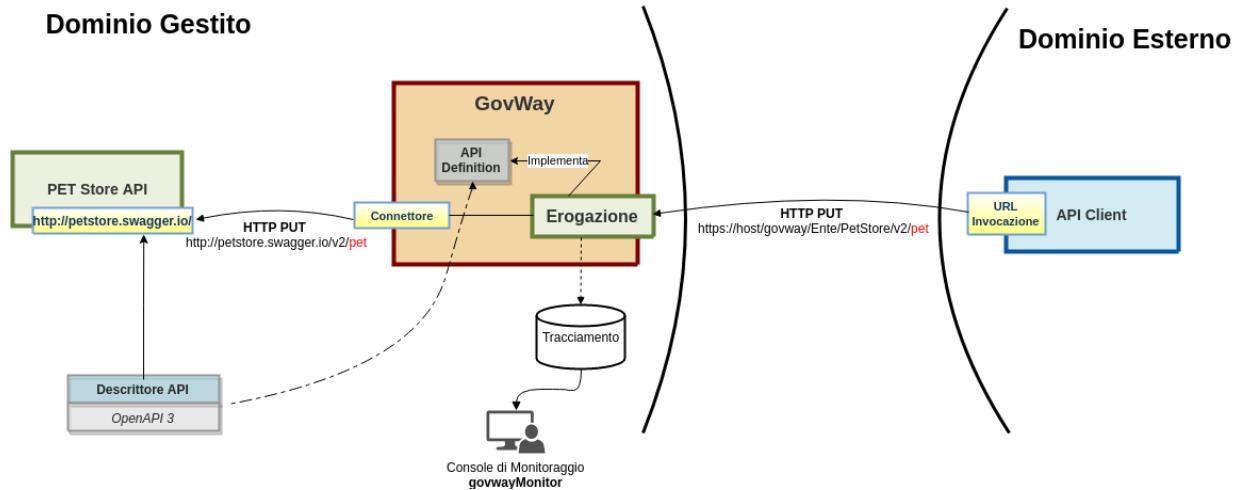


Figure2.2: Erogazione ad accesso pubblico

2.1.1 Esecuzione

I fruitori del servizio «PetStore» invocano le operazioni disponibili tramite i propri client senza utilizzare alcuna forma di autenticazione, utilizzando come “base-uri” la url di invocazione di GovWay

Avvalendosi del progetto Postman a corredo, eseguire «IN public (findByStatus)» per verificare l'esecuzione dell'erogazione del servizio PetStore con libero accesso.

2.1.2 Configurazione

In questa sezione vengono mostrate le parti di interesse relative alla configurazione con accesso pubblico.

Si assume che sia stata configurata una API “PetStore” con il descrittore OpenAPI 3 (scaricabile al seguente [indirizzo](#)).

Per registrare una erogazione dell'API “PetStore” pubblicamente accessibile si deve cliccare sul pulsante «Aggiungi» all'interno della sezione «Erogazione» (Fig. 2.5):

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_connatori_https`. Poichè non è obiettivo di questo scenario si suggerisce di disabilitare la validazione del certificato server se si rilevano problematiche di trust del certificato server.

4. Salvare la configurazione dell'erogazione.
5. Nel dettaglio della configurazione dell'erogazione è possibile vedere come non vi sia abilitato alcun controllo nella voce “Controllo Accessi”.

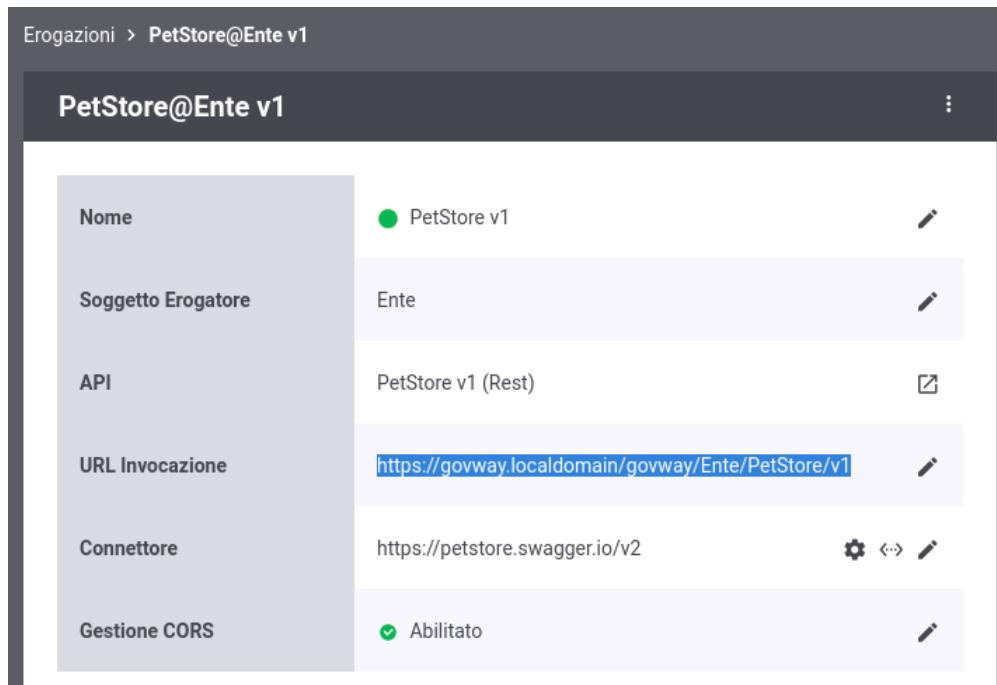


Figure2.3: Erogazione pubblica, url di invocazione

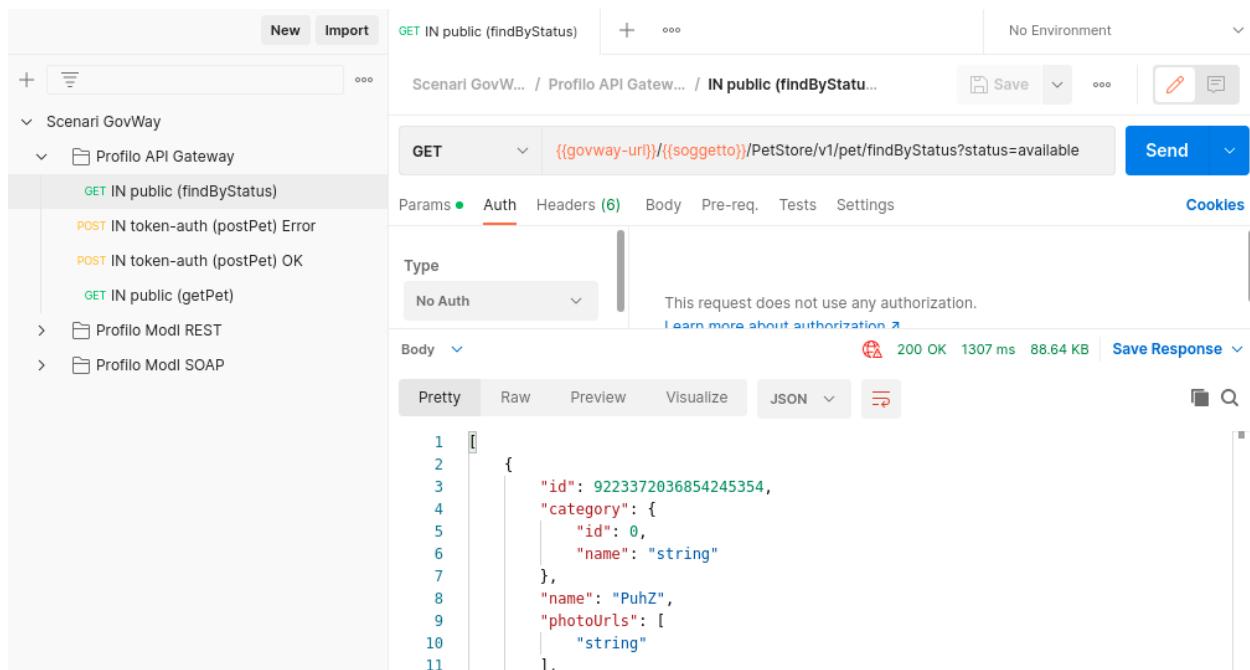


Figure2.4: Erogazione pubblica, esecuzione da Postman

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:

AutenticazioneHttps:

Proxy:

Ridefinisci Tempi Risposta:

Autenticazione Https

Tipologia: TLSv1.3

Verifica Hostname:

Autenticazione Server

Verifica:

Autenticazione Client

Abilitato:

SALVA

Figure2.5: Creazione di un'erogazione ad accesso pubblico

Nota

Esaminando l'erogazione preconfigurata si può notare come le risorse siano state suddivise in due gruppi in cui varia proprio il controllo degli accessi, e la risorsa invocata (GET /pet/findByStatus) rientra nel gruppo “Predefinito” dove il controllo degli accessi risulta disabilitato. L'altro gruppo verrà descritto nello scenario *Erogazione OAuth*.

Figure2.6: Configurazione dell'erogazione

2.2 Erogazione OAuth

Obiettivo

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

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.

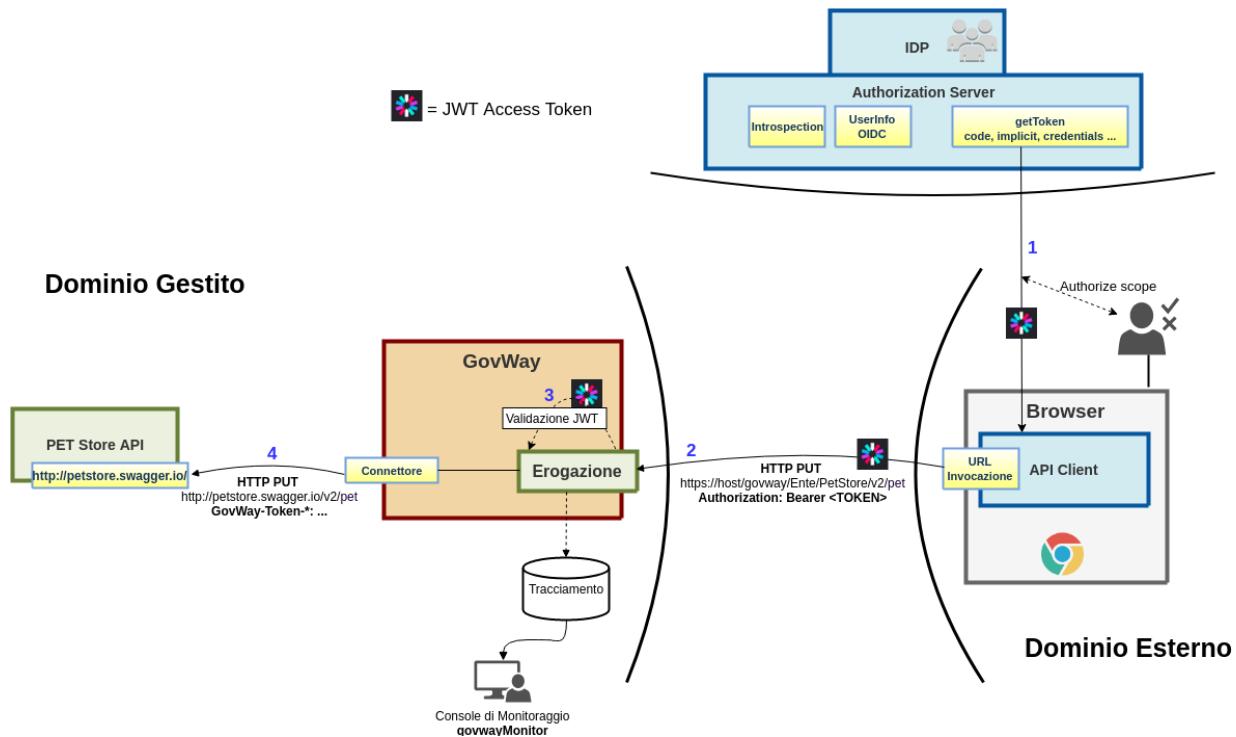


Figure2.7: Erogazione OAuth

2.2.1 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 «IN token-auth (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. 2.8.
2. Successivamente si passa alla chiamata della «POST /pet» seguendo il flusso OAuth2 richiesto per l'approvvigionamento del token di autorizzazione. Posizionarsi sulla request «IN token-auth (postPet) OK»:
 - Nella sezione «Authorization» selezionare il Type «OAuth 2.0» e premere il pulsante «Get New Access Token»
 - La maschera fornita deve essere compilata con i parametri necessari ad richiedere un token all'authorization server (sono forniti esempi a seconda della versione utilizzata di Postman in Fig. 2.9 e Fig. 2.10). 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

The screenshot shows the Postman interface with the following details:

- Left Sidebar:** Shows a tree structure with "Scenari GovWay" expanded, containing "Profilo API Gateway" with "IN public (findByStatus)" and "IN token-auth (postPet) Error".
- Request Section:**
 - Method: POST
 - URL: `{{govway-url}}/{{soggetto}}/PetStore/v1/pet`
 - Params tab is selected.
 - Body tab is selected.
 - Response status: 401 Unauthorized
 - Response time: 33 ms
 - Response size: 618 B
- Body Section:**
 - Pretty tab is selected.
 - Raw tab is available.
 - Preview tab is available.
 - Visualize tab is available.
 - JSON tab is selected.
 - Copy icon is available.
 - Search icon is available.
 - Response content (Pretty JSON):

```

1  [
2   "type": "https://govway.org/handling-errors/401/TokenAuthenticationRequired.",
3   "html",
4   "title": "TokenAuthenticationRequired",
5   "status": 401,
6   "detail": "A token is required",
7   "govway_id": "22f108c4-4f90-11ed-9b8f-0242ac140002"

```

Figure2.8: Invocazione della POST /pet senza token

Configure New Token

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

Figure2.9: Ottenimento nuovo token (versioni di Postman più recenti)

GET NEW ACCESS TOKEN X

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

Request Token

Figure2.10: Ottenimento nuovo token

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. 2.11).

The screenshot shows the Scenari GovWay interface. On the left, there's a sidebar with a tree view of scenarios and profiles. The main area shows a POST request to 'IN token-auth (postPet)'. The 'Auth' tab is selected, showing 'OAuth 2.0' as the type. The response body is a JSON object representing a pet:

```

1  {
2   "id": 32,
3   "category": {
4     "id": 0,
5     "name": "Alano"
6   },
7   "name": "Leo",
8   "photoUrls": [
9     "string"
10 ]

```

Figure2.11: Invocazione della risorsa “POST /pet” con token

3. Possiamo verificare che le limitazioni sull’accesso non sono efficaci nel caso di invocazione di operazioni di lettura. Il passo «IN public (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 (Fig. 2.12).

2.2.2 Configurazione

L’erogazione è già stata preconfigurata per prevedere un controllo degli accessi differente tra le risorse che riguardano operazioni di scrittura (POST, PUT, DELETE) e le risorse che riguardano solo lettura (GET).

Di seguito vengono descritti i passi che sono stati effettuati per arrivare alla configurazione esistente partendo dall’erogazione configurata con accesso pubblico.

I passi di configurazione finalizzati a limitare l’accesso alle sole operazioni di scrittura sono i seguenti:

1. Dal dettaglio dell’erogazione, si procede con la creazione di una nuova configurazione, cui diamo il nome «Scritture» (Fig. 2.13).

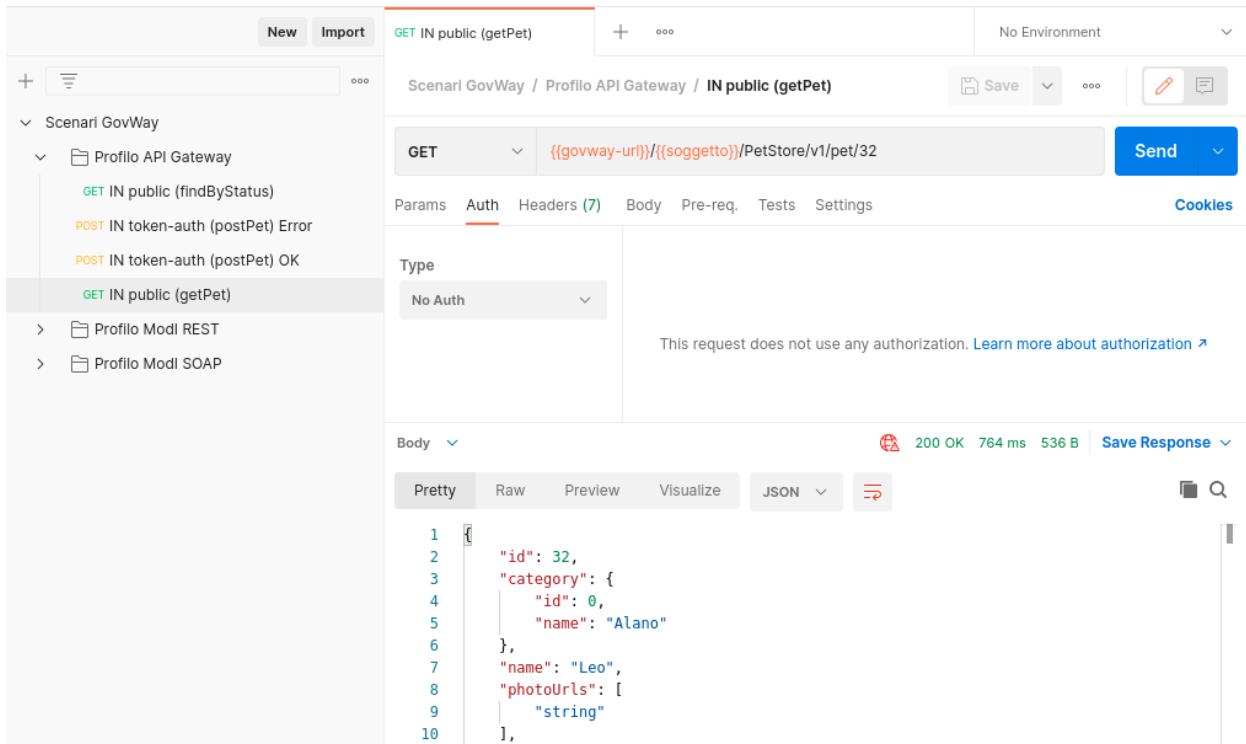


Figure2.12: Invocazione della risorsa “GET /pet/id” con token

- 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. 2.14):
- 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. 2.15.

Erogazioni > PetStore v1 (Test) > Configurazione > Aggiungi

Note: (*) Campi obbligatori

Configurazione

Nome Gruppo *	Scrittura
Risorse *	<ul style="list-style-type: none">POST /petPUT /petGET /pet/findByStatusGET /pet/findByTagsDELETE /pet/{petId}GET /pet/{petId}POST /pet/{petId}POST /pet/{petId}/uploadImageGET /store/inventoryPOST /store/order
Modalità	Nuova

Controllo degli Accessi

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

SALVA

Figure2.13: 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

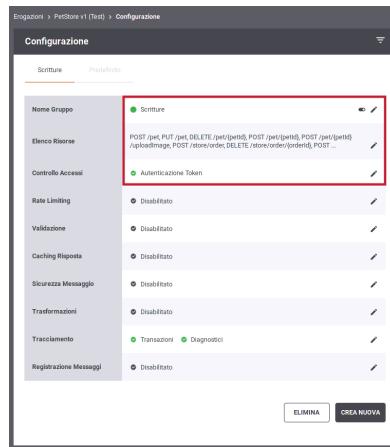


Figure2.15: Riepilogo della configurazione effettuata

CHAPTER 3

Profilo “ModI”

Nelle sezioni successive verranno mostrati degli scenari di esempio di API Rest e API SOAP erogate o fruite con profilo “ModI” in accordo alla normativa prevista dal Modello di Interoperabilità.

I scenari descritti si differenziano rispetto ai pattern di sicurezza associati alle API erogate o fruite:

- nella sezione *Pattern “ID_AUTH”* le API sono configurate tramite il pattern modipa_idar01;
- nella sezione *Pattern “INTEGRITY_01”* viene utilizzato il pattern modipa_idar03;
- nella sezione *Pattern “ID_AUTH” via PDND* le API sono configurate tramite il pattern modipa_pdnd;
- nella sezione *Pattern “ID_AUTH” via PDND + “INTEGRITY_01”* viene utilizzato il pattern modipa_pdnd_integrity;
- nella sezione *Pattern “ID_AUTH” via PDND + “INTEGRITY_REST_02”* viene utilizzato il pattern modipa_idar04;
- nella sezione *Pattern “AUDIT_REST_01”* viene descritto come aggiungere un token di audit conforme al pattern modipa_infoUtente_audit01;
- nella sezione *Pattern “AUDIT_REST_02”* il token di audit è invece conforme al pattern modipa_infoUtente_audit02.

Nota

Per una consultazione mirata alle informazioni di interesse per lo scenario si consiglia di impostare nel menù in alto a destra il profilo “ModI” e la selezione del soggetto “Ente” come mostrato nella figura Fig. 2.1.



Figure3.1: Selezione del profilo “ModI”

3.1 Pattern “ID_AUTH”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_idar01.

3.1.1 Erogazione API REST

Obiettivo

Esportare un servizio, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza “ID_AUTH_REST_01” descritto nella sezione modipa_idar01.

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 il trust del certificato X.509 in modo da assicurare sia a livello di canale che a livello di messaggio l'autenticazione e autorizzazione del fruitore.

La figura seguente descrive graficamente questo scenario.

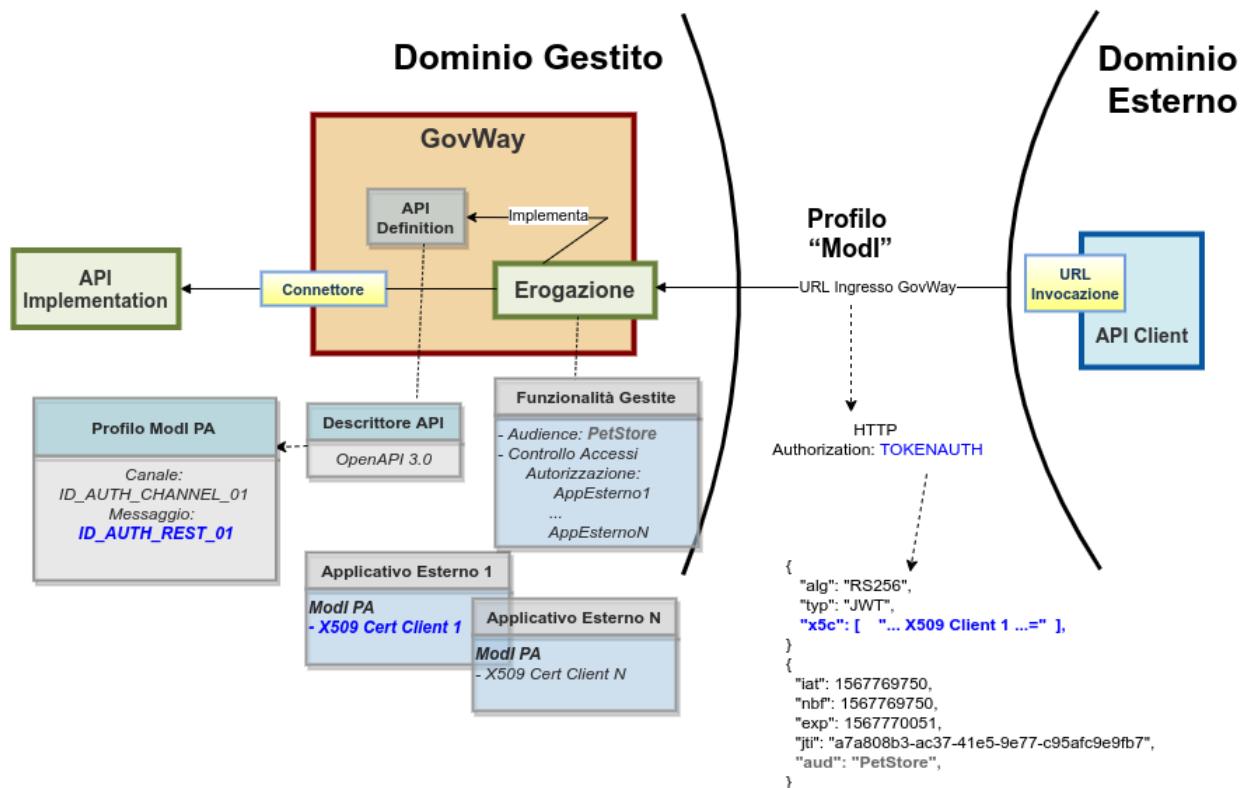


Figure3.2: Erogazione di una API REST con profilo “ModI”, pattern ID_AUTH_REST_01

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»;

3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Monitoraggio
Soggetto: Ente
Profilo: ModI

Figure3.3: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API REST di esempio (PetStore) definita con pattern di interazione “CRUD” e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «ID_AUTH_REST_01»;
- un'istanza Govway per la gestione del profilo ModI nel dominio dell'erogatore;
- un client del dominio esterno che invoca la risorsa «POST /pet» dell'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 «Profilo ModI REST - IDAuth - IN App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

Figure3.4: Pattern IDAuth - Erogazione API REST, esecuzione da Postman

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. 3.5).

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

Figure3.5: 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. 3.6. Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization», che contiene il token di sicurezza.
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. Nella fase di validazione del token si può notare come la sezione header (Fig. 3.7) riporti l'identità del fruitore e il suo certificato X.509, mentre la sezione payload (Fig. 3.8) contenga i riferimenti temporali (iat, nbf, exp) e l'audience (aud).
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 dell'audience ricevuto con quello atteso. 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. 3.9). 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. 3.6).
6. Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al certificato X.509 presente all'interno del token. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IDAuth - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

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. 3.5);
2. la sicurezza messaggio applicata è quella del pattern «ID_AUTH_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. l'identificazione del fruitore avviene rispetto al certificato X.509 presente all'interno del token. È stato anche mostrato come sia possibile configurare criteri autorizzativi puntuali.

Headers	
Nome	
Content-Type	application/json
X-Message-Id	1f46c4b4-4f9b-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	cde738cd-acfc-4785-a59a-eb751595a001
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yh2UWZlHrQDLuBSuHsJQWfc2Wp16rbtLxvMqKS0Nk6lxmWknBch1hXBwzeTmPAkNHcDoYpqhmdR
X-Forwarded-Port	443
Pragma	no-cache
Accept-Encoding	gzip, deflate, br

Figure3.6: Messaggio inviato dal fruttore

HEADER: ALGORITHM & TOKEN TYPE	
<pre> id { "alg": "RS256", "typ": "JWT", "kid": "app1.enteesterno.govway.org", "x5c": ["MIIE/jCCAuagAwIBAgICAPgwDQYJKoZIhvcNAQELBQAwNjELMAkGA1 UEBhMCaXQxEzARBgNVBAoMCmdvdndheS5vcmcxEjAQBgNVBAMMCUdvd 1dheSBQTAefw0yMjEwMTkwNzU1NTThaFw0zNzEwMTUwNzU1NTThaMEgx CzAJBgNVBAYTAm10MRMwEQYDVQQKDApnb3Z3YXkub3JnMSQwIgYDVQQ DBBthcHAXLmVudGVFc3R1cm5vLmdvdndheS5vcmcwggEiMA0GCSqGSI b3DQEBAQAA4IBDwAwggEKAoIBAQc1/cfENX06hdvEVxJiJAF0ePjn 5Sh/HIJ2du8hRv0zA+KFFieaF4xh1mSOT1oq/vwwxdFxqvfd2k1bTJ37r jBo6DKuQZor83j/Do87x3sFJe/epGKx96Q3PRE9mA1qx3Y5FFShfGNZ zG2RFNA2jhVQ/bsd9E051FC3XshF90CtJJs9LgvT2+0+uJK3siA6ht KcYQ58UcK1W1Y109MnXqaz82T1h93eTSkk33w0A9atzC0w3JAVmcRRk d0hFBjMeEvNR86cdNfy9Xit7ZDR11IB8te10/fI/oAW0oK/3TbF1X0r VL1QhMc1JdqS3NwJLayoqmqZT/Xh50qjD17ldghwbAgMBAAGjggECMIH /MAKGA1UdEwQCMAAwEQYJYIZIAYb40gE8BAQDAgeAMDMGCWCGSAGG+E IBDQqmF1RPcGVuU1NMIEd1bmVYXXR1ZCBDG11bnQgQ2VydG1maWNhd GUwHQYDVR0OBBYEFCBwk8Bs9JS+6c/vTU+JX0eqX81BMGYGA1UdIwRf MF2AFCqHFNpm2RdIA3igRXzNEeJ5ivegoTqk0DA2MQswCQYDVQGGEwJ pdDETMBEGA1UECgwKZ292d2F5Lm9yZzESMBAGA1UEAwwJR292V2F5IE NBggkA4tGAdmeSJF4wDgYDVR0PAQH/BAQDAgXgMBMGA1UdJQQMMAoGC CsGAQUBFwMCMA0GCSqGSIB3DQEBCwUAA4ICAQDRj52cdYwcqFDNmC29 CY0DR0N0TM/5RKq9sL6sgI7z4cUmkYIeGh/9YQDoRFhDBVGZ80rx0ka sZ/Po0Iuw+41f9IDTBe04Ym0CK3M1M9H2LiEKe9hngRtjzGw5tFRQnq KbLLX6l0tJAXuE488SrSAMbEDez1bZt+V1Sgc48fOKsjShUs8CwSW0G 6RE5w4Q4oa0dX971PTziWDoFnxBfN17/HAYA0625/vcp8PrZLqhTIGH 7dt+1T4hb+i10wKBS7B8Cab0Gh0sp1HDDdGNEyX50d1ZYmWJQ10ysK6 1Yx1WtCrKPfmsvSeqiVxJPHUgwTsFPrgoVrt+dT1NnAdXYxFk0Yxz7z n7qeKD16cXHLLtsYet1cQfedyDPE0r1i4GFL1KY37NFqRtJx5NadkJk6 GXk43zIFQo119PGJ8nVHupB6IBJ1h/6xem1TTMSt52zcjV4b5zRHL8Z qNF+S0QnJKch2FcYAYuGjuVj0qa5rhi5wNcy7ilcDShM8tsPJ5qpW1M E0hmhWWY+w5KBCpMoBn9cvqAn/N19L3e3SqH1KLp8Hw05CtH4/tLEe 3N+0z+8xzcmldqbAZ9nD7YVLVoyt5Y+Ixuj17F18dzEh9dzcLhJojsB mPjoFMMyu1bpjZG0A1TjKVpkxyXgaqsd9Hjs4Atg79V8U/GnEXJhXQ xU2TYw=="], "x5t#S256": "agRQxqs- VYDP2NIzbR7XH2GiInWH2bcL1xMPhimfMKk" } </pre>	

Figure3.7: Sezione «Header» del Token di sicurezza

PAYLOAD: DATA
<pre>{ "iat": 1666176318, "nbf": 1666176318, "exp": 1666176378, "jti": "1f46c4b4-4f9b-11ed-a5ac-0242ac140002", "aud": "petstore.ente.govway.org", "client_id": "app1.enteesterno.govway.org", "iss": "SoloPerDemoEnteEsterno", "sub": "SoloPerDemoFirmatarioApp1" }</pre>

Figure3.8: Sezione «Payload» del Token di sicurezza

Informazioni Modelli	
Sicurezza Messaggio	ID_AUTH_REST_01
Sicurezza Canale	ID_AUTH_CHANNEL_02
Interazione	Accesso CRUD
Sicurezza Messaggio	
ClientId	app1.enteesterno.govway.org
Subject	SoloPerDemoFirmatarioApp1
Issuer	SoloPerDemoEnteEsterno
MessageId	1f46c4b4-4f9b-11ed-a5ac-0242ac140002
Audience	petstore.ente.govway.org
NotBefore	2022-10-19_12:45:18.000
Expiration	2022-10-19_12:46:18.000
IssuedAt	2022-10-19_12:45:18.000
X509-Issuer	CN=GovWay CA, O=govway.org, C=it
X509-Subject	CN=app1.enteEsterno.govway.org, O=govway.org, C=it

Figure3.9: Traccia della richiesta elaborata dall'erogatore

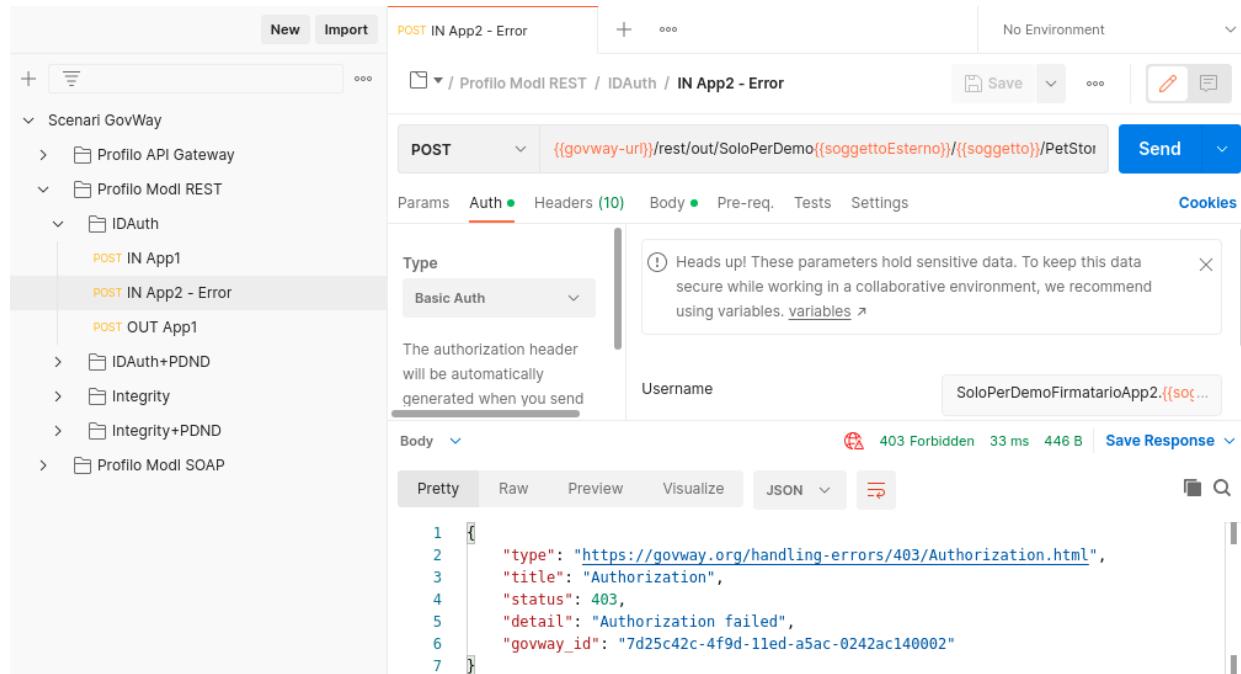


Figure3.10: Pattern IDAuth - Erogazione API REST - Autorizzazione negata, esecuzione da Postman

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾ Profilo: ModI ▾

Figure3.11: Profilo ModI della govwayConsole

Registrazione API

Viene registrata l’API «PetStoreAuth» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.12).

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.

API > PetStoreAuth v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale

Pattern ▼
Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern ▼
Direct Trust con certificato X.509

Header HTTP del Token ▼

Applicabilità ▼

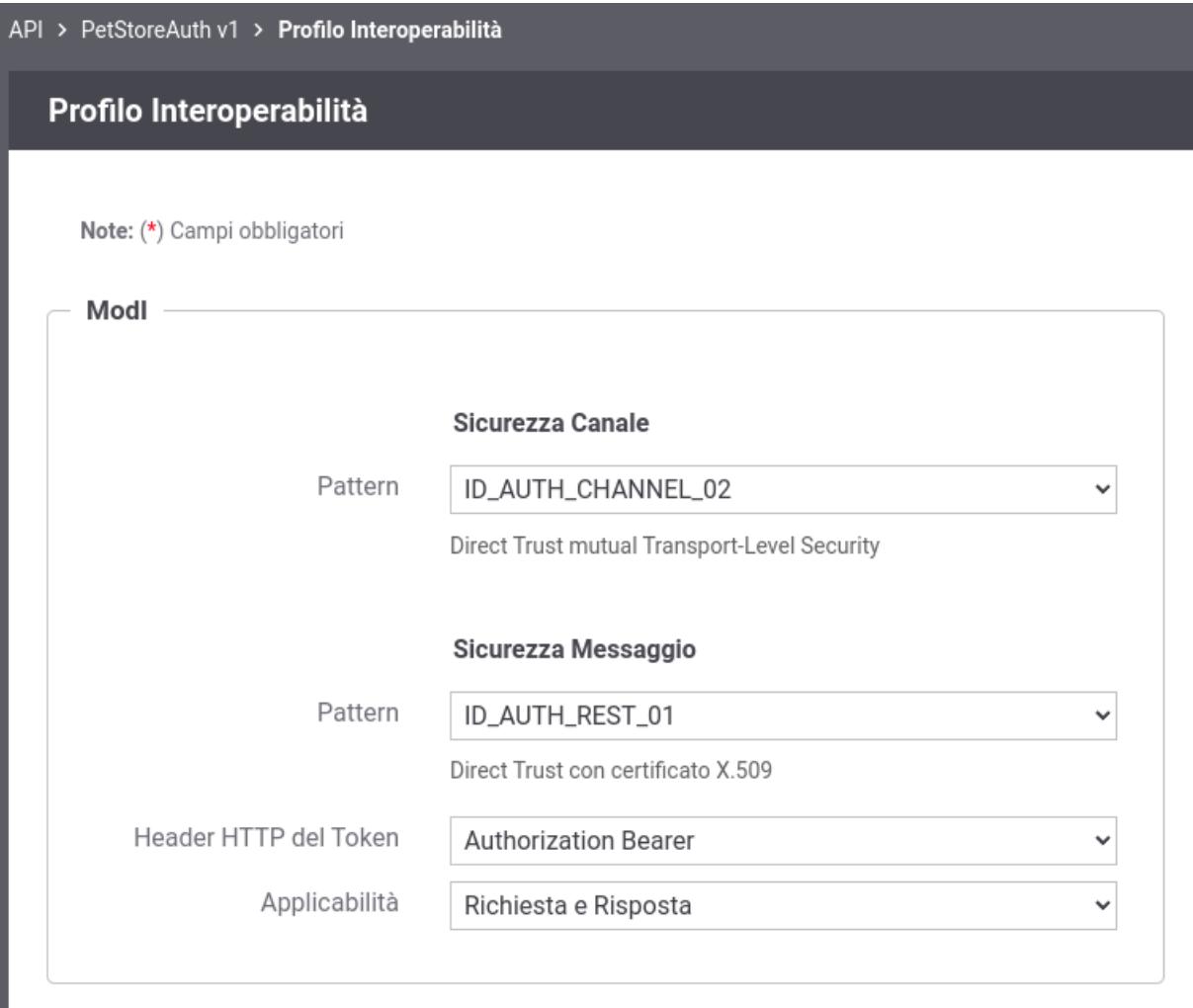


Figure3.12: Configurazione Pattern ModI «ID_AUTH_REST_01» sulla API REST

- 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. 3.13). Questo scenario è quello preconfigurato.

Applicativi > App1-ModI

App1-ModI

Note: (*) Campi obbligatori

Applicativo

Dominio	Esterno
Soggetto	EnteEsterno
Nome *	App1-ModI
Tipo	Client
Proprietà(0)	

Ruoli

[visualizza\(0\)](#)

ModI

Sicurezza Messaggio	Authorization ModI
Certificato	
Cambia Certificato	
Aggiungi Certificato	
Download	
Verifica	<input checked="" type="checkbox"/>
Subject	/c=it/cn=app1.enteEsterno.govway.org/o=govway.org/
Issuer	/c=it/cn=GovWay CA/o=govway.org/
Serial Number	248
(Hex) 00:F8	
Self Signed	No
Not Before	19/10/2022 09:55:00
Not After	15/10/2037 09:55:00

Figure3.13: Configurazione applicativo esterno (fruitore)

Erogazione

Si registra l'erogazione «PetStoreAuth», relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.14). 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. 3.15).

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

Figure3.14: 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

Figure3.15: Configurazione risposta dell'erogazione

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. Questo scenario è quello preconfigurato come mostrato nelle figure Fig. 3.16 e Fig. 3.17.

The screenshot shows the 'Controllo Accessi' configuration page. At the top, there is a breadcrumb navigation: Erogazioni > PetStoreAuth v1 (Ente) > Configurazione > Controllo Accessi. The main title is 'Controllo Accessi'. Below it, there are two main sections: 'Autenticazione Token' and 'Autenticazione Canale'. Under 'Autenticazione Canale', the 'Stato' is set to 'https'. Under 'Autenticazione', the 'Stato' is set to 'abilitato'. This section contains two sub-sections: 'Autorizzazione Canale' and 'Autorizzazione Messaggio'. In 'Autorizzazione Canale', 'per Richiedente' is checked, and 'Soggetti (1)' is listed. In 'Autorizzazione Messaggio', 'per Richiedente' is checked, and 'Applicativi (1)' is listed. The 'per Ruoli' checkboxes are empty in both sections.

Figure3.16: Controllo accessi con autorizzazione degli applicativi esterni

3.1.2 Fruizione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza “ID_AUTH_REST_01” descritto nella sezione modipa_idar01.

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

Erogazioni > PetStoreAuth v1 (Ente) > Configurazione > Controllo Accessi > Autorizzazione Messaggio - Applicativi	
Autorizzazione Messaggio - Applicativi	
Visualizzati record [1-1] su 1	
Soggetto	Applicativo
<input type="checkbox"/> EnteEsterno	App1-ModI

Figure3.17: Lista degli applicativi esterni autorizzati

particolare andiamo ad illustrare lo scenario, tra quelli prospettati nel Modello di Interoperabilità di AGID, che prevede il trust del certificato X.509 in modo da assicurare sia a livello di canale che a livello di messaggio l'autenticazione e autorizzazione del fruitore.

La figura seguente descrive graficamente questo scenario.

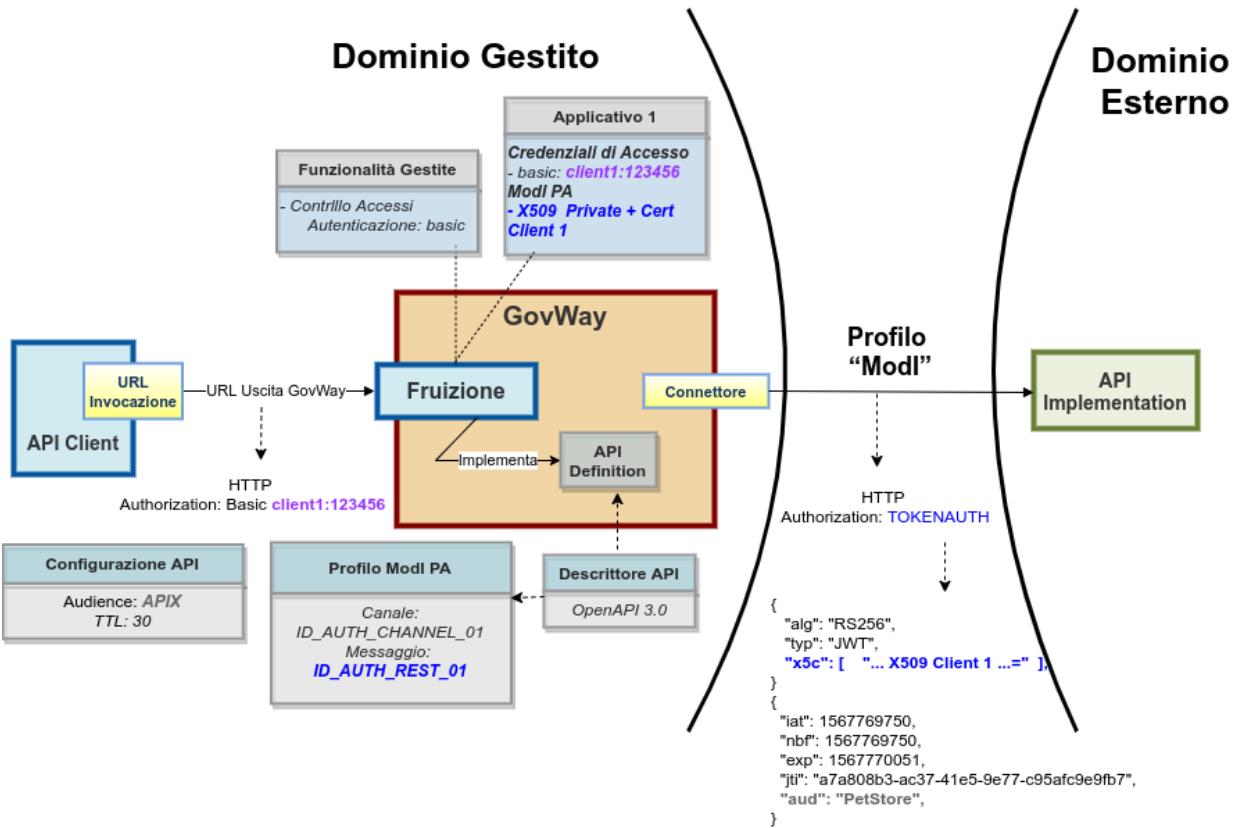


Figure3.18: Fruizione di una API REST con profilo "ModI", pattern ID_AUTH_REST_01

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. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.19: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API REST di esempio (PetStore) definita con pattern di interazione “CRUD” e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «ID_AUTH_REST_01»;
- un'istanza Govway per la gestione del profilo ModI nel dominio del fruitore;
- un client che invoca la risorsa «POST /pet» con un messaggio di esempio diretto alla fruizione configurata su Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IDAuth - OUT App1» che è stata preconfigurata 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 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 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. 3.21).
2. L'header e il payload del token sono identici a quelli visualizzati nello scenario di erogazione REST, relativamente al messaggio in ingresso (Fig. 3.7 e Fig. 3.8). Le informazioni inserite nel token vengono anche tracciate e sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.22). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal token di sicurezza presente nel messaggio.
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. 3.23).
4. Govway riceve la risposta dell'erogatore, dalla quale estraе il token di sicurezza al fine di effettuare i relativi controlli di validità e conservare la traccia. Consultando la traccia relativa alla trasmissione della risposta, sono visibili tra le altre informazioni i dati di autenticazione dell'erogatore e i riferimenti temporali.

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

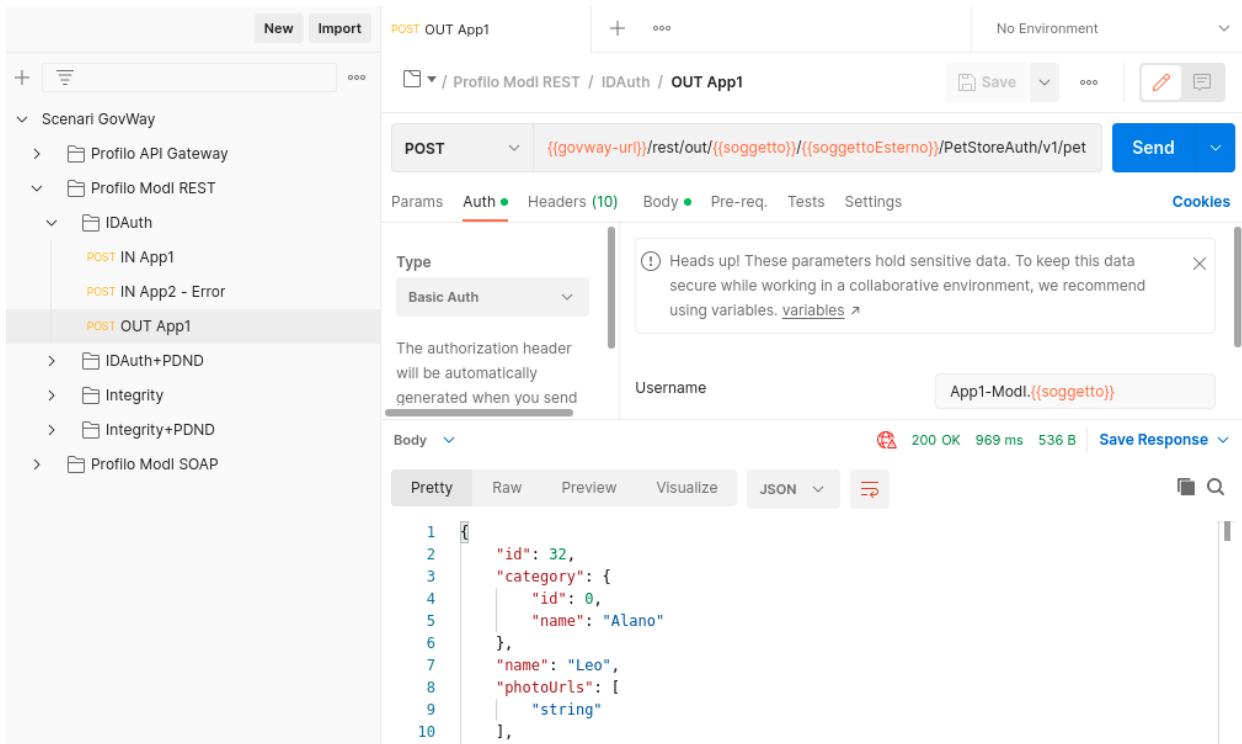


Figure3.20: Pattern IDAuth - Fruizione API REST, esecuzione da Postman

(Fig. 3.23);

2. la sicurezza messaggio applicata è quella dei pattern «ID_AUTH_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).

