
Scenari Applicativi

Release 3.2.0.rc1

30 set 2019

Indice

1 Ambiente di esecuzione	1
1.1 Prerequisiti	1
1.2 Avvio	1
2 Erogazione pubblica	5
2.1 Obiettivo	5
2.2 Sintesi	5
2.3 Esecuzione	5
2.4 Configurazione	5
3 Erogazione OAuth	11
3.1 Obiettivo	11
3.2 Sintesi	11
3.3 Esecuzione	11
3.4 Configurazione	15
4 Erogazione REST ModI PA	19
4.1 Obiettivo	19
4.2 Sintesi	19
4.3 Esecuzione	21
4.4 Configurazione	25
5 Fruizione REST ModI PA	31
5.1 Obiettivo	31
5.2 Sintesi	31
5.3 Esecuzione	33
5.4 Configurazione	36
6 Erogazione SOAP ModI PA	39
6.1 Obiettivo	39
6.2 Sintesi	39
6.3 Esecuzione	40
7 Fruizione SOAP ModI PA	45
7.1 Obiettivo	45
7.2 Sintesi	45
7.3 Esecuzione	47

8 Monitoraggio	49
8.1 Transazione in errore	50
8.2 Transazione con esito corretto	50

CAPITOLO 1

Ambiente di esecuzione

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

1.1 Prerequisiti

Per l'avvio dell'ambiente di esecuzione degli scenari è necessario prima compiere i seguenti passi:

- Scaricare l'archivio di installazione al seguente indirizzo <http://www.govway.org>
- 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

1.2 Avvio

Dopo aver scompattato l'archivio distribuito dovranno essere installate le singole componenti incluse:

- *Archivio di Inizializzazione*: un file zip da scompattare nella cartella di destinazione scelta per ospitare l'ambiente di esecuzione degli scenari.
- *Ambiente Docker*: la configurazione dell'ambiente docker necessaria per il dispiegamento e avvio dei componenti necessari. L'avvio dell'ambiente viene effettuato eseguendo il comando “docker-compose up” nella cartella di destinazione dell'ambiente, dove deve essere presente il file di configurazione docker distribuito “docker-compose.yml” (Fig. 1.1).

I componenti avviati sono i seguenti:

- gateway: l'istanza di Govway
- PGSQ95: il database Postgres
- govauth: il service provider SAML (SPID)

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

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

- spid_testenv: IDP SPID di test
- keycloak: l'authorization server
- traefik: il load balancer
- *Progetto Postman*: la collection Postman che comprende le request utilizzate nei vari scenari presentati ([Fig. 1.2](#)). La collection deve essere caricata sul proprio Postman tramite la funzionalità di import.

Dopo aver avviato l'ambiente docker è possibile verificare l'accesso alla console govwayMonitor, dalla quale si potranno consultare le transazioni gestite da Govway ([Fig. 1.3](#)).

