Manuale Operativo

Servizio per la verifica e trasmissione telematica delle pratiche di Comunicazione Unica e di deposito del bilancio

Versione	4.2	Data Versione:	04/02/2026
Descrizione modifiche	Al capitolo 5 è stato chiarito l'utilizzo delle url relative ai servizi soap		
Motivazioni			

Indice

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il presente documento rappresenta il Manuale Operativo del servizio erogato da InfoCamere, per conto del sistema camerale, che consente di verificare e trasmettere telematicamente pratiche di Comunicazione Unica e di Bilancio (Servizio), via Web Service.

L'erogazione delle funzionalità per la presentazione via Web Service delle pratiche di Comunicazione Unica è disciplinata dal DPCM del 6 maggio 2009.

Il documento è rivolto ai produttori di software (Società Richiedente) che intendono integrare il Servizio all'interno delle proprie soluzioni applicative (Software di Compilazione). A tal fine, il documento fornisce le informazioni operative necessarie e descrive nel dettaglio le caratteristiche tecniche del Servizio.

La versione più aggiornata del presente manuale è disponibile in un'apposita sezione del portale www.registroimprese.it.

1.2 Precedenti emissioni

Versione	4.1	Data Versione:	03/02/2026
Descrizione modifiche	Al capitolo 4.4 modificata url dell'ambiente di collaudo		
Motivazioni			

Versione	4	Data Versione:	25/11/2025
Descrizione modifiche	Aggiornato capitolo 5.2 (modificato esempio di messaggio SOAP)		
Motivazioni			

Versione	3	Data Versione:	14 / 07 / 2025
Descrizione modifiche	Aggiornato capitolo 4 (URL degli ambienti e indicazione degli stessi nel flusso di autenticazione)		
Motivazioni			

1.3 Riferimenti

[1] OAuth 2.0: https://openid.net/specs/openid-igov-oauth2-1_0-02.html
[2] PKCE: https://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.3.1.7
[3] Allegato A - Controlli:
https://www.registroimprese.it/documents/20195/0/ALLEGATO_A-Servizio_per_il_controllo_e_la_trasmissione_delle_pratiche_di_Comunicazione_Unica_e_Bilancio/

[4] Specifiche ComUnica: https://www.registroimprese.it/web/guest/specifiche-tecniche

1.4 Termini e definizioni

Di seguito i termini specifici di questo documento:

Termine	Descrizione
Access Token	Chiave, prevista dal protocollo Oauth 2.0 con espansione PKCE, necessaria per l'accesso in modo sicuro a risorse protette del Servizio
Authorization Code	Chiave, prevista dal protocollo Oauth 2.0 con espansione PKCE, necessaria per ottenere l'Access Token
AgID	Agenzia per l'Italia Digitale
CIE	Carta d'Identità Elettronica
CNS	Carta Nazionale dei Servizi
Società Richiedente	Soggetto che richiede di aderire al Servizio per integrarlo in soluzioni software per la compilazione di pratiche di Comunicazione Unica e di Bilancio
IAM	Identity and Access Management, servizio di autenticazione di InfoCamere
InfoCamere	InfoCamere S.C.p.A., soggetto erogatore del Servizio, per conto del sistema camerale
Messaggio SOAP di accettazione	È il messaggio di risposta a fronte dell'invio di un messaggio di fruizione del servizio. Il messaggio di accettazione contiene l'identificativo per verificare l'esito dell'elaborazione del servizio.
Messaggio SOAP di elaborazione	È il messaggio di risposta a fronte dell'invio di un messaggio di richiesta di esito del servizio.
Messaggio SOAP di fruizione	È il messaggio con attachments inviato che contiene le credenziali di accesso, il nome del servizio, i parametri di input per invocare il servizio.
Messaggio SOAP di richiesta esito	È il messaggio che contiene l'identificativo presente nel messaggio di accettazione per verificare l'esito dell'elaborazione del servizio.
MIME	Multi-purpose Internet Mail Extension
mTLS	mutual TLS (Transport Layer Security), metodo per l'autenticazione che garantisce che le parti a ciascuna estremità di una connessione di rete siano chi affermano di essere
MTOM	Message Transmission Optimization Mechanism per Web Service SOAP
OAuth 2.0	Protocollo standard che consente alle applicazioni di accedere alle risorse protette di un servizio per conto dell'Utente Telemaco.
PKCE	Proof Key for Code Exchange (RFC7636), estensione del protocollo OAuth 2.0.
SCIA	Segnalazione certificata di inizio attività
Servizio	Software che tramite integrazione applicativa permette la verifica e la trasmissione di pratiche di Comunicazione Unica e di Bilancio
SOAP	Simple Object Access Protocol, protocollo per lo scambio di informazioni in ambiente distribuito e decentralizzato, basato su tecnologie XML

Termine	Descrizione
Software di Compilazione	Applicativo della Società Richiedente per la compilazione di pratiche di Comunicazione Unica e/o di Bilancio
SPID	Sistema Pubblico di Identità Digitale
SSO	Single Sign-On
Token Autorizzativo Telemaco	Chiave che permette l'accesso al Servizio da parte dell'Utente Telemaco. Modalità alternativa a SPID, CIE, CNS e credenziali Telemaco che può essere gestita dall'Utente Telemaco in un'apposita sezione autenticata del portale www.registroimprese.it
Utente Telemaco	Soggetto registrato al servizio Telemaco per l'accesso alle Banche Dati delle Camere di Commercio e alla trasmissione di pratiche telematiche secondo le modalità indicate nel portale www.registroimprese.it e utilizza un Software di Compilazione.
Web Service	Software che permette l'interoperabilità tra sistemi in un contesto distribuito.
WSDL	Web Services Description Language, tecnologia XML per descrivere in modo standardizzato l'interfaccia di un Web Service SOAP.
XML	eXtensible Markup Language
XML schema	Descrittore che consente di specificare la struttura ed i vincoli dei documenti XML, rendendo possibile la descrizione della grammatica dei documenti XML.

