(ALLEGATO)
SERVIZI DI INTEROPERABILITA' PER I SOGGETTI REGISTRATI AI SERVIZI TELEMATICI ENTRATEL E FISCONLINE

VERSIONE 1.0 DEL 25 GIUGNO 2026

INDICE

1. GENERALITÀ

Sono descritte nel documento le modalità per richiedere l'attivazione di un generico servizio erogato mediante la piattaforma di interoperabilità dell'AE per gli utenti registrati ai servizi telematici Entratel e Fisconline dell'Agenzia Entrate e per il successivo richiamo del servizio stesso, potendo essere necessarie in funzione delle specificità dei singoli servizi ulteriori informazioni che saranno indicate nelle specifiche tecniche di questi.

2. PREREQUISITI PER LA FRUIZIONE DI UN SERVIZIO

La prima attività da svolgere per fruire di un servizio è la richiesta di attivazione, accedendo con le credenziali di identità digitale o ove disponibili con quelle rilasciate dall'Agenzia delle entrate, all'applicazione 'Catalogo dei servizi di Interoperabilità', nell'ambito dell'Area Riservata del portale dell'Agenzia delle entrate.

A fronte della richiesta di attivazione per la fruizione del servizio, i soggetti richiedenti dello specifico servizio otterranno una chiave di sicurezza (client_secret), da utilizzare in fase di invocazione del servizio. Nella medesima applicazione saranno rese disponibili le informazioni per consentire di simulare il richiamo del servizio in ambiente di Validazione, con dati non reali.

Per implementare la cornice di sicurezza necessaria per gestire l'autenticazione e autorizzazione in fase di invocazione di un servizio, adottando i pattern di sicurezza previsti dal ModiPA, è necessario inoltre che i soggetti fruitori siano in possesso dei certificati rilasciati dalla Certification Authority (CA) dell'Agenzia delle entrate, ad oggi utilizzati per la firma e la cifratura dei flussi trasmessi da parte degli utenti registrati ai servizi telematici, sia persone fisiche che persone giuridiche.

3. PRINCIPALI CARATTERISTICHE DEI SERVIZI

I servizi sono realizzati in tecnologia REST e resi disponibili sia in ambiente di Validazione per effettuare esclusivamente delle prove di richiamo del servizio con dati non reali, che nell'ambiente di Produzione.

Gli endpoint di riferimento e i descrittori dei servizi per l'invocazione nell'ambiente di Validazione e in quello di Produzione sono resi disponibili agli utenti nell'ambito dell'applicazione 'Catalogo dei servizi di Interoperabilità' all'atto della richiesta di attivazione dello specifico servizio.

I servizi possono essere basati su un'unica interazione che a fronte dell'invocazione del servizio restituisce in modo sincrono quanto atteso o prevedere un'interazione di tipo asincrono che a fronte dell'invocazione del servizio per effettuare una richiesta, prevede una successiva interazione con il servizio stesso per verificare se elaborato quanto richiesto e ottenerlo.

Per questa ultima tipologia di servizi, utilizzata principalmente per ottenere informazioni massive o che richiedono elaborazioni differite, saranno normalmente previste tre distinte risorse per ciascun servizio mediante le quali:

- sottomettere una richiesta di elaborazione.
- monitorare lo stato di elaborazione di una richiesta precedentemente sottomessa e prelevare l'esito prodotto al completamento dell'elaborazione stessa.
- consentire di monitorare lo stato del servizio attivo/non-attivo.

Nel caso di servizi che prevedono un'unica interazione saranno generalmente presenti due risorse, la prima sempre presente per sottomettere la richiesta ed avere la risposta, la seconda per consentire di monitorare lo stato del servizio attivo/non-attivo.

3.1 PATTERN DI SICUREZZA

I servizio applicano i seguenti pattern di sicurezza individuati dal modello ModiPA e descritti nel dettaglio al par. 4.

- **[ID_AUTH_CHANNEL_01]** Direct Trust Transport-Level Security
- **[ID_AUTH_REST_01]** Direct Trust con certificato X.509
- **[INTEGRITY_REST_01]** Integrità del payload messaggio REST
- **[AUDIT_REST_01]** Inoltro dati tracciati nel dominio del Fruitore REST

In fase di invocazione del servizio, il fruitore dovrà fornire:

- un token di autorizzazione da indicare nell'header **Authorization**
- un token di integrità da indicare nell'header **Agid-JWT-Signature**
- un token di audit da indicare nell'header **Agid-JWTTrackingEvidence**

Tutti e tre i token devono essere firmati con la chiave privata associata al certificato rilasciato dall'Agenzia delle Entrate e nella disponibilità del fruitore.

