Interoperabilità e Cooperazione Applicativa delle Regioni

Azione di transizione ai nuovi standard

ICAR Playground

Pattern di Interoperabilità

Task: INF-1 (Regione Toscana)
Seconda annualità

Versione 1.2

Indice

1 Introduzione

Questo documento descrive lo strumento **ICAR Playground** realizzato nell'ambito delle attività evolutive previste nel progetto ICAR a fronte dei cambiamenti in materia di interoperabilità applicativa sul fronte nazionale ed europeo. In ambito nazionale, in particolare, AGID ha rilasciato le specifiche del nuovo modello di interoperabilità, che andrà gradualmente a sostituire il precedente modello basato sul protocollo SPCoop e le Porte di Dominio. Questo elemento, insieme agli altri scenari che si stanno delineando sia in Europa, con il progetto *CEF eDelivery*, e ai nuovi standard internazionali, ha definito come esigenza in ambito regionale l'attuazione di un piano di migrazione dell'architettura e dei flussi, sviluppati con il progetto ICAR, al fine di individuare i nuovi casi d'uso, a partire dai quali sviluppare soluzioni che recepiscano le novità normative ed in particolare consentano di conseguire:

1. La piena conformità alle specifiche normative contenute nel nuovo modello di interoperabilità di AGID;
2. L'interoperabilità con i protocolli previsti in ambito europeo dal progetto CEF eDelivery;
3. Il pieno supporto degli standard di mercato.

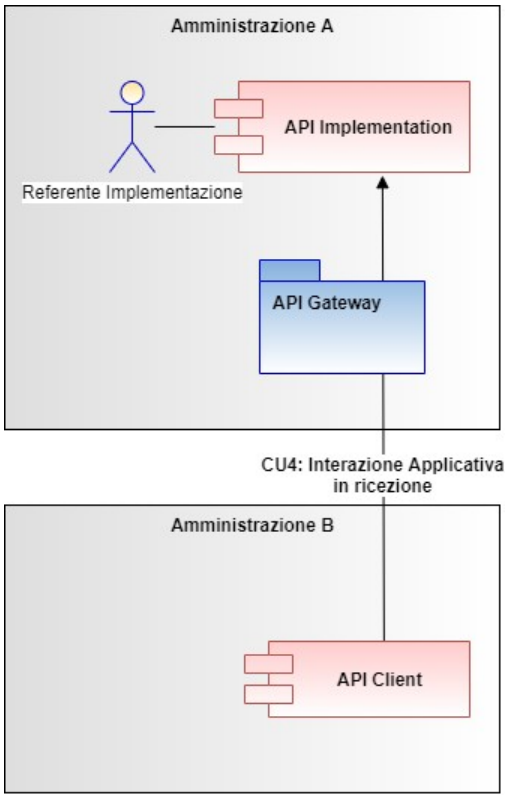
Al fine di poter condividere, sperimentare e far evolvere i temi più operativi del progetto è prevista la realizzazione di un ambiente di test, denominato ICAR Playground, tramite il quale mostrare il corretto uso e buon funzionamento dei pattern di interoperabilità previsti.

2 Gli esempi preconfigurati

La piattaforma di interoperabilità contenuta nel Playground è stata corredata di alcuni scenari di interazione preconfigurati sulla base dei requisiti espressi nel documento ***Task: INF-1 - Pattern Architetturali per l'Interoperabilità Applicativa***, precedente deliverable del progetto. In particolare, le interazioni realizzate seguono le specifiche fornite per i casi d'uso "*CU4: Interazione applicativa in ricezione da domini esterni*" e "*CU5: Interazione applicativa in trasmissione verso domini esterni*" ed i relativi pattern di interoperabilità.

2.1 CU4: Interazione applicativa in ricezione da domini esterni

Il caso d'uso preso a modello per gli esempi è "CU4: Interazione applicativa in ricezione da domini esterni" rappresentato schematicamente nella figura seguente.

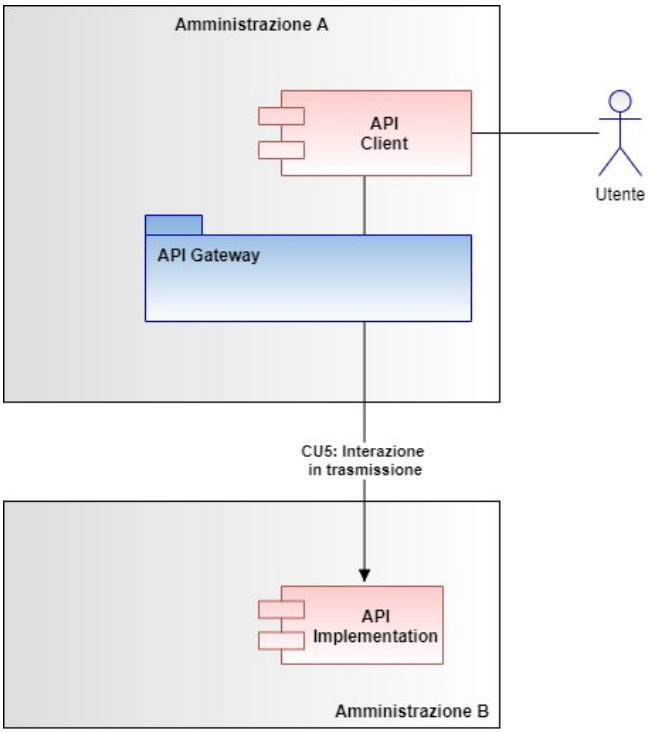


In questo caso d'uso un ente ha la necessità di esporre un servizio ad un suo utilizzatore appartenente ad un altro ente. L'esposizione del servizio avviene attraverso la piattaforma di interoperabilità e in conformità alle linee guida di AGID "ModI". Il pattern di interoperabilità cui si fa riferimento è quindi *CU4-P1: Erogazione Modi.*

Per garantire maggiore completezza negli argomenti trattati il medesimo pattern di interoperabilità è stato sviluppato per i due casi previsti relativi al protocollo: REST e SOAP.

2.2 CU5: Interazione applicativa in trasmissione verso domini esterni

Il caso d'uso preso a modello per gli esempi è "CU5: Interazione applicativa in trasmissione verso domini esterni" rappresentato schematicamente nella figura seguente.



In questo caso d'uso un ente ha la necessità di accedere un servizio erogato da un ente esterno, per conto di un proprio utente. L'accesso al servizio esterno avviene attraverso la piattaforma di interoperabilità e in conformità alle linee guida di AGID "ModI". Il pattern di interoperabilità cui si fa riferimento è quindi *CU5-P1: Fruizione Modi con Identificazione Utente.*

2.3 I servizi di esempio

Per quanto riguarda le implementazioni dei servizi riferiti nei casi di esempio sono stati utilizzati due endpoint pubblici appositamente creati per effettuare dei test:

- **PetStore**: la simulazione del negozio di animali basata su API REST

  endpoint: https://petstore.swagger.io/v2

- **LuhnCheckerSoap**: un servizio di verifica carte di credito basato su API SOAP

  endpoint: https://ws.cdyne.com/creditcardverify/luhnchecker.asmx

I due endpoint devono risultare raggiungibili dall'API Gateway e quindi dall'ambiente dove sono stati dispiegati i docker.

3 Le interazioni previste

In base alle configurazioni presenti sull'API Gateway si possono verificare quelle che sono le interazioni previste dagli esempi del Playground ICAR, riscontrabili anche nella collection Postman inclusa (il cui indice è quello della figura seguente).

Le interazioni presenti nella collection Postman sono:

1. **Erogazione Pubblica (findByStatus)**

   Operazione di lettura (servizio REST) di una lista al fine di recuperare l'identificativo di un elemento. Erogazione sul dominio interno fruita da un dominio esterno con protocollo trasparente.

2. **Erogazione Pubblica (getPet)**

   Operazione di lettura (servizio REST) per recuperare il dettaglio dell'elemento individuato con l'interazione precedente. Erogazione sul dominio interno fruita da un dominio esterno con protocollo trasparente.

3. **Erogazione REST ModI (Post Pet)**

   Operazione di scrittura su servizio REST erogato da dominio interno la cui richiesta proviene da un dominio esterno. Erogazione sul dominio interno fruita da un dominio esterno con protocollo ModI.

4. **Erogazione SOAP ModI (CheckCCResult)**

   Operazione di scrittura su servizio SOAP erogato da dominio interno la cui richiesta proviene da un dominio esterno. Erogazione sul dominio interno fruita da un dominio esterno con protocollo ModI.

5. **Fruizione REST OAuth2 + ModI (Post Order)**

   Operazione di scrittura su servizio REST fruito dal dominio interno ed erogata da un dominio esterno. La fruizione avviene tramite protocollo ModI.

6. **Fruizione REST OAuth2 con Asserzione JWT**

   Operazione di scrittura su servizio REST fruito dal dominio interno ed erogata da un dominio esterno. Il servizio erogato richiede l’autenticazione del client tramite invio di un

access token rilasciato dal dominio erogatore. Per il rilascio del token è necessario autenticarsi sull'authorization server tramite un'asserzione JWT firmata attraverso un certificato X.509 del client in relazione di trust con il dominio erogatore.

7. **Fruizione REST con accesso tramite PDND**

   Operazioni per l'accesso ad un "e-Service" erogato dall'ente esterno per il quale è stato sottoscritto un accordo di interoperabilità tramite la PDND. Per l'accesso autenticato al servizio l'API Gateway negozia l'access token sulla PDND, in base a quanto previsto dalla normativa di riferimento per l'utilizzo di tale piattaforma.

Di seguito una descrizione dettagliata di tutti i casi previsti.

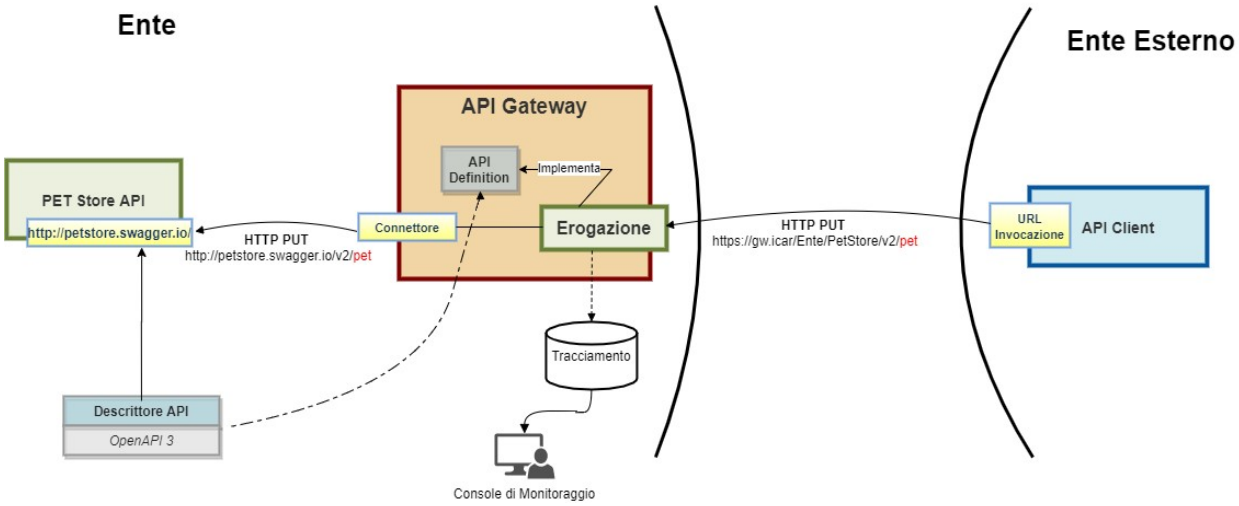
3.1 Erogazione Pubblica

PetStore@Ente v1

API Rest: PetStore v1

Erogazione del servizio PetStore basata sul protocollo REST. Questa erogazione non prevede meccanismi di autenticazione nè autorizzazione, consente quindi un libero accesso al servizio da parte di qualunque client tramite la relativa API REST.

