L'AGENZIA DELLE ACCISE, DOGANE E MONOPOLI

PROGETTO WEB SERVICES DOGANE

"SERVIZIO ACQUISIZIONE INFORMAZIONI INTEROPERABILITÀ"

DESTINATARI AUTORIZZATI

MANUALE UTENTE

Versione del 03 Gennaio 23

Sommario

1. GENERALITÀ

1.1. CANALI DI COMUNICAZIONE DEI SISTEMI

I web services sono esposti da SOGEI utilizzando gli standard più diffusi (SOAP, REST) e sono fruibili attraverso canali di comunicazione sicuri data la sensibilità dei dati scambiati.

La cooperazione tra ente interessato e SOGEI verrà effettuata attraverso un canale https bilanciato (certificato client e server).

L'autenticazione necessita di un certificato rilasciato agli utenti registrati che ne facciano opportuna richiesta. I meccanismi di autenticazione ed autorizzazione sono descritti in dettaglio nel paragrafo "Modalità di accreditamento".

I messaggi xml dove previsto vengono firmati dal client e trasmessi sfruttando il messaggio SOAP. Gli xml di cui sopra devono essere creati seguendo schemi xsd, rispettandone il contenuto e tutti i vincoli di obbligatorietà e molteplicità. Pertanto durante la fase di ricezione del messaggio, oltre alla verifica della firma che serve a preservarne l'integrità, viene fatta una validazione rispetto allo schema xsd, tesa a controllare formalmente il contenuto del messaggio.

2. SOA DOMINIO ESTERNO

2.1. DESCRIZIONE DELL'OGGETTO DI INTERSCAMBIO

Rispetto alla specificità del servizio erogato sarà rilasciato uno specifico tracciato dati XSD che contiene tutti i campi necessari alla sottomissione delle richieste di elaborazione ed alla gestione dei messaggi di ritorno. I campi utilizzati da un servizio web possono essere di input o di output. I campi di input obbligatori per ciascun servizio sono riprodotti nei documenti allegati nella sezione riguardante il servizio. I restanti campi, cioè quelli del DTO esclusi quelli di input, sono campi di output e in generale, ma non sempre, sono riempiti alla risposta dal servizio web invocato.

2.2. MODALITA' DI ACCREDITAMENTO

Per usufruire dei servizi offerti, l'operatore economico interessato deve:

- dotarsi di **credenziali SPID** (Sistema Pubblico di Identità Digitale) <u>strettamente di livello 2</u> e di Persona Fisica o di una **CNS** (Carta Nazionale dei Servizi) di Persona Fisica o di una **CIE** (Carta d'Identità Elettronica) per l'accesso al portale istituzionale PUDM (Portale Unico delle Dogane e dei Monopoli) dell'Agenzia;
  le tipologie di identità digitali ammesse sono le seguenti:
  - identità digitale della persona fisica
  - identità digitale ad uso professionale della persona fisica
  - identità digitale ad uso professionale per la persona giuridica

- richiedere, tramite la funzione "**Mio Profilo**" del MAU (Modello Autorizzativo Unico), l'autorizzazione connessa all'attività svolta.

Le credenziali SPID di livello 2 permettono l'accesso ai servizi con nome utente e password insieme ad un codice temporaneo che viene inviato all'utente mediante sms o con app mobile.
Per ulteriori informazioni sull'ottenimento delle credenziali SPID, CNS e CIE si rimanda ai rispettivi fornitori del servizio di Identity Management.
Per ottenere l'**autorizzazione** all'utilizzo dei servizi offerti da ADM, l'operatore economico deve effettuare l'accesso all'**Area riservata** del PUDM (www.adm.gov.it), selezionando la tab SPID, CNS o CIE sulla pagina di login proposta. A valle della fase di autenticazione, dovrà quindi accedere alla funzione "**Mio Profilo**", disponibile tra i **Servizi online.**
In tale fase, l'operatore economico dovrà individuare il "**Gestore**", Persona Fisica a cui il soggetto giuridico - che ha titolo ad utilizzare i servizi digitali - conferisce delega per l'attribuzione e la gestione delle autorizzazioni.
Il "Gestore", ricevuta la delega, attribuisce le autorizzazioni ai vari servizi secondo le necessità operative dell'operatore economico.
L'individuazione del Gestore non è necessaria nel caso in cui l'operatore economico sia una ditta individuale e le autorizzazioni siano gestite direttamente dal titolare.
Per Destinatari Autorizzati sono stati definiti sul MAU due appositi profili con le seguenti caratteristiche:

