Specifiche Web Services

Gestione Concessionari

SH

Storia del Documento

Il seguente registro cronologico delle modifiche contiene una registrazione delle modifiche apportate al presente documento:

|  |  |  |
| --- | --- | --- |
| **Versione** | **Data** | **Note** |
| 1.01 | 02/04/2025 | Prima emissione |
| 1.02 | 02/09/2025 | Aggiornamento JSON e HTML per modifica stato PRESERVATO rinominato CEDUTO |

Indice del Documento

[1 Introduzione 4](#_Toc198040147)

[1.1 Scopo e campo di applicazione 4](#_Toc198040148)

[1.2 Applicabilità 4](#_Toc198040149)

[1.3 Standard 4](#_Toc198040150)

[2 URL DEI SERVIZI 5](#_Toc198040151)

[2.1 AMBIENTE DI ESERCIZIO 5](#_Toc198040152)

[2.2 AMBIENTE DI FORMAZIONE 5](#_Toc198040153)

[3 DIAGRAMMA DI PROCESSO 6](#_Toc198040154)

[3.1 DESCRIZIONE 6](#_Toc198040155)

[3.2 ELENCO STATI RICHIESTA 9](#_Toc198040156)

[3.3 Diagramma dei Casi D’Uso 10](#_Toc198040157)

[4 DEFINIZIONE DEI SERVIZI 13](#_Toc198040158)

[4.1 HTML 13](#_Toc198040159)

[4.2 JSON 13](#_Toc198040160)

[4.3 ESEMPI DI CHIAMATE AI SERVIZI 14](#_Toc198040161)

[4.4 TIPOLOGICHE 14](#_Toc198040162)

[4.4.1 STATI VFU 14](#_Toc198040163)

[4.4.2 STATI FASCICOLO 14](#_Toc198040164)

[4.4.3 TIPO DOCUMENTO 15](#_Toc198040165)

[4.4.4 TIPO VEICOLO 15](#_Toc198040166)

[5 MODALITÀ DI AUTENTICAZIONE DI UN UTENTE PER L’UTILIZZO DEI WEB SERVICE 16](#_Toc198040167)

[5.1 Specifiche OpenID Provider 17](#_Toc198040168)

[5.1.1 URL SERVIZI DI AUTENTICAZIONE 17](#_Toc198040169)

[5.1.1.1 AMBIENTE DI ESERCIZIO 17](#_Toc198040170)

[5.1.1.2 AMBIENTE DI FORMAZIONE 17](#_Toc198040171)

[5.1.2 OIDC TOKENS 17](#_Toc198040172)

[5.2 Informazioni DI INTEGRAZIONE 19](#_Toc198040173)

[5.3 Flusso di Autenticazione 20](#_Toc198040174)

[5.3.1 AUTHENTICATE 21](#_Toc198040175)

[5.3.2 AUTHORIZE 22](#_Toc198040176)

[5.3.3 ACCESS TOKEN 23](#_Toc198040177)

[5.4 AGGIORNAMENTO Token 24](#_Toc198040178)

[5.5 Logout 25](#_Toc198040179)

[6 APPENDICE B: Termini ed acronimi 26](#_Toc198040180)

# Introduzione

## Scopo e campo di applicazione

Il presente documento intende fornire la specifica dei servizi esposti dal MIMS verso le Software House, realizzati con la tecnologia dei RESTful Web Services, per il Nuovo Sistema Gestione Pagamenti.

## Applicabilità

I servizi web descritti nel presente documento sono rivolti al solo profilo ‘Concessionario’

## Standard

N.a.

# URL DEI SERVIZI

## AMBIENTE DI ESERCIZIO

L’indirizzo in ambiente di esercizio dei servizi è il seguente:

*{{baseUrl}}=* [*https://www.ilportaledeltrasporto.it/*](https://www.ilportaledeltrasporto.it/)

## AMBIENTE DI FORMAZIONE

L’indirizzo in ambiente di formazione dei servizi è il seguente:

*{{baseUrl}}=* [*https://formazione.ilportaledeltrasporto.it/*](https://formazione.ilportaledeltrasporto.it/)

# DIAGRAMMA DI PROCESSO

## DESCRIZIONE

Il progetto ha come obiettivo quello di istituire e gestire il Registro Digitale dei Veicoli Fuori Uso.

In questo contesto si rende necessario

* garantire un “unico punto di accesso” alle funzionalità per i soggetti abilitati alla gestione del registro
* definire un processo di business che gestisca l’iter procedurale dal ritiro del veicolo fino alla radiazione e rottamazione
* consentire la consultazione della situazione di uno specifico veicolo avviato alla demolizione, da parte degli interlocutori interessati, ivi comprese le forze di pubblica sicurezza deputate ai controlli.

Gli attori coinvolti nel progetto sono:

* concessionari, case costruttrici e automercati, che possono ritirare un veicolo da avviare alla rottamazione, per conto di un centro di raccolta, rilasciando il certificato di rottamazione digitale
* centri di raccolta, che devono
* prendere in carico i veicoli da rottamare,
* svolgere gli accertamenti sulla documentazione
* richiedere la radiazione del veicolo
* procedere con la rottamazione
* studi di consulenza/agenzie, ai quali si possono rivolgere i centri di raccolta per essere supportati nella fase di radiazione del veicolo, in particolare per quelli con obbligo di iscrizione al PRA
* gli uffici PRA/UMC che sovrintendono alle operazioni di radiazione ai quali deve essere consentita la consultazione del registro
* le forze dell’ordine, che devono poter consultare il registro ai fini di accertamento

Si seguito si riportano le macro-aree di cui si compone il progetto:

1. Censimento soggetti abilitati alla gestione del registro: concessionari, case costruttrici, automercati e centri di raccolta potranno accedere alle funzionalità di gestione del Registro mediante accesso al Portale del Trasporto (PdT) messo a disposizione dal MIT, e pertanto dovranno essere dotati di credenziali di accesso. si rende quindi necessario

* effettuare un primo censimento massivo dei soggetti abilitati attualmente attivi, ai quali saranno attribuite credenziali di accesso da notificare tramite e-mail, secondo il processo già in essere per gli utenti del PdT.
* permettere la gestione tanto di nuovi soggetti che si aggiungono a quelli già autorizzati ad operare, quanto di quelli che cessano a vario titolo l’attività, ai quali deve essere consentito di portare a termine le attività già avviate, oltre a consentire la consultazione nel periodo stabilità dalla norma per la conservazione della documentazione

Considerata la numerosità dei soggetti e le possibili variazioni, è messa a disposizione una funzionalità di verifica dello stato di accreditamento dei soggetti, a disposizione degli uffici territoriali UMC e PRA.

1. Gestione della delega che ciascun Centro di Raccolta può concedere ad uno o più concessionari, che potranno ritirare i veicoli da rottamare per proprio conto.  Il Centro di Raccolta dovrà

* indicare i soggetti che intende delegare specificando il periodo di durata di detta delega,
* potrà modificare il periodo precedentemente indicato, e infine
* potrà revocare la nel momento in cui cessi il rapporto privato stabilito.
* in qualsiasi momento potrà verificare tramite funzioni di consultazione lo stato dei suoi rapporti di delega attivi.

1. Ritiro, da parte dei concessionari, dei veicoli consegnati da intestatari/delegati, con

* verifica di radiabilità del veicolo
* conferimento del veicolo ad un Centro di Raccolta
* rilascio del Certificato di Rottamazione Digitale, generato dal sistema, e nel solo caso dei veicoli fuori uso senza obbligo di iscrizione al PRA, rilascio della ricevuta di presa in carico della documentazione, per la successiva consegna all’UMC per la radiazione.
* Ai concessionari è consentita la consultazione dei veicoli ritirati

1. Ritiro, da parte dei centri di raccolta, dei veicoli consegnati da intestatari/delegati, con

* verifica di radiabilità del veicolo
* rilascio del Certificato di Rottamazione Digitale, generato dal sistema,
* rilascio, nel solo caso dei veicoli fuori uso senza obbligo di iscrizione al PRA, della ricevuta di presa in carico della documentazione, per la successiva consegna all’UMC per la radiazione.