La figura seguente fornisce una rappresentazione d'insieme dell'intero flusso applicativo.

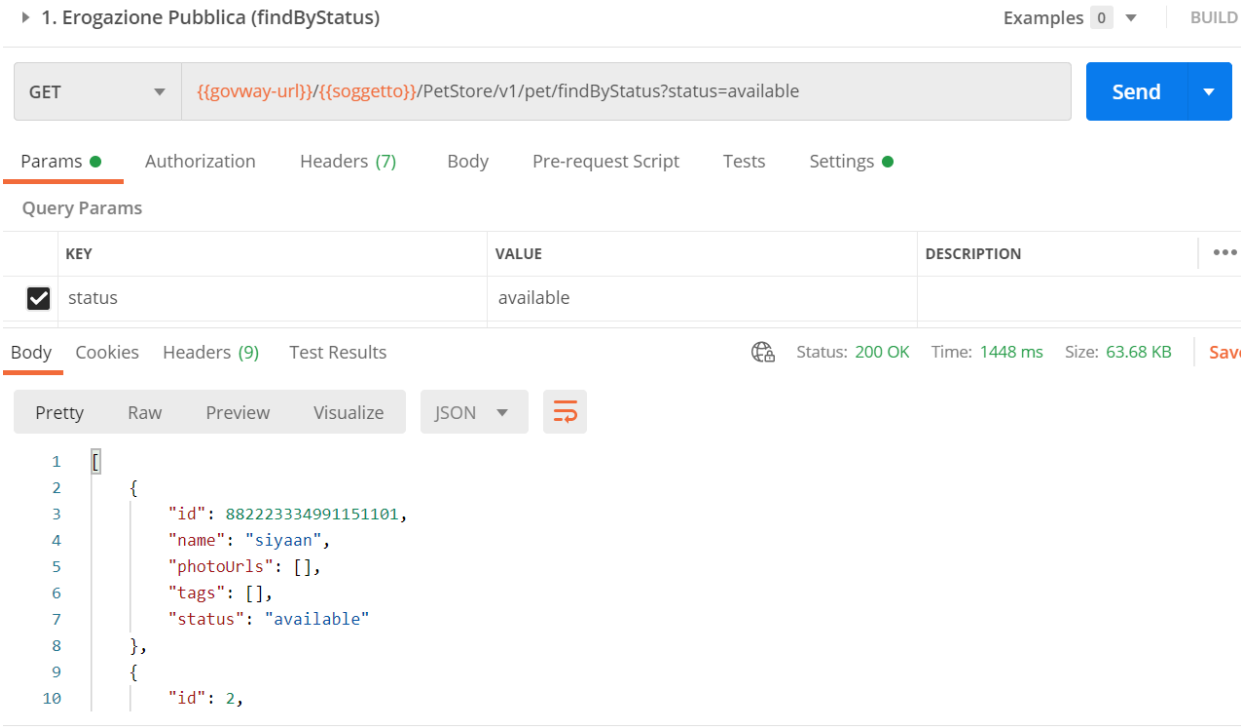


L'esecuzione può essere effettuata tramite la due interazioni presenti nella collection Postman:

- **Erogazione Pubblica (findByStatus)**

  interazione che esegue l'operazione *GET /pet/findByStatus* al fine di interrogare l'archivio degli animali dello store filtrando in base allo stato dell'item.

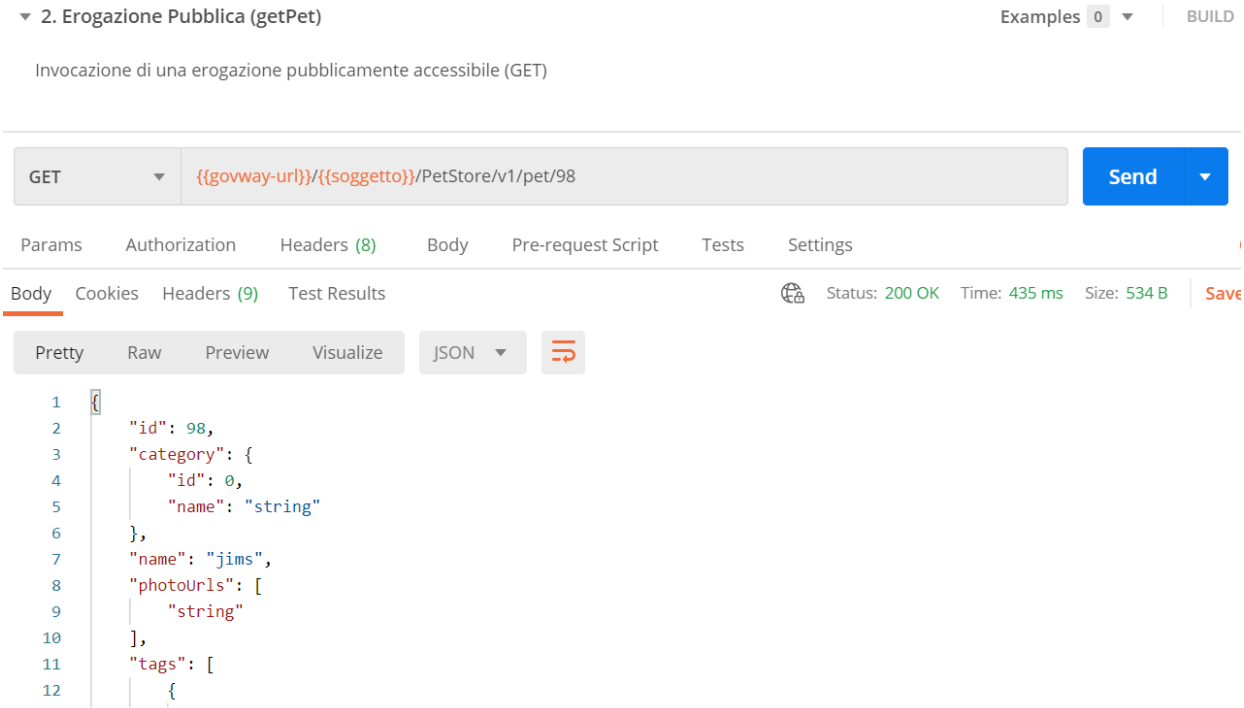
  La figura seguente mostra l'effetto dell'esecuzione dopo aver premuto il pulsante "Send".



- **Erogazione Pubblica (getPet)**

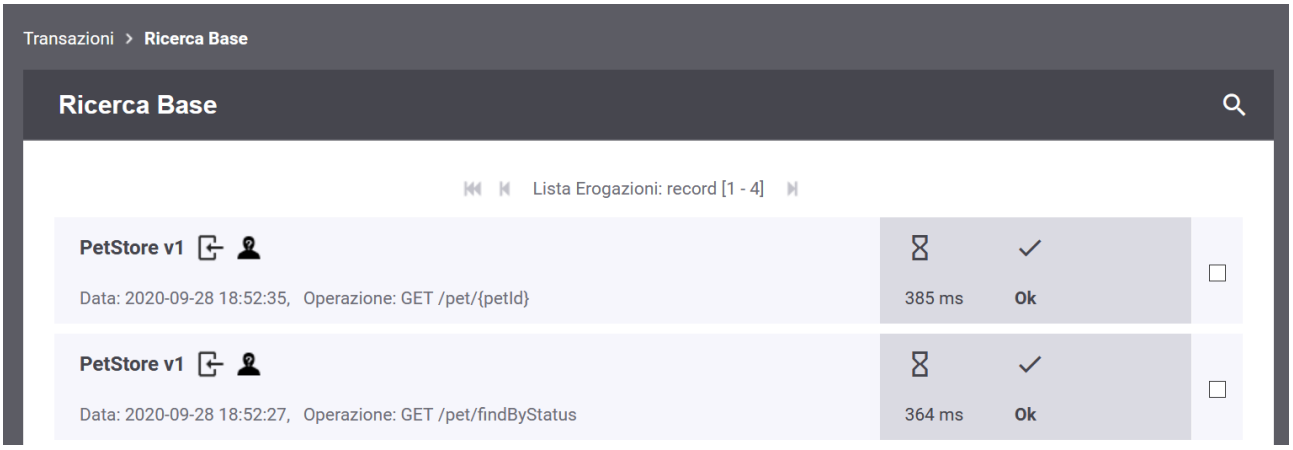
  interazione che esegue l'operazione *GET /pet/{id_pet}* al fine di ottenere il dettaglio di un animale dello store fornendone l'identificativo come parametro.

  La figura seguente mostra l'effetto dell'esecuzione dopo aver premuto il pulsante "Send".



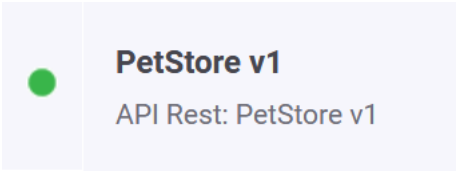
Il riscontro di quanto avvenuto con le due interazioni precedenti si può verificare attraverso la console di monitoraggio dell'API Gateway:

1. Selezionare la voce di menu "Monitoraggio > Transazioni" e scegliere la Ricerca Generica "Base"
2. Selezionare la Modalità di Ricerca di tipo "Erogazione"
3. Le due interazioni appena effettuate saranno visibili in cima all'elenco visualizzato



4. I dati presenti in ciascun elemento in elenco forniscono in sintesi di dati della transazione rilevati dall'API Gateway. La selezione di un singolo elemento consente di visualizzare il dettaglio della transazione.

