



PROGETTO WEB SERVICES DOGANE

“SERVIZIO ACQUISIZIONE INFORMAZIONI INTEROPERABILITÀ”

DOGANE IMPORT

Ambiente di Addestramento

Manuale operativo - versione del 3 agosto 2022

Sommario

1. GENERALITÀ	3
1.1. Canali di comunicazione dei sistemi	3
2. SOA DOMINIO ESTERNO.....	4
2.1. Descrizione dell'oggetto di interscambio	4
2.2. Modalità di accreditamento	4
2.3. Modalità Di Firma Dei Messaggi XML	7
3. IL SERVIZIO IMPORT	8
3.1. Endpoint	8
3.2. Metodo Process.....	8
3.2.1. Dati di Input	9
3.2.2. Dati di Output	9
3.3. Tipologie di dichiarazioni d'importazione accolte.....	10
3.3.1. Modalità di invio	10
3.3.2. Acquisizione di una dichiarazione	11
3.3.3. Rettifica di una dichiarazione.....	12
3.3.4. Annullamento di una dichiarazione	13
3.3.5. Notifica di svincolo	14
3.4. Ricevute	15
3.4.1. Ricevuta di I livello	15
3.4.2. Ricevuta di II livello	16
4. CODICI ERRORE/SEGNALAZIONE.....	16
5. SERVIZIO INTEROPRSERVICE - CONTROLLO DELLO STATO	16
5.1. Endpoint in Ambiente di Prova.....	18
6. SERVIZIO INTEROPSERVICE - RECUPERO DELL'ESITO.....	18
6.1. Endpoint	19
7. CODICI STATO PER I SERVIZI.....	19
8. ALLEGATI TECNICI.....	20
8.1. Documentazione Tracciati Dati di Input.....	20
8.2. Documentazione Tracciati Dati di Esito.....	23
8.3. Documentazione Open Api del Servizio Rest InteropRService	28

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 avviene attraverso un canale https bilanciato (certificato client e server).

L'autenticazione necessita di un certificato (cosiddetto Certificato di autenticazione – CA Dogane) rilasciato agli utenti che ne facciano opportuna richiesta. I meccanismi di autenticazione e autorizzazione sono descritti in dettaglio nel paragrafo “Modalità di accreditamento”.

I messaggi XML, ove 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 è 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. Modalità di accreditamento

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

- dotarsi di credenziali SPID (Sistema Pubblico di Identità Digitale) strettamente di livello 2 e di Persona Fisica (anche ad uso professionale) 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.
- 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 e CNS 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 o CNS 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 le **dichiarazioni d'importazione** è stato definito sul MAU un apposito profilo con le seguenti caratteristiche:

Nome applicazione/servizio	Servizio Presentazione Dichiarazioni Doganali di Importazione
Codice	dlr_dichimport
Categoria	Dogane
Descrizione autorizzazione	Consente l'invio delle Dichiarazioni doganali e di consultare gli esiti elaborativi
Necessita approvazione	NO
Tipologia di utenza	Persone fisiche e persone giuridiche
Livello di Autenticazione	Consistente(SPID/CNS)
Tipologia di interazione	System To System, User To System

Tabella 1 - Caratteristiche del profilo per le Dichiarazioni d'Importazione definito sul MAU

Nome applicazione/servizio	Servizio Presentazione Dichiarazioni Doganali di Importazione
Codice	dlr_dichimport_firma
Categoria	Dogane
Descrizione autorizzazione	Consente di firmare digitalmente le Dichiarazioni doganali
Necessita approvazione	NO
Tipologia di utenza	Persone fisiche e persone giuridiche
Livello di Autenticazione	Consistente(SPID/CNS)
Tipologia di interazione	System To System

Tabella 2 - Caratteristiche del profilo di firma per le Dichiarazioni di Importazione definito sul MAU

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

Le istruzioni di dettaglio sono disponibili, come di consueto, nell'assistenza online alla voce, "Come fare per" → "Utilizzare le Altre applicazioni doganali" → "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 "Altri servizi" → "Nuovo modello autorizzativo: Gestione autorizzazioni".