Ai demolitori è consentito di emettere un certificato di rottamazione cartaceo, per sopperire a situazioni particolari in cui non è possibile procedere con l’iter ordinario. Il veicolo deve comunque essere inserito nel registro entro i termini stabiliti (entro le 24 ore successive) e il certificato cartaceo deve essere caricato nel sistema e firmato con la firma digitale remota.

Ai demolitori è inoltre consentito di “forzare” la presa in carico di un veicolo che presenti vincoli di ostatività, nel caso ritenga di poterle risolvere per poi procedere con la rottamazione.

1. Presa in carico o trasferimento di veicoli conferiti, cioè ritirati per proprio conto da un concessionario, mediante

* conferma di presa in carico del veicolo conferito
* trasferimento di un veicolo conferito ad altro centro di raccolta, nel caso di indisponibilità a demolirlo.

1. Rottamazione di un veicolo fuori uso da parte di un centro di raccolta, che deve

* verificare la mancanza di vincoli ostativi alla rottamazione
* acquisire la documentazione richiesta in base al regime del veicolo
* predisporre la radiazione del veicolo.

Nel caso dei veicoli con obbligo di iscrizione al PRA la radiazione avviene mediate l’utilizzo delle funzionalità del Documento Unico. Tale operazione può essere effettuata direttamente dal demolitore se questi decide di procedere in autonomia o, nel caso in cui scelga di avvalersi di uno studio di consulenza (agenzia), da uno STA. In quest’ultimo caso, il demolitore può predisporre una lista di veicoli da associare ad uno studio di consulenza che si occuperà di effettuare la radiazione per suo conto.

Nel caso di veicoli senza obbligo di iscrizione al PRA le operazioni di radiazione sono a carico degli UMC, che operano mediante le procedure del sistema MCTC, a fronte della presentazione, da parte del detentore del veicolo, della ricevuta di presa in carico della documentazione, rilasciata dal demolitore. L’adeguamento delle funzioni citate esula dallo scopo del progetto.

1. Radiazione del veicolo fuori uso, nel caso di veicolo con obbligo di iscrizione al PRA. L’operazione può essere svolta direttamente dal centro di raccolta o per il tramite di uno studio di consulenza, mediante la funzione di Radiazione per demolizione disponibile nell’area Documento Unico, che sarà modificata per consentire

* la verifica della presenza di un certificato di rottamazione
* la visualizzazione e l’acquisizione dei documenti già inseriti nel fascicolo associato al registro dei veicoli fuori uso
* l’aggiornamento del registro a fronte della convalida della pratica di radiazione e l’inserimento della ricevuta di radiazione nel fascicolo del registro

L’adeguamento delle funzioni citate esula dallo scopo del progetto.

1. Registrazione della demolizione, che è conseguente alla conferma di cancellazione del veicolo dagli archivi PRA e MCTC dei veicoli circolanti. I demolitori hanno inoltre l’obbligo della conservazione della documentazione per il periodo stabilito dalla normativa (10 anni), e solo dopo tale periodo possono procedere con la relativa distruzione.
2. Consultazione del Registro Veicolo Fuori Uso, da parte degli uffici territoriali del PRA, limitatamente alla sezione del registro riferita ai veicoli CON obbligo di iscrizione al PRA, che potranno consultare i dati del registro procedendo con

* Ricerca del veicolo in Registro Veicoli Fuori Uso
* Visualizzazione dei dati di dettaglio del veicolo e stato di lavorazione dello stesso
* Visualizzazione del Fascicolo associato al registro
* Lista dei documenti inclusi nel Fascicolo del registro, con la possibilità di visionarli

1. Consultazione del Registro Veicolo Fuori Uso da parte di utenti preposti all’assistenza, come Help Desk e Poli, abilitando la verifica dello stato di lavorazione del procedimento di rottamazione.

Rientrano nel perimetro del progetto i web service di accesso al registro, mentre ciascuna amministrazione provvederà ad integrarli nelle proprie applicazioni di gestione dell’assistenza.

1. Consultazione del Registro Veicolo Fuori Uso, da parte degli uffici territoriali della MCTC (UMC), che devono poter

* Ricercare il veicolo in Registro Veicoli Fuori Uso
* Visualizzare i dati di dettaglio
* Visualizzare il Fascicolo associato al registro
* Visualizzare i documenti inclusi nel Fascicolo del registro

Gli uffici UMC potranno scegliere tra le 2 sezioni del registro (Veicoli CON e SENZA obbligo di iscrizione al PRA). La funzione sarà realizzata all’interno dei sistemi MCTC e utilizzerà i servizi messi a disposizione per la consultazione del registro ed esula dallo scopo del progetto.

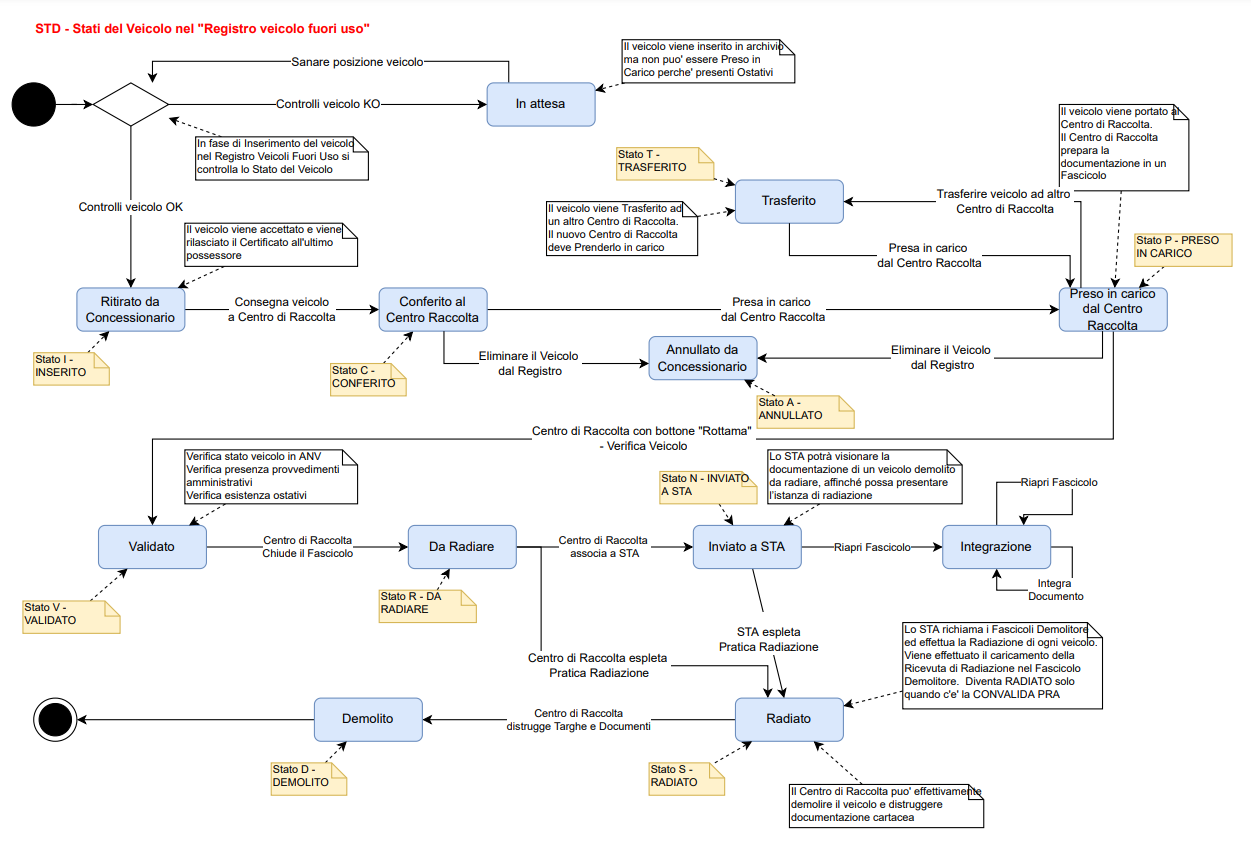
1. Consultazione del Registro Veicolo Fuori Uso, da parte delle Forze di Polizia, che devono poter