3.2 Erogazione REST ModI



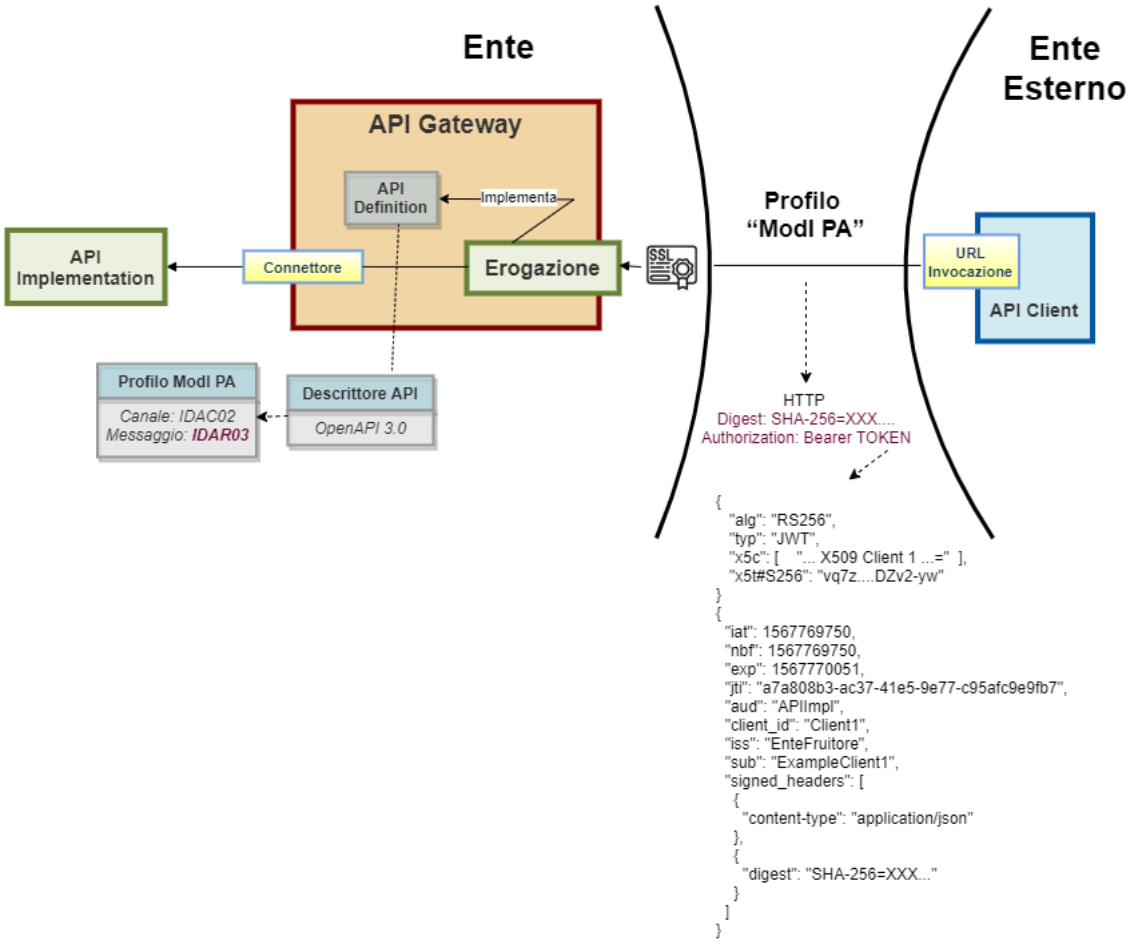
Erogazione del servizio PetStore basata sul profilo di interoperabilità ModI (compatibile alle linee guida di AGID) e protocollo REST.

Le principali caratteristiche di questa interazione sono le seguenti:

1. L'erogazione del servizio verso i client è fornita attraverso il profilo di sicurezza canale IDAC02. Quindi è necessario che i domini coinvolti abbiano attuato il trust dei reciproci certificati SSL al fine di garantire la mutua autenticazione dei sistemi.
2. L'autenticazione degli applicativi, effettivamente mittente e destinatario della comunicazione, è garantita tramite l'applicazione del profilo di sicurezza messaggio IDAR02 con l'integrazione del profilo IDAR03 a garanzia dell'integrità del payload scambiato.
3. Tracciatura a norma degli scambi effettuati, sia riguardo la comunicazione di richiesta che quella di risposta. La conservazione delle tracce, complete delle evidenze di trasmissione, fornisce supporto al non ripudio.

La figura successiva fornisce una rappresentazione d'insieme dell'intero flusso applicativo:

- L'API PetStore, basata su REST, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAR02 e IDAR03.
- L'API Gateway Govway per la gestione del profilo ModI nel dominio dell'erogatore.
- Il client del dominio esterno che invoca la *POST /pet* diretta all'erogazione esposta da Govway.
- Il server PetStore (API Implementation) che riceve le richieste inoltrate dal Govway e produce le relative risposte.



Il flusso applicativo prevede in dettaglio:

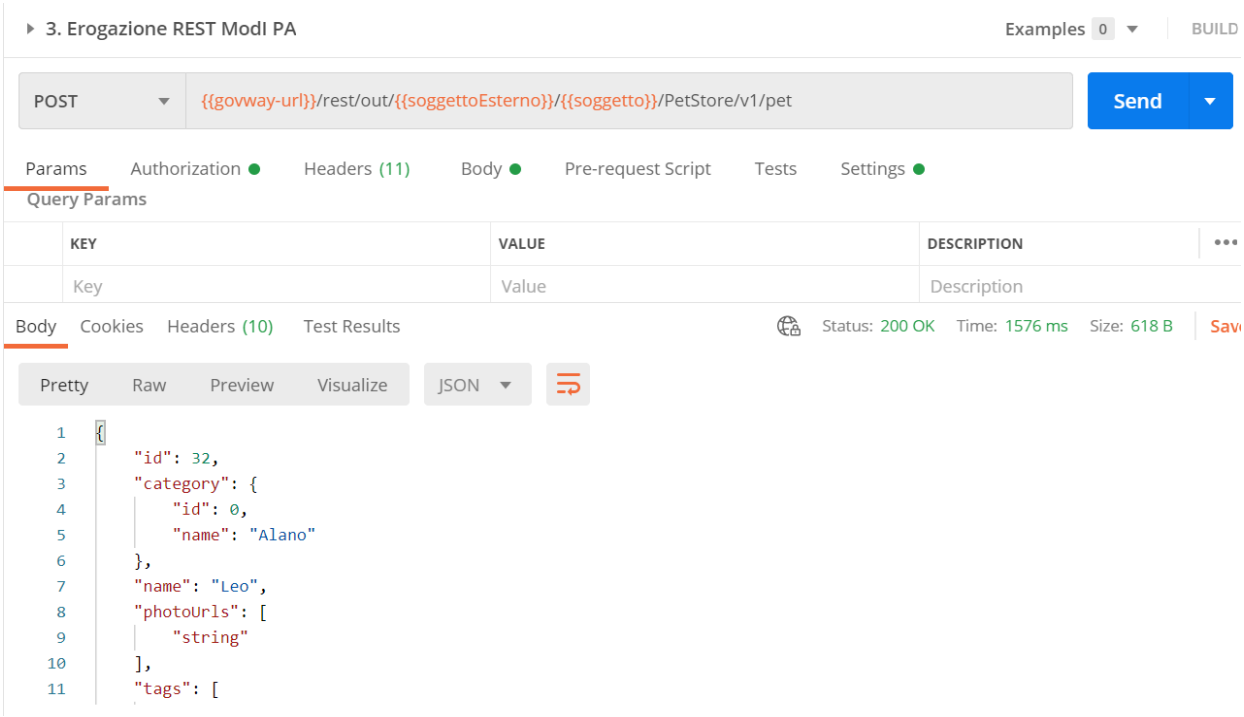
1. L'invio della richiesta da parte del client fruitore (Postman). La richiesta è comprensiva del token di sicurezza, composto in accordo al profilo di sicurezza messaggio IDAR02 + IDAR03. La comunicazione avviene in SSL con autenticazione del client in accordo al profilo di sicurezza canale IDAC02.
2. Il Reverse Proxy termina la comunicazione SSL occupandosi dell'autenticazione del client tramite il repository dei certificati "trusted". Inoltra quindi la richiesta pervenuta, insieme al cerificato SSL ricevuto, all'API Gateway.
3. L'API Gateway, tramite il certificato SSL ricevuto, identifica il dominio mittente attuando eventuali politiche di autorizzazione.

4. L'API Gateway effettua la validazione del token Modi, per la sicurezza messaggio, tramite il repository dei certificati degli applicativi "trusted". Tali controlli sono volti all'autenticazione dell'applicativo mittente ed alla verifica dell'integrità del payload.
5. L'API Gateway effettua il tracciamento dei dati inerenti la richiesta con tutti i dati estratti nel corso dell'elaborazione effettuata. La traccia della richiesta comprende anche il token Modi originale inviato dal mittente (ai fini del non ripudio).
6. L'API Gateway inoltra la richiesta al servizio erogato (API Implementation, PetStore in questo caso specifico). La richiesta inviata è corredata da un elemento contenente i dati di integrazione che comprende le informazioni ricavate dal token Modi, accessibili in maniera semplice dal servizio. In opzione è possibile configurare l'inoltro al servizio del token originale.
7. PetStore produce ed invia la risposta all'API Gateway.
8. L'API Gateway produce il token Modi da inserire nella risposta avvalendosi di un Keystore relativo agli applicativi interni.
9. L'API Gateway effettua il tracciamento dei dati inerenti la risposta, mantenendo la correlazione alla richiesta ed includendo il token prodotto al passo precedente.
10. L'API Gateway inoltra la risposta, completa di token Modi, al Reverse Proxy .
11. Il Reverse Proxy chiude la comunicazione HTTPS girando la risposta al Client ModI (Postman).

L’esecuzione può essere effettuata tramite l'interazione Erogazione REST ModI presente nella collection Postman:

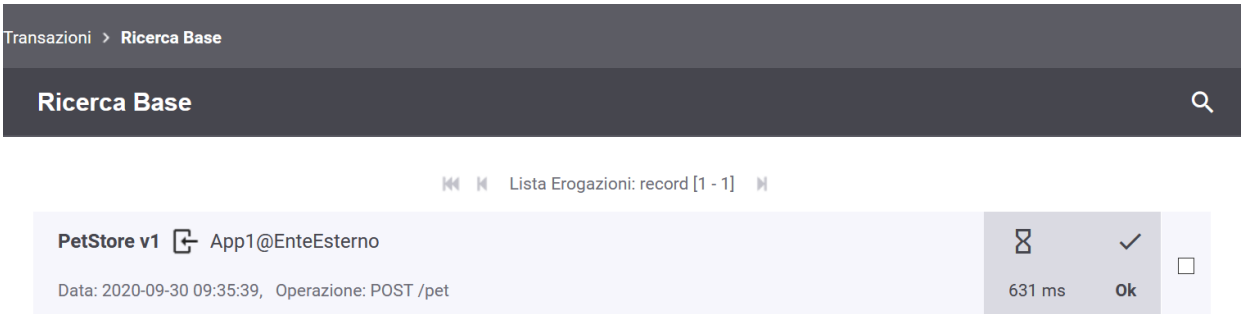
- **Erogazione REST ModI**

  La figura seguente mostra l’effetto dell’esecuzione dopo aver premuto il pulsante “Send”.



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 di monitoraggio dell'API Gateway:

1. Selezionare la voce di menu "Monitoraggio > Transazioni" e scegliere la Ricerca Generica "Base"
2. Selezionare la Modalità di Ricerca di tipo "Erogazione"
3. La transazione appena effettuata è visualizzata nell'elenco con i principali dati (servizio invocato, soggetto mittente, timestamp, ecc).



4. Accedendo al dettaglio della transazione, nella sottosezione "Diagnostici", è possibile verificare come lo scambio del messaggio con il dominio fruitore (comunicazione interdominio) avvenga in accordo al profilo IDAC02 e quindi con protocollo SSL e autenticazione client. Nei diagnostici sono visibili i dati di validazione del certificato ricevuto durante la fase di autenticazione.

2020-09-30 09:35:39.592	infoIntegration	RicezioneBuste	Ottenute credenziali di accesso (SSL-Subject 'CN=enteEsterno.icar, O=icar.it, C=it') fornite da Traefik
2020-09-30 09:35:39.592	infoIntegration	RicezioneBuste	Autenticazione [ssl] in corso (SSL-Subject 'CN=enteEsterno.icar, O=icar.it, C=it') ...
2020-09-30 09:35:39.600	infoIntegration	RicezioneBuste	Autenticazione [ssl] effettuata con successo

6. Nella sezione del dettaglio "Dettagli Messaggio > Dettagli Richiesta" si può visualizzare il messaggio che è stato inviato dal fruitore (Contenuti Ingresso > Visualizza). Come si nota, al payload JSON è associato un insieme di header HTTP tra i quali
   - *Authorization*, che contiene il token di sicurezza
   - *Digest*, che contiene il valore per la verifica dell'integrità del payload.
7. Il token di sicurezza ricevuto viene decodificato e validato dall'API Gateway assieme alla verifica del digest del messaggio. Eseguendo la decodifica del token (ad esempio con JWT.io) si può verificare come la sezione "header" riporti l'identità del client (claim *kid*) e il relativo certificato X.509 (claim *x5c*).