Nome applicazione/servizio	CONCLUSIONE TRANSITO PRESSO DESTINATARI AUTORIZZATI
Codice	dlr_destaut
Categoria	Dogane
Descrizione autorizzazione	Consente di presentare i messaggi per la conclusione delle operazioni di transito presso i Destinatari Autorizzati
Necessita approvazione	NO
Tipologia di utenza	Persone fisiche e persone giuridiche
Livello di Autenticazione	Consistente(SPID/CNS/CIE)
Tipologia di interazione	System To System

Tabella 1 - Caratteristiche del profilo per Destinatari Autorizzati – Conclusione Transito

Nome applicazione/servizio	FIRMA DESTINATARI AUTORIZZATI
Codice	dlr_destaut_firma
Categoria	Dogane
Descrizione autorizzazione	Consente di firmare digitalmente i messaggi inviati dai Destinatari Autorizzati Il dichiarante dovrà delegare il profilo dlr_destaut_firma ad una persona fisica, che sarà così abilitata alla firma digitale dei messaggi.
Necessita approvazione	NO

Tipologia di utenza	Persone fisiche e persone giuridiche
Livello di Autenticazione	Consistente(SPID/CNS/CIE)
Tipologia di interazione	System To System

Tabella 2 - Caratteristiche del profilo per Destinatari Autorizzati – Firma Destinatari Autorizzati

Il dichiarante dovrà delegare il profilo dlr_destaut_firma ad una persona fisica, che sarà così abilitata alla firma digitale dei dati predisposti in formato xml.

Il profilo "dlr_destaut_firma" deve essere delegato ad una persona fisica e, nel caso il delegato non coincida con il legale rappresentante, la delega dovrà essere approvata da un funzionario doganale a seguito di presentazione, da parte dell'operatore, di idonea procura scritta.

Le istruzioni di dettaglio sono disponibili, come di consueto, nell'assistenza *on line* alla voce, "Come fare per" → "Utilizzare gli Altri Servizi e le Altre applicazioni doganali" → "SERVIZI DAL PORTALE ADM > Elenco Servizi" → "**Mio profilo**", dove è possibile reperire ulteriori informazioni riguardanti la figura del "Gestore" e le funzionalità disponibili (attribuzioni di autorizzazioni, deleghe, revoche), nonché alla voce "Come fare per" → "Utilizzare gli Altri Servizi e le Altre applicazioni doganali" → "SERVIZI DAL PORTALE ADM > Elenco Servizi" → "**Registrati**" e "**Gestione Certificati**".
È di riferimento, per le modalità di accesso sopra rappresentate, la nota prot. n. 104198/RU del 14 settembre 2017 - "Nuovo Modello Autorizzativo e modalità per l'accesso ai servizi digitali disponibili sul Portale Nazionale", e seguenti, cui si rimanda per completezza.
Gli operatori economici, oltre che dotarsi delle credenziali SPID, CNS o CIE, dovranno richiedere l'autorizzazione al servizio "Gestione certificati" **dlr_gestione_certificati_aut** (od eventualmente delegarlo), che permette di accedere alla linea di lavoro Area Riservata > Servizi online > Interattivi > Gestione Certificati, ove sono presenti le istruzioni per generare:

- il **Certificato di autenticazione di addestramento**, da utilizzare se l'utente dovrà operare in ambiente di addestramento;
- il **Certificato di autenticazione di produzione**, da utilizzare se l'utente dovrà operare in ambiente reale.

Dal momento in cui l'operatore è già in possesso di un certificato di autenticazione precedentemente rilasciato, è possibile usufruire dei servizi per cui è stato abilitato.
Nell'ambito della sicurezza e delle modalità di accreditamento descritte, l'accesso ai servizi cooperativi si articola in due fasi ben distinte, **autenticazione** e **autorizzazione,** così come già avviene per l'accesso ai servizi web on-line; in particolare:

- autenticazione utente: l'accesso ai Web Services è consentito ai soli utenti in possesso di uno specifico "**Certificato di Autenticazione**" rilasciato dall'Agenzia delle Dogane e dei Monopoli (ADM);

- autorizzazione utente: l'utilizzo dello specifico servizio è sottoposto al preventivo controllo di **autorizzazione** del singolo utente richiedente.