* ricercare uno specifico veicolo per verificare i requisiti per la circolazione
* ricercare un centro di raccolta, per valutare la lista dei veicoli fuori uso trattati

La funzione sarà realizzata all’interno dei sistemi MCTC nell’area InfoWEB e utilizzerà i servizi messi a disposizione per la consultazione del registro ed esula dallo scopo del progetto.

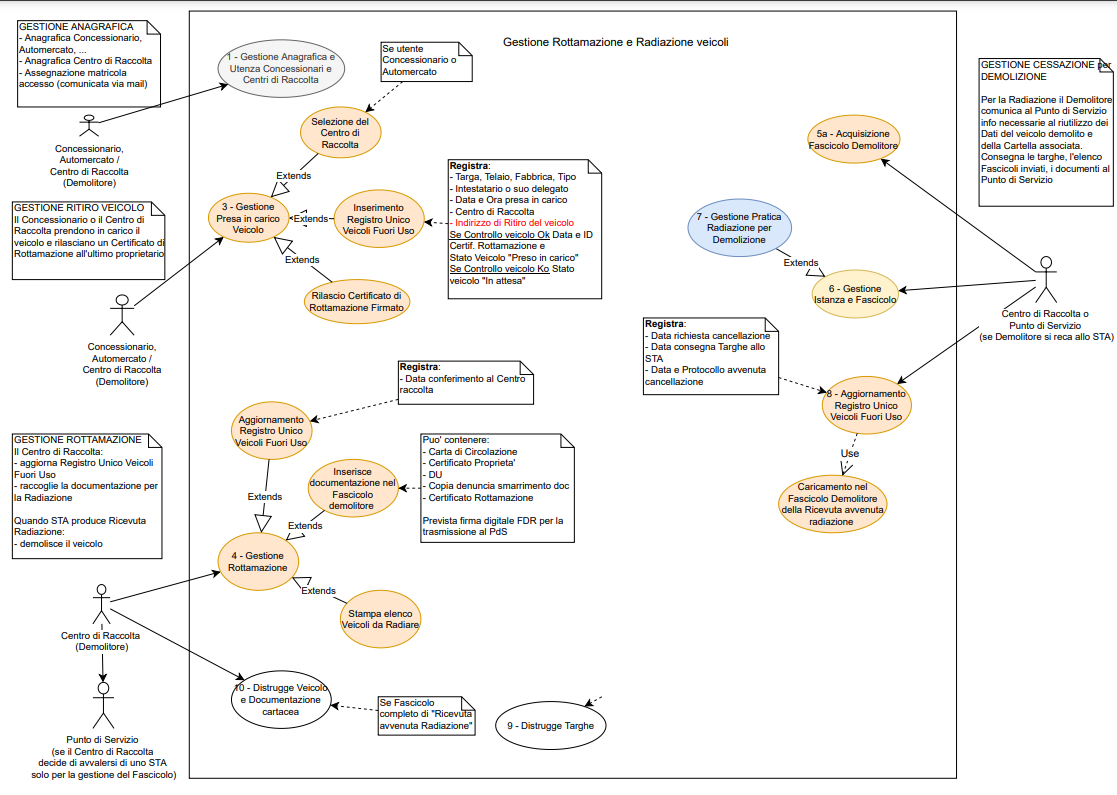
## ELENCO STATI RICHIESTA

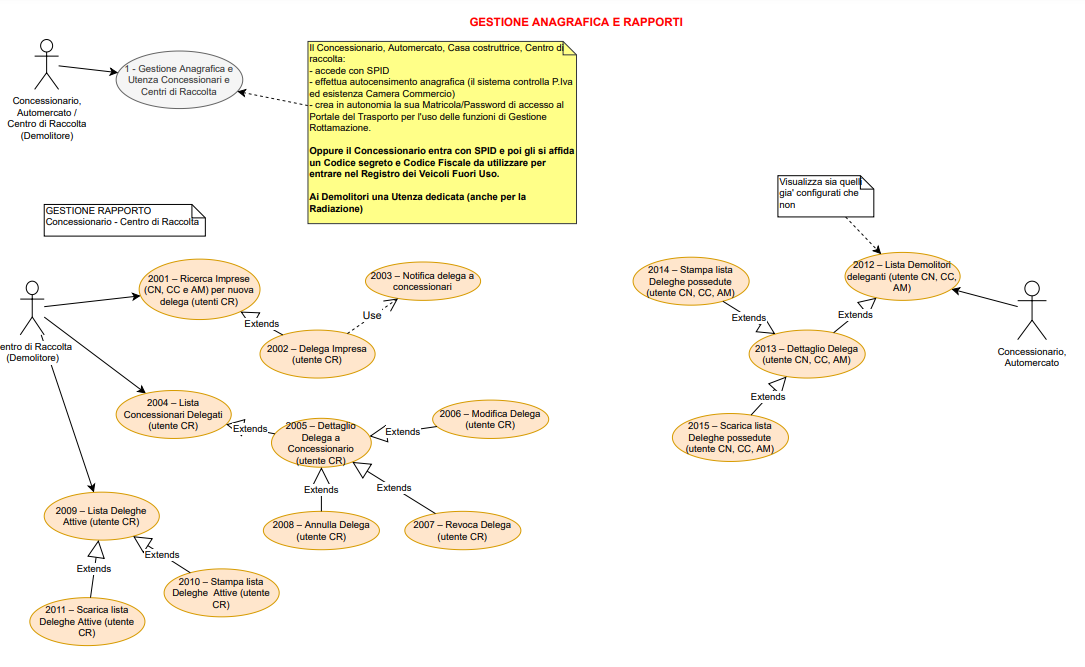
Di seguito il diagramma degli stati che può assumere un veicolo nel Registro veicoli fuori uso:

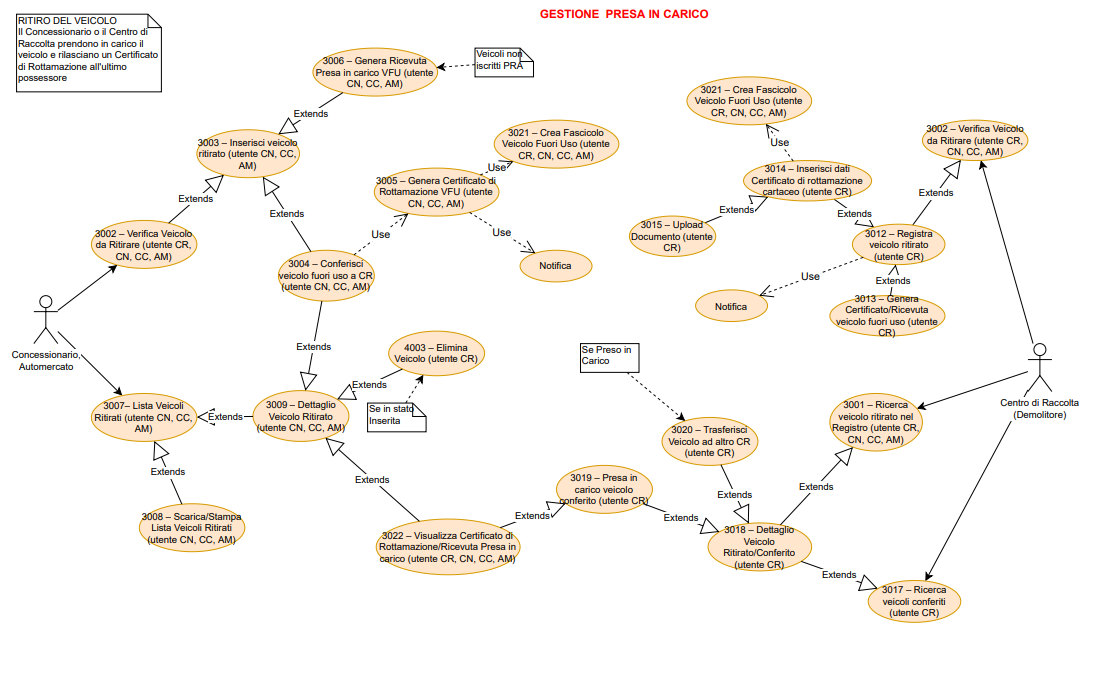


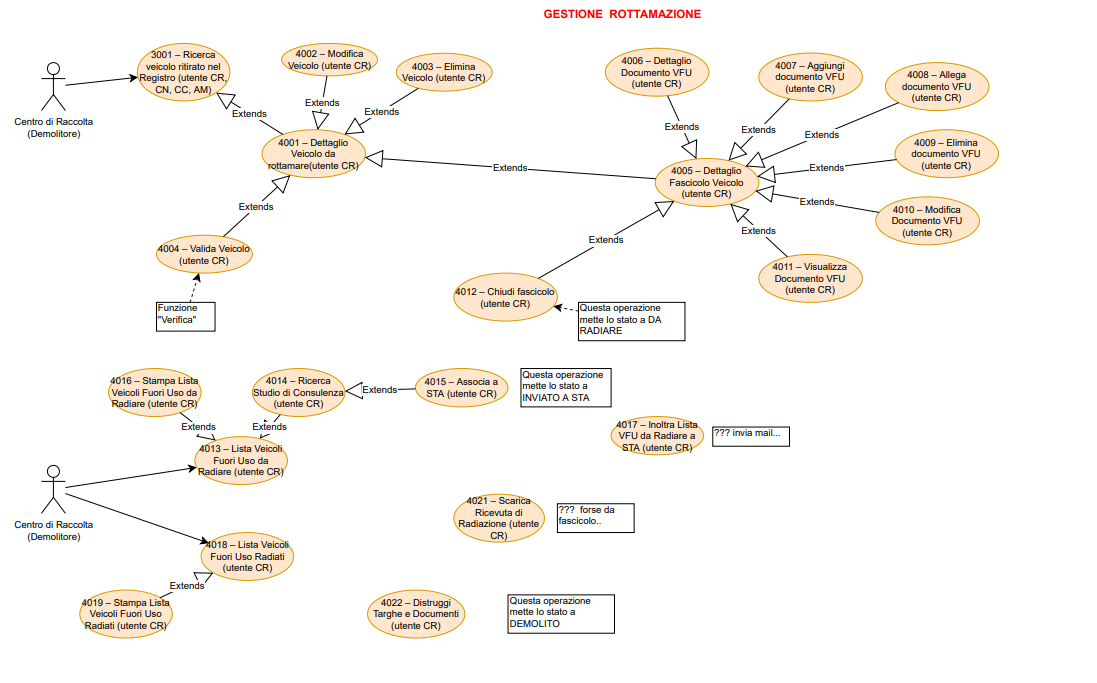
## Diagramma dei Casi D’Uso

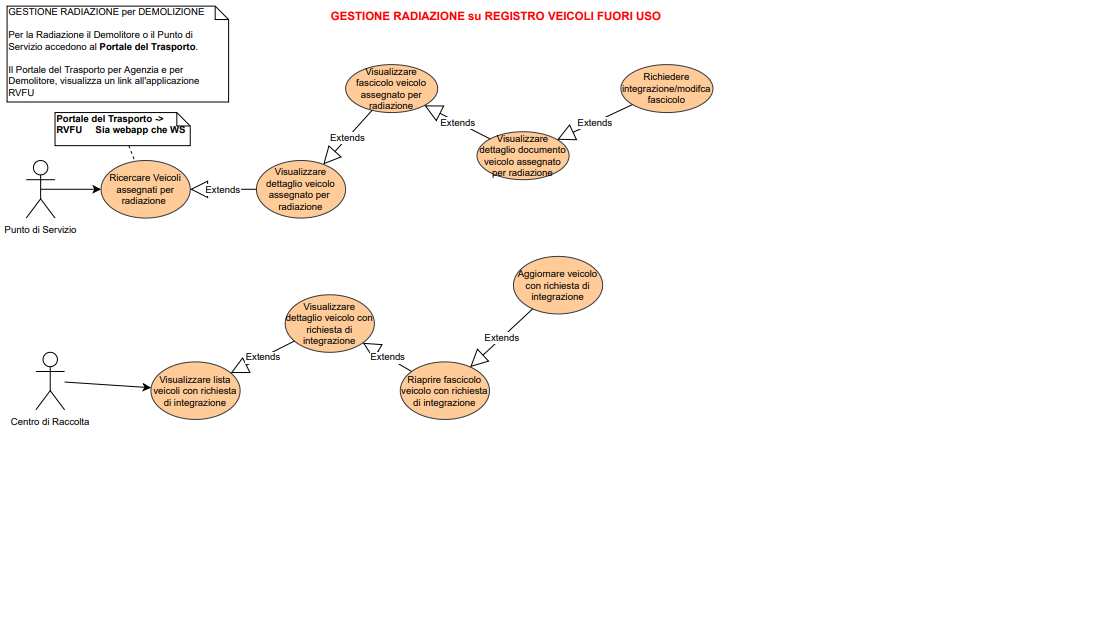
Il diagramma che segue descrive l’interazione uomo-macchina che può aiutare nella comprensione dei servizi disponibili e di come operano.