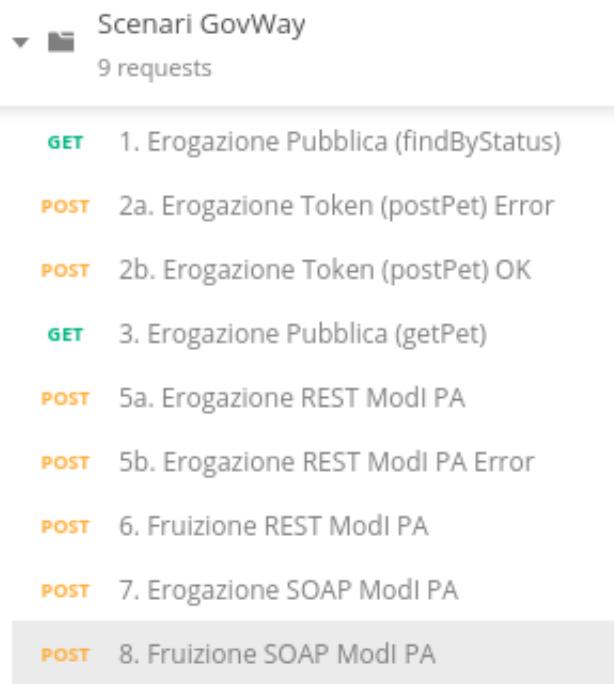


Fig. 1.2: Indice della collection Postman

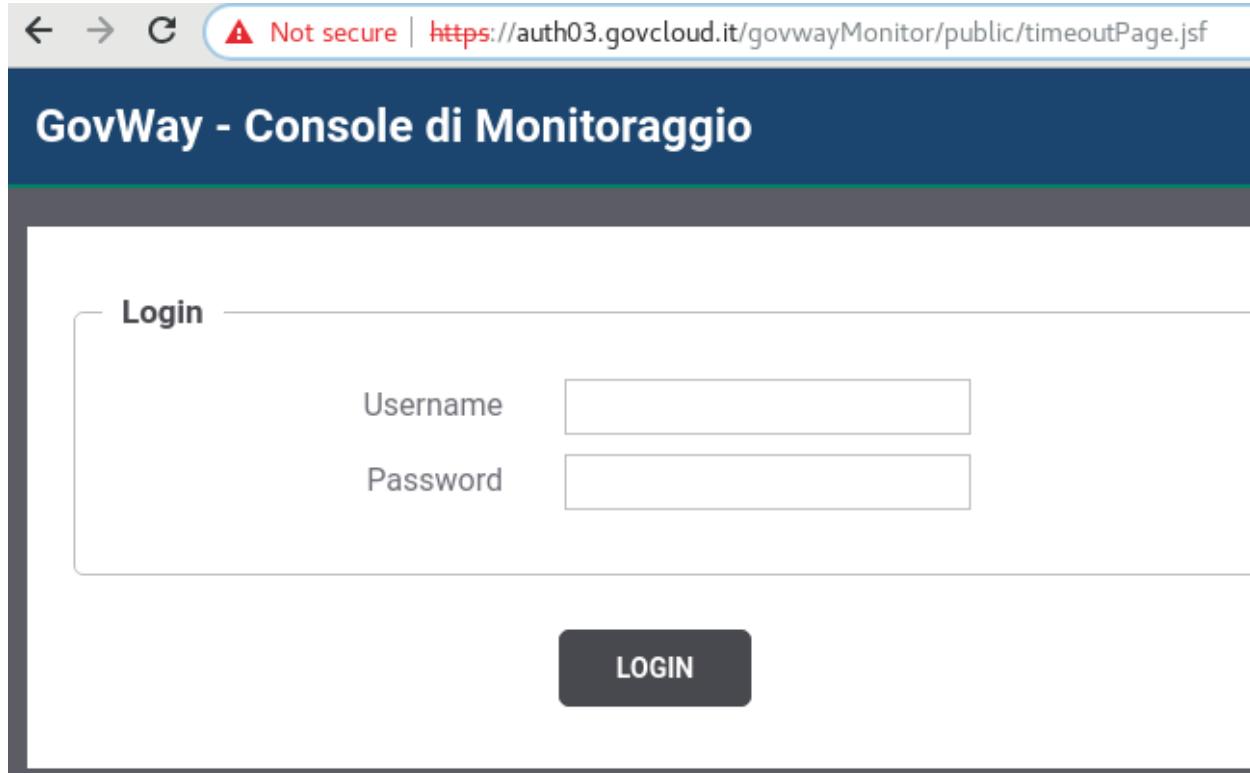


Fig. 1.3: Accesso alla console di monitoraggio

CAPITOLO 2

Erogazione pubblica

2.1 Obiettivo

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

2.2 Sintesi

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

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

La figura seguente descrive graficamente questo scenario.

2.3 Esecuzione

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

2.4 Configurazione

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

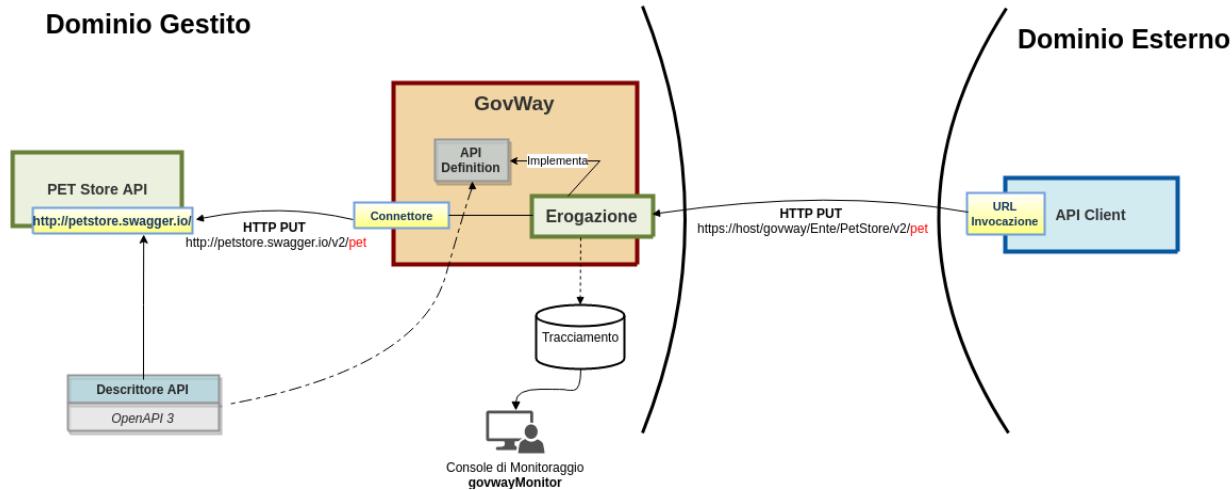


Fig. 2.1: Erogazione ad accesso pubblico

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

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

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

The screenshot shows the Postman application interface. At the top, there is a header bar with the title "Scenari Applicativi, Release 3.2.0.rc1". Below the header, a navigation bar includes links for "Home", "Scenari", "Progetti", "Analisi", "Report", "Configurazione", and "Help". A search bar is also present.

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

The request details are as follows:

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

The response status is shown as "Status: 200 OK".

The response body is displayed in JSON format:

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

Fig. 2.2: Erogazione pubblica, esecuzione da Postman

Erogazioni > Aggiungi

Note: (*) Campi obbligatori

Informazioni Generali

API

Nome: PetStore v1

Tipo: Rest

Controllo degli Accessi

Accesso API: pubblico

Connettore

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

Autenticazione Http:

Autenticazione Token:

AutenticazioneHttps:

Proxy:

Ridefinisci Tempi Risposta:

SALVA

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

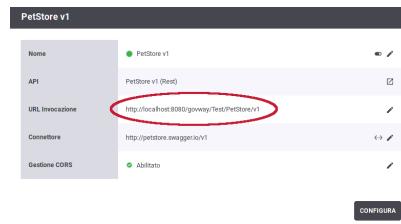


Fig. 2.4: Dettaglio dell'erogazione

CAPITOLO 3

Erogazione OAuth

3.1 Obiettivo

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

3.2 Sintesi

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

La figura seguente descrive graficamente questo scenario.