La fase di autenticazione utente inizia con il riconoscimento del Certificato. Superata l'autenticazione il certificato viene sottoposto al controllo tramite l'invocazione di appositi servizi che ne verificano il titolare ed il firmatario. A questo punto scatta la fase di autorizzazione utente, in analogia a quanto previsto per l'autorizzazione all'utilizzo dei servizi web-on-line. Tramite il controllo delle autorizzazioni è possibile stabilire se l'utenza è abilitata ad effettuare l'operazione richiesta.

2.3. MODALITA' DI FIRMA DEI MESSAGGI XML

Per la modalità di firma digitale dei messaggi XML - il DPCM 22 febbraio 2013, articolo 63 comma 3 - Codifica firma XAdES descrive le caratteristiche delle applicazioni di generazione della firma XML. I certificati di firma sono rilasciati dai certificatori accreditati secondo quanto definito nella Deliberazione CNIPA n. 45 del 21 maggio 2009. La deliberazione prescrive (art. 21, comma 16) che "Ai sensi del comma 8, sono altresì riconosciuti il formato di busta crittografica e di firma descritti nei documenti ETSI TS 101 903 – XAdES (versione 1.4.1) e ETSI TS 102 904 (versione 1.1.1).". L'art. 9 della Deliberazione prescrive che "L'elemento KeyInfo, opzionale nella specifica RFC 3275, deve essere sempre presente nella busta crittografica.". La specifica ETSI TS 101 903 prescrive che possa essere usato l'elemento KeyInfo ovvero il SigningCertificate.
Visto quanto disposto al sopra citato art. 21 della deliberazione, considerata l'esigenza di salvaguardare la validità delle firme XML generate con strumenti forniti da certificatori accreditati in altri Stati membri dell'Unione, si chiarisce che, fermo restando il rispetto della citata specifica ETSI, l'assenza dell'elemento KeyInfo non ha come conseguenza l'invalidità della firma XAdES.
Delle tre tipologie di firma XML citate nella deliberazione è necessario che il client di firma generi firme digitali di tipo XAdES-BES enveloped.
Il messaggio xml trasferito come byte[] deve essere firmato con XML Digital Signature e deve inoltre soddisfare i seguenti requisiti tecnici:

- La firma XML è di tipo Enveloped dove l'elemento caratterizzante la firma digitale **ds:Signature** sarà posto come ultimo elemento della radice della struttura XML. Tale documento viene firmato digitalmente tramite l'utilizzo di chiavi e relativo certificato di firma a disposizione dell'operatore.

- uso obbligatorio dell'attributo Id per i tag **<ds:Signature>**, e **<ds:SignatureValue>**

Per il certificato di firma digitale occorre avvalersi di un Prestatore di servizi fiduciari indicato da lista AGID ed europea, presente ai seguenti link

https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-servizi-fiduciari-qualificati

http://tlbrowser.tsl.website/tools/index.jsp

I certificati di firma rilasciati dai Prestatori di servizi fiduciari qualificati devono essere FEQ eIDAS.

Nella sola fase di sperimentazione da effettuare nell'ambiente di addestramento sarà possibile utilizzare un Certificato di Firma, denominato "Certificato di Firma UNICO ADM", generato dalla CA "NON qualificata" dell'Agenzia Dogane e Monopoli, che potrà essere scaricato dall'applicazione Gestione certificati, disponibile nell'Area riservata del Portale ADM.
Nell'ambiente di addestramento sarà sempre possibile utilizzare i certificati di firma FEQ eidas.
Si fa altresì presente che successivamente ad una prima fase di test, l'utente dovrà assolutamente procedere con un test mediante certificato di firma FEQ eidas, ai fini della conformità di integrazione rispetto a quanto offerto in ambiente di esercizio, dove saranno

accettati solo Certificati di firma FEQ eidas.

2.4. Creazione Profilo di firma

Il dichiarante dovrà delegare un profilo di firma ad una persona fisica e questa sarà abilitata a firmare le dichiarazioni.

3. DESTINATARI AUTORIZZATI

I servizi relativi all'invio dei dati per Destinatari Autorizzati, identificati nella fase attuale, sono i seguenti:

- invioNotificaIE007
- invioEsitoIE044

Di seguito per ogni servizio si riporta la descrizione dei dati di interscambio, dell'operazione e dei parametri di input/output.

