



# **Linee Guida per Fruttori Esterni di API ModI relative al profilo INPS-MODI-P1**

**versione 1.0 del 12/07/2021**

# Indice

|  |   |
|--|---|
| 1. Introduzione.....   | 3 |
| 2. Il profilo di interoperabilità INPS-MODI-P1.....                            | 4 |
| 2.1 Uso dell'header Identity.....  | 4 |
| 3. L'Adesione ai servizi INPS.....   | 5 |
| 3.1 Censimento del Soggetto Fruitore.....                                      | 5 |
| 4. Dati tecnici per l'Utilizzo dei Profili di Interoperabilità.....            | 7 |
| 4.1 Riferimenti comuni per l'accesso ai servizi ModI di INPS.....              | 7 |
| 4.2 Riferimenti specifici per l'accesso al singolo servizio INPS/MODI.....     | 7 |
| 5. Allegato "A": Lo schema XSD di validazione del SOAP header 'Identity' ..... | 9 |

## 1. Introduzione

Con la recente pubblicazione del Modello di Interoperabilità (in breve anche **ModI**), AGID ha fornito le nuove indicazioni per la realizzazione di scenari di cooperazione applicativa tra enti della pubblica amministrazione, che sostituiscono il precedente modello SPCoop basato sull'uso della Porta di Dominio. La specifica ModI è costituita da 4 diversi documenti tecnici operativi reperibili a partire dal seguente indirizzo web:

- <https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita>

Negli scenari descritti dalla specifica operano i seguenti attori principali:

- I domini, fruitori ed erogatori, che rappresentano il perimetro all'interno del quale sono operativi i sistemi applicativi di ciascun ente amministrativo; le comunicazioni tra due domini devono essere affidate a canali con determinati livelli di sicurezza a livello di trasporto;
- i sistemi applicativi, fruitori ed erogatori, che rappresentano rispettivamente l'origine e la destinazione di ciascuna comunicazione; gli scambi informativi tra tali sistemi possono prevedere specifiche misure di sicurezza a livello dei messaggi scambiati.

Dal punto di vista degli aspetti di sicurezza, la specifica si compone di articolate regole tecniche che riguardano:

- I pattern di sicurezza, a garanzia delle comunicazioni, suddivisi tra pattern per la sicurezza relativi al canale di comunicazione e pattern di sicurezza relativi ai messaggi scambiati.
- I profili di interoperabilità che, partendo da specifiche esigenze funzionali, tipiche degli scambi da supportare tra enti della PA, compongono i diversi pattern di sicurezza da utilizzare, al fine di definire uno scenario di interazione completo.

Scopo di questo documento è quello di descrivere le modalità previste per l'adesione ai servizi INPS erogati sul canale ModI esclusivamente tramite il profilo di interoperabilità "INPS-MODI-P1". Per i dettagli riguardanti l'adesione ai servizi erogati con gli altri profili di interoperabilità si rimanda al documento di linee guida fruitori esterni in versione completa.

## 2. Il profilo di interoperabilità INPS-MODI-P1

L'accesso ai servizi erogati da INPS è consentito ai soggetti esterni che abbiano formalizzato l'adesione alle singole API in accordo alle procedure previste e diffuse da INPS. Le comunicazioni dovranno essere veicolate verso gli endpoint forniti al termine dell'adesione e utilizzeranno canali HTTPS gestiti in conformità con i requisiti della specifica ModI.

Sulla base del servizio o della specifica operazione/risorsa acceduta, la comunicazione dovrà avvenire in conformità ad uno dei tre profili di interoperabilità adottati da INPS, tutti conformi con i pattern previsti da ModI.

In questo documento sono descritte esclusivamente le modalità di accesso al primo dei 3 profili, INPS-MODI-P1, a vantaggio dei fruitori di quei servizi che non utilizzano i profili INPS-MODI-P2 e INPS-MODI-P3. Nel caso i servizi di interesse utilizzino profili diversi da "INPS-MODI-P1" fare riferimento al documento completo di documentazione per i fruitori esterni: "Linee Guida per Fruitori Esterni di API ModI".

Il Profilo "INPS-MODI-P1" prevede la sola autenticazione del soggetto mittente tramite autenticazione HTTPS del Client, così come prevista dal pattern di sicurezza ModI 'ID\_AUTH\_CHANNEL\_02'; per questo profilo non sono quindi previste ulteriori modalità di sicurezza sui messaggi scambiati.

### 2.1 Uso dell'header Identity

Oltre ad autenticarsi tramite HTTPS, i fruitori dovranno comunque popolare tutte le richieste applicative con le seguenti informazioni di header relative all'origine della richiesta applicativa :

- **CodiceUfficio:** codice che identifica la sede o l'ufficio dell'ente da cui è stata richiesta l'invocazione; se l'organizzazione dell'ente non lo prevede, il dato potrà essere popolato con il codice '001';
- **Userid:** codice fiscale o username che identifica univocamente l'operatore dell'ente che ha determinato l'invocazione del servizio; se la tipologia della richiesta applicativa non lo prevede, il dato dovrà essere comunque popolato con un codice significativo a discrezione dell'ente (es: 'OperazioneBatch').

I dati di cui sopra dovranno essere inseriti in tutte le richieste applicative SOAP o REST, come indicato di seguito:

- per i servizi SOAP, le buste inviate dal fruitore dovranno obbligatoriamente includere il SOAP header 'Identity', contenente i due attributi UserId e CodiceUfficio, con struttura come da xsd in allegato "A";
- per i servizi REST, le richieste HTTP inviate da fruitore dovranno obbligatoriamente includere i due header HTTP INPS-Identity-UserId e INPS-Identity-CodiceUfficio.