I passi previsti sono i seguenti:

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

3.3 Esecuzione

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

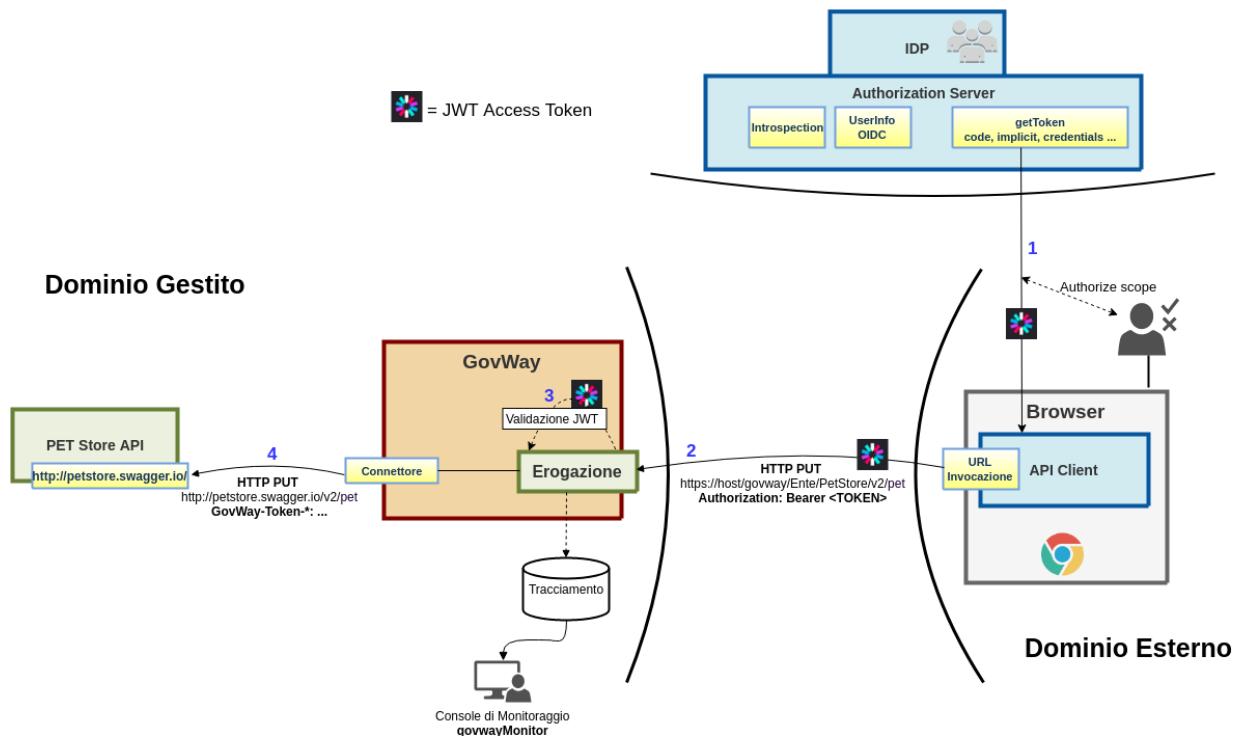


Fig. 3.1: Erogazione OAuth

1. All'inizio possiamo verificare come il client non riesca ad accedere al servizio senza l'utilizzo del token. La request «2a. Erogazione Token (postPet) Error» effettua una chiamata alla risorsa «POST /pet» in assenza del token richiesto. Govway respinge la richiesta con la restituzione dell'errore mostrato in Fig. 3.2.
2. Successivamente si passa alla chiamata della «POST /pet» seguendo il flusso OAuth2 richiesto per l'approvigionamento del token di autorizzazione. Posizionarsi sulla request «2b. Erogazione Token (postPet) OK»:
 - Nella sezione «Authorization» selezionare il Type «OAuth 2.0» e premere il pulsante «Get New Access Token», quindi «Request Token» sulla finestra popup successiva (i campi del form sono compilati con i valori presenti nella configurazione del progetto). *** CAPIRE QUALI VALORI INDICARE ***
 - Completare il processo di autenticazione dell'utente seguendo il flusso proposto. *** CREDENZIALI UTENTE? ***
 - Superata l'autenticazione, viene restituito l'access token (mostrato a video sulla finestra popup).
 - Inserire il token nella richiesta premendo il pulsante «Use Token».
 - Eseguire la richiesta tramite il pulsante «Send».
 - L'operazione viene eseguita con successo e restituito l'esito (Fig. 3.3).
3. Possiamo verificare che le limitazioni sull'accesso non sono efficaci nel caso di invocazione di operazioni di lettura. Il passo «3. Erogazione Pubblica (getPet)» esegue una GET. Si noti come la sezione Authorization abbia l'impostazione del Type su «No Auth». Questa request legge il dato creato con la POST precedente e, come è possibile riscontrare al termine dell'esecuzione, viene correttamente eseguita in assenza di credenziali.

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

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

Fig. 3.2: Invocazione della POST /pet senza token

The screenshot shows the Postman application interface. At the top, there is a header bar with a red button labeled "Test". Below the header, the URL is set to `POST {{govway-url}}/{{soggetto}}/PetStore/v1/pet`. The "Authorization" tab is selected, showing "OAuth 2.0" as the type. A token field contains a long string of characters, and a "Get New Access Token" button is visible. The "Params", "Headers (10)", "Body", "Pre-request Script", "Tests", "Cookies", and "Code" tabs are also present. In the main body area, there is a note about automatic token generation when sending the request, a "Preview Request" button, and a "Body" tab containing a JSON response. The response body is a JSON object with the following structure:

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

Fig. 3.3: Invocazione della POST /pet con token

3.4 Configurazione

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

1. Dal dettaglio dell'erogazione, si procede con la creazione di una nuova configurazione, cui diamo il nome «*Scritture*» (Fig. 3.4).
 - 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*

The screenshot shows the configuration interface for a PetStore v1 (Test) service. The top navigation bar includes 'Erogazioni', 'PetStore v1 (Test)', 'Configurazione', and 'Aggiungi'. A note at the top says 'Note: (*) Campi obbligatori'. The main configuration section has a title 'Configurazione'. It contains three fields: 'Nome Gruppo' set to 'Scritture', 'Risorse' containing a list of API endpoints (POST /pet, PUT /pet, GET /pet/findByStatus, GET /pet/findByTags, DELETE /pet/{petId}, GET /pet/{petId}, POST /pet/{petId}, POST /pet/{petId}/uploadImage, GET /store/inventory, POST /store/order), and 'Modalità' set to 'Nuova'. Below this is a 'Controllo degli Accessi' section with 'Accesso API' set to 'autenticato'. At the bottom is a 'SALVA' button.