Per l'implementazione dei token si rimanda alle linee guida Versione 1.2 del 29/11/2023 del ModiPA fermo restando che:

tutti e tre i token devono riportare i claim:

- **alg** (RS256)
- **typ** (JWT)
- **x5c** certificato di firma utilizzato per firmare i token.

Il token di autenticazione, veicolato attraverso l'header **Authorization**, dovrà inoltre riportare i seguenti claim:

- **jti**: come da specifiche ModiPA
- **iss**: contenente il CN del certificato rilasciato dall'Agenzia delle entrate nella disponibilità del fruitore
- **aud**: da valorizzare, in base all'ambiente (verifica/produzione), con quanto indicato come audience nella documentazione di ciascun servizio (all'interno del file readme) disponibile nel 'Catalogo dei servizi di Interoperabilità'
- **sub**: contenente il CN del certificato rilasciato dall'Agenzia delle entrate nella disponibilità del fruitore
- **iat**: come da specifiche ModiPA
- **nbf**: come da specifiche ModiPA
- **exp**: valorizzare prevedendo una durata del token pari a 300 secondi
- **client_id**: contenente il CN del certificato Entratel nella disponibilità del fruitore

Anche la risposta prodotta seguirà il pattern **INTEGRITY_REST_01**, sarà quindi compito del fruitore validare l'integrità della risposta ottenuta (il token sarà veicolato attraverso l'header **Agid-JWT-Signature**).

All'interno del token verrà indicato nel claim '**request_digest**' il contenuto del digest della richiesta per fornire una prova di non ripudio al richiedente.

Il token di audit, veicolato attraverso l'header **Agid-JWTTrackingEvidence**, dovrà inoltre riportare i seguenti claim, secondo quanto richiesto dalle specifiche ModiPA :

- **userID**: un identificativo univoco dell'utente interno al dominio del fruitore (ad esempio la matricola o la chiave di autenticazione per accedere ad un'applicazione sw del fruitore che richiama il servizio per richiedere e consultare i dati)
- **userLocation**: un identificativo univoco della postazione/sistema interni al dominio del fruitore (ad esempio un indirizzo ip della postazione dalla quale utilizzata l'applicazione sw del fruitore di cui al punto precedente)
- **LoA**,: livello di sicurezza o di garanzia adottato nel processo di autenticazione informatica nel dominio del fruitore (ad esempio una Basic Authentication, Multi Factor Authentication, Identità Digitale o altra per accedere all'applicazione sw di cui ai punti precedenti)

Le informazioni relative al token di audit unitamente ad altre informazioni presenti nella richiesta e risposta, saranno oggetto di tracciamento dell'utilizzo dei servizi da parte dei fruitori.

3.2 ESEMPIO DI GENERICO SERVIZIO CON INTERAZIONE ASINCRONA

Per questa tipologia di servizi è prevista una risorsa per gestire la richiesta e una seconda risorsa per monitorarne lo stato di elaborazione e prelevare l'esito quando prodotto.

La sottomissione di una richiesta (in base anche al riferimento al descrittore dello specifico servizio) prevede oltre ai token di sicurezza, un payload json di input che generalmente a meno di specificità del singolo servizio include:

- **client_secret:** rilasciato dall'applicazione per l'attivazione del servizio
- **codicefiscale_operatore**: codice fiscale della persona che presenta la richiesta a proprio nome o a nome del soggetto lo ha autorizzato in qualità di incaricato (per autorizzare gli incaricati all'utilizzo dei servizi uno dei gestori deve utilizzare le funzionalità "Gestione incarichi come gestore - Gestisci servizi" presenti nel profilo utente del soggetto incaricante)
- **sede_operatore:** sede telematica del richiedente che effettua la richiesta se Entratel (opzionale)**.**
- **Dati di input della richiesta,** dipendenti dal singolo servizio.

A meno di errori di validazione o autorizzativi la risorsa del servizio utilizzata per inoltrare la richiesta risponde restituendo un numero identificativo di questa, che deve essere utilizzato successivamente come elemento per verificare lo stato di elaborazione della richiesta e, al completamento della stessa, ottenere l'esito prodotto. Di seguito un esempio di risposta in assenza di errori:

```
{
   "esito":0,
   "messaggio":"Operazione completata con successo",
   "protocollo":"numeroprotocollo"
}
```

Eventuali errori di validazione o autorizzativi saranno restituiti generalmente con una struttura di risposta similare a quella seguente, a meno di specificità dei singoli servizi.