3.1. ENDPOINT

In ambiente di prova l'endpoint con cui il servizio è esposto è:

- https://interoptest.adm.gov.it/DestinatariAutorizzatiServiceWeb/services/DestinatariAutorizzatiService

In ambiente reale l'endpoint con cui il servizio è esposto:

- https://interop.adm.gov.it/DestinatariAutorizzatiServiceWeb/services/DestinatariAutorizzatiService

3.2. METODO PROCESS

Il metodo *process* permette l'elaborazione dei dati di Destinatari Autorizzati.
Ogni operazione è identificata mediante un *serviceId*.
Per ogni elaborazione effettuata verrà indicata l'operazione che è stata innescata con i relativi dati di input (Richiesta) e di output (Risposta).

Il servizio del tipo EJB - WS, avrà la seguente operazione esposta:

- Risposta *process*(Richiesta input)

ed i seguenti parametri:

Metodo	Input	Output
process	Richiesta	Risposta

Tabella 2 - Descrizione metodo process

I dati in input relativi al tracciato "Richiesta" sono descritti in dettaglio nell'allegato tecnico.

Il tipo di dati in output "Risposta" descritto in dettaglio nell'allegato tecnico, contiene i seguenti elementi:

- *IUT*: identificativo univoco transazione;
- *esito*: contiene il codice e la descrizione del messaggio che indica lo stato di elaborazione della richiesta, più propriamente descritto nel paragrafo 7;
- *data*: in questo elemento sarà presente la risposta codificata in base64Binary (opzionale);
- *data di registrazione:* data in cui il messaggio è pervenuto al sistema di accoglienza.

3.2.1 invioNotificaIE007

Il servizio 'invioNotificaIE007' del tipo EJB - WS, consente di dichiarare le informazioni riguardanti la ricezione della merce da parte del/dei destinatari.

Per invocare il servizio, viene creato un messaggio SOAP di fruizione che deve contenere nel tipo di dati in input "Richiesta" i seguenti campi obbligatori:

- serviceId
- data
  - xmlList
  - dichiarante

Segue la descrizione dei campi:

- *serviceId*: indica il tipo di operazione da eseguire. Necessario per effettuare il dispatching verso i servizi richiesti. Nel caso specifico della suddetta operazione va indicato: "invioNotificaIE007"*;*
- *data*: rappresenta una collezione di oggetti contenenti:
  - *xmlList*: contiene il messaggio xml valido per l'XSD descritto in dettaglio nell'allegato tecnico (CC007C.xsd) firmato digitalmente secondo le indicazioni espresse nel paragrafo 2.3 e codificato in base64Binary;
  - *dichiarante*: l'identificazione dell'utente dichiarante (codice fiscale del soggetto per il quale si sta inviando il messaggio).

Una volta inviato il messaggio, il servizio restituirà in output un oggetto "Risposta" descritto in dettaglio nell'allegato tecnico che contiene i seguenti elementi:

- *IUT*: identificativo univoco transazione;

- *esito*: contiene il codice e la descrizione del messaggio che indica lo stato di elaborazione della richiesta, più propriamente descritto nel paragrafo 7;

- *data:* in questo elemento sarà presente la risposta codificata in base64Binary (opzionale);

- *data di registrazione: data* in cui il messaggio è pervenuto al sistema di accoglienza.

3.2.2 InvioEsitoIE044

Il servizio 'InvioEsitoIE044' del tipo EJB – WS consente a speditore e destinatario, a seguito di indicazione di CRS e numero progressivo, di ricevere nel file di esito i dati validati su Destinatari Autorizzati. In caso di progressivo pari a 1, l'esito contiene anche il documento in formato pdf.

Per invocare il servizio, viene creato un messaggio SOAP di fruizione che deve contenere nel tipo di dati in input "Richiesta" i seguenti campi obbligatori:

- serviceId
- data
  - xmlList
  - dichiarante

Segue la descrizione dei campi:

- *serviceId*: indica il tipo di operazione da eseguire. Necessario per effettuare il dispatching verso i servizi richiesti. Nel caso specifico della suddetta operazione va indicato: "InvioEsitoIE044"*;*

- *data*: rappresenta una collezione di oggetti contenenti:

  - *xmlList*: contiene il messaggio xml valido per l'XSD descritto in dettaglio nell'allegato tecnico (CC044C.xsd) firmato digitalmente secondo le indicazioni espresse nel paragrafo 2.3 e codificato in base64Binary;

  - *dichiarante*: l'identificazione dell'utente dichiarante (codice fiscale del soggetto per il quale si sta inviando il messaggio).