Fig. 3.4: Creazione di una configurazione specifica per le operazioni di scrittura

2. Nella nuova configurazione «*Scritture*» si va ad aggiornare la sezione «*Controllo Accessi*» effettuando le seguenti azioni (Fig. 3.5):

- Abilitare l'autenticazione token selezionando la policy «*KeyCloak*» (configurazione preesistente per l'integrazione all'authorization server), lasciando invariate le altre opzioni del medesimo riquadro.
 - Disabilitare le altre funzionalità di controllo degli accessi: Autenticazione Trasporto, Autorizzazione e Autorizzazione Contenuti.
3. Dopo aver salvato la nuova configurazione, verificare il riepilogo delle informazioni, che devono corrispondere a quanto riportato in [Fig. 3.6](#).

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

Controllo Accessi del gruppo 'Scrittura'

Note: (*) Campi obbligatori

Autenticazione Token

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

Required Claims

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

Autenticazione Trasporto

Stato	disabilitato
-------	--------------

Autorizzazione

Stato	disabilitato
-------	--------------

Autorizzazione Contenuti

Stato	disabilitato
-------	--------------

SALVA

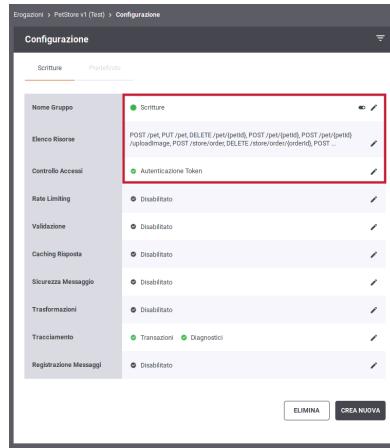


Fig. 3.6: Riepilogo della configurazione effettuata

CAPITOLO 4

Erogazione REST Modelli PA

4.1 Obiettivo

Esporre un servizio REST accessibile in accordo alla normativa prevista dal Modello di Interoperabilità 2018.

4.2 Sintesi

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

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

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

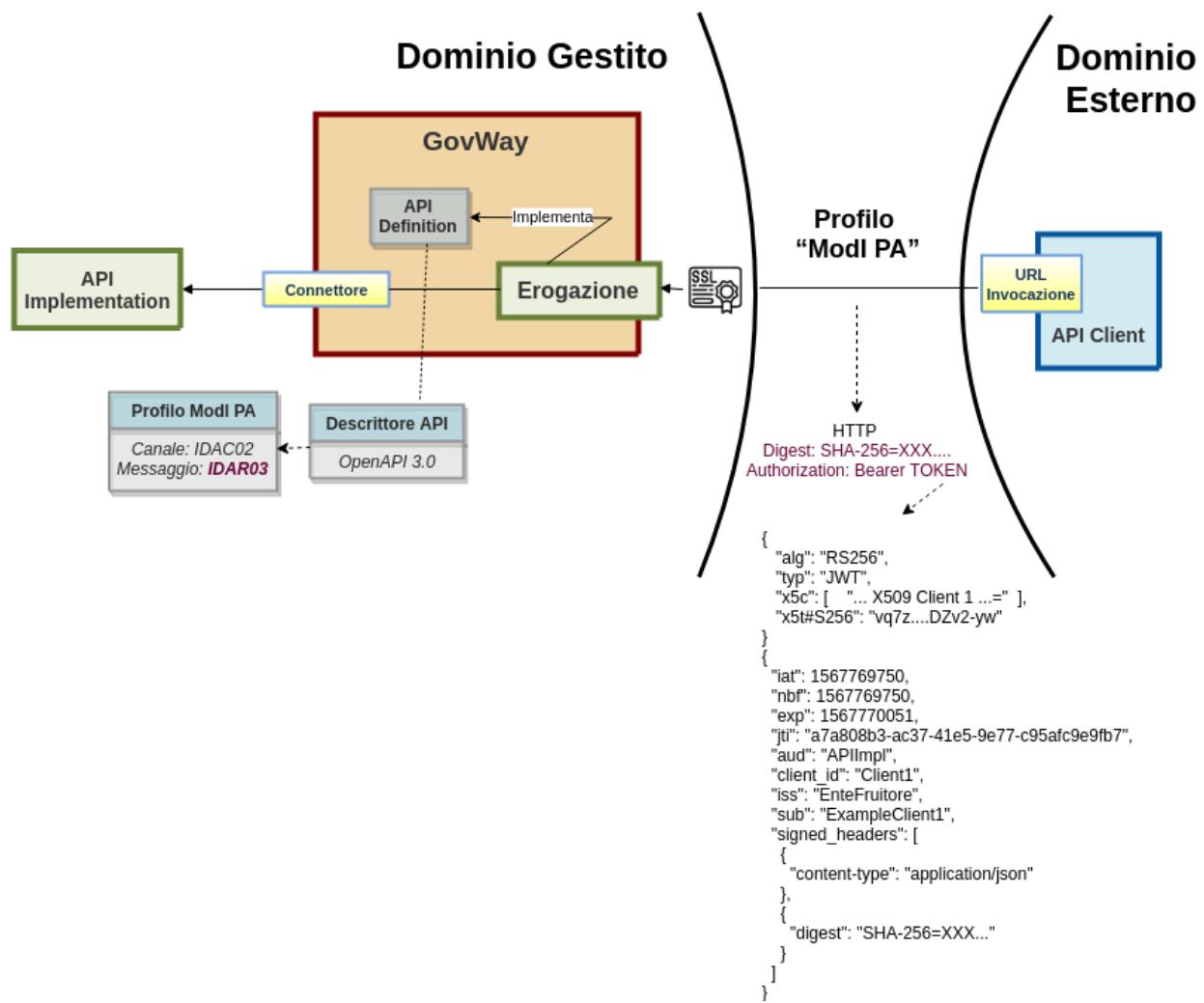


Fig. 4.1: Erogazione ModI PA

4.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API «PetStore», basata su REST, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAR02 e IDAR03.
- un'istanza Govway per la gestione del profilo ModI PA nel dominio dell'erogatore.
- un client del dominio esterno che invoca la «POST /pet» diretto all'erogazione esposta da Govway.
- il server PetStore di esempio che riceve le richieste inoltrate dal Govway e produce le relative risposte.