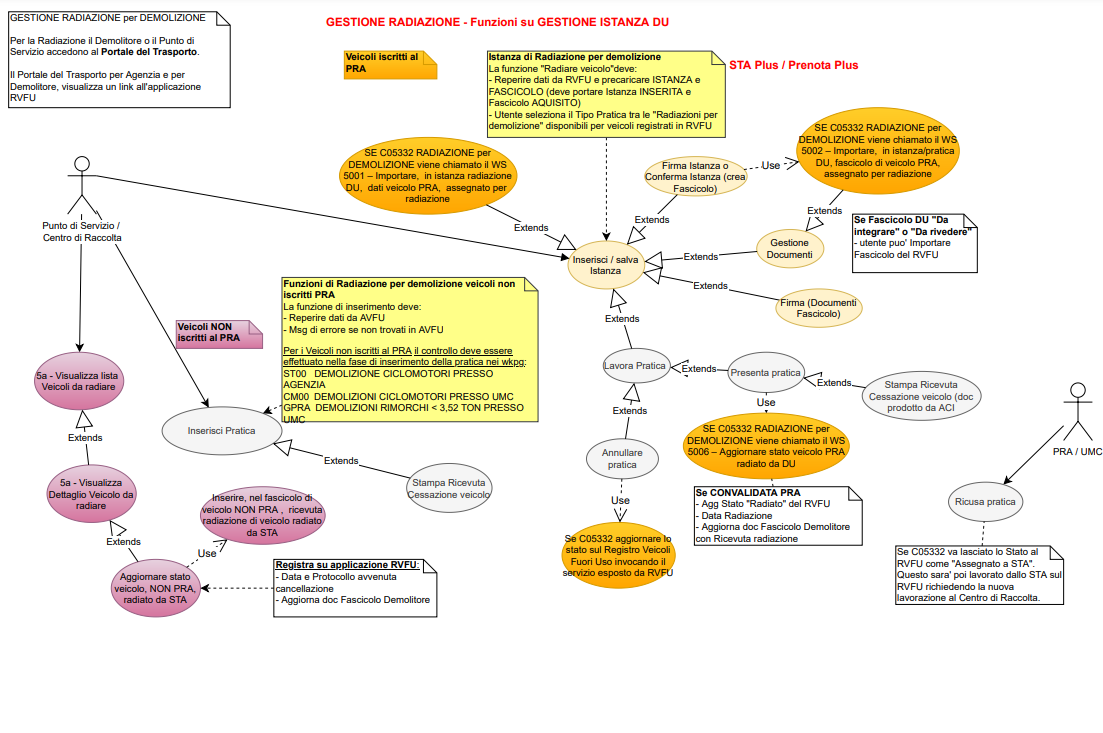












# DEFINIZIONE DEI SERVIZI

Nel presente capitolo viene fornita una descrizione completa delle operazioni (file HTML) disponibili e sono contenuti i json.

Ogni operazione ha come risposta due elementi:

un esito (obbligatorio), che indica al chiamante se la chiamata è andata a buon fine (CodiceEsito=OK) oppure se è stato riscontrato un problema che non ha permesso la corretta esecuzione dell’operazione richiesta (CodiceEsito=KO) Di seguito un esempio di un esito indicando un problema in fase di esecuzione dell’operazione:

un risultato (opzionale), che contiene il dettaglio dei dati di risposta se ci sono

|  |
| --- |
| {  "esito": {    "codice": "KO",    "descrizione": "Descrizione dell’errore"   }  "risultato": {}  } |

## HTML

La documentazione è specificata nel seguente documento html:

****

## JSON

Nel file json sono presenti tutti gli endpoint esposti alle swh; i servizi rivolti al profilo concessionario sono quelli che iniziano con il seguente path:

/demolitori-aci-ws/rest/concessionario/



## ESEMPI DI CHIAMATE AI SERVIZI

Di seguito si riportano gli esempi sugli endpoint dei WS comprensivi del dettaglio dei parametri nelle request, dei valori ammessi proveniente da tipologiche e la lunghezza dei campi string.



## TIPOLOGICHE

Di seguito le tipologiche relative agli Stati del Veicolo e agli stati del Fascicolo.

Per le altre Tipologiche fare riferimento agli esempi del paragrafo 4.3

### STATI VFU

|  |  |
| --- | --- |
| **CODICE** | **DESCRIZIONE** |
| C | CONFERITO |
| T | TRASFERITO |
| P | PRESO IN CARICO |
| R | DA RADIARE |
| N | INVIATO A STA |
| S | RADIATO |
| D | DEMOLITO |
| A | ANNULLATO |
| I | INSERITO |
| V | VALIDATO |
| Z | CEDUTO |

### STATI FASCICOLO

|  |  |
| --- | --- |
| **CODICE** | **DESCRIZIONE** |
| I | Inserito |
| C | Chiuso |
| S | Integrazione |

### TIPO DOCUMENTO

|  |  |
| --- | --- |
| **CODICE** | **DESCRIZIONE** |
| A | Attestazione presentazione formalità |
| B | Cdp |
| C | Certificato di rottamazione |
| D | Denuncia |
| E | Ricevuta radiazione |
| F | Foglio complementare |
| I | Documento di identità intestatario |
| L | Altro |
| M | Documento di identità detentore |
| P | Certificato di proprietà |
| R | Ricevuta presa in carico |
| S | Denuncia di smarrimento |
| T | Procura del detentore |
| U | Documento Unico |
| V | Verbale di consegna |
| Z | Carta di circolazione |

### TIPO VEICOLO

|  |  |
| --- | --- |
| **CODICE** | **DESCRIZIONE** |
| A | AUTOVEICOLO |
| B | ALTRO |
| C | CICLOMOTORE |
| F | FILOBUS |
| M | MOTOVEICOLO PRA |
| N | MACCHINE OPERATRICI TRAINATE |
| P | MACCHINE OPERATRICI SEMOVENTI |
| R | RIMORCHIO |
| S | MACCHINE AGRICOLE SEMOVENTI DUE ASSI |
| T | RIMORCHI AGRICOLI |
| U | MACCHINE AGRICOLE SEMOVENTI UN ASSE |
| V | MACCHINE AGRICOLE OPERATRICI |
| X | MACCHINE AGRICOLE TRAINATE |
| Z | MACCHINE OPERATRICI NON CIRCOLANTI |
| Y | RIMORCHI AGRICOLI CON MASSA |

# MODALITÀ DI AUTENTICAZIONE DI UN UTENTE PER L’UTILIZZO DEI WEB SERVICE

Vengono di seguito descritte delle linee guida di integrazione per permettere alle applicazioni di integrarsi con il sistema IAM mediante OpenID Connect.

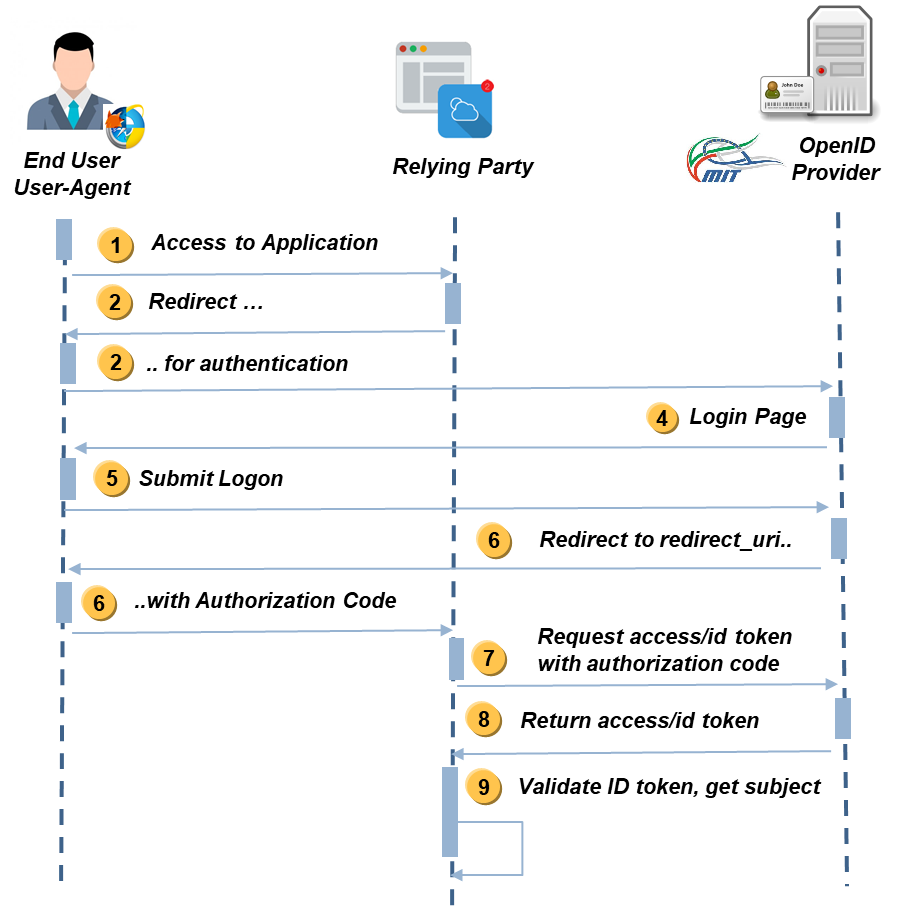
Secondo il modello di autenticazione OIDC, l’infrastruttura IAM agirà da OpenID Provider (OP) e l’applicazione da integrare da Relying Party (RP) in accordo alle specifiche del protocollo OpenID Connect 1.0 [<https://openid.net/connect/>]. Per un livello di sicurezza adeguato, è necessario garantire un canale sicuro tra i client e l’OpenID Provider.