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.24: Profilo ModI della govwayConsole

Registrazione API

Viene registrata l’API «PetStoreAuth» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.25).

Headers	
Nome	
Content-Type	application/json
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
X-Forwarded-Port	443
Accept-Encoding	gzip, deflate, br
Postman-Token	d924391e-10cd-4c75-8063-4cbfaa74639a
User-Agent	GovWay
Accept	*/*
GovWay-Message-ID	5ade2322-4fac-11ed-a5ac-0242ac140002
GovWay-Transaction-ID	5acd8134-4fac-11ed-a5ac-0242ac140002
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCI6ImFwcDEuZW50ZS5nb3Z3YXkub3JrWyISJxWAFBE4zpeb4JpJRwmafmwJLqddHy7j8bMjGx9x3IG0ws6AhiTAKaK2HPGbpD

Figure3.21: Messaggio di richiesta in uscita (con token di sicurezza inserito nell'header HTTP)

Informazioni Modl

Sicurezza Messaggio ID_AUTH_REST_01

Sicurezza Canale ID_AUTH_CHANNEL_02

Interazione 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

Subject App1-Modl

Issuer Ente

ClientId app1.ente.govway.org

Audience petstore.enteEsterno.govway.org

Messageld 5ade2322-4fac-11ed-a5ac-0242ac140002

Expiration 2022-10-19_14:49:39.000

NotBefore 2022-10-19_14:48:39.000

IssuedAt 2022-10-19_14:48:39.000

Figure3.22: Traccia della richiesta generata dal fruitore

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) ...

Figure3.23: Sicurezza canale «ID_AUTH_CHANNEL_02» sulla fruizione

API > PetStoreAuth v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale	
Pattern	ID_AUTH_CHANNEL_02
Direct Trust mutual Transport-Level Security	
Sicurezza Messaggio	
Pattern	ID_AUTH_REST_01
Direct Trust con certificato X.509	
Header HTTP del Token	Authorization Bearer
Applicabilità	Richiesta e Risposta

Figure3.25: Configurazione Pattern ModI «ID_AUTH_REST_01» sulla API

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. 3.26). Alla registrazione dell'applicativo vengono associate credenziali “basic” che consentono a GovWay di identificarlo.

Fruizione

Si registra la fruizione «PetStoreAuth», relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.27). In particolare è possibile specificare l'audience atteso dall'erogatore e il tempo di validità del token.

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. 3.28).

3.1.3 Erogazione API SOAP

Obiettivo

Esportare un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza “ID_AUTH_SOAP_01” descritto nella sezione modipa_idar01.

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 il trust del certificato X.509 in modo da assicurare sia a livello di canale che a livello di messaggio l'autenticazione e autorizzazione del fruitore.

La figura seguente descrive graficamente questo scenario.

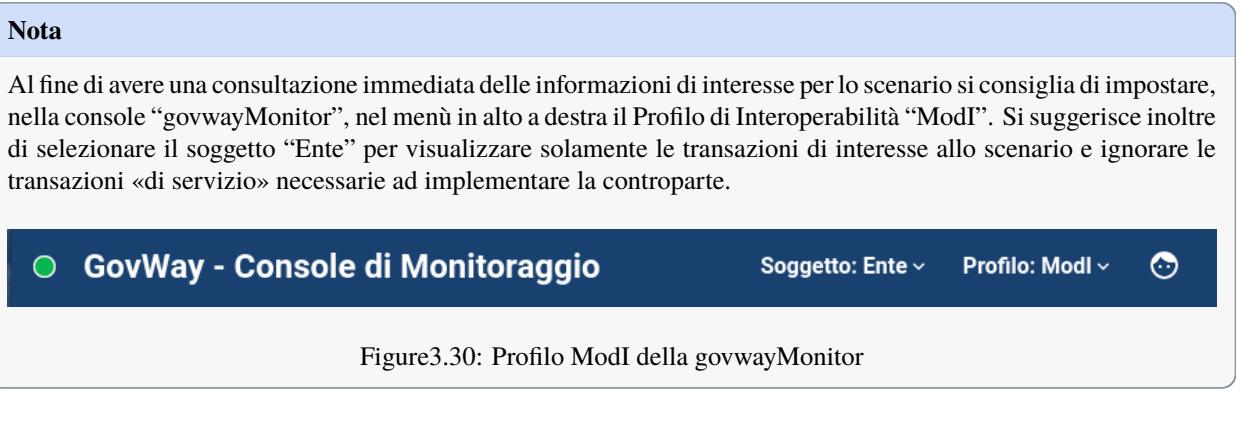
Le caratteristiche principali di questo scenario sono:

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



GovWay - Console di Monitoraggio Soggetto: Ente Profilo: ModI

Figure3.30: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

Applicativi > App1-Modl

App1-Modl

Note: (*) Campi obbligatori

Applicativo

Dominio	Interno
Soggetto	Ente
Nome *	App1-Modl
Tipo	Client
Proprietà(0)	

Modalità di Accesso

Tipo	http-basic
Utente *	App1-Modl.Ente
Modifica Password	<input type="checkbox"/>

Ruoli

[visualizza\(0\)](#)

Modi - Sicurezza Messaggio

KeyStore

Abilitato	<input checked="" type="checkbox"/>
Modalità	File System
Path *	/etc/goway/keys/keystore_app1.ente.pkcs12

Tipo	PKCS12
Password *	123456
Alias Chiave Privata *	app1.ente.goway.org
Password Chiave Privata *	123456

[Certificato](#)

Authorization Modl

Identificativo Client	app1.ente.goway.org	i
-----------------------	---------------------	-------------------

Figure3.26: Configurazione applicativo fruitore

Modi - Richiesta

Sicurezza Messaggio

Algoritmo	<input type="text" value="RS256"/>
Riferimento X.509	<input type="text" value="x5c (Certificate)"/> x5t#256 (Certificate SHA-256 Thumbprint) x5u (URL)
Certificate Chain	<input type="checkbox"/>
Time to Live (secondi) *	<input type="text" value="60"/>
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token	
Audience	<input type="text" value="petstore.enteEsterno.govway.org"/> 
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	
Claims	<input type="text"/>
Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli 	

Figure3.27: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

Riferimento X.509	<input type="text" value="Utilizza impostazioni della Richiesta"/>
TrustStore Certificati	<input type="text" value="Default"/>
Time to Live	<input type="text" value="Default"/>
Verifica Audience	<input checked="" type="checkbox"/> La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente
<input type="text"/> 	

Figure3.28: Configurazione risposta della fruizione

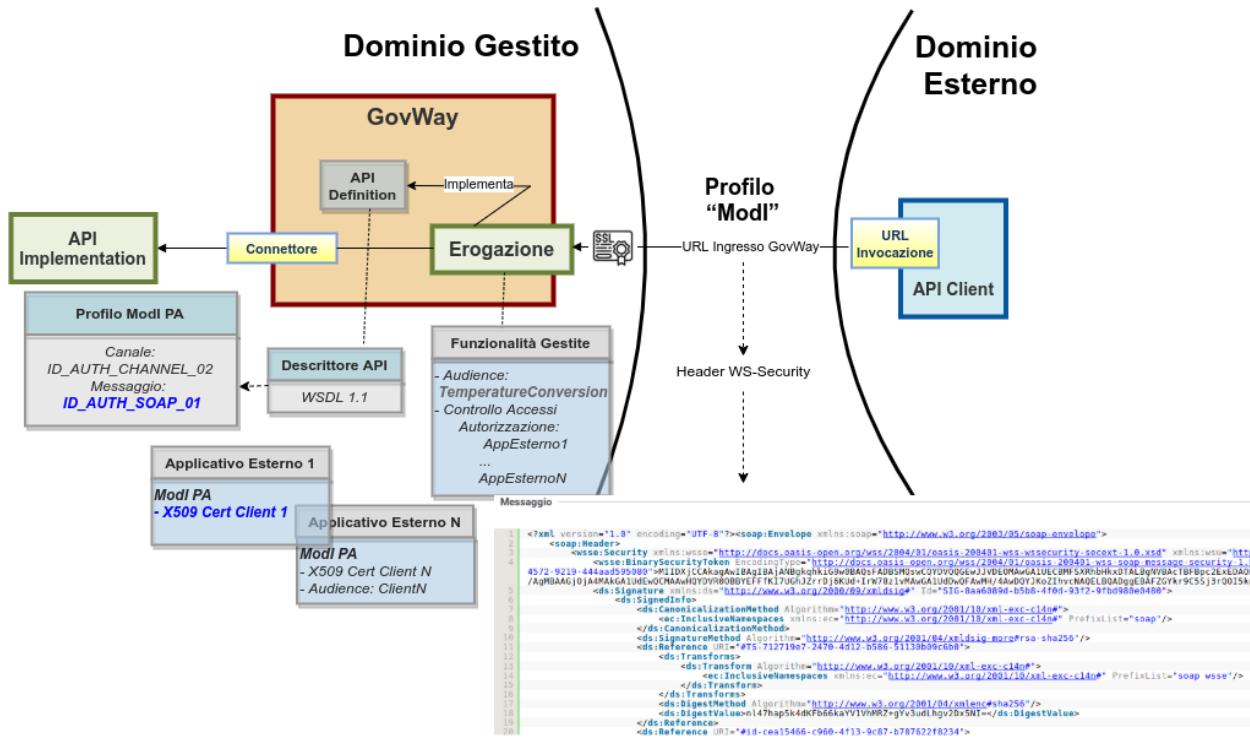


Figure3.29: Erogazione di una API SOAP con profilo “ModI”, pattern ID_AUTH_SOAP_01

- una API SOAP di esempio (Temperature Conversion) definita con pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «ID_AUTH_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 «CelsiusToFahrenheit» dell’erogazione esposta da Govway;
- il server “Temperature Conversion” 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://www.w3schools.com/xml/tempconvert.asmx>”.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth - IN App1» che è stata preconfigurata 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 [Esecuzione](#)
2. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in [Fig. 3.32](#). Come si nota, il messaggio SOAP contiene nell’header WS-Security sia il token di sicurezza (elemento «BinarySecurityToken») sia l’elemento «WSAddressing - To» 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 dell’audience ricevuto con quello atteso. 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. 3.33](#)). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal

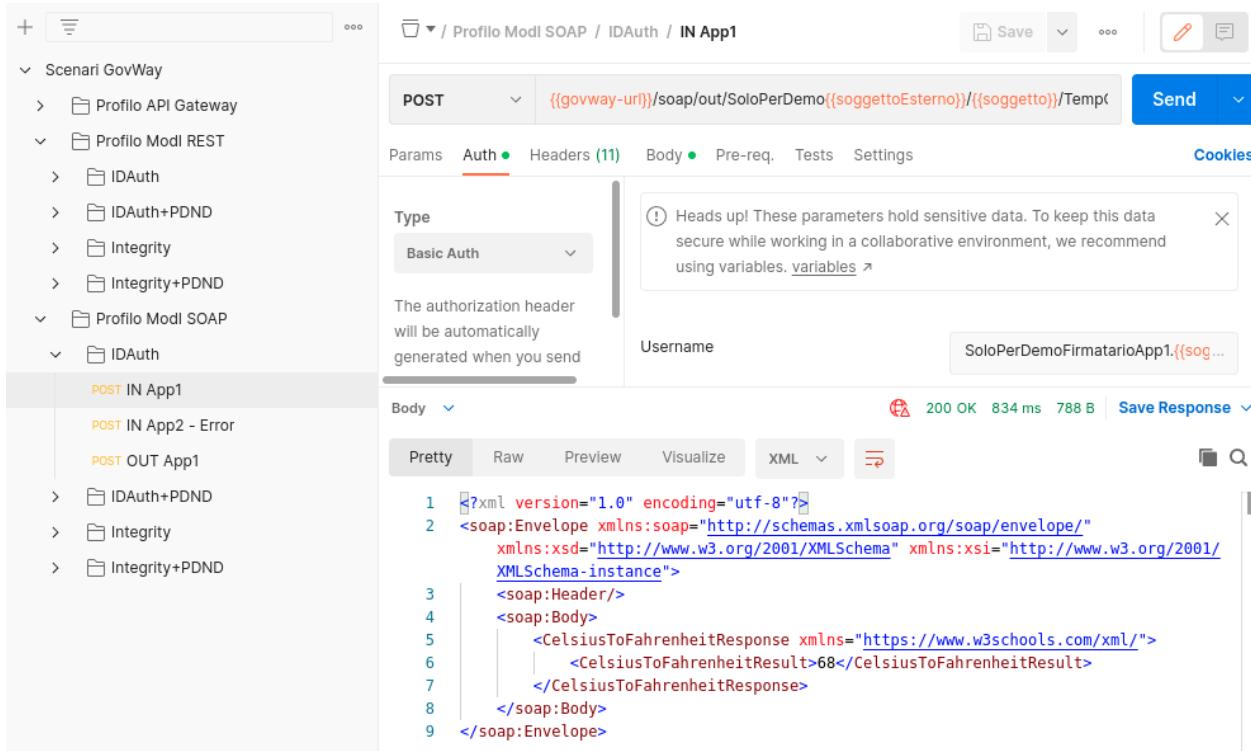


Figure3.31: Pattern IDAuth - Erogazione API SOAP, esecuzione da Postman

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-ws-soap-message-security-1.0#"
4        <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws-soap-message-security-1.0#"
5          c7761d94d64f">MIIE/zCAuegAwIBAgICAN4wDQYJKoZIhvNAQELBQAwNjELMAkGA1UEBhMCaX0xEzARBgNVBAoMCmdvdndheS5vcmcxEjAQBgNVBAMMCUdvdldheSB0TAEf
6          /Wud06/rYXIVIDHLYmjypb/fL0SL8SKA6uW9swPXdcoGPk9aqw0iv0/8w2Lpvi1657H+BtNjeFhSmUnNl7C25Hba/WivKh782i3F5LYc4sY8H9nfC/fa6QouidLTxWohKwzNl
7          /zAJBgNVHRMEAjAAMBEGCWCG5AG+EIBAQQAeWIHgDAzBgLghkgBhvhCAQ8EjhYKT3B1bNTTCBH2W5lcmF02W0gQ2xpZW50IElnRpZmljYXRlMB0GA1UdDg0WBGRUaIcyEn
8          /JIBWmVuatppwNcJRTZ106qmIElqmoBTWLZj0MxI/+zSWWQUTMNGNsUzzTDS11rmet1dRcbKVvNcxtrPHH4ysh5jdip1fn7G314CaTjJHBo2Ufuadeb63dfqgRc6QzmeR
9          /OFgpiDpcA7fxITX0gDokm+WqgMAZ7s6DEmgW=h7KL6ub0hewzukba5dpYbqcyioDaomD4ywvaI5csvmubwSRIalRH80uew0JcyeJSfEY8FslFudoBLG9340tI4HnT2CBM8
10         /NKL76fLQPRGachtEV4x0nCe8N0m280Ap1ohYpPUTv5YIP5y=</wsse:BinarySecurityToken>
11         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-4b6e4224-d2df-4f57-814c-2b8a47ec328d">
12           <ds:SignedInfo>
13             <ds:CanonicalizationMethod 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"/>
15             </ds:CanonicalizationMethod>
16             <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
17             <ds:Reference URI="#TS-91e2766f-c512-4440-bfa1-046bbbdec9b7">
18               <ds:Transforms>
19                 <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
20                   <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap wsse"/>
21                 </ds:Transform>
22               </ds:Transforms>
23             </ds:Reference>
24           </ds:SignedInfo>
25         </ds:Signature>
26       </soap:Header>
27     <soap:Body>
28       <CelsiusToFahrenheitResponse xmlns="https://www.w3schools.com/xml/">
29         <CelsiusToFahrenheitResult>68</CelsiusToFahrenheitResult>
30       </CelsiusToFahrenheitResponse>
31     </soap:Body>
32   </soap:Envelope>

```

Figure3.32: Messaggio inviato dal fruttore

token di sicurezza presente nell'header soap.

Informazioni ModI

Sicurezza Messaggio ID_AUTH_SOAP_01

Sicurezza Canale ID_AUTH_CHANNEL_02

Interazione Bloccante

Sicurezza Messaggio

MessageID cf25feec-c310-11ed-8b12-0242c0a8d002

WSA-From app1.enteesterno.govway.org

WSA-To TempConvertSoap.ente.govway.org

Expiration 2023-03-15_10:27:58.622

IssuedAt 2023-03-15_10:26:58.622

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

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

Elementi SOAP Firmati

ReplyTo http://www.w3.org/2005/08/addressing

MessageID http://www.w3.org/2005/08/addressing

Action http://www.w3.org/2005/08/addressing

From http://www.w3.org/2005/08/addressing

To http://www.w3.org/2005/08/addressing

Timestamp http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

Figure3.33: Traccia della richiesta elaborata dall'erogatore

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. 3.32](#)).
5. Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al certificato X.509 presente all'interno dell'header WSSecurity. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

Conformità ai requisiti ModI

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

Configurazione

Nota

Per operare con la govwayConsole in modo conforme a quanto previsto dalla specifica del Modello di

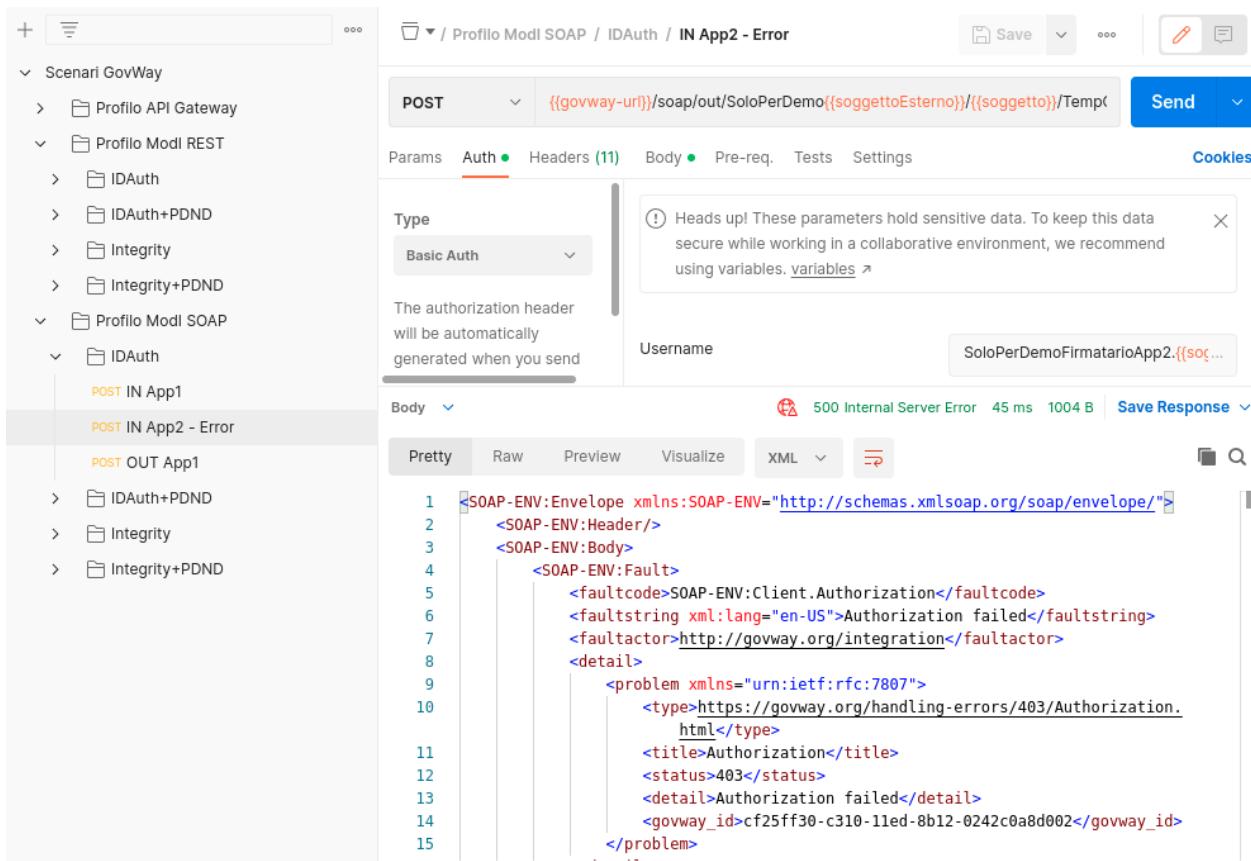


Figure3.34: Pattern IDAuth - Erogazione API SOAP - Autorizzazione negata, esecuzione da Postman

Interoperabilità si deve attivare, nella testata dell’interfaccia, il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

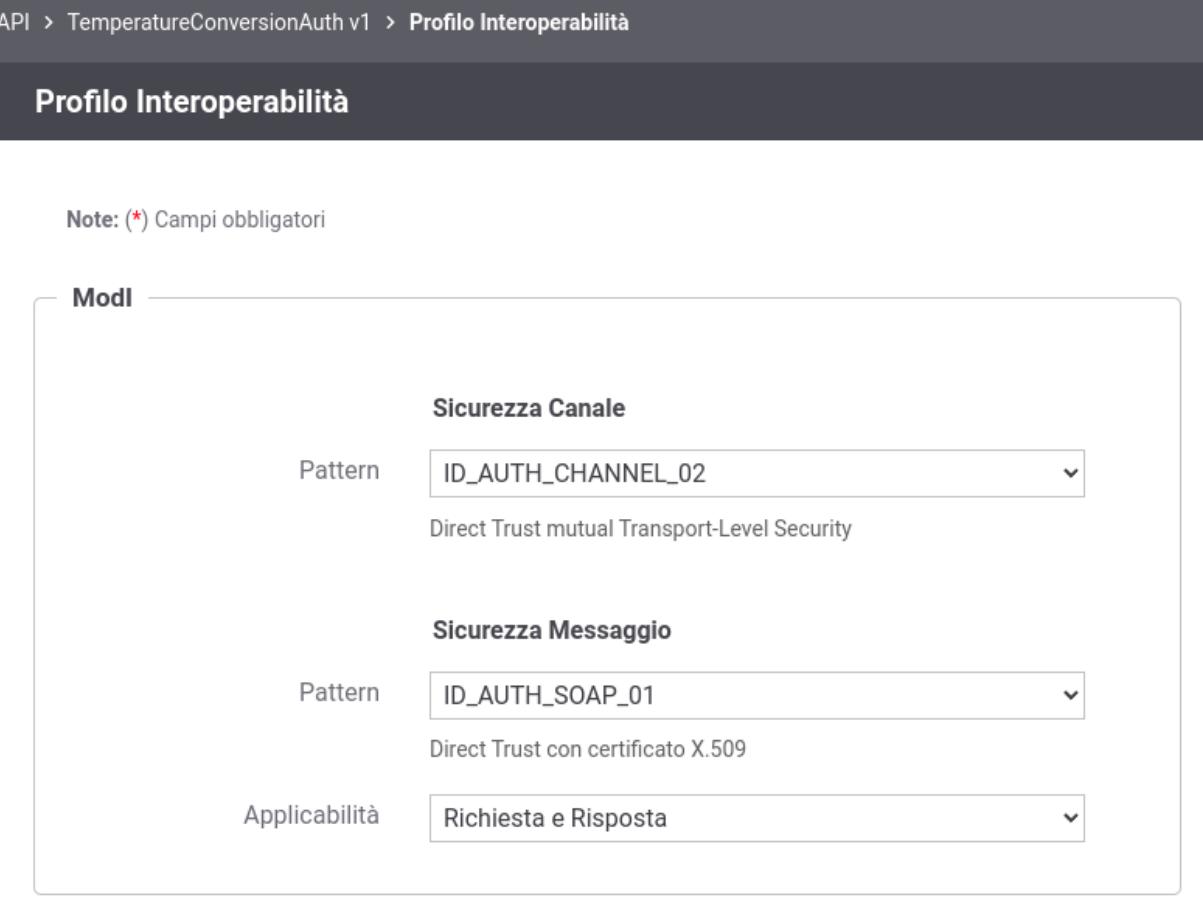


Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario *Configurazione*. Nel seguito sono evidenziate le sole differenze.

L’interfaccia wsdl del servizio soap è ottenibile all’indirizzo “<https://www.w3schools.com/xml/tempconvert.asmx?wsdl>”.

Registrazione API

Viene registrata l’API «TemperatureConversionAuth» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.36).



The screenshot shows the configuration interface for the TemperatureConversionAuth API. The top navigation bar shows "API > TemperatureConversionAuth v1 > Profilo Interoperabilità". The main title is "Profilo Interoperabilità". A note at the top says "Note: (*) Campi obbligatori". The "ModI" section is expanded, showing two configuration groups: "Sicurezza Canale" and "Sicurezza Messaggio". Under "Sicurezza Canale", the "Pattern" dropdown is set to "ID_AUTH_CHANNEL_02" (Direct Trust mutual Transport-Level Security). Under "Sicurezza Messaggio", the "Pattern" dropdown is set to "ID_AUTH_SOAP_01" (Direct Trust con certificato X.509), and the "Applicabilità" dropdown is set to "Richiesta e Risposta".

Figure3.36: Configurazione Pattern ModI «ID_AUTH_SOAP_01» sulla API SOAP

Erogazione

Si registra l'erogazione SOAP “TempConvertSoapAuth”, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.37). In questo contesto vengono inseriti i dati necessari per validare le richieste in ingresso.

ModI - Richiesta

Sicurezza Messaggio

TrustStore Certificati	Default
Time to Live	Default
WSAddressing To	TempConvertSoap.ente.govway.org

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

Figure3.37: 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. 3.38).

3.1.4 Fruizione API SOAP

Obiettivo

Fruire di un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza “ID_AUTH_SOAP_01” descritto nella sezione modipa_idar01.

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 il trust del certificato X.509 in modo da assicurare sia a livello di canale che a livello di messaggio l'autenticazione e autorizzazione del fruitore.

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. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_01».

Modi - Risposta

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	Default
Time to Live (secondi) *	60

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

Figure3.38: Configurazione risposta dell'erogazione

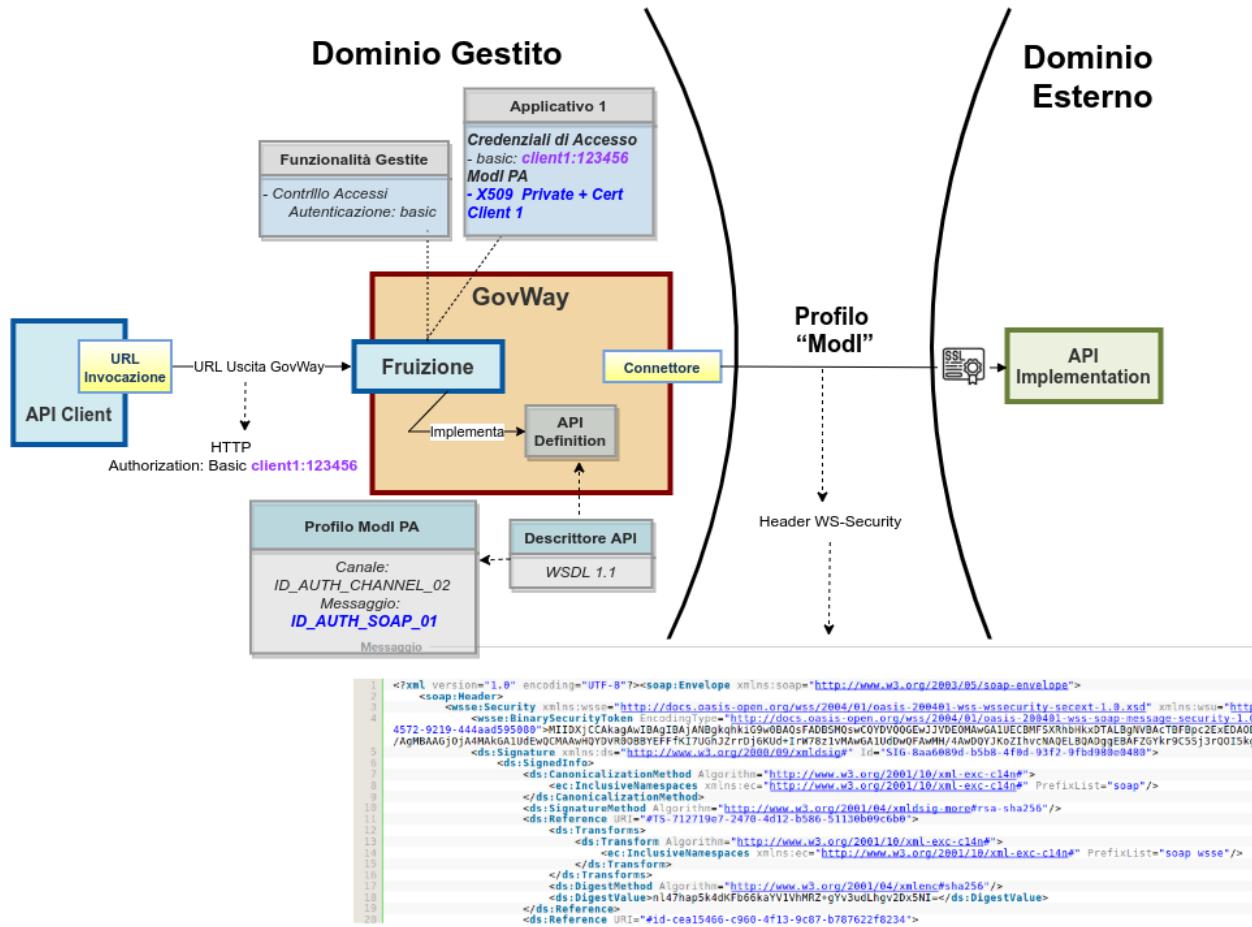


Figure3.39: Fruizione di una API SOAP con profilo "ModI", pattern ID_AUTH_SOAP_01

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.40: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API SOAP di esempio (Temperature Conversion) definita con pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_02» e «ID_AUTH_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 «CelsiusToFahrenheit» sulla fruizione configurata su Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

Figure3.41: Pattern IDAuth - Fruizione API SOAP, esecuzione da Postman

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 gowayMonitor si può visualizzare il messaggio di richiesta in uscita, analogo a quanto già visto in [Fig. 3.32](#).
2. Per verificare l'utilizzo del canale SSL, in accordo al pattern «ID_AUTH_CHANNEL_02», si procede come già illustrato per [Esecuzione](#).
3. 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. Consultando la traccia relativa alla trasmissione della risposta, sono visibili tra le altre informazioni i dati di autenticazione dell'erogatore e i riferimenti temporali.

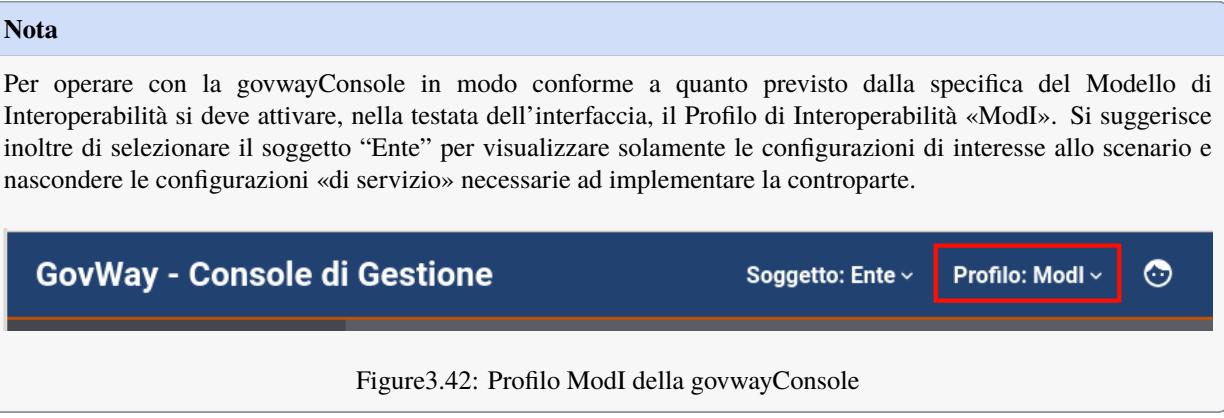
Conformità ai requisiti ModI

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

Configurazione

Nota

Per operare con la gowayConsole in modo conforme a quanto previsto dalla specifica del Modello di Interoperabilità si deve attivare, nella testata dell'interfaccia, il Profilo di Interoperabilità «ModI». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.42: Profilo ModI della gowayConsole

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

Registrazione API

Viene registrata l'API «TemperatureConversionAuth» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» ([Fig. 3.36](#)).

Fruizione

Si registra la fruizione SOAP “TempConvertSoapAuth”, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» ([Fig. 3.44](#)).

La sezione «ModI Risposta» definisce i criteri per la validazione dei messaggi di risposta ([Fig. 3.45](#)).

3.2 Pattern “INTEGRITY_01”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_idar03.

API > TemperatureConversionAuth v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern ▼
Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern ▼
Direct Trust con certificato X.509

Applicabilità ▼

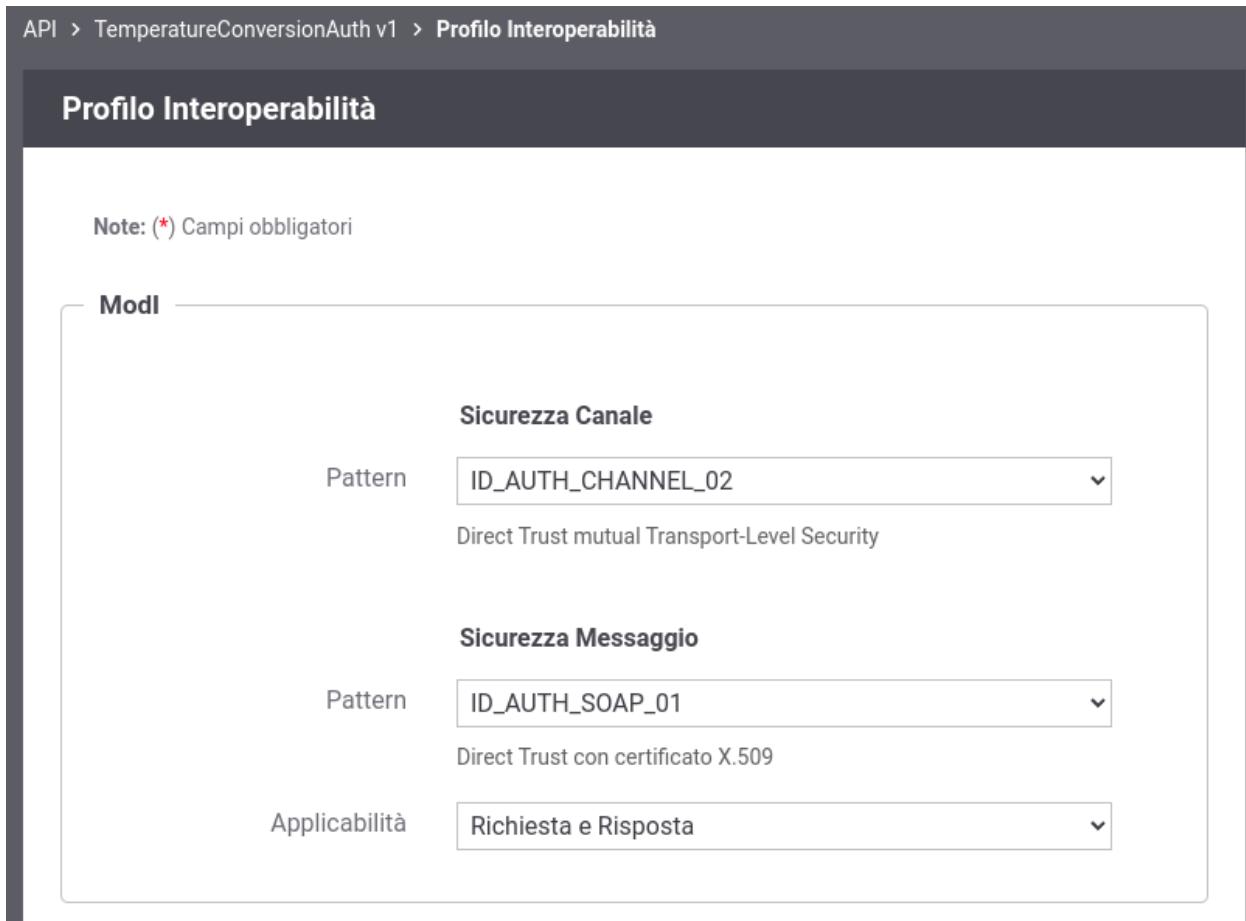


Figure3.43: Configurazione Pattern ModI «ID_AUTH_SOAP_01» sulla API SOAP

Modi - Richiesta

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	Definito nell'applicativo
Time to Live (secondi) *	60

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

WSAddressing To 

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

Figure3.44: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

TrustStore Certificati	Default
Time to Live	Default

Verifica WSAddressing To La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente



Figure3.45: Configurazione risposta della fruizione

3.2.1 Erogazione API REST

Obiettivo

Esportare un servizio, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza «INTEGRITY_REST_01» descritto nella sezione modipa_idar03.

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 oltre a garantire l'autenticazione dell'interlocutore un supporto a garanzia dell'integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

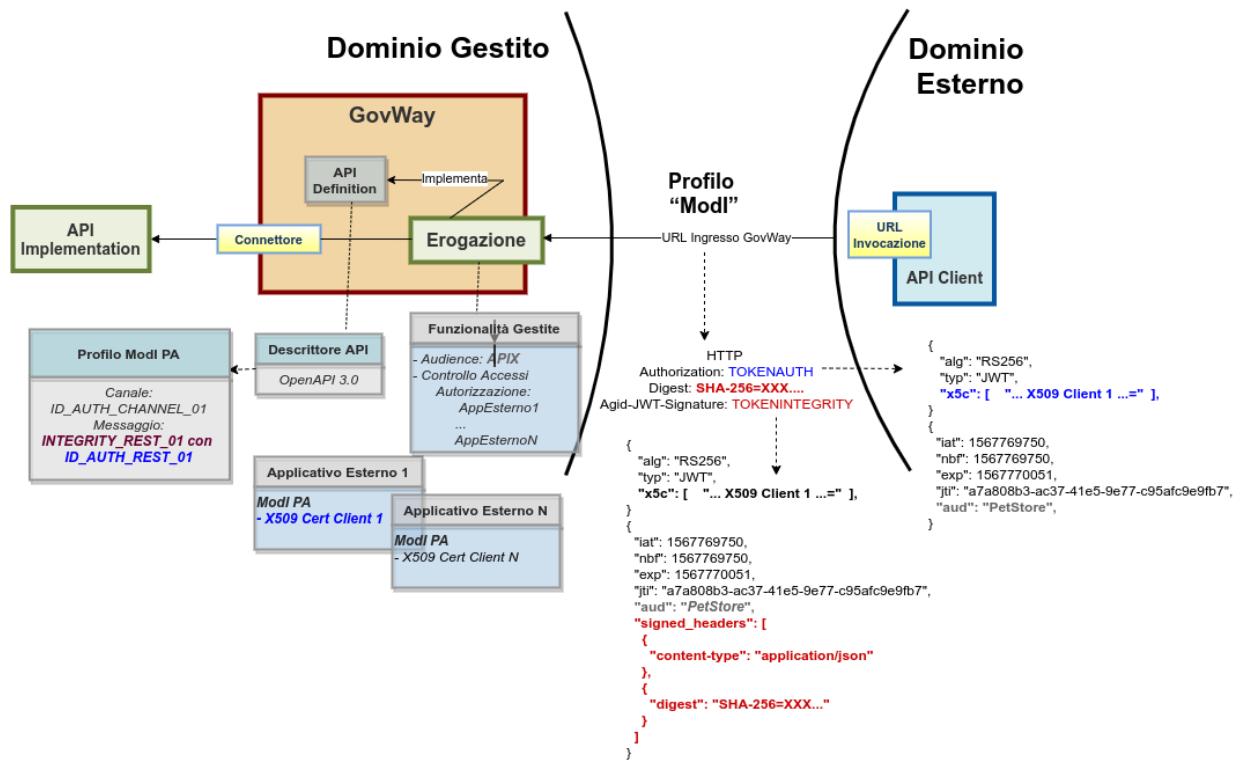


Figure3.46: Erogazione di una API REST con profilo «ModI», pattern INTEGRITY_REST_01 con ID_AUTH_REST_01

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

● **GovWay - Console di Monitoraggio**

Soggetto: Ente
Profilo: ModI

Figure3.47: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di sicurezza utilizzato che in questo scenario è «INTEGRITY_REST_01 con ID_AUTH_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity - IN App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

```

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

```

Figure3.48: Pattern Integrity - Erogazione API REST, esecuzione da Postman

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”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.49.

Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization» e «Agid-Jwt-Signature» che contengono rispettivamente il token di sicurezza per l'autenticazione e per l'integrità. È inoltre presente l'header http «Digest» che contiene il valore per la verifica dell'integrità del payload.

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fbb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCl6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6xWQdfvHBaJT3on7jaCV6LVEXEaqAqfDWwl48L8SextE3UyuuGh-1s-g6320H8j6SIFr8tzsK4p-Fc94Wc1xhMJxjXAer6Sh80
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCl6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6WyJNSjllVuNpGcBUWGoh1dKhK Cv6nd6LFjWiFSdExxjto5i8iBty ExSu06IHL0iaD2p1jkYrG37MgE6f-1xBYCqjElCchD6GQ8R4fEc5
Digest	SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
Accept	/*
Govway-Transaction-Id	d1a3b973-4fbb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

Figure3.49: Messaggio inviato dal fruttore

- Grazie alle configurazioni presenti nell'erogazione, ed in particolare alla relazione di trust stabilita con il fruttore, Govway è in grado di validare i dati di sicurezza ricevuti andando a decodificare il token. Nella fase di validazione del token si può notare come la sezione header (Fig. 3.50) di entrambi i token «Authorization» e «Agid-Jwt-Signature» riportano l'identità del fruttore e il suo certificato X.509.
- Il messaggio ricevuto dal Govway viene quindi validato, sulla base dei pattern di sicurezza previsti nello scambio, verificando in questo caso l'identità del fruttore, la validità temporale, la corrispondenza dell'audience ricevuto con quello atteso e la corrispondenza del digest con il payload e con il valore interno al token «Agid-Jwt-Signature». 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. 3.53). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di sicurezza presenti, tra cui si può notare il digest e gli header http firmati.
- Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al

HEADER: ALGORITHM & TOKEN TYPE	
→ {	<pre> "alg": "RS256", "typ": "JWT", "kid": "app1.enteesterno.govway.org", "x5c": ["MIIE/jCCAuagAwIBAgICAPgwDQYJKoZIhvcNAQELBQAwNjELMAkGA1 UEBhMCaXQxEzARBgNVBAoMCmdvdndheS5vcmcxJzAQBgNVBAMCUdvd 1dheSBDDQTAeFw0yMjEwMTkwNzU1NTThaFw0zNzEwMTUwNzU1NTThaMEgx CzAJBgNVBAYTAm10MRMwEQYDVQQKDApnb3Z3YXkub3JnMSQwIgYDVQQ DDBthcHAXLmVudGVFc3R1cm5vLmdvdndheS5vcmcwggEiMA0GCSqGSI b3DQEBAQAA4IBDwAwggEKAoIBAQCl/cfENX06hdvEVxJiJAF00ePjn 5Sh/HIJ2du8hRv0zA+KFFieaF4xh1mSOT1oq/vwwxFxqvdk1bTJ37r jBo6DKuQZor83j/Do87x3sFJe/epGKx96Q3PRE9mA1qx3Y5FFShfGNZ zG2RFNA2jhVQ/bs8d9E051FC3XshF90CtJJs9LgvT2+0+uJK3siA6ht KcYQ58UcK1W1Y109MnXqaz82TiH93eTSkk33w0A9atzC0w3JAVmcRRk d0hFBjMeEvNR86cdNfy9Xit7ZDR11IB8te10/fI/oAWo0K/3TbF1X0r VL1QhMc1JdqS3NwJLayoqmqZT/Xh5DqjD17ldghwbAgMBAAGjggECMIH /MAkGA1UdEwQCMAAwEQQYJYIZIAb40gEBBAQDAgeAMDMGCWCGSAGG+E IBDQQmF1RPcGVuU1NMIEd1bmVYXR1ZCBDbG11bnQgQ2VydGImaWNhd GUwHQYDVVR00BBYEFCBwk8Bs9JS+6c/vTU+JX0eqX81BMGYGA1UdIwRf MF2AFCqhfNpm2RdIA3igRXzNEeJ5ivegoTqkODA2MQswCQYDVQQGEwJ pdDETMBeGA1UECgwKZ292d2F5Lm9yZzESMBAGA1UEAwwJR292V2F5IE NBggkA4tGAdmeSJF4wDgYDVR0PAQH/BAQDAgXgMBMGA1UdJQQMMAoGC CsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQDRj52cdYwcqFDNmC29 CY0DR0N0TM/5RKq9sL6sgI7z4cUmkyIEGh/9YQD0RFhDBVGZ80rx0ka sZ/Po0Iuw+41f9IDTBe04Ym0CK3M1M9H2LiEKe9hngRtjzGw5tFRQNq KbLLX61otJAXuE488SrSAMbEDez1bZt+V1Sgc48fOKsjShUs8CwSW0G 6RE5w4Q4oa0dX971PTziWd0FnxBfN17/HAYA0625/vcp8PrZLqhTIGH 7dt+1T4Hb+i10wKBS7B8Cab0Gh0spIHdDGNEyX50d1ZYmWJQ10ysK6 1Yx1WtCrKPfmsvSeqiVxJPHUgwTsFPrgoVRt+dT1NnAdXYxFk0Yxz7z n7qeKD16cXHLTsYet1cQfedyDPE0r1i4GFL1KY37NFqRtJx5NadkJk6 GXk43zIFQo119PGJ8nVHupB6IBJ1h/6xem1TTMSt52zcjV4b5zRHL8Z qNF+S0QnJKch2FcyAYuGjuVj0qa5rhi5wNcy71lcDShM8tsPJ5qpW1M E0hmhWWY+w5KBCpMoLBn9cvqAn/N19L3e3SqH1KLp8Hw05CtH4/tLEe 3N+0z+8xzcmLdqbAZ9nD7YVLVoyt5Y+Ixuj17F18dzEh9dzcLhJojsB mPjoFMMyulbpjZG0A1TjKVpkxyXgaqsd9Hjs4ATg79Vk8U/GnEXJhXQ xU2TYw=="], "x5t#S256": "agRQxqs- VYDP2NIzbR7XH2GiInWH2bcL1xMPhimfMKK" } </pre>

Figure3.50: Sezione «Header» del Token di sicurezza «Authorization» e «Agid-Jwt-Signature»
 I payload dei due token invece differiscono (Fig. 3.51 e Fig. 3.52). In entrambi sono presenti i riferimenti temporali (iat, nbf, exp) e l'audience (aud), mentre solamente nel payload del token «Agid-Jwt-Signature» è presente il claim “signed_headers” utilizzato per la verifica dell'integrità.

PAYLOAD: DATA
{ "iat": 1666176318, "nbf": 1666176318, "exp": 1666176378, "jti": "1f46c4b4-4f9b-11ed-a5ac-0242ac140002", "aud": "petstore.ente.govway.org", "client_id": "app1.enteesterno.govway.org", "iss": "SoloPerDemoEnteEsterno", "sub": "SoloPerDemoFirmatarioApp1" }

Figure3.51: Sezione «Payload» del Token di sicurezza «Authorization»

PAYLOAD: DATA
{ "iat": 1666190361, "nbf": 1666190361, "exp": 1666190421, "jti": "d1b37101-4fbb-11ed-a5ac-0242ac140002", "aud": "petstore.ente.govway.org", "client_id": "app1.enteesterno.govway.org", "iss": "SoloPerDemoEnteEsterno", "sub": "SoloPerDemoFirmatarioApp1", "signed_headers": [{ "digest": "SHA- 256=0hjWocHmylM/B4HeXlp1NxygvqU7zKjERTUMDPVfhPY=", "content-type": "application/json" }] }

Figure3.52: Sezione «Payload» del Token di sicurezza «Agid-Jwt-Signature»

Informazioni Mod

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_REST_01 con ID_AUTH_REST_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione Accesso CRUD

Sicurezza Messaggio

Digest SHA-256=0hjWocHmyIM/B4HeXIplNxygvqU7zKjERTUMDPVfhPY=
ClientId app3.enteesterno.govway.org
Subject SoloPerDemoFirmatarioApp3
Issuer SoloPerDemoEnteEsterno
MessageId 20fb762b-08fe-11ee-9028-0242c0a85002
Audience petstore.ente.govway.org
NotBefore 2023-06-12_11:42:54.000
Expiration 2023-06-12_11:43:54.000
IssuedAt 2023-06-12_11:42:54.000
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app3.enteEsterno.govway.org, O=govway.org, C=it

Headers HTTP Firmati

content-type application/json
digest SHA-256=0hjWocHmyIM/B4HeXIplNxygvqU7zKjERTUMDPVfhPY=

Figure3.53: Traccia della richiesta elaborata dall'erogatore

certificato X.509 presente all'interno del token. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

The screenshot shows the Postman interface with the following details:

- Left Sidebar:** Shows a tree structure of scenarios and profiles, including "Scenari GovWay", "Profilo ModI REST" (selected), "IDAuth", "IN App1", "IN App2 - Error" (selected), "OUT App1", "Integrity", and "Profilo ModI SOAP".
- Request Details:**
 - Method: POST
 - URL: `({govway-url})/rest/out/SoloPerDemo({soggettoEsterno})/({soggetto})/PetStore`
 - Headers: (10)
 - Body: (empty)
 - Tests: (empty)
 - Settings: (empty)
- Params:** A table with one row: "Key" (Value) and "Description" (Description).
- Body:** A JSON response with status 403 Forbidden, 46 ms, 446 B. The JSON content is:

```

1  {
2    "type": "https://govway.org/handling-errors/403/Authorization.html",
3    "title": "Authorization",
4    "status": 403,
5    "detail": "Authorization failed",
6    "govway_id": "6072f3df-4fbe-11ed-a5ac-0242ac140002"
7  }

```

Figure3.54: Pattern Integrity - Erogazione API REST - Autorizzazione negata, esecuzione da Postman

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. 3.5);
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. l'identificazione del fruitore avviene rispetto al certificato X.509 presente all'interno del token. È stato anche mostrato come sia possibile configurare criteri autorizzativi puntuali.

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con le sole differenze dovute al differente pattern di sicurezza utilizzato «INTEGRITY_REST_01 con ID_AUTH_REST_01».

Registrazione API

Viene registrata l'API «PetStoreIntegrity» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_REST_01 con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.56).

API > PetStoreIntegrity v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_02

Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_REST_01 con ID_AUTH_REST_01

Integrità payload del messaggio

Header HTTP del Token: Agid-JWT-Signature + Authorization Bearer

Applicabilità: Richiesta e Risposta

Digest Richiesta: Non ripudiabilità della trasmissione (i)

Informazioni Utente: Dati dell'utente che effettua la richiesta (i)

Figure3.56: Configurazione Pattern ModI «INTEGRITY_REST_01 con ID_AUTH_REST_01» sulla API REST

Erogazione

Si registra l'erogazione «PetStoreIntegrity», relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.57). In questo contesto vengono inseriti i dati necessari per validare le richieste in ingresso.

Figure3.57: 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. 3.58).

3.2.2 Fruzione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza “INTEGRITY_REST_01” descritto nella sezione modipa_idar03.

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 oltre a garantire l'autenticazione dell'interlocutore un supporto a garanzia dell'integrità del messaggio.

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. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01»;

Modi - Risposta

Sicurezza Messaggio

Algoritmo: RS256

HTTP Headers da firmare *: Digest x, Content-Type x, Content-Encoding x

Riferimento X.509: Utilizza impostazioni della Richiesta

Certificate Chain:

KeyStore: Default

Time to Live (secondi) *: 60

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

Claims: ⓘ

Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli

▼ Contemporaneità Token Authorization e Agid-JWT-Signature

Figure3.58: Configurazione risposta dell'erogazione

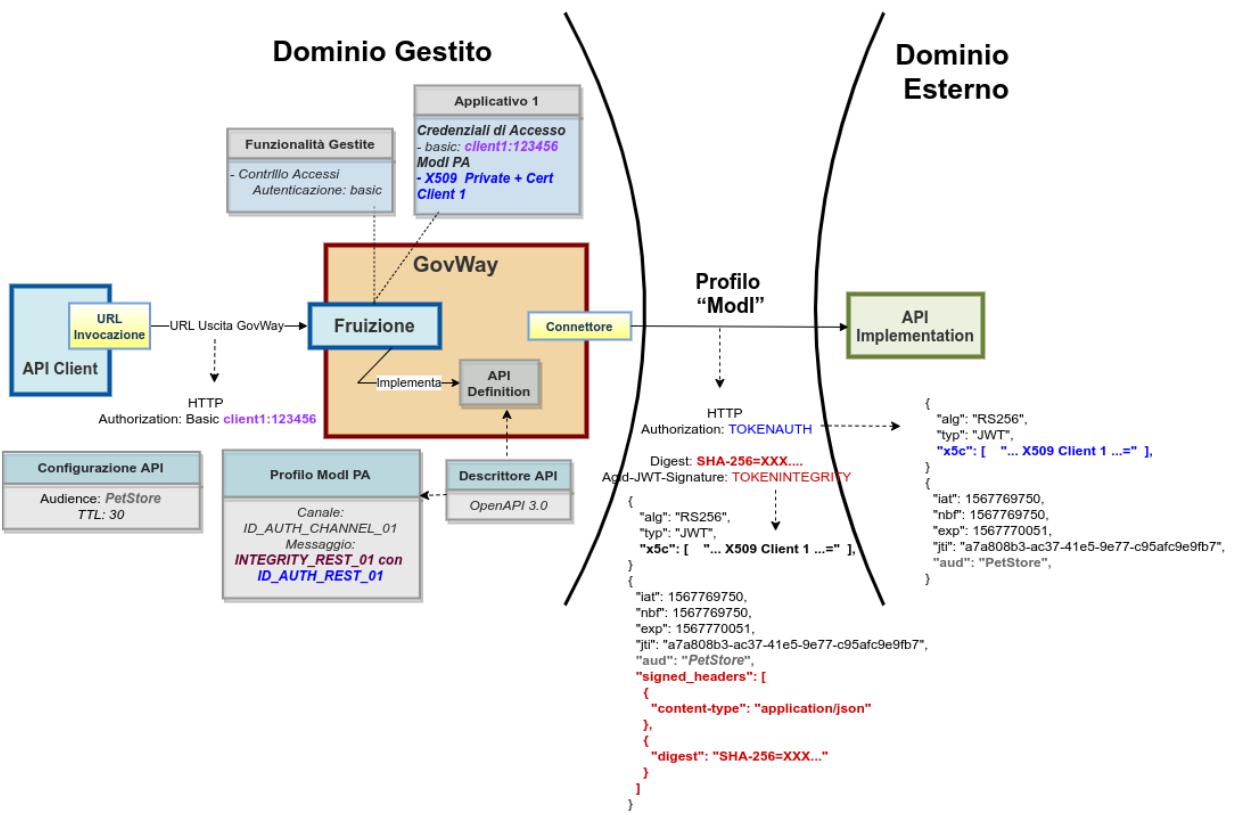


Figure3.59: Fruizione di una API REST con profilo "ModI", pattern INTEGRITY_REST_01 con ID_AUTH_REST_01

4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.60: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza utilizzato che in questo scenario è «INTEGRITY_REST_01 con ID_AUTH_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

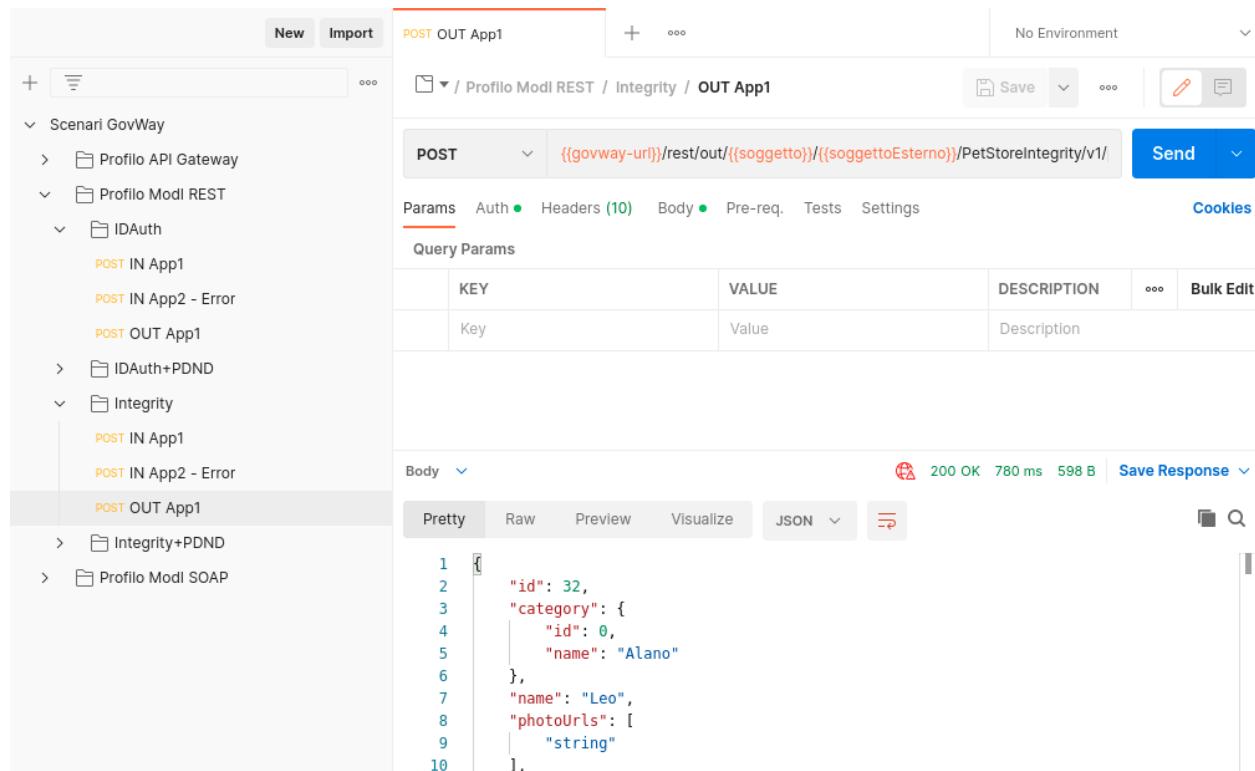


Figure3.61: Pattern Integrity - Fruizione API REST, esecuzione da Postman

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 la console “govwayMonitor”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- 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 sono stati aggiunti gli header HTTP «*Authorization*» e «*Agid-Jwt-Signature*» che contengono rispettivamente il token di sicurezza per l'autenticazione e per l'integrità. È inoltre presente l'header http «*Digest*» che contiene il valore utilizzabile dall'erogatore per la verifica dell'integrità del payload. (Fig. 3.62).

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCl6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6xWqdhfvHBaJT3on7jaCV6LVEXEaqAqfDWl48L8SextE3UyuuGh-1s-g6320H8j6SIf8tzsK4p-Fc94WclxhMJxjXAer6Sh80
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCl6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6WyJNSillVuNpGcBUWGoh1dKhKCv6nd6LFjWiFSdExxjto5i8iBtyjExSu06iHLOiaD2pI1jkYrG37MgE6f-1xBYCqjElCchD6GQ8R4fEc5
Digest	SHA-256=OhjWochHmylM/B4HeXplNxygyqU7zKjERTUMDPVfhPY=
Accept	/*
Govway-Transaction-Id	d1a3b973-4fb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

Figure3.62: Messaggio di richiesta in uscita (con token di sicurezza inseriti nell'header HTTP)

- L'header e i payload dei token sono identici a quelli visualizzati nello scenario di erogazione REST, relativamente al messaggio in ingresso (Fig. 3.50, Fig. 3.51 e Fig. 3.52). Le informazioni inserite nel token vengono anche tracciate e sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.63). Nella sezione «*Sicurezza Messaggio*» sono riportate le informazioni estratte dai token di sicurezza, tra cui si può notare il digest e gli header http firmati.

Conformità ai requisiti ModI

Informazioni Modl

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_REST_01 con ID_AUTH_REST_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione 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=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
Subject App1-PDND
Issuer Ente
ClientId App1-PDND
Audience petstore.enteEsterno.govway.org
MessageId 25c1b125-08fe-11ee-9028-0242c0a85002
Expiration 2023-06-12_11:48:01.000
NotBefore 2023-06-12_11:47:01.000
IssuedAt 2023-06-12_11:47:01.000

Headers HTTP Firmati

content-type application/json
digest SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=

Figure3.63: Traccia della richiesta generata dal fruttore

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. 3.23);
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).

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.64: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con le sole differenze dovute al differente pattern di sicurezza utilizzato «INTEGRITY_REST_01 con ID_AUTH_REST_01».

Registrazione API

Viene registrata l’API «PetStoreIntegrity» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_REST_01 con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.65).

Fruizione

Si registra la fruizione «PetStoreIntegrity», relativa all’API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.66). In particolare è possibile specificare l’audience atteso dall’erogatore e il tempo di validità del token.

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. 3.67).

3.2.3 Erogazione API SOAP

Obiettivo

Esporre un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza “INTEGRITY_SOAP_01” descritto nella sezione modipa_idar03.

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 oltre a garantire l’autenticazione dell’interlocutore un supporto a garanzia dell’integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

API > PetStoreIntegrity v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_02

Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_REST_01 con ID_AUTH_REST_01

Integrità payload del messaggio

Header HTTP del Token: Agid-JWT-Signature + Authorization Bearer

Applicabilità: Richiesta e Risposta

Digest Richiesta: Non ripudiabilità della trasmissione (i)

Informazioni Utente: Dati dell'utente che effettua la richiesta (i)

Figure3.65: Configurazione Pattern ModI «INTEGRITY_REST_01 con ID_AUTH_REST_01» sulla API

Modi - Richiesta

Sicurezza Messaggio

Algoritmo	RS256	<input type="button" value="▼"/>
HTTP Headers da firmare *	<input checked="" type="checkbox"/> Digest <input checked="" type="checkbox"/> Content-Type <input checked="" type="checkbox"/> Content-Encoding	
Riferimento X.509	x5c (Certificate) x5t#256 (Certificate SHA-256 Thumbprint) x x5u (URL)	
Certificate Chain	<input type="checkbox"/>	
Time to Live (secondi) *	60	<input type="button" value=""/>
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token		
Audience	petstore.enteEsterno.govway.org <input type="button" value="i"/>	
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore		
Claims	<input type="button" value=""/>	
Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli		
▼ Contemporaneità Token Authorization e Agid-JWT-Signature		

Figure3.66: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

Riferimento X.509	Utilizza impostazioni della Richiesta
TrustStore Certificati	Default
Time to Live	Default
Verifica Audience	<input checked="" type="checkbox"/> La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente

Contemporaneità Token Authorization e Agid-JWT-Signature

Figure3.67: Configurazione risposta della fruizione

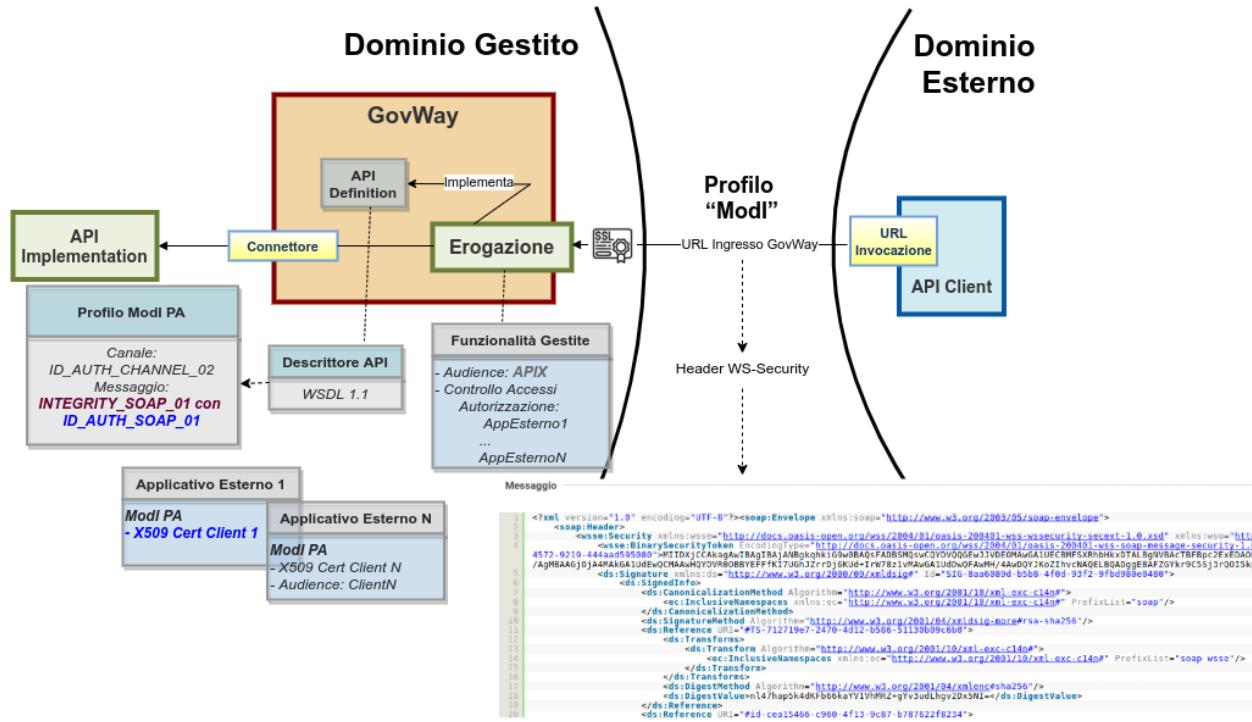


Figure3.68: Erogazione di una API SOAP con profilo "Modi", pattern INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_01»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_SOAP_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.69: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza utilizzato che in questo scenario è «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity - IN App1» che è stata preconfigurata 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.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario [Esecuzione](#). Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in [Fig. 3.32](#). Come si nota, il messaggio SOAP contiene nell'header WS-Security sia il token di sicurezza (elemento «BinarySecurityToken») sia l'elemento «WSAddressing - To» e il digest del payload (elemento «DigestValue») prodotti dal fruitore con la relativa firma digitale (elemento «SignatureValue»).
- 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 dell'audience ricevuto con quello atteso e la corrispondenza del digest rispetto 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. 3.72](#)). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal token di sicurezza presente nell'header soap.
- Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al certificato X.509 presente all'interno dell'header WSSecurity. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

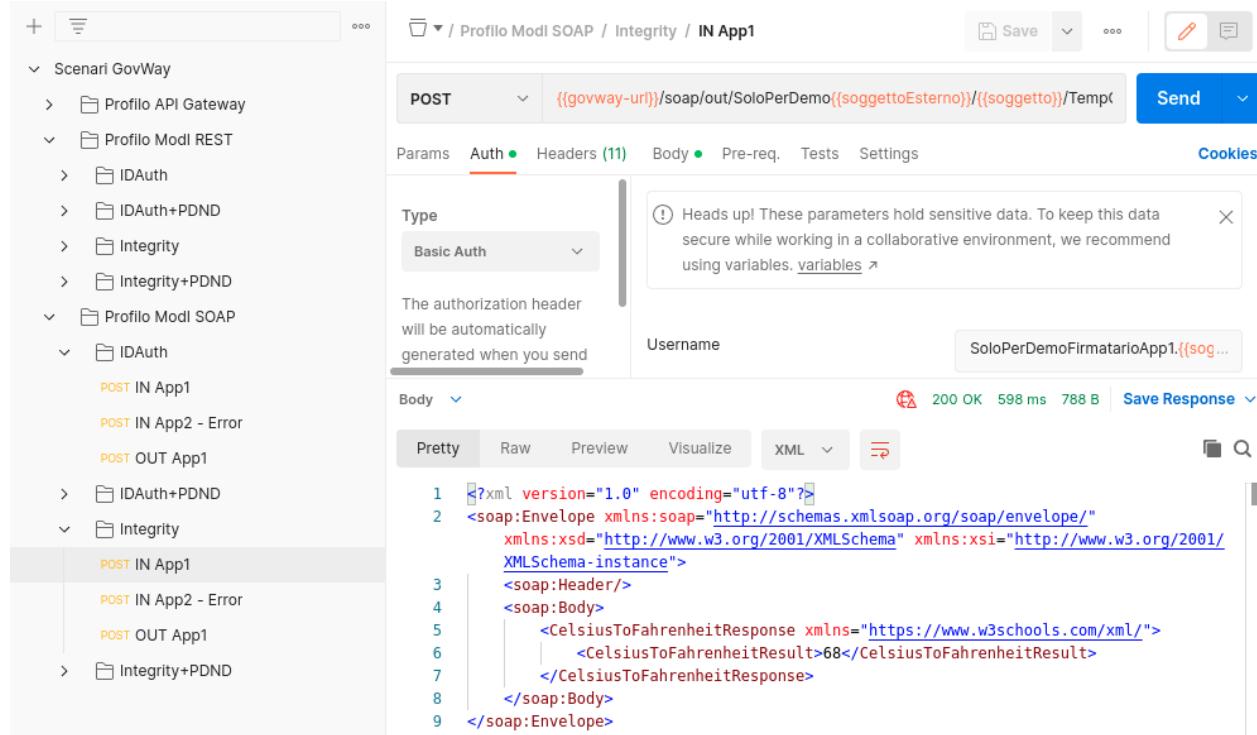


Figure3.70: Pattern Integrity - Erogazione API SOAP, esecuzione da Postman

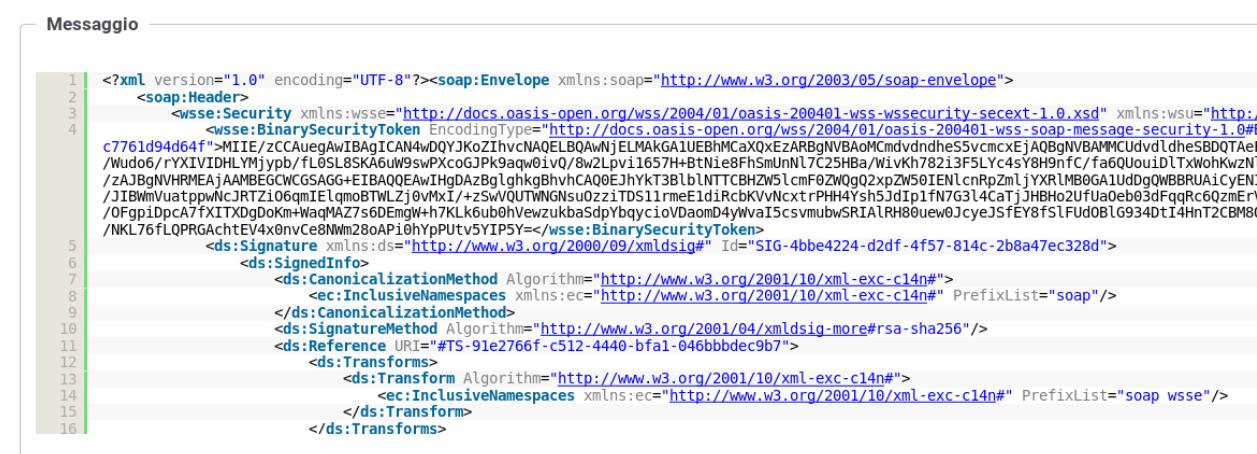


Figure3.71: Messaggio inviato dal fruttore

Informazioni Modl

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione Bloccante

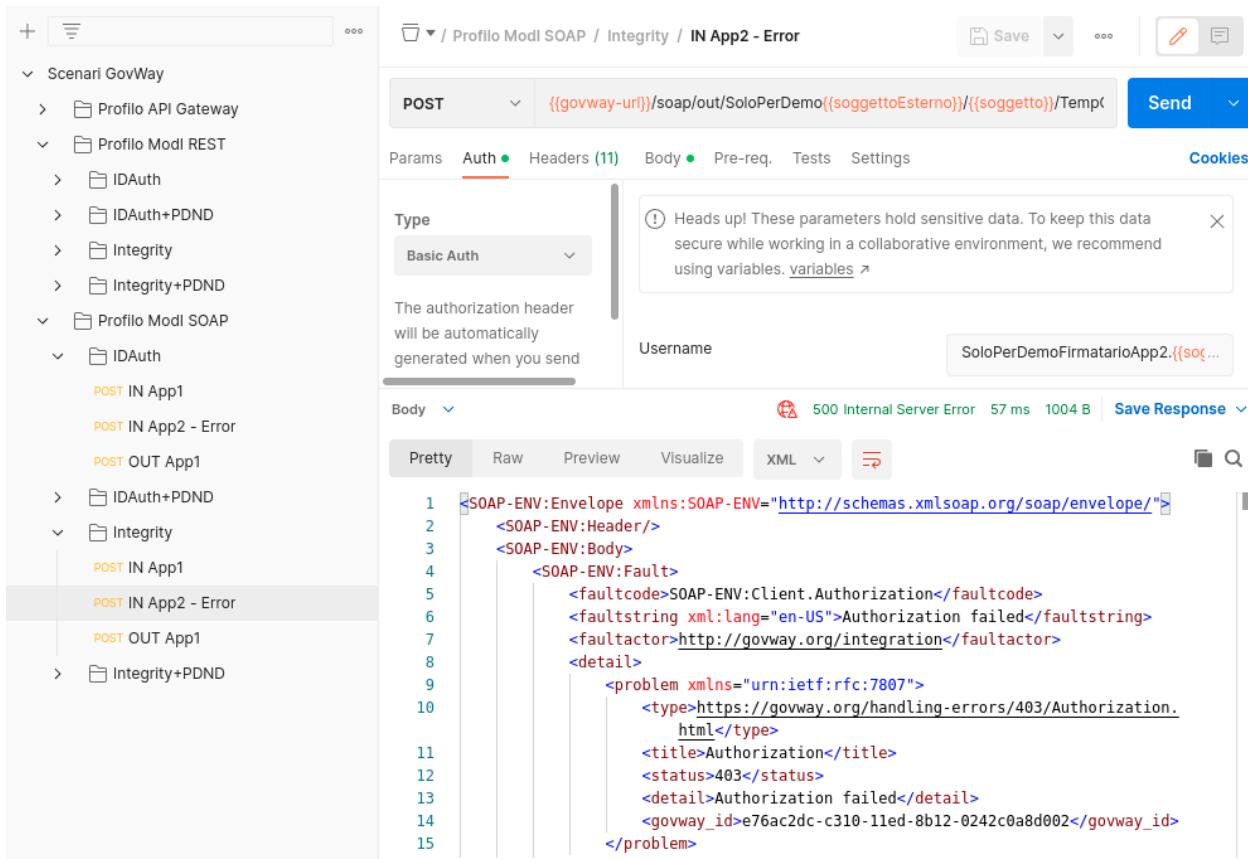
Sicurezza Messaggio

MessageID 297123d9-08fe-11ee-9028-0242c0a85002
WSA-From app3.enteesterno.govway.org
WSA-To TempConvertSoap.ente.govway.org
Digest SHA256=6uByffAl2Xht8Mm1FBluUkvRM83c/Qh4YPvzxEYaqAw=
Expiration 2023-06-12_11:50:37.258
IssuedAt 2023-06-12_11:49:37.258
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app3.enteEsterno.govway.org, O=govway.org, C=it

Elementi SOAP Firmati

Body http://schemas.xmlsoap.org/soap/envelope/
ReplyTo http://www.w3.org/2005/08/addressing
MessageID http://www.w3.org/2005/08/addressing
Action http://www.w3.org/2005/08/addressing
From http://www.w3.org/2005/08/addressing
To http://www.w3.org/2005/08/addressing
Timestamp http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

Figure3.72: Traccia della richiesta elaborata dall'erogatore



The screenshot shows the Postman interface with the following details:

- Left Sidebar:** Shows a tree structure of scenarios and profiles, including "Scenari GovWay", "Profilo API Gateway", "Profilo Modl REST", "Profilo Modl SOAP", and "IDAuth" profiles.
- Header:** The URL is `Profile Modl SOAP / Integrity / IN App2 - Error`.
- Method:** POST
- URL:** `{govway-uri}/soap/out/SoloPerDemo({soggettoEsterno})/({soggetto})/Temp`
- Auth:** Basic Auth (selected)
- Headers:** (11)
- Body:** (Pretty, Raw, Preview, Visualize, XML)
- Body Content (Pretty):**

```

1  <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
2    <SOAP-ENV:Header/>
3    <SOAP-ENV:Body>
4      <SOAP-ENV:Fault>
5        <faultcode>SOAP-ENV:Client.Authorization</faultcode>
6        <faultstring xml:lang="en-US">Authorization failed</faultstring>
7        <faultactor>http://govway.org/integration</faultactor>
8        <detail>
9          <problem xmlns="urn:ietf:rfc:7807">
10            <type>https://govway.org/handling-errors/403/Authorization.html</type>
11            <title>Authorization</title>
12            <status>403</status>
13            <detail>Authorization failed</detail>
14            <govway_id>e76ac2dc-c310-11ed-8b12-0242c0a8d002</govway_id>
15          </problem>

```
- Response:** 500 Internal Server Error, 57 ms, 1004 B
- Buttons:** Save, Send, Cookies

Figure3.73: Pattern Integrity - Erogazione API SOAP - Autorizzazione negata, esecuzione da Postman

Conformità ai requisiti ModI

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

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.74: Profilo ModI della govwayConsole

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

L’interfaccia wsdl del servizio soap è ottenibile all’indirizzo “<https://www.w3schools.com/xml/tempconvert.asmx?wsdl>”.

Registrazione API

Viene registrata l’API «TemperatureConversionIntegrity» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.75).

Erogazione

Si registra l’erogazione SOAP “TempConvertSoapIntegrity”, relativa all’API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.76). 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. 3.77).

3.2.4 Fruizione API SOAP

Obiettivo

Fruire di un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza “INTEGRITY_SOAP_01” descritto nella sezione modipa_idar03.

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 oltre a garantire l’autenticazione dell’interlocutore un supporto a garanzia dell’integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

API > TemperatureConversionIntegrity v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_02

Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01

Integrità payload del messaggio

Applicabilità: Richiesta e Risposta

Digest Richiesta: Non ripudiabilità della trasmissione i

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

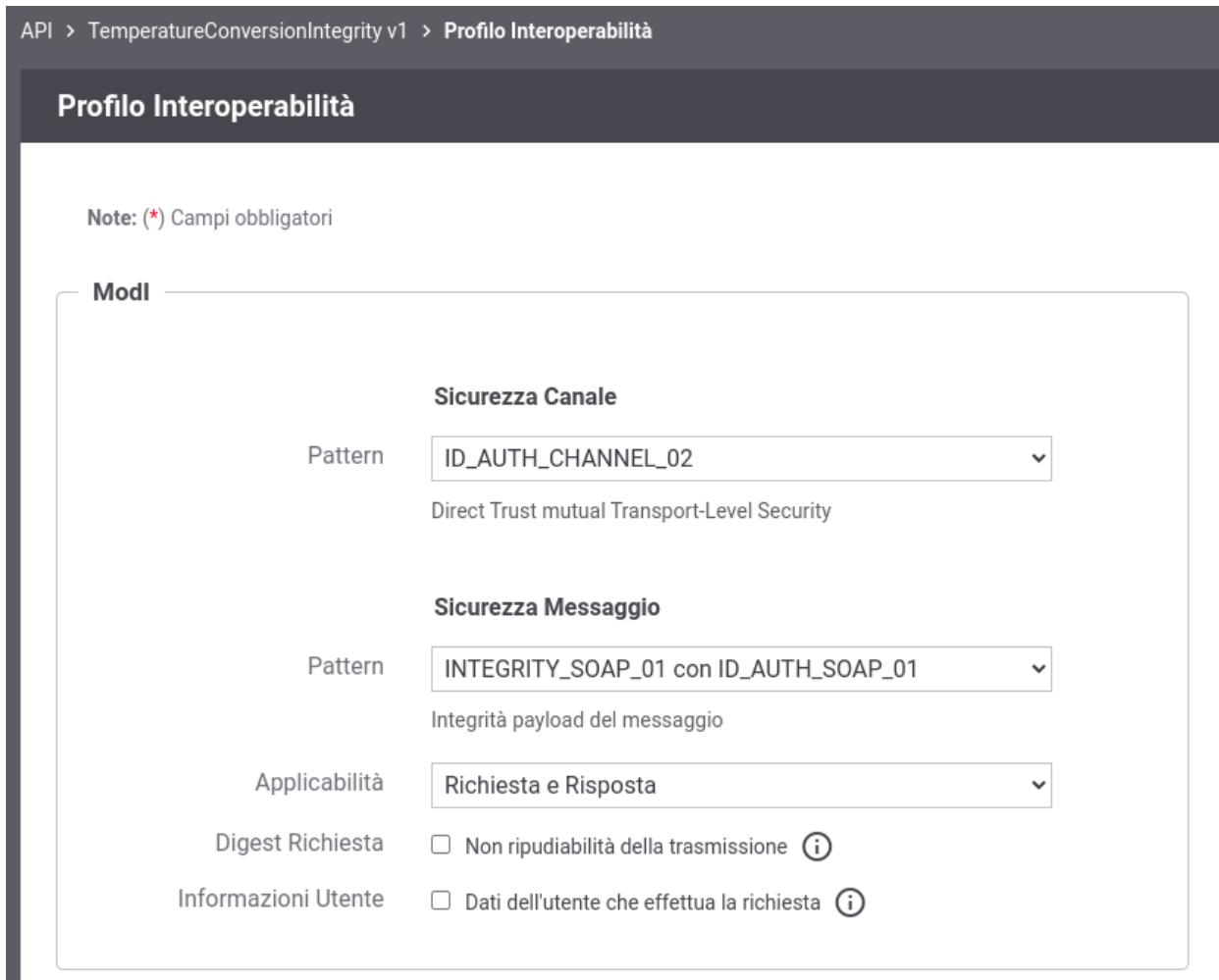


Figure3.75: Configurazione Pattern ModI «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» sulla API SOAP

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati: Default

Time to Live: Default

WSAddressing To: TempConvertSoap.ente.govway.org

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



Figure3.76: Configurazione richiesta dell'erogazione

Modi - Risposta

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	Default
Time to Live (secondi) *	60

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

Figure3.77: Configurazione risposta dell'erogazione

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. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_01»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_SOAP_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Monitoraggio

Soggetto: Ente Profilo: ModI

Figure3.79: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza utilizzato che in questo scenario è «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01».

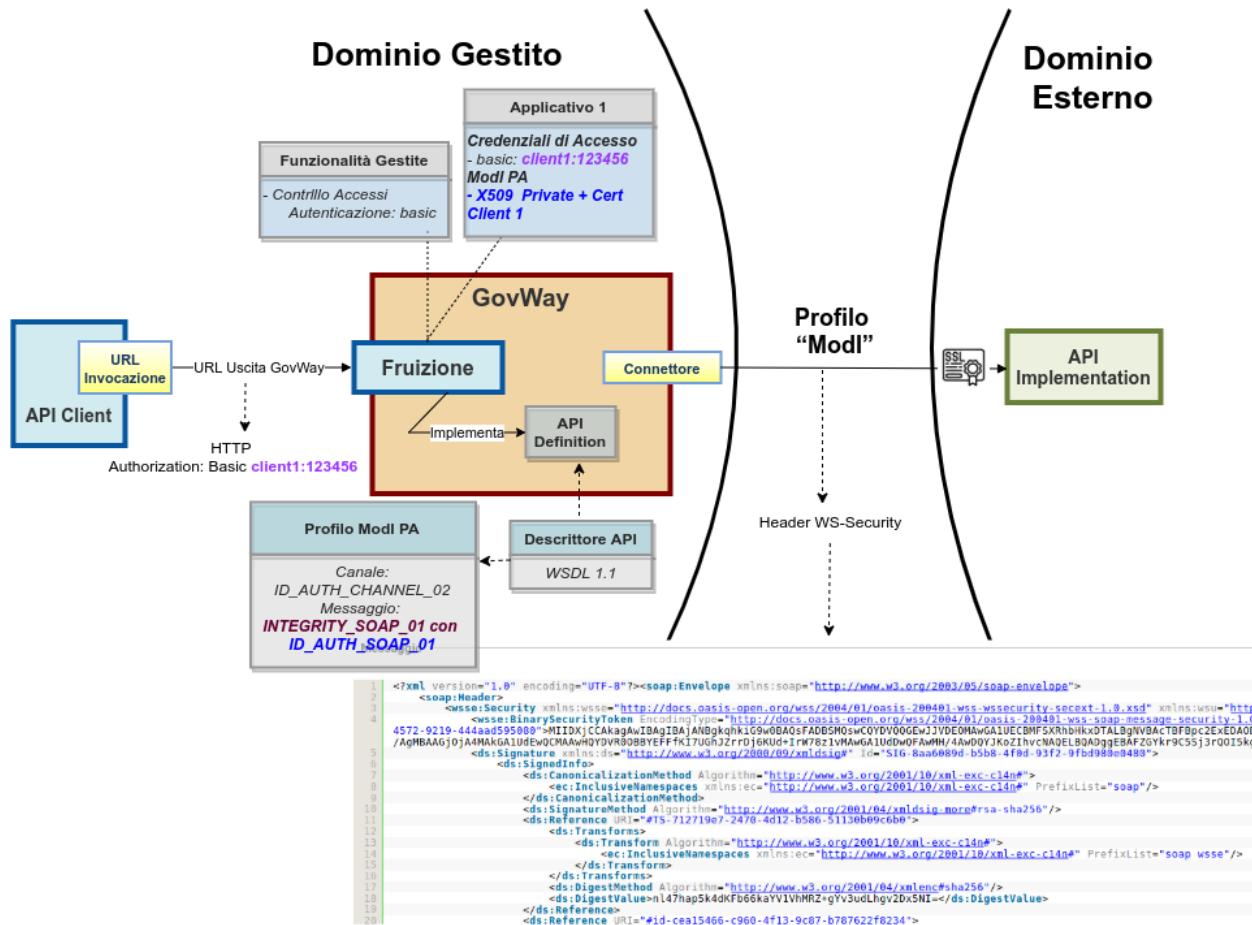


Figure3.78: Fruizione di una API SOAP con profilo “ModI”, pattern INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3   <soap:Header/>
4   <soap:Body>
5     <CelsiusToFahrenheitResponse xmlns="https://www.w3schools.com/xml/">
6       <CelsiusToFahrenheitResult>68</CelsiusToFahrenheitResult>
7     </CelsiusToFahrenheitResponse>
8   </soap:Body>
9 </soap:Envelope>

```

Figure3.80: Pattern Integrity - Fruizione API SOAP, esecuzione da Postman

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”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*.

Conformità ai requisiti ModI

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

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione
Soggetto: Ente ▾
Profilo: ModI ▾
⚙️

Figure3.81: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con le sole differenze dovute al differente pattern di sicurezza utilizzato «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01».

Registrazione API

Viene registrata l'API «TemperatureConversionIntegrity» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_02» (sicurezza canale) e «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» (Fig. 3.82).

API > TemperatureConversionIntegrity v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_02

Direct Trust mutual Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01

Integrità payload del messaggio

Applicabilità: Richiesta e Risposta

Digest Richiesta: Non ripudiabilità della trasmissione (i)

Informazioni Utente: Dati dell'utente che effettua la richiesta (i)

Figure3.82: Configurazione Pattern ModI «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» sulla API SOAP

Fruizione

Si registra la fruizione SOAP “TempConvertSoapIntegrity”, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.83).

La sezione «ModI Risposta» definisce i criteri per la validazione dei messaggi di risposta (Fig. 3.84).

Modi - Richiesta

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	Definito nell'applicativo
Time to Live (secondi) *	60

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

WSAddressing To 

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

Figure3.83: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

TrustStore Certificati	Default
Time to Live	Default

Verifica WSAddressing To La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente



Figure3.84: Configurazione risposta della fruizione

3.3 Pattern “ID_AUTH” via PDND

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_pdnd.

3.3.1 Erogazione API REST

Obiettivo

Esporre un servizio, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd.

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio.

La figura seguente descrive graficamente questo scenario.

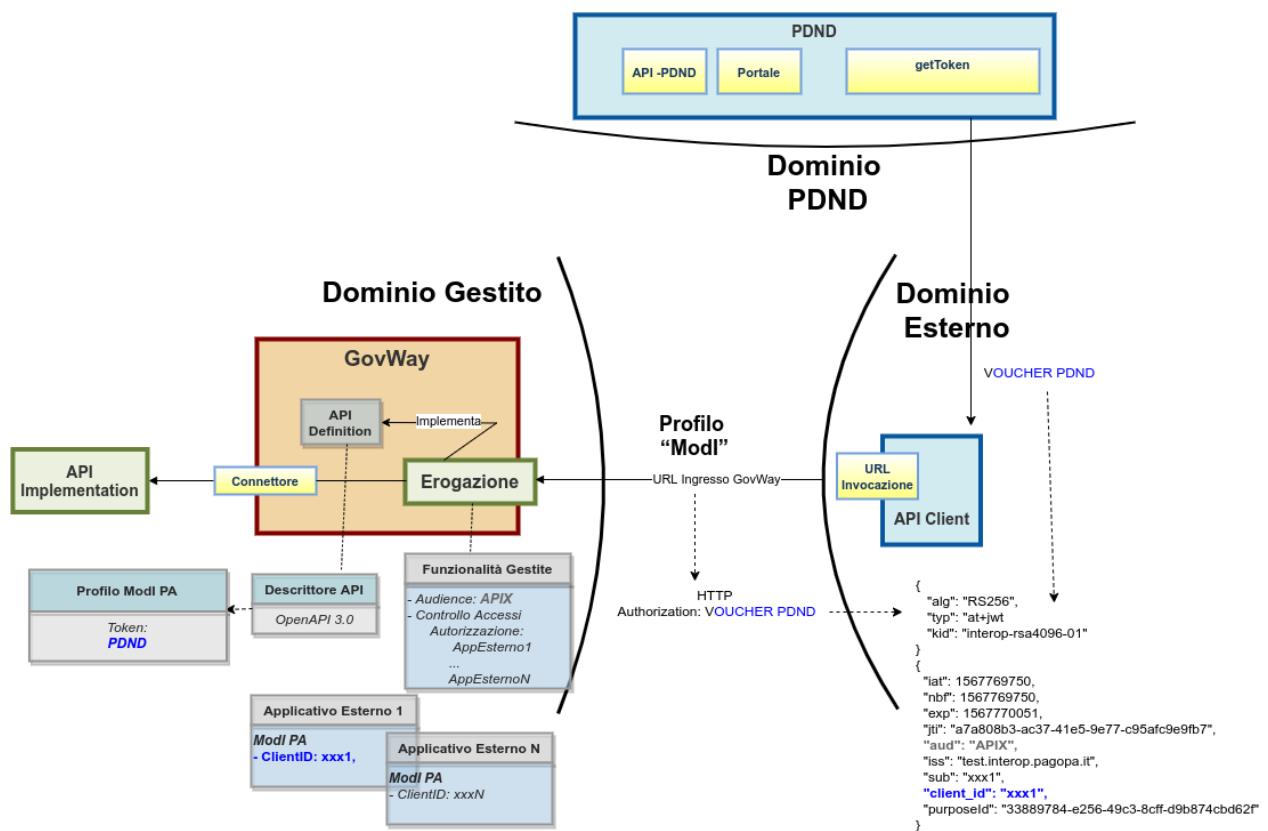


Figure3.85: Erogazione di una API REST con profilo “Modi”, pattern ID_AUTH_REST_01 via PDND

Le caratteristiche principali di questo scenario sono:

1. un applicativo eroga un servizio, rivolto a fruitori di domini esterni, registrandolo sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.86: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API REST di esempio (PetStore) definita con pattern di interazione “CRUD” e pattern di sicurezza «ID_AUTH_CHANNEL_01» e «ID_AUTH_REST_01 via PDND»;
- un'istanza Govway per la gestione del profilo ModI nel dominio dell'erogatore;
- un'authorization server che simula la PDND;
- un client del dominio esterno che invoca la risorsa «POST /pet» dell'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 «Profilo ModI REST - IDAuth+PDND - IN App1» che è stata preconfigurata 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. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.88. Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali ««Authorization», che contiene il token di sicurezza che il fruitore ha ottenuto dalla PDND.
2. Grazie alle configurazioni presenti nell'erogazione, ed in particolare all'indicazione che il token ricevuto deve essere validato tramite Token Policy PDND, GovWay è in grado di validare i dati di sicurezza ricevuti (Fig. 3.89) e decodificare il token.
3. Analizzando il token ricevuto nella sezione header (Fig. 3.90) si può notare che non viene riportata l'identità del fruitore tramite certificato X.509 come avveniva per il pattern ID_AUTH_REST_01 descritto nella scenario *Esecuzione*. L'identità del fruitore è presente nella sezione payload (Fig. 3.91) all'interno del claim *client_id*, insieme ai riferimenti temporali (iat, nbf, exp) e all'audience (aud). Da notare inoltre la presenza del claim “purposeId” che indica la finalità per cui il fruitore sta fruendo del servizio.

Nota

Il token ritornato dall'authorization server demo che simula la PDND contiene ulteriori claims che possono essere ignorati poiché non utili alla descrizione dello scenario e non presenti in un token PDND reale.

4. Il messaggio ricevuto dal Govway viene quindi validato, sulla base della configurazione realizzata, verificando in questo caso l'identità del fruitore, la validità temporale, la corrispondenza dell'audience ricevuto con quello atteso. Solo in caso di superamento dell'intero processo di validazione, il messaggio viene inoltrato al servizio erogatore. Se

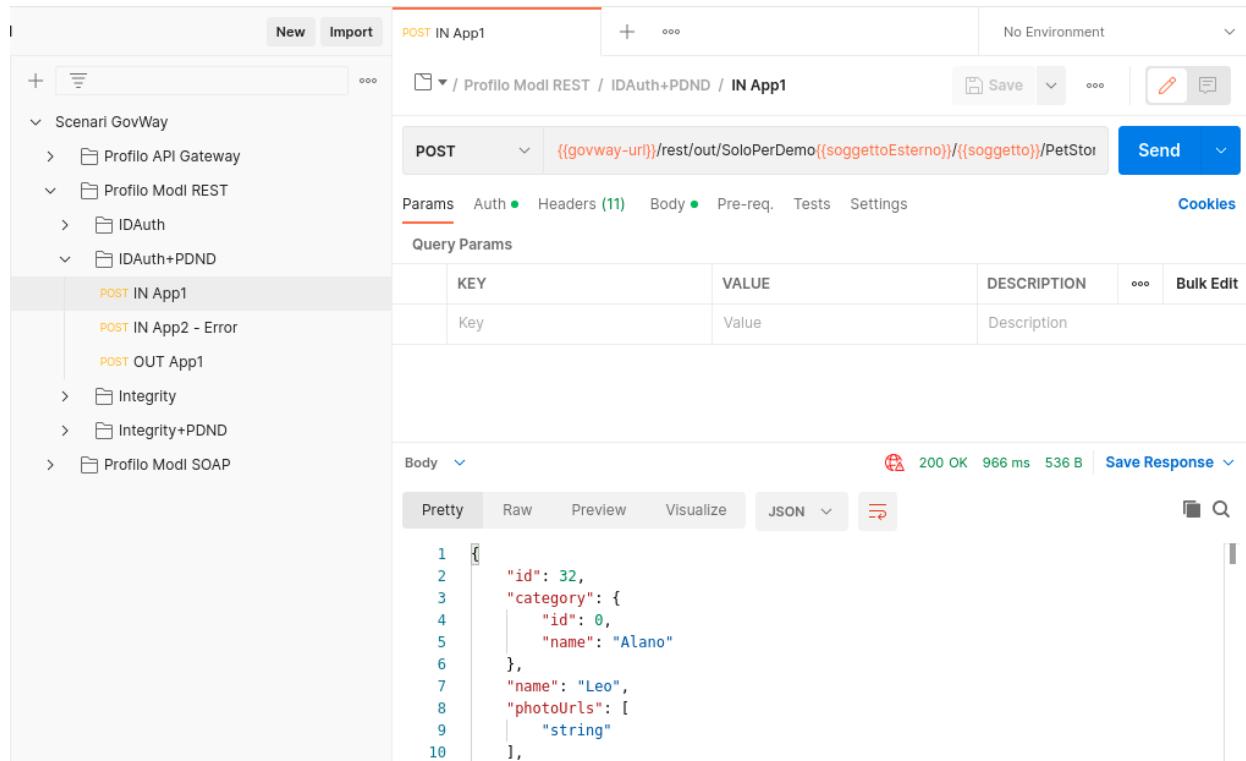


Figure3.87: Pattern IDAuth+PDND - Erogazione API REST, esecuzione da Postman

il processo di validazione del token ha successo è possibile consultare i dati interni al token ricevuto tramite la console come mostrato nelle figure [Fig. 3.92](#) e [Fig. 3.93](#).

5. Esaminando il messaggio inoltrato al backend è possibile vedere come tra gli header HTTP inoltrati vi sia l'header “GovWay-Token-PurposeId” contenente il valore del claim “purposeId” presente nel token ricevuto dalla PDND ([Fig. 3.94](#)).
6. Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al claim “client_id” presente all'interno del token. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IDAuth+PDND - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

Conformità ai requisiti ModI

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

1. la sicurezza messaggio applicata è quella dei pattern «ID_AUTH_REST_01 via PDND» come ampiamente mostrato precedentemente dove sono stati mostrati i token validati e i criteri autorizzativi;
2. l'identificazione del fruitore avviene rispetto al claim “client_id” presente all'interno del token. È stato anche mostrato come sia possibile configurare criteri autorizzativi puntuali.