2 Oggetto del Servizio

Il Servizio è un applicativo che la Società Richiedente può integrare all'interno di un Software di Compilazione e permette agli Utenti Telemaco di verificare e trasmettere telematicamente pratiche di Comunicazione Unica e di Bilancio, direttamente dal Software di Compilazione.

Il Servizio è composta da:

- una componente per l'**Autenticazione dell'Utente Telemaco (IAM),** che comprende sia delle funzionalità web destinate all'Utente Telemaco per l'autenticazione, che delle funzionalità che permettono alla Società Richiedente, al termine del processo di autenticazione dell'Utente Telemaco, di ottenere l'Access token da utilizzare nelle chiamate alle altre componenti autenticate del Servizio.
- dalle seguenti componenti autenticate:
    - **Verifica preliminare pratica**: permette di effettuare controlli sulle pratiche di Comunicazione Unica e di Bilancio, prima della loro trasmissione. La componente funziona in modalità asincrona e ritorna l'identificativo della richiesta;
    - **Trasmissione pratica**: permette la trasmissione di pratiche di Comunicazione Unica e di Bilancio. La componente funziona in modalità asincrona e ritorna l'identificativo della richiesta;
    - **Verifica esito richiesta**: permette di verificare l'esito dell'elaborazione di una richiesta alla componente "*Verifica preliminare pratica*" o "*Trasmissione pratica*".

Il Servizio è esposto in rete internet tramite protocolli sicuri e richiede:

- L'adesione al Servizio da parte della Società Richiedente, secondo le modalità specificate nel capitolo 3;
- La registrazione dell'Utente Telemaco al servizio Telemaco per l'accesso alle Banche Dati delle Camere di Commercio e alla trasmissione di pratiche telematiche, secondo le modalità indicate nel portale www.registroimprese.it.

3 Adesione al Servizio

La Società Richiedente che intende integrare il Servizio nel proprio Software di Compilazione deve seguire la seguente procedura di adesione:

1. Compilare il modulo di richiesta di adesione disponibile nell'apposita pagina web informativa all'interno del sito www.registroimprese.it. La richiesta comprende, oltre ai dati anagrafici della Società Richiedente, anche l'URL di reindirizzamento *"redirect uri"* necessario nel processo di autenticazione.
2. Sottoscrivere digitalmente il modulo e trasmetterlo ad InfoCamere, inviandolo via PEC all'indirizzo: api_pratiche_ri@pec.infocamere.it.

Con l'adesione al Servizio, la Società Richiedente si impegna:

- a comunicare ad InfoCamere qualunque variazione dei dati anagrafici forniti, entro 15 giorni dalla data in cui questi sono variati;
- a comunicare ad InfoCamere eventuali variazioni al "redirect_uri", che verranno recepite da InfoCamere entro 15 giorni;
- a non cedere a terzi i parametri di connessione ai sistemi di autenticazione InfoCamere

Una volta verificata la correttezza della documentazione trasmessa e approvata la richiesta di adesione, InfoCamere invierà all'indirizzo PEC utilizzato dalla Società Richiedente per inoltrare la richiesta i seguenti parametri da utilizzare nel flusso di autenticazione:

- *scope*: identificativo del Servizio al quale la Società Richiedente ha aderito;
- *client_id* e *client_secret:* credenziali di accesso associate alla Società Richiedente. Verranno fornite più coppie *client_id* e *client_secret,* una coppia per ciascun ambiente e pagina di autenticazione.

L'adesione al Servizio non comporta costi per la Società Richiedente. La trasmissione di un pratica telematica di Comunicazione Unica o di Bilancio prevede oneri in carico all'Utente Telemaco (es. diritti di segreteria), stabiliti dalla normativa vigente. La Società Richiedente deve autonomamente provvedere a dotarsi di idonee infrastrutture tecnologiche (hardware e software) e dei collegamenti informatici necessari per poter usufruire del Servizio e delle relative funzionalità tramite la rete internet.

3.1 Requisiti tecnici per la Società Richiedente

Con l'adesione al Servizio, la Società Richiedente si impegna a rispettare i seguenti requisiti tecnici:

- ad utilizzare, in caso di "redirect_uri", un indirizzo HTTPS che rispetti le raccomandazioni di sicurezza di AgID, ad esempio rispettando le indicazioni in tema di TLS e Cipher Suite o un custom scheme (come ad esempio myapp://auth)

InfoCamere si riserva la facoltà di disattivare il Servizio qualora la società richiedente:

- non rispetti i requisiti tecnici sopra elencati;