OpenID Connect 1.0 è l’identity layer costruito on top al protocollo OAuth 2.0 [<https://tools.ietf.org/html/rfc6749>]. Permette al client di verificare l’identità dell’utente finale sulla base dell’autenticazione effettuata verso l’OpenID Provider ed ottenere allo stesso tempo informazioni aggiuntive relative all’utente.

OpenID Connect ha ereditato da OAuth2 degli standard denominati Grant Types (chiamati anche flows o protocol flows) che descrivono come il client può interagire con l’OpenID Provider per ricevere un token autorizzativo.

Il flusso utilizzato per l’integrazione all’interno dell’infrastruttura IAM è ***Authorization Code Flow****.*

Di seguito, a titolo di esempio, il diagramma di flusso che rappresenta l’autenticazione di un RP con grant type **Authorization Code Flow**:



OIDC Authorization Code Flow (Standard)

## Specifiche OpenID Provider

### URL SERVIZI DI AUTENTICAZIONE

### AMBIENTE DI ESERCIZIO

L’indirizzo in ambiente di esercizio dei servizi di autenticazione è il seguente:

*{{baseUrl}}=* [*https://sso.ilportaledeltrasporto.it/sso*](https://sso.ilportaledeltrasporto.it/sso/)

### AMBIENTE DI FORMAZIONE

L’indirizzo in ambiente di collaudo dei servizi di autenticazione è il seguente:

*{{baseUrl}}=* [*https://ssoformazione.ilportaledeltrasporto.it/sso*](https://ssoformazione.ilportaledeltrasporto.it/sso/)

Di seguito sono riportati gli EndPoint utilizzati:

|  |  |
| --- | --- |
| **Nome Servizio** | **URL** |
| Authenticate | [*{{baseUrl}}*/json/authenticate](https://ssoformazione.ilportaledeltrasporto.it/sso/json/authenticate) |
| Authorize | *{{baseUrl}}*/oauth2/authorize |
| AccessToken | *{{baseUrl}}*/oauth2/access\_token |
| EndSession | *{{baseUrl}}*[/oauth2/connect/endSession](https://ssoformazione.ilportaledeltrasporto.it/sso/oauth2/connect/endSession) |

Tra gli endpoint disponibili vi sono:

* */sso/oauth2/authorize***:** definito in [rfc6749](https://tools.ietf.org/html/rfc6749)serve per raccogliere il consenso e l’autorizzazione per il proprietario della risorsa.
* */sso/oauth2/access\_token:* definito in [rfc6749](https://tools.ietf.org/html/rfc6749)serve per ottenere I token richiesti dall’applicazione (access, refresh e Id token)
* */sso/oauth2/connect/endSession:*definito in [openid\_spec](https://openid.net/specs/openid-connect-session-1_0.html#rfc.section.4.1)termina la sessione dell’utente autenticato**.**

### OIDC TOKENS

Nella risposta che l’OP fornisce al RP vi sono i seguenti token:

* L’ **ID Token,** in formato*JWT*, specifico per il protocollo *OpenID Connect*, contiene tra gli altri i claims relativi all’informazione dell’utente.
* L’ **Access Token,** specifico per il protocollo *OAuth2*,è il token che può essere speso per essere autorizzati ad accedere direttamente ad una risorsa.
* Il **Refresh Token,** specifico per il protocollo *OAuth2*, contiene informazioni necessarie a recuperare un nuovo access token, tipicamente quando l’access token è scaduto. *Tale token viene rilasciato solo su richiesta del client qualora necessario per scopi applicativi.*

L’ ID Token e l’Access Token, di solito, hanno una validità temporale molto limitata. Anche i Refresh Token scadono ma tipicamente hanno una lunga durata e sono soggetti a vincoli di memorizzazione stringenti per evitare che siano trafugati da un attaccante.

Di seguito un esempio di access token, id token e refresh token rilasciati dall’infrastruttura IAM:

*{"access\_token":"fdhYNyTikmph8MCI2MgMq2MVdGE","refresh\_token":"jRo-4GUC8ImpgiJ6eNeYoVGjQsI","scope":"openid profile","id\_token":"eyJ0eXAiOiJKV1QiLCJraWQiOiIxTi9xbkgrUnJSZVk5V29pN00zRW02eDZ1S0E9IiwiYWxnIjoiUlMyNTYifQ.*eyJhdF9oYXNoIjoiY0dZcG9kRmdETHVoaUFjTUpCOTMtZyIsInN1YiI6IkFHUk0wNjQ5MDEiLCJhdWRpdFRyYWNraW5nSWQiOiJmYTEzNjY2Ny05YzllLTQxNTQtYWQzNy0wNWMzZmE2NWJmOTItMTUzNzM5IiwiaXNzIjoiaHR0cDovL3Nzb2Zvcm1hemlvbmUuaWxwb3J0YWxlZGVsdHJhc3BvcnRvLml0L3Nzby9vYXV0aDIiLCJ0b2tlbk5hbWUiOiJpZF90b2tlbiIsIm5vbmNlIjoiMTIzYWJjIiwiYXVkIjoic29.VAVGrzlwq72wkDOUQPJ1W\_y1UmD\_s9jJlzRyiFi3RqQCiUchAiPvo4K0Xu9PTuSxWKd3ETtC\_zG0QiXjbrJzyaXLiAemOwIl0sPVIyCGhdqFHG84mP1Jwys167BjZ3lvR2UG6Y8\_GOC44grJKpiwA1h\_6z06iFNW42AnfUQMmtArMK2A62hbUrCoCtqgGtaiQxepk0CkafGygT-nUGmBgsoTyhtYH\_D8VOrMigSLXsD6mWrIEm-ELoTkQIJA-6GNQCUXOyLTyIDexW31c278KvvCZdK7oa4SXOcTyUih2x6GSHij7hsGQOam2MPnZhCh-oM0SZdbY1rfVZje0MkNEg","token\_type":"Bearer","expires\_in":1799,"nonce":"123abc"}

L’ID token, essendo un JWT, è diviso in *tre sezioni*, separate da carattere punto (.), come da indicazioni [openid\_spec\_idtoken](https://openid.net/specs/openid-connect-core-1_0.html#IDToken).

Nella prima parte sono riportate le informazioni relative al tipo di token ed algoritmo utilizzato (in questo caso RS256). Nella seconda (evidenziata in grigio), è presente il payload codificato in base64 con le claim relative all’utente autenticato ed i dati relativi all’emissione del ticket, tra i quali:

* sub: subject per il quale è stato rilasciato il token
* iss: URL dell’Authorization server issuer
* auth\_time: timestamp dell’autenticazione
* exp: scadenza del token

Di seguito, viene rappresentato a titolo di esempio in ambiente di **FORMAZIONE** il payload decodificato dell’id\_token :

*{*

*"sub": "<UserIdAgenzia>",*

*"auditTrackingId": "fa136667-9c9e-4154-ad37-05c3fa65bf92-139234",*

*"iss": "http://ssoformazione.ilportaledeltrasporto.it/sso/oauth2",*

*"tokenName": "id\_token",*

*"nonce": "123abc",*

*"aud": "softwarehouse1",*

*"c\_hash": "7QZnkWwiQVZMsxLZfxIgNA",*

*"acr": "0",*

*"org.forgerock.openidconnect.ops": "E9l3hJoCe9GT0h-2NRjxFYXimUY",*

*"s\_hash": "bKE9UspwyIPg8LsQHkJaiQ",*

*"azp": "softwarehouse1",*

*"auth\_time": 1623243153,*

*"name": "<NomeAgenzia>",*

*"realm": "/",*

*"exp": 1623268788,*

*"tokenType": "JWTToken",*

*"family\_name": "<Agenzia>",*

*"iat": 1623243588*

*}*

nella terza ed ultima parte è specificata la signature per la verifica della stessa.