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 o CNS, dovranno richiedere l'autorizzazione al servizio "Gestione certificati" (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:

1. 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);
2. 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. Modalità 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/prestatoriservizi-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. IL SERVIZIO IMPORT

Le operazioni relative all'accoglienza delle dichiarazioni d'importazione sono le seguenti:

- invioDichiarazione;
- rettificaDichiarazione;
- annullaDichiarazione;

Di seguito sono descritti i dati di interscambio ed i parametri di input/output per ogni operazione elencata.

3.1. Endpoint

In ambiente reale il servizio è esposto con il seguente endpoint:

<https://interoptest.adm.gov.it/ImportServiceWeb/services/ImportService>

3.2. Metodo Process

Il metodo process permette l'elaborazione dei dati delle dichiarazioni d'importazione. Ogni operazione è identificata mediante un serviceId.

Per ogni elaborazione da effettuare deve essere indicata l'operazione che si dovrà innescare con i relativi dati di input (Richiesta) e di output (Risposta). Ogni

operazione è identificata mediante un `serviceld`, secondo quanto indicato nella documentazione dei Tracciati Dati di Input (paragrafo 8.1).

3.2.1. Dati di Input

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:

- `serviceld`
- `data`:
 - `xmlList`
 - `dichiarante`

Segue la descrizione dei campi:

- `serviceld`: indica il tipo di operazione da eseguire. Necessario per effettuare il dispatching verso l'operazione richiesta. Viene accettato uno dei valori elencati di seguito: “**invioDichiarazione**”, “**rettificaDichiarazione**”, “**annullaDichiarazione**”;
- `data`: rappresenta una collezione di oggetti contenenti:
 - `xmlList`: contiene il messaggio xml valido per l'XSD associato all'operazione che si vuole richiamare. Tale messaggio deve essere 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).

3.2.2. Dati di Output

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*

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

- *IUT*: identificativo univoco transazione;
- *esito*: con il codice e la descrizione del messaggio che indica lo stato di elaborazione della richiesta, più propriamente descritto nel paragrafo 8.2;
- *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.

3.3. Tipologie di dichiarazioni d'importazione accolte

L'accoglienza di una dichiarazione doganale avviene attraverso l'invio di un file xml generato a partire dalla struttura dati definita nello schema pubblicato sul sito istituzionale di ADM. Le tipologie di dichiarazioni doganali di importazione sono le seguenti:

Tipologie di dichiarazioni	Descrizione delle dichiarazioni
H1	Immissione in libera pratica e regime uso speciale – uso specifico – dichiarazione di uso finale
H2	Regime speciale - custodia – dichiarazione per il deposito doganale
H3	Regime speciale – uso speciale – dichiarazione per l'ammissione temporanea
H4	Regime speciale – trasformazione – dichiarazione per il perfezionamento attivo
H5	Dichiarazione per l'introduzione di merci nell'ambito degli scambi con territori fiscali speciali
H6	Dichiarazioni in dogana nel traffico postale per l'immissione in libera pratica
H7	Dichiarazioni in dogana per spedizioni bassi valori
I1	Dichiarazione semplificata di importazione
I2	Presentazione in dogana delle merci in caso di iscrizione nelle scritture del dichiarante o nel quadro di dichiarazioni in dogana inoltrate prima della presentazione delle merci all'importazione

Tabella 3 - Descrizione delle diverse tipologie di dichiarazioni doganali di importazione

3.3.1. Modalità di invio

La modalità di invio di una dichiarazione, per operazioni di acquisizione e rettifica, è ammessa sia in modalità completa,

<dichCompl>= S

quindi attraverso l'invio di tutti i dati in un'unica soluzione, sia attraverso invii progressivi e parziali,

<dichCompl>= N

che prevedono sempre come unità minima l'**intestazione** ed almeno un **record di articolo**. In quest'ultimo caso il legame tra i diversi invii avviene attraverso il campo della dichiarazione

<TestataHn><RiferimentiMessaggiDocumentiCertificatiAutorizzazioni><LRN>

che deve essere il medesimo in tutti gli invii parziali.

Il LRN (Local Reference Number) è quindi un numero univoco stabilito autonomamente dall'operatore economico che trasmette la dichiarazione (per il formato si rimanda ai tracciati pubblicati sul sito istituzionale di ADM). L'univocità del LRN nell'ambito di un anno solare deve essere garantita dall'operatore economico stesso.