Configurazione

Nota

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”. Si suggerisce

Headers	
Nome	
Content-Type	application/json
X-Message-Id	1f46c4b4-4f9b-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	cde738cd-acfc-4785-a59a-eb751595a001
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZC16ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9y h2UWZlHrQDLuBSuHsJQWfc2Wp16rbtLvxMqKSONk6lxmWknBch1hXBwzeTmPAkNHcDoYpqhmdR
X-Forwarded-Port	443
Pragma	no-cache
Accept-Encoding	gzip, deflate, br

Figure3.88: Messaggio inviato dal fruttore

2022-10-20 11:06:27.473	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) in corso ...
2022-10-20 11:06:27.474	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) completata con successo

Figure3.89: Evidenza diagnostica della validazione del token

HEADER: ALGORITHM & TOKEN TYPE
<pre>{ "typ": "at+jwt", "alg": "RS256", "use": "sig", "kid": "interop-rsa4096-01" }</pre>

Figure3.90: Sezione «Header» del Token PDND

```
PAYOUT: DATA

{
  "aud": "PetStore",
  "sub": "App1-Esterno-PDND",
  "client_id": "App1-Esterno-PDND",
  "purposeId": "54806042-5e7f-4c70-9ee0-a4f100a079f7",
  "iss": "test.interop.pagopa.it",
  "exp": 1666258251,
  "iat": 1666257651,
  "nbf": 1666257651,
  "jti": "32c30a37-ed2e-4a50-a42e-0093b50773dc"
}
```

Figure3.91: Sezione «Payload» del Token PDND

Transazioni > Ricerca Base > **Dettagli Transazione**

Dettagli Transazione

Informazioni Generali Informazioni Mittente Dettagli Messaggio Diagnostici Informazioni Avanzate

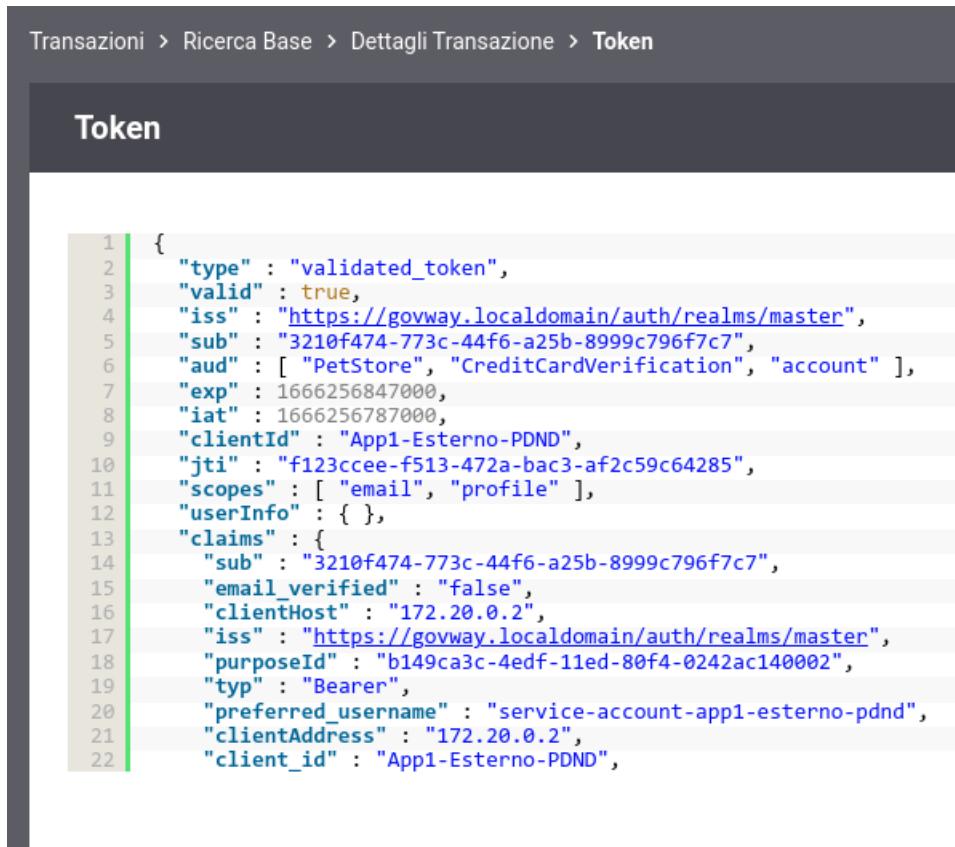
Informazioni Mittente

Fruitore EnteEsterno
Applicativo Fruitore App1-PDND
ID Autenticato /o=govway.org/c=it/cn=enteEsterno.govway.org/
Metodo HTTP POST
URL Invocazione [in] /govway/rest/in/Ente/PetStoreAuthPDND/v1/pet
Client IP 172.20.0.2
X-Forwarded-For 172.20.0.2
Codice Risposta Client 200

Token

Issuer https://govway.localdomain/auth/realm/master
Subject 3210f474-773c-44f6-a25b-8999c796f7c7
Client ID App1-Esterno-PDND
Applicativo Client App1-PDND
Token [Visualizza](#)

Figure3.92: Dati principali presenti nel Token PDND



```

1  {
2    "type" : "validated_token",
3    "valid" : true,
4    "iss" : "https://govway.locaLdomain/auth/realmS/master",
5    "sub" : "3210f474-773c-44f6-a25b-8999c796f7c7",
6    "aud" : [ "PetStore", "CreditCardVerification", "account" ],
7    "exp" : 1666256847000,
8    "iat" : 1666256787000,
9    "clientId" : "App1-Esterno-PDND",
10   "jti" : "f123ccee-f513-472a-bac3-af2c59c64285",
11   "scopes" : [ "email", "profile" ],
12   "userInfo" : { },
13   "claims" : {
14     "sub" : "3210f474-773c-44f6-a25b-8999c796f7c7",
15     "email_verified" : "false",
16     "clientHost" : "172.20.0.2",
17     "iss" : "https://govway.locaLdomain/auth/realmS/master",
18     "purposeId" : "b149ca3c-4edf-11ed-80f4-0242ac140002",
19     "typ" : "Bearer",
20     "preferred_username" : "service-account-app1-esterno-pdnd",
21     "clientAddress" : "172.20.0.2",
22     "client_id" : "App1-Esterno-PDND",

```

Figure3.93: Claim presenti nel Token PDND

Headers	
Nome	Valore
X-Real-Ip	172.20.0.1
GovWay-Token-ClientId	App1-Esterno-PDND
GovWay-Token-Audience	PetStore,CreditCardVerification,account
GovWay-Sender	EnteEsterno
Cache-Control	no-cache
GovWay-Application	App1-PDND
GovWay-Token-Jti	51bb4e16-1592-43a4-a263-070ed8a58241
GovWay-Token-Issuer	https://govway.locaLdomain/auth/realmS/master
GovWay-Transaction-ID	cba1b693-5072-11ed-a5ac-0242ac140002
Content-Type	application/json
GovWay-Token-PurposeId	b149ca3c-4edf-11ed-80f4-0242ac140002
User-Agent	GovWay
GovWay-Token-Application	App1-PDND

Figure3.94: Header HTTP “GovWay-Token-PurposeId” inoltrato al backend

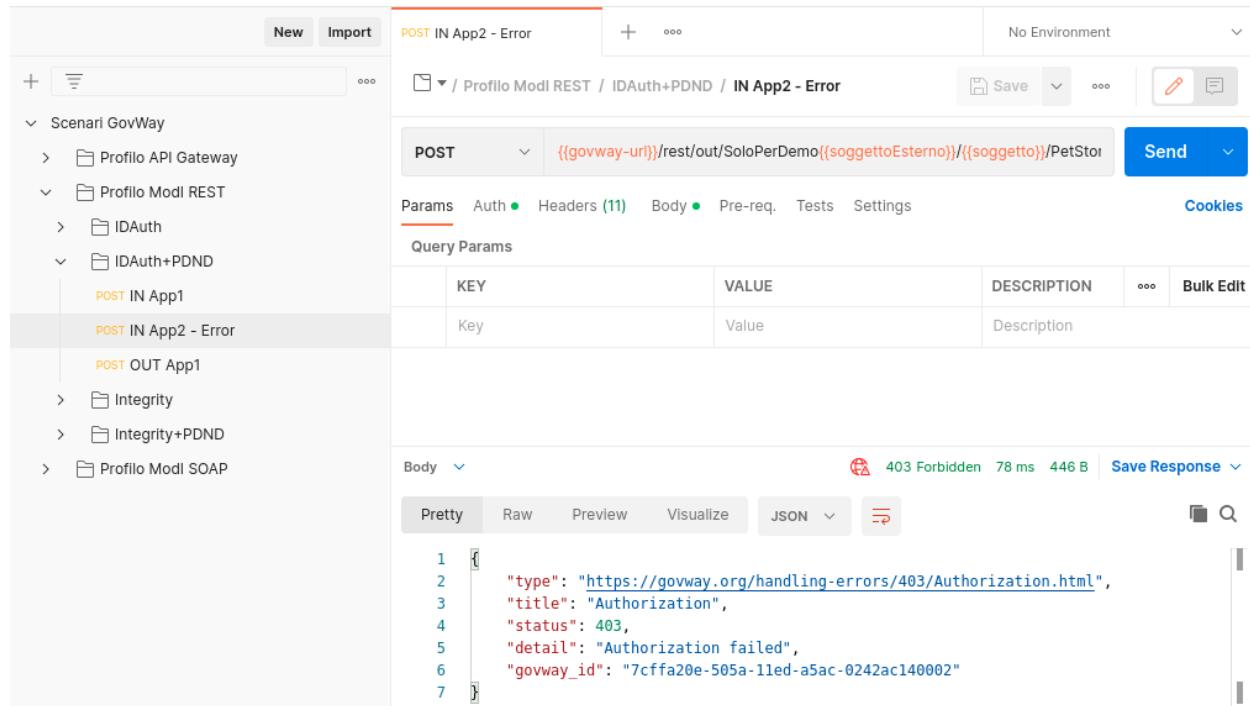


Figure3.95: Pattern IDAuth+PDND - Erogazione API REST - Autorizzazione negata, esecuzione da Postman

inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.96: Profilo ModI della govwayConsole

Registrazione API

Viene registrata l’API «PetStoreAuthPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.97).

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 si desidera autorizzare qualsiasi fruitore proveniente dalla PDND, questo passo può anche essere omesso. La validazione del token è sufficiente a stabilire che il fruitore ha ottenuto un voucher dalla PDND valido per il servizio invocato.
- In alternativa è possibile configurare una autorizzazione puntuale procedendo alla registrazione degli applicativi fornendo i singoli “client_id” necessari all’identificazione (Fig. 3.98). Questo scenario è quello preconfigurato.

Token Policy PDND

Con il prodotto viene fornita built-in la token policy “PDND” (Fig. 3.99) da finalizzare nella sezione “TrustStore”,

API > PetStoreAuthPDND v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern ▼
Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern ▼
Direct Trust con certificato X.509

Generazione Token ▼
Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Figure3.97: Configurazione Pattern ModI con «ID_AUTH_CHANNEL_01» senza sicurezza messaggio

Applicativo

Profilo Interoperabilità	Modl
Dominio	Esterno
Soggetto	EnteEsterno
Nome *	<input type="text" value="App1-PDND"/>
Tipo	Client
<u>Proprietà(0)</u>	

Ruoli

visualizza(0)

Modi

Sicurezza Messaggio	<input type="text" value="Authorization PDND"/>
ClientId registrato sulla PDND	
Token Policy *	<input type="text" value="PDND"/>
Identificativo *	<input type="text" value="App1-Esterno-PDND"/>

Figure3.98: Configurazione applicativo esterno (fruitore)

come descritto nel manuale “Console di Gestione” nella sezione modipa_passiPreliminari_trustStore_pdnd. La configurazione utilizzata per gli scenari (Fig. 3.100) simula la PDND tramite i certificati predisposti su “Keycloak”:

- File: deve essere indicato un path su file system che contiene il certificato di firma della PDND ottenibile tramite la url “`.../.well-known/jwks.json`” fornita dalla PDND stessa;
- Alias Certificato: deve contenere l’alias (il kid) della chiave pubblica utilizzata dalla PDND per firmare i token rilasciati, corrispondente al valore del claim “`kid`” presente nel JWKSet configurato al punto precedente;
- Token Forward: deve essere eventualmente configurata la modalità di forward delle informazioni presenti nel token verso il backend, utile nel nostro scenario per far arrivare il valore del claim “`purposeId`” al backend nell’header HTTP “`GovWay-Token-PurposeId`”.

Token Policy > PDND

PDND

Note: (*) Campi obbligatori

Token Policy

Tipo	Validazione
Nome	PDND
Descrizione	

Informazioni Generali

Token

Posizione	JWS
Validazione	RFC 6750 - Bearer Token Usage

Elaborazione Token

Validation JWT	<input checked="" type="checkbox"/>
Token Introspection	<input type="checkbox"/>
OIDC - UserInfo	<input type="checkbox"/>
Token Forward	<input checked="" type="checkbox"/>

Figure3.99: Token Policy PDND (Dati Generali)

Erogazione

Si registra l’erogazione «`PetStoreAuthPDND`», relativa all’API precedentemente inserita, abilitando la validazione del token ricevuto dalla PDND tramite la omonima policy (Fig. 3.101).

Si può notare nella sezione “Autenticazione Canale” del Controllo degli Accessi come l’autenticazione https sia opzionale per essere aderenti al pattern di sicurezza canale «`ID_AUTH_CHANNEL_01`» (Fig. 3.102).

Nella sezione “Autorizzazione” si può invece vedere come nella voce “Autorizzazione per Token Claims” vi sia configurato il valore del claim “`aud`” atteso.

Figure3.100: Token Policy PDND (Aspetti da Configurare)

Se si è scelto inoltre di registrare gli applicativi esterni, fruitori del servizio, saranno specificati i singoli applicativi fruitori autorizzati ad effettuare richieste al servizio erogato. Questo scenario è quello preconfigurato come mostrato nelle figure Fig. 3.103 e Fig. 3.104.

3.3.2 Fruizione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio.

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 registrata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND».

Erogazioni > PetStoreAuthPDND v1 (Ente) > Configurazione > **Controllo Accessi**

Controllo Accessi

Note: (*) Campi obbligatori

^ Autenticazione Token

Policy *	PDND
Validazione JWT	abilitato
Token Forward	abilitato

Required Claims

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

Figure3.101: Controllo degli Accessi - Autenticazione Token

^ Autenticazione Canale

Stato	https
Opzionale	<input checked="" type="checkbox"/>

Figure3.102: Controllo degli Accessi - Autenticazione Canale

Autorizzazione

Stato

Autorizzazione Canale

per Richiedente

per Ruoli

Autorizzazione Messaggio

per Richiedente

Applicativi (1)

per Ruoli

Autorizzazione per Token Claims

Abilitato

Claims

Indicare per riga i claims richiesti (nome=valore); visualizzare 'info' per maggiori dettagli

Figure3.103: Controllo accessi con autorizzazione dell'audience e degli applicativi esterni

Erogazioni > PetStoreAuthPDND v1 (Ente) > Configurazione > Controllo Accessi > **Autorizzazione Messaggio - Applicativi**

Autorizzazione Messaggio - Applicativi

Visualizzati record [1-1] su 1

<input type="checkbox"/>	Soggetto	Applicativo	<input type="checkbox"/>
<input type="checkbox"/>	EnteEsterno	App1-PDND	<input type="checkbox"/>

Figure3.104: Lista degli applicativi esterni autorizzati

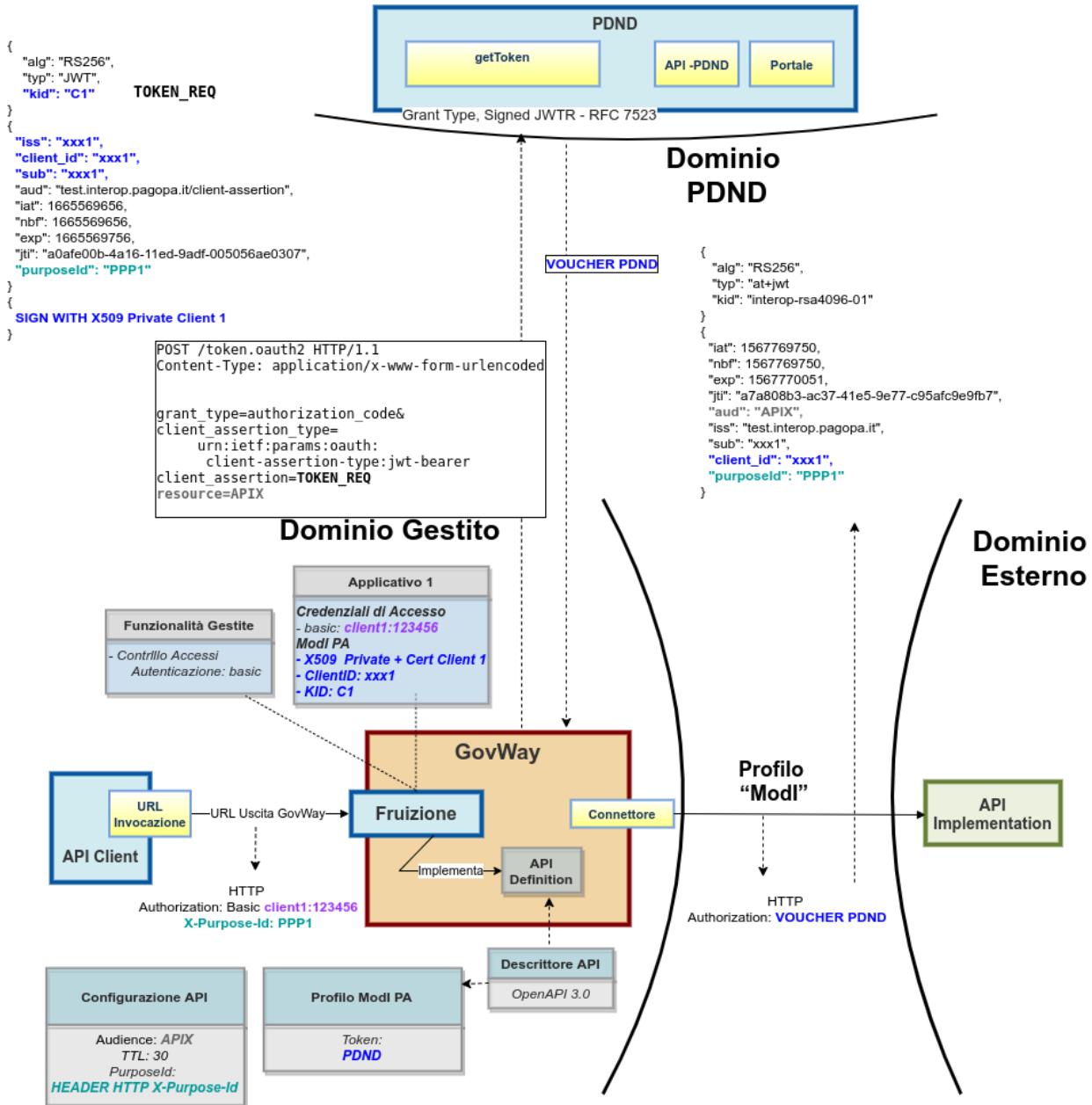


Figure3.105: Fruizione di una API REST con profilo "Modi", pattern ID_AUTH_REST_01 via PDND

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.106: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API REST di esempio (PetStore) definita con pattern di interazione “CRUD” e pattern di sicurezza «ID_AUTH_CHANNEL_01» e «ID_AUTH_REST_01 via PDND»;
- un'istanza Govway per la gestione del profilo ModI nel dominio del fruitore;
- un'authorization server che simula la PDND;
- un client che invoca la risorsa «POST /pet» con un messaggio di esempio diretto alla fruizione configurata su Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IDAuth+PDND - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

The screenshot shows the Postman interface with the following details:

- Request URL:** {{govway-url}}/rest/out/{{soggetto}}/{{soggettoEsterno}}/PetStoreAuthPDND/
- Method:** POST
- Params:** Query Params (Key: Key, Value: Value, Description: Description)
- Body:** JSON (Pretty, Raw, Preview, Visualize, JSON, JSONP, XML, YAML, Text, Form, Binary, Form Data, URL Encoded, URL Encoded Data, Form Data (Multipart), Form Data (Multipart), Form Data (Multipart))
- Response:** 200 OK 931 ms 536 B (Save Response)

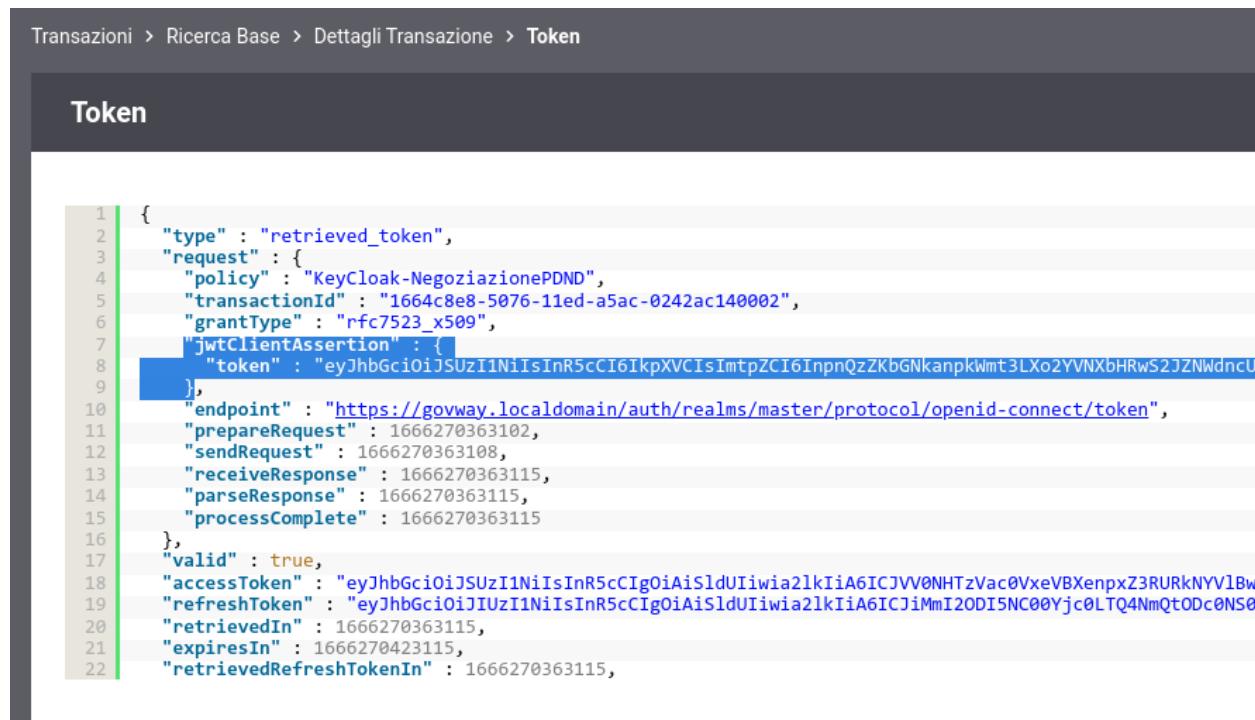
```

1  [
2      "id": 32,
3      "category": {
4          "id": 0,
5          "name": "Alano"
6      },
7      "name": "Leo",
8      "photoUrls": [
9          "string"
10     ],
11 ]
  
```

Figure3.107: Pattern IDAuth+PDND - Fruizione API REST, esecuzione da Postman

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 la console “govwayMonitor”.

- 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 un token di sicurezza da inviare alla PDND con il quale ottenere indietro un voucher spendibile per il servizio desiderato. Tramite la console è possibile esaminare sia l'asserzione JWT inviata alla PDND (Fig. 3.108) che l'access token ottenuto dalla PDND (Fig. 3.109).



```

1  {
2   "type" : "retrieved_token",
3   "request" : {
4     "policy" : "KeyCloak-NegoziazionePDND",
5     "transactionId" : "1664c8e8-5076-11ed-a5ac-0242ac140002",
6     "grantType" : "rfc7523_x509",
7     "jwtClientAssertion" : [
8       "token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InpnQzzKbGNkanpkWimt3LXo2YVNxbHRwS2JZNwdncU
9     ],
10    "endpoint" : "https://govway.localdomain/auth/realm/master/protocol/openid-connect/token",
11    "prepareRequest" : 1666270363102,
12    "sendRequest" : 1666270363108,
13    "receiveResponse" : 1666270363115,
14    "parseResponse" : 1666270363115,
15    "processComplete" : 1666270363115
16  },
17  "valid" : true,
18  "accessToken" : "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJV0NHTzVac0VxeVBXenpxZ3RURkNYVlBw
19  "refreshToken" : "eyJhbGciOiJIUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJiMmI2ODI5NC00Yjc0LTQ4NmQtODc0NS0
20  "retrievedIn" : 1666270363115,
21  "expiresIn" : 1666270423115,
22  "retrievedRefreshTokenIn" : 1666270363115,

```

Figure3.108: Evidenza dell'asserzione JWT inviata alla PDND

- Esaminando l'header e il payload dell'asserzione JWT inviata alla PDND (Fig. 3.110) si può notare:
 - Valore del claim “kid” associato all'applicativo mittente in configurazione
 - Valore del claim “client_id” (uguale per i claim “sub” e “iss”) associato all'applicativo mittente in configurazione
 - Valore del claim “purposeId” indicato dal client (nell'esempio Postman) tramite un header http “X-Purpose-Id”
- Analizzando l'access token ricevuto dalla PDND, nella sezione header (Fig. 3.111) si può notare che non viene riportata l'identità del fruitore tramite certificato X.509 come avveniva per il pattern ID_AUTH_REST_01 descritto nella scenario *Esecuzione*. L'identità del fruitore è presente nella sezione payload (Fig. 3.112) all'interno del claim *client_id*, insieme ai riferimenti temporali (iat, nbf, exp) e all'audience (aud) del servizio per cui si è richiesto il voucher. Da notare inoltre la presenza del claim “purposedId” che servirà ad indicare la finalità per cui il fruitore sta fruendo del servizio all'erogatore.

Nota

Il token ritornato dall'authorization server demo che simula la PDND contiene ulteriori claims che possono essere ignorati poiché non utili alla descrizione dello scenario e non presenti in un token PDND reale.

- Tramite la console 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 l'access token ottenuto dalla PDND tra gli header HTTP all'interno dell'header «Authorization» (Fig. 3.113).

Transazioni > Ricerca Base > Dettagli Transazione > **Token**

Token

```

1  {
2    "type" : "retrieved_token",
3    "request" : {
4      "policy" : "Keycloak-NegoziazionePDND",
5      "transactionId" : "1664c8e8-5076-11ed-a5ac-0242ac140002",
6      "grantType" : "rfc7523_x509",
7      "jwtClientAssertion" : {
8        "token" : "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InpnQzZKbGNkanpkWmt3LXo2YVNxbHRwS2JZNWdncU1Ub3p3aFFjN0",
9      },
10     "endpoint" : "https://govway.localdomain/auth/realm/master/protocol/openid-connect/token",
11     "prepareRequest" : 1666270363102,
12     "sendRequest" : 1666270363108,
13     "receiveResponse" : 1666270363115,
14     "parseResponse" : 1666270363115,
15     "processComplete" : 1666270363115
16   },
17   "valid" : true,
18   "accessToken" : "eyJhbGciOiJSUzI1NiIsInR5cCIg0IAiSldUiIwia2IkIIA6ICJV0NHTzVac0VxeVBXenpxZ3RURkNYV1BwWWRYRjhmeFZhi",
19   "refreshToken" : "eyJhbGciOiJIUzI1NiIsInR5cCIg0IAiSldUiIwia2IkIIA6ICJiMmI2ODI5NC00Yjc0LTQ4NmQtODc0NS02N2VkMDFlyTNI",
20   "retrievedIn" : 1666270363115,
21   "expiresIn" : 1666270423115,
22   "retrievedRefreshTokenIn" : 1666270363115,

```

Figure3.109: Evidenza dell'access token ottenuto dalla PDND

HEADER: ALGORITHM & TOKEN TYPE
<pre> { "alg": "RS256", "typ": "JWT", "kid": "zgO6JlcjdZkw-z6aSW1tpKbY5ggqMTozwhQc7FUSM" } </pre>
PAYLOAD: DATA
<pre> { "iss": "App1-PDND", "client_id": "App1-PDND", "sub": "App1-PDND", "aud": "https://govway.localdomain/auth/realm/master", "iat": 1666270363, "nbf": 1666270363, "exp": 1666270663, "jti": "1664c8e8-5076-11ed-a5ac-0242ac140002", "purposeId": "b149ca3c-4edf-11ed-80f4-0242ac140002" } </pre>

Figure3.110: Header e Payload dell'asserzione JWT inviata alla PDND

```
HEADER: ALGORITHM & TOKEN TYPE

{
  "typ": "at+jwt",
  "alg": "RS256",
  "use": "sig",
  "kid": "interop-rsa4096-01"
}
```

Figure3.111: Sezione «Header» del Token PDND

```
PAYLOAD: DATA

{
  "aud": "PetStore",
  "sub": "App1-Esterno-PDND",
  "client_id": "App1-Esterno-PDND",
  "purposeId": "54806042-5e7f-4c70-9ee0-a4f100a079f7",
  "iss": "test.interop.pagopa.it",
  "exp": 1666258251,
  "iat": 1666257651,
  "nbf": 1666257651,
  "jti": "32c30a37-ed2e-4a50-a42e-0093b50773dc"
}
```

Figure3.112: Sezione «Payload» del Token PDND

5. Govway riceve la risposta dell’erogatore grazie al fatto che ha inviato un voucher PDND correttamente validato dall’erogatore.

Conformità ai requisiti ModI

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

1. viene effettuata una negoziazione del voucher PDND come mostrato nelle tracce relative ai token scambiati con la PDND;
2. l’invocazione del servizio avviene fornendo il voucher della PDND precedentemente negoziato.

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.114: Profilo ModI della govwayConsole

Headers	
Nome	
Content-Type	application/json
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
X-Forwarded-Port	443
Accept-Encoding	gzip, deflate, br
Postman-Token	d924391e-10cd-4c75-8063-4cbfaa74639a
User-Agent	GovWay
Accept	*/*
GovWay-Message-ID	5ade2322-4fac-11ed-a5ac-0242ac140002
GovWay-Transaction-ID	5acd8134-4fac-11ed-a5ac-0242ac140002
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCI6ImFwcDEuZW50ZS5nb3Z3YXkub3JrWyISJxWAFBE4zpeb4JpJRwmafmwJLqddHy7j8bMjGx9x3IG0ws6AhiTAKaK2HPGbpD

Figure3.113: Messaggio di richiesta in uscita (con voucher PDND inserito nell'header HTTP)

Registrazione API

Viene registrata l'API «PetStoreAuthPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.97).

Figure3.115: Configurazione Pattern ModI con «ID_AUTH_CHANNEL_01» senza sicurezza messaggio

Applicativo

Si configura l'applicativo mittente indicando, nella sezione ModI, i parametri del keystore e i parametri di identificazione sulla PDND necessari affinché Govway possa produrre il token di sicurezza firmando per conto dell'applicativo (Fig. 3.116 e Fig. 3.117). Alla registrazione dell'applicativo vengono associate credenziali “basic” che consentono a GovWay di identificarlo.

Token Policy PDND

Per la configurazione delle fruizioni con un pattern di sicurezza via PDND è necessario registrare una Token Policy di Negoziazione del tipo descritto nella sezione “tokenNegoziazionePolicy_pdnd”.

Una volta effettuata la registrazione della Token Policy, per utilizzarla in una fruizione è sufficiente associarla al connettore della fruizione come descritto nella sezione avanzate_connatori_tokenPolicy.

Di seguito vengono riportate tutte le informazioni più importanti della policy:

- Tipo: SignedJWT;

Applicativo

Dominio	Interno
Soggetto	Ente
Nome *	<input type="text" value="App1-PDND"/>
Tipo	Client
Proprietà(0)	

Modalità di Accesso

Tipo	<input type="text" value="http-basic"/>
Utente *	<input type="text" value="App1-PDND.Ente"/>
Modifica Password	<input type="checkbox"/>

Figure3.116: Configurazione applicativo fruitore (Dati Generali)

- PDND: flag attivato;
- URL: endpoint esposto dalla PDND su cui è possibile richiedere lo stacco del voucher;
- JWT Keystore: parametri di accesso al keystore contenente la chiave privata corrispondente alla chiave pubblica caricata sulla PDND durante la registrazione dell'applicativo client. I parametri variano in funzione del tipo di keystore selezionato e nello scenario preconfigurato è stata scelta la modalità “Definito nell'applicativo ModI” nella quale il keystore utilizzato per firmare l'asserzione JWT inviata alla PDND sarà quello definito nell'applicativo ModI richiedente (Fig. 3.119).

Nota

Questa modalità consente di definire un'unica TokenPolicy di negoziazione utilizzabile da più applicativi richiedenti ognuno configurato con la propria coppia di chiavi di firma e i relativi identificativi “client_id” e “kid”.

- JWT Signature: algoritmo di firma
- JWT Header:
 - Type (typ): lasciare il valore “JWT”;
 - Key Id (kid): deve essere indicato l'identificativo univoco (KID) associato al certificato caricato sulla PDND e ottenuto al termine della registrazione dell'applicativo client. Può essere fornito tramite differenti modalità e nello scenario preconfigurato è stata scelta la modalità “Definito nell'applicativo ModI” nella quale il valore del KID viene configurato sull'applicativo richiedente (Fig. 3.119).
- JWT Payload:

l'identificativo univoco dell'applicativo client (“client_id” o “sub”) ottenuto al termine della registrazione dell'applicativo sulla PDND deve essere indicato nei seguenti campi:

 - Client ID

Modi - Sicurezza Messaggio

KeyStore

Abilitato	<input checked="" type="checkbox"/>
Modalità	File System
Path *	/etc/govway/keys/keystore_app1.ente.pkcs12
Tipo	PKCS12
Password *	123456
Alias Chiave Privata *	app1.ente.govway.org
Password Chiave Privata *	123456
Certificato	<input type="button" value="Choose File"/> No file chosen

Authorization ModI

Identificativo Client	<input type="text"/>	<small>(i)</small>
Identificativo dell'applicativo scambiato nei token di sicurezza		
URL (x5u)	<input type="text"/>	<small>(i)</small>
URL che riferisce un certificato (o certificate chain) X.509 corrispondente alla chiave firmataria del security token		

Authorization OAuth

Abilitato	<input checked="" type="checkbox"/>
Token Policy di Validazione	<input type="text" value="-"/>
<small>!!Attenzione!! Per consentire un'identificazione dell'applicativo su API erogate da altri soggetti di dominio interno selezionare una token policy.</small>	
Identificativo *	<input type="text" value="App1-PDND"/>
Key Id (kid) del Certificato	<input type="text" value="zgC6JlcjdZkw-z6aSWltpKbY5ggqMTozwhQc7FU5M"/>

Figure3.117: Configurazione applicativo fruitore (Configurazione Modi)

Token Policy > Keycloak-NegoziazionePDND

Keycloak-NegoziazionePDND

Note: (*) Campi obbligatori

Token Policy

Tipo: Negoziazione
Nome: Keycloak-NegoziazionePDND
Descrizione:

Token Endpoint

Tipo: Signed JWT
PDND:
URL: ⓘ
Connection Timeout: 5000
Read Timeout: 10000
Https:
Proxy:

Figure3.118: Token Policy di Negoziazione PDND (Endpoint)

JWT KeyStore

Tipo: Definito nell'applicativo ModI

JWT Signature

Signature Algorithm: RS256

JWT Header

Key Id (kid): Definito nell'applicativo ModI
X.509 Certificate: -
Digest X.509 Certificate: -
Type (typ): * JWT
Content Type (cty):

Figure3.119: Token Policy di Negoziazione PDND (Keystore definito nell'applicativo ModI)

- Issuer
 - Subject

Nello scenario preconfigurato è stato però scelta la modalità alternativa in cui il ClientID ottenuto dalla PDND deve essere configurato sull'applicativo richiedente e la token policy viene configurata per utilizzare tale valore (Fig. 3.120).

Gli altri campi presenti nella sezione “JWT Payload” rappresentano (Fig. 3.120):

- Audience: indica il servizio di stacco del voucher della PDND. Il valore, fornito dalla PDND, è indipendente dal servizio per cui si vuole richiedere un voucher e varia solamente in funzione dell’ambiente di validazione o produzione della PDND stessa;
 - Identifier: consente di configurare la modalità di valorizzazione del claim “`“jti”`” presente all’interno del token di richiesta inviato alla PDND. Si suggerisce di valorizzare il campo con la keyword “`“${transaction:id}”`” al fine di utilizzare l’identificativo di transazione della richiesta;
 - Time to Live (secondi): consente di indicare la durata del token di richiesta inviato alla PDND (es. 100 sec);
 - Purpose ID: identificativo univoco della finalità per cui si intende fruire di un servizio. Il valore può essere fornito staticamente o può contenere una keyword risolta a runtime in modo da valorizzare il claim `“purposeId”` con un valore prelevato dai dati della richiesta o dalla configurazione della fruizione. Nello scenario preconfigurato il `“purposeId”` viene indicato dall’applicativo richiedente tramite l’header HTTP “`“X-Purpose-Id”`”.
 - Informazioni Sessione: consente di valorizzare il claim “`“sessionInfo”`” previsto dalla PDND. La valorizzazione può essere statica o formata da parti dinamiche risolte a runtime dal Gateway (per maggiori dettagli `“valoriDinamici”`).

JWT Payload

Client ID	Definito nell'applicativo Mod1	
Issuer	ClientID dell'applicativo Mod1	
Subject	ClientID dell'applicativo Mod1	
Audience *	<code>https://govway.localdomain/auth/realm/master</code>	
Identifier	<code>#{transaction:id}</code>	
Time to Live (secondi) *	300	
Indica la validità temporale, in secondi, a partire dalla data di creazione dell'asserzione		
Purpose ID *	<code>#{header:X-Purpose-Id}</code>	
Informazioni Sessione		
Indicare per riga i claims (nome=valore) da aggiungere nell'oggetto 'sessionInfo'		
Claims		
Indicare per riga gli ulteriori claims (nome=valore)		

Figure3.120: Token Policy di Negoziazione PDND (JWT Payload)

- Dati Richiesta:

- Resource: indica l’audience/url del servizio per cui si vuole richiedere un voucher; nello scenario preconfigurato il valore viene preso dalla proprietà “PDND-resource” della fruizione configurata.
- Client ID: deve essere indicato il medesimo valore inserito nel campo “Client ID” della sezione “JWT Payload”; nello scenario preconfigurato viene infatti utilizzato il valore configurato sull’applicativo richiedente.

Dati Richiesta

Scope	<input type="text"/>	i
Elencare più scope separandoli con la virgola		
Audience	<input type="text"/>	i
Client ID	<input type="text" value="ClientID dell’applicativo Mod1"/>	i
Resource	<input type="text" value="\${config:PDND-resource}"/>	i
Parametri	<input type="text"/>	
Indicare per riga gli ulteriori parametri (nome=valore)		

Figure3.121: Token Policy di Negoziazione PDND (Dati Richiesta)

Fruizione

Si registra la fruizione «PetStoreAuthPDND», relativa all’API precedentemente inserita, indicando l’utilizzo della token policy di negoziazione sul connettore (Fig. 3.122).

Tra le proprietà della fruizione viene definita la proprietà “PDND-resource” contenente il valore da inserire nella richiesta di voucher effettuata alla PDND che identifica il servizio di cui si sta richiedendo il token (Fig. 3.123).

3.3.3 Erogazione API SOAP

Obiettivo

Esporre un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd.

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all’erogatore insieme alla normale richiesta di servizio.

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, registrandolo sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l’autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND».

Fruizioni > PetStoreAuthPDND@EnteEsterno v1 > Connettore

Connettore

Note: (*) Campi obbligatori

Connettore

Endpoint *	<input type="text" value="https://govway.localdomain/govway/rest/SoloPerDemoEnteEsterno/PetStoreAuthPDND/v1"/>	
Autenticazione Token	Negoziazione Token tramite PDND	
Autenticazione Https	<input checked="" type="checkbox"/>	
Proxy	<input type="checkbox"/>	
Ridefinisci Tempi Risposta	<input type="checkbox"/>	

Autenticazione Token

Policy *	<input type="text" value="Keycloak-NegoziatorePDND"/>	
----------	---	--

Figure3.122: Associazione della Token Policy di Negoziazione al connettore

Fruizioni > PetStoreAuthPDND@Ente v1 > Configurazione > Proprietà

Proprietà

Visualizzati record [1-1] su 1

	Nome	Valore
<input type="checkbox"/>	<u>PDND-resource</u>	PetStore

Figure3.123: Proprietà “PDND-resource”

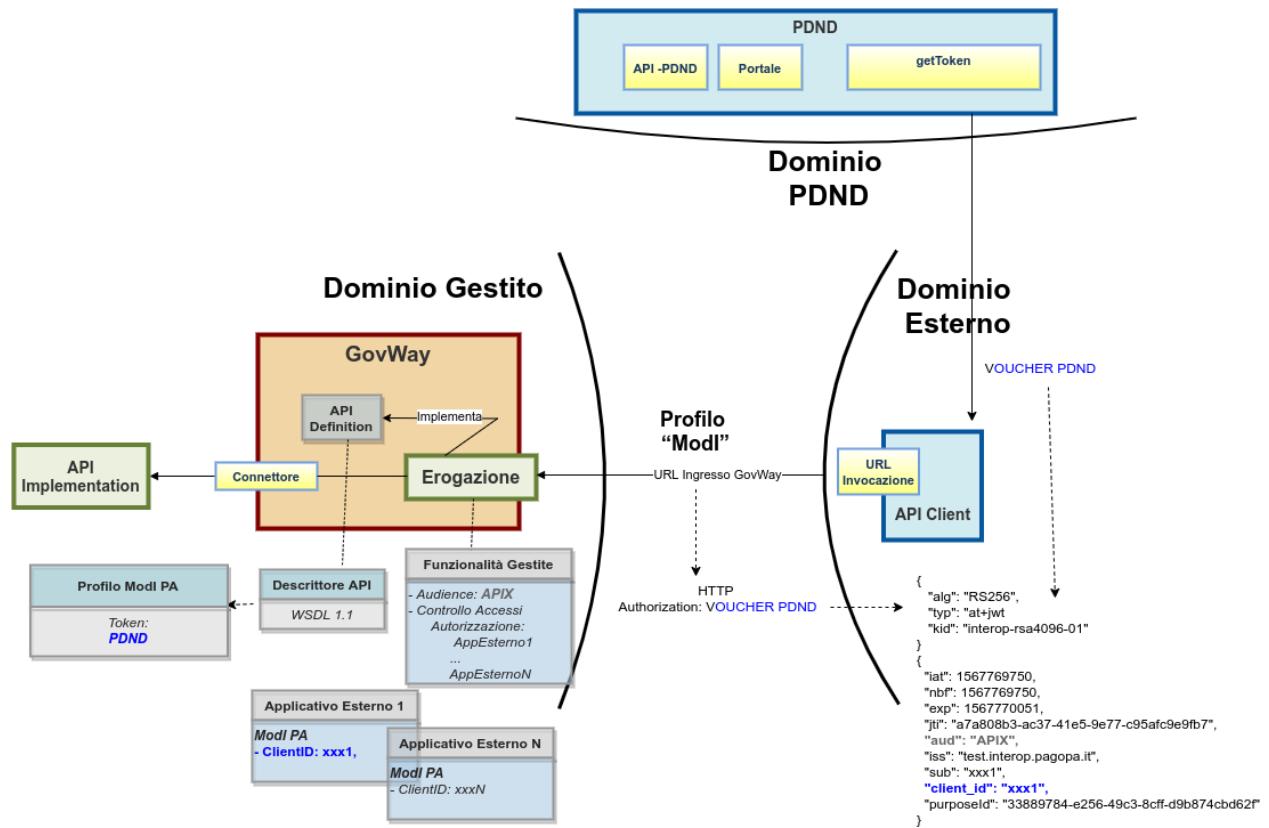


Figure3.124: Erogazione di una API SOAP con profilo “ModI”, pattern ID_AUTH_REST_01 via PDND

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.125: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API SOAP di esempio (Temperature Conversion) definita con pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_01» e «ID_AUTH_REST_01 via PDND»;
- un'istanza Govway per la gestione del profilo ModI nel dominio dell'erogatore;
- un'authorization server che simula la PDND;
- un client del dominio esterno che invoca l'azione di esempio «CelsiusToFahrenheit» dell'erogazione esposta da Govway;
- il server “Temperature Conversion” 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://www.w3schools.com/xml/tempconvert.asmx>”.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth+PDND - IN App1» che è stata preconfigurata 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.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*.

Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App1-ModI” identificato grazie al claim “client_id” presente all'interno del token. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth+PDND - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

Conformità ai requisiti ModI

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

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

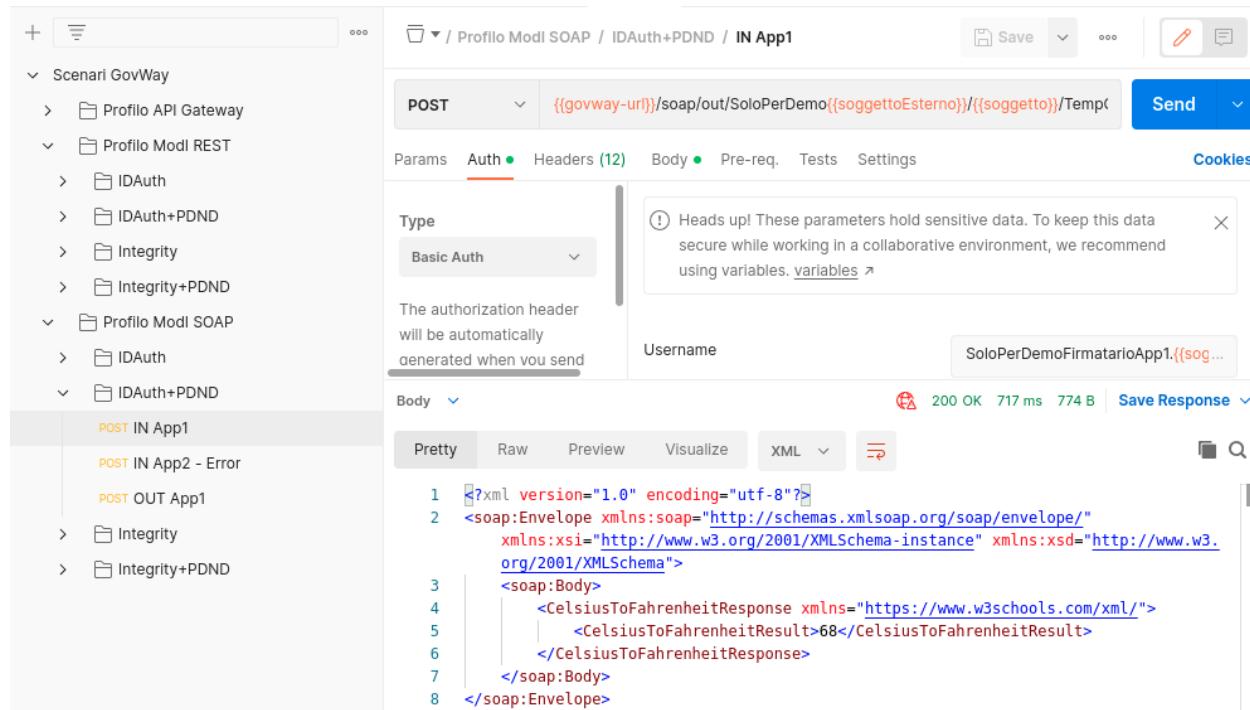


Figure3.126: Pattern IDAuth+PDND - Erogazione API SOAP, esecuzione da Postman



Figure3.127: Profilo ModI della govwayConsole

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario [Esecuzione](#). Nel seguito viene riporta solamente la differenza relativa alla registrazione dell'API.

Registrazione API

Viene registrata l'API «TemperatureConversionAuthPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.128).

3.3.4 Fruizione API SOAP

Obiettivo

Fruire di un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio.

API > TemperatureConversionAuthPDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern ▼
Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern ▼
Direct Trust con certificato X.509

Generazione Token ▼
Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Figure3.128: Configurazione Pattern ModI con «ID_AUTH_CHANNEL_01» senza sicurezza messaggio

La figura seguente descrive graficamente questo scenario.

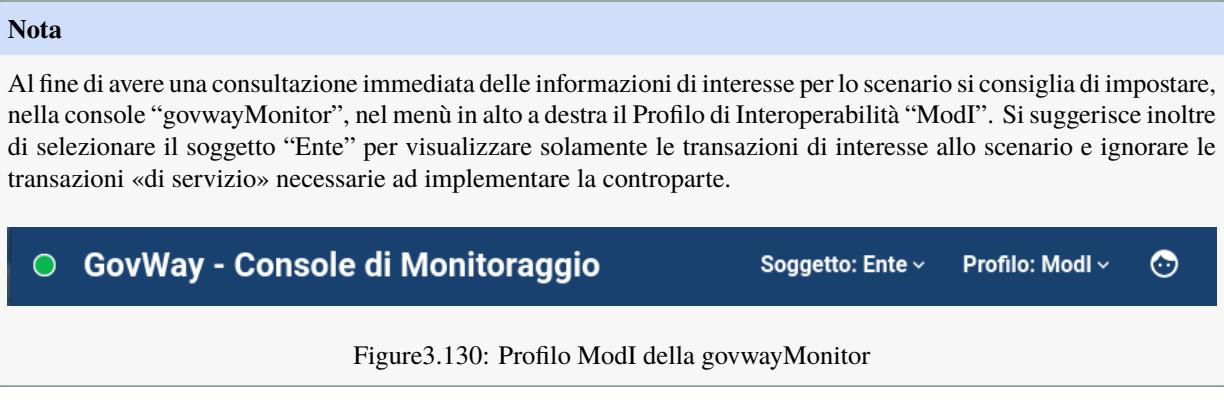
Le caratteristiche principali di questo scenario sono:

1. un applicativo fruitore che dialoga con il servizio erogato in modalità ModI in accordo ad una API condivisa registrata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



GovWay - Console di Monitoraggio

Soggetto: Ente ▾ Profilo: ModI ▾



Figure3.130: Profilo ModI della govwayMonitor

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API SOAP di esempio (Temperature Conversion) definita con pattern di interazione Bloccante e pattern di sicurezza «ID_AUTH_CHANNEL_01» e «ID_AUTH_REST_01 via PDND»;
- un'istanza Govway per la gestione del profilo ModI nel dominio del fruitore;
- un'authorization server che simula la PDND;
- un client del dominio gestito che invoca l'azione di esempio «CelsiusToFahrenheit» sulla fruizione configurata su Govway.