Il contenuto del *messaggio_dettaglio* permetterà al fruitore di individuare la motivazione dell'errore.

```
{
    "detail": messaggio_dettaglio,
    "instance": "",
    "status": 400,
    "title": "Errore di validazione",
    "type": "about:blank"
}
```

I controlli principali effettuati sono i seguenti:

- il Secret deve risultare valido (la validità è annuale),
- il Secret deve essere associato al soggetto che ha firmato la richiesta e coerente con il servizio richiamato,
- l'utente che ha firmato la richiesta deve risultare abilitato al servizio telematico e registrato con una delle tipologie autorizzate all'utilizzo del servizio,
- in caso di soggetto richiedente diverso dal soggetto che ha firmato la richiesta, è verificato che il soggetto che opera sia incaricato del soggetto e autorizzato a presentare la richiesta.

- altri controlli specifici dei singoli servizi.

3.2.1 RECUPERO DELL'ESITO DI UNA RICHIESTA

Il recupero dell'esito prodotto (in base anche al riferimento al descrittore del servizio) avviene mediante l'invocazione di una seconda risorsa del servizio, la quale prevede, oltre alla indicazione dei token di sicurezza, un payload json di input che generalmente a meno di specificità del singolo servizio include:

- **client_secret**: rilasciato dall'applicazione di attivazione
- **codicefiscale_operatore**: codice fiscale della persona che presenta la richiesta a proprio nome o a nome del soggetto lo ha autorizzato in qualità di incaricato (per autorizzare gli incaricati all'utilizzo dei servizi uno dei gestori deve utilizzare le funzionalità "Gestione incarichi come gestore - Gestisci servizi" presenti nel profilo utente del soggetto incaricante)
- **sede_operatore:** sede telematica del richiedente che effettua la richiesta se Entratel (opzionale)
- **identificativo telematico:** il codice identificativo restituito a seguito della sottomissione della richiesta

Il servizio a meno di errori di validazione o autorizzativi risponde nel seguente modo:

- se la richiesta è ancora in lavorazione viene restituito un HTTP Status Code 202 con il seguente possibile payload:

```
{
    "esito": 0,
    "messaggio": "In elaborazione"
}
```

- se la richiesta si è conclusa con uno scarto viene restituito un HTTP Status Code 200 con il seguente possibile payload:

```
{
    "esito": 1,
    "dati_scarto": File o altri dati,
    "messaggio": "Scartato"
}
```

- se la richiesta si è conclusa con successo ed è stato prodotto un esito viene restituito un HTTP Status Code 200 con il seguente possibile payload nel caso ad esempio di restituzione di un file con i dati elaborati:

```
{
    "esito": 0,
    "file_dati": filedati,
    "messaggio": "Download completato (mock)"
}
```

Eventuali errori di validazione o autorizzativi saranno restituiti per averne evidenza nel richiamo del servizio. A titolo di esempio di seguito delle possibili codifiche, dipendenti quelle effettive dalle specifiche del singolo servizio.

TP Status	Codice / Tipo errore	Descrizione
403 – Forbidden	client_secret invalido	Il client_secret fornito non è valido
	client_secret scaduto	Il client_secret risulta scaduto
	Utente non autorizzato	Utente non abilitato o non presente in *utenti_unif*
	Utente senza partita IVA attiva	Utente privo di partita IVA attiva (solo per servizi che la richiedono)
	Operatore non autorizzato	Utente non abilitato o non registrato ai servizi telematici
	Operazione non autorizzata	Operatore incaricato non autorizzato per l'operazione richiesta. L'autorizzazione è rilasciata dal gestore incaricato tramite le funzionalità disponibili nella sezione "Gestione incarichi come gestore - Gestisci servizi" del profilo utente del soggetto incaricante
400 – Bad Request	*nomecampo* mancante	Campo (*nomecampo)* obbligatorio non valorizzato
	Errore costruzione richiesta	Dati richiesta non corretti

4. DETTAGLIO DEI PATTERN DI SICUREZZA APPLICATI

In riferimento alle linee guida Versione 1.2 del 29/11/2023 del ModiPA che li riportano in maggiore dettaglio si descrivono brevemente di seguito i pattern di sicurezza adottati.

[ID_AUTH_CHANNEL_01] DIRECT TRUST TRANSPORT-LEVEL SECURITY

Questo pattern è necessario a garantire un canale confidenziale e sicuro permettendo al tempo stesso il riconoscimento del solo erogatore da parte del fruitore (mediante trust del certificato digitale presentato).

Garantisce quindi una comunicazione tra fruitore ed erogatore che assicuri, a livello di canale:

- confidenzialità;
- integrità;
- identificazione del solo erogatore, quale organizzazione;
- difesa dalle minacce derivanti dagli attacchi: Replay Attack e Spoofing.

Nell'ambito dell'esposizione presa in considerazione si prevederà la configurazione di un certificato SSL server di cui il fruitore dovrà effettuare il trust.