L'indicazione dello stadio dell'invio parziale è regolato dal campo

<UltimoInvio>

che può assumere i seguenti valori:

C = ultimo invio senza dati; N = invio intermedio;

S = ultimo invio con dati.

in modo da permettere di definire un momento di fine nell'accoglimento progressivo dei dati di una singola dichiarazione, identificata dal suo **LRN**. Nell'invio di una dichiarazione in modalità completa il campo <UltimoInvio> deve essere valorizzato a S.

L'invio deve essere ultimato in un intervallo di tempo di 30 giorni. Ad ogni invio corrisponde una ricevuta di I livello (3.3.1) ed una ricevuta di II livello (3.3.2).

Nel caso di invio completo <dichCompl>= S e di <UltimoInvio>= C o S vengono ripetuti tutti i controlli per permettere l'eventuale accettazione della dichiarazione. Nel caso di esito negativo, la dichiarazione non è accettabile e pertanto viene scartata.

3.3.2. Acquisizione di una dichiarazione

L'acquisizione di una dichiarazione avviene attraverso l'invio di un file xml generato a partire dalla struttura dati definita nello schema (dichiarazione.xsd) pubblicato sul sito istituzionale di ADM.

Tale xml deve contenere uno solo dei seguenti elementi:

- DichiarazioneH1;
- DichiarazioneH2;
- DichiarazioneH3;
- DichiarazioneH4;
- DichiarazioneH5;
- DichiarazioneH6;
- DichiarazioneH7;
- DichiarazioneI1;
- DichiarazioneI2.
-

in caso contrario il sistema genera una ricevuta di II livello negativa.

Indipendentemente dalla modalità d'invio scelta (3.2.1), il sistema effettua i controlli sostanziali dei dati dichiarati a valle dei quali notifica all'operatore, attraverso una ricevuta di II livello, il superamento degli stessi o l'elenco di tutti gli errori riscontrati.

Nel caso di `<dichCompl>=N` e di `<UltimoInvio>=N`, ossia di invio intermedio in modalità parziale, la ricevuta positiva di II livello, è una comunicazione di avvenuta acquisizione parziale della dichiarazione, invece, in merito alla ricevuta negativa di II livello, si evidenzia che l'operatore economico, fino all'ultimo invio (`<UltimoInvio>=S o C`), può correggere i flussi parziali che hanno avuto una ricevuta negativa attraverso il rinvio degli stessi, opportunamente modificati.

Nel caso di `<dichCompl>=S` oppure di `<dichCompl>=N` e `<UltimoInvio>=S o C`, invio in modalità completa o invio finale in modalità parziale, la ricevuta positiva di II livello, è la comunicazione di accettazione della dichiarazione con l'indicazione del MRN.

Solo nel caso di `<TipoDichiarazioneSupplementare>=D` (**campo 1/2**), la ricevuta di II livello diviene la comunicazione di avvenuta registrazione della dichiarazione; l'accettazione di questo tipo di dichiarazione avviene al ricevimento del messaggio *DichiarazioneI2 - notifica di arrivo delle merci*.

In merito alla ricevuta negativa di II livello restituita all'accettazione di una dichiarazione, si evidenzia che indica lo scarto completo della stessa.

A seguito della ricevuta di accettazione, per ogni articolo della dichiarazione, il sistema continua il processo di sdoganamento attraverso la valutazione del livello del rischio e tutte le verifiche relative la svincolabilità delle merci. Al termine di tale processo, viene notificato all'operatore, il codice di svincolo o la non svincolabilità per ogni articolo della dichiarazione attraverso una ricevuta di II livello.

3.3.3. Rettifica di una dichiarazione

La rettifica di una dichiarazione avviene attraverso l'invio di un file xml generato a partire dalla struttura dati definita nello schema (dichiarazione.xsd) pubblicato sul sito istituzionale di ADM.

La rettifica e la revisione su istanza dell'Operatore Economico di una dichiarazione sono sottoposte alla valutazione dell'ufficio doganale, che può rigettarle o accettarle.

Ogni flusso di rettifica o di richiesta di modifica di una dichiarazione deve obbligatoriamente avere i seguenti campi valorizzati:

- <Mrn> → MRN della dichiarazione che si vuole rettificare;
- <Causale> → causale per cui si vuole effettuare l'operazione di rettifica;
- <RifNorma> → riferimento normativo a cui si fa riferimento per l'operazione di rettifica.