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - IDAuth+PDND - OUT App1» che è stata preconfigurata 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”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*.

Conformità ai requisiti ModI

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

Configurazione

Nota

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». Si suggerisce

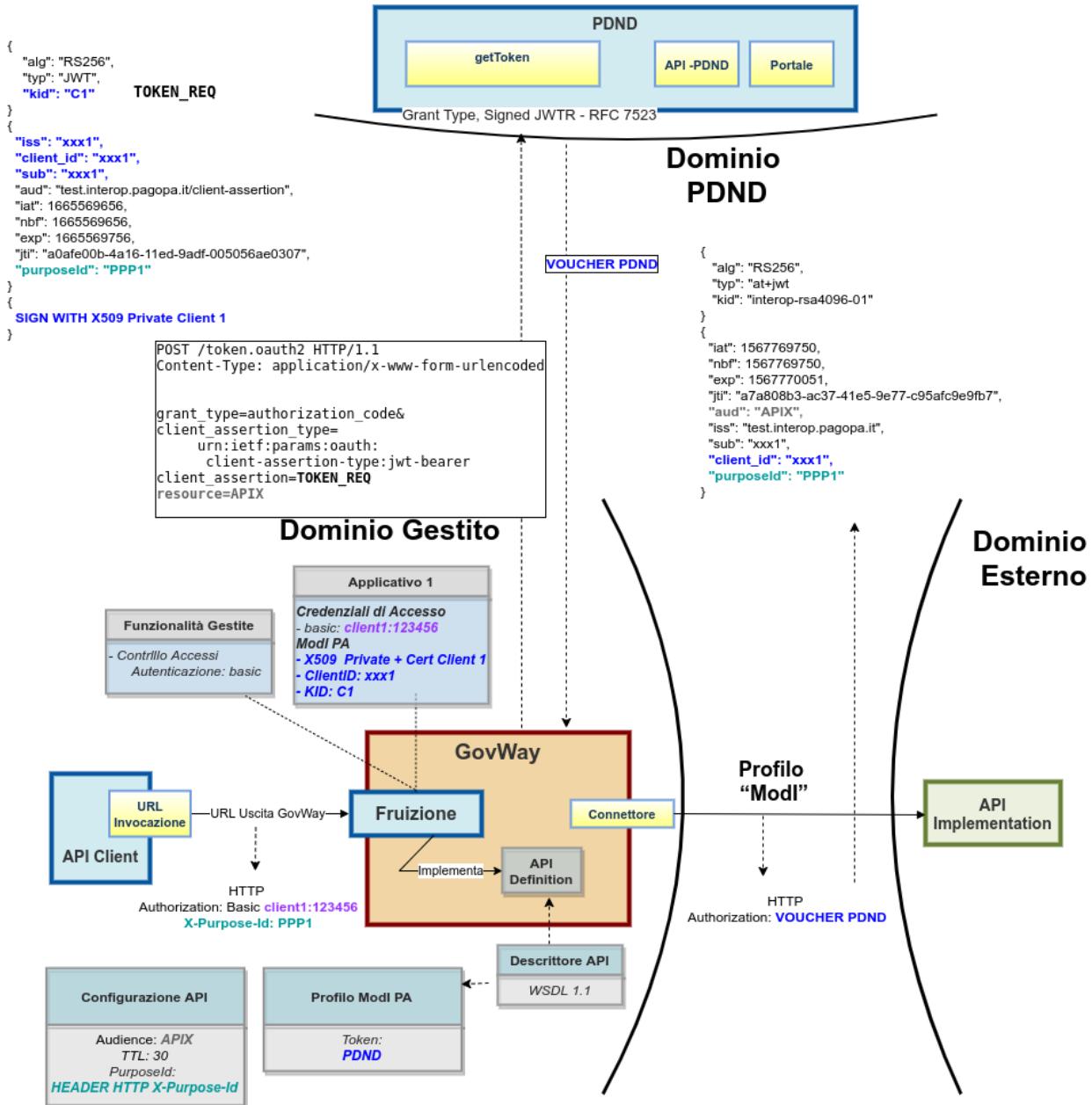


Figure3.129: Fruizione di una API SOAP con profilo “Modi”, pattern ID_AUTH_REST_01 via PDND

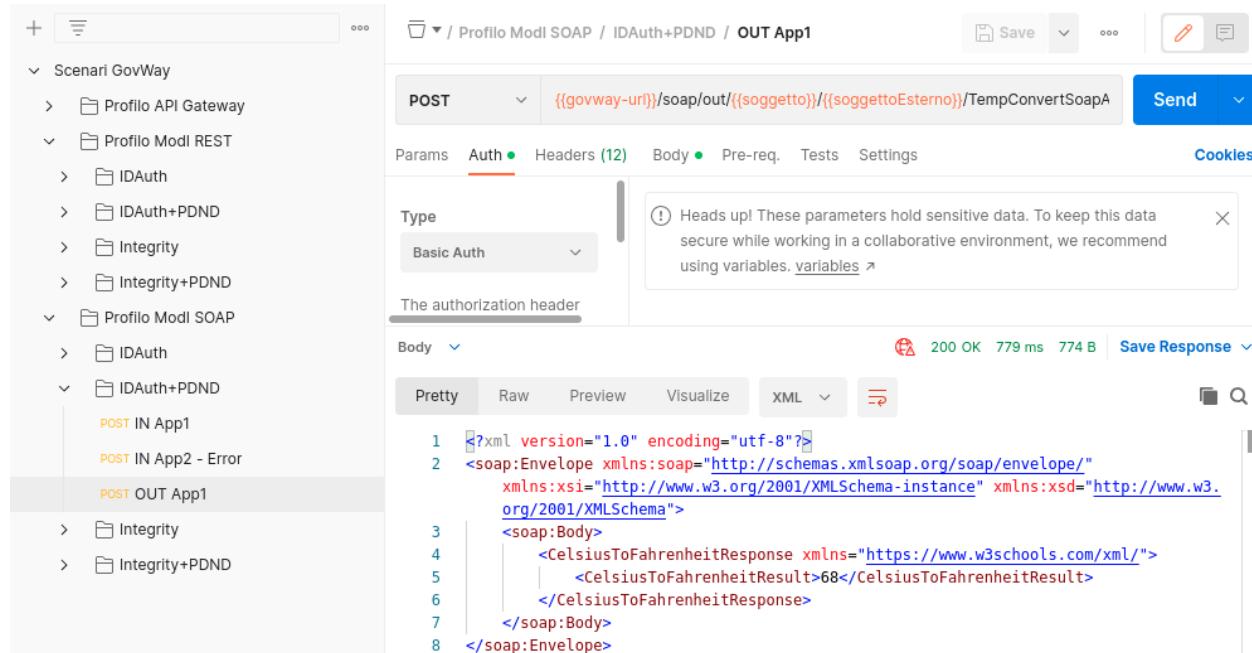


Figure3.131: Pattern IDAuth+PDND - Fruizione API SOAP, esecuzione da Postman

inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.132: Profilo ModI della govwayConsole

Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario *Configurazione*. Nel seguito viene riporta solamente la differenza relativa alla registrazione dell’API.

Registrazione API

Viene registrata l’API «TemperatureConversionAuthPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.133).

3.4 Pattern “ID_AUTH” via PDND + “INTEGRITY_01”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_pdnd_integrity.

3.4.1 Erogazione API REST

Obiettivo

Esportare un servizio, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd_integrity.

Sintesi

API > TemperatureConversionAuthPDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern ▼
Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern ▼
Direct Trust con certificato X.509

Generazione Token ▼
Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Figure3.133: Configurazione Pattern ModI con «ID_AUTH_CHANNEL_01» senza sicurezza messaggio

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_01» a garanzia dell'integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

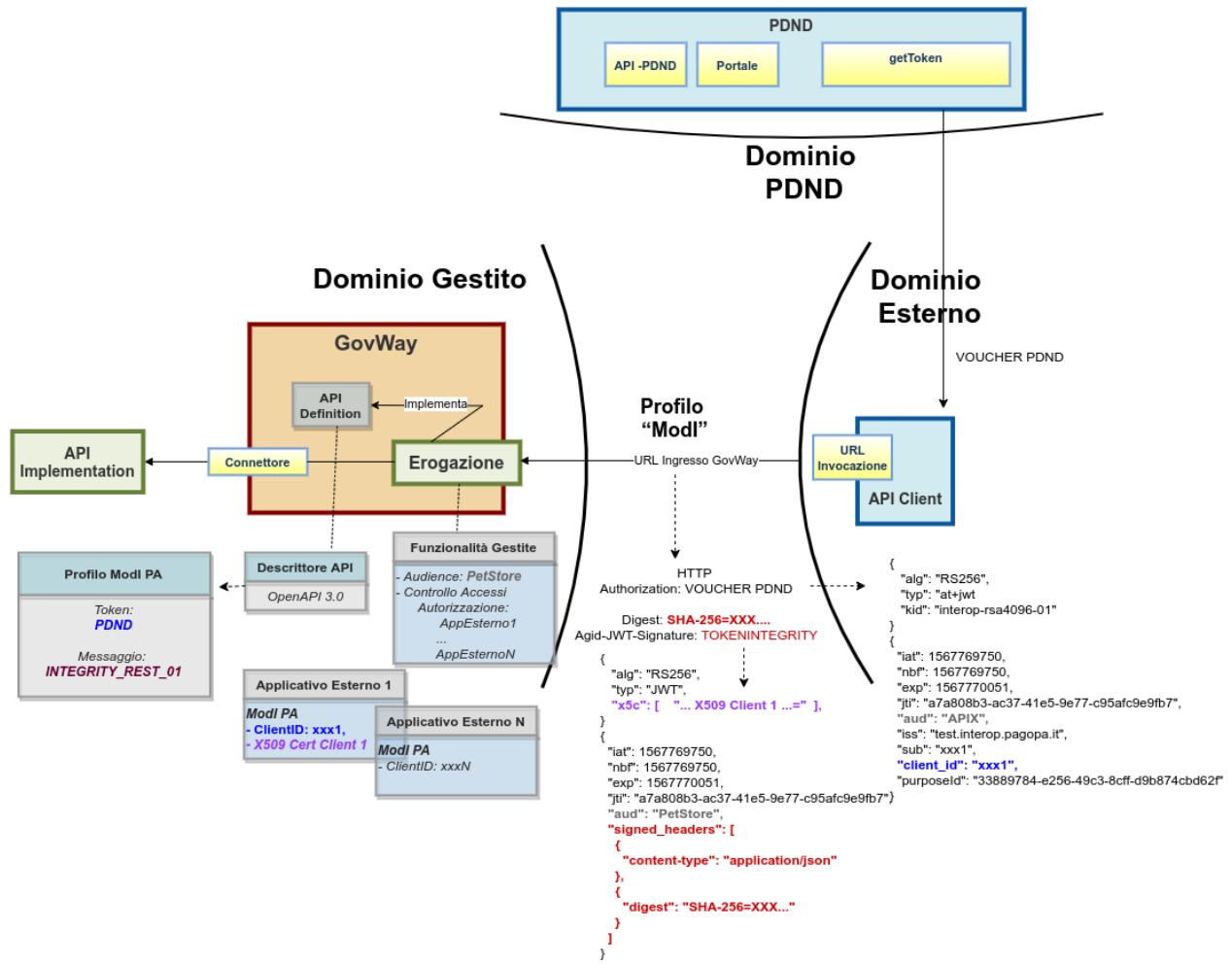


Figure3.134: Erogazione di una API REST con profilo “ModI”, pattern INTEGRITY_REST_01 e pattern ID_AUTH_REST_01 via PDND

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 e il servizio viene registrato sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

● GovWay - Console di Monitoraggio

Soggetto: Ente
Profilo: ModI

Figure3.135: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity+PDND - IN App3» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

```

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

```

Figure3.136: Pattern Integrity+PDND - Erogazione API REST, esecuzione da Postman

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”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.137.

Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization» e «Agid-Jwt-Signature» che contengono rispettivamente il token di sicurezza che il fruitore ha ottenuto dalla PDND e il token di integrità. È inoltre presente l'header http «Digest» che contiene il valore per la verifica dell'integrità del payload.

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fbb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCJ6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6xWqdhfHBaJT3on7jaCV6LVEXEaqfDWwI48L8SextE3UyuuGh-1s-g6320H86SIFr8tzsK4p-Fc94WclxhMjxjXAer6Sh8C
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCJ6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6WyJNSjIiVuNpGcBUWGoh1dKhKCv6nd6LFjWiFSdExxjto5i8iBtyjExSu06IHL0iaD2pI1jYrG37MqE6f-1xBYCqlElCchD6GQ8R4fEc5
Digest	SHA-256=OhjWocHmyIM/B4HeXlpINxyqvqU7zKjERTUMDPVfhPY=
Accept	*/*
Govway-Transaction-Id	d1a3b973-4fbb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

Figure3.137: Messaggio inviato dal fruitore

- Tutte le analisi che riguardano il token di autenticazione generato dalla PDND sono le medesime descritte nello scenario *Esecuzione*.
- Inoltre 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 nel token «Agid-JWT-Signature». Nella fase di validazione del token si può notare come nella sezione header (Fig. 3.138) viene riportata l'identità del fruitore sotto forma di certificato X.509 a differenza di quello ottenuto dalla PDND.
- 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 dell'audience ricevuto con quello atteso e la corrispondenza del digest con il payload e con il valore interno al token «Agid-Jwt-Signature». Solo in caso di superamento dell'intero processo di validazione, il messaggio viene inoltrato al servizio erogatore.

HEADER: ALGORITHM & TOKEN TYPE	
<pre> ID { "alg": "RS256", "typ": "JWT", "kid": "app1.enteesterno.govway.org", "x5c": ["MIIE/jCCAuagAwIBAgICAPgwDQYJKoZIhvcNAQELBQAwNjELMAkGA1 UEBhMCAxOxEzARBgNVBAoMCmdvdndheS5vcmcxEjAQBgNVBAMMCUvdv 1dheSBQTAefWw0yMjEwMTkwNzU1NTThaFw0zNzEwMTUwNzU1NTThaMEgx CzAJBgNVBAYTAm10MRMwEQYDVQQKDApnb3Z3YXku3JnMSQwIgYDVQQ DBBthcHAXLmVudGVFc3R1cm5vLmdvdndheS5vcmcwggEiMA0GCSqGSI b3DQEBAQUAA4IBDwAwggEKAoIBAACQ1/cfENX06hdvEVxJiJAF00ePjn 5Sh/HIj2du8hRv0zA+KFFieaF4xhImSOT1oq/vwwxFxqvdk1bTJ37r jBo6DKuQZor83j/Do87x3sFJe/epGKx96Q3PRE9mA1qx3Y5FFShfGNZ zG2RFNA2jhVQ/bsd9E051FC3XshF90CtJJs9LgvT2+0+uJK3siA6ht KcYQ58UcK1W1Y109MnXqaz82TiH93eTSkk33wO9atzC0w3JAVmcRRk d0hFbjMeEvNR86cdNfy9Xit7ZDR11IB8t10/fI/oAW0oK/3TbF1X0r VL1QhMc1JdqS3NwJLayoqmZT/Xh50qjD1ldghwbAgMBAAGjggECMIH /MAkGA1UdEwQCMAwEQYJYIZIAYb40gEBBAQDAgeAMDMGCGWSAGG+E IBDQqmF1RPcGVuU1NMIEd1bmVyYXR1ZCBDbG11bnQgQ2VydG1maWnhd GUwHQYDVR00BBYEFCBwk8Bs9JS+6c/vTU+JX0eqX81BMGYGA1UdIwRf MF2AFCqHFNpm2RdIA3igRXzNEeJ5ivegoTqk0DA2MQswCQYDVQGGEwJ pdDETMBEA1UECgwKZ292d2F5Lm9yZzESMBAGA1UEAwwJR292V2F5IE NBggkA4tGAdmeSJF4wDgYDVR0PAQH/BAQDAgXgMBMGA1UdJQQMMAoGC CsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQDRj52cdYwcqFDNmC29 CY0DR0N0TM/5RKq9sL6sgI7z4cUmkYIeGh/9YQDoRFhDBVGZ80rx0ka sZ/Po0Iuw+41f9IDTBe04Ym0CK3M1M9H2LiEKe9hngRtjzGw5tFRQnq KbLLX61otJAXuE488SrSAMbEDezlbZt+V1Sgc48fOKsjShUs8CwSW0G 6RE5w4Q4oa0dX971PTziWDoFnxBfN17/HAYA0625/vcp8PrZLqhTIGH 7dt+1T4Hb+i10wKB87B8Cab0Gh0spIHDdDGNEyX50d1ZyMwJQ10ysK6 1Yx1WtCrKPfmsvSeqiVxJPHUgwTsFPrgoVRT+dT1NnAdXYxFk0Yxz7z n7qeKD16cXHLTsYet1cQfedyDPE0r1i4GFL1KY37NFqRtJx5NadkJk6 GXk43zIFQo119PGJ8nVHupB6IBJ1h/6xem1TTMSt52zcjV4b5zRHL8Z qNF+S0QnJKch2FcyAYuGjuVj0qa5rh5wNcy71lcDSHm8tsPj5qpW1M E0mhmmWWY+w5KBCpMoLbn9cvqAn/N19L3e3SqH1KLp8Hw05CtH4/tLEe 3N+0z+8xzcmLdqbAZ9nD7YVLVoyt5Y+Ixuj17F18dzEh9dzcLhJojsB mPjoFMMyulbpjZG0A1TjKVpkxyXgaqsd9Hjs4ATg79Vk8U/GnEXJhXQ xU2TYw=="], "x5t#S256": "agRQxqs- VYDP2NIzbR7XH2GiInWH2bcL1xMPhimfMKk" } </pre>	

Figure3.138: Sezione «Header» del Token di sicurezza «Agid-Jwt-Signature»

Nel payload del token «Agid-JWT-Signature» (Fig. 3.139) sono invece presenti i riferimenti temporali (iat, nbf, exp), l'audience (aud) e il claim «signed_headers» utilizzato per la verifica dell'integrità.



```
PAYOUT: DATA

{
  "iat": 1666190361,
  "nbf": 1666190361,
  "exp": 1666190421,
  "jti": "d1b37101-4fbb-11ed-a5ac-0242ac140002",
  "aud": "petstore.ente.govway.org",
  "client_id": "app1.enteesterno.govway.org",
  "iss": "SoloPerDemoEnteEsterno",
  "sub": "SoloPerDemoFirmatarioApp1",
  "signed_headers": [
    {
      "digest": "SHA-256=0hjWocHmy1M/B4HeX1plNxygvqU7zKjERTUMDPVfhPY=",
      "content-type": "application/json"
    }
  ]
}
```

Figure3.139: Sezione «Payload» del Token di sicurezza «Agid-Jwt-Signature»

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario *Esecuzione*.

Le evidenze del processo di validazione relativo al pattern «INTEGRITY_REST_01» sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.140). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di sicurezza presenti, tra cui si può notare il digest e gli header http firmati.

- Lo scenario è preconfigurato per autorizzare puntualmente l'applicativo “App3-ModI” identificato grazie al claim “client_id” presente all'interno del token della PDND. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity+PDND - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

Conformità ai requisiti ModI

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

1. la sicurezza messaggio applicata è quella dei pattern «ID_AUTH_REST_01» via PDND» + «INTEGRITY_REST_01» come ampiamente mostrato precedentemente dove sono stati mostrati i token validati e i criteri autorizzativi;
2. l'identificazione del fruitore avviene rispetto al claim “client_id” presente all'interno del token. È stato anche mostrato come sia possibile configurare criteri autorizzativi puntuali.

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

Informazioni Mod

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_REST_01 con ID_AUTH_REST_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione Accesso CRUD

Sicurezza Messaggio

Digest SHA-256=0hjWocHmyIM/B4HeXIplNxygvqU7zKjERTUMDPVfhPY=
ClientId app3.enteesterno.govway.org
Subject SoloPerDemoFirmatarioApp3
Issuer SoloPerDemoEnteEsterno
MessageId 20fb762b-08fe-11ee-9028-0242c0a85002
Audience petstore.ente.govway.org
NotBefore 2023-06-12_11:42:54.000
Expiration 2023-06-12_11:43:54.000
IssuedAt 2023-06-12_11:42:54.000
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app3.enteEsterno.govway.org, O=govway.org, C=it

Headers HTTP Firmati

content-type application/json
digest SHA-256=0hjWocHmyIM/B4HeXIplNxygvqU7zKjERTUMDPVfhPY=

Figure3.140: Traccia della richiesta elaborata dall'erogatore

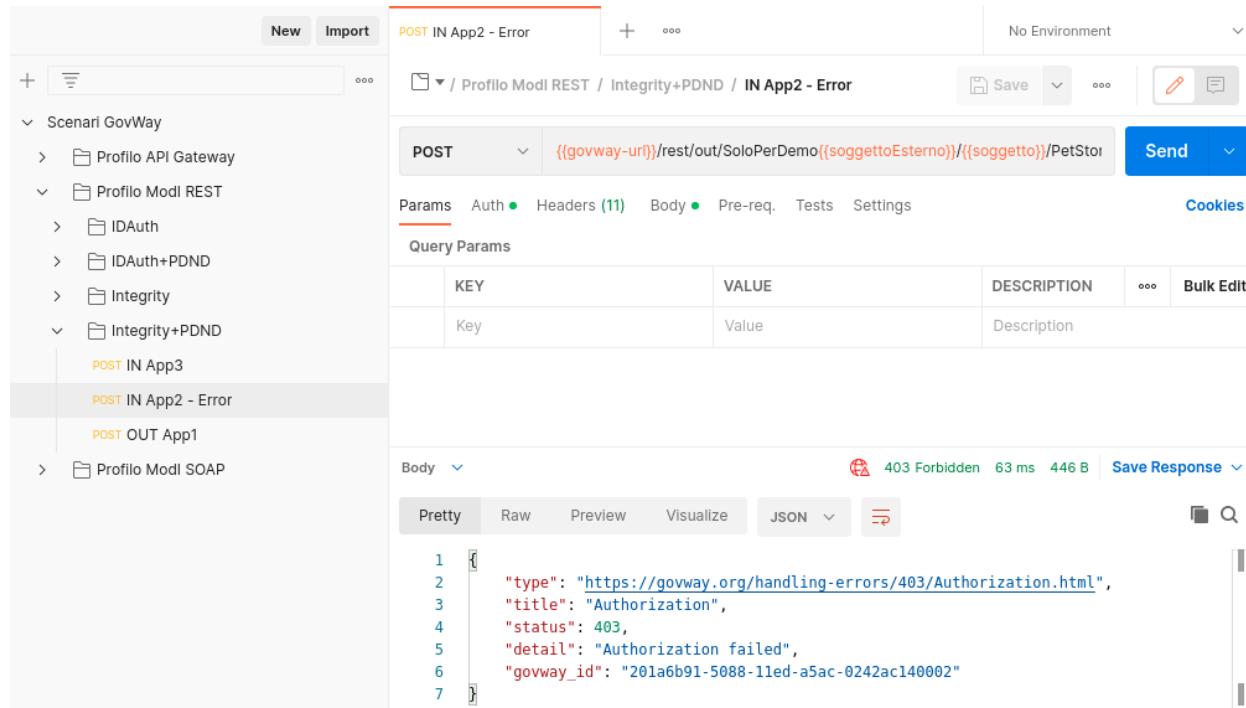


Figure3.141: Pattern Integrity+PDND - Erogazione API REST - Autorizzazione negata, esecuzione da Postman



Figure3.142: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_01».

Registrazione API

Viene registrata l'API «PetStoreIntegrityPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_REST_01 con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.56).

Applicativo Esterno

È opzionalmente possibile registrare l'applicativo esterno che corrisponde al fruitore del servizio come descritto nello scenario nello scenario *Configurazione*.

La registrazione comporta l'associazione all'applicativo sia del "client_id" necessario all'identificazione che del certificato di firma che verrà atteso nell'header HTTP "Agid-JWT-Signature" (Fig. 3.144). Questo scenario è quello preconfigurato.

Erogazione

Nell'erogazione «PetStoreIntegrityPDND», relativa all'API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.145) necessari per validare le richieste in ingresso relativamente al token "Agid-JWT-Signature".

API > PetStoreIntegrityPDND v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_01

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_REST_01 con ID_AUTH_REST_01

Integrità payload del messaggio

Generazione Token

Authorization PDND

Token ID_AUTH negoziato con la PDND

Header HTTP del Token

Agid-JWT-Signature + Authorization Bearer

Applicabilità

Richiesta e Risposta

Digest Richiesta

Non ripudiabilità della trasmissione (i)

Informazioni Audit

Dati del dominio del fruttore

Figure3.143: Configurazione Pattern ModI «INTEGRITY_REST_01 con ID_AUTH_REST_01» sulla API REST

Applicativo

Dominio	Esterno
Soggetto	EnteEsterno
Nome *	App3-PDND
Tipo	Client
Proprietà(0)	

Ruoli

visualizza(0)

Modi

Sicurezza Messaggio	Authorization PDND + Integrity	▼
Certificato		
Cambia Certificato		
Aggiungi Certificato		
Download		
Verifica	<input checked="" type="checkbox"/>	
Subject	/c=it/cn=app3.enteEsterno.govway.org/o=govway.org/	
Issuer	/c=it/cn=GovWay CA/o=govway.org/	
Serial Number	250 (Hex) 00:FA	
Self Signed	No	
Not Before	20/10/2022 09:45:00	
Not After	16/10/2037 09:45:00	
Clientid registrato sulla PDND		
Token Policy *	PDND	
Identificativo *	App3-Esterno-PDND	

Figure3.144: Configurazione applicativo esterno (fruitore)

ModI - Richiesta

Sicurezza Messaggio

Riferimento X.509	x5c (Certificate) x5t#256 (Certificate SHA-256 Thumbprint) x5u (URL)
TrustStore Certificati	Default
Time to Live	Default
Audience	petstore.ente.govway.org

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

Figure3.145: Configurazione richiesta dell'erogazione

La sezione «ModI Risposta» si utilizza per indicare i parametri per la produzione del token di sicurezza “Agid-JWT-Signature” da inserire nel messaggio di risposta (Fig. 3.146).

3.4.2 Fruizione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd_integrity.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore devo anche presentare il token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_01» a garanzia dell'integrità del messaggio.

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 e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_01».

Modi - Risposta

Sicurezza Messaggio

Algoritmo	RS256
HTTP Headers da firmare *	Digest <input checked="" type="checkbox"/> Content-Type <input checked="" type="checkbox"/> Content-Encoding <input checked="" type="checkbox"/>
Riferimento X.509	Utilizza impostazioni della Richiesta
Certificate Chain	<input type="checkbox"/>
KeyStore	Default
Time to Live (secondi) *	60
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token della risposta	
Claims	<input type="text"/> i
Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli	

Figure3.146: Configurazione risposta dell'erogazione

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Monitoraggio Soggetto: Ente i Profilo: ModI i

Figure3.148: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Integrity+PDND - OUT App1» che è stata preconfigurata 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 la console “govwayMonitor”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario [Esecuzione](#). Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

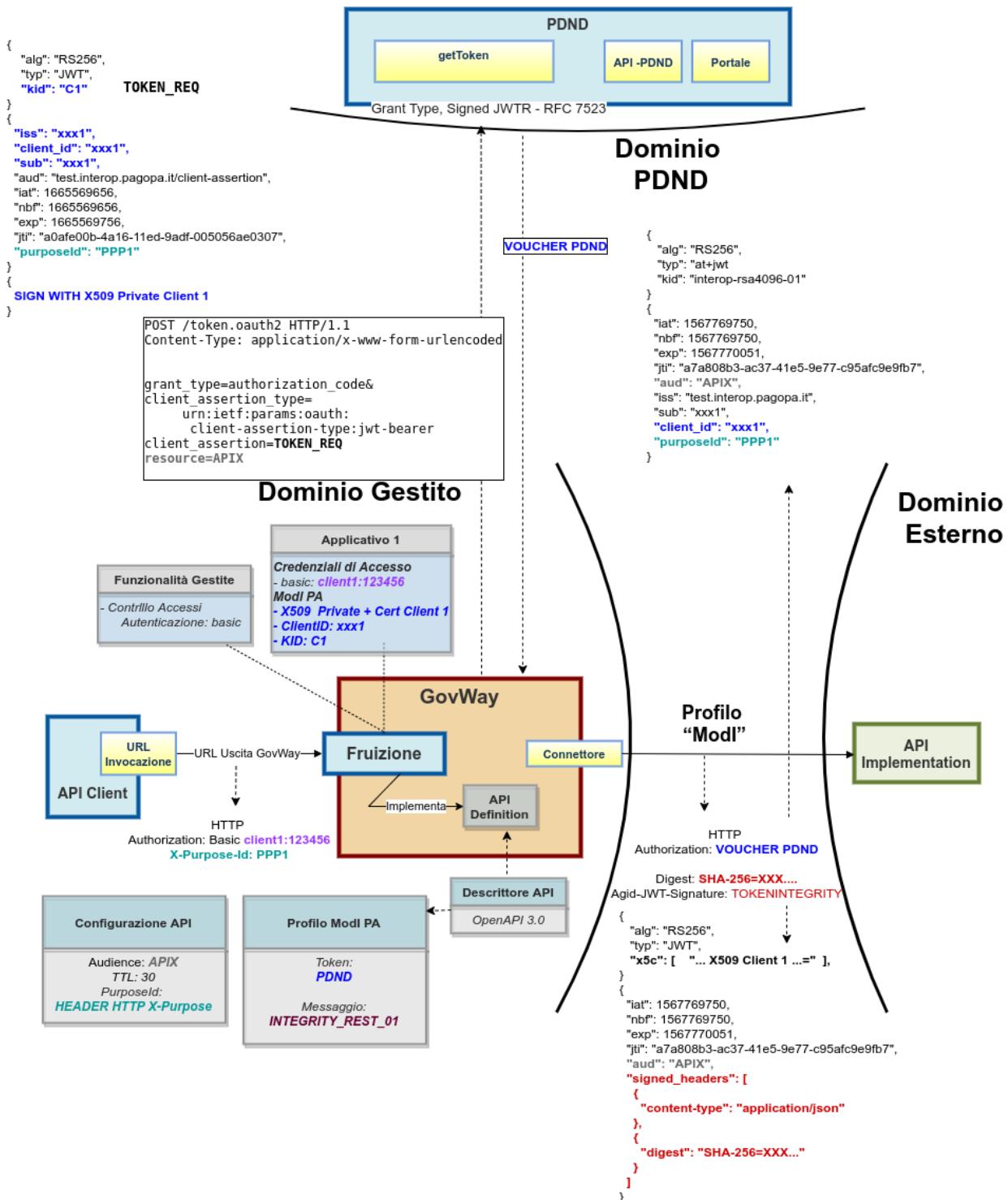


Figure3.147: Fruizione di una API REST con profilo "ModI", pattern INTEGRITY_REST_01 e pattern ID_AUTH_REST_01 via PDND

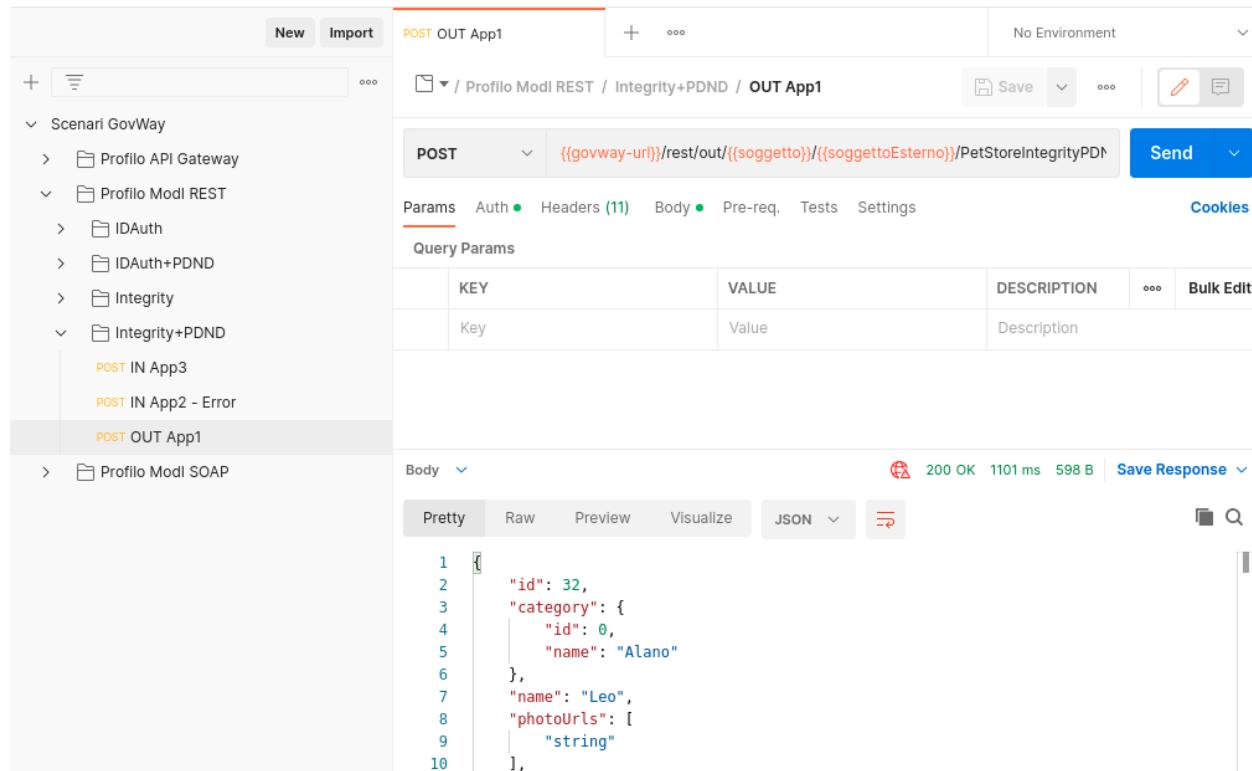


Figure3.149: Pattern Integrity+PDND - Fruizione API REST, esecuzione da Postman

- 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 un token di sicurezza da inviare alla PDND con il quale ottenere indietro un voucher spendibile per il servizio desiderato. Questa parte è stata ampiamente mostrata nella scenario [Esecuzione](#).

Oltre al token della PDND, GovWay produce un ulteriore token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_01». Da govwayMonitor si può visualizzare il messaggio di richiesta in uscita che è il medesimo di quello in entrata con la differenza che sono stati aggiunti gli header HTTP «Authorization» e «Agid-Jwt-Signature» che contengono rispettivamente il token ottenuto dalla PDND e il token dell'integrità. È inoltre presente l'header http «Digest» che contiene il valore utilizzabile dall'erogatore per la verifica dell'integrità del payload. (Fig. 3.150).

- L'header e i payload del token «Agid-JWT-Signature» sono identici a quelli già visualizzati nello scenario di erogazione REST, relativamente al messaggio in ingresso (Fig. 3.138 e Fig. 3.139). Le informazioni inserite nel token vengono anche tracciate e sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.151). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di sicurezza, tra cui si può notare il digest e gli header http firmati.

Conformità ai requisiti ModI

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

- viene effettuata una negoziazione del voucher PDND come mostrato nelle tracce relative ai token scambiati con la PDND;
- l'invocazione del servizio avviene fornendo il voucher della PDND precedentemente negoziato;
- vengono inoltre prodotti gli header http «Agid-Jwt-Signature» e «Digest» previsti dal pattern di sicurezza «INTEGRITY_REST_01».

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fbb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVClsImtpZC16ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsIng1Yyl6xWqdhfvHBaJT3on7jaCV6LVEXEaqAqfDWwI48L8SextE3UyuuGh-1s-g6320H8j6SIFr8tzsK4p-Fc94WcIxhMJxjXAer6Sh80
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVClsImtpZC16ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsIng1Yyl6WyJNSilVuNpGcBUWGoh1dKhKCv6nd6LFjWiFsdExxjto5i8iBtyjExSu06IHL0iaD2p1jKyRG37MgE6f-1xBYCqjElCchD6GQ8R4fEc5
Digest	SHA-256=OhjWochHmyIM/B4HeXiplNxygvqU7zKjERTUMDPVfhPY=
Accept	/*
Govway-Transaction-Id	d1a3b973-4fbb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

Figure3.150: Messaggio di richiesta in uscita (con token di sicurezza inseriti nell'header HTTP)

Informazioni Modl

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_REST_01 con ID_AUTH_REST_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione 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=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
Subject App1-PDND
Issuer Ente
ClientId App1-PDND
Audience petstore.enteEsterno.govway.org
MessageId 25c1b125-08fe-11ee-9028-0242c0a85002
Expiration 2023-06-12_11:48:01.000
NotBefore 2023-06-12_11:47:01.000
IssuedAt 2023-06-12_11:47:01.000

Headers HTTP Firmati

content-type application/json
digest SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=

Figure3.151: Traccia della richiesta generata dal fruttore

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.152: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_01».

Registrazione API

Viene registrata l’API «PetStoreIntegrityPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_REST_01» con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.153).

Fruizione

Nella fruizione «PetStoreIntegrityPDND», relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.154) necessari a generare il token “Agid-JWT-Signature”. In particolare è possibile specificare l’audience atteso dall’erogatore e il tempo di validità del token.

La sezione «ModI Risposta» definisce i criteri per la validazione del token di sicurezza “Agid-JWT-Signature” presente nel messaggio di risposta, come il truststore per l’autenticazione dell’erogatore (Fig. 3.155).

3.4.3 Erogazione API SOAP

Obiettivo

Esporre un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd_integrity.

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all’erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_SOAP_01» a garanzia dell’integrità del messaggio.

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 e il servizio viene registrato sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;

API > PetStoreIntegrityPDND v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_01

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_REST_01 con ID_AUTH_REST_01

Integrità payload del messaggio

Generazione Token

Authorization PDND

Token ID_AUTH negoziato con la PDND

Header HTTP del Token

Agid-JWT-Signature + Authorization Bearer

Applicabilità

Richiesta e Risposta

Digest Richiesta

Non ripudiabilità della trasmissione (i)

Informazioni Audit

Dati del dominio del fruttore

Figure3.153: Configurazione Pattern ModI «INTEGRITY_REST_01 con ID_AUTH_REST_01» sulla API REST

Modi - Richiesta

Sicurezza Messaggio

Algoritmo	RS256
HTTP Headers da firmare *	Digest <input checked="" type="checkbox"/> Content-Type <input checked="" type="checkbox"/> Content-Encoding <input checked="" type="checkbox"/>
Riferimento X.509	x5c (Certificate) x5t#256 (Certificate SHA-256 Thumbprint) x5u (URL)
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	
Audience	petstore.enteEsterno.govway.org 
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	
Claims	
Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli	

Figure3.154: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

Riferimento X.509	Utilizza impostazioni della Richiesta
TrustStore Certificati	Default
Time to Live	Default
Verifica Audience	<input checked="" type="checkbox"/> La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente
	

Figure3.155: Configurazione risposta della fruizione

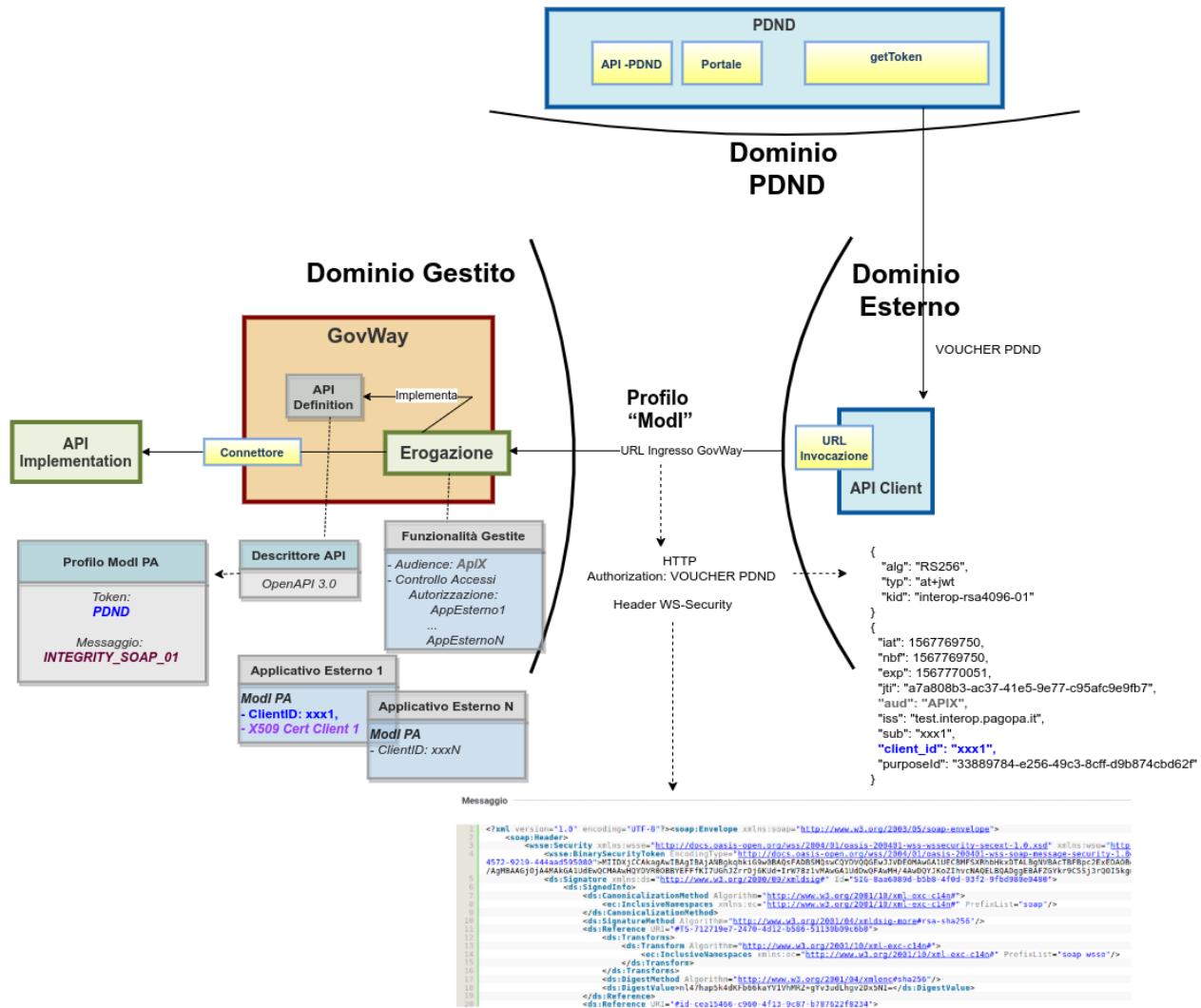


Figure3.156: Erogazione di una API SOAP con profilo “ModI”, pattern INTEGRITY_SOAP_01 e pattern ID_AUTH_REST_01 via PDND

3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_SOAP_01».

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Monitoraggio

Soggetto: Ente
Profilo: ModI

Figure3.157: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_SOAP_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity+PDND - IN App3» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

Figure3.158: Pattern Integrity+PDND - Erogazione API SOAP, esecuzione da Postman

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.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.32. Come si nota, il messaggio SOAP contiene nell’header WS-Security sia il token di sicurezza (elemento «BinarySecurityToken») sia l’elemento «WSAddressing - To» e il digest del payload (elemento «DigestValue») prodotti dal fruitore con la relativa firma digitale (elemento «SignatureValue») come previsto dal pattern «INTEGRITY_SOAP_01».