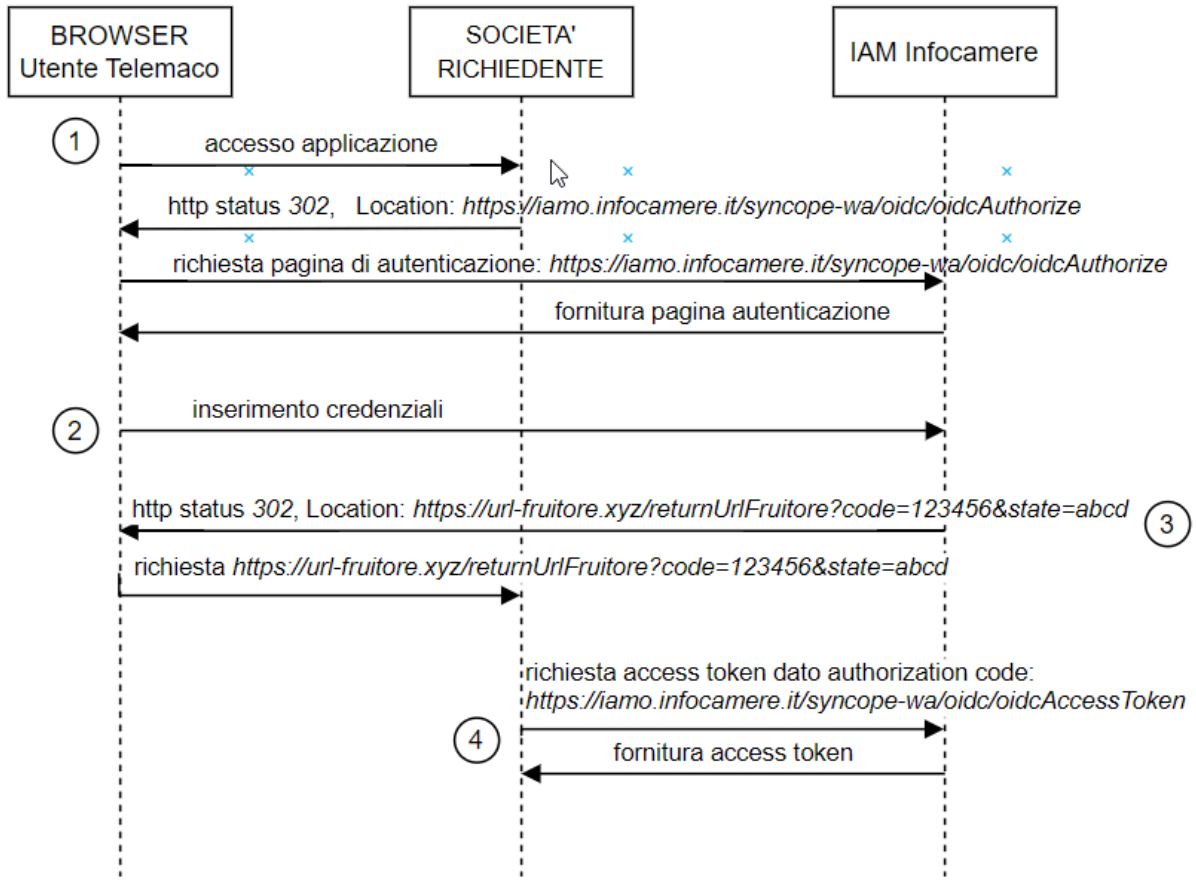
- non utilizzi il Servizio per un periodo di oltre 12 mesi.

4 Autenticazione del Servizio

Le componenti del Servizio prevedono la preventiva autenticazione dell'Utente Telemaco che intende utilizzarle. La Società Richiedente deve perciò integrare nel Software di Compilazione il flusso di autenticazione previsto dal Servizio, basato sul protocollo OAuth 2.0 con estensione PKCE.

Il funzionamento e le diverse fasi previste nell'autenticazione tramite OAuth 2.0 con estensione PKCE può essere approfondito nella documentazione tecnica dello standard utilizzato, disponibile, ad esempio, ai link [1] e [2] indicati nella sezione Riferimenti del presente documento.

Semplificando, il flusso di autenticazione prevede le seguenti fasi:



1. La Società Richiedente reindirizza l'Utente Telemaco alla pagina web di autenticazione dell'IAM di InfoCamere;

2. L'Utente Telemaco si autentica sull'IAM Infocamere utilizzando una delle due pagine di autenticazione messe a disposizione, in base alla configurazione prevista per lo specifico Utente Telemaco.
3. L'Utente Telemaco viene reindirizzato dall'IAM Infocamere alla "*redirect uri*" della Società Richiedente. Con la redirect viene passato alla Società Richiedente l'authorization code e il parametro "status". Il parametro "status" è un parametro utile per la sicurezza (protezione CSRF) e la gestione del contesto applicativo nel flusso di autorizzazione, garantendo che le risposte del server di autorizzazione siano legate in modo sicuro e corretto alla richiesta originale dell'applicazione client;
4. La Società Richiedente richiama l'IAM Infocamere inviando parametri tra cui l'authorization code e ottiene in risposta l'access token

L'access token potrà essere utilizzato, durante la sessione di lavoro dell'Utente Telemaco, per l'autenticazione nelle chiamate alle componenti autenticate del Servizio.
Le URL delle pagine web dell'IAM InfoCamere sono:

- Ambiente di collaudo

```
URL IAM Infocamere per l'apertura della maschera di
autenticazione:
https://iamocl.infocamere.it/syncope-wa/oidc/oidcAuthorize

URL IAM per l'ottenimento dell'access token:
https://iamocl.infocamere.it/syncope-wa/oidc/oidcAccessToken
```

- Ambiente di produzione:

```
URL IAM Infocamere per l'apertura della maschera di
autenticazione:
https://iamo.infocamere.it/syncope-wa/oidc/oidcAuthorize

URL IAM per l'ottenimento dell'access token:
https://iamo.infocamere.it/syncope-wa/oidc/oidcAccessToken
```

4.1 Autenticazione dell'Utente Telemaco

Per ogni ambiente, l'IAM prevede 2 differenti pagine di autenticazione, a seconda della modalità configurata per l'autenticazione dell'Utente Telemaco:

- Una pagina per gli Utenti Telemaco configurati per l'autenticazione tramite SPID, CIE, CNS e credenziali Telemaco. L'autenticazione con questa pagina genera anche una sessione di lavoro autenticata che consente l'accesso alle applicazioni web InfoCamere tramite Single Sign-On.

- Una pagina per gli Utenti Telemaco configurati per l'autenticazione tramite user e Token autorizzativo Telemaco (soluzione legacy). L'autenticazione con questa pagina non consente l'accesso alle applicazioni web InfoCamere tramite Single Sign-On.

A ciascuna pagina di autenticazione sono associati specifici *client_id* e *client_secret*. Pertanto, la Società Richiedente, impostando opportunamente i parametri della richiesta, potrà reindirizzare l'Utente Telemaco verso la pagina di autenticazione corrispondente alla modalità di accesso configurata per lo specifico Utente Telemaco.