Se tali campi non sono valorizzati, il sistema invia all'operatore una ricevuta negativa di II livello, ossia il flusso di rettifica viene scartato.

La rettifica di una dichiarazione, oltre a gestire la modifica dei dati precedentemente dichiarati, permette di aggiungere e/o eliminare uno o più articoli. Aggiungere uno o più articoli ad una dichiarazione è possibile attraverso l'invio dell'elemento <Intestazione>, modificato per adeguare i dati derivati dagli n articoli da integrare, e degli n elementi <Articolo> da aggiungere. L'eliminazione di uno o più articoli di una dichiarazione avviene attraverso la valorizzazione del campo:

<NumeroArticoloDaEliminare> → Numero di articolo della dichiarazione che si vuole eliminare

Si evidenzia che il messaggio di rettifica può essere composto o dai soli elementi modificati, aggiunti e/o eliminati oppure dal set di dati completo della dichiarazione, ossia anche da tutti quegli elementi che non sono stati oggetto di alcuna variazione.

A valle della ricezione dell'xml di rettifica il sistema esegue i controlli sostanziali su tutti i campi della dichiarazione, non considerando solo i dati modificati, aggiunti e/o eliminati. A valle dei controlli, come avviene per l'acquisizione, notifica all'operatore il superamento degli stessi o l'elenco di tutti gli errori riscontrati attraverso una ricevuta di II livello.

Si sottolinea che l'operazione di rettifica o di revisione non produce un nuovo identificativo MRN, viene mantenuto quello ante rettifica con un sequenziamento della dichiarazione.

3.3.4. Annullamento di una dichiarazione

L'annullamento di una dichiarazione avviene attraverso l'invio di un file xml generato a partire dalla struttura dati definita nello schema (annullamento.xsd) pubblicato sul sito istituzionale di ADM.

La richiesta di annullamento di una dichiarazione da parte dell'Operatore Economico è sempre sottoposta alla valutazione dell'ufficio doganale, che può rigettarla o accettarla.

Ogni flusso di richiesta di annullamento di una dichiarazione deve obbligatoriamente avere i seguenti campi valorizzati:

- <Mrn> → L'MRN della dichiarazione che si vuole annullare;
- <Causale> → La causale per cui si vuole effettuare l'operazione di annullamento;
- <RifNorma> → Il riferimento normativo a cui si fa riferimento per l'operazione di annullamento.

Se tali campi non sono valorizzati, il sistema invia all'operatore una ricevuta negativa di II livello, quindi il flusso di annullamento è scartato.

A valle della ricezione dell'xml di annullamento il sistema esegue i controlli sostanziali e, infine, notifica all'operatore il superamento degli stessi o l'elenco di tutti gli errori riscontrati, attraverso una ricevuta di II livello.

3.3.5. Notifica di svincolo

Lo svincolo della merce avviene per articolo della dichiarazione, tranne che per i seguenti due casi:

- per le dichiarazioni bassi valori (tracciato H7);
- nel caso in cui l'Operatore Economico manifesti la volontà di ottenere lo svincolo per l'intera dichiarazione attraverso l'utilizzo del documento di carattere nazionale (33YY) dichiarabile a livello di intestazione nel campo <CodiceTipDocIdentificativo> (campo 2/3) del gruppo RiferimentiMessaggiDocumentiCertificatiAutorizzazioni (gruppo 2). La presenza di tale codice documento comporta la gestione del processo di svincolo per dichiarazione e non per articolo.

A valle dell'esito positivo dei controlli di svincolabilità il sistema genera il codice di svincolo e l'eventuale A93 notificandoli all'operatore economico attraverso una ricevuta di II livello.