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">MIIE/zCAuegAwIBAgICAM4wDQYJKoZIhvNAQELBQAwNjELMAkGA1UEBMCaX0xEzARBgNVBaoICmdvdndheS5vcmcxEjAOBgNVBAMMCUdvl dhesBDOTAf
/Wu06/YXIVIDHLYMjypb/fL0SL8SKA6uW9swpXcoGJPK9aqw0iV0/Bw2LpvI1657H+btNiLeBfhSmUnNL7C25Hba/WivKh78213F5LYC4sY8l9nfC/fa6QUouu1DltxWohKwzNf
/zJBgnVHRMejaAMBEGCGWC5AGG+ETBAQ0EAvIHoDazBg1ghkgBvhvbCA0QEJhYKT3B1b1NTTCBHZwS5cmF0Zw0g02xpZw50IEN1cnRpZmljYXRlMB0GA1UdQgQWBBRUAiCyEM
/JIBWmVuatppwNCJRTzI06qmIElgm0BTWlZj0MxI/+zSWQUTMNGNs0zzTDS11rme1diRcbKVvNcxtrPHH4sh5JdIp1f7G314CaTjJHBH02UfUa0eb03dFqqRc6QzmEr
/OfppiDpcA7fXITX0gDokm-WaMAZ7s6DEmgW=h7KL6u0hewzukbasDpYbqycioDaom4yWva15svmubwSRIAlRH80uew0jcyejSfEY8fslFudoBLG934Dt14HnT2CBM8
/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>

```

Figure3.159: Messaggio inviato dal fruitore

- Tutte le analisi che riguardano il token di autenticazione generato dalla PDND sono le medesime descritte nello scenario *Esecuzione*.
- 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 dell’audience ricevuto con quello atteso e la corrispondenza del digest rispetto 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. 3.160). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dal token di sicurezza presente nell’header soap.
- Lo scenario è preconfigurato per autorizzare puntualmente l’applicativo “App3-ModI” identificato grazie al claim “client_id” presente all’interno del token della PDND. È possibile utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity+PDND - IN App2 - Error» per verificare che una richiesta proveniente da un differente applicativo non viene autorizzata.

Conformità ai requisiti ModI

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

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

Informazioni Modelli

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione Bloccante

Sicurezza Messaggio

MessageID 297123d9-08fe-11ee-9028-0242c0a85002
WSA-From app3.enteesterno.govway.org
WSA-To TempConvertSoap.ente.govway.org
Digest SHA256=6uByffAl2Xht8Mm1FBluUkvRM83c/Qh4YPvzxEYaqAw=
Expiration 2023-06-12_11:50:37.258
IssuedAt 2023-06-12_11:49:37.258
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app3.enteEsterno.govway.org, O=govway.org, C=it

Elementi SOAP Firmati

Body http://schemas.xmlsoap.org/soap/envelope/
ReplyTo http://www.w3.org/2005/08/addressing
MessageID http://www.w3.org/2005/08/addressing
Action http://www.w3.org/2005/08/addressing
From http://www.w3.org/2005/08/addressing
To http://www.w3.org/2005/08/addressing
Timestamp http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

Figure3.160: Traccia della richiesta elaborata dall'erogatore

The screenshot shows the Postman interface with the following details:

- Left Sidebar:** Shows a tree structure of scenarios: Scenari GovWay, Profilo API Gateway, Profilo Modi REST, Profilo Modi SOAP, and a specific POST request for IN App2 - Error.
- Request Section:**
 - Method: POST
 - URL: {{govway-url}}/soap/out/SoloPerDemo{{soggettoEsterno}}/{{soggetto}}/Temp
 - Auth tab is selected, showing "Basic Auth" selected.
 - Headers (12) tab is selected.
 - Body tab is selected, showing the SOAP fault message.
- Response Section:**
 - Status: 500 Internal Server Error
 - Time: 79 ms
 - Size: 1004 B
 - Save Response button is available.
- Message Content:**

```

1  <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
2    <SOAP-ENV:Header/>
3    <SOAP-ENV:Body>
4      <SOAP-ENV:Fault>
5        <faultcode>SOAP-ENV:Client.Authorization</faultcode>
6        <faultstring xml:lang="en-US">Authorization failed</faultstring>
7        <faultactor>http://govway.org/integration</faultactor>
8        <detail>
9          <problem xmlns="urn:ietf:rfc:7807">
10            <type>https://govway.org/handling-errors/403/Authorization_
11              html</type>
12            <title>Authorization</title>
13            <status>403</status>
14            <detail>Authorization failed</detail>
15            <govway_id>f90ade9d-c312-11ed-8b12-0242c0a8d002</govway_id>
</problem>

```

Figure3.161: Pattern Integrity+PDND - Erogazione API SOAP - Autorizzazione negata, esecuzione da Postman



Il processo di configurazione per questo scenario è del tutto analogo a quello descritto per lo scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_SOAP_01».

Registrazione API

Viene registrata l'API «TemperatureConversionIntegrityPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_SOAP_01» con ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.163).

Erogazione

Nell'erogazione SOAP “TempConvertSoapIntegrityPDND”, relativa all'API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.76) necessari per validare l'header WSSecurity previsto dal pattern «INTEGRITY_SOAP_01».

La sezione «ModI Risposta» si utilizza per indicare i parametri per la produzione del token di sicurezza da inserire nel messaggio di risposta (Fig. 3.165).

3.4.4 Fruizione API SOAP

Obiettivo

Fruire di un servizio SOAP, definito tramite una interfaccia WSDL, accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_pdnd_integrity.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore devo anche presentare il token di sicurezza WSSecurity previsto dal pattern «INTEGRITY_SOAP_01» a garanzia dell'integrità del messaggio.

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 e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra fruitore ed erogatore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_SOAP_01».

API > TemperatureConversionIntegrityPDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale	
Pattern	<input type="text" value="ID_AUTH_CHANNEL_01"/> ▼
Direct Trust Transport-Level Security	
Sicurezza Messaggio	
Pattern	<input type="text" value="INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01"/> ▼
Integrità payload del messaggio	
Generazione Token	<input type="text" value="Authorization PDND"/> ▼
Token ID_AUTH negoziato con la PDND	
Applicabilità	<input type="text" value="Richiesta e Risposta"/> ▼
Digest Richiesta	<input type="checkbox"/> Non ripudiabilità della trasmissione 
Informazioni Audit	<input type="checkbox"/> Dati del dominio del fruitore

Figure3.163: Configurazione Pattern ModI «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» sulla API SOAP

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati	<input type="text" value="Default"/>
Time to Live	<input type="text" value="Default"/>
WSAddressing To	<input type="text" value="TempConvertSoap.ente.govway.org"/>

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

Figure3.164: Configurazione richiesta dell'erogazione

Modi - Risposta

Sicurezza Messaggio

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

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

Figure3.165: Configurazione risposta dell'erogazione

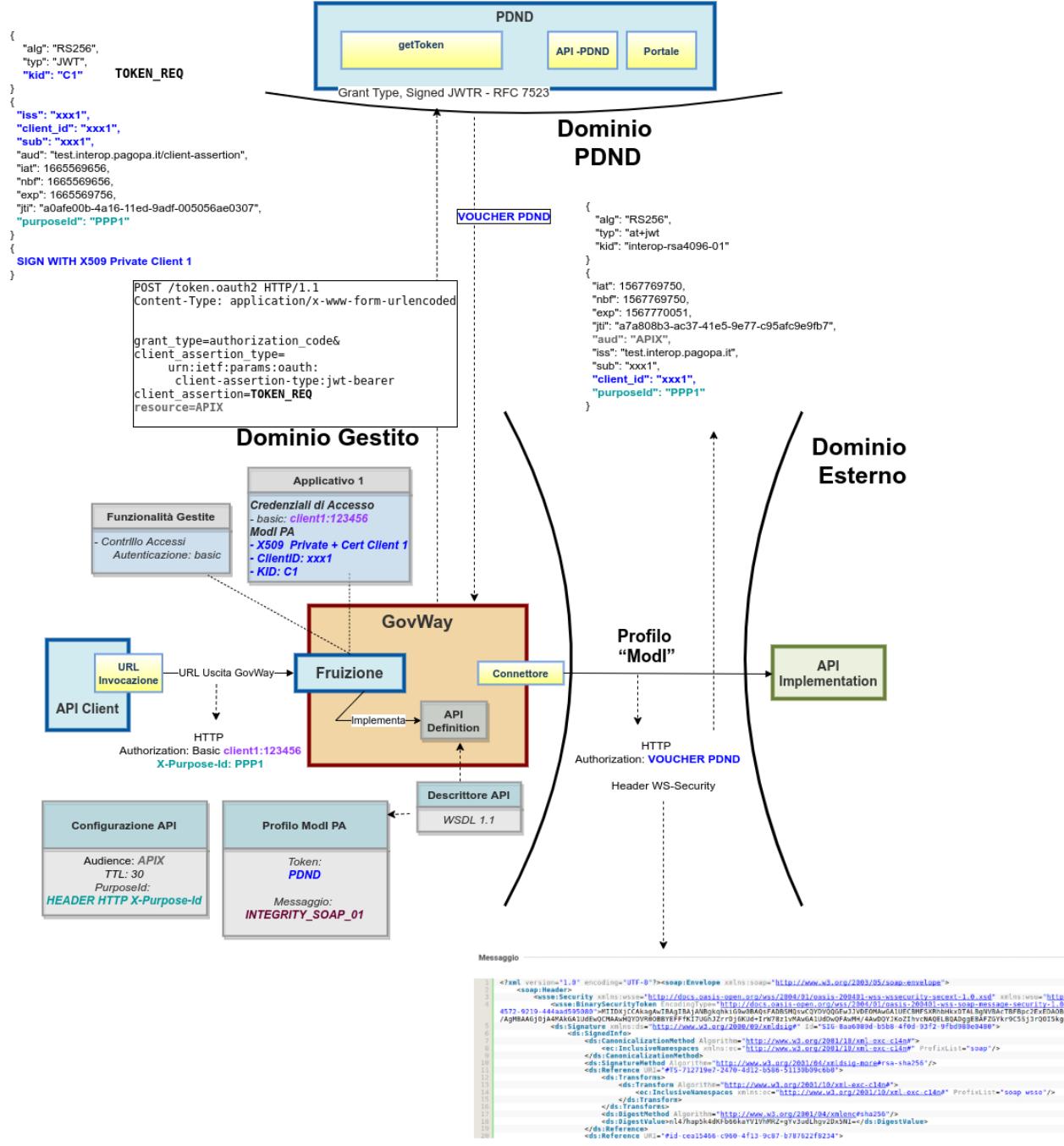


Figure3.166: Fruizione di una API SOAP con profilo "ModI", pattern INTEGRITY_SOAP_01 e pattern ID_AUTH_REST_01 via PDND

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

● **GovWay - Console di Monitoraggio**

Soggetto: Ente
Profilo: ModI

Figure3.167: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_SOAP_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Integrity+PDND - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

The screenshot shows the Postman interface with a configured API request. The left sidebar shows a tree structure of scenarios, with 'Profilo ModI SOAP' expanded. The main area shows a POST request to `{{govway-uri}}/soap/out/{{soggetto}}/{{soggettoEsterno}}/TempConvertSoap1`. The 'Auth' tab is selected, showing 'Basic Auth' selected. The 'Body' tab shows a SOAP message in XML format:

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3   <soap:Header>
4     <soap:Body>
5       <CelsiusToFahrenheitResponse xmlns="https://www.w3schools.com/xml/">
6         <CelsiusToFahrenheitResult>68</CelsiusToFahrenheitResult>
7       </CelsiusToFahrenheitResponse>
8     </soap:Body>
9   </soap:Envelope>

```

Figure3.168: Pattern Integrity+PDND - Fruizione API SOAP, esecuzione da Postman

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”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato all'erogatore, come in Fig. 3.169. Come si nota, il messaggio SOAP contiene nell'header WS-Security sia il token di sicurezza (elemento

«BinarySecurityToken») sia l'elemento «WSAddressing - To» e il digest del payload (elemento «DigestValue») prodotti dal fruitore con la relativa firma digitale (elemento «SignatureValue») come previsto dal pattern «INTEGRITY_SOAP_01».

Messaggio

Figure3.169: Messaggio inviato dal fruitore

Conformità ai requisiti ModI

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

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

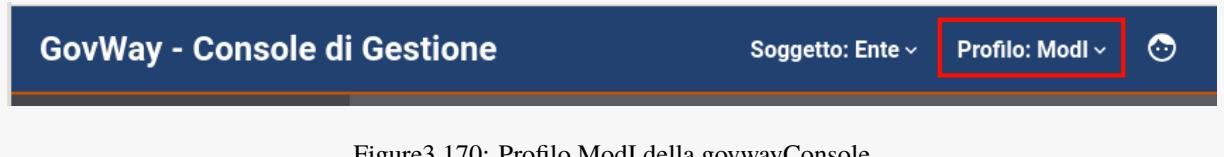


Figure3.170: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY SOAP 01».

Registrazione API

Viene registrata l'API «TemperatureConversionIntegrityPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_SOAP_01» con ID_AUTH_SOAP_01 (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.171).

Fruizione

Nella fruizione SOAP “TempConvertSoapIntegrityPDND”, relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.83) necessari a generare l’header WSSecurity previsto dal pattern «INTEGRITY_SOAP_01». In particolare è possibile specificare l’audience atteso dall’erogatore e il tempo di validità del token.

API > TemperatureConversionIntegrityPDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale	
Pattern	ID_AUTH_CHANNEL_01
Direct Trust Transport-Level Security	
Sicurezza Messaggio	
Pattern	INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01
Integrità payload del messaggio	
Generazione Token	Authorization PDND
Token ID_AUTH negoziato con la PDND	
Applicabilità	Richiesta e Risposta
Digest Richiesta	<input type="checkbox"/> Non ripudiabilità della trasmissione 
Informazioni Audit	<input type="checkbox"/> Dati del dominio del fruitore

Figure3.171: Configurazione Pattern ModI «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01» sulla API SOAP

ModI - Richiesta

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	Definito nell'applicativo
Time to Live (secondi) *	60
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token	
WSAddressing To	TempConvertSoap.enteEsterno.govway.org 
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	

Figure3.172: Configurazione richiesta della fruizione

La sezione «ModI Risposta» definisce i criteri per la validazione dei messaggi di risposta (Fig. 3.84).

3.5 Pattern “ID_AUTH” via PDND + “INTEGRITY_REST_02”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_idar04.

3.5.1 Erogazione API REST

Obiettivo

Esporre un servizio, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_idar04.

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_02» a garanzia dell'integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

Modi - Risposta

Sicurezza Messaggio

TrustStore Certificati	Default
Time to Live	Default
Verifica WSAddressing To	<input checked="" type="checkbox"/> La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente

Informazioni ⓘ

Figure3.173: Configurazione risposta della fruizione

1. un applicativo eroga un servizio, rivolto a fruitori di domini esterni, in conformità al Modello di Interoperabilità AGID e il servizio viene registrato sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_02»;
5. la validazione del token di integrità viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
6. vengono inoltre recuperate e associate alla traccia maggiori informazioni sull'organizzazione afferente al “client-id” presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Monitoraggio **Soggetto: Ente** **Profilo: ModI** ⓘ

Figure3.175: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_02».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IntegrityRest02+PDND - IN App3» che è stata preconfigurata per il funzionamento con le caratteristiche descritte

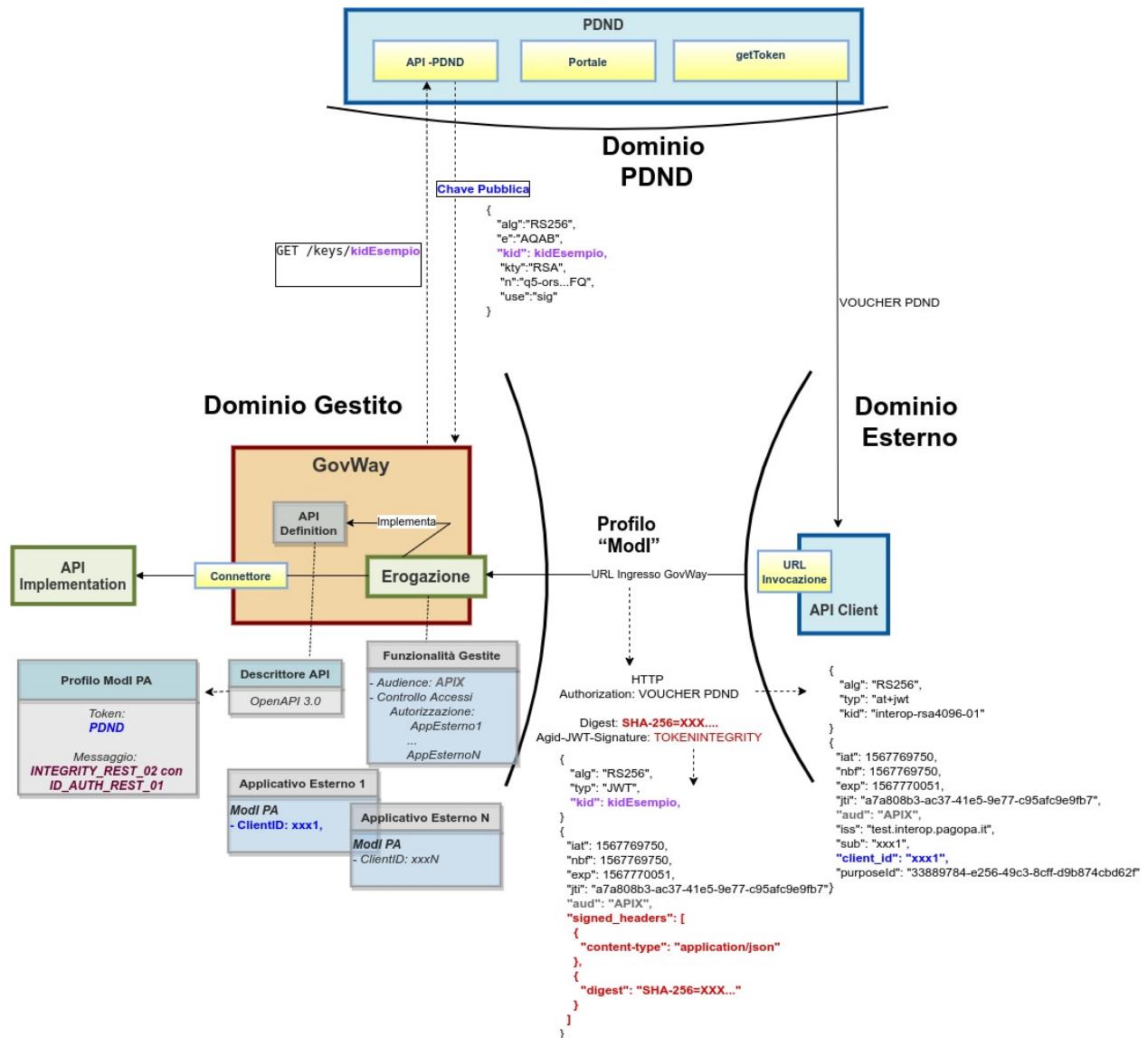


Figure3.174: Erogazione di una API REST con profilo “ModI”, pattern INTEGRITY_REST_02 e pattern ID_AUTH_REST_01 via PDND

sopra.

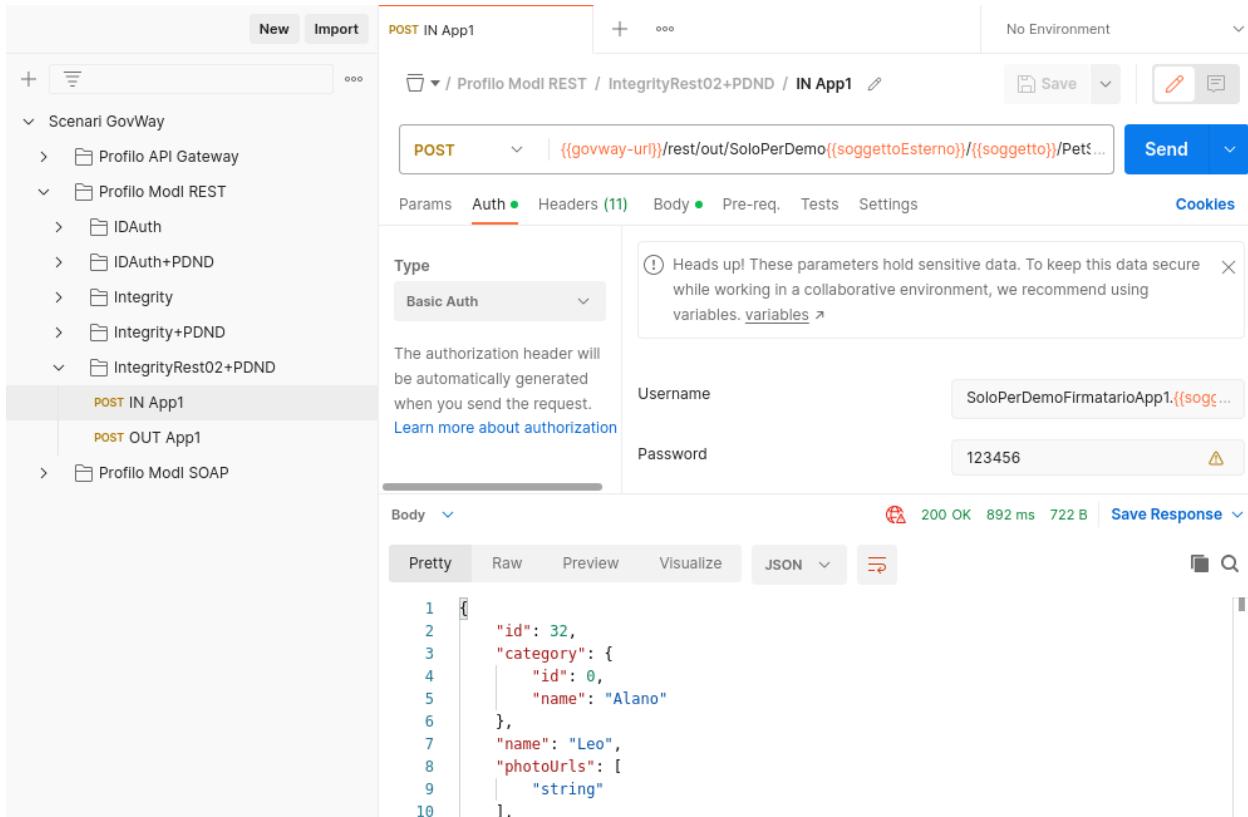


Figure3.176: Pattern IntegrityRest02+PDND - Erogazione API REST, esecuzione da Postman

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”.

Nota

Le informazioni ottenute tramite le modipa_passiPreliminari_api_pdnd (chiavi pubbliche JWK e informazioni sui client) vengono salvate su cache locali. Al fine di forzare nuove invocazioni verso la «PDND simulata» è necessario attendere un minuto rispetto a precedenti invocazioni ed effettuare il reset delle cache locali di GovWay accedendo alla sezione strumenti_runtime della console di gestione “govwayConsole” e cliccando sul link “Svuota tutte le Cache”.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario *Esecuzione*.

1. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.137. Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization» e «Agid-Jwt-Signature» che contengono rispettivamente il token di sicurezza che il fruitore ha ottenuto dalla PDND e il token di integrità. È inoltre presente l’header http «Digest» che contiene il valore per la verifica dell’integrità del payload.
2. Grazie alle configurazioni presenti nell’erogazione, ed in particolare all’indicazione che il token ricevuto deve essere validato tramite Token Policy PDND, GovWay è in grado di validare i dati di sicurezza ricevuti (Fig. 3.177) e decodificare il token.
3. Vengono inoltre validati gli ulteriori header «Agid-Jwt-Signature» e «Digest» rispetto al pattern

Headers

Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fbb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6xWqdhfvHBaJT3on7jaCV6LVEXEaqAqfDWwI48L8SextE3UyuuGh-1s-g632OH8j6SIFr8tzsK4p-Fc94Wc1xhMJxjXAer6Sh80
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsInq1Yyl6WyJNSilVuNpGcBUWGoh1dKhKCv6nd6LFjWiFSdExxjto5i8iBtyjExSu06iHLOiaD2pI1jkYrG37MgE6f-1xBYCqjElCchD6GQ8R4fEc5
Digest	SHA-256=OhjWochmylM/B4HeXiplNxygvqU7zKjERTUMDPVfhPY=
Accept	/*
Govway-Transaction-Id	d1a3b973-4fbb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

2022-10-20 11:06:27.473	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) in corso ...
2022-10-20 11:06:27.474	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) completata con successo

Figure3.177: Evidenza diagnostica della validazione del token

“INTEGRITY_REST_02” indicato nella configurazione dell’API (Fig. 3.178). La validazione del token di integrità viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd. Nello storico delle transazioni è possibile vedere come GovWay durante la gestione della richiesta di erogazione scaturisca un’ulteriore chiamata verso la PDND per ottenere la chiave pubblica (Fig. 3.179). La chiave pubblica una volta prelevata dalla PDND verrà aggiunta in una cache locale e le successive richieste non provocheranno ulteriori chiamate verso la PDND.

2023-06-12 16:38:57.663	infolntegration	Modi	Validazione security token Modi 'INTEGRITY' della richiesta in corso ...
2023-06-12 16:38:57.666	infolntegration	Modi	Validazione security token Modi 'INTEGRITY' della richiesta effettuata con successo

Figure3.178: Evidenza diagnostica della validazione del token di integrità

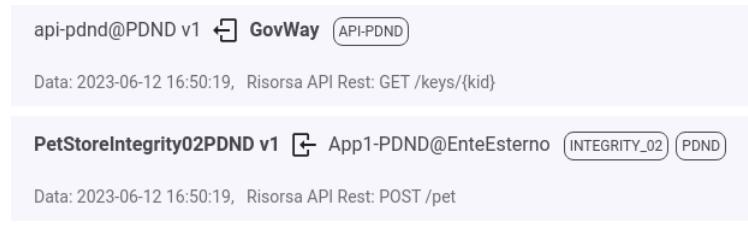


Figure3.179: Evidenza diagnostica della chiamata verso la PDND per ottenere la chiave pubblica

- Analizzando il token di integrità «Agid-Jwt-Signature» ricevuto nella sezione header (Fig. 3.180) si può notare che non viene riportata l’identità del fruttore tramite certificato X.509 come avveniva per il pattern INTEGRITY_REST_01 descritto nella scenario *Pattern “INTEGRITY_01”* ma bensì tramite il claim “kid” che corrisponde all’identificativo della chiave pubblica registrata sulla PDND. L’identificativo “kid” verrà utilizzato da GovWay per richiedere la chiave pubblica tramite le modipa_passiPreliminari_api_pdnd (Fig. 3.181). Nella sezione payload (Fig. 3.182) sono invece presenti gli header http firmati (tra cui il valore dell’header “Digest”) che servono a garantire l’integrità della richiesta, insieme ai riferimenti temporali (iat, nbf, exp) e all’audience (aud).

HEADER: ALGORITHM & TOKEN TYPE
<pre>{ "alg": "RS256", "typ": "JWT", "kid": "na06nCwyWQ1iEofx4j3iNRxMHM9Cb75IVXD_z27t2A" }</pre>

Figure3.180: Sezione «Header» del Token “Agid-Jwt-Signature” con pattern “INTEGRITY_REST_02”

- Vengono inoltre recuperate e associate alla traccia maggiori informazioni sull’organizzazione afferente al “client-id” presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd (Fig. 3.183). Nello storico delle transazioni è possibile vedere come GovWay durante la gestione della richiesta di erogazione scaturisca due ulteriori chiamate verso la PDND per ottenere maggiori informazioni sul client e sull’organizzazione (Fig. 3.184). Le informazioni recuperate dalla PDND verranno aggiunte in una cache locale e le successive richieste non provocheranno ulteriori chiamate verso la PDND.
- Le evidenze del processo di validazione relativo al pattern «INTEGRITY_REST_02» sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.185). Nella sezione «Sicurezza

Dettagli Transazione

Informazioni Generali Informazioni Mittente Dettagli Messaggio Diagnostici Informazioni Avanzate

Informazioni Mittente

Fruitore: Ente
 Applicativo Fruitore: GovWay
 ID Autenticato: GovWay
 Metodo HTTP: GET
 URL Invocazione: [out] /govway/rest/out/Ente/PDND/api-pdnd/v1/keys/[na06nCwyrWQ1iEofx4j3iNRxMHM9Cb75IVXD_z27t2A](#)
 Client IP: 127.0.0.1
 Codice Risposta Client: 200
 Credenziali: BasicUsername 'GovWay'

Token
 Token: [Visualizza](#)

Figure3.181: Dettaglio della url di invocazione utilizzata da GovWay per prelevare la chiave pubblica dalla PDND

PAYOUT: DATA

```
{
  "iat": 1686581418,
  "nbf": 1686581418,
  "exp": 1686581478,
  "jti": "6f603422-0930-11ee-8a0d-0242c0a88002",
  "aud": "petstore.ente.govway.org",
  "client_id": "App1-Esterno-PDND",
  "iss": "SoloPerDemoEnteEsterno",
  "sub": "SoloPerDemoFirmatarioApp1",
  "signed_headers": [
    {
      "digest": "SHA-256=0hjWocHmy1M/B4HeX1plNxygvqU7zKjERTUMDPVfhPY="
    },
    {
      "content-type": "application/json"
    }
  ]
}
```

Figure3.182: Sezione «Payload» del Token “Agid-Jwt-Signature” con pattern “INTEGRITY_REST_02”

Dettagli Transazione

[Informazioni Generali](#) [Informazioni Mittente](#) [Dettagli Messaggio](#) [Diagnostics](#) [Informazioni Avanzate](#)

Informazioni Mittente

Fruitore	EnteEsterno
Applicativo Fruitore	App1-PDND
ID Autenticato	/o=govway.org/c=it/cn=enteEsterno.govway.org/
Metodo HTTP	POST
URL Invocazione	[in] /govway/rest/in/Ente/PetStoreIntegrity02PDND/v1/pet
Client IP	192.168.128.2
X-Forwarded-For	192.168.128.2
Codice Risposta Client	200
Credenziali	SSL-Subject 'CN=enteEsterno.govway.org, O=govway.org, C=it' SSL-Issuer 'CN=GovWay CA, O=govway.org, C=it' SSL-ClientCert-SerialNumber '246'

Token

Issuer	https://govway.localdomain/auth/realm/master
Subject	3210f474-773c-44f6-a25b-8999c796f7c7
Client ID	App1-Esterno-PDND
Applicativo Client	App1-PDND
PDND Organization	Comune di Esempio category: Comuni e loro Consorzi e Associazioni externalId: IPA c_c000
Token	Visualizza

Figure3.183: Informazioni recuperate dalla PDND sull'organizzazione associata al "client-id"



Figure3.184: Evidenza diagnostica delle chiamate verso la PDND per ottenere maggiori informazioni sul “client-id”

Messaggio» sono riportate le informazioni estratte dai token di sicurezza presenti, tra cui si può notare il digest e gli header http firmati.

Conformità ai requisiti ModI

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

1. la sicurezza messaggio applicata è quella dei pattern «ID_AUTH_REST_01» via PDND» + «INTEGRITY_REST_02» come ampiamente mostrato precedentemente dove sono stati mostrati i token validati e i criteri autorizzativi;
2. la validazione del token di integrità viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
3. l'identificazione del fruttore avviene rispetto al claim “client_id” presente all'interno del token e ulteriori informazioni sull'organizzazione afferente vengono ottenute invocando le modipa_passiPreliminari_api_pdnd.

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.186: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_02».

Registrazione API

Informazioni Modelli	
Generazione Token	Authorization PDND
Sicurezza Messaggio	INTEGRITY_REST_02 con ID_AUTH_REST_01
Sicurezza Canale	ID_AUTH_CHANNEL_01
Interazione	Accesso CRUD
Sicurezza Messaggio	
Digest	SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
ClientId	App1-Esterno-PDND
Subject	SoloPerDemoFirmatarioApp1
Issuer	SoloPerDemoEnteEsterno
MessageId	6f603422-0930-11ee-8a0d-0242c0a88002
Audience	petstore.ente.govway.org
NotBefore	2023-06-12_16:50:18.000
Expiration	2023-06-12_16:51:18.000
IssuedAt	2023-06-12_16:50:18.000
Kid	na06nCwyrWQ1iEofx4j3iNRxMHM9Cb75IVXD_z27t2A
Headers HTTP Firmati	
content-type	application/json
digest	SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=

Figure3.185: Traccia della richiesta elaborata dall'erogatore, con pattern “INTEGRITY_REST_02”

Viene registrata l'API «PetStoreIntegrity02PDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_REST_02 con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.187).

API > PetStoreIntegrity02PDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

ModI

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_01

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern: INTEGRITY_REST_02 con ID_AUTH_REST_01

Integrità payload del messaggio

Generazione Token

Pattern: Authorization PDND

Token ID_AUTH negoziato con la PDND

Header HTTP del Token

Pattern: Agid-JWT-Signature + Authorization Bearer

Applicabilità

Pattern: Richiesta e Risposta

Digest Richiesta

Non ripudiabilità della trasmissione (i)

Informazioni Audit

Dati del dominio del fruitore

Figure3.187: Configurazione Pattern ModI «INTEGRITY_REST_02 con ID_AUTH_REST_01» sulla API REST

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 si desidera autorizzare qualsiasi fruitore proveniente dalla PDND, questo passo può anche essere omesso. La validazione del token è sufficiente a stabilire che il fruitore ha ottenuto un voucher dalla PDND valido per il servizio invocato. Questo scenario è quello preconfigurato.

- In alternativa è possibile configurare una autorizzazione puntuale procedendo alla registrazione degli applicativi fornendo i singoli “client_id” necessari all’identificazione (Fig. 3.188).

Applicativo

Profilo Interoperabilità	ModI
Dominio	Esterno
Soggetto	EnteEsterno
Nome *	<input type="text" value="App1-PDND"/>
Tipo	Client
Proprietà(0)	

Ruoli

visualizza(0)

ModI

Sicurezza Messaggio	<input type="text" value="Authorization PDND"/>
ClientId registrato sulla PDND	
Token Policy *	<input type="text" value="PDND"/>
Identificativo *	<input type="text" value="App1-Esterno-PDND"/>

Figure3.188: Configurazione applicativo esterno (fruitore)

Erogazione

Nell’erogazione «PetStoreIntegrity02PDND», relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.145) necessari per validare le richieste in ingresso relativamente al token “Agid-JWT-Signature”. Si noti come è stato selezionato un truststore basato sulla PDND al fine di scaricare la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

La sezione «ModI Risposta» si utilizza per indicare i parametri per la produzione del token di sicurezza “Agid-JWT-Signature” da inserire nel messaggio di risposta (Fig. 3.146). Si noti come è stato indicato nel campo «Key Id (kid) del Certificato» l’identificativo kid associato alla chiave pubblica registrata sulla PDND.

3.5.2 Fruzione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), accessibile in accordo al pattern di sicurezza descritto nella sezione modipa_idar04.

Sintesi

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati	<input type="text" value="Ridefinito"/>
Time to Live	<input type="text" value="Default"/>
Audience	<input type="text" value="petstore.ente.govway.org"/>

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

▼ **Coesistenza Token Authorization e Agid-JWT-Signature**

TrustStore Certificati

Tipo	<input type="text" value="PDND"/>
------	-----------------------------------

Figure3.189: Configurazione richiesta dell'erogazione

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore devo anche presentare il token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_02» a garanzia dell'integrità del messaggio.

La figura seguente descrive graficamente questo scenario.

Nella figura “Fig. 3.192” viene raffigurato lo scenario di fruizione durante la fase di validazione del token di risposta tramite un truststore dinamico in cui GovWay utilizza le modipa_passiPreliminari_api_pdnd per ottenere la chiave pubblica necessaria a validare il token di risposta.

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 e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND»;
4. l'integrità del messaggio scambiato è garantita tramite sicurezza messaggio aggiuntiva prevista nel pattern «INTEGRITY_REST_02»;
5. la validazione del token di integrità della risposta viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

Esecuzione

Nota

Modi - Risposta

Sicurezza Messaggio

Algoritmo: RS256

HTTP Headers da firmare *: Digest, Content-Type, Content-Encoding

KeyStore: Ridefinito

Time to Live (secondi) *: 300
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token della risposta

Claims: i

Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli

KeyStore

Modalità: File System

Tipo: PKCS12

Path *: /etc/govway/keys/keystore_app1.ente.pkcs12

Password *: 123456

Alias Chiave Privata *: app1.ente.govway.org

Password Chiave Privata *: 123456

Key Id (kid) del Certificato: zgC6JlcdjzdZkw-z6aSWltpKbY5ggqMTozwhQc7FU5M i

Identificativo: i

Figure3.190: Configurazione risposta dell'erogazione

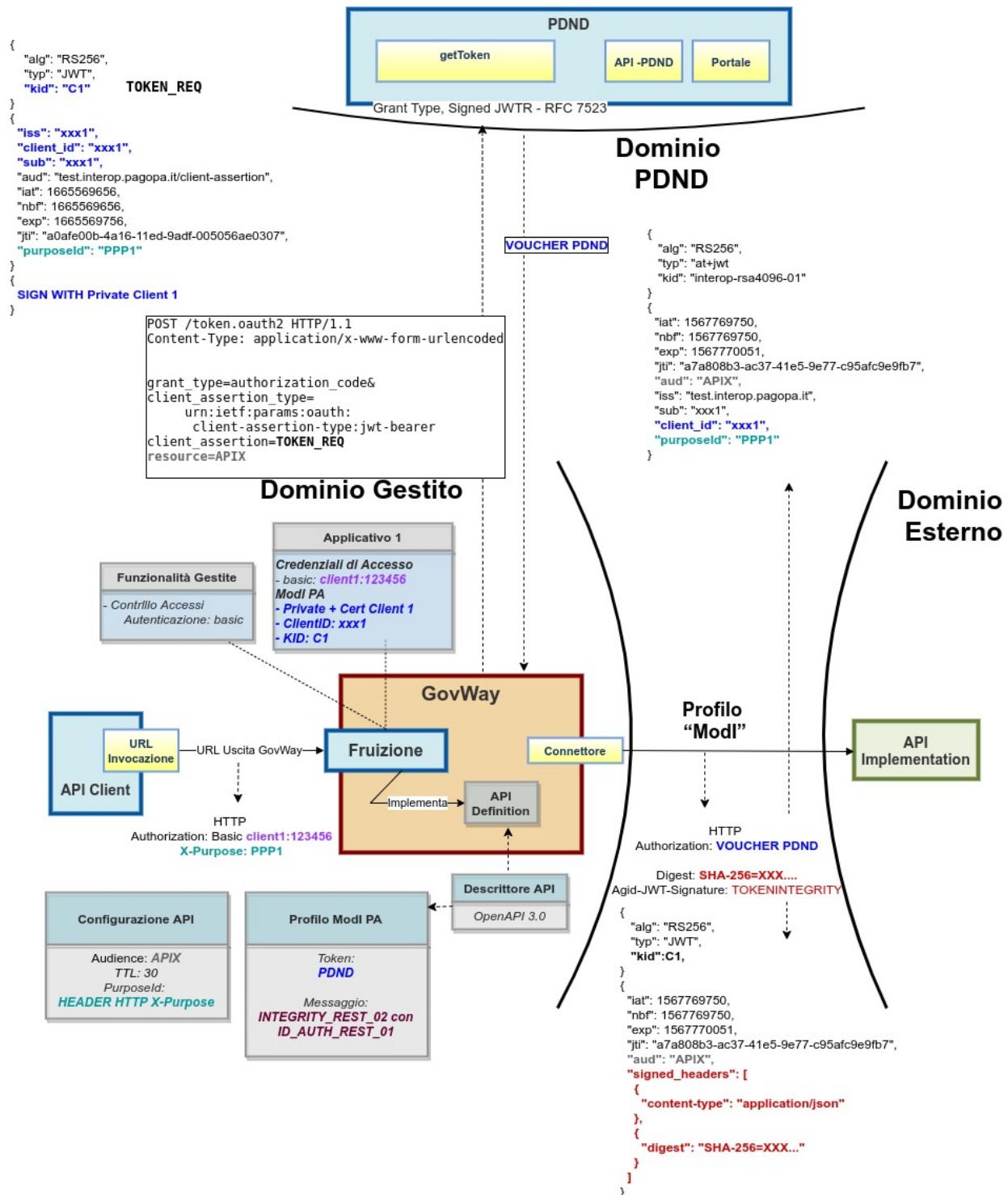


Figure3.191: Fruizione di una API REST con profilo “ModI”, pattern INTEGRITY_REST_02 e pattern ID_AUTH_REST_01 via PDND

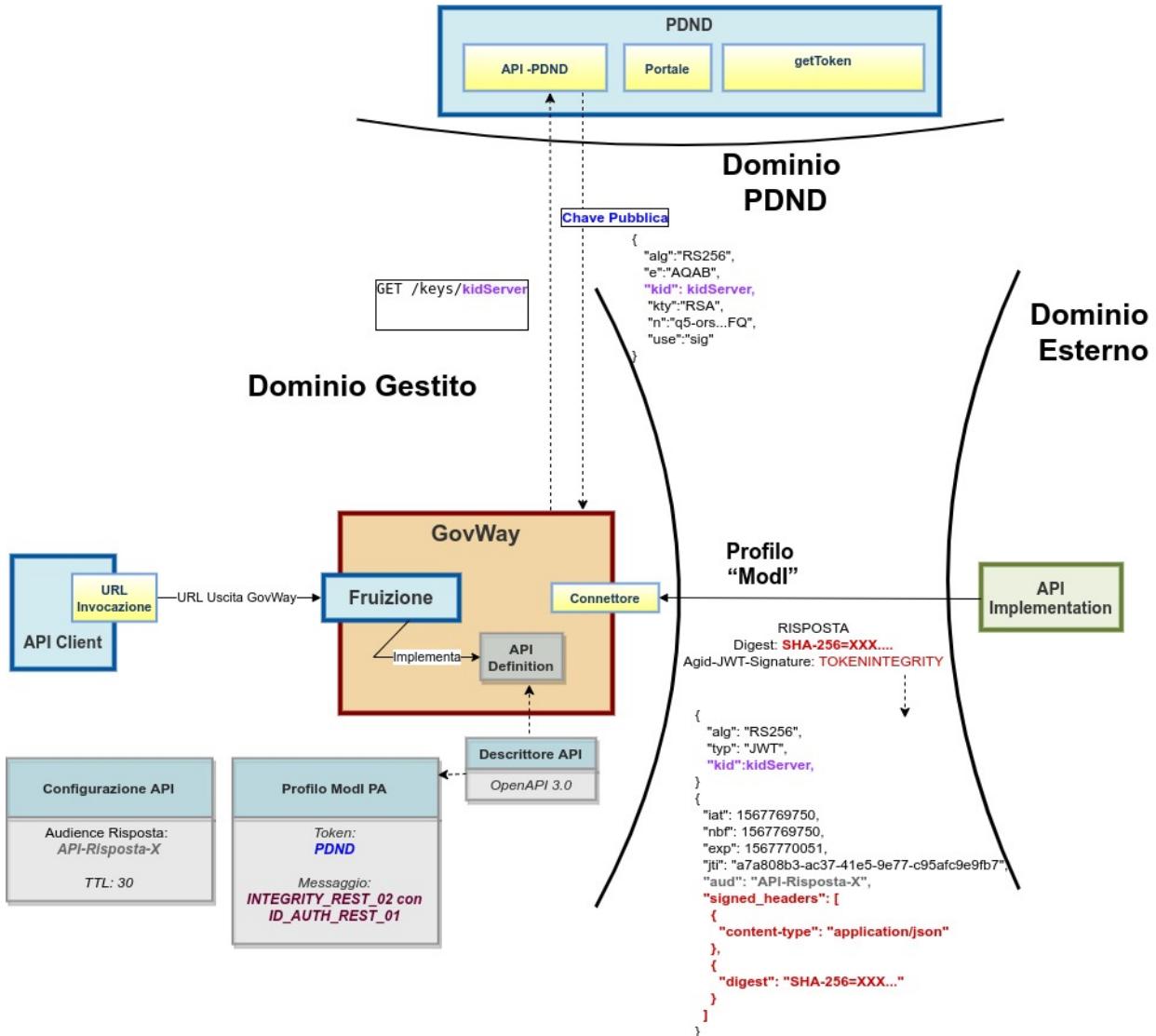


Figure3.192: Fruizione con Profilo di Interoperabilità “ModI”, pattern “INTEGRITY_REST_02”: utilizzo delle API PDND per ottenere la chiave pubblica per validare la risposta

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_02».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - IntegrityRest02+PDND - OUT App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

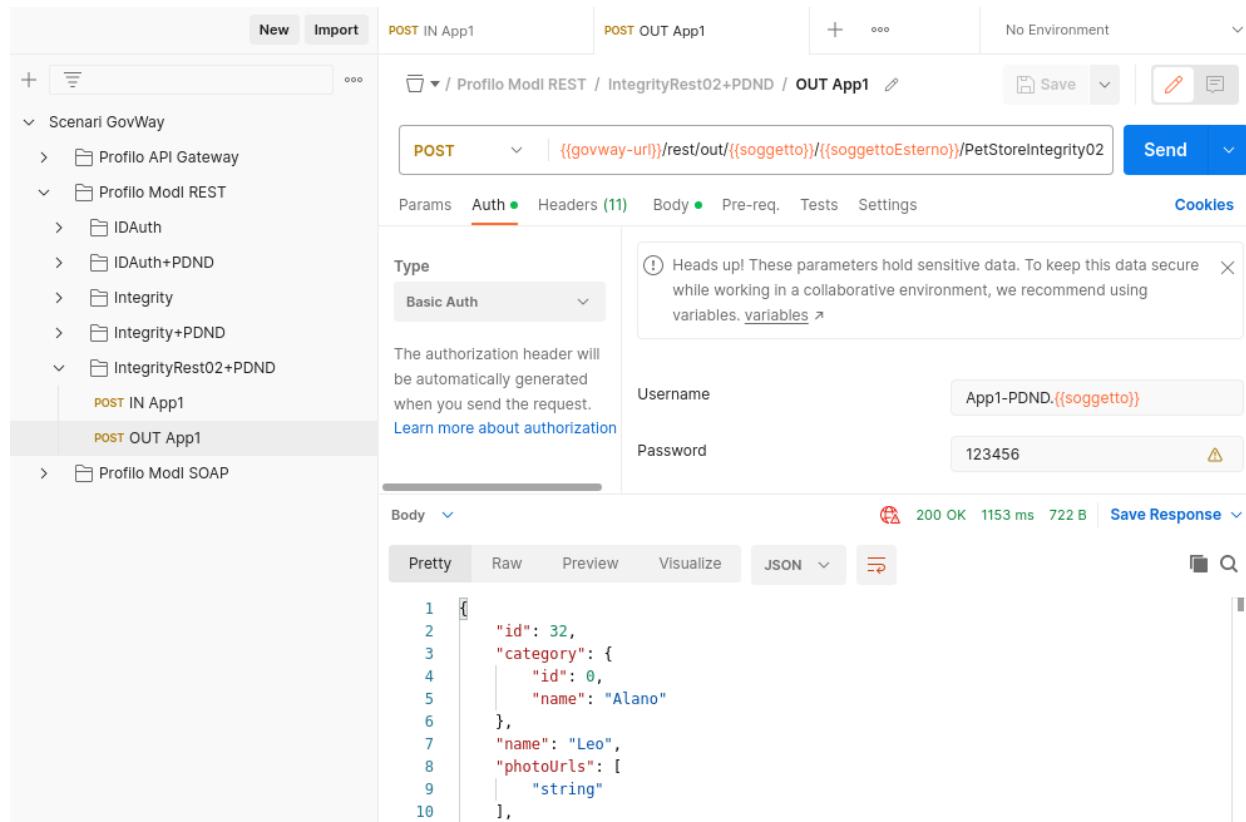


Figure3.194: Pattern IntegrityRest02+PDND - Esecuzione API REST, esecuzione da Postman

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 la console “govwayMonitor”.

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di sicurezza diverso utilizzato.

- 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 un token di sicurezza da inviare alla PDND con il

quale ottenere indietro un voucher spendibile per il servizio desiderato. Questa parte è stata ampiamente mostrata nella scenario [Esecuzione](#).

Oltre al token della PDND, GovWay produce un ulteriore token di sicurezza «Agid-JWT-Signature» previsto dal pattern «INTEGRITY_REST_02». Da govwayMonitor si può visualizzare il messaggio di richiesta in uscita che è il medesimo di quello in entrata con la differenza che sono stati aggiunti gli header HTTP «Authorization» e «Agid-Jwt-Signature» che contengono rispettivamente il token ottenuto dalla PDND e il token dell'integrità. È inoltre presente l'header http «Digest» che contiene il valore utilizzabile dall'erogatore per la verifica dell'integrità del payload. (Fig. 3.195).

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	d1b37101-4fbb-11ed-a5ac-0242ac140002
X-Forwarded-Server	411885f186f6
X-Real-Ip	172.20.0.1
Postman-Token	0ab5fecb-2b64-497f-9a8e-ff0a6dbd24ab
X-Forwarded-For	172.20.0.2
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsIn1YyI6xWqdhfvHBaJT3on7jaCV6LVEXEaqAqfDWwI48L8SextE3UyuuGh-1s-g632OH8j6SIf8tzsK4p-Fc94WclxhMJxjXAer6Sh80
Agid-Jwt-Signature	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImFwcDEuZW50ZWVzdGVybm8uZ292d2F5Lm9yZylsIn1YyI6WyJNSjIiVuNpGcBUWGoh1dKhKCv6nd6LFjWIFsdExxjto5i8iBtyjExSu06IHL0iaD2pI1jkYrG37MgE6f-1xBYCqlEICchD6GQ8R4fEc5
Digest	SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
Accept	*/*
Govway-Transaction-Id	d1a3b973-4fbb-11ed-a5ac-0242ac140002
Transfer-Encoding	chunked

Figure3.195: Messaggio di richiesta in uscita (con token di sicurezza inseriti nell'header HTTP)

- L'header e i payload del token «Agid-JWT-Signature» sono identici a quelli già visualizzati nello scenario di erogazione REST, relativamente al messaggio in ingresso (Fig. 3.180 e Fig. 3.182). Le informazioni inserite nel token vengono anche tracciate e sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.196). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di sicurezza, tra cui si può notare il digest e gli header http firmati.
- Vengono inoltre validati anche gli header «Agid-Jwt-Signature» e «Digest» presenti nella risposta rispetto al pattern «INTEGRITY_REST_02» indicato nella configurazione dell'API (Fig. 3.197). La validazione del token

Informazioni Modl

Generazione Token Authorization PDND
Sicurezza Messaggio INTEGRITY_REST_02 con ID_AUTH_REST_01
Sicurezza Canale ID_AUTH_CHANNEL_01
Interazione 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
Kid zgC6JlcdjzdZkw-z6aSWltpKbY5ggqMTozwhQc7FU5M
Digest SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=
Subject App1-PDND
Issuer Ente
ClientId App1-PDND
Audience petstore.enteEsterno.govway.org
MessageId 07b59acc-0936-11ee-8a0d-0242c0a88002
Expiration 2023-06-12_18:40:58.000
NotBefore 2023-06-12_18:35:58.000
IssuedAt 2023-06-12_18:35:58.000

Headers HTTP Firmati

content-type application/json
digest SHA-256=OhjWocHmyIM/B4HeXlpINxygvqU7zKjERTUMDPVfhPY=

Figure3.196: Traccia della richiesta generata dal fruitore

di integrità della risposta viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd. Nello storico delle transazioni è possibile vedere come GovWay durante la gestione della richiesta di fruizione scaturisca un'ulteriore chiamata verso la PDND per ottenere la chiave pubblica (Fig. 3.179). La chiave pubblica una volta prelevata dalla PDND verrà aggiunta in una cache locale e le successive richieste non provocheranno ulteriori chiamate verso la PDND.

2023-06-12 18:35:59.105	infolntegration	ModI	Validazione security token ModI 'INTEGRITY' della risposta in corso ...
2023-06-12 18:35:59.166	infolntegration	InoltroBuste	Ricezione dati della risposta completata
2023-06-12 18:35:59.167	infolntegration	ModI	Validazione security token ModI 'INTEGRITY' della risposta effettuata con successo

Figure3.197: Evidenza diagnostica della validazione del token di integrità della risposta

api-pdnd@PDND v1	GovWay	API-PDND
Data: 2023-06-12 18:35:59, Risorsa API Rest: GET /keys/{kid}		
PetStoreIntegrity02PDND@EnteEsterno v1	App1-PDND	INTEGRITY_02 PDND
Data: 2023-06-12 18:35:58, Risorsa API Rest: POST /pet		

Figure3.198: Evidenza diagnostica della chiamata verso la PDND per ottenere la chiave pubblica con cui è stato firmato il token integrity di risposta

Nota

Le informazioni ottenute tramite le modipa_passiPreliminari_api_pdnd (chiavi pubbliche JWK) vengono salvate su cache locali. Al fine di forzare nuove invocazioni verso la «PDND simulata» è necessario attendere un minuto rispetto a precedenti invocazioni ed effettuare il reset delle cache locali di GovWay accedendo alla sezione strumenti_runtime della console di gestione “govwayConsole” e cliccando sul link “Svuota tutte le Cache”.

Conformità ai requisiti ModI

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

1. viene effettuata una negoziazione del voucher PDND come mostrato nelle tracce relative ai token scambiati con la PDND;
2. l'invocazione del servizio avviene fornendo il voucher della PDND precedentemente negoziato;
3. vengono inoltre prodotti gli header http «Agid-Jwt-Signature» e «Digest» previsti dal pattern di sicurezza «INTEGRITY_REST_02»;
4. la validazione del token di integrità della risposta viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

Configurazione

Nota

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». Si suggerisce

inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.199: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «INTEGRITY_REST_02».

Registrazione API

Viene registrata l'API «PetStoreIntegrity02PDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «INTEGRITY_REST_02 con ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND» (Fig. 3.200).