### 3. L'Adesione ai servizi INPS

L'adesione ad un servizio erogato dalla piattaforma ModI INPS avviene tramite la formalizzazione di un accordo tra le parti che comporta lo scambio delle informazioni necessarie per configurare gli apparati e quindi permettere la corretta instaurazione della comunicazione.

Per finalizzare il processo di adesione, sono a carico dell'Ente aderente le seguenti attività:

1. Individuare il Servizio/API dell'Istituto a cui si intende aderire, ottenendo da INPS i riferimenti tecnici del servizio per gli ambienti di stage e produzione.
2. Tutti gli scambi applicativi con INPS dovranno quindi essere conformi alle linee di indirizzo ModI, così come indicato nelle specifiche tecniche di ogni servizio erogato da INPS. Il profilo di interoperabilità, per i casi trattati dal presente documento, è fissato a INPS-MODI-P1.
3. Per l'accesso a tutti i servizi erogati da INPS, indipendentemente dagli ulteriori requisiti richiesti, è sempre necessario che il soggetto fruitore sia censito da INPS, comunicando il certificato utilizzato per l'autenticazione HTTPS prevista dal pattern di sicurezza ModI 'ID\_AUTH\_CHANNEL\_02', seguendo la procedura indicata nella successiva sezione "Censimento del Soggetto Fruitore".
4. Dopo che INPS avrà completato la gestione della richiesta di adesione, l'Ente riceverà i certificati richiesti ad INPS e sarà abilitato alla fruizione dei servizi in accordo alle specifiche tecniche della singola API di proprio interesse.

#### 3.1 Censimento del Soggetto Fruitore

Al momento della richiesta di censimento, l'Ente Fruitore deve indicare a INPS:

- il certificato che identifica il Soggetto nelle comunicazioni HTTPS da utilizzare per instaurare le comunicazioni HTTPS con il gateway INPS, così come previsto dal pattern di sicurezza a livello trasporto 'ModI ID\_AUTH\_CHANNEL\_02'.
- gli IP di provenienza delle comunicazioni da parte del Soggetto

Per quanto riguarda il certificato, sono possibili due opzioni:

- l'Ente invia ad INPS il proprio certificato. In tal caso il certificato dovrà rispondere ai seguenti requisiti:

- per l'ambiente di produzione dovrà essere un certificato valido, rilasciato da una CA pubblica;
  - per l'ambiente di collaudo, potrà essere anche un certificato self-signed generato dall'ente richiedente.
- L'Ente richiede ad INPS la generazione del certificato, utilizzando il modulo **SICCERT-02**, debitamente compilato e firmato dal responsabile dell'ente richiedente, unitamente ad una copia del relativo documento di riconoscimento. In tal caso l'Ente dovrà produrre una **CSR (Certificate Request)** per il certificato richiesto, predisposta secondo le indicazioni dettagliate nella seconda pagina del modello di cui sopra e con chiave 2048 bit. L'Istituto rilascerà un certificato per ogni ambiente di utilizzo (collaudo e produzione).

## 4. Dati tecnici per l'Utilizzo dei Profili di Interoperabilità

In questa sezione vengono riepilogati i dati tecnici scambiati tra Istituto e Ente fruitore e come questi siano correlati ai diversi pattern Modl.

I dati che l'ente deve utilizzare per le proprie configurazioni si dividono in:

- Riferimenti comuni per l'accesso ai servizi Modl erogati da INPS, che rimangono immutati per tutti i servizi a cui si intenda accedere.
- Riferimenti specifici per ciascun servizio che sono quindi indicati nel descrittore eService del singolo servizio.

### 4.1 Riferimenti comuni per l'accesso ai servizi Modl di INPS

| Descrizione                   | Riferimenti  | Note  |
|-------------------------------|--|---|
| <b>IP Erogazione</b>          | Collaudo: 89.97.59.151<br>(api.collaudo.inps.it)   | L'IP sul quale sono attestati i servizi erogati da INPS. Può essere utilizzato per la configurazione del firewall dell'Ente fruitore. |
|                               | Produzione: 89.97.59.148<br>(api.inps.it)  |   |
| <b>Certificato HTTPS INPS</b> | Collaudo:<br>api.collaudo.inps.it_chain.pem<br>(incluso nello zip allegato inps-modi-auth-certs.zip) | La catena dei certificati utilizzati dai frontend di INPS nelle comunicazioni HTTPS e che quindi dovrà essere accettato dall'Ente.    |
|                               | Produzione:<br>api.inps.it_chain.pem<br>(incluso nello zip allegato inps-modi-auth-certs.zip)        |   |



## 4.2 Riferimenti specifici per l'accesso al singolo servizio INPS/MODI

I seguenti riferimenti variano per ogni servizio e saranno quindi riportati nel descrittore eService dello specifico servizio:

- interfaccia del servizio nei formati previsti da ModI (WSDL 1.1 o OpenAPI 3.0);
- interfaccia del servizio di risposta, se previsto, nei formati previsti da ModI (WSDL 1.1 o OpenAPI 3.0);
- endpoint di erogazione del servizio;
- per ogni operazione/risorsa prevista dall'API sarà indicato il profilo di interoperabilità richiesto. Nel caso siano riferiti profili diversi da "INPS-MODI-P1" fare riferimento al documento completo di documentazione per i fruitori esterni: "Linee Guida per Fruitori Esterni di API ModI".

## 1 Allegato "A": Lo schema XSD di validazione del SOAP header 'Identity'

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:inps="http://inps.it/" targetNamespace="http://inps.it/">
  <xs:element name="Identity">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="UserId" minOccurs="1" maxOccurs="1" type="xsd:string" />
        <xs:element name="CodiceUfficio" minOccurs="1" maxOccurs="1" type="xsd:string" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```