In particolare, si avranno nel campo informazione dell'elemento data della ricevuta le seguenti valorizzazioni:

- <Codice> → 0 codice identificativo dell'informazione;
- <Descrizione> → descrizione dell'informazione;
- <Numero> → Nel caso di livello=S indica il codice di svincolo. Nel caso di livello=P indica il numero di A93;
- <Data> → Nel caso di livello=S indica la data di svincolo. Nel caso di livello=P indica l'anno dell' A93 e la data di scadenza delle diverse metodologie di pagamento afferenti l'A93;
- <Livello> → S informazione relativa allo svincolo, P informazione relativa al pagamento (A93);

1. <NumeroArticolo> → numero dell'articolo a cui si riferisce l'informazione.
Esempi:Svincolo per intera dichiarazione:

```
<Informazione>
  <Codice>0</Codice>
  <Descrizione>La dichiarazione 21ITQV304AA09972R0 è stata
svincolata con codice di svincolo 8WQMPD in data 05/03/2021</Descrizione>
  <Numero>8WQMPD</Numero>
  <Data>05/03/2021</Data>
  <Livello>S</Livello>
  <NumeroArticolo>0</NumeroArticolo>
</Informazione>
<Informazione>
  <Codice>0</Codice>
  <Descrizione>Per la dichiarazione 21ITQV304AA09972R0 è stato
generato il codice A93 123456</Descrizione>
  <Numero>123456</Numero>
  <Data>2021-23/03/2021E-23/03/2021G</Data>
  <Livello>P</Livello>
  <NumeroArticolo>0</NumeroArticolo>
</Informazione>
```

2. Esito per articolo:

```
<Informazione>
  <Codice>0</Codice>
  <Descrizione>L'articolo n° 1 della dichiarazione
21ITQV304AA09972R0 è stato svincolato con codice di svincolo 8WQMPD in
data 05/03/2021</Descrizione>
  <Numero>8WQMPD</Numero>
  <Data>05/03/2021</Data>
  <Livello>S</Livello>
  <NumeroArticolo>1</NumeroArticolo>
</Informazione>
<Informazione>
  <Codice>0</Codice>
  <Descrizione>Per l'articolo n° 1 della dichiarazione
21ITQV304AA09972R0 è stato generato il codice A93 123456</Descrizione>
  <Numero>123456</Numero>
  <Data>2021-23/03/2021E-23/03/2021G</Data>
  <Livello>P</Livello>
  <NumeroArticolo>1</NumeroArticolo>
</Informazione>
```

3.4. Ricevute

3.4.1. Ricevuta di I livello

Il servizio di accoglienza assegna ad ogni comunicazione dell'Operatore un Identificativo Univoco della Transazione (IUT) e comunica la ricevuta di I livello con i seguenti elementi:

- **IUT**: identificativo univoco transazione;
- **esito**: indica lo stato di elaborazione del messaggio;
- **data**: in questo elemento è presente la risposta codificata in base64Binary (opzionale);
- **data di registrazione** del messaggio XML nel sistema di accoglienza.

3.4.2. Ricevuta di II livello

A valle dell'elaborazione sostanziale del messaggio, viene emessa la ricevuta di II livello, che ha la stessa struttura della precedente ma il cui fulcro sono i dati contenuti nella sezione **data**, in cui sono riportati gli esiti, positivi o negativi, dell'elaborazione.

Il sistema genera una ricevuta di II livello che comprende tutte le segnalazioni di errore riscontrate nel singolo file. Per gli invii parziali, tale esito non è bloccante per la registrazione, ma permette all'operatore di correggere quanto dichiarato. Tale ricevuta è prodotta dal sistema di back-end più volte, a seconda delle fasi operative che la dichiarazione doganale attraversa.

4. CODICI ERRORE/SEGNALAZIONE

I controlli effettuati dalle procedure di back-end del servizio possono restituire, all'interno dell'elemento *data*, uno o più codici di Errore o Segnalazione. In caso di Codice Esito generale uguale a 198 – "Elaborazione KO: con esito" o 200 "Elaborazione OK: completata con esito finale".

La tabella contenente la descrizione dei codici di errore sarà pubblicata sul sito istituzionale dell'Agenzia delle Dogane e dei Monopoli.

5. SERVIZIO INTEROPRSERVICE - CONTROLLO DELLO STATO

Per favorire l'integrazione di sistema è disponibile un Web Service 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.