Fruizione

Nella fruizione «PetStoreIntegrity02PDND», relativa all'API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.201) necessari a generare il token “Agid-JWT-Signature”. In particolare è possibile specificare l'audience atteso dall'erogatore e il tempo di validità del token.

La sezione «ModI Risposta» definisce i criteri per la validazione del token di sicurezza “Agid-JWT-Signature” presente nel messaggio di risposta, come il truststore per l'autenticazione dell'erogatore (Fig. 3.202). Si noti come è stato selezionato un truststore basato sulla PDND al fine di scaricare la chiave pubblica, corrispondente al kid presente nel token della risposta, tramite le modipa_passiPreliminari_api_pdnd.

3.6 Pattern “AUDIT_REST_01”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_infoUtente_audit01.

3.6.1 Erogazione API REST

Obiettivo

Esporre un servizio, definito tramite una API REST (OpenAPI 3.0), che richieda per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit01.

Nota

Il token descritto nel pattern modipa_infoUtente_audit01 va in aggiunta rispetto agli altri token di sicurezza e quindi può essere utilizzato in combinazione con qualsiasi dei token descritti nei precedenti scenari, anche senza la PDND. In questo scenario verrà utilizzato insieme al token “Authorization” ottenuto tramite la PDND, descritto negli scenari *Pattern “ID_AUTH” via PDND*.

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

API > PetStoreIntegrity02PDND v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi

Sicurezza Canale	
Pattern	ID_AUTH_CHANNEL_01
Direct Trust Transport-Level Security	
Sicurezza Messaggio	
Pattern	INTEGRITY_REST_02 con ID_AUTH_REST_01
Integrità payload del messaggio	
Generazione Token	Authorization PDND
Token ID_AUTH negoziato con la PDND	
Header HTTP del Token	Agid-JWT-Signature + Authorization Bearer
Applicabilità	Richiesta e Risposta
Digest Richiesta	<input type="checkbox"/> Non ripudiabilità della trasmissione (i)
Informazioni Audit	<input type="checkbox"/> Dati del dominio del fruitore

Figure3.200: Configurazione Pattern ModI «INTEGRITY_REST_02 con ID_AUTH_REST_01» sulla API REST

Modi - Richiesta

Sicurezza Messaggio

Algoritmo	RS256
HTTP Headers da firmare *	Digest <input checked="" type="checkbox"/> Content-Type <input checked="" type="checkbox"/> Content-Encoding <input checked="" type="checkbox"/>
KeyStore	Definito nell'applicativo
Time to Live (secondi) *	300
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token	
Audience	petstore.enteEsterno.govway.org 
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	
Claims	
Indicare per riga i claims (nome=valore); visualizzare 'info' per maggiori dettagli	

Figure3.201: Configurazione richiesta della fruizione

Modi - Risposta

Sicurezza Messaggio

TrustStore Certificati	Ridefinito
Time to Live	Default
Verifica Audience	<input checked="" type="checkbox"/> La verifica utilizza, se configurato, il valore indicato di seguito altrimenti quello configurato nell'applicativo mittente
	

TrustStore Certificati

Tipo	PDND
------	------

Figure3.202: Configurazione risposta della fruizione

ad illustrare lo scenario in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_01».

La figura seguente descrive graficamente questo scenario.

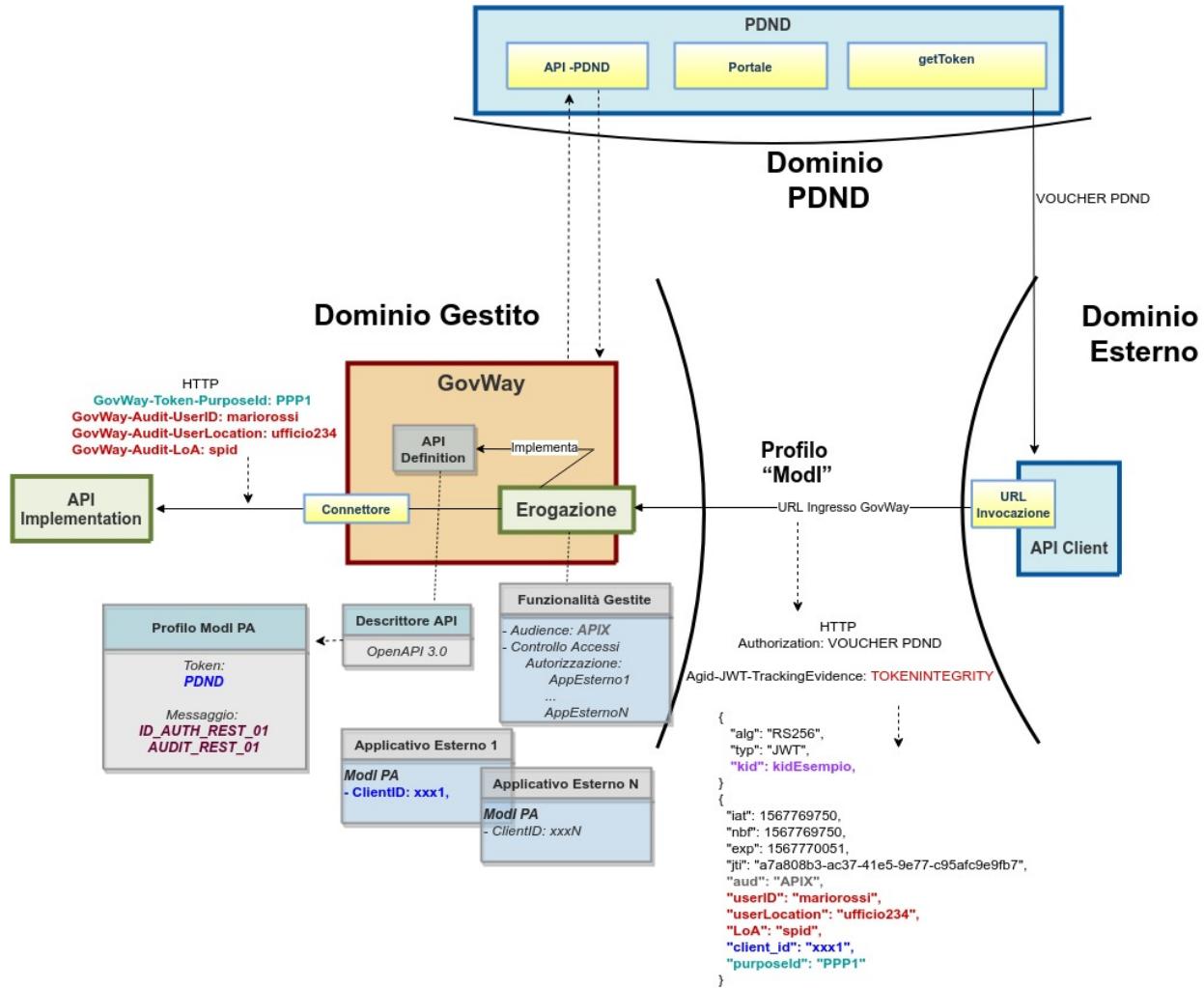


Figure3.203: Erogazione di una API REST con profilo “Modi”, pattern AUDIT_REST_01 e pattern ID_AUTH_REST_01 via PDND

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 e il servizio viene registrato sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND»;
4. per la fruizione viene richiesto un token aggiuntivo, conforme al pattern «AUDIT_REST_01», adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore;

5. la validazione del token di audit viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
6. vengono inoltre recuperate e associate alla traccia maggiori informazioni sull'organizzazione afferente al "client-id" presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console "govwayMonitor", nel menù in alto a destra il Profilo di Interoperabilità "ModI". Si suggerisce inoltre di selezionare il soggetto "Ente" per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.

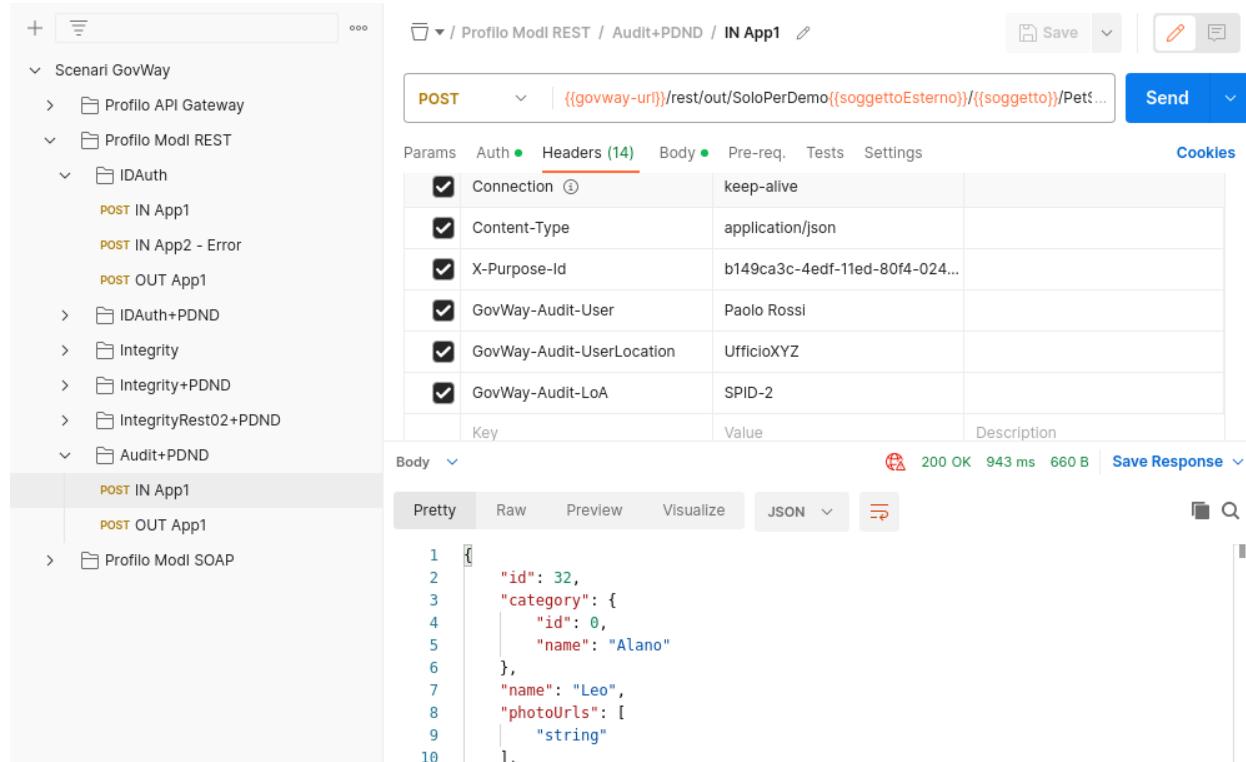
GovWay - Console di Monitoraggio

Soggetto: Ente
Profilo: ModI

Figure3.204: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione* con la sola eccezione del pattern di audit aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Audit+PDND - IN App1» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.



The screenshot shows the Postman interface with the following details:

- Left Sidebar:** Shows a tree structure under "Scenari GovWay". The "Profilo ModI REST" node is expanded, showing sub-nodes for "IDAuth", "IDAuth+PDND", "Integrity", "Integrity+PDND", "IntegrityRest02+PDND", and "Audit+PDND".
- Request Details:**
 - Method:** POST
 - URL:** {{govway-url}}/rest/out/SoloPerDemo({{soggettoEsterno}})/{{soggetto}}/Pet...
 - Headers:** (14) (highlighted in red)
 - Connection: keep-alive
 - Content-Type: application/json
 - X-Purpose-Id: b149ca3c-4edf-11ed-80f4-024...
 - GovWay-Audit-User: Paolo Rossi
 - GovWay-Audit-UserLocation: UfficioXYZ
 - GovWay-Audit-LoA: SPID-2
 - Body:** (Pretty, Raw, Preview, Visualize, JSON)
 - Body content (Pretty):

```

1  {
2   "id": 32,
3   "category": {
4     "id": 0,
5     "name": "Alano"
6   },
7   "name": "Leo",
8   "photoUrls": [
9     "string"
10    ],

```
- Status Bar:** 200 OK 943 ms 660 B Save Response

Figure3.205: Pattern Audit+PDND - Erogazione API REST, esecuzione da Postman

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”.

Nota

Le informazioni ottenute tramite le modipa_passiPreliminari_api_pdnd (chiavi pubbliche JWK e informazioni sui client) vengono salvate su cache locali. Al fine di forzare nuove invocazioni verso la «PDND simulata» è necessario attendere un minuto rispetto a precedenti invocazioni ed effettuare il reset delle cache locali di GovWay accedendo alla sezione strumenti_runtime della console di gestione “govwayConsole” e cliccando sul link “*Svuota tutte le Cache*”.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario *Esecuzione*.

1. Dal dettaglio della richiesta si può visualizzare il messaggio che è stato inviato dal fruitore, come in Fig. 3.206. Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali «Authorization» e «Agid-Jwt-TrackingEvidence» che contengono rispettivamente il token di sicurezza che il fruitore ha ottenuto dalla PDND e il token di audit.

Headers

Nome	
Content-Type	application/json
Govway-Message-Id	65ef0893-09c7-11ee-893d-0242c0a8a002
X-Forwarded-Server	2ceae888c6d1
X-Real-Ip	192.168.160.1
Postman-Token	912a7384-6c33-4e70-8a90-63ee382a2b18
X-Forwarded-For	192.168.160.2
X-Purpose-Id	b149ca3c-4edf-11ed-80f4-0242ac140002
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NiIsInR5cClgOiAiSldeUliwia2IkliA6ICJV0NHTzVac0VxeVBXenpxZ3RURkNYViBwWW
Agid-Jwt-TrackingEvidence	eyJhbGciOiJSUzI1NiIsInR5cCl6IkpxVCIsImtpZCI6Im5hMDZuQ3d5cldRMWIFb2Z4NGozaU5SeE1ITTDYjc1SVZ
Pragma	no-cache
Accept-Encoding	gzip, deflate, br

Figure3.206: Evidenza diagnostica degli header «Authorization» e «Agid-Jwt-TrackingEvidence»

2. Grazie alle configurazioni presenti nell’erogazione, ed in particolare all’indicazione che il token ricevuto deve essere validato tramite Token Policy PDND, GovWay è in grado di validare i dati di sicurezza ricevuti (Fig. 3.207) e decodificare il token.

2022-10-20 11:06:27.473	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) in corso ...
2022-10-20 11:06:27.474	infolntegration	RicezioneBuste	Gestione Token [PDND] (Validazione JWT) completata con successo

Figure3.207: Evidenza diagnostica della validazione del token

3. Viene inoltre validato l’ulteriore header «Agid-Jwt-TrackingEvidence» rispetto al pattern “AUDIT_REST_01” indicato nella configurazione dell’API (Fig. 3.208). La validazione del token di audit viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd. Nello storico delle transazioni è possibile vedere come GovWay durante la gestione della richiesta di erogazione scaturisca un’ulteriore chiamata verso la PDND per ottenere la chiave pubblica (Fig. 3.209). La chiave pubblica una volta prelevata dalla PDND verrà aggiunta in una cache locale e le successive richieste non provocheranno ulteriori chiamate verso la PDND.

2023-06-13 10:58:52.965	infolntegration	Modl	Validazione security token Modl 'AUDIT' della richiesta in corso ...
2023-06-13 10:58:53.018	infolntegration	Modl	Validazione security token Modl 'AUDIT' della richiesta effettuata con successo

Figure3.208: Evidenza diagnostica della validazione del token di audit

api-pdnd@PDND v1	←	GovWay@Ente	API-PDND
Data: 2023-06-13 10:58:52, Risorsa API Rest: GET /keys/{kid}			
PetStoreAuditPDND@Ente v1	←	App1-PDND@EnteEsterno	AUDIT_01 PDND
Data: 2023-06-13 10:58:52, Risorsa API Rest: POST /pet			

Figure3.209: Evidenza diagnostica della chiamata verso la PDND per ottenere la chiave pubblica

4. Analizzando il token di audit «Agid-Jwt-TrackingEvidence» ricevuto nella sezione header (Fig. 3.210) si può notare la presenza del claim “kid” che corrisponde all’identificativo della chiave pubblica registrata sulla PDND. L’identificativo “kid” verrà utilizzato da GovWay per richiedere la chiave pubblica tramite le modipa_passiPreliminari_api_pdnd (Fig. 3.211). Nella sezione payload (Fig. 3.212) sono invece presenti le informazioni utili all’erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore (userId, userLocation, LoA), insieme ai riferimenti temporali (iat, nbf, exp), all’audience (aud) e al “purposeId” utilizzato dal fruitore per richiedere il token di autorizzazione alla PDND.
5. Vengono inoltre recuperate e associate alla traccia maggiori informazioni sull’organizzazione afferente al “client-id” presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd (Fig. 3.213). Nello storico delle transazioni è possibile vedere come GovWay durante la gestione della richiesta di erogazione scaturisca due ulteriori chiamate verso la PDND per ottenere maggiori informazioni sul client e sull’organizzazione (Fig. 3.214). Le informazioni recuperate dalla PDND verranno aggiunte in una cache locale e le successive richieste non provocheranno ulteriori chiamate verso la PDND.
6. Le evidenze del processo di validazione relativo al pattern «AUDIT_REST_01» sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.215). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di sicurezza presenti, tra cui si può notare le informazioni sull’utente fruitore.
7. Esaminando il messaggio inoltrato al backend è possibile vedere come tra gli header HTTP inoltrati vi sia l’header “GovWay-Token-PurposeId” contenente il valore del claim “purposeId” presente sia nel token ricevuto dalla PDND che nel token di audit e gli header “GovWay-Audit-UserID”, “GovWay-Audit-UserLocation” e “GovWay-Audit-LoA” presenti nel token di audit (Fig. 3.216).

```
HEADER: ALGORITHM & TOKEN TYPE

{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "na06nCwyWQ1iEofx4j3iNRxMHM9Cb75IVXD_z27t2A"
}
```

Figure3.210: Sezione «Header» del Token “Agid-Jwt-TrackingEvidence” con pattern “AUDIT_REST_01”

Dettagli Transazione

Informazioni Generali Informazioni Mittente Dettagli Messaggio Diagnostici Informazioni Avanzate

Informazioni Mittente

Fruitore Ente
 Applicativo Fruitore GovWay
 ID Autenticato GovWay
 Metodo HTTP GET
 URL Invocazione [out] /govway/rest/out/Ente/PDND/api-pdnd/v1/keys/**na06nCwyWQ1iEofx4j3iNRxMHM9Cb75IVXD_z27t2A**
 Client IP 127.0.0.1
 Codice Risposta Client 200
 Credenziali BasicUsername 'GovWay'

Token

Token [Visualizza](#)

Figure3.211: Dettaglio della url di invocazione utilizzata da GovWay per prelevare la chiave pubblica, utilizzata per firmare il token di audit, dalla PDND

```

PAYLOAD: DATA

{
  "iat": 1686646732,
  "nbf": 1686646732,
  "exp": 1686647032,
  "jti": "65efa4d6-09c7-11ee-893d-0242c0a8a002",
  "aud": "petstore.ente.govway.org",
  "userID": "Paolo Rossi",
  "userLocation": "UfficioXYZ",
  "LoA": "SPID-2",
  "iss": "App1-Esterno-PDND",
  "purposeId": "b149ca3c-4edf-11ed-80f4-0242ac140002"
}

```

Figure3.212: Sezione «Payload» del Token “Agid-Jwt-TrackingEvidence” con pattern “AUDIT_REST_01”

Conformità ai requisiti ModI

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

1. la sicurezza messaggio applicata è quella dei pattern «ID_AUTH_REST_01 via PDND» + «AUDIT_REST_01» come ampiamente mostrato precedentemente dove sono stati mostrati i token validati e i criteri autorizzativi;
2. la validazione del token di audit viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
3. l'identificazione del fruitore avviene rispetto al claim “client_id” presente all'interno del token e ulteriori informazioni sull'organizzazione afferente vengono ottenute invocando le modipa_passiPreliminari_api_pdnd;
4. le informazioni sul fruitore presenti nel token di audit vengono aggiunte alla traccia.

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.217: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Dettagli Transazione

[Informazioni Generali](#) [Informazioni Mittente](#) [Dettagli Messaggio](#) [Diagnostici](#) [Informazioni Avanzate](#)

Informazioni Mittente

Fruitore EnteEsterno
Applicativo Fruitore App1-PDND
ID Autenticato /o=govway.org/c=it/cn=enteEsterno.govway.org/
Metodo HTTP POST
URL Invocazione [in] /govway/rest/in/Ente/PetStoreAuditPDND/v1/pet
Client IP 192.168.160.2
X-Forwarded-For 192.168.160.2
Codice Risposta Client 200
Credenziali SSL-Subject 'CN=enteEsterno.govway.org, O=govway.org, C=it'
 SSL-Issuer 'CN=GovWay CA, O=govway.org, C=it'
 SSL-ClientCert-SerialNumber '246'

Token

Issuer https://govway.localdomain/auth/realm/master
Subject 3210f474-773c-44f6-a25b-8999c796f7c7
Client ID App1-Esterno-PDND
Applicativo Client App1-PDND
PDND Organization Comune di Esempio
 category: Comuni e loro Consorzi e Associazioni
 externalId: IPA c_c000

Token [Visualizza](#)

Figure3.213: Informazioni recuperate dalla PDND sull'organizzazione associata al “client-id”



Figure3.214: Evidenza diagnostica delle chiamate verso la PDND per ottenere maggiori informazioni sul “client-id”

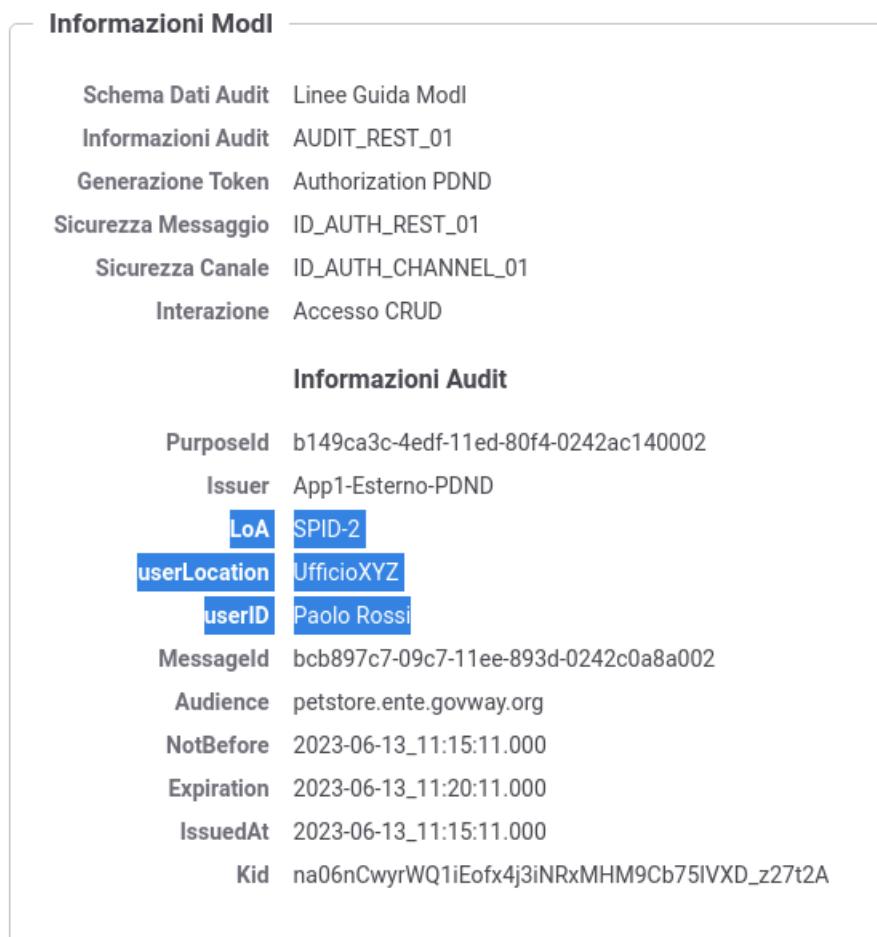


Figure3.215: Traccia della richiesta elaborata dall’erogatore, con pattern “AUDIT_REST_01”

Headers	
Nome	
X-Forwarded-Server	2ceae888c6d1
GovWay-Audit-UserLocation	UfficioXYZ
GovWay-Audit-UserID	Paolo Rossi
GovWay-Token-PurposeId	b149ca3c-4edf-11ed-80f4-0242ac140002
GovWay-Audit-LoA	SPID-2
User-Agent	GovWay

Figure3.216: Header HTTP “GovWay-Token-PurposeId”, “GovWay-Audit-UserID”, “GovWay-Audit-UserLocation” e “GovWay-Audit-LoA” inoltrati al backend

Registrazione API

Viene registrata l’API «PetStoreAuditPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l’opzione “Informazioni Audit” e selezionato il pattern «AUDIT_REST_01» e lo schema dei dati «Linee Guida ModI» (Fig. 3.218). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

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 si desidera autorizzare qualsiasi fruitore proveniente dalla PDND, questo passo può anche essere omesso. La validazione del token è sufficiente a stabilire che il fruitore ha ottenuto un voucher dalla PDND valido per il servizio invocato. Questo scenario è quello preconfigurato.
- In alternativa è possibile configurare una autorizzazione puntuale procedendo alla registrazione degli applicativi fornendo i singoli “client_id” necessari all’identificazione (Fig. 3.219).

Erogazione

Nell’erogazione «PetStoreAuditPDND», relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.220) necessari per validare le richieste in ingresso relativamente al token “Agid-JWT-TrackingEvidence”. Si noti come è stato selezionato un truststore basato sulla PDND al fine di scaricare la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

Modi

Sicurezza Canale

Pattern ▼

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern ▼

Direct Trust con certificato X.509

Generazione Token ▼

Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Informazioni Audit

Pattern ▼

Schema Dati ▼ ⓘ

Opzionale

Figure3.218: Configurazione Pattern ModI «AUDIT_REST_01» sulla API REST

Applicativo

Profilo Interoperabilità	Modl
Dominio	Esterno
Soggetto	EnteEsterno
Nome *	<input type="text" value="App1-PDND"/>
Tipo	Client
Proprietà(0)	

Ruoli

[visualizza\(0\)](#)

Modi

Sicurezza Messaggio	<input type="text" value="Authorization PDND"/>
ClientId registrato sulla PDND	
Token Policy *	<input type="text" value="PDND"/>
Identificativo *	<input type="text" value="App1-Esterno-PDND"/>

Figure3.219: Configurazione applicativo esterno (fruitore)

Erogazioni > PetStoreAuditPDND@Ente v1 > Profilo Interoperabilità

Profilo Interoperabilità

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati	<input type="text" value="Ridefinito"/>
Time to Live	<input type="text" value="Default"/>
Audience	<input type="text" value="petstore.ente.govway.org"/>

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

▼ **Informazioni Audit**

TrustStore Certificati

Tipo	<input type="text" value="PDND"/>
------	-----------------------------------

Figure3.220: Configurazione richiesta dell'erogazione

3.6.2 Fruizione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), che richiede per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit01.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore deve anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_01».

La figura seguente descrive graficamente questo scenario.

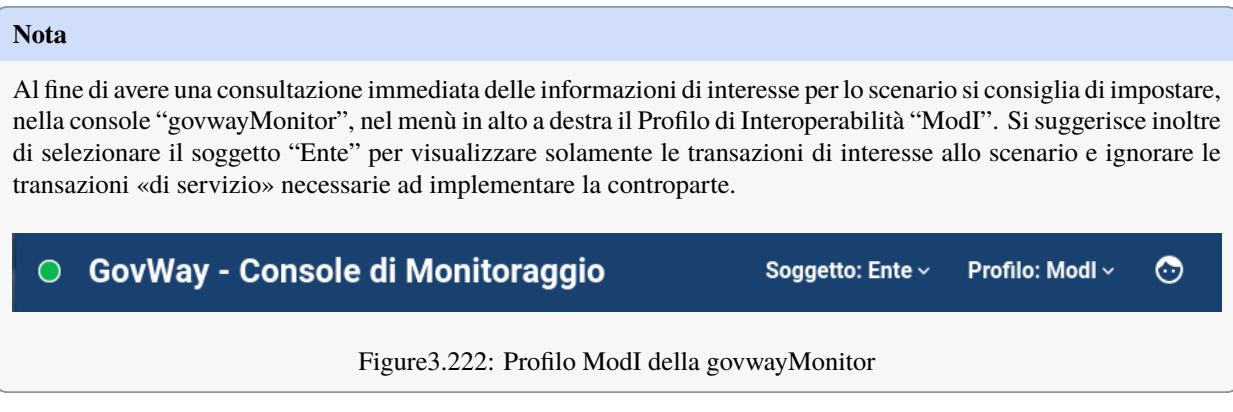
Le caratteristiche principali di questo scenario sono:

1. un applicativo fruitore che dialoga con il servizio erogato in modalità ModI in accordo ad una API condivisa e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND»;
4. le informazioni di audit, richieste dall'erogatore per identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore, vengono inserite in un token di audit conforme al pattern «AUDIT_REST_01». Le informazioni vengono fornite dall'applicativo fruitore tramite header HTTP.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



GovWay - Console di Monitoraggio Soggetto: Ente Profilo: ModI

Figure3.222: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Audit+PDND - OUT App1» che è stata preconfigurata 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 la console “govwayMonitor”.

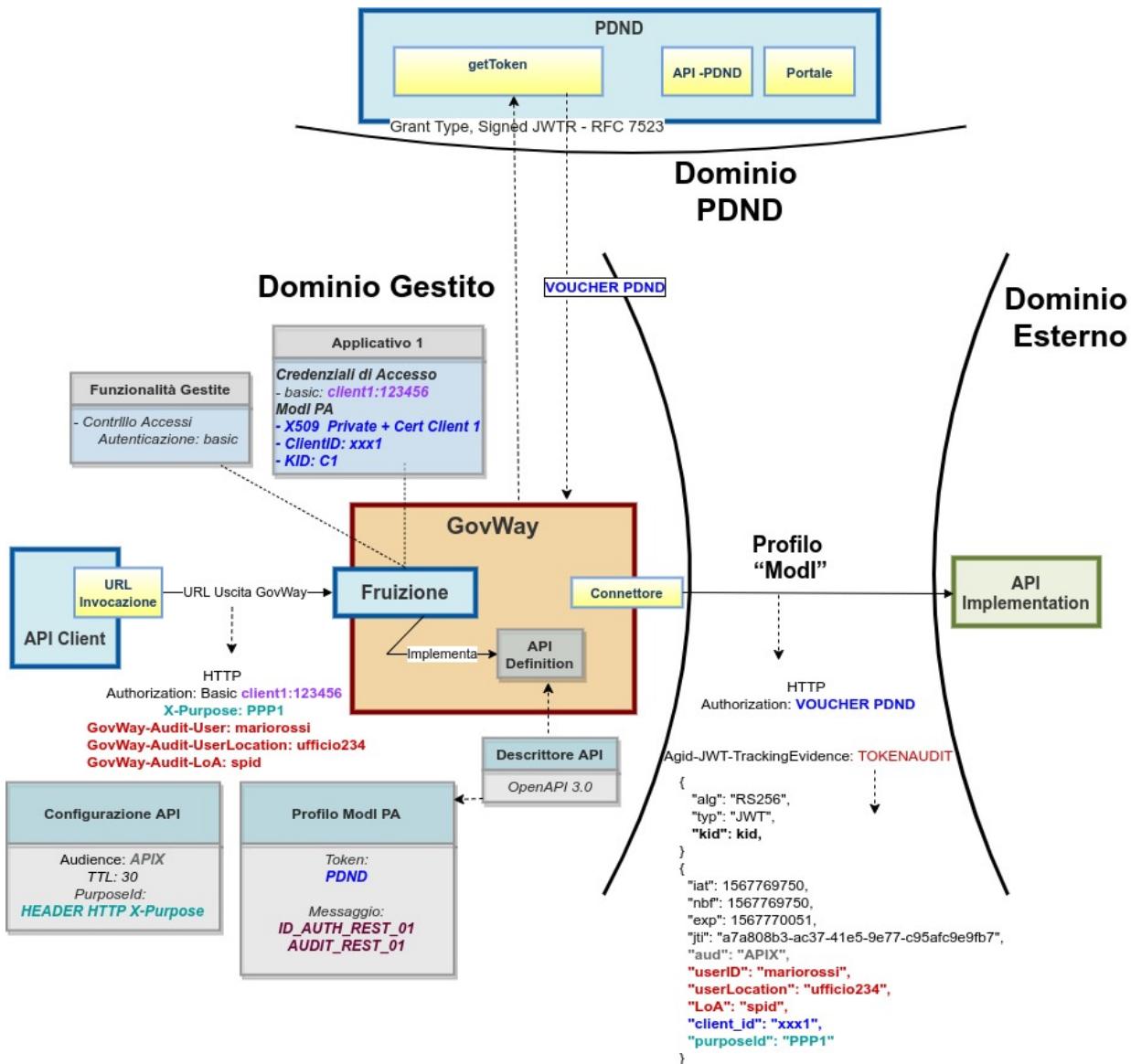


Figure3.221: Fruizione di una API REST con profilo "ModI", pattern AUDIT_REST_01 e pattern ID_AUTH_REST_01 via PDND

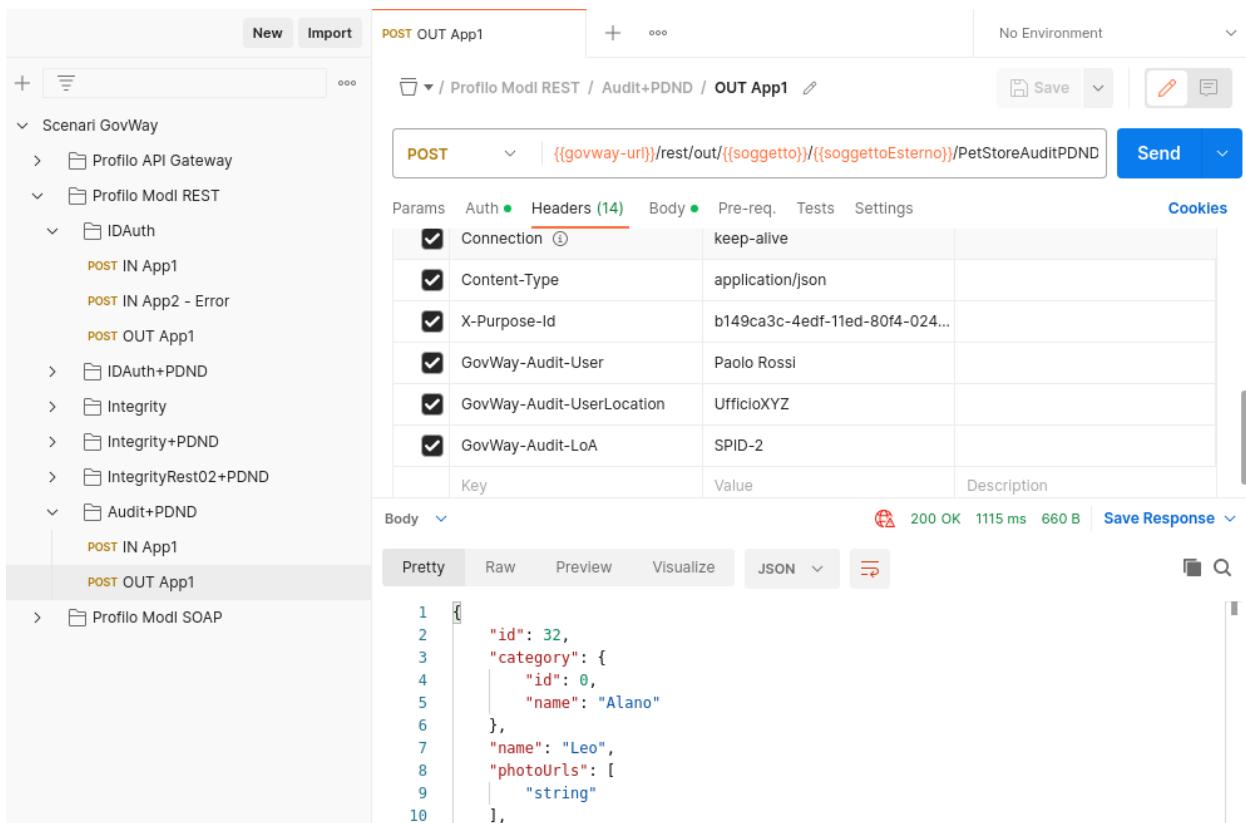


Figure3.223: Pattern Audit+PDND - Fruizione API REST, esecuzione da Postman

Le verifiche da effettuare sono le medesime di quelle descritte nello scenario *Esecuzione*. Di seguito vengono riportati solo i punti salienti in cui emerge una differenza dovuta al pattern di audit utilizzato.

- Il messaggio di richiesta inviato dal fruitore contiene tra gli header HTTP le informazioni da inserire nel token di audit (Fig. 3.224) e il purpose-id da inserire nella richiesta del voucher alla PDND.

Nome	Valore
Content-Type	application/json
X-Forwarded-Server	2ceae888c6d1
Content-Length	216
Postman-Token	e68f2ba0-4fd9-433c-bcb4-8da668594143
Govway-Audit-Userlocation	UfficioXYZ
X-Purpose-Id	b149ca3c-4edf-11ed-80f4-0242ac140002
Govway-Audit-Loa	SPID-2
Govway-Audit-User	Paolo Rossi
Accept	*/*

Figure3.224: Messaggio di richiesta in ingresso (con informazioni sull’utente fruitore inserite negli header HTTP)

- 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 un token di sicurezza da inviare alla PDND con il quale ottenere indietro un voucher spendibile per il servizio desiderato. Questa parte è stata ampiamente mostrata nella scenario *Esecuzione*.

Oltre al token della PDND, GovWay produce un ulteriore token «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_01». Da govwayMonitor si può visualizzare il messaggio di richiesta in uscita che è il medesimo di quello in entrata con la differenza che sono stati aggiunti gli header HTTP «Authorization» e «Agid-Jwt-TrackingEvidence» che contengono rispettivamente il token ottenuto dalla PDND e il token di audit. (Fig. 3.225).

- L’header e i payload del token «Agid-JWT-TrackingEvidence» sono identici a quelli già visualizzati nello scenario di erogazione REST, relativamente al messaggio in ingresso (Fig. 3.210 e Fig. 3.212). Le informazioni inserite nel token vengono anche tracciate e sono visibili sulla govwayMonitor, andando a consultare la traccia del messaggio di richiesta (Fig. 3.226). Nella sezione «Sicurezza Messaggio» sono riportate le informazioni estratte dai token di audit.

Conformità ai requisiti ModI

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

- viene effettuata una negoziazione del voucher PDND come mostrato nelle tracce relative ai token scambiati con la PDND;
- l’invocazione del servizio avviene fornendo il voucher della PDND precedentemente negoziato;

Headers	
Nome	
Content-Type	application/json
Govway-Message-Id	65ef0893-09c7-11ee-893d-0242c0a8a002
X-Forwarded-Server	2ceae888c6d1
X-Real-Ip	192.168.160.1
Postman-Token	912a7384-6c33-4e70-8a90-63ee382a2b18
X-Forwarded-For	192.168.160.2
X-Purpose-Id	b149ca3c-4edf-11ed-80f4-0242ac140002
Cache-Control	no-cache
Authorization	Bearer eyJhbGciOiJSUzI1NilsInR5cClgOiAiSldeUliwia2IkliA6ICJV0NHTzVac0VxeVBXenpxZ3RURkNYViBwWW
Agid-Jwt-TrackingEvidence	eyJhbGciOiJSUzI1NilsInR5cCl6IkpxVCIsImtpZCI6Im5hMDZuQ3d5cldRMWIFb2Z4NGozaU5SeE1ITTDYjc1SVZ
Pragma	no-cache
Accept-Encoding	gzip, deflate, br

Figure3.225: Messaggio di richiesta in uscita (con token di sicurezza inseriti nell'header HTTP)

Informazioni Modl	
Schema Dati Audit	Linee Guida Modl
Informazioni Audit	AUDIT_REST_01
Generazione Token	Authorization PDND
Sicurezza Messaggio	ID_AUTH_REST_01
Sicurezza Canale	ID_AUTH_CHANNEL_01
Interazione	Accesso CRUD
Informazioni Audit	
X509-Issuer	CN=GovWay CA, O=govway.org, C=it
X509-Subject	CN=app1.ente.govway.org, O=govway.org, C=it
Kid	zgC6JlcdjzdZkw-z6aSWltpKbY5ggqMTozwhQc7FU5M
PurposeId	b149ca3c-4edf-11ed-80f4-0242ac140002
Issuer	App1-PDND
LoA	SPID-2
userLocation	UfficioXYZ
userID	Paolo Rossi
Audience	petstore.enteEsterno.govway.org
MessageId	ccc01c53-09ca-11ee-893d-0242c0a8a002
Expiration	2023-06-13_12:01:08.000
NotBefore	2023-06-13_11:56:08.000
IssuedAt	2023-06-13_11:56:08.000

Figure3.226: Traccia della richiesta generata dal fruttore

3. viene inoltre prodotto l'header http «Agid-Jwt-TrackingEvidence» previsto dal pattern di audit «AUDIT_REST_01».

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente ▾

Profilo: ModI ▾



Figure3.227: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di audit aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Registrazione API

Viene registrata l'API «PetStoreAuditPDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l'opzione “Informazioni Audit” e selezionato il pattern «AUDIT_REST_01» e lo schema dei dati «Linee Guida ModI» (Fig. 3.228). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

Fruizione

Nella fruizione «PetStoreAuditPDND», relativa all'API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.229) necessari a generare il token “Agid-JWT-TrackingEvidence”. In particolare è possibile specificare l'audience atteso dall'erogatore e il tempo di validità del token.

3.6.3 Erogazione API SOAP

Obiettivo

Esporre un servizio SOAP, definito tramite una interfaccia WSDL, che richieda per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit01.

Nota

Il token descritto nel pattern modipa_infoUtente_audit01 va in aggiunta rispetto agli altri token di sicurezza e quindi può essere utilizzato in combinazione con qualsiasi dei token descritti nei precedenti scenari, anche senza la PDND. In questo scenario verrà utilizzato insieme al token “Authorization” ottenuto tramite la PDND, descritto negli scenari *Pattern “ID_AUTH” via PDND*.

Sintesi

Modi

Sicurezza Canale

Pattern

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern

Direct Trust con certificato X.509

Generazione Token

Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Informazioni Audit

Pattern

Schema Dati 

Opzionale

Figure3.228: Configurazione Pattern ModI «AUDIT_REST_01» sulla API REST

Fruizioni > PetStoreAuditPDND@EnteEsterno v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi - Richiesta

Sicurezza Messaggio	
Algoritmo	RS256
KeyStore	Definito nell'applicativo
Time to Live (secondi) *	300
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token	
Audience	petstore.enteEsterno.govway.org i
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	
▼ Informazioni Audit	

Figure3.229: Configurazione richiesta della fruizione

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_01».

La figura seguente descrive graficamente questo scenario.

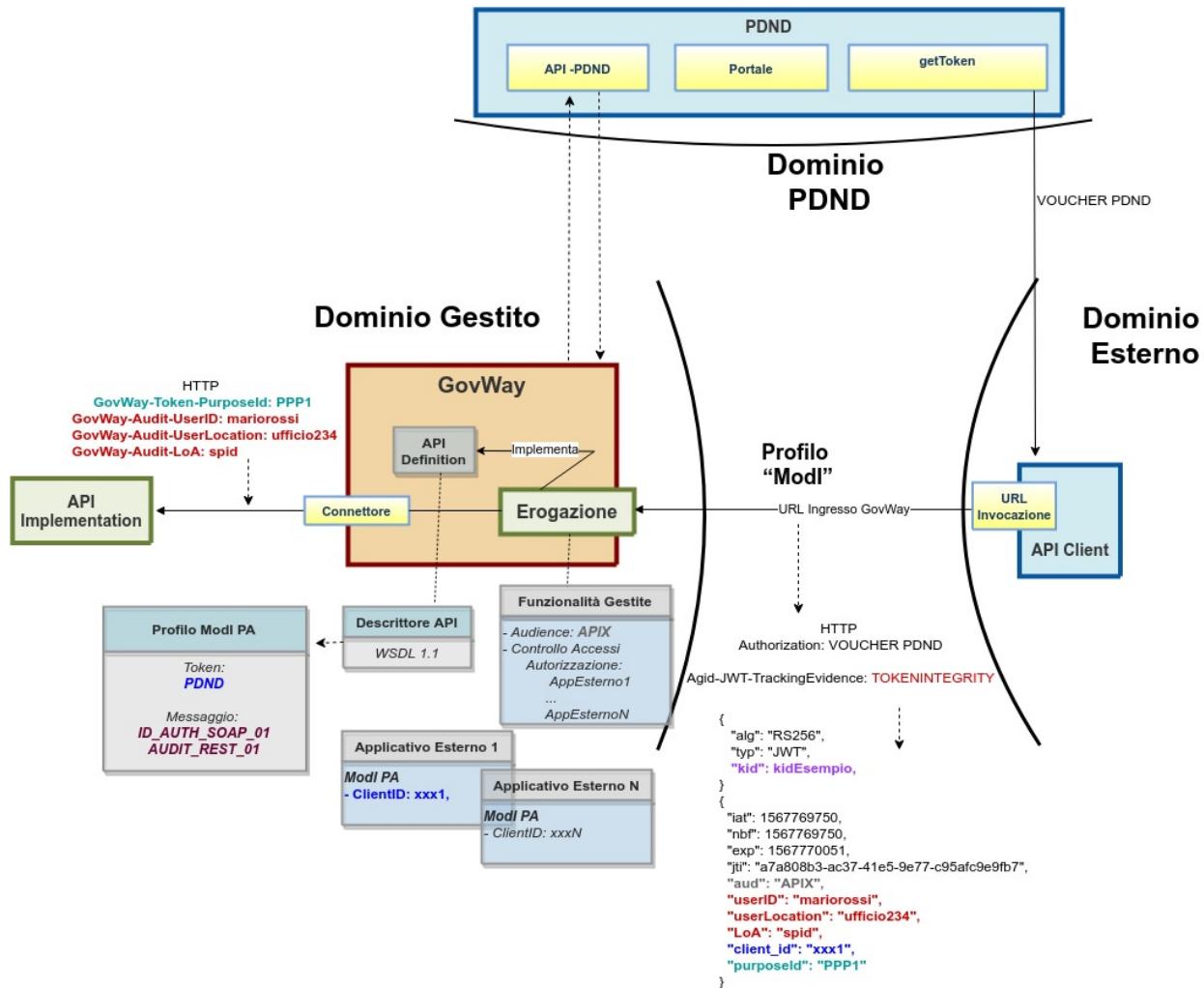


Figure3.230: Erogazione di una API SOAP con profilo “ModI”, pattern AUDIT_REST_01 e pattern ID_AUTH_REST_01 via PDND

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 il pattern di sicurezza canale «ID_AUTH_CHANNEL_02»;
 3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND»;
 4. per la fruizione viene richiesto un token aggiuntivo, conforme al pattern «AUDIT_REST_01», adibito a contenere

informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore;

5. la validazione del token di audit viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
6. vengono inoltre recuperate e associate alla traccia maggiori informazioni sull'organizzazione afferente al "client-id" presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console "govwayMonitor", nel menù in alto a destra il Profilo di Interoperabilità "ModI". Si suggerisce inoltre di selezionare il soggetto "Ente" per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.231: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di audit aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Audit+PDND - IN App1» che è stata preconfigurata 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.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario [Esecuzione](#).

Le evidenze del processo di validazione del token di audit «Agid-Jwt-TrackingEvidence» sono le stesse descritte nello scenario [Esecuzione](#).