HEADER: ALGORITHM & TOKEN TYPE

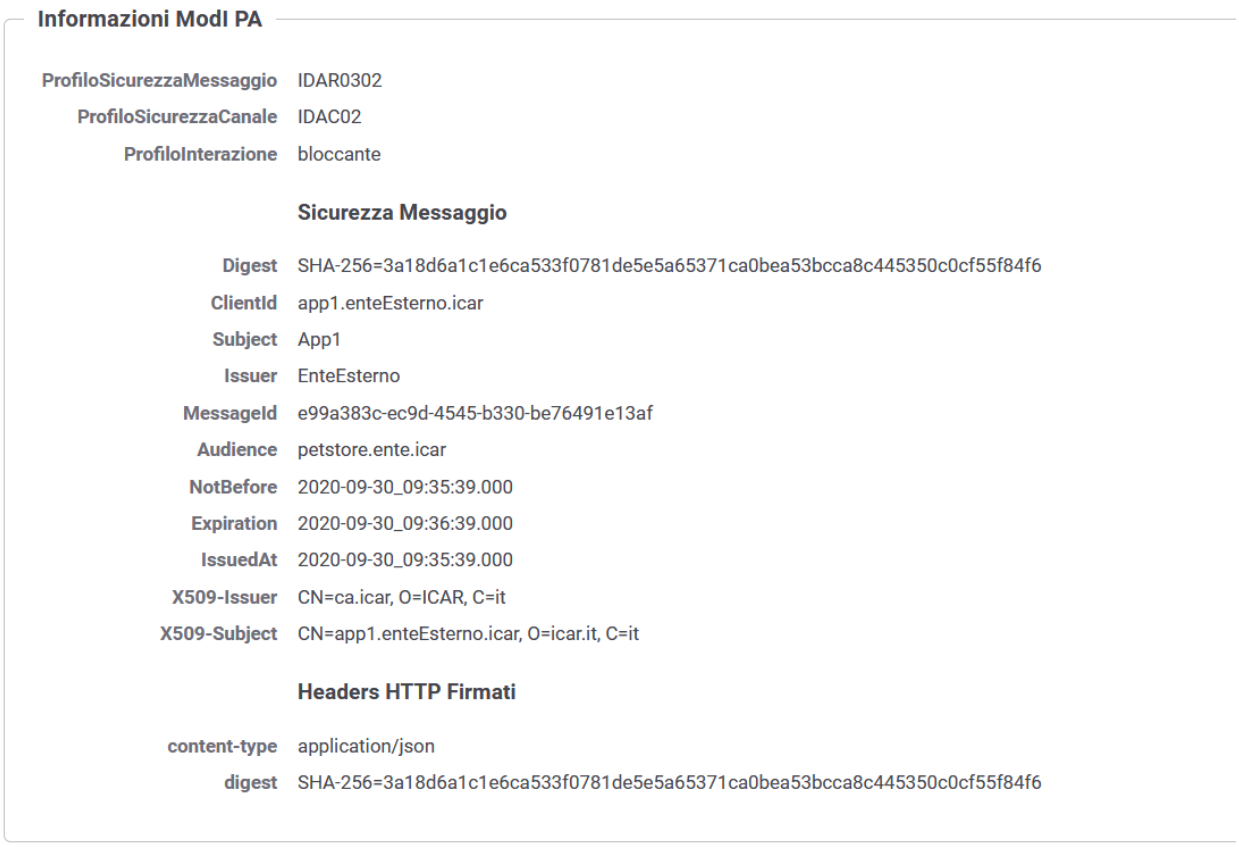

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "app1.enteEsterno.icar",
  "x5c": [

"MIIE8TCCAtmgAwIBAgICAQIwDQYJKoZIhvcNAQELBQAwLjELMAkGA1
UEBhMCaXQxDTALBgNVBAoMBElDQVIxEDAOBgNVBAMMB2NhLmljYXIwH
hcNMjAwOTI5MTUzNTUwWhcNMjIwOTE5MTUzNTUwWjA/MQswCQYDVQQG
EwJpdDEQMA4GA1UECgwHaWNhci5pdDEeMBwGA1UEAwwVYXBwMS5lbnR
lRXN0ZXJuby5pY2FyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
KCAQEAyJbp5wkF3JyXXC
/prI1xvpfWGpW2vBAklKAW48HQE6Jk6hnyD+no6nUcn+4I4Ug+YcQOi
LnioOzsPGa1q573swBdgXHkRm2salzOkddnuAHfh78UopAgSaRr+9dT
d2Ugj2emaqaaoH7Vrt6jZ3TmwI8ng
/2aYG9JGxUjYLgNuPQ7tqVTVMmtsxrYcOlcpzIRzA824HC43pTbFXae
c1aR03suSxtu3iemoIyLE4Ecb6VR
/OIvuL8zd4skyzlWe+avl+L9CQ3UmIvU806H6HbJJfdCaH
/J2ZXiqvQy98EjfSzBVVLE3zICXjxZY1RpDxAWMpIntKZ/757SZuJu
/D/4kwIDAQABo4IBBjCCAQIwCQYDVR0TBAIwADARBglghkgBhvhCAQE
EBAMCB4AwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIE
NsaWVudCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUMxp2DQ4mKbFxdm+zz
b9+ClazhHswaQYDVR0jBGIwYIAUH7U5My19ZEDjY3JAzIuoT
```


8. La sezione "Payload" del token di sicurezza contiene i riferimenti temporali e le componenti firmate del messaggio di richiesta, compreso il digest.

PAYLOAD: DATA

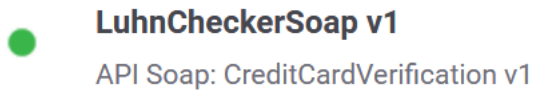

```
{
  "iat": 1601451339,
  "nbf": 1601451339,
  "exp": 1601451399,
  "jti": "e99a383c-ec9d-4545-b330-be76491e13af",
  "aud": "petstore.ente.icar",
  "client_id": "app1.enteEsterno.icar",
  "iss": "EnteEsterno",
  "sub": "App1",
  "signed_headers": [
    {
      "digest":
"SHA-256=3a18d6a1c1e6ca533f0781de5e5a65371ca0bea53bcca8
c445350c0cf55f84f6"
    },
    {
      "content-type": "application/json"
    }
  ]
}
```


9. L'intero processo di validazione del token viene effettuato dall'API Gateway 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 (il servizio PetStore in questo caso).
10. La sezione "Dettagli Messaggio > Dettagli Richiesta", nel dettaglio della transazione della console di monitoraggio dell'API Gateway, selezionando "Traccia > Visualizza", il riquadro "Informazioni ModI > Sicurezza Messaggio" riporta la traccia con le informazioni di sicurezza estratte dal token.



11. Dopo l'inoltro al servizio erogatore, l'API Gateway riceve la risposta e la elabora producendo il relativo token di sicurezza. Nel dettaglio della transazione è possibile visualizzare il messaggio di risposta in uscita, dove si rileva la presenza del token prodotto nell'header HTTP Authorization (analogamente a quanto visto per il messaggio di richiesta).

3.3 Erogazione SOAP ModI



Erogazione del servizio CreditCardVerification basata sul profilo di interoperabilità ModI e protocollo SOAP.

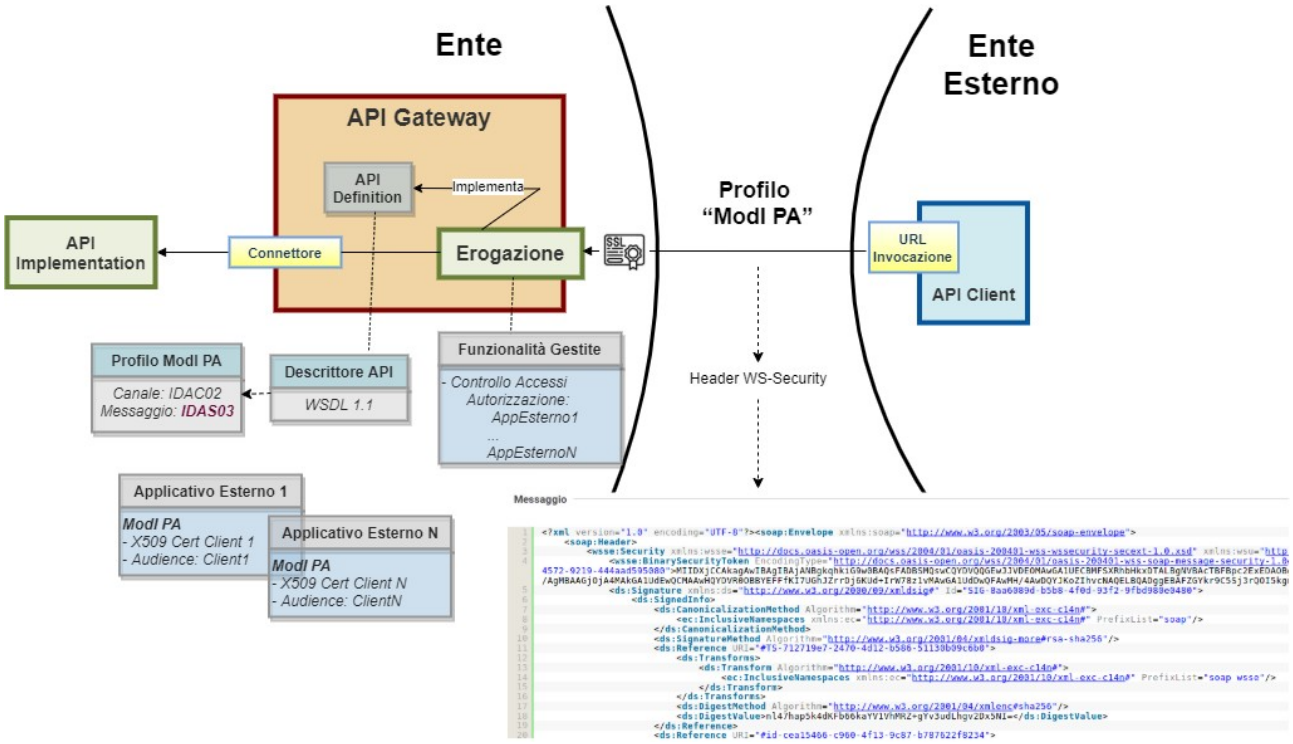
Le principali caratteristiche di questa interazione sono le seguenti:

1. L'erogazione del servizio verso i client è fornita attraverso il profilo di sicurezza canale IDAC02. Quindi è necessario che i domini coinvolti abbiano attuato il trust dei reciproci certificati SSL al fine di garantire la mutua autenticazione dei sistemi.
2. L'autenticazione degli applicativi, effettivamente mittente e destinatario della comunicazione, è garantita tramite l'applicazione del profilo di sicurezza messaggio IDAS02 con l'integrazione del profilo IDAS03 a garanzia dell'integrità del contenuto scambiato.

3. Tracciatura a norma degli scambi effettuati, sia riguardo la comunicazione di richiesta che quella di risposta. La conservazione delle tracce, complete delle evidenze di trasmissione, fornisce supporto al non ripudio.

La figura successiva fornisce una rappresentazione d'insieme dell'intero flusso applicativo:

- L'API di esempio (Credit Card Verification), basata su SOAP, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAS02 e IDAS03.
- L'API Gateway per la gestione del profilo ModI nel dominio dell'erogatore.
- Il client Postman del dominio esterno che invoca l'azione di esempio «CheckCC».
- il server "Credit Card Verification" di esempio che riceve le richieste inoltrate dall'API Gateway e produce le relative risposte.



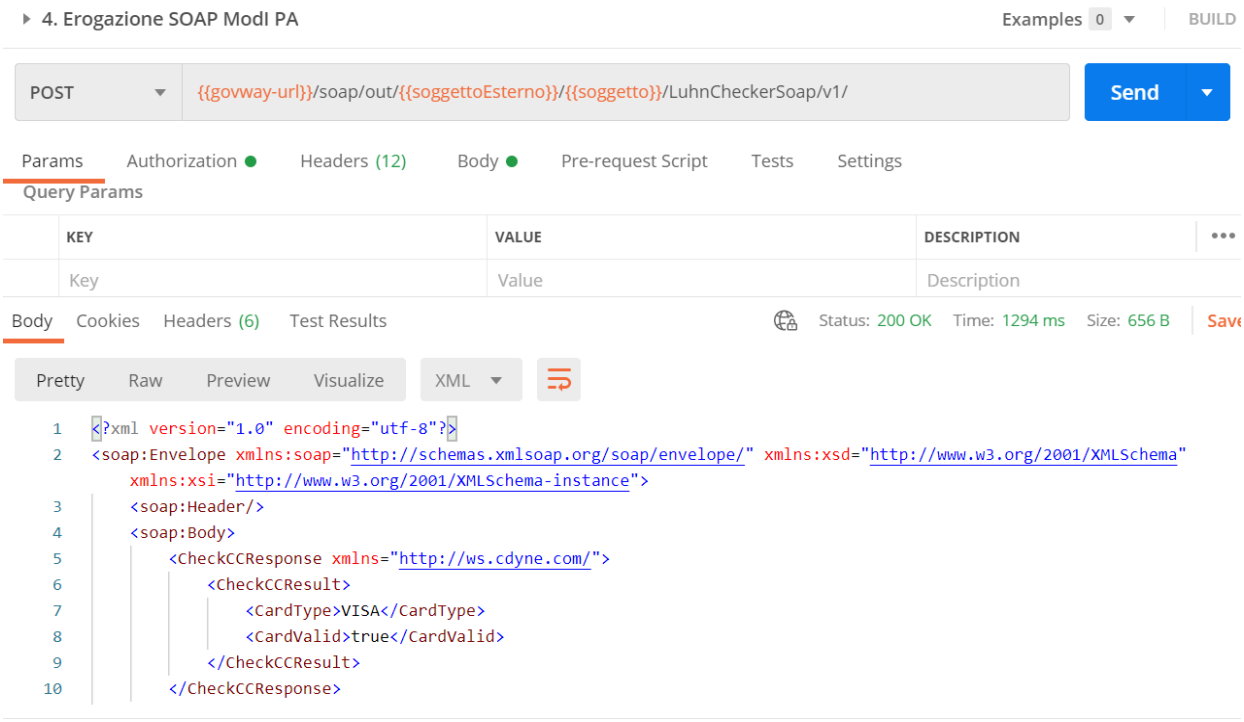
Il flusso applicativo di questa interazione è del tutto analogo a quanto già descritto nel caso dell'erogazione REST nella sezione precedente.

L'esecuzione può essere effettuata tramite l'interazione Erogazione SOAP ModI presente nella collection Postman:

- **Erogazione SOAP ModI**

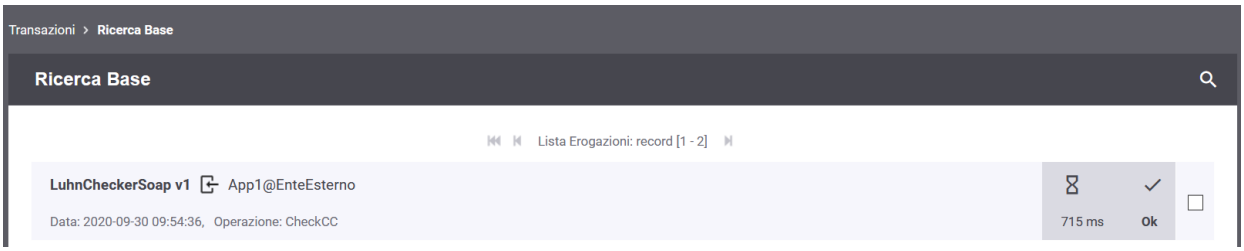
  Interazione che esegue la soapAction "http://ws.cdyne.com/CheckCC" per la verifica di una carta di credito i cui riferimenti sono indicati nel messaggio di richiesta.

  La figura seguente mostra l'effetto dell'esecuzione dopo aver premuto il pulsante "Send".



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 di monitoraggio dell'API Gateway:

1. Selezionare la voce di menu "Monitoraggio > Transazioni" e scegliere la Ricerca Generica "Base"
2. Selezionare la Modalità di Ricerca di tipo "Erogazione"
3. La transazione appena effettuata è visualizzata nell'elenco con i principali dati (servizio invocato, soggetto mittente, timestamp, ecc).



4. Dal dettaglio della richiesta, analogamente a quanto visto per il caso REST, possono essere verificate le evidenze del flusso applicativo. In particolare il messaggio ricevuto dal mittente che, come si nota per il caso 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*).

Messaggio