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

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

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

2019-09-12 17:21:16.848	infolntegration	RicezioneBuste	Autenticazione [ssl] in corso (SSL-Subject 'CN=Soggetto1, OU=test, O=openspcoop.org, L=Pisa, ST=Italy, C=IT, EMAILADDRESS=apoli@link.it') ...
2019-09-12 17:21:16.848	infolntegration	RicezioneBuste	Autenticazione [ssl] effettuata con successo

Fig. 4.2: Sicurezza canale IDAC02

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

4.3.1 Conformità ai requisiti ModI PA

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

Messaggio

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

Headers

Nome

x-forwarded-
proto https

host auth03.govcloud.it

content-type application/json

postman-
token c4e9048a-1038-4c3e-8fa5-18138099b483

user-agent GovWay

HEADER: ALGORITHM & TOKEN TYPE

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

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

PAYLOAD: DATA

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

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

Informazioni ModI PA

ProfiloSicurezzaMessaggio IDAR0302
ProfiloSicurezzaCanale IDAC02
ProfiloInterazione bloccante

Sicurezza Messaggio

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

Headers HTTP Firmati

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

Fig. 4.6: Traccia della richiesta elaborata dall'erogatore

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

4.4 Configurazione

Per la configurazione dello scenario descritto è necessario intervenire sulla govwayConsole (lato fruitore ed erogatore in base all'ambito di propria competenza). Per operare con la govwayConsole in modo conforme a quanto previsto dalla specifica del Modello di Interoperabilità 2018 si deve attivare, nella testata dell'interfaccia, il Profilo di Interoperabilità «ModI PA» (Fig. 4.7).



Fig. 4.7: Profilo ModI PA della govwayConsole

4.4.1 Salvataggio Messaggi

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

A screenshot of the "Richiesta" configuration page in the GovWay console. The page has a header "Richiesta". Underneath, there are two main sections: "Ingresso" and "Uscita". Each section contains three dropdown menus: "Headers", "Body", and "Attachments". In the "Ingresso" section, all three dropdowns show "disabilitato". In the "Uscita" section, all three dropdowns show "abilitato".

Section	Header	Body	Attachments
Ingresso	disabilitato	disabilitato	disabilitato
Uscita	abilitato	abilitato	abilitato

Fig. 4.8: Abilitazione del salvataggio delle richieste in uscita

Si procede quindi con i passi di configurazione del servizio.

4.4.2 Registrazione API

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

Risposta

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

Fig. 4.9: Abilitazione del salvataggio delle risposte in ingresso

Modi PA

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

Fig. 4.10: Profilo ModI PA della govwayConsole

4.4.3 Applicativo Esterno

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

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

Applicativo

Dominio	Esterno
Soggetto	EnteFruitore
Nome *	ExampleClient1

Modi PA

Sicurezza Messaggio

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

Reply Audience/WSA-To

Identificativo dell'applicativo scambiato nei token di sicurezza delle risposte

Fig. 4.11: Configurazione applicativo esterno (fruitore)

4.4.4 Erogazione

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

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

Modi PA - Richiesta

Profilo Sicurezza Messaggio

Riferimento X.509	x5c (Certificate Chain) x5t#256 (Certificate SHA-256 Thumbprint) x5u (URL)
TrustStore Certificati	Default
Audience	PetStore

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

Fig. 4.12: Configurazione richiesta dell'erogazione

Modi PA - Risposta

Profilo Sicurezza Messaggio

Algoritmo	RS256
HTTP Headers da firmare *	Digest x Content-Type x Content-Encoding x
Riferimento X.509	Utilizza impostazioni della Richiesta
KeyStore	Default
Time to Live (secondi) *	300

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

Fig. 4.13: Configurazione risposta dell'erogazione

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



Fig. 4.14: Controllo accessi con autorizzazione degli applicativi esterni

CAPITOLO 5

Fruizione REST ModI PA

5.1 Obiettivo

Fruire di un servizio REST accessibile in accordo alla normativa prevista dal Modello di Interoperabilità 2018.