Conformità ai requisiti ModI

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

Configurazione

Nota

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". Si suggerisce inoltre di selezionare il soggetto "Ente" per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.233: Profilo ModI della govwayConsole

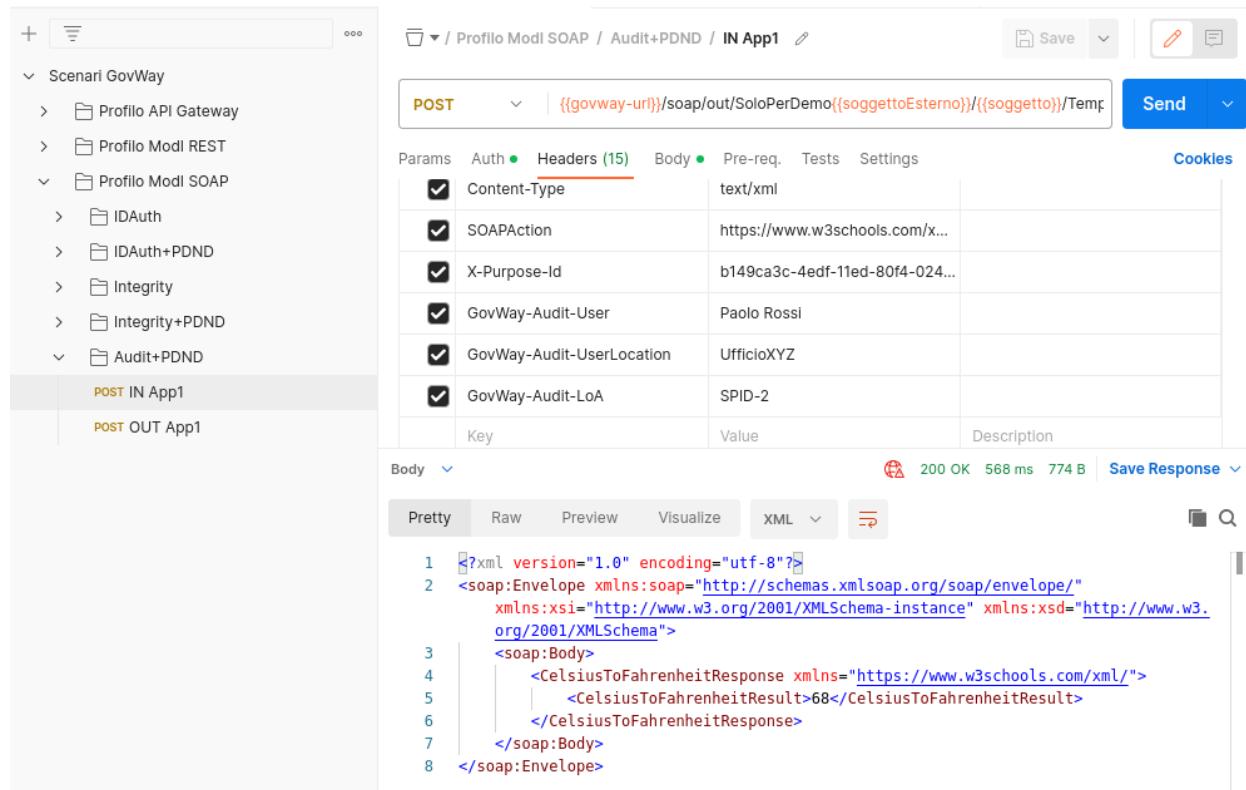


Figure3.232: Pattern Audit+PDND - Erogazione API SOAP, esecuzione da Postman

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

L’interfaccia wsdl del servizio soap è ottenibile all’indirizzo “<https://www.w3schools.com/xml/tempconvert.asmx?wsdl>”.

Registrazione API

Viene registrata l’API «TemperatureConversionAuditPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l’opzione «Informazioni Audit» e selezionato il pattern «AUDIT_REST_01» e lo schema dei dati «Linee Guida ModI» (Fig. 3.234). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

Erogazione

Si registra l’erogazione SOAP “TempConvertSoapAuditPDND”, relativa all’API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.235) necessari per validare le richieste in ingresso relativamente al token “Agid-JWT-TrackingEvidence”. Si noti come è stato selezionato un truststore basato sulla PDND al fine di scaricare la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

Modi

Sicurezza Canale

Pattern

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern

Direct Trust con certificato X.509

Generazione Token

Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Informazioni Audit

Pattern

Schema Dati 

Opzionale

Figure3.234: Configurazione Pattern ModI «AUDIT_REST_01» sulla API SOAP

Erogazioni > TempConvertSoapAuditPDND@Ente v1 > Profilo Interoperabilità

Profilo Interoperabilità

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati	<input type="text" value="Ridefinito"/>
Time to Live	<input type="text" value="Default"/>
Audience	<input type="text" value="TempConvertSoap.ente.govway.org"/>

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

▼ **Informazioni Audit**

TrustStore Certificati

Tipo	<input type="text" value="PDND"/>
------	-----------------------------------

Figure3.235: Configurazione richiesta dell'erogazione

3.6.4 Fruizione API SOAP

Obiettivo

Fruire di un servizio SOAP, definito tramite una interfaccia WSDL, che richiede per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit01.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore deve anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_01».

La figura seguente descrive graficamente questo scenario.

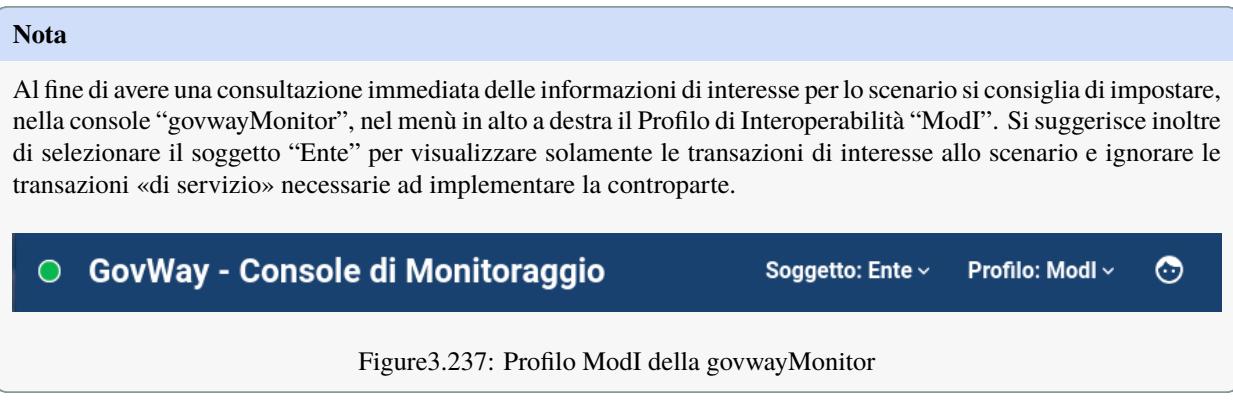
Le caratteristiche principali di questo scenario sono:

1. un applicativo fruitore che dialoga con il servizio erogato in modalità ModI in accordo ad una API condivisa e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_SOAP_01 via PDND»;
4. le informazioni di audit, richieste dall'erogatore per identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore, vengono inserite in un token di audit conforme al pattern «AUDIT_REST_01». Le informazioni vengono fornite dall'applicativo fruitore tramite header HTTP.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



GovWay - Console di Monitoraggio Soggetto: Ente Profilo: ModI

Figure3.237: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#) con la sola eccezione del pattern di audit aggiuntivo utilizzato in questo scenario: «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI SOAP - Audit+PDND - OUT App1» che è stata preconfigurata 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”.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario [Esecuzione](#).

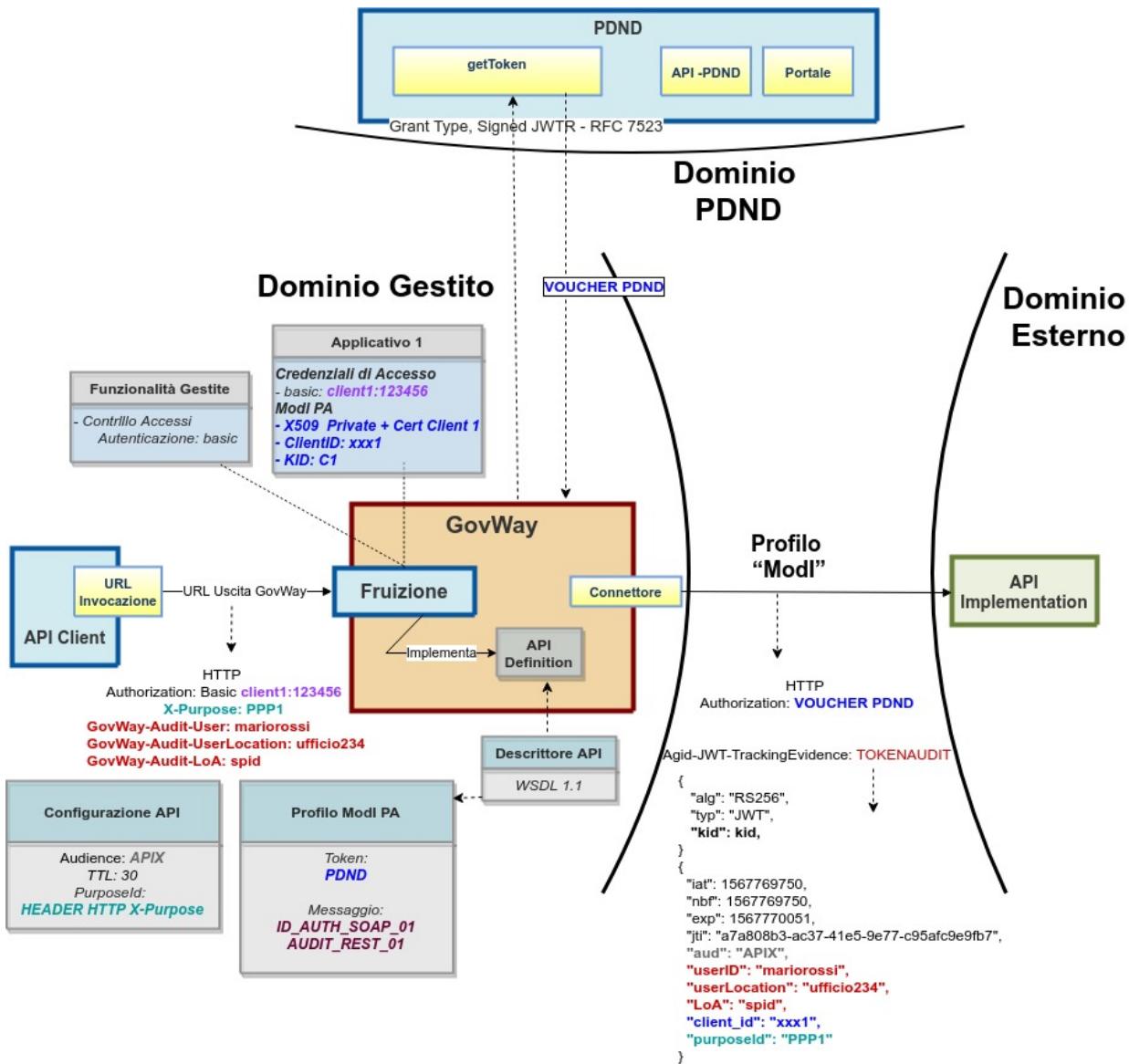


Figure3.236: Fruizione di una API SOAP con profilo "ModI", pattern AUDIT_REST_01 e pattern ID_AUTH_SOAP_01 via PDND

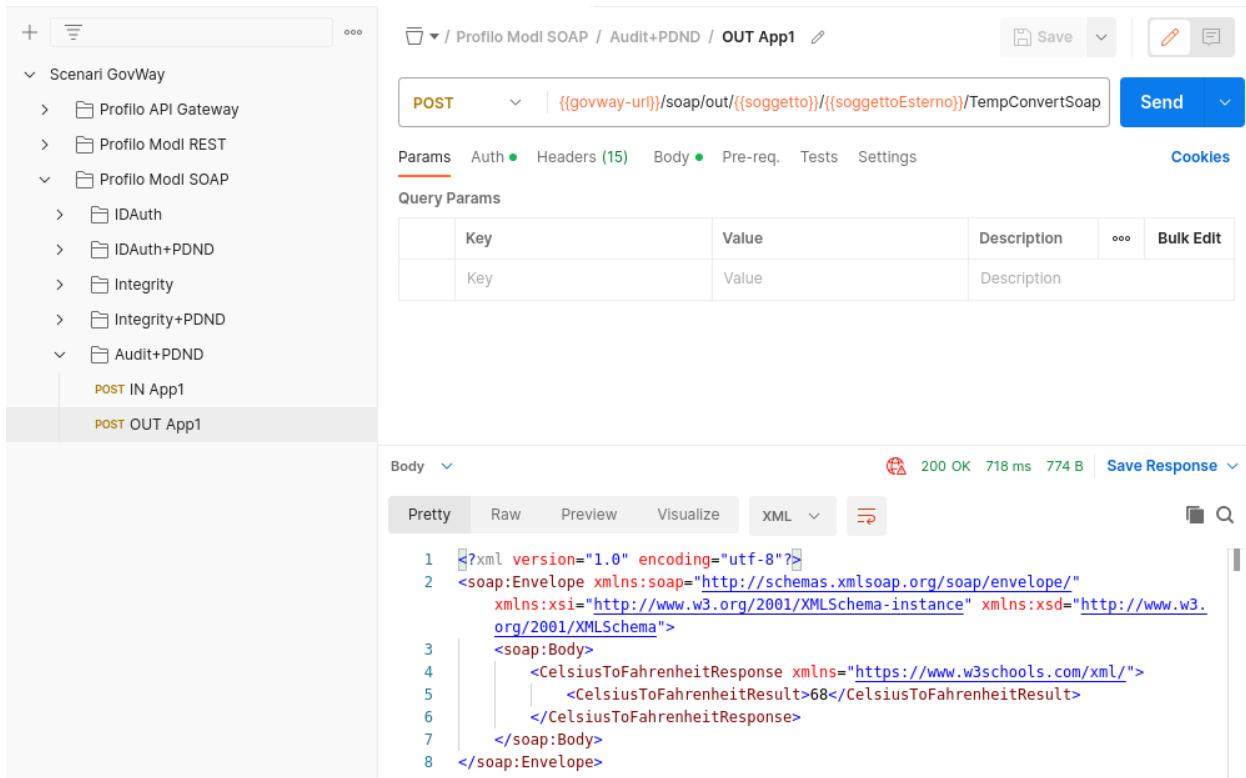


Figure3.238: Pattern Audit+PDND - Fruizione API SOAP, esecuzione da Postman

Le evidenze del processo di validazione del token di audit «Agid-Jwt-TrackingEvidence» sono le stesse descritte nello scenario *Esecuzione*.

Conformità ai requisiti ModI

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

Configurazione

Nota

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». Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.

GovWay - Console di Gestione

Soggetto: Ente

Profilo: ModI



Figure3.239: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con le sole differenze dovute al differente pattern di sicurezza utilizzato «INTEGRITY_SOAP_01 con ID_AUTH_SOAP_01».

Registrazione API

Viene registrata l'API «TemperatureConversionAuditPDND» con il relativo descrittore WSDL. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_SOAP_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l'opzione “Informazioni Audit” e selezionato il pattern «AUDIT_REST_01» e lo schema dei dati «Linee Guida ModI» (Fig. 3.240). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

ModI

Sicurezza Canale

Pattern: ID_AUTH_CHANNEL_01
Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern: ID_AUTH_SOAP_01
Direct Trust con certificato X.509

Generazione Token: Authorization PDND
Token ID_AUTH negoziato con la PDND

Informazioni Audit: Dati del dominio del fruitore

Informazioni Audit

Pattern: AUDIT_REST_01
Schema Dati: Linee Guida ModI i

Opzionale:

Figure3.240: Configurazione Pattern ModI «AUDIT_REST_01» sulla API SOAP

Fruizione

Si registra la fruizione SOAP “TempConvertSoapAuditPDND”, relativa all'API precedentemente inserita, indicando i dati specifici nella sezione «ModI Richiesta» (Fig. 3.241) necessari a generare il token “Agid-JWT-TrackingEvidence”. In particolare è possibile specificare l'audience atteso dall'erogatore e il tempo di validità del token.

3.7 Pattern “AUDIT_REST_02”

Gli scenari riportati in questa sezione riguardano API configurate con pattern modipa_infoUtente_audit02.

Fruizioni > Ente -> TempConvertSoapAuditPDND@EnteEsterno v1 > **Profilo Interoperabilità**

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi - Richiesta

Sicurezza Messaggio	
Algoritmo	RS256
KeyStore	Definito nell'applicativo
Time to Live (secondi) *	300
Indica la validità temporale, in secondi, a partire dalla data di creazione del security token	
Audience	TempConvertSoap.enteEsterno.govway.org
Indica a chi è riferito il security token; se non viene fornito un valore verrà utilizzata la url del connettore	
▼ Informazioni Audit	

Figure3.241: Configurazione richiesta della fruizione

3.7.1 Erogazione API REST

Obiettivo

Esporre un servizio, definito tramite una API REST (OpenAPI 3.0), che richieda per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit02.

Nota

Il token descritto nel pattern modipa_infoUtente_audit02 va in aggiunta rispetto agli altri token di sicurezza e quindi può essere utilizzato in combinazione con qualsiasi dei token descritti nei precedenti scenari purchè il token “Authorization” sia negoziato tramite la PDND.

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 in cui un servizio è stato registrato sulla PDND, e i fruitori per poterlo fruire devono ottenere un voucher dalla PDND che successivamente devono inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher devono anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_02». Da notare come nel pattern modipa_infoUtente_audit02 sia previsto che nel voucher della PDND sia presente il digest del token di audit utile a verificare la correlazione tra i due token.

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 e il servizio viene registrato sulla PDND;
2. la comunicazione con i domini esterni avviene su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01» via PDND»;
4. per la fruizione viene richiesto un token aggiuntivo, conforme al pattern «AUDIT_REST_02», adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore;
5. la validazione del token di audit viene effettuata scaricando la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd;
6. la verifica di correlazione tra il token di audit e il token di autenticazione avviene tramite il calcolo del digest del token di audit «Agid-JWT-TrackingEvidence» e la comparazione con il valore del digest presente nel token «Authorization»;
7. vengono inoltre recuperate e associate alla traccia maggiori informazioni sull'organizzazione afferente al “client-id” presente nel token, sempre attraverso le modipa_passiPreliminari_api_pdnd.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre

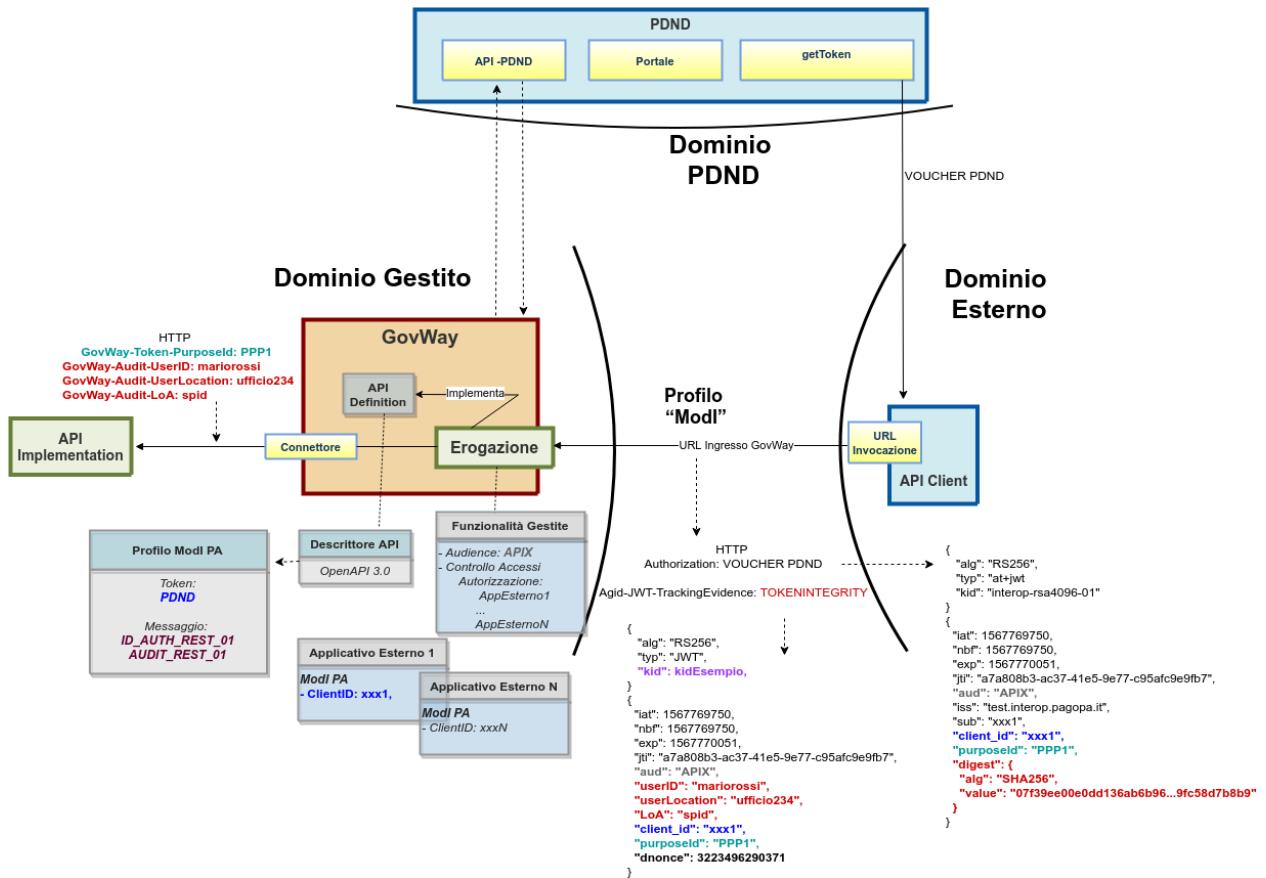


Figure3.242: Erogazione di una API REST con profilo “ModI”, pattern AUDIT_REST_02 e pattern ID_AUTH_REST_01 via PDND

di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario *Esecuzione*. Di seguito verranno evidenziate solamente le differenze che comporta l'utilizzo del pattern «AUDIT_REST_02» al posto di «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Audit02+PDND - IN App4» che è stata preconfigurata per il funzionamento con le caratteristiche descritte sopra.

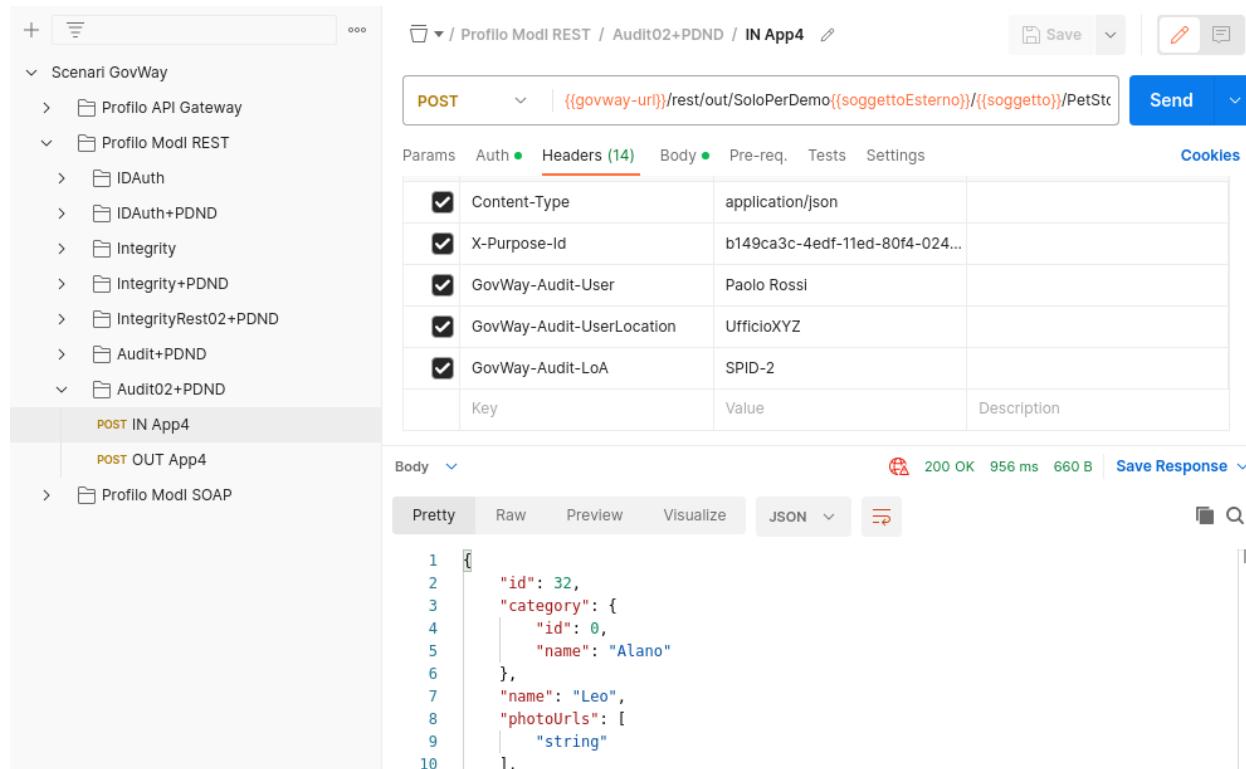


Figure3.244: Pattern Audit02+PDND - Erogazione API REST, esecuzione da Postman

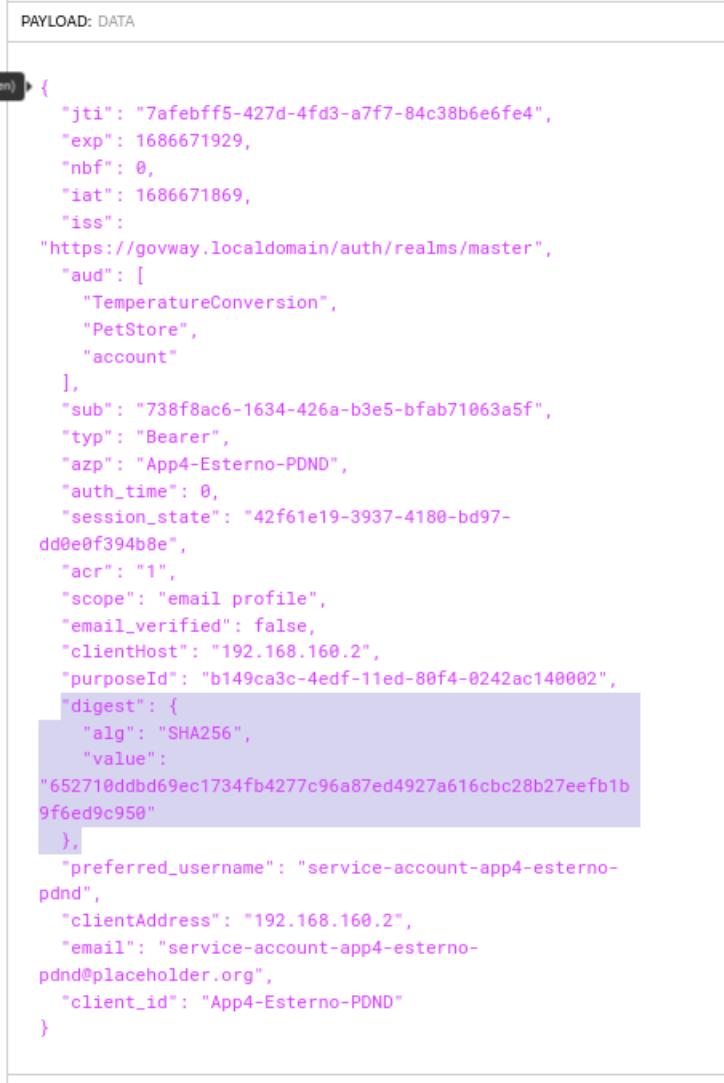
Dopo aver eseguito la «Send» e verificato il corretto esito dell'operazione è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console “govwayMonitor”.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario *Esecuzione*.

Le evidenze del processo di validazione del token di audit «Agid-Jwt-TrackingEvidence» sono le stesse descritte nello scenario *Esecuzione*. Di seguito viene riportato solamente un dettaglio differente presente all'interno del token «Authorization» e richiesto dal pattern «AUDIT_REST_02» per implementare la correlazione tra il token di autenticazione e il token di audit.

Analizzando il token di auth «Authorization» ricevuto nella sezione payload (Fig. 3.245) oltre alle consuete informazioni sull'identità del fruitore (client_id), i riferimenti temporali (iat, nbf, exp), l'audience (aud) e il “purposId”

utilizzato dal fruitore per richiedere il token di autorizzazione alla PDND, è presente anche il claim “digest” utilizzato dall’erogatore per verificare la corrispondenza rispetto al digest calcolato sul token di audit «Agid-Jwt-TrackingEvidence» ricevuto.



```

PAYLOAD: DATA

{
  "jti": "7afebfff5-427d-4fd3-a7f7-84c38b6e6fe4",
  "exp": 1686671929,
  "nbf": 0,
  "iat": 1686671869,
  "iss": "https://govway.localdomain/auth/realmss/master",
  "aud": [
    "TemperatureConversion",
    "PetStore",
    "account"
  ],
  "sub": "738f8ac6-1634-426a-b3e5-bfab71063a5f",
  "typ": "Bearer",
  "azp": "App4-Esterno-PDND",
  "auth_time": 0,
  "session_state": "42f61e19-3937-4180-bd97-
dd0e0f394b8e",
  "acr": "1",
  "scope": "email profile",
  "email_verified": false,
  "clientHost": "192.168.160.2",
  "purposeId": "b149ca3c-4edf-11ed-80f4-0242ac140002",
  "digest": {
    "alg": "SHA256",
    "value": "652710ddbd69ec1734fb4277c96a87ed4927a616cbc28b27eefb1b
9f6ed9c950"
  },
  "preferred_username": "service-account-app4-esterno-
pdnd",
  "clientAddress": "192.168.160.2",
  "email": "service-account-app4-esterno-
pdnd@placeholder.org",
  "client_id": "App4-Esterno-PDND"
}

```

Figure3.245: Sezione «Payload» del Token “Authorization” con pattern “AUDIT_REST_02”

Conformità ai requisiti ModI

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

Configurazione

Nota

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”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di sicurezza aggiuntivo utilizzato in questo scenario: «AUDIT_REST_02».

Registrazione API

Viene registrata l'API «PetStoreAudit02PDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l'opzione “Informazioni Audit” e selezionato il pattern «AUDIT_REST_02» e lo schema dei dati «Linee Guida ModI» (Fig. 3.247). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

ModI	
Sicurezza Canale	
Pattern	ID_AUTH_CHANNEL_01
Direct Trust Transport-Level Security	
Sicurezza Messaggio	
Pattern	ID_AUTH_REST_01
Direct Trust con certificato X.509	
Generazione Token	Authorization PDND
Token ID_AUTH negoziato con la PDND	
Informazioni Audit	<input checked="" type="checkbox"/> Dati del dominio del fruitore
Informazioni Audit	
Pattern	AUDIT_REST_02
Schema Dati	Linee Guida ModI
Opzionale	<input type="checkbox"/>

Figure3.247: Configurazione Pattern ModI «AUDIT_REST_02» sulla API REST

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 si desidera autorizzare qualsiasi fruitore proveniente dalla PDND, questo passo può anche essere omesso. La validazione del token è sufficiente a stabilire che il fruitore ha ottenuto un voucher dalla PDND valido per il servizio invocato. Questo scenario è quello preconfigurato.
- In alternativa è possibile configurare una autorizzazione puntuale procedendo alla registrazione degli applicativi fornendo i singoli “client_id” necessari all’identificazione (Fig. 3.248).

Applicativo

Profilo Interoperabilità	ModI
Dominio	Esterno
Soggetto	EnteEsterno
Nome *	<input type="text" value="App1-PDND"/>
Tipo	Client
Proprietà(0)	

Ruoli

visualizza(0)

ModI

Sicurezza Messaggio	<input type="text" value="Authorization PDND"/>
ClientId registrato sulla PDND	
Token Policy *	<input type="text" value="PDND"/>
Identificativo *	<input type="text" value="App1-Esterno-PDND"/>

Figure3.248: Configurazione applicativo esterno (fruitore)

Erogazione

Nell’erogazione «PetStoreAudit02PDND», relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.249) necessari per validare le richieste in ingresso relativamente al token “Agid-JWT-TrackingEvidence”. Si noti come è stato selezionato un truststore basato sulla PDND al fine di scaricare la chiave pubblica, corrispondente al kid presente nel token, tramite le modipa_passiPreliminari_api_pdnd.

Erogazioni > PetStoreAudit02PDND@Ente v1 > Profilo Interoperabilità

Profilo Interoperabilità

Modi - Richiesta

Sicurezza Messaggio

TrustStore Certificati	Ridefinito
Time to Live	Default
Audience	petstore.ente.govway.org

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

▼ **Informazioni Audit**

TrustStore Certificati

Tipo	PDND
------	------

Figure3.249: Configurazione richiesta dell'erogazione

3.7.2 Fruzione API REST

Obiettivo

Fruire di un servizio REST, definito tramite una API REST (OpenAPI 3.0), che richiede per l'accesso oltre ai token di sicurezza descritti nei precedenti scenari anche un token aggiuntivo adibito a contenere informazioni utili all'erogatore a identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore. Il token di audit deve rispettare il pattern di sicurezza descritto nella sezione modipa_infoUtente_audit02.

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 in cui il servizio è stato registrato sulla PDND, e il fruitore per poterlo fruire deve ottenere un voucher dalla PDND che successivamente deve inviare all'erogatore insieme alla normale richiesta di servizio. Oltre al voucher il fruitore devo anche presentare il token di audit «Agid-JWT-TrackingEvidence» previsto dal pattern «AUDIT_REST_02». Da notare come il pattern modipa_infoUtente_audit02 prevede che nella richiesta del voucher verso la PDND e nel voucher restituito debba essere presente il digest del token di audit che verrà poi utilizzato dall'erogatore per verificare la correlazione tra i due token.

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 e pubblicata su PDND;
2. la comunicazione diretta verso il dominio erogatore veicolata su un canale gestito con il pattern di sicurezza canale «ID_AUTH_CHANNEL_01»;
3. l'autenticità della comunicazione tra il servizio erogato e ciascun fruitore è garantita tramite sicurezza a livello messaggio con pattern «ID_AUTH_REST_01 via PDND»;

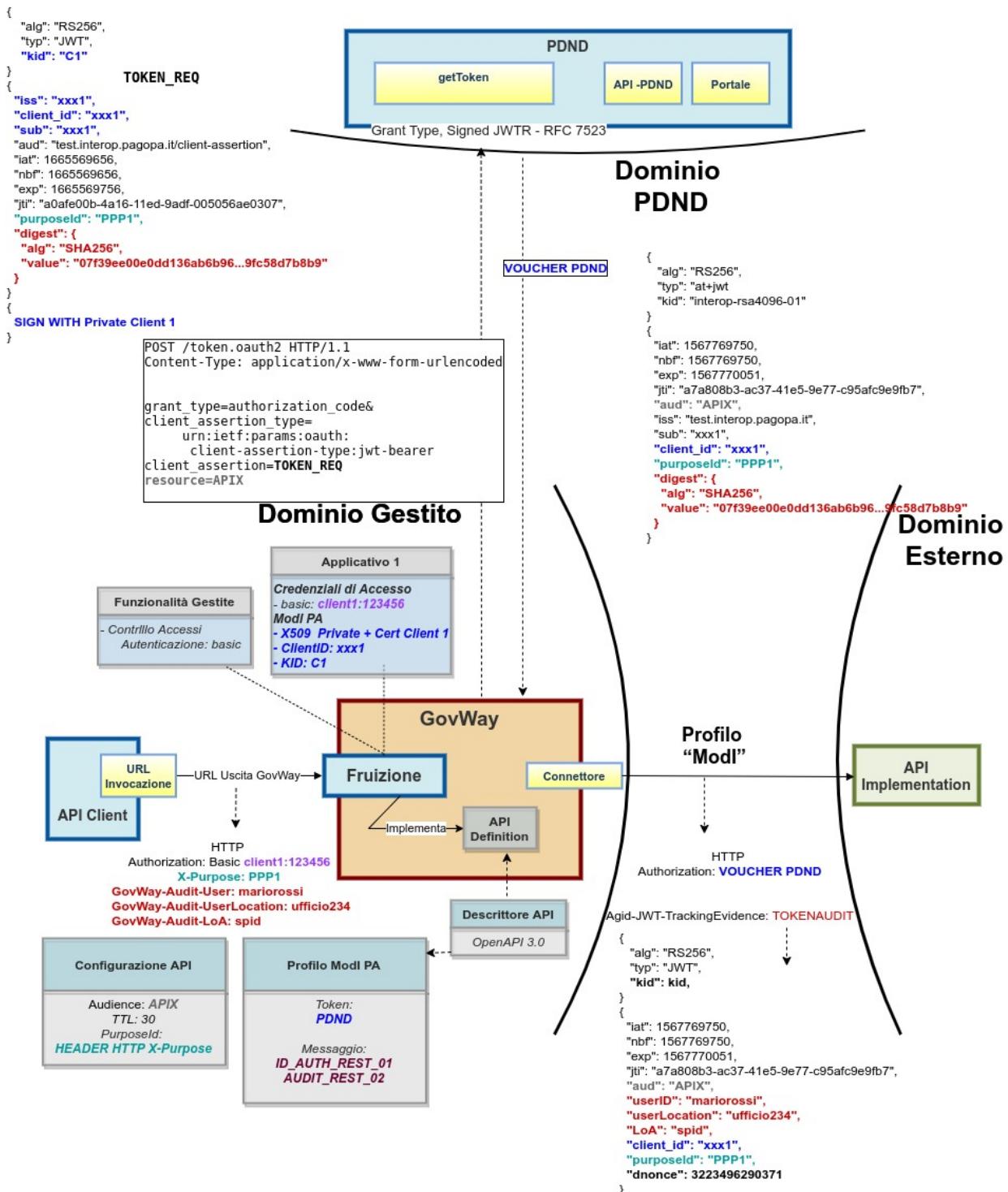


Figure3.250: Fruizione di una API REST con profilo "ModI", pattern AUDIT_REST_02 e pattern ID_AUTH_REST_01 via PDND

4. le informazioni di audit, richieste dall'erogatore per identificare la specifica provenienza di ogni singola richiesta di accesso ai dati effettuata dal fruitore, vengono inserite in un token di audit conforme al pattern «AUDIT_REST_02». Le informazioni vengono fornite dall'applicativo fruitore tramite header HTTP;
5. la negoziazione del voucher con la PDND prevede l'inserimento nella richiesta del digest del token di audit che verrà a sua volta incluso dalla PDND nel voucher restituito e sarà utilizzabile dall'erogatore per verificare la correlazione tra il token di audit e il token di autenticazione.

Esecuzione

Nota

Al fine di avere una consultazione immediata delle informazioni di interesse per lo scenario si consiglia di impostare, nella console “govwayMonitor”, nel menù in alto a destra il Profilo di Interoperabilità “ModI”. Si suggerisce inoltre di selezionare il soggetto “Ente” per visualizzare solamente le transazioni di interesse allo scenario e ignorare le transazioni «di servizio» necessarie ad implementare la controparte.



Figure3.251: Profilo ModI della govwayMonitor

L'esecuzione dello scenario è del tutto analogo a quello descritto nello scenario [Esecuzione](#). Di seguito verranno evidenziate solamente le differenze che comporta l'utilizzo del pattern «AUDIT_REST_02» al posto di «AUDIT_REST_01».

Per eseguire e verificare lo scenario si può utilizzare il progetto Postman a corredo con la request «Profilo ModI REST - Audit02+PDND - OUT App4» che è stata preconfigurata 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 la console “govwayMonitor”.

Le evidenze del processo di validazione relative al token PDND sono le medesime descritte nella scenario [Esecuzione](#).

Le evidenze del processo di validazione del token di audit «Agid-Jwt-TrackingEvidence» sono le stesse descritte nello scenario [Esecuzione](#). Di seguito viene riportato solamente un dettaglio differente presente all'interno del token «Authorization» e richiesto dal pattern «AUDIT_REST_02» per implementare la correlazione tra il token di autenticazione e il token di audit.

Analizzando il token di auth «Authorization», ottenuto dalla PDND ed inviato all'erogatore, nella sezione payload (Fig. 3.253) oltre alle consuete informazioni sull'identità del fruitore (client_id), i riferimenti temporali (iat, nbf, exp), l'audience (aud) e il “purposeId” utilizzato dal fruitore per richiedere il token di autorizzazione alla PDND, è presente anche il claim “digest” utilizzato dall'erogatore per verificare la corrispondenza rispetto al digest calcolato sul token di audit «Agid-Jwt-TrackingEvidence» ricevuto.

Conformità ai requisiti ModI

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

Configurazione

Nota

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». Si suggerisce

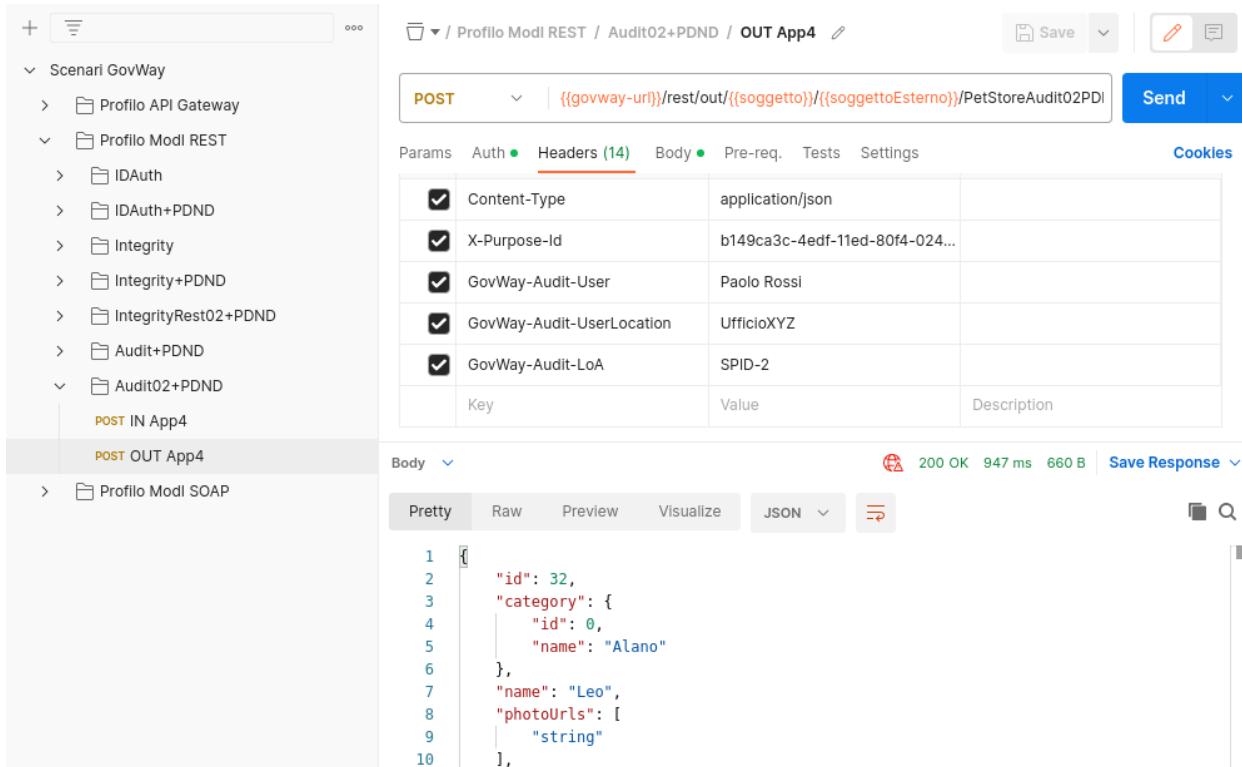


Figure3.252: Pattern Audit02+PDND - Fruizione API REST, esecuzione da Postman

inoltre di selezionare il soggetto “Ente” per visualizzare solamente le configurazioni di interesse allo scenario e nascondere le configurazioni «di servizio» necessarie ad implementare la controparte.



Figure3.254: Profilo ModI della govwayConsole

La configurazione dello scenario è del tutto analogo a quello descritto nello scenario *Configurazione* con la sola eccezione del pattern di audit aggiuntivo utilizzato in questo scenario: «AUDIT_REST_02».

Registrazione API

Viene registrata l’API «PetStoreAudit02PDND» con il relativo descrittore OpenAPI 3. Vengono selezionati i pattern «ID_AUTH_CHANNEL_01» (sicurezza canale) e «ID_AUTH_REST_01» (sicurezza messaggio) nella sezione «ModI» indicando nel campo «Generazione Token» il valore «Authorization PDND». Viene infine abilitata l’opzione “Informazioni Audit” e selezionato il pattern «AUDIT_REST_02» e lo schema dei dati «Linee Guida ModI» (Fig. 3.255). Per ulteriori dettagli sullo schema dei dati di un token di audit si rimanda alle sezioni modipa_infoUtente_audit01_schema e modipa_infoUtente_audit01_schema_custom.

Fruizione

Nella fruizione «PetStoreAudit02PDND», relativa all’API precedentemente inserita, vanno indicati i dati specifici nella sezione «ModI Richiesta» (Fig. 3.256) necessari a generare il token “Agid-JWT-TrackingEvidence”. In particolare è possibile specificare l’audience atteso dall’erogatore e il tempo di validità del token.



The image shows a JSON object representing a token payload. The object is enclosed in a box labeled "PAYLOAD: DATA". The content of the payload is as follows:

```
{
  "jti": "7afebfff5-427d-4fd3-a7f7-84c38b6e6fe4",
  "exp": 1686671929,
  "nbf": 0,
  "iat": 1686671869,
  "iss": "https://govway.localdomain/auth/realm/master",
  "aud": [
    "TemperatureConversion",
    "PetStore",
    "account"
  ],
  "sub": "738f8ac6-1634-426a-b3e5-bfab71063a5f",
  "typ": "Bearer",
  "azp": "App4-Esterno-PDND",
  "auth_time": 0,
  "session_state": "42f61e19-3937-4180-bd97-
dd0e0f394b8e",
  "acr": "1",
  "scope": "email profile",
  "email_verified": false,
  "clientHost": "192.168.160.2",
  "purposeId": "b149ca3c-4edf-11ed-80f4-0242ac140002",
  "digest": {
    "alg": "SHA256",
    "value": "652710ddbd69ec1734fb4277c96a87ed4927a616cbc28b27eefb1b
9f6ed9c950"
  },
  "preferred_username": "service-account-app4-esterno-
pdnd",
  "clientAddress": "192.168.160.2",
  "email": "service-account-app4-esterno-
pdnd@placeholder.org",
  "client_id": "App4-Esterno-PDND"
}
```

Figure3.253: Sezione «Payload» del Token “Authorization” con pattern “AUDIT_REST_02”

Modi

Sicurezza Canale

Pattern ▼

Direct Trust Transport-Level Security

Sicurezza Messaggio

Pattern ▼

Direct Trust con certificato X.509

Generazione Token ▼

Token ID_AUTH negoziato con la PDND

Informazioni Audit Dati del dominio del fruitore

Informazioni Audit

Pattern ▼

Schema Dati ▼ ⓘ

Opzionale

Figure3.255: Configurazione Pattern ModI «AUDIT_REST_02» sulla API REST

Fruizioni > Ente > PetStoreAudit02PDND@EnteEsterno v1 > Profilo Interoperabilità

Profilo Interoperabilità

Note: (*) Campi obbligatori

Modi - Richiesta

Sicurezza Messaggio

Algoritmo	RS256
KeyStore	Definito nell'applicativo
Time to Live (secondi) *	300

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

Audience: petstore.enteEsterno.govway.org i

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

▼ Informazioni Audit

Figure3.256: Configurazione richiesta della fruizione

CHAPTER 4

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. 4.1](#)).

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

4.1 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. 4.2](#).

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. 4.3](#)).
- 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. 4.4](#)).
- Il riquadro «Informazioni Mittente» fornisce dettagli sulla provenienza della richiesta.

Transazioni > Ricerca Base			
Ricerca Base			
Lista Transazioni: record [1 - 6]			
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:23:09, Risorsa API Rest: GET /pet/{petId}	719 ms	HTTP 200	<input type="checkbox"/>
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:22:39, Risorsa API Rest: POST /pet	722 ms	HTTP 200	<input type="checkbox"/>
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:21:43, Risorsa API Rest: POST /pet	66 ms	Gestione Token 401	<input type="checkbox"/>
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:21:21, Risorsa API Rest: POST /pet	93 ms	Token non Presente 401	<input type="checkbox"/>
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:20:19, Risorsa API Rest: GET /pet/findByStatus	783 ms	HTTP 200	<input type="checkbox"/>
PetStore@Ente v1			<input type="checkbox"/>
Data: 2020-11-16 16:19:33, Risorsa API Rest: GET /pet/findByStatus	599 ms	HTTP 302	<input type="checkbox"/>

Figure4.1: 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
Diagnostic	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	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

Figure4.2: Dettaglio della transazione in errore
4.1. Transazione in errore

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

Lista Diagnostici: record [1 - 6] su 6

Data	Severità	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

Figure4.3: Messaggi diagnostici della transazione in errore

Visualizza Transazioni (Live) > Dettagli Transazione > **Fault Uscita**

Fault Uscita

```

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 }
```

Figure4.4: Fault in uscita

- Il riquadro «Informazioni Avanzate» fornisce dati aggiuntivi riguardo la transazione.

4.2 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. 4.5).

Informazioni Generali	
Tipologia	Erogazione (API Gateway)
Erogatore	Test
API	PetStore v1
Azione	POST_pet
Profilo Collaborazione	Sincrono
Esito	Ok
Diagnostici	Visualizza Esporta

Figure4.5: 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. 4.6).
- 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. 4.7.
- Dalla sezione mittente è possibile aprire una finestra per visualizzare la versione in chiaro del token ricevuto con la richiesta (Fig. 4.8).

Visualizza Transazioni (Live) > Dettagli Transazione > Messaggi Diagnostici			
Lista Diagnostici: record [1 - 8] su 8			
Data	Severità	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

Figure4.6: Messaggi diagnostici della transazione con esito regolare

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/realms/testrealm
 Client ID: testclient
 Subject: 22158fb1-cea7-46c9-8180-1e30ccb4f944
 Username: testuser
 Token Info: [Visualizza](#)

Figure4.7: Informazioni mittente con presenza del token

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" : "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://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

Figure4.8: Visualizzazione del token