```
<?xml version="1.0" encoding="UTF-8"?><soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://doc
            <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base6
/VbSmOhMqQwMC4xCzAJBgNVBAYTAml0MQ0wCwYDVQQKDARJQ0FSMRAwDgYDVQQDDAdjYS5pY2FyghR9hbZEMrGLrj98cuuc6XLRNXFLBjAOBgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAww
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-2f0b0803-427b-46a5-8631-05dbff7eef3a">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soapenv"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <ds:Reference URI="#TS-7d6b42c4-07eb-4dd2-bc06-07c5cde3e7c4">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse soapenv"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>phmdGjtPiVZqjSCgVZPl7f46IDpHCRDQquDi2iFnliA=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#id-5b675c73-659c-435e-9e4f-763d01ac66eb">
                        <ds:Transforms>
```

5. Il messaggio ricevuto dall'API Gateway 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 console di monitoraggio dell'API Gateway, andando a consultare la traccia del messaggio di richiesta. Nella sezione "Sicurezza Messaggio" sono riportate le informazioni estratte dal token di sicurezza presente nell'header SOAP.

Informazioni ModI PA

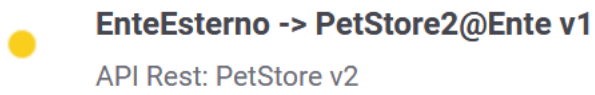
ProfiloSicurezzaMessaggio	IDAS0302
ProfiloSicurezzaCanale	IDAC02
ProfiloInterazione	bloccante

Sicurezza Messaggio

MessageId	f3b72c05-f262-4d7f-af77-1d6b306e9108
WSA-From	app1.enteEsterno.icar
WSA-To	luhnCheckerSoap.ente.icar
Digest	SHA256=1cbcf3e1d623ae2828537af84c2f7f172879e99f96c95d222c6433a421b9ac79
Expiration	2020-09-30_09:55:35.970
IssuedAt	2020-09-30_09:54:35.970
X509-Issuer	CN=ca.icar, O=ICAR, C=it
X509-Subject	CN=app1.enteEsterno.icar, O=icar.it, C=it

6. Dopo l'inoltro al servizio erogatore, l'API Gateway riceve la risposta e la elabora producendo il relativo header ws-security da inserire nel messaggio di risposta. Sulla console di monitoraggio è possibile visualizzare il messaggio di risposta in uscita analogamente al caso del messaggio di richiesta.

3.4 Fruizione REST ModI



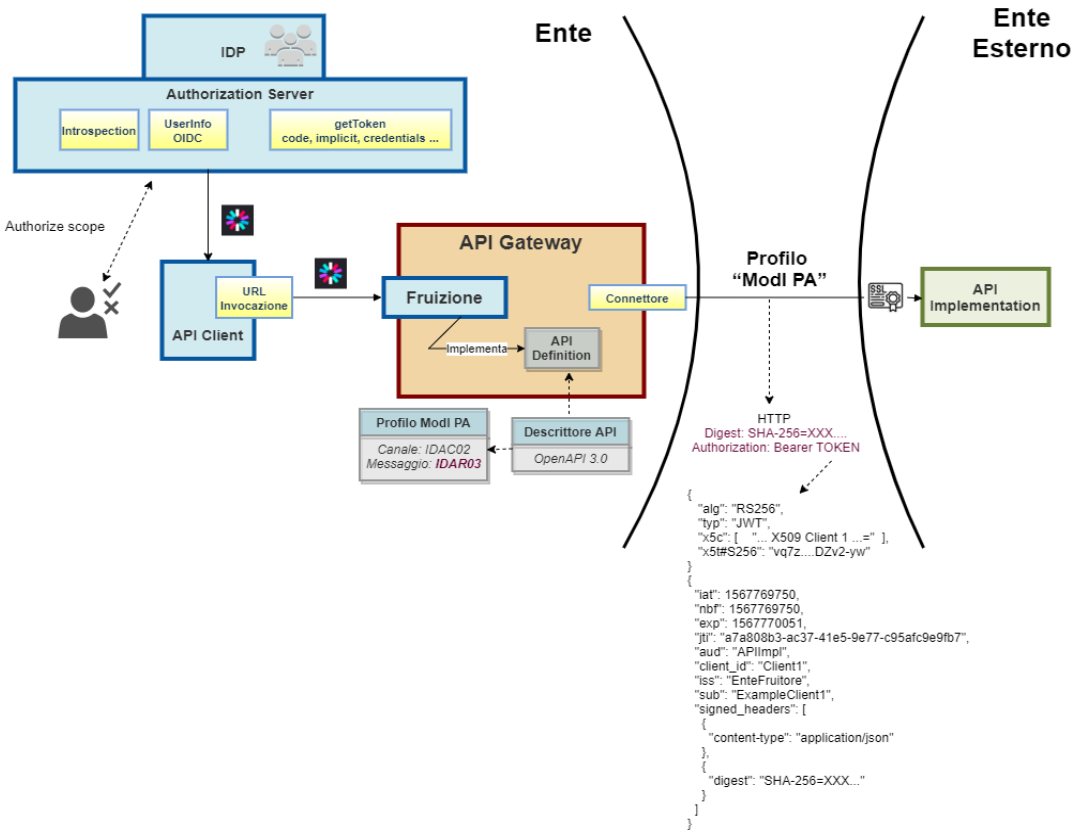
Fruizione del servizio PetStore basata sul profilo di interoperabilità ModI (compatibile alle linee guida di AGID) e protocollo REST.

Le principali caratteristiche di questa interazione sono le seguenti:

1. Il client negozia l'access token con l'Authorization Server coinvolgendo nel processo l'utente che deve autenticarsi e fornire il consenso all'operazione in delega sul client.
2. Il client effettua l'invocazione verso l'API Gateway utilizzando il token ottenuto. Il token ha lo scopo di consentire l'identificazione, da parte del gateway, sia dell'utente che dell'applicativo client, al fine di includere le relative credenziali nel token di sicurezza ModI scambiato nella comunicazione interdominio.
3. L'invio della richiesta al servizio destinatario avviene attraverso il profilo di sicurezza canale IDAC02. Quindi è necessario che i domini coinvolti abbiano attuato il trust dei reciproci certificati SSL al fine di garantire la mutua autenticazione dei sistemi.
4. L'autenticazione degli applicativi, effettivamente mittente e destinatario della comunicazione, è garantita tramite l'applicazione del profilo di sicurezza messaggio IDAR02 con l'integrazione del profilo IDAR03 a garanzia dell'integrità del payload scambiato.
5. Tracciatura a norma degli scambi effettuati, sia riguardo la comunicazione di richiesta che quella di risposta. La conservazione delle tracce, complete delle evidenze di trasmissione, fornisce supporto al non ripudio.

La figura successiva fornisce una rappresentazione d'insieme dell'intero flusso applicativo:

- L'API PetStore, basata su REST, profilo di interazione Bloccante e profili di sicurezza IDAC02, IDAR02 e IDAR03.
- L'Authorization Server per il rilascio dell'access token utilizzato dal client per l'accesso al servizio
- L’API Gateway per la validazione dell'access token, identificazione del client e dell'utente e gestione del profilo ModI per la comunicazione a norma con il dominio esterno.
- Il client, su attivazione dell'utente, che invia la richiesta verso la fruizione esposta dall'API Gateway.



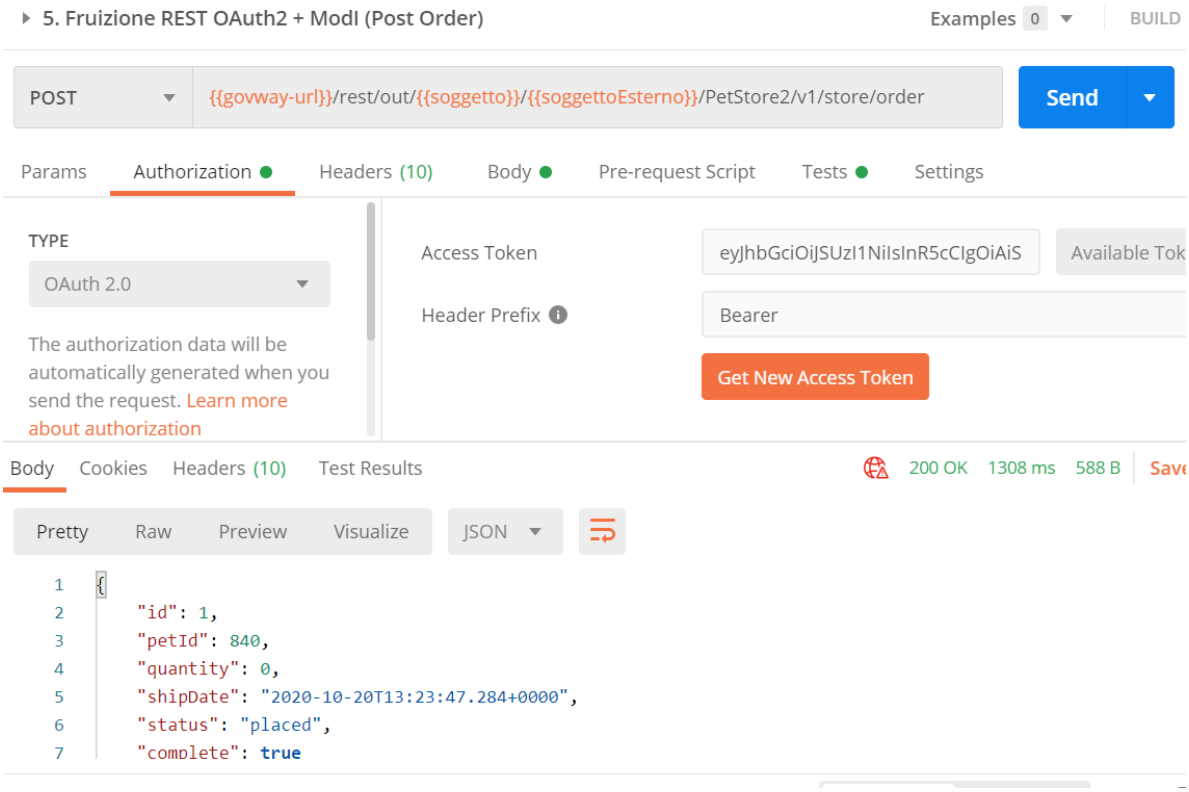
Il flusso applicativo prevede in dettaglio:

1. Il client entra in possesso dell'access token, previa autenticazione e consenso dell'utente richiedente sull'Authorization Server. Il flusso adottato è Authorization Code relativo allo standard OAuht v2.0