## Informazioni DI INTEGRAZIONE

Per procedere all’integrazione con la piattaforma IAM, la Software House dovrà condividere le seguenti informazioni:

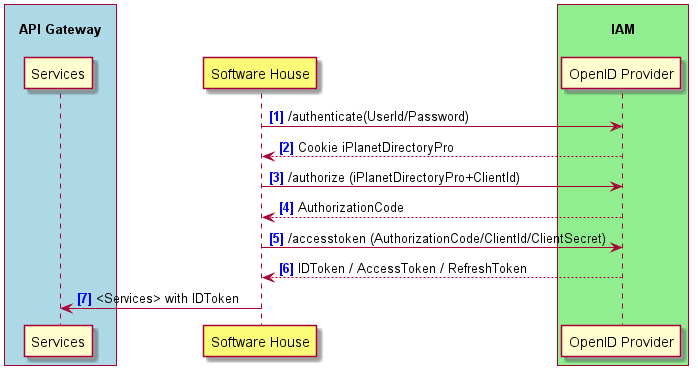
|  |  |  |
| --- | --- | --- |
| **Nome** | **Descrizione** | **Note** |
| ClientID | Nome del client | CodiceUtente di IdentificativoSoftwareHouse |
| Client Secret | Password del Client | PasswordUtente di IdentificativoSoftwareHouse |
| Redirection URIs | URL di redirect | <https://localhost/> |
| Post Logout URIs | URL di Post Logout | <https://localhost/> |
| AuthorizationCode LifeTime | Durata del Authorization Code | Il valore di default, se non specificato dal client è pari a 2 minuti |
| AccessToken LifeTime | Durata del Access Token | Il valore di default, se non specificato dal client è pari a 30 minuti |
| IDToken LifeTime | Durata del ID Token | Se non specificato dal client è pari a 4 ore |
| RefreshToken LifeTime | Durata del Refresh Token | Il valore di default, se non diversamente richiesto è pari a 2 giorni |

**Il metodo di autenticazione utilizzato è client\_secret\_post.**

## Flusso di Autenticazione

Prima del flusso standard di **Authorization Code Flow**, dovrà essere implementata una chiamata all’endpoint */authenticate* per evitare la richiesta della pagina di Login nella chiamata ai Web Services.

Pertanto il flusso implementato sarà il seguente:



Di seguito sono descritti gli step da effettuare per l’autenticazione:

1. Il client effettua la chiamata all’enpoint ***/autenticate*** per avviare una sessione autenticata con le credenziali dell’agenzia.
2. Il Provider, verifica le credenziali passate e, se valide, restituisce il cookie iPlanetDirectoryPro
3. Il client chiama l’endpoint ***/authorize*** necessario per la prosecuzione del flusso passando il cookie iPlanetDirectoryPro e il ClientId
4. Il Provider verifica le informazioni e restituisce l’AuthorizationCode.
5. Il Client chiama l’endpoint ***/accesstoken*** passando l’AuthorizationCode e le credenziali del Client (ClientID/ClientSecret)
6. Il Provider verifica le informazioni e restituisce l’IDToken, l’AccessToken e il RefreshToken
7. Il Client chiama l’API Gateway passando l’IDToken (Bearer ) nel Header Authorization.

**Tutte le chiamate della fase di autenticazione devono essere fatte in POST.**

### AUTHENTICATE

Per avviare il flusso di autenticazione, necessario per accedere ad una risorsa protetta, il Client dovrà richiamare l’endpoint */authenticate* passando le credenziali di accesso.

Nella chiamata all’endpoint */authenticate*, i parametri necessari sono:

* *user\_id*: è l’identificativo dell’agenzia
* *password*: è la password dell’agenzia
* *Content-Type:* è un valore fisso impostato a “***application/json*”**
* *Accept-API-Version:* è un valore fisso impostato a “***Accept-API-Version*”**

Nella tabella di seguito vengono descritti i parametri di **Input**:

|  |  |  |
| --- | --- | --- |
| **Param** | **Tipologia** | **Valore** |
| Content-Type | header | **application/json** |
| X-OpenAM-Username | header | <UserID Agenzia> |
| X-OpenAM-Password | header | <Passwd Agenzia> |
| Accept-API-Version | header | **Accept-API-Version** |

A titolo di esempio una chiamata, per l’ endpoint dell’ambiente di **FORMAZIONE**, mediante curl:

curl --request POST --header "Content-Type: application/json" --header "X-OpenAM-Username: <UserIDAgenzia>" --header "X-OpenAM-Password: <PasswdAgenzia>" --header "Accept-API-Version: resource=2.0, protocol=1.0" <https://ssoformazione.ilportaledeltrasporto.it/sso/json/authenticate>

Il Sistema IAM verificherà le credenziali passate, e se corrette ritornerà al chiamante il cookie iPlanetDirectoryPro che attesta l’avvenuta autenticazione sul sistema.

Di seguito un esempio di risposta in caso di autenticazione avvenuta con successo, che contiene l’IPlanetDirectoryPro (in grassetto con il nome di **tokenID**):

{

"tokenId": "**k2tqmxhjYYfH4cYirncim0zHgxk.\*AAJTSQACMDIAAlNLABxxemtTT3hYeGNvK1dsT3hOVVQrUURNMVpvTGM9AAR0eXBlAANDVFMAAlMxAAIwNA..\***",

"successUrl": "/sso/console",

"realm": "/"

}

Di seguito un esempio di risposta in caso di **autenticazione fallita**

{

"code": 401,

"reason": "Unauthorized",

"message": "Authentication Failed"

}

### AUTHORIZE

La chiamata all’endpoint */authorize* serveper ottenere l’**authorization** **code**, necessario per la prosecuzione del flusso. I parametri necessari sono:

* *iPlanetDirectoryPro*: è il valore del Cookie ritornato dal servizio /*authenticate*.
* *scope*: è un valore fisso impostato a “**openid profile**”.
* *response\_type*: è un valore fisso impostato a “**code**”.
* *client\_id*: è l’identificativo univoco del client indicato nelle informazioni di integrazione.
* csrf: è il valore del Cookie ritornato dal servizio /*authenticate*.
* *redirect\_uri*: è il valore di redirect indicato nelle informazioni di integrazione.
* *state*: è un valore fisso impostato a “**abc123**”*.*
* *nonce*: è un valore fisso impostato a “**123abc**”*.*
* *decision*: è un valore fisso impostato a “**allow**”*.*

Nella tabella di seguito vengono riepilogati i parametri di **Input**:

|  |  |  |
| --- | --- | --- |
| **Param** | **Tipologia** | **Valore** |
| iPlanetDirectoryPro | Cookie | <Valore del cookie tornato dalla chiamata /authenticate> |
| scope | data | **openid profile** |
| response\_type | data | **code** |
| client\_id | data | <ClientID della SoftwareHouse> |
| csrf | data | <Valore del cookie tornato dalla chiamata /authenticate> |
| redirect\_uri | data | <Redirection URI SoftwareHouse> |
| state | data | **abc123** |
| nonce | data | **123abc** |
| decision | data | **allow** |