5.2 Sintesi

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

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

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

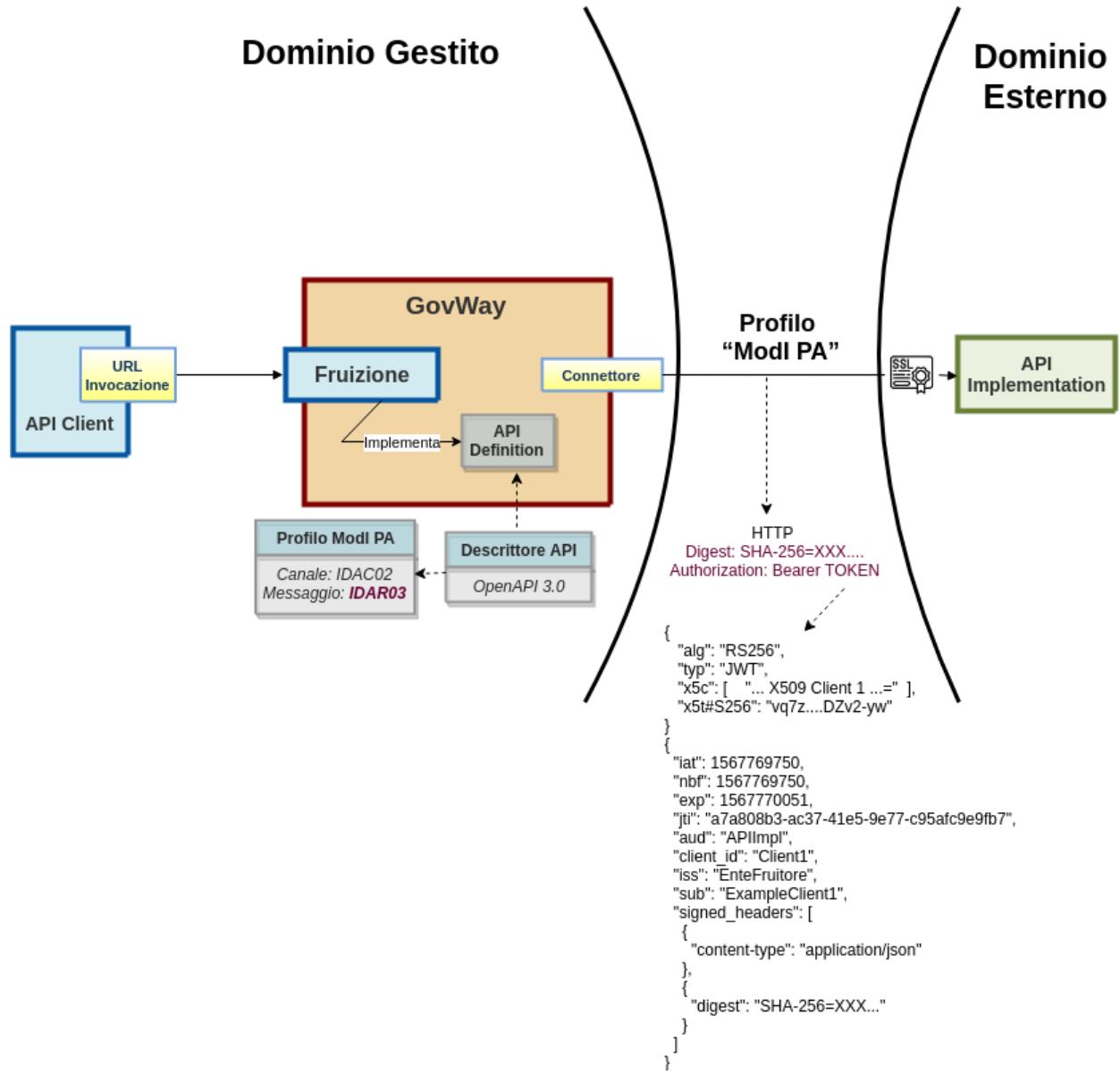


Fig. 5.1: Fruizione ModI PA

5.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

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

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

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

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

5.3.1 Conformità ai requisiti ModI PA

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

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

Messaggio

```

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

Headers

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

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

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

Fig. 5.3: Sicurezza canale IDAC02 sulla fruizione

Informazioni Modelli PA

ProfiloSicurezzaMessaggio IDAR0302
ProfiloSicurezzaCanale IDAC02
ProfiloInterazione bloccante

Sicurezza Messaggio

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

Headers HTTP Firmati

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

Fig. 5.4: Traccia della richiesta elaborata dall'erogatore

5.4 Configurazione

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

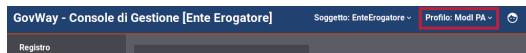


Fig. 5.5: Profilo ModI PA della govwayConsole

5.4.1 Salvataggio Messaggi

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

Si procede quindi con i passi di configurazione del servizio.

5.4.2 Registrazione API

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

5.4.3 Applicativo

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

5.4.4 Fruizione

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

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

Modi PA

Sicurezza Messaggio

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

Identificativo dell'Applicativo scambiato nei token di sicurezza delle risposte

Fig. 5.6: Configurazione applicativo fruitore

Modi PA - Richiesta

Profilo Sicurezza Messaggio

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

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

Audience	PetStore
----------	----------

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

Fig. 5.7: Configurazione richiesta della fruizione

Modi PA - Risposta

Profilo Sicurezza Messaggio

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

Fig. 5.8: Configurazione risposta della fruizione

CAPITOLO 6

Erogazione SOAP Modelli PA

6.1 Obiettivo

Esporre un servizio SOAP accessibile in accordo alla normativa prevista dal Modello di Interoperabilità 2018.

6.2 Sintesi

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

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

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

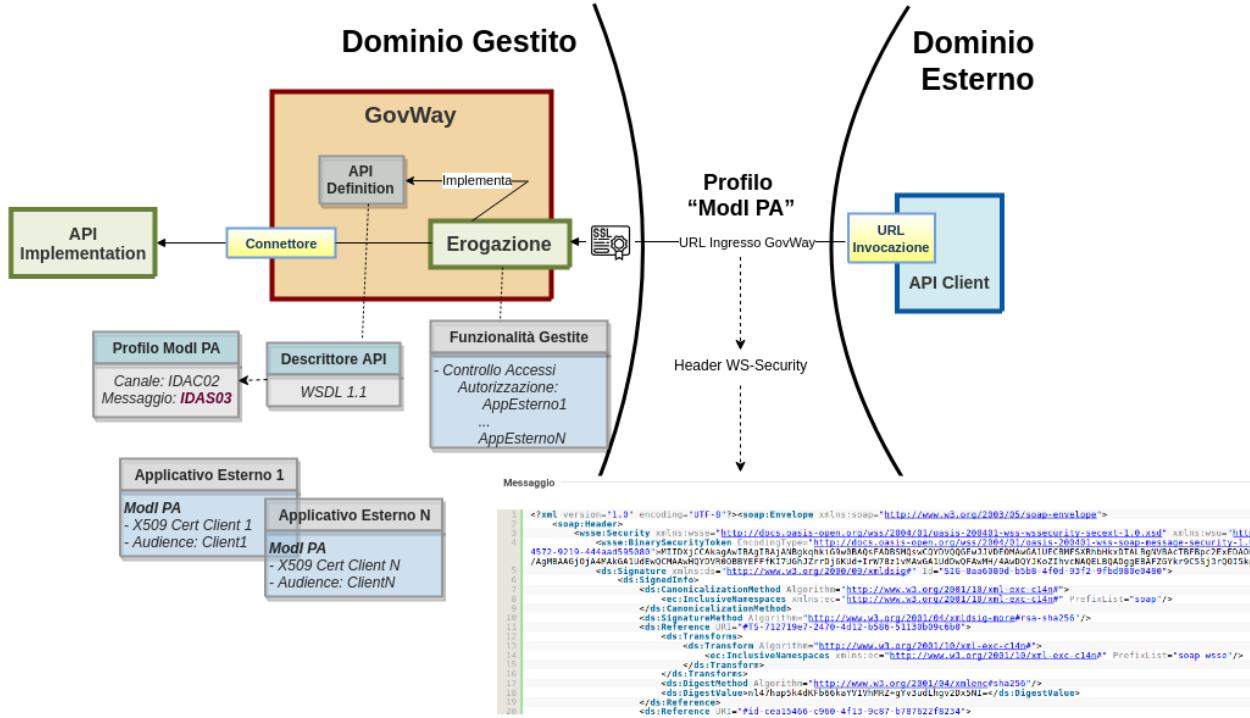


Fig. 6.1: Erogazione SOAP ModI PA

6.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

- una API di esempio (SOAPBlockingImpl), basata su SOAP, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAS02 e IDAS03.
- un'istanza Govway per la gestione del profilo ModI PA nel dominio dell'erogatore.
- un client del dominio esterno che invoca l'azione di esempio «MRequest».
- il server SOAPBlockingImpl di esempio che riceve le richieste inoltrate dal Govway e produce le relative risposte.

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

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

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

Messaggio