Al momento del reindirizzamento, la Società Richiedente dovrà impostare i seguenti parametri nella richiesta HTTP GET:

- `response_type="code"`
- `client_id`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione, che dipende dalla pagina di autenticazione
- `redirect_uri`=valore che deve corrispondere con quanto indicato dalla Società Richiedente nel modulo di adesione
- `scope`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione
- `code_challenge`=valore impostato dalla Società Richiedente secondo le specifiche PKCE, RFC7636
- `code_challenge_method=` valore impostato dalla Società Richiedente con "S256".
- `state=` valore alfanumerico impostato dalla Società Richiedente

L'Utente Telemaco, una volta autenticato, viene redirezionato dall'IAM verso la "*redirect_uri*" della Società Richiedente. Nel reindirizzamento l'IAM imposta i seguenti parametri GET:

- `code`=AUTHORIZATION_CODE generato dall'IAM Infocamere
- `state`=impostato con il valore fornito dalla Società Richiedente nella chiamata iniziale all'IAM Infocamere

4.2 Ottenimento dell'Access Token da parte della Società Richiedente

Con le informazioni fornite dall'IAM al "redirect_uri", la Società Richiedente è in grado di ottenere l'Access token richiamando l'IAM con metodo HTTP POST e valorizzando:

Header HTTP:

```
Content-Type: application/x-www-form-urlencoded
```

I seguenti parametri:

- `grant_type="authorization_code"`
- `client_id`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione, che dipende dalla pagina di autenticazione
- `client_secret`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione, che dipende dalla pagina di autenticazione
- `code`=AUTHORIZATION_CODE generato dall'IAM e passato alla "redirect_uri" del Società Richiedente
- `redirect_uri`=valore che deve corrispondere con quanto indicato dalla Società Richiedente nel modulo di adesione
- `code_verifier`=valore impostato dalla Società Richiedente e univoco per sessione Utente Telemaco

In risposta, la Società Richiedente riceverà un JSON nel seguente formato (RFC-6749):

```
{
    "access_token": "eyJ[...]CAmxg",
    "id_token": "ey[...]MiJ9.",
    "refresh_token":"RT[...]i3g"
    "token_type": "Bearer",
    "expires_in": 300,
    "scope": "SC-INVIO-PRAT"
}
```

4.3 Uso e validità del token di accesso

L'Access token ottenuto dall'IAM è utilizzabile dalla Società Richiedente per tutte le chiamate dell'Utente Telemaco alle componenti del Servizio, fino alla scadenza indicata nell'Access token stesso.
L'Access token ha una durata di 24h, superato questo limite, è necessario aggiornarlo.

Per utilizzare l'Access token nelle chiamate alle componenti del Servizio è necessario impostare:

L'Header HTTP:

```
Authorization: Bearer XYZ
```

```
Content-type: application/json
```

Dove per *XYZ* si intende il valore dell'Access Token rilasciato dall'IAM alla Società Richiedente.

Nel caso in cui venga utilizzato un token scaduto si otterrà una risposta con codice `HTTP 500`, come previsto dalle specifiche del protocollo SOAP, nel formato "SOAP Fault", ad esempio:

```
<env:Envelope
xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Header/>
   <env:Body>
      <env:Fault>
         <env:Code>
            <env:Value>env:Sender</env:Value>
            <env:Subcode>
               <env:Value
xmlns:integration="http://govway.org/integration/fault">integrat
ion:TokenExpired</env:Value>
            </env:Subcode>
         </env:Code>
         <env:Reason>
            <env:Text xml:lang="en-US">Expired token</env:Text>
         </env:Reason>
         <env:Role>http://govway.org/integration</env:Role>
         <env:Detail>
            <problem xmlns="urn:ietf:rfc:7807">

<type>https://govway.org/handling-errors/401/TokenExpired.html</
type>
               <title>TokenExpired</title>
               <status>401</status>
               <detail>Expired token</detail>

<govway_id>aa6b4618-2043-11f0-bf63-005056b0f163</govway_id>
            </problem>
         </env:Detail>
      </env:Fault>
   </env:Body>
</env:Envelope>
```

4.4 Logout Utente Telemaco

Il Software di Compilazione della Società Richiedente può rendere disponibile all'Utente Telemaco una funzione di logout che invalida la sessione autenticata creata durante il login,

nel caso di autenticazione tramite SPID, CIE, CNS o Credenziali Telemaco. Il logout pertanto disabilita l'accesso alle applicazioni web di InfoCamere tramite il sistema di Single Sign-On.

Il logout avviene reindirizzando l'Utente Telemaco all'URL indicato di seguito:

- per l'ambiente di collaudo:

```
https://logints.infocamere.it/eacologin/logout.action?
    fw=true&
    redirect_uri=https://iamocl.infocamere.it/syncope-wa/logout
```

- per l'ambiente di produzione:

```
https://login.infocamere.it/eacologin/logout.action?
    fw=true&
    redirect_uri=https://iamo.infocamere.it/syncope-wa/logout
```

Si segnala che il logout non invalida l'Access Token, che rimarrà valido fino a scadenza.

4.5 Refresh di un access token

La Società Richiedente può effettuare il refresh dell'Access Token prima della sua scadenza, per estenderne la validità.