A titolo di esempio una chiamata, per gli endpoint dell’ambiente di **FORMAZIONE**, mediante curl:

curl --dump-header - --request POST --Cookie "iPlanetDirectoryPro=GcJUXdAjFcCFjYdnIVw8qM7clFU.\*AAJTSQACMDIAAlNLABxNTFNZZGxRTUE4T2pETk5NWEp5SGRCTW5RV2M9AAR0eXBlAANDVFMAAlMxAAIwMQ..\*" --data "scope=openid profile" --data "response\_type=code" --data "client\_id=softwarehouse1" --data "csrf=GcJUXdAjFcCFjYdnIVw8qM7clFU.\*AAJTSQACMDIAAlNLABxNTFNZZGxRTUE4T2pETk5NWEp5SGRCTW5RV2M9AAR0eXBlAANDVFMAAlMxAAIwMQ..\*" --data "redirect\_uri=http://localhost/" --data "state=abc123" --data "nonce=123abc" --data "decision=allow" https://ssoformazione.ilportaledeltrasporto.it/sso/oauth2/authorize

Questo un esempio di risposta, che contiene l’authorization code (in grassetto):

<redirect url>?code=**1AxzjSmuIkEG9MTF4wrff\_5PpLs**&iss=http%3A%2F%2Fssoformazione.ilportaledeltrasporto.it%2Fsso%2Foauth2&state=abc123&client\_id=softwarehouse1

Riferirsi comunque alle specifiche del proprio client oidc/oauth2.

### ACCESS TOKEN

Nella chiamata all’endpoint */access\_token*, i parametri necessari sono:

* *grant\_type*: valore fisso impostato a “*authorization\_code”*.
* *code*: è l’authorization code ottenuto in precedenza dall’endpoint /*authorize.*
* *client\_id*: è l’identificativo univoco del client della SoftwareHouse, definito nelle informazioni di integrazione.
* *client\_secret*: è la password del client della SoftwareHouse, definito nelle informazioni di integrazione.
* *redirect\_uri*: è il valore di redirect indicato nelle informazioni di integrazione.

Nella tabella di seguito vengono riepilogati i parametri di **Input**:

|  |  |  |
| --- | --- | --- |
| **Param** | **Tipologia** | **Valore** |
| grant\_type | data | **authorization\_code** |
| code | data | <Valore ritornato dalla chiamata /*authorize*> |
| client\_id | data | <ClientID della SoftwareHouse> |
| client\_secret | data | <ClientIPassword della SoftwareHouse> |
| redirect\_uri | data | <Redirection URI SoftwareHouse> |

A titolo di esempio una chiamata, per gli endpoint dell’ambiente di **FORMAZIONE**, mediante curl:

curl --request POST --data "grant\_type=authorization\_code" --data "code=R\_rdi4dn0dTtOgDzLzVV83pACYw" --data "client\_id=softwarehouse1" --data "client\_secret=<Password>" --data "redirect\_uri=http://localhost/" https://ssoformazione.ilportaledeltrasporto.it/sso/oauth2/access\_token

Questo un esempio di risposta, che contiene i Token:

{"**access\_token**":"4snJehFX6iIcJm4JS-bPHSUKf\_U","**refresh\_token**":"J1KdkBSuM8VUWJfnZlBdgIvB4-0","scope":"openid profile","**id\_token**":"eyJ0eXAiOiJKV1QiLCJraWQiOiIxTi9xbkgrUnJSZVk5V29pN00zRW02eDZ1S0E9IiwiYWxnIjoiUlMyNTYifQ.eyJhdF9oYXNoIjoiM2R6Rl9TUC1tcllzN0EzcGZOUFZSUSIsInN1Y…","token\_type":"Bearer","expires\_in":1799,"nonce":"123abc"}

Riferirsi comunque alle specifiche del proprio client oidc/oauth2.

## AGGIORNAMENTO Token

La funzione di aggiornamento del Token, serve per ottenere un nuovo token di accesso quanto il token corrente non è più valido. Per effettuare il refresh del token, viene utilizzato l’’endpoint */access\_token*, e i parametri necessari sono:

* *grant\_type*: valore fisso impostato a “*refresh\_token”*.
* *refresh\_token*: è il token precedentemente memorizzato dalla chiamata ad /*access\_token*.
* *client\_id*: è l’identificativo univoco del client della SoftwareHouse, definito nelle informazioni di integrazione.
* *client\_secret*: è la password del client, definito nelle informazioni di integrazione.
* *scope*: è un valore fisso impostato a “**openid profile**”.

Nella tabella di seguito vengono riepilogati i parametri di **Input**:

|  |  |  |
| --- | --- | --- |
| **Param** | **Tipologia** | **Valore** |
| grant\_type | data | **refresh\_token** |
| refresh\_token | data | <valore del token precedentemente memorizzato> |
| client\_id | data | <ClientID della SoftwareHouse> |
| client\_secret | data | <ClientIPassoword della SoftwareHouse> |
| scope | data | **openid profile** |

A titolo di esempio una chiamata, per gli endpoint dell’ambiente di **FORMAZIONE**, mediante curl:

curl --request POST --data "grant\_type=refresh\_token" --data "refresh\_token=xTQx4lqw0VxzLxTl9XtvpiMjHAw" --data "client\_id=softwarehouse1" --data "client\_secret=<Password>" --data "scope=openid%20profile" https://ssoformazione.ilportaledeltrasporto.it/sso/oauth2/access\_token

Questo un esempio di risposta, che contiene i Token:

{"**access\_token**":" OSoUB2kkHtbZ5a1vSxBLLw4qtJw ","**refresh\_token**":" kd9hxvEx73sMkzNVuVWe84X5Xgo ","scope":"openid profile","**id\_token**":" eyJ0eXAiOiJKV1QiLCJraWQiOiIxTi9xbkgrUnJ SZVk5V29pN00zRW02eDZ1S0E9IiwiYWxnIjoiUlMyNTYifQ.eyJhdF9oYXNoIjoiM2R6Rl9TUC1tcllzN0EzcGZOUFZSUSIsInN1Y…","token\_type":"Bearer","expires\_in":1799,"nonce":"123abc"}

Riferirsi comunque alle specifiche del proprio client oidc/oauth2.

## Logout

Quando l’utente effettua la logout direttamente dal RP, quest’ultimo dovrà eseguire le chiamata verso gli endpoint /endSession per cancellare la sessione, l’access token e il refresh token. **E’ a carico del RP la cancellazione delle sessioni applicative dell’utente.**

Nella chiamata all’endpoint /endSession, i parametri necessari sono:

* *client\_id:* è l’identificativo univoco del client (RP)
* *id\_token\_hint*: è il valore dell’ID Token dell’utente che sta effettuando la logout.
* *post\_logout\_redirect\_uri*: è il valore di post-logout-redirect URL indicato nelle informazioni di integrazione.

In questo caso, la chiamata viene fatta in **GET**.

A titolo di esempio una chiamata, per gli endpoint dell’ambiente di **FORMAZIONE**, mediante curl:

curl --request GET https://ssoformazione.ilportaledeltrasporto.it/sso/oauth2/connect/endSession?id\_token\_hint=eyJ0eXAiOiJKV1QiLCJraW...&client\_id=softwarehouse1&post\_logout\_redirect\_uri=http://localhost/

# APPENDICE B: Termini ed acronimi

| **Termine** | **Definizione** |
| --- | --- |
| JSON | JavaScript Object Notation |
| RVFU | Registro veicoli fuori uso |
| CR | Centro Raccolta |
| CN | Concessionario |