```
1 <?xml version="1.0" encoding="UTF-8"?><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
2   <soap:Header>
3     <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0#">
4       <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0#"
c7761d94d64f>-MIIEcCAuegAwIBAgICAN4wDQYJKoZIhvcNAQELBQAwNjELMAKGA1UEBhMCXQhxEABgNBAMCUDvldhewSBDDAteWlWdo6/rXYXIVIDHLYMkEAjBf0L85LBkA6lwJQGPKqawqIvQ/Bw2LpvI1657H+BtNjeFhsSmnNL725HBa/WiVkh78213f5LYC45Y8H9nfC/fa6QJouuDLTxWhkWzNl/ZAjBgNVHRMEAjAAjBEGCWCGSAGG+EIBAQEwIHdGaBzlghkgBhvihCA0EjHjKT3blbNTCBHZw5LcmF0Zwq02xpZw501ENrCnPZmIjYXRlMB0GA1UdDgQWBRRUAiCyEN/JIBWhmVuaptppwNcJRTzI06qmElQmoBTWzbLj0vMXi+zsWPUTWNGNs0z2z1TD51lmeEid1RckBvKvNxcrTrH4Y5shd5ip1Tn73l4C1jTHBHo2ufauobed3fdFqRc6Q2zmEr/0FgpjdpcA7XTXDTdgDkm+WaqMZ7s6DmgW+h7KLk6ub0vEwvzukbaBqycoivDaomD4yWa15csvmubwsRIALRH80uew0JcyeJsfYE87sLFu0bLG934Dt1HnT2CBM8/NKL76LfLQPRGAc7Ev4v0Nc8Wm28Ap01YhpTwPU5Y5P=><wsse:BinarySecurityToken>
5     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-4bbe4224-d2df-4f57-814c-2b8a47ec328d">
6       <ds:SignedInfo>
7         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
8           <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap"/>
9         </ds:CanonicalizationMethod>
10        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
11        <ds:Reference URI="#TS-91e2766f-c512-4440-bfa1-046bbdec9b7">
12          <ds:Transforms>
13            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
14              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap wsse"/>
15            </ds:Transform>
16          </ds:Transforms>

```

Fig. 6.2: Messaggio inviato dal frutto

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

- Informazioni ModI PA

ProfiloSicurezzaMessaggio	IDAS0302
ProfiloSicurezzaCanale	IDAC01
ProfiloInterazione	bloccante

Sicurezza Messaggio

MessageId e137cd92-6dcc-4afd-a502-1d4fc2da677c
WSA-From app1.enteesterno.govcloud.it
WSA-To soapblocking.ente.govcloud.it
Digest SHA256=fa876310714e6e2b1b51a1a0e72e545de9a59a376f8bf5f62efdb039e7955433
Expiration 2019-09-16_18:45:29.899
IssuedAt 2019-09-16_18:44:29.899
X509-Issuer CN=GovWay CA, O=govway.org, C=it
X509-Subject CN=app1.enteEsterno.govcloud.it, O=govway.org, C=it

Fig. 6.3: Traccia della richiesta elaborata dall'erogatore

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

6.3.1 Conformità ai requisiti ModI PA

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

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

6.3.2 Registrazione API

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

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

6.3.3 Erogazione

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

The screenshot shows the 'ModI PA - Richiesta' configuration interface. Under the 'Profilo Sicurezza Messaggio' section, there is a dropdown menu labeled 'Default' and a text input field containing 'soapblocking.ente.govcloud.it'. A note below states: 'Se non viene fornito un valore, il valore atteso all'interno del security token corrisponderà all'url di invocazione'.

Fig. 6.4: Configurazione richiesta dell’erogazione

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

Modi PA - Risposta

Profilo Sicurezza Messaggio

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

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

KeyStore

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

Fig. 6.5: Configurazione risposta dell'erogazione

CAPITOLO 7

Fruizione SOAP ModI PA

7.1 Obiettivo

Fruire di un servizio SOAP accessibile in accordo alla normativa prevista dal Modello di Interoperabilità 2018.

7.2 Sintesi

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

La figura seguente descrive graficamente questo scenario.

Le caratteristiche principali di questo scenario sono:

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

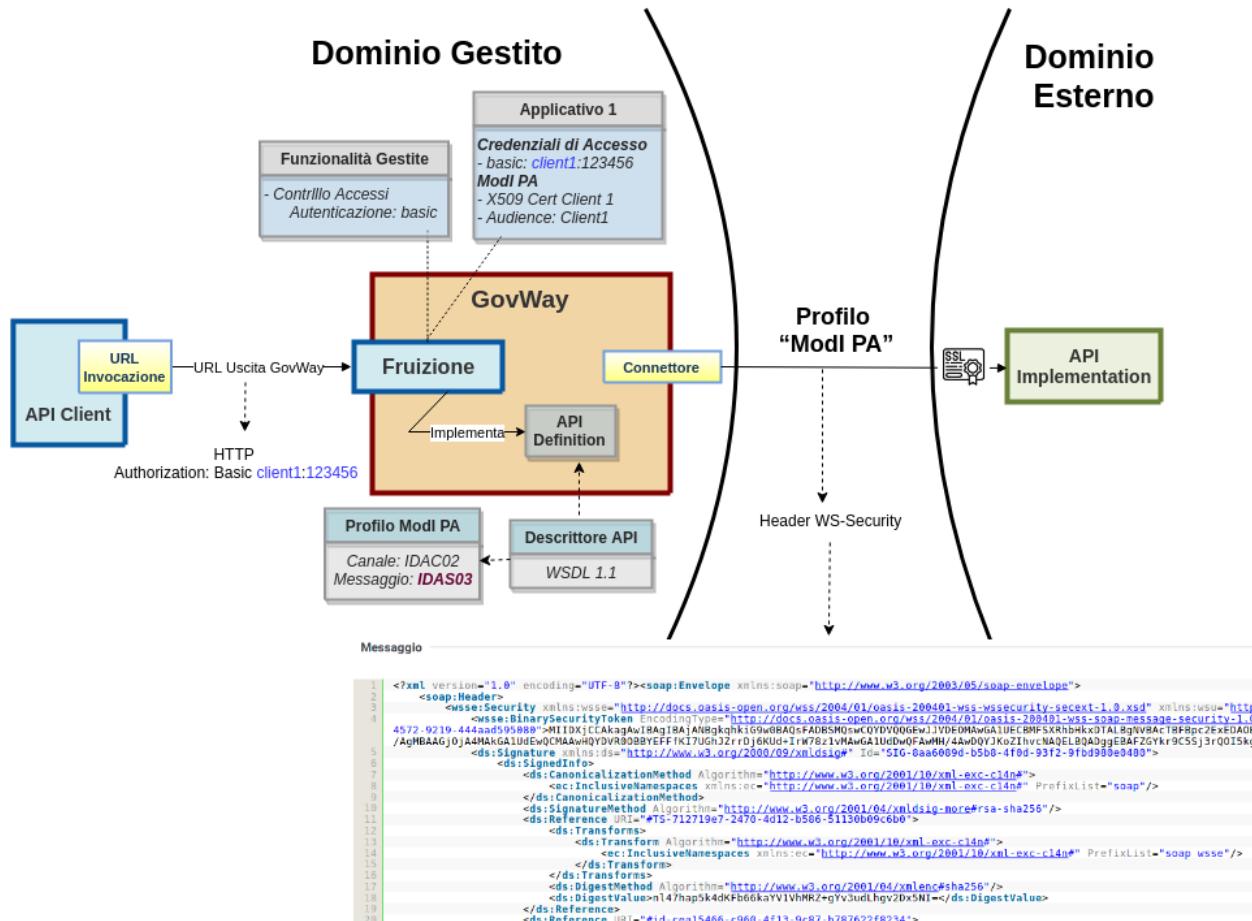


Fig. 7.1: Fruizione SOAP ModI PA

7.3 Esecuzione

L'esecuzione dello scenario si basa sui seguenti elementi:

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

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

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

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

Informazioni ModI PA

ProfiloSicurezzaMessaggio	IDAS0302
ProfiloSicurezzaCanale	IDAC01
ProfiloInterazione	bloccante

Sicurezza Messaggio

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

Fig. 7.2: Traccia della richiesta elaborata dall'erogatore

7.3.1 Conformità ai requisiti ModI PA

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

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

7.3.2 Registrazione API

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

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

7.3.3 Fruizione

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

ModI PA - Richiesta

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

Fig. 7.3: Configurazione richiesta della fruizione

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

ModI PA - Risposta

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

Fig. 7.4: Configurazione risposta della fruizione

CAPITOLO 8

Monitoraggio

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

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

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

	Data Richiesta	Tipologia	API	Operazione	Mittente	Esito
✓	2019-09-05 11:32:00	Erogazione	PetStore v1 (Test)	POST_pet		Ok
!	2019-09-05 10:53:01	Erogazione	PetStore v1 (Test)	POST_pet		Gestione Token Fallita
✓	2019-09-04 16:26:19	Erogazione	PetStore v1 (Test)	GET_pet.petId		Ok
✓	2019-09-04 16:26:06	Erogazione	PetStore v1 (Test)	GET_pet.petId		Ok
✓	2019-09-04 16:25:30	Erogazione	PetStore v1 (Test)	POST_pet		Ok
!	2019-09-04 16:24:05	Erogazione	PetStore v1 (Test)	POST_pet		Gestione Token Fallita
!	2019-09-04 16:22:30	Erogazione	PetStore v1 (Test)	POST_pet		Gestione Token Fallita

Fig. 8.1: Elenco delle transazioni

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

8.1 Transazione in errore

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

Il dettaglio della transazione:

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

8.2 Transazione con esito corretto

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

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

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. ??).

Messaggi diagnostici della transazione con esito regolare

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

Informazioni mittente con presenza del token

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

Visualizzazione del token

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

Dettagli Transazione

Informazioni Generali

Tipologia	Erogazione (API Gateway)
Erogatore	Test
API	PetStore v1
Azione	POST_pet
⚠️ Esito	Gestione Token Fallita
Diagnostici	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

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

ESPORTA

Fig. 8.3: Messaggi diagnostici della transazione in errore

The screenshot shows a user interface for viewing transaction details. At the top, there's a breadcrumb navigation: "Visualizza Transazioni (Live) > Dettagli Transazione > Fault Uscita". Below this, the title "Fault Uscita" is displayed. The main content area contains a JSON object with the following structure:

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

Fig. 8.4: Fault in uscita

Informazioni Generali

Tipologia	Erogazione (API Gateway)
Erogatore	Test
API	PetStore v1
Azione	POST_pet
Profilo Collaborazione	Sincrono
Esito	Ok
Diagnostici	Visualizza Esporta

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

Informazioni Mittente

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

Token Info

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

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

Token Info

```

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

```

[DOWNLOAD](#)