Per effettuare il refresh dell'Assess Token è necessario effettuare una chiamata POST all'URL dell'IAM, valorizzando:

Header HTTP:

```
Content-Type: application/x-www-form-urlencoded
```

I seguenti parametri:

- `grant_type="refresh_token"`
- `client_id`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione, che dipende dalla pagina di autenticazione
- `client_secret`=valore fornito da InfoCamere alla Società Richiedente al termine del processo di adesione, che dipende dalla pagina di autenticazione
- `redirect_uri`=valore che deve corrispondere con quanto indicato dalla Società Richiedente nel modulo di adesione

- `refresh_token`=valore ottenuto dall'access token sul quale si vuole effettuare il refresh

In output si otterrà un JSON nel seguente formato:

```
{
    "access_token": "[...]",
    "id_token": "[...]",
    "token_type": "Bearer",
    "expires_in": 300,
    "scope": "SC-INVIO-PRAT"
}
```

5 Componenti autenticate del Servizio

Le componenti autenticate del Servizio, per la verifica preliminare e la trasmissione telematica di una pratica di Comunicazione Unica o di Bilancio al Registro delle Imprese, sono disponibili ai seguenti URL:

- Ambiente di collaudo

```
https://serviziweb.cl.infocamere.it/modi/soap/in/infocamere/comun
      icazione-pratiche-ri/v1
```

- Ambiente di produzione:

```
https://serviziweb.infocamere.it/modi/soap/in/infocamere/comunica
      zione-pratiche-ri/v1
```