Una volta inviato il messaggio, il servizio restituirà in output un oggetto "Risposta" descritto in dettaglio nell'allegato tecnico che contiene i seguenti elementi:

- *IUT*: identificativo univoco transazione;

- *esito*: contiene il codice e la descrizione del messaggio che indica lo stato di elaborazione della richiesta, più propriamente descritto nel paragrafo 7;
- *data:* in questo elemento sarà presente la risposta codificata in base64Binary (opzionale);
- *data di registrazione: data* in cui il messaggio è pervenuto al sistema di accoglienza.

4. CODICI ERRORE/SEGNALAZIONE

I controlli effettuati dalle procedure di back-end del servizio possono restituire, all'interno dell'elemento *data*:

- un codice di Errore e, opzionalmente, uno o più codici Segnalazione in caso di Codice Esito generale uguale a 198 – "Elaborazione KO: con esito";
- opzionalmente, uno o più codici di Segnalazione in caso di Codice Esito generale uguale a 200 "Elaborazione OK: completata con esito finale".

La descrizione dei codici errore o segnalazione può essere reperita nel file "Destinatari Autorizzati - Tabella Codici Errore - Segnalazione".

5. SERVIZIO INTEROPRSERVICE DI CONTROLLO DELLO STATO

Per favorire l'integrazione di sistema è disponibile un WebService REST che consente, dato uno IUT (identificativo univoco transazione), di controllare lo stato di accoglienza o di elaborazione relativo all'operazione per cui è stato generato quello specifico IUT.

Al paragrafo "8. Allegati tecnici" di questo documento sono riportate le informazioni riguardanti le api Open Api e Swagger, utili a generare i client.

E' possibile generare in modo automatizzato un client in diversi linguaggi di programmazione attraverso i tools messi a disposizione dal sito online per mezzo della documentazione fornita in allegato al servizio e nel paragrafo:

"8.3 Documentazione Open Api del servizio REST InteropRService"

Un esempio di invocazione REST in ambiente di prova è la seguente:

```
Curl Request


        curl -X GET --header 'Accept: application/json'
        'https://interoptest.adm.gov.it/InteropRServiceWeb/servic
        es/InteropRService/selezionaStato/20180426M4000000013'


Request URL
```

```
https://interoptest.adm.gov.it/InteropRServiceWeb/service
s/InteropRService/selezionaStato/20180426M4000000013


Response Body
        20


Response Code
        200



Response Headers
        {
          "x-powered-by": "Servlet/3.0",
          "content-type": "application/json",
          "content-language": "it-IT",
          "transfer-encoding": "chunked",
          "date": "Fri, 07 Jul 2017 10:12:33 GMT"
        }
```

In questo esempio è stato richiesto lo stato per lo IUT: 20180426M4000000013

La risposta in Response Code "200" indica che la chiamata è avvenuta con successo.

La risposta in Response Body "20" indica che lo stato della richiesta per lo IUT indicato ha codice "20", che come descritto nella tabella di decodifica corrisponde alla descrizione: "Input Acquisito a sistema".

Questo esempio di invocazione del servizio può essere valido anche come esempio in ambiente reale, basterà cambiare l'endpoint nella "Request URL" come descritto nel paragrafo successivo.

5.1. ENDPOINT IN AMBIENTE DI PROVA

In ambiente di prova l'endpoint con cui il servizio viene esposto è:

https://interoptest.adm.gov.it/InteropRServiceWeb/services/InteropRService

Installando il certificato di autenticazione nel Browser è possibile consultare la documentazione on line agli indirizzi:

https://interoptest.adm.gov.it/InteropRServiceWeb/services/InteropRService/api/InteropRService.json

https://interoptest.adm.gov.it/InteropRServiceWeb/services/InteropRService/api/InteropRService.yaml

5.2. ENDPOINT IN AMBIENTE REALE

In ambiente reale l'endpoint con cui il servizio viene esposto è:

https://interop.adm.gov.it/InteropRServiceWeb/services/InteropRService

Installando il certificato di autenticazione nel Browser è possibile consultare la documentazione on line agli indirizzi:

https://interop.adm.gov.it/InteropRServiceWeb/services/InteropRService/api/InteropRService.json

https://interop.adm.gov.it/InteropRServiceWeb/services/InteropRService/api/InteropRService.yaml

6. SERVIZIO INTEROPSERVICE - RECUPERO DELL'ESITO

Viene messo a disposizione un Web Service SOAP che permette di recuperare tramite lo IUT l'esito codificato in bytearray nel campo data nell'oggetto di Risposta, qualora sia previsto e prodotto dai servizi descritti nel paragrafo 3.