2. Il client utilizza tale token per inviare la richiesta di fruizione all'API Gateway.
3. L'API Gateway valida il token ricevuto e verifica i criteri di controllo degli accessi.
4. L'API Gateway identifica il client tramite il claim "azp" presente nel token fornito.
5. L'API Gateway estrae le informazioni utente:
   - Ente mittente corrispondente al client identificato
   - Codice Fiscale dell'utente dal claim "codice_fiscale" presente nel token
   - IP della postazione
6. Il Gateway produce il token ModI tramite la chiave ssl del client identificato.
7. Il Gateway inoltra la richiesta al gateway del dominio erogatore includendo il token ModI prodotto tramite l'header HTTP "Authorization" in accordo alla specifica del Modello di Interoperabilità di AGID.
8. Il servizio erogatore produce la risposta e quindi il flusso di ritorno avviene come già descritto in precedenza per il caso di erogazione.

9. L'API Gateway effettua il tracciamento dei dati inerenti la richiesta e la risposta ottenuta, mantenendo la correlazione ed includendo i token scambiati.

L'esecuzione può essere effettuata tramite l'interazione Erogazione REST ModI presente nella collection Postman:

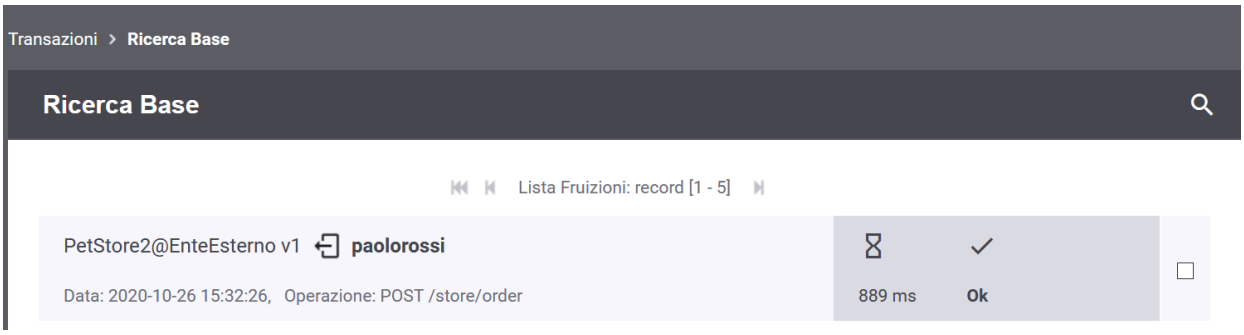
- **Fruizione REST OAuth2 + ModI**
  - Il primo passo è quello di richiedere il token all'authorization server. Dal tab "Authorization", tramite l'autorizzazione "OAuth 2.0", si utilizza il pulsante "Get New Access Token.
  - Il form è precompilato con i dati di accesso all'authorizazion server. Con il pulsante "Request Token" si viene rediretti alla maschera di autenticazione dove si devono inserire le credenziali dell'utente (username: paolorossi, password: 123456).
  - Superata la fase di autenticazione viene mostrato a video il token restituito. Utilizzare il pulsante "Use Token" e quindi procedere all'invio della richiesta tramite il pulsante "Send".



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 di monitoraggio dell'API Gateway:

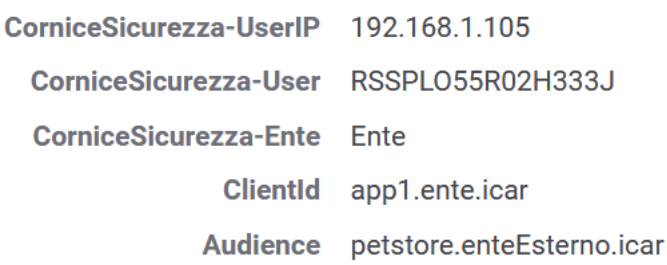
1. Selezionare la voce di menu "Monitoraggio > Transazioni" e scegliere la Ricerca Generica "Base"

2. Selezionare la Modalità di Ricerca di tipo "Fruizione"
3. La transazione appena effettuata è visualizzata nell'elenco con i principali dati (servizio invocato, soggetto mittente, timestamp, ecc).



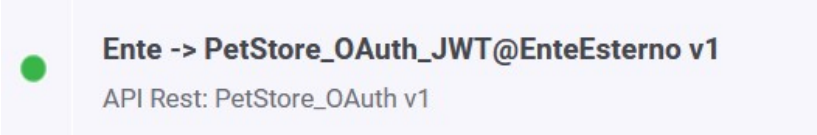
4. Accedendo al dettaglio della transazione, nella sottosezione "Diagnostici", è possibile verificare la fase di autenticazione del client e la validazione del token ricevuto da parte dell'API Gateway.

5. Nella sezione del dettaglio "Dettagli Messaggio > Dettagli Richiesta" si può visualizzare la traccia dove si possono visualizzare le informazioni estratte dal token OAuth2 che sono state inserite nel token ModI



6. Le ulteriori verifiche non differiscono da quanto già descritto in precedenza nel caso dell'erogazione REST.

3.5 Fruizione OAuth2 con Asserzione JWT firmata con X.509



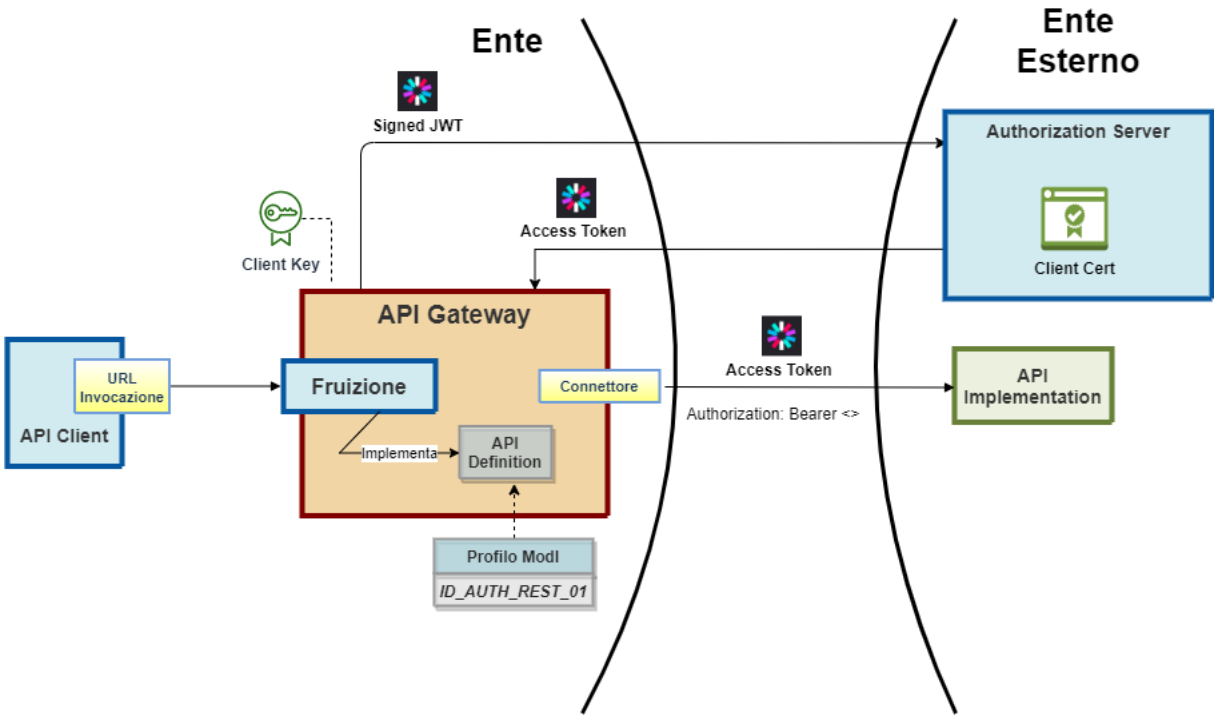
Fruizione del servizio PetStore basata sul protocollo REST con accesso al servizio erogato basato su autenticazione del client tramite accesso token OAuth2.

Le principali caratteristiche di questa interazione sono le seguenti:

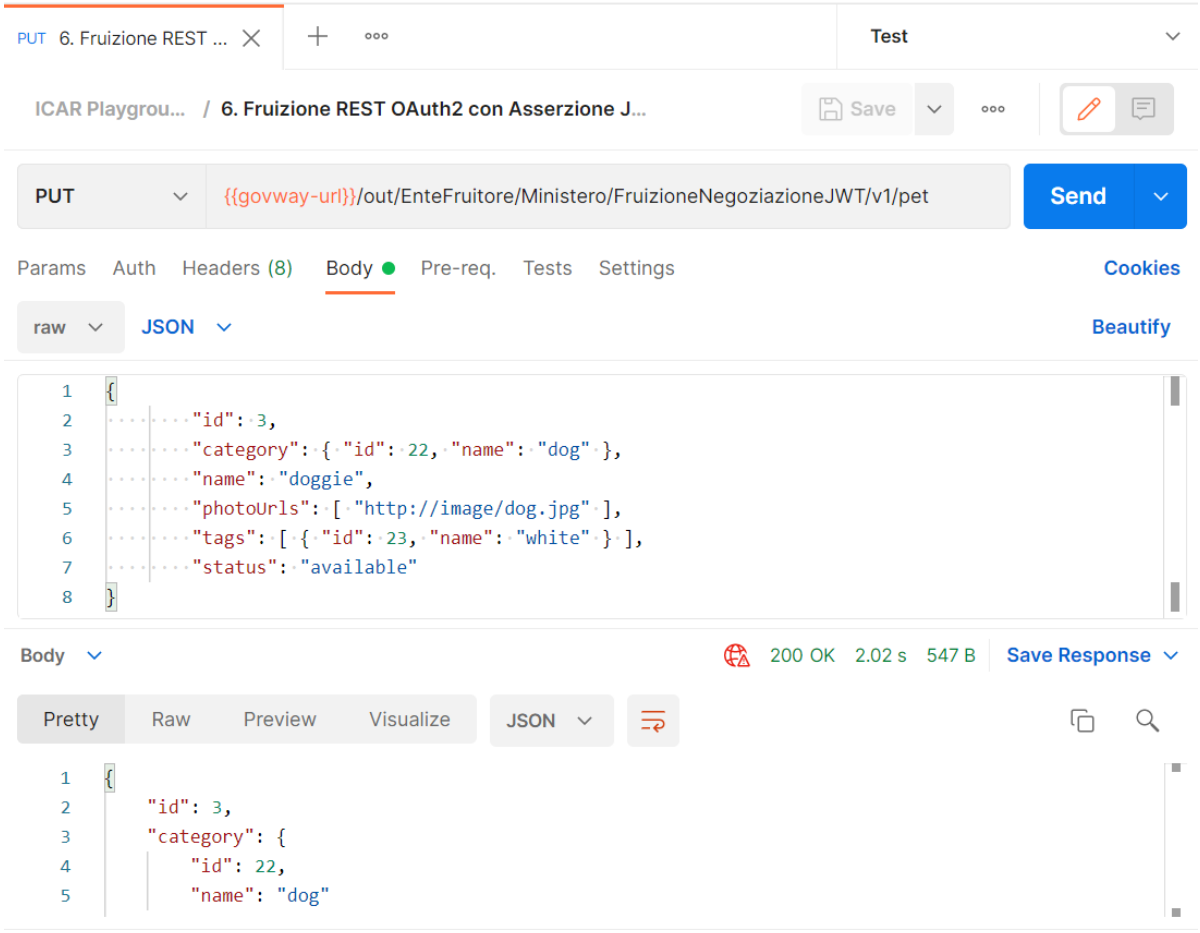
1. Il client effettua l'invocazione del servizio inviando la richiesta alla URL di invocazione messa a disposizione dall'API Gateway.
2. L'API Gateway utilizza la chiave privata del client per produrre un'asserzione JWT firmata in accordo allo standard RFC 7523 (https://datatracker.ietf.org/doc/html/rfc7523#section-2.2).
3. L'API Gateway invia all'authorization server dell'erogatore la richiesta del token utilizzando l'asserzione JWT come credenziale.
4. L'autorization server valida l'asserzione JWT grazie al certificato del client in proprio possesso e restituisce all'API Gateway l'access token completo dei claim di autenticazione.
5. L'API Gateway invoca il servizio erogato fornendo l'access token sull'header Authorization della richiesta HTTP.
6. Il servizio erogatore valida il token ricevuto e identifica il client grazie ai relativi claim contenuti.
7. Il servizio erogatore applica i criteri di autorizzazione, basati sull'identità del client, e rilascia gli eventuali scope richiesti. Procede quindi con l'elaborazione della richiesta ed invio della risposta.