Queste componenti del Servizio rispondono a chiamate realizzate secondo lo standard SOAP (l'URL quindi non risponde ad un'interrogazione via browser) e prevedono il seguente descrittore WSDL:

```
<wsdl:definitions
xmlns:tns="https://serviziweb.infocamere.it/modi/soap/in/infocamere/comu
nicazione-pratiche-ri"
     xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
     xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
     xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
     xmlns:xmime="http://www.w3.org/2005/05/xmlmime"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
```

```
      xmlns="http://schemas.xmlsoap.org/wsdl/"

targetNamespace="https://serviziweb.infocamere.it/modi/soap/in/infocamer
e/comunicazione-pratiche-ri">

<wsdl:documentation>WebServices Comunicazione Pratiche
RI</wsdl:documentation>

<!--  DEFINIZIONE DEI TIPI -->
<wsdl:types>
      <xsd:schema xmlns="http://schemas.xmlsoap.org/wsdl/"
            attributeFormDefault="qualified"
            elementFormDefault="qualified"

targetNamespace="https://serviziweb.infocamere.it/modi/soap/in/infocamer
e/comunicazione-pratiche-ri">

            <!--  COMPLEX TYPE -->
            <xsd:complexType name="PraticaRequestType">
                  <xsd:sequence>
                        <xsd:element minOccurs="0" name="praticaSign"
      type="xsd:string" />
                        <xsd:element minOccurs="0" name="presentazione"
            type="xsd:base64Binary"
xmime:expectedContentTypes="application/octet-stream" />
                        <xsd:element minOccurs="0" name="pratica"
            type="xsd:base64Binary"
xmime:expectedContentTypes="application/octet-stream" />
                  </xsd:sequence>
            </xsd:complexType>
            <xsd:complexType name="PraticaResponseType">
                  <xsd:sequence>
                        <xsd:element minOccurs="0" name="esito"
      type="xsd:base64Binary" />
                  </xsd:sequence>
            </xsd:complexType>

            <!--  ELEMENT -->
            <xsd:element name="PraticaRequest"
type="tns:PraticaRequestType" />
            <xsd:element name="ControllaPraticaRequest"
type="tns:PraticaRequestType" />
            <xsd:element name="PraticaResponse"
type="tns:PraticaResponseType" />
            <xsd:element name="PraticaID"        type="xsd:string" />
            <xsd:element name="PraticheRIWsError" type="xsd:string" />
      </xsd:schema>
</wsdl:types>

<!--  DEFINIZIONE DEI MESSAGGI -->
<!--  COMUNE A TUTTI I SERVIZI -->
<!--  INVIO PRATICA -->
<wsdl:message name="inviaPraticaMessageRequest">
      <wsdl:part name="inviaPraticaMessageRequest"
element="tns:PraticaRequest" />
</wsdl:message>
<wsdl:message name="inviaPraticaMessageResponse">
```

```
      <wsdl:part name="inviaPraticaMessageResponse"
element="tns:PraticaID" />
</wsdl:message>
<wsdl:message name="controllaPraticaMessageRequest">
      <wsdl:part name="controllaPraticaMessageRequest"
element="tns:ControllaPraticaRequest" />
</wsdl:message>
<wsdl:message name="controllaPraticaMessageResponse">
      <wsdl:part name="controllaPraticaMessageResponse"
element="tns:PraticaID" />
</wsdl:message>
<wsdl:message name="esitoMessageRequest">
      <wsdl:part name="esitoMessageRequest" element="tns:PraticaID" />
</wsdl:message>
<wsdl:message name="esitoMessageResponse">
      <wsdl:part name="esitoMessageResponse"
element="tns:PraticaResponse" />
</wsdl:message>
<wsdl:message name="praticheRIWsFault">
     <wsdl:part name="praticheRIWsFault" element="tns:PraticheRIWsError"
/>
</wsdl:message>

<!--  DEFINIZIONE PORTE -->
<wsdl:portType name="ComunicazionePraticheModiRIPortType">
      <!--  invio pratica -->
      <wsdl:operation name="inviaPratica">
            <wsdl:input message="tns:inviaPraticaMessageRequest"
name="inputInviaPratica" />
            <wsdl:output message="tns:inviaPraticaMessageResponse"
name="outputInviaPratica" />
            <wsdl:fault message="tns:praticheRIWsFault"
name="faultInviaPratica" />
      </wsdl:operation>
      <!--  controllo correttezza formale pratica -->
      <wsdl:operation name="controllaPratica">
            <wsdl:input message="tns:controllaPraticaMessageRequest"
name="inputControllaPratica" />
            <wsdl:output message="tns:controllaPraticaMessageResponse"
name="outputControllaPratica" />
            <wsdl:fault message="tns:praticheRIWsFault"
name="faultControllaPratica" />
      </wsdl:operation>
      <!--  controllo stato pratica -->
      <wsdl:operation name="getEsito">
            <wsdl:input message="tns:esitoMessageRequest"
name="inputGetEsito" />
            <wsdl:output message="tns:esitoMessageResponse"
name="outputGetEsito" />
            <wsdl:fault message="tns:praticheRIWsFault"
name="faultGetEsito" />
      </wsdl:operation>
</wsdl:portType>

<!--  BINDING -->
<wsdl:binding name="ComunicazionePraticheModiRISOAP12Binding"
type="tns:ComunicazionePraticheModiRIPortType">
```

```
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document" />
    <wsdl:operation name="inviaPratica">
        <soap12:operation soapAction="" style="document" />
        <wsdl:input name="inputInviaPratica">
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output name="outputInviaPratica">
            <soap12:body use="literal" />
        </wsdl:output>
        <wsdl:fault name="faultInviaPratica">
            <soap12:fault name="faultInviaPratica" use="literal"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="controllaPratica">
        <soap12:operation soapAction="" style="document" />
        <wsdl:input name="inputControllaPratica">
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output name="outputControllaPratica">
            <soap12:body use="literal" />
        </wsdl:output>
        <wsdl:fault name="faultControllaPratica">
            <soap12:fault name="faultControllaPratica" use="literal"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="getEsito">
        <soap12:operation soapAction="" style="document" />
        <wsdl:input name="inputGetEsito">
            <soap12:body use="literal" />
        </wsdl:input>
        <wsdl:output name="outputGetEsito">
            <soap12:body use="literal" />
        </wsdl:output>
        <wsdl:fault name="faultGetEsito">
            <soap12:fault name="faultGetEsito" use="literal"/>
        </wsdl:fault>
    </wsdl:operation>
</wsdl:binding>

<!-- SERVICE -->
<wsdl:service name="ComunicazionePraticheModiRI">
    <wsdl:port name="ComunicazionePraticheModiRISOAP12port_http"
binding="tns:ComunicazionePraticheModiRISOAP12Binding">
        <soap12:address
location="https://serviziweb.infocamere.it/modi/soap/in/infocamere/comun
icazione-pratiche-ri" />
    </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

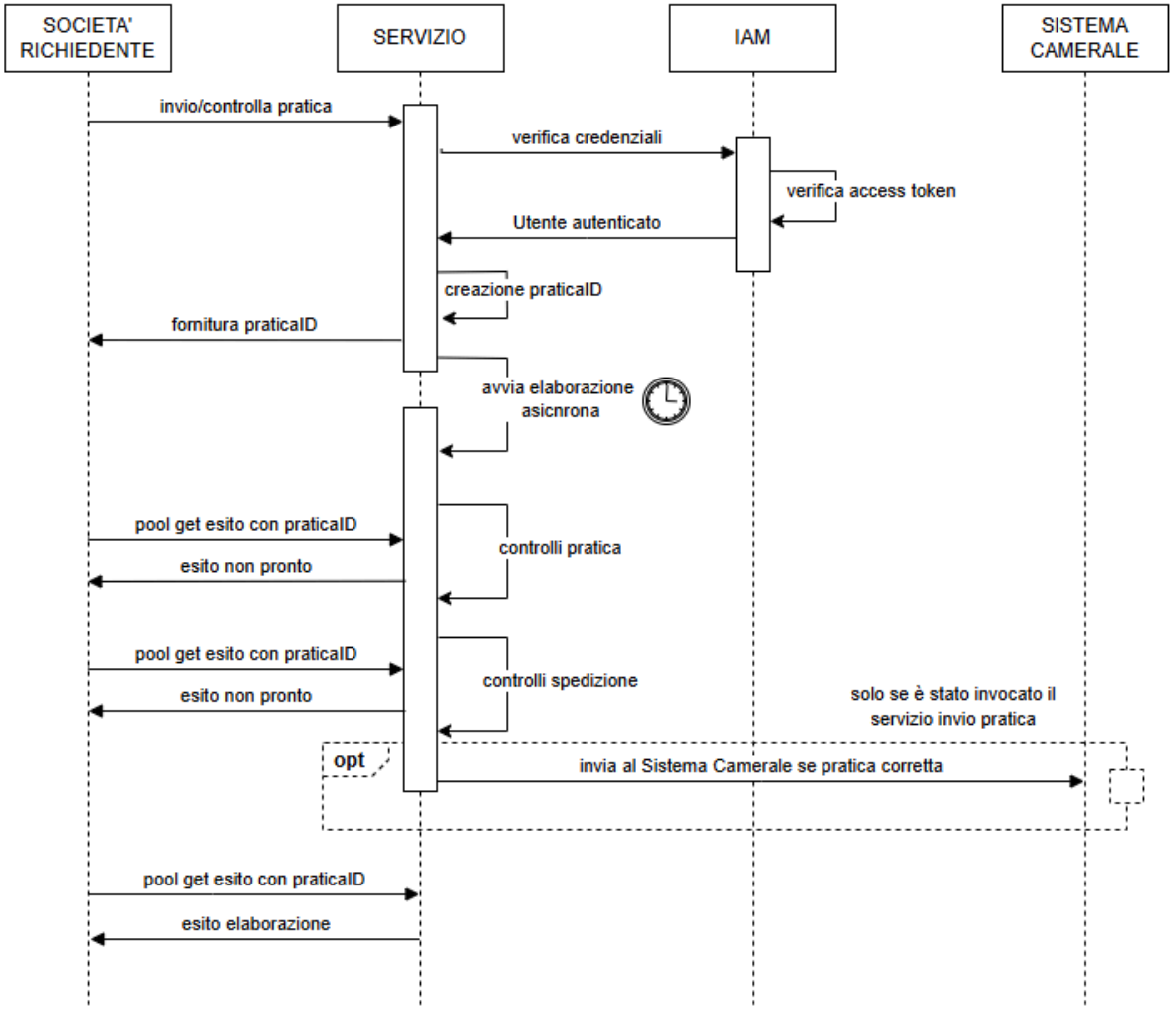
Il servizio prevede le seguenti componenti autenticate:

- **Verifica preliminare pratica**: permette di effettuare controlli sulle pratiche di Comunicazione Unica e di Bilancio, prima della loro trasmissione. La componente funziona in modalità asincrona e ritorna l'identificativo della richiesta (praticaID);
- **Trasmissione pratica**: permette la trasmissione di pratiche di Comunicazione Unica e di Bilancio. Alla trasmissione, la pratica viene verificata eseguendo i controlli previsti anche dalla componente "Verifica preliminare pratica". La componente funziona in modalità asincrona e ritorna l'identificativo della richiesta (praticaID);
- **Verifica esito richiesta**: permette di verificare l'esito dell'elaborazione di una richiesta alla componente "*Verifica preliminare pratica*" o "*Trasmissione pratica*".

La componente "Trasmissione pratica" esegue tutte le verifiche previste anche dalla componente "Verifica preliminare pratica". Quest'ultima pertanto può essere utilizzata quando si desidera controllare la pratica in un momento antecedente alla trasmissione effettiva. Poiché entrambe le componenti effettuano le medesime verifiche, si sconsiglia di utilizzarle in sequenza, per evitare controlli ridondanti. L'elenco dei controlli effettuati è disponibile nell'Allegato A presente al link [3] nella sezione Riferimenti del presente documento.

L'esito delle elaborazioni fornito dalla componente "Verifica esito richiesta" è asincrono, pertanto, è buona prassi richiamare tale componente almeno dopo 5 secondi dalla chiamata alla componente "Verifica preliminare pratica" o "Trasmissione pratica".

Il seguente sequence diagram chiarisce il flusso di chiamate previste:



5.1 Verifica preliminare pratica

La verifica preliminare della pratica può essere effettuata tramite l'interfaccia "**controllaPratica**".
Per invocare tale interfaccia si deve creare un messaggio SOAP che dovrà contenere:

- `<pratica>`: file compresso in formato zip contenente i file che definiscono la pratica. L'elenco dei file che definiscono la pratica è documentato fare riferimento alle specifiche ComUnica al link [4]
- `<presentazione>`: file di accompagnamento, in formato XML, contenente i metadati necessari per la presentazione della pratica. L'XML-SCHEMA di tale file è descritto al paragrafo "XML-SCHEMA presentazione pratica".
- `<praticaSign>`: stringa che rappresenta il digest calcolato con l'algoritmo di hash SHA-256

Esempio di messaggio SOAP:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:ser="https://serviziweb.infocamere.it/modi/soap/in/infocamere/
comunicazione-pratiche-ri">

   <soap:Body>
      <ser:ControllaPraticaRequest>
         <ser:praticaSign>…</ser:praticaSign>
         <ser:presentazione>…</ser:presentazione>
         <ser:pratica>…</ser:pratica>
      </ser:ControllaPraticaRequest>
   </soap:Body>
</soap:Envelope>
```