Il file di esito disponibile al recupero è sigillato elettronicamente (con firma digitale), secondo lo standard XAdES-BES enveloped con riferimento alle regole tecniche definite dalla DELIBERAZIONE N. 45 DEL 21 MAGGIO 2009, secondo il regolamento UE n° 910/2014 – eIDAS.

L'intestatario del certificato di firma usato nelle operazioni è l'Agenzia delle Dogane e dei Monopoli.

Il servizio del tipo EJB - WS, avrà la seguente operazione esposta:

Risposta recuperaEsito (String IUT) con i seguenti parametri:

Metodo	Input	Output
recuperaEsito	IUT	Risposta

Tabella 3 - Descrizione metodo recupera esito

6.1. ENDPOINT

In ambiente di prova l'endpoint con cui il servizio è esposto è:

https://interoptest.adm.gov.it/InteropServiceWEB/services/InteropService

In ambiente reale l'endpoint con cui il servizio è esposto è:

https://interop.adm.gov.it/InteropServiceWEB/services/InteropService

7. CODICI STATO PER IL SERVIZIO DI RECUPERA STATO O ESITO

Codice	Descrizione dello stato o dell'errore
0	Servizio non disponibile
1	La verifica della firma è fallita
2	Il certificato utilizzato per la firma non è valido
3	L'Autorità di certificazione non è ritenuta sicura
4	La verifica dell'integrità del messaggio è fallita
5	Messaggio non firmato
7	CA verifica certificato: fallita
9	Service ID non esistente
10	Verifica xsd: fallita
11	Errore in accodamento richiesta
12	Richiesta non ancora elaborata
13	Condizioni xsd violate
14	Utente non autorizzato
15	Dati di input non validi
16	Certificato autenticazione non valido
18	Firmatario non autorizzato
20	Acquisito a sistema
50	In elaborazione
51	In elaborazione: controllo sostanziale superato
189	Elaborazione OK: completa con esito senza pdf
197	Elaborazione KO: senza esito
198	Elaborazione KO: con esito
199	Elaborazione OK: completata senza esito finale
200	Elaborazione OK: completata con esito finale

Tabella 4 - Codici di stato o di errore dei Web Services

8. ALLEGATI TECNICI

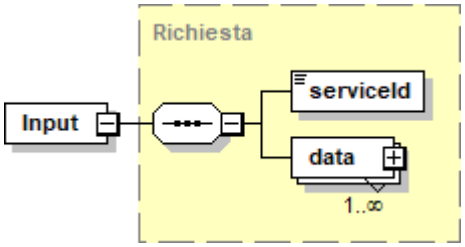
8.1. DOCUMENTAZIONE TRACCIATI DATI DI INPUT

Viene riportata di seguito la struttura dello schema **definitorio.xsd**

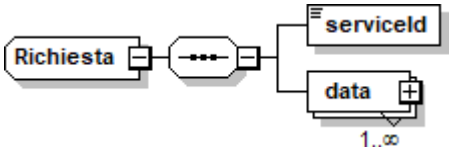
schema location:	definitorio.xsd
attributeFormDefault:	
elementFormDefault:	**qualified**
targetNamespace:	**http://destinatariautorizzatiservice.domest.sogei.it**

Elements	Complex types
Input	**Richiesta**

element **Input**

diagram	
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**
type	**Richiesta**
properties	content complex
children	**serviceId data**
source	`<xs:element name="Input" type="Richiesta"/>`

complexType **Richiesta**

diagram	
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**
children	**serviceId data**
used by	element **Input**

source	`<xs:complexType name="Richiesta">`
	`  <xs:sequence>`
	`  <xs:element name="serviceId">`
	`  <xs:simpleType>`

```
          <xs:restriction base="xs:string">

            <xs:enumeration value="invioNotificaIE007"/>
            <xs:enumeration value="invioEsitoIE044"/>




          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="data" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="xml" type="xs:base64Binary"/>
            <xs:element name="dichiarante">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:pattern value="([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-
Z]{1}[0-9]{3}[A-Z]{1}|[0-9]{11})"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
```