[ID_AUTH_REST_01] DIRECT TRUST CON CERTIFICATO X.509 SU REST

Questo pattern consente di individuare a livello di messaggio il fruitore che sta accedendo al servizio: questi, infatti, fornisce un token JWT firmato di durata limitata di cui l'erogatore può verificarne la firma e la validità temporale ai fini dell'erogazione del servizio.

Il pattern, quindi, assicura a livello di messaggio:

- accesso del soggetto fruitore, quale organizzazione o unità organizzativa fruitore, o entrambe le parti

Il presente profilo declina l'utilizzo di:

- JSON Web Token (JWT) definita dal RFC 7519
- JSON Web Signature (JWS) definita dal RFC 7515

[INTEGRITY_REST_01] INTEGRITÀ DEL PAYLOAD MESSAGGIO REST

Questo pattern consente di assicurare che i messaggi (header e payload) scambiati fra fruitore ed erogatore non siano stati alterati fra l'invio e la ricezione.

Estende quindi i pattern **ID_AUTH_REST_01** aggiungendo alla comunicazione tra fruitore ed erogatore a livello di messaggio:

- integrità del payload del messaggio

Il presente profilo propone l'utilizzo di:

- semantica HTTP RFC 7231;
- Digest HTTP header RFC 3230 per l'integrità della rappresentazione della risorsa;
- JSON Web Token (JWT) definita dal RFC 7519;
- JSON Web Signature (JWS) definita dal RFC 7515.

Per assicurare l'integrità del messaggio il fruitore calcola il valore del Digest header dei representation data secondo le indicazioni in RFC 3230, quindi individua l'elenco degli HTTP Header da firmare, incluso Digest e se presenti HTTP header Content-Type e HTTP header Content-Encoding.

Il token JWS risultante viene posizionato nell'header Agid-JWT-Signature.

L'erogatore decodifica il JWS, verifica la firma e verifica la corrispondenza del contenuto dei claim di integrità con quanto presente negli header http inviati dal fruitore: se la verifica è ok viene erogato il servizio.

In sintesi dal momento che il JWT firmato contenente i claim relativi alla verifica dell'integrità può essere stato generato solo dal fruitore (in quanto firmato con la chiave privata), la corrispondenza dei claim con quelli presenti nell'header della request assicura che il messaggio non sia stato alterato.

[AUDIT_REST_01] INOLTRO DATI TRACCIATI NEL DOMINIO DEL FRUITORE REST

Questo pattern, obbligatorio per gestire il tracciamento della fruizione dei servizi, consente al fruitore di inoltrare le informazioni di tracciamento (ad esempio chi sta effettuando la chiamata e/o da quale postazione) richieste dall'erogatore senza includerle nel corpo del messaggio ma inviandole in un apposito token JWT di Audit che viaggia in uno degli header della request (Agid-JWTTrackingEvidence)

Aggiunge alla comunicazione tra fruitore ed erogatore a livello di messaggio:

- la capacità del fruitore di inoltrare i dati tracciati nel proprio dominio richiesti dall'erogatore

Il presente pattern declina l'utilizzo di:

- JSON Web Token (JWT) definita dal RFC 7519;
- JSON Web Signature (JWS) definita dal RFC 7515.

Esempi di claim che POSSONO essere inclusi nel JWT di audit sono:

- **userID**: un identificativo univoco dell'utente interno al dominio del fruitore (ad esempio la matricola o la chiave di autenticazione per accedere ad un'applicazione sw del fruitore che richiama il servizio per richiedere e consultare i dati)
- **userLocation**: un identificativo univoco della postazione/sistema interni al dominio del fruitore (ad esempio un indirizzo ip della postazione dalla quale utilizzata l'applicazione sw del fruitore di cui al punto precedente)
- **LoA**,: livello di sicurezza o di garanzia adottato nel processo di autenticazione informatica nel dominio del fruitore (ad esempio una Basic Authentication, Multi Factor Authentication, Identità Digitale o altra per accedere all'applicazione sw di cui ai punti precedenti)

Per dare seguito all'inoltro dei dati tracciati nel dominio del fruitore all'erogatore:

- il fruitore DEVE predisporre la rappresentazione dei dati tracciati e firmare la stessa utilizzando il materiale crittografico scambiato nel trust definito (JWS di audit), ove non disponga di una rappresentazione opaca dei dati tracciati e firmati già predisposta nei modi indicati ancora valida nel proprio dominio;
- il fruitore nella request all'erogatore deve includere nell'header Agid-JWTTrackingEvidence la rappresentazione dei dati tracciati e firmati (JWS di audit);
- l'erogatore DEVE verificare la firma del JWS di audit ricevuto nell'header AgidJWT-TrackingEvidence, utilizzando il materiale crittografico scambiato nel trust definito. Nell'attuazione dei precedenti passi il fruitore è responsabile della valorizzazione dei claim inclusi nel JWS di audit.