Se il Servizio riesce a elaborare la richiesta, restituirà un messaggio di accettazione contenente l'identificativo assegnato (praticaID), necessario per verificare successivamente l'esito della richiesta. In caso contrario, verrà restituita un'eccezione con l'indicazione dell'anomalia riscontrata.

5.2 Trasmissione Pratica

La trasmissione di una pratica può essere effettuata tramite l'interfaccia **"inviaPratica"**.

Per invocare tale interfaccia si deve creare un messaggio SOAP che dovrà contenere:

- `<pratica>`: file compresso in formato zip contenente i file che definiscono la pratica (per l'elenco dei file che definiscono la pratica fare riferimento alle specifiche ComUnica al link [4])
- `<presentazione>`: file di accompagnamento, in formato XML, contenente i metadati necessari per la presentazione della pratica. L'XML-SCHEMA di tale file è descritto al paragrafo "XML-SCHEMA presentazione pratica".
- <`praticaSign`>: stringa che rappresenta il digest calcolato con l'algoritmo di hash SHA-256

Esempio di messaggio SOAP:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:ser="https://serviziweb.infocamere.it/modi/soap/in/infocamere/comu
nicazione-pratiche-ri">
   <soap:Body>
      <ser:PraticaRequest>
          <ser:praticaSign> …</ser:praticaSign>
         <ser:presentazione>…</ser:presentazione>
         <ser:pratica>….</ser:pratica>
      </ser:PraticaRequest>
   </soap:Body>
</soap:Envelope>
```

Se il Servizio riesce a elaborare la richiesta, restituirà un messaggio di accettazione contenente l'identificativo assegnato (praticaID), necessario per verificare successivamente l'esito della richiesta. In caso contrario, verrà restituita un'eccezione con l'indicazione dell'anomalia riscontrata.

5.3 Verifica esito richiesta

La verifica dell'esito di una richiesta di "Verifica preliminare pratica" o di "Trasmissione pratica" può essere effettuata tramite l'interfaccia **"getEsito"**.
Per invocare tale interfaccia si deve creare un messaggio SOAP con l'identificativo della richiesta che è stato restituito in precedenza dal Servizio.

Esempio di messaggio SOAP:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:ser="https://serviziweb.infocamere.it/modi/soap/in/infocamere/co
municazione-pratiche-ri">
    <soap:Body>
        <ser:PraticaID>123456</ser:PraticaID>
    </soap:Body>
</soap:Envelope>
```

Il Servizio restituirà un messaggio SOAP il cui contenuto è descritto dall'XML-SCHEMA descritto al paragrafo "XML-SCHEMA esito".