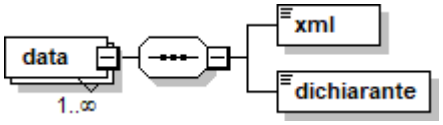
element **Richiesta/serviceId**

diagram	serviceId
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**
type	restriction of **xs:string**
properties	content simple
facets	Kind / Value / Annotation enumeration invioNotificaIE007 enumeration invioEsitoIE044

source	`<xs:element name="serviceId">`
	`  <xs:simpleType>`
	`  <xs:restriction base="xs:string">`
	`<xs:enumeration value="invioNotificaIE007"/>`
	`  <xs:enumeration value="invioEsitoIE044"/>`

```
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

element **Richiesta/data**

diagram	
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**
properties	minOcc 1 maxOcc unbounded content complex
children	**xml dichiarante**

source

```
<xs:element name="data" maxOccurs="unbounded">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="xml" type="xs:base64Binary"/>
      <xs:element name="dichiarante">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:pattern value="([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-
9]{3}[A-Z]{1}|[0-9]{11})"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

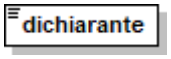
element **Richiesta/data/xml**

diagram	
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**
type	**xs:base64Binary**
properties	content simple

source

```
<xs:element name="xml" type="xs:base64Binary"/>
```

element **Richiesta/data/dichiarante**

diagram	
namespace	**http://destinatariautorizzatiservice.domest.sogei.it**

type	restriction of **xs:string**
properties	content simple
facets	Kind: pattern Value: ([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}|[0-9]{11}) Annotation

source	`<xs:element name="dichiarante">`
	`  <xs:simpleType>`
	`  <xs:restriction base="xs:string">`
	`  <xs:pattern value="([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}|[0-9]{11})"/>`
	`  </xs:restriction>`
	`  </xs:simpleType>`
	`</xs:element>`

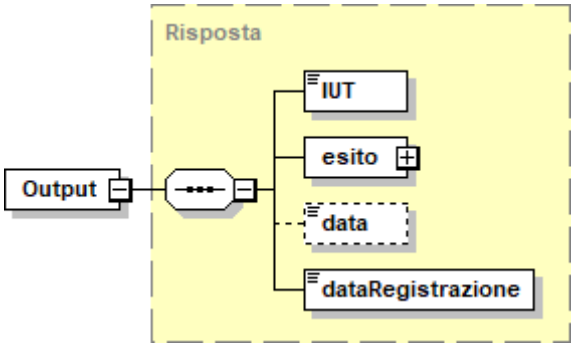
8.2. DOCUMENTAZIONE TRACCIATI DATI DI ESITO

Viene riportata di seguito la struttura dello schema **esitoServizi.xsd**

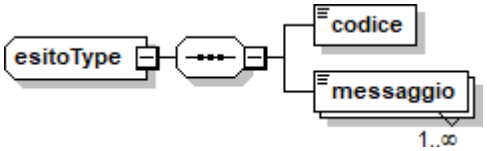
schema location: **esitoServizi.xsd**
attributeFormDefault:
elementFormDefault: **qualified**
targetNamespace: **http://ws.sogei.it/output/**

Elements	Complex types
Output	**esitoType**
	Risposta

element **Output**

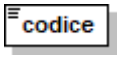
diagram	
namespace	http://ws.sogei.it/output/
type	**Risposta**
properties	content complex
children	**IUT esito data dataRegistrazione**
source	`<xs:element name="Output" type="Risposta"/>`

complexType **esitoType**

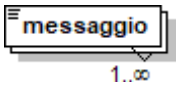
diagram	
namespace	http://ws.sogei.it/output/
children	**codice messaggio**
used by	element **Risposta/esito**

source	`<xs:complexType name="esitoType">`
	`  <xs:sequence>`
	`  <xs:element name="codice" type="xs:string"/>`
	`  <xs:element name="messaggio" type="xs:string" maxOccurs="unbounded"/>`
	`  </xs:sequence>`
	`</xs:complexType>`