La figura successiva fornisce una rappresentazione d'insieme dell'intero flusso applicativo:

- L'API PetStore, basata su REST con profilo di sicurezza ID_AUTH_REST_01.
- L'API Gateway per la negoziazione dell'access token, previa richiesta con invio di JWT firmato con la chiave del client e successiva gestione della richiesta al servizio tramite l'access token ottenuto.
- L'Authorization Server lato erogatore, in grado di validare le asserzioni JWT firmate con il certificato del client e quindi rilasciare l'access token utilizzato per l'accesso al servizio.
- Il client che invia la richiesta verso la fruizione esposta dall'API Gateway.



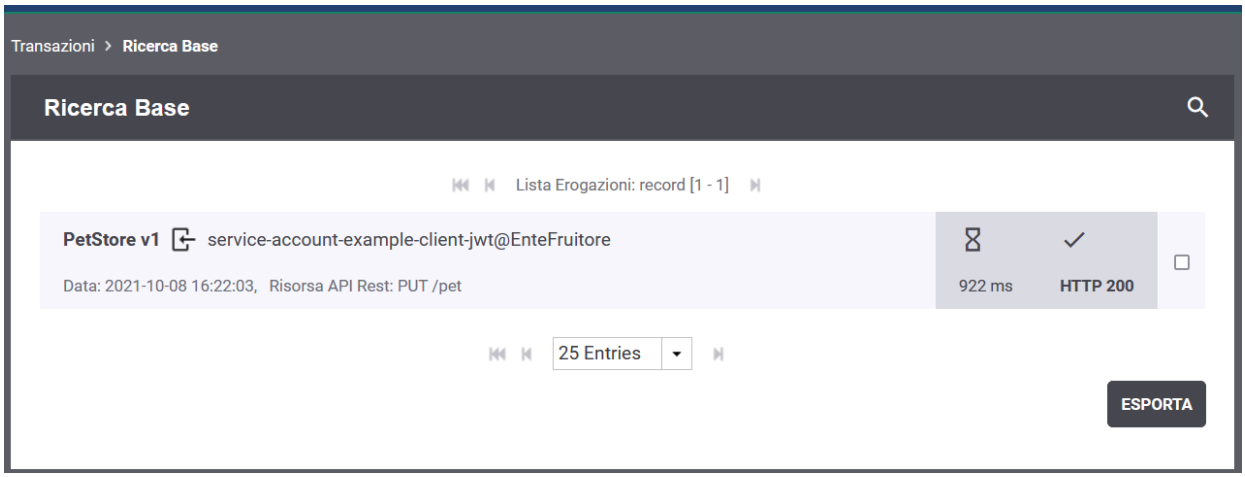
L’esecuzione può essere effettuata tramite l'interazione “Fruizione REST OAuth2 con Asserzione JWT” presente nella collection Postman:



- **Fruizione REST OAuth2 con Asserzione JWT**
  - L'operazione predisposta è una PUT. L'API Gateway si occupa di negoziare il token e richiedere gli scope "example-create" ed "example-delete", indispensabili per le operazioni di creazione/modifica e cancellazione.
  - Per avviare l'esecuzione è sufficiente premere il pulsante "Send" e verificare l'esito dell'operazione nel riquadro basso.
  - L'esito atteso è il codice http 200 sulla risposta ed il messaggio con la rappresentazione dell'entità modificata in seguito all'esecuzione.

Una volta completata l'esecuzione e verificato l'esito è possibile andare a verificare cosa è accaduto, nel corso dell'elaborazione della richiesta, andando a consultare la console di monitoraggio dell'API Gateway:

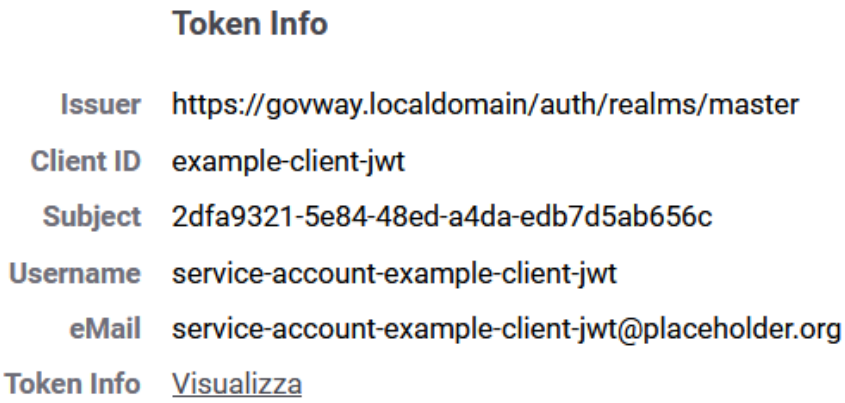
1. Selezionare la voce di menu "Monitoraggio > Transazioni" e scegliere la Ricerca Generica "Base"
2. Selezionare la Modalità di Ricerca di tipo "Erogazione"
3. La transazione appena effettuata è visualizzata nell'elenco con i principali dati (servizio invocato, soggetto mittente, timestamp, ecc).



4. Accedendo al dettaglio della transazione, nella sottosezione "Diagnostici", è possibile verificare la fase di validazione del token ricevuto da parte dell'API Gateway mittente e la fase di autenticazione del client con estrazione dell'identificativo e applicazione delle politiche di autorizzazione.

2021-10-08 16:22:03.878	infoIntegration	RicezioneBuste	Gestione Token [KeyCloack] (Validazione JWT) in corso ...
2021-10-08 16:22:03.929	infoIntegration	RicezioneBuste	Gestione Token [KeyCloack] (Validazione JWT) completata con successo
2021-10-08 16:22:03.931	infoIntegration	RicezioneBuste	Autenticazione [principal] in corso ...
2021-10-08 16:22:03.945	infoIntegration	RicezioneBuste	Autenticazione [principal] effettuata con successo
2021-10-08 16:22:04.126	infoProtocol	RicezioneBuste	Ricevuto messaggio di cooperazione con identificativo [1bf4cb0d-2843-11ec-9e12-0242ac160003] inviato dalla parte mittente [gw/EnteFruitore]
2021-10-08 16:22:04.129	infoIntegration	RicezioneBuste	Verifica autorizzazione [authenticated] messaggio con identificativo [1bf4cb0d-2843-11ec-9e12-0242ac160003] fruitore [gw/EnteFruitore] -> servizio [gw/Ministero:gw /PetStore:1:PUT_pet] identitaServizioApplicativoFruitore [example-client-jwt] in corso ...
2021-10-08 16:22:04.142	infoIntegration	RicezioneBuste	Verifica autorizzazione [authenticated] messaggio con identificativo [1bf4cb0d-2843-11ec-9e12-0242ac160003] fruitore [gw/EnteFruitore] -> servizio [gw/Ministero:gw /PetStore:1:PUT_pet] identitaServizioApplicativoFruitore [example-client-jwt] completata con successo

5. Nella sezione "Informazioni Mittente > Token Info" si possono visualizzare le informazioni estratte dal token ed in particolare il dettaglio dell'identificativo client:



con la possibilità di visualizzare il dettaglio compelto dei valori presenti nel token ricevuto

3.6 Fruizione REST con accesso tramite PDND

Fruizione del servizio PetStore basata sul protocollo REST con accesso al servizio erogato basato su autenticazione del client tramite access token PDND.

Allo stato attuale la PDND non è ancora stata resa disponibile per l'utilizzo e di conseguenza non sono ancora noti i riferimenti per l'accesso.

Allo scopo di rendere le configurazioni pronte all'uso, al momento del rilascio della PDND, sono state predisposte le seguenti entità di configurazioni in bozza:

1. Una Token Policy "PDND" di tipo "Signed JWT" per la gestione della negoziazione del token sulla PDND. I riferimenti inseriti, quali ad esempio la URL "Token Endpoint" (o il Purpose ID) sono puramente inventati e dovranno essere sostituiti con quelli veri, una volta comunicati dalla PDND.

   I campi interessati per la personalizzazione sono i seguenti:

Elemento Configurazione	Descrizione
Token Endpoint > PDND	flag "attivo"
Token Endpoint > URL	Url di negoziazione token sulla PDND
Token Endpoint > JWT Keystore	Riferimenti alla chiave privata da utilizzare per firmare l'asserzione JWT richiesta dalla PDND
Token Endpoint > JWT Header > KID	Opzione "Personalizzato" specificando nel campo testuale sottostante il valore del KID fornito dalla PDND dopo la sottoscrizione del client
Token Endpoint > JWT Payload > Client ID	Client-id assegnato dalla PDND dopo la sottoscrizione del client
Token Endpoint > JWT Payload > Audience	Valore "Audience" comunicato dalla PDND per l'operazione di negoziazione
Token Endpoint > JWT Payload > Issuer	Client-id assegnato dalla PDND dopo la sottoscrizione del client
Token Endpoint > JWT Payload > Subject	Client-id assegnato dalla PDND dopo la sottoscrizione del client
Token Endpoint > JWT Payload > Purpose ID	Identificativo del Purpose ottenuto con la sottoscrizione dell'accordo di interoperabilità. Possono essere fornite varie soluzioni per l'estrazione di tale valore. Può essere indicato dal client oppure dallo stesso gateway.

2. Una Token Policy "PDND_validazione" di tipo "JWS" per la gestione della validazione dei token in ingresso rilasciati dalla PDND. Anche in questo caso, il certificato usato per la validazione è di puro esempio e dovrà essere sostituito con quello fornito dalla PDND.

   I campi interessati per la personalizzazione sono i seguenti:

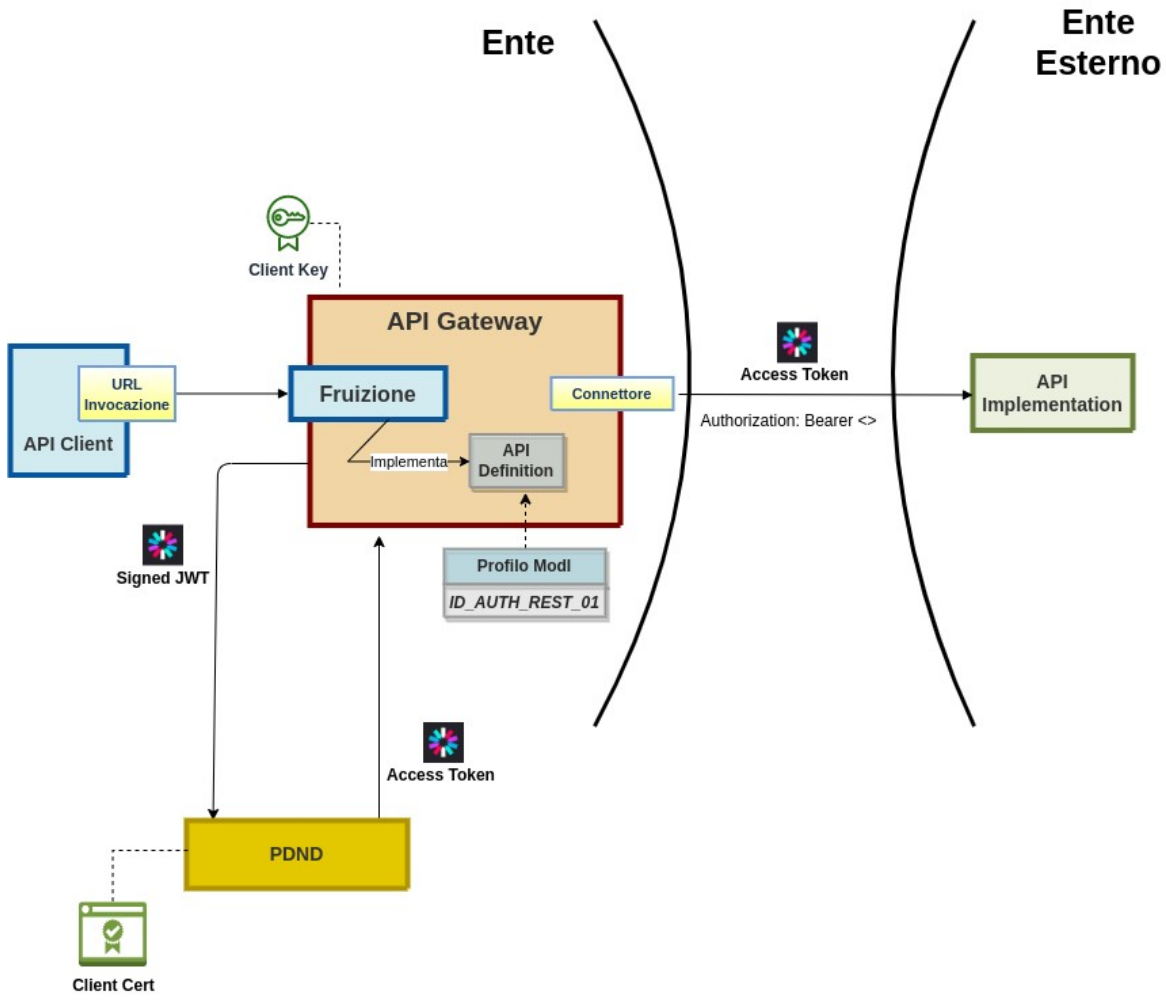
Elemento Configurazione	Descrizione
Validazione JWT	File ed alias certificato della PDND

3. Una Erogazione “PetStore_PDND@EnteEsterno v1”, che implementa l’API “PetStore_OAuth v1”, da utilizzarsi per simulare il servizio erogato dall’ente esterno. Tale erogazione è configurata in modo da applicare la token policy “PDND_validazione”.

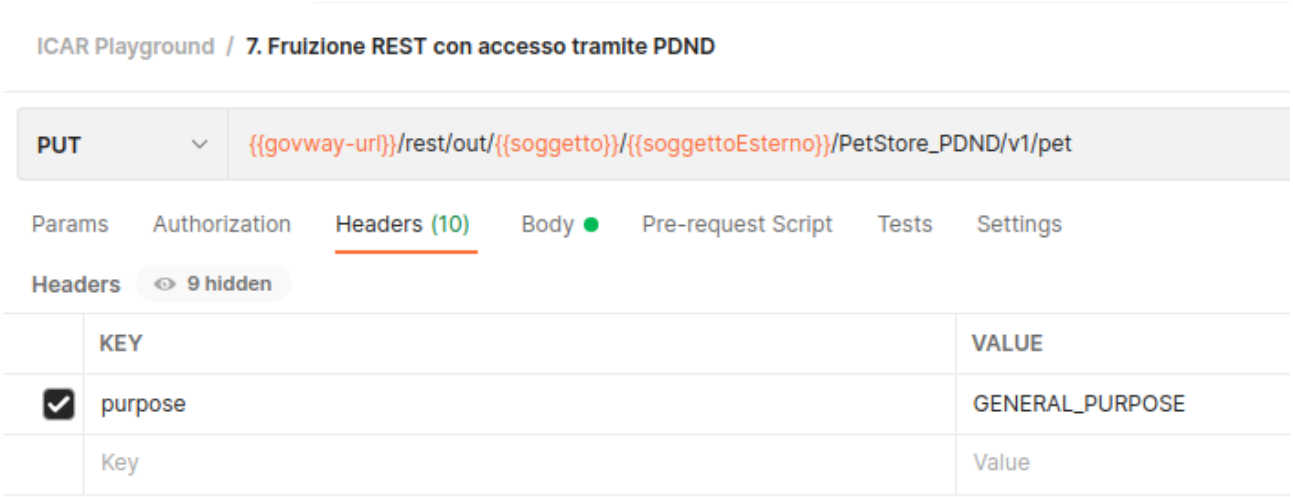
   I campi interessati per la personalizzazione sono i seguenti:

Elemento Configurazione	Descrizione
Controllo Accessi > Autenticazione Token > Policy	Indicare la policy per la validazione dei Token PDND
Controllo Accessi > Autenticazione Token > Required Claims	I claims Issuer, ClientId e Subject sono presenti nel token rilasciato dalla PDND
Controllo Accessi > Autorizzazione Canale > Autorizzazione per Token Claims	Possibile validare i valori dei claims presenti nel Token PDND: • *sub* → con il valore clientId assegnato dalla PDND • *client_id* → con il valore clientId assegnato dalla PDND • *aud* → con il valore audience previsto dall’accordo di interoperabilità

4. Una Fruizione “Ente -> PetStore_PDND@EnteEsterno v1”, che implementa l’API “PetStore_OAuth v1”, al fine di gestire l’esigenza per cui nasce lo use case. La fruizione è configurata in modo da applicare la token policy “PDND” per la fase di negoziazione del token. La policy è stata configurata in modo da utilizzare il valore “Purpose ID”. Se si sceglie di far censire questo valore al gateway è necessario registrare nel contesto della fruizione una proprietà avente tale valore.



L’esecuzione può essere effettuata tramite l'interazione “Fruizione REST con accesso tramite PDND” presente nella collection Postman:



Come si può notare in questo caso, il Purpose ID viene fornito dal client tramite un apposito header HTTP.

4 Configurazione dell'ambiente

Per gestire i flussi dei casi di esempio sono stati registrati i due soggetti "Ente" ed "EnteEsterno". I componenti dell'ambiente complessivo che costituisce il Playground sono stati configurati in modo da rendere possibile l'esecuzione automatizzata delle interazioni descritte in questo documento.

Si possono consultare le configurazioni esistenti e procedere ad eventuali estensioni accedendo le relative console di configurazione:

- **Authorization Server Administration Console (KeyCloak)**

  URL: https://gw.icar/auth

  username: admin

  password: admin

- **API Gateway Configuration Console (Govway Console)**

  URL: https://gw.icar/govwayConsole

  username: amministratore

  password: 123456

- **API Gateway Monitor Console (Govway Monitor)**

  URL: https://gw.icar/govwayMonitor

  username: operatore

password: 123456