È possibile generare in modo automatizzato un client in diversi linguaggi di programmazione attraverso i tool 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 è la seguente:

Curl Request

```
curl -X GET --header 'Accept: application/json'  
'https://platform.adm.gov.it/InteropRServiceWeb/services/InteropRService/selezionaStato/20180426M4000000013'
```

Request URL

```
https://platform.adm.gov.it/InteropRServiceWeb/services/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 il servizio viene esposto con il seguente endpoint:

<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>

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

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'ADM.

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 4 - Descrizione del metodo recuperaEsito

6.1. Endpoint

In ambiente di prova il servizio è esposto con il seguente endpoint:

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

7. CODICI STATO PER I SERVIZI

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
20	Acquisito a sistema
50	In elaborazione
51	In elaborazione: controllo sostanziale superato
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 5 - 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://importservice.domest.sogei.it>

Elements Complex types
[Input](#) [Richiesta](#)

element Input


diagram	
namespace	http://importservice.domest.sogei.it
type	Richiesta
properties	content complex
children	serviceld data
source	<code><xs:element name="Input" type="Richiesta"/></code>

complexType Richiesta

diagram	
namespace	http://importservice.domest.sogei.it
children	serviceld data
used by	element Input

source	<pre> <xs:complexType name="Richiesta"> <xs:sequence> <xs:element name="serviceId"> <xs:simpleType> <xs:restriction base="xs:string"> <xs:enumeration value="invioDichiarazione"/> <xs:enumeration value="rettificaDichiarazione"/> <xs:enumeration value="annullaDichiarazione"/> </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> </pre>
--------	--

element Richiesta/serviceId

diagram			
namespace	http://importservice.domest.sogei.it		
type	restriction of xs:string		
properties	content simple		
facets	Kind	Value	Annotation
	enumeration	invioDichiarazione	
	enumeration	rettificaDichiarazione	
	enumeration	annullaDichiarazione	

source	<pre><xs:element name="serviceId"> <xs:simpleType> <xs:restriction base="xs:string"> <xs:enumeration value="invioDichiarazione"/> <xs:enumeration value="rettificaDichiarazione"/> <xs:enumeration value="annullaDichiarazione"/> </xs:restriction> </xs:simpleType> </xs:element></pre>
--------	--


element Richiesta/data

diagram	
namespace	http://importservice.domest.sogei.it
properties	minOcc 1 maxOcc unbounded content complex
children	xml dichiarante
source	<pre><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></pre>

element Richiesta/data/xml

diagram	
namespace	http://importservice.domest.sogei.it
type	xs:base64Binary
properties	content simple
source	<pre><xs:element name="xml" type="xs:base64Binary"/></pre>

element **Richiesta/data/dichiarante**

diagram							
namespace	http://importservice.domest.sogei.it						
type	restriction of xs:string						
properties	content simple						
facets	<table border="1"> <thead> <tr> <th>Kind</th> <th>Value</th> <th>Annotation</th> </tr> </thead> <tbody> <tr> <td>pattern</td> <td>([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}[0-9]{11})</td> <td></td> </tr> </tbody> </table>	Kind	Value	Annotation	pattern	([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}[0-9]{11})	
Kind	Value	Annotation					
pattern	([A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}[0-9]{11})						
source	<pre><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></pre>						

8.2. Documentazione Tracciati Dati di Esito

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

Tale schema è univoco per tutti i servizi citati in questo documento.

schema location: [esitoServizi.xsd](#)
 attributeFormDefault: elementFormDefault:
qualified
 targetNamespace: <http://ws.sogei.it/output/>

Elements
[Output](#)

Complex types
[esitoType](#)
[Risposta](#)

element **Output**

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

complexType esitoType


diagram	
namespace	http://ws.sogei.it/output/
children	codice messaggio
used by	element Risposta/esito
source	<pre> <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> </pre>

element esitoType/codice

diagram	
namespace	http://ws.sogei.it/output/
type	xs:string

properties	content simple
source	<code><xs:element name="codice" type="xs:string"/></code>

element esitoType/messaggio

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

complexType Risposta

diagram	
namespace	http://ws.sogei.it/output/
children	IUT esito data dataRegistrazione
used by	element Output
source	<pre> <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> </pre>

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

element Risposta/esito

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

element Risposta/data

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

element Risposta/dataRegistrazione

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

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>
- 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 6 - Parametri chiamata REST

Risposte

Codice HTTP	Descrizione	Schema
200	Il codice indicante lo stato	Nessun commento
403	Accesso negato	Nessun commento
404	Nessuno stato trovato relativo al codice IUT in input	Nessun commento
406	Dati input errati	Nessun commento
500	Errore interno	Nessun commento

Tabella 7 - Codici HTTP di risposta alla chiamata REST

- **Esempio di richiesta http**

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