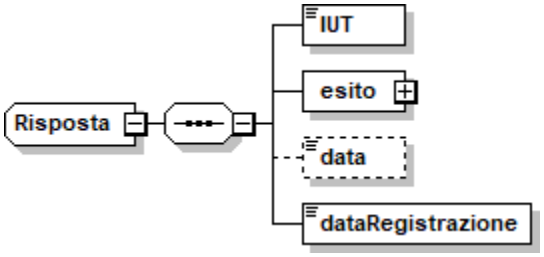
element **esitoType/codice**

diagram	
namespace	http://ws.sogei.it/output/
type	**xs:string**
properties	content simple
source	`<xs:element name="codice" type="xs:string"/>`

element **esitoType/messaggio**

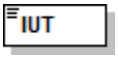
diagram	
namespace	http://ws.sogei.it/output/
type	**xs:string**
properties	minOcc 1 maxOcc unbounded content simple
source	`<xs:element name="messaggio" type="xs:string" maxOccurs="unbounded"/>`

complexType **Risposta**

diagram	
namespace	http://ws.sogei.it/output/
children	**IUT** **esito** **data** **dataRegistrazione**
used by	element **Output**

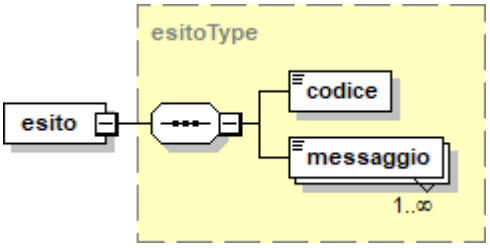
source	`<xs:complexType name="Risposta">`
	`  <xs:sequence>`
	`  <xs:element name="IUT">`
	`  <xs:simpleType>`
	`  <xs:restriction base="xs:string">`
	`  <xs:maxLength value="20"/>`
	`  </xs:restriction>`
	`  </xs:simpleType>`
	`  </xs:element>`
	`  <xs:element name="esito" type="esitoType"/>`
	`  <xs:element name="data" type="xs:base64Binary" minOccurs="0"/>`
	`  <xs:element name="dataRegistrazione" type="xs:date"/>`
	`  </xs:sequence>`
	`</xs:complexType>`

element **Risposta/IUT**

diagram	
namespace	http://ws.sogei.it/output/
type	restriction of **xs:string**
properties	content simple
facets	Kind Value Annotation maxLength 20

source	`<xs:element name="IUT">`
	`  <xs:simpleType>`
	`  <xs:restriction base="xs:string">`
	`  <xs:maxLength value="20"/>`
	`  </xs:restriction>`
	`  </xs:simpleType>`
	`</xs:element>`

element **Risposta/esito**

diagram	
namespace	http://ws.sogei.it/output/
type	**esitoType**
properties	content complex
children	**codice messaggio**
source	`<xs:element name="esito" type="esitoType"/>`

element **Risposta/data**

diagram	
namespace	http://ws.sogei.it/output/
type	**xs:base64Binary**
properties	minOcc 0 maxOcc 1 content simple
source	`<xs:element name="data" type="xs:base64Binary" minOccurs="0"/>`

element **Risposta/dataRegistrazione**

diagram	
namespace	http://ws.sogei.it/output/
type	**xs:date**
properties	content simple
source	`<xs:element name="dataRegistrazione" type="xs:date"/>`

8.3. DOCUMENTAZIONE OPEN API DEL SERVIZIO REST INTEROPRSERVICE

Si riportano di seguito le informazioni utili per la generazione di un client che permetta l'invocazione del Web Service REST per il controllo dello stato.

INFORMAZIONI SULLA VERSIONE

Versione: 1.0.2

SCHEMA URI

BasePath : /InteropRServiceWeb/services

TAGS

InteropRService

OPERAZIONI

selezionaStato

SELEZIONA STATO

- Method: GET
- Endpoint (prova): https://interoptest.adm.gov.it
- Endpoint (reale): https://interop.adm.gov.it
- Resource: /InteropRServiceWeb/services/InteropRService/selezionaStato/{iut}

Descrizione

Il servizio restituisce lo stato di accoglienza o di elaborazione relativo all'operazione per cui è stato generato uno specifico IUT.

Parametri

Tipo	Nome	Descrizione	Schema
Path	**iut** Obbligatorio	IUT di cui si vuole recuperare lo stato	string

Tabella 5 - Parametri chiamata REST

Risposte

Codice HTTP	Descrizione	Schema
200	Il codice indicante lo stato	Nessun commento
403	Accesso negato	Nessun commento

Codice HTTP	Descrizione	Schema
404	Nessuno stato trovato relativo al codice IUT in input	Nessun commento
406	Dati input errati	Nessun commento
500	Errore interno	Nessun commento

Tabella 6 - Codici HTTP di risposta alla chiamata REST

- **Esempio di richiesta http**

https://interoptest.adm.gov.it/InteropRServiceWeb/services/InteropRService/selezionaStato/20180426M4000000013