L'esito delle elaborazioni asincrone di "verifica preliminare" o di "trasmissione di una pratica" è da considerare positivo (pratica corretta o pratica corretta ed inviata) se si ottiene una risposta con codice `HTTP 200` il cui messaggio ricevuto contiene l'elemento `<report>` con l'attributo `<returnCode>` di valore 0.

Nel caso in cui la pratica trasmessa non superi i controlli e si ottenga un esito negativo, questa può essere corretta ed inviata nuovamente senza dover creare una nuova pratica (con relativo identificativo).

5.4 XML-SCHEMA

Di seguito gli XML-SCHEMA usati dal Servizio:

5.4.1 XML-SCHEMA presentazione pratica

```
<?xml version="1.0" encoding="utf-8" ?>
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:simpleType name="tipo-protocollazione">
        <xs:restriction base="xs:string">
            <xs:enumeration value="AUTOMATICA"/>
        </xs:restriction>
    </xs:simpleType>
```

```
    <xs:simpleType name="email-address">
           <xs:restriction base="xs:string">
                 <xs:maxLength value="255"/>
                 <xs:pattern value=".*@.*"/>
           </xs:restriction>
     </xs:simpleType>
    <xs:element name="presentazione">
        <xs:complexType>
            <xs:sequence>
                <xs:choice>
                 <!--
                  usare questo elemento per invio nuova pratica da
protocollare
                   -->
                   <xs:element name="protocollazione">
                       <xs:complexType>
                           <xs:sequence>
                               <xs:element name="diritti"
type="xs:decimal"/>
                               <xs:element minOccurs="0"
name="diritto-annuo" type="xs:decimal"/>
                               <xs:element name="diritto-annuo-F24"
type="xs:boolean" minOccurs="0"/>
<!-- l'assenza del tag bollo si traduce nella richiesta del calcolo
automatico dello stesso-->
<!--per le pratiche con modello base TA deve obbligatoriamente essere
indicato il valore del bollo-->
                <xs:element minOccurs="0" name="bollo">
                                    <xs:complexType>
                                        <xs:choice>
                                           <xs:element
name="esente-bollo" type="xs:boolean" minOccurs="0"/>
                                           <xs:element name="importo"
type="xs:decimal" minOccurs="0"/>
                                        </xs:choice>
                                    </xs:complexType>
                               </xs:element>

                               <!--
                               l'uso del parametro "permettiRettifica"
valorizzato a "true"
                               è obbligatorio ed è riferito alla presa
d'atto da parte dell'Utente Telemaco
                               che invia la pratica (da esplicitare in
fase di compilazione),
                               che la camera può effettuare una
rettifica importi durante l'istruttoria
                               -->
                               <xs:element name="permettiRettifica"
type="xs:boolean" minOccurs="0"/>
                               <xs:element name="emailDichiarante"
type="email-address" minOccurs="0"/>
                                    <xs:element
name="presenteAllegatoIntegrazioneXbrl" type="xs:boolean"
minOccurs="0"/>
                           </xs:sequence>
                           <!-- tipo-protocollazione sempre AUTOMATICA
-->
```

```
                            <xs:attribute name="tipo-protocollazione"
type="tipo-protocollazione" use="required"/>
                        </xs:complexType>
                    </xs:element>
                    <!--
                         usare questo elemento per reinviare una pratica
                               in sostituzione della precedente gia'
protocollata
                    -->
                    <xs:element name="reinvio">
                        <xs:complexType>
                             <xs:sequence>
                                 <xs:element name="emailDichiarante"
type="email-address" minOccurs="0"/>
                                      <xs:element
name="presenteAllegatoIntegrazioneXbrl" type="xs:boolean"
minOccurs="0"/>
                             </xs:sequence>
                            <xs:attribute name="numero-protocollo-ri"
type="xs:positiveInteger" use="required"/>
                            <xs:attribute name="anno" type="xs:gYear"
use="required"/>
                        </xs:complexType>
                    </xs:element>
                </xs:choice>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

5.4.2 XML-SCHEMA esito

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="esito">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="report">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="dettaglio" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="nome" type="xs:string">
                    </xs:element>
                    <xs:element name="valore" type="xs:string">
                    </xs:element>
                    <xs:element name="messaggio" type="xs:string">
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute name="servizio" type="xs:string" use="required">
```

```
            </xs:attribute>
            <xs:attribute name="id" type="xs:string" use="required">
            </xs:attribute>
            <xs:attribute name="dt-esecuzione" type="xs:dateTime"
use="required">
            </xs:attribute>
            <xs:attribute name="returnCode" type="xs:integer" use="required">
            </xs:attribute>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="id" type="xs:string" use="required">
      </xs:attribute>
    </xs:complexType>
  </xs:element>
 </xs:schema>
```

6 Allegazione di una SCIA contestuale alla pratica di Comunicazione Unica

A partire dalla data di entrata in vigore del nuovo sistema SSU, prevista dal D.M. 26/09/2023, la trasmissione di una SCIA tramite Comunicazione Unica richiede l'adozione delle nuove regole tecniche.
A tal fine, la Società Richiedente è tenuta ad integrare nelle proprie soluzioni software il "*Servizio di integrazione applicativa Comunicazione Unica con SCIA contestuale* ", realizzato da InfoCamere, che consente il collegamento applicativo con il sistema SSU previsto dall'allegato tecnico al DPR n.160/2010. In particolare, la completa integrazione con i servizi consentirà agli Utenti la corretta allegazione di una pratica SUAP alla pratica di Comunicazione Unica.

Per utilizzare il "*Servizio di integrazione applicativa Comunicazione Unica con SCIA contestuale*" è necessario che la Società Richiedente abbia preventivamente sottoscritto il relativo modulo di adesione. Il modulo e il manuale operativo del servizio sono disponibili nel portale www.registroimprese.it, alla sezione Sportello Pratiche → Comunicazione Unica d'Impresa → Strumenti → Specifiche Tecniche.