ADEL S.r.l. **GEADE Rel 5.0**

NOTA INFORMATIVA

Anno: 2020

Numero: 0003

Data: 11/09/2020

DAS Elettronico

Acquisizione delle credenziali per l'utilizzo del servizio

Con l'avvicinarsi dell'entrata in vigore del DAS Elettronico si invitano le Aziende utenti a dotarsi delle credenziali di accesso ai servizi forniti dall'Agenzia delle Dogane per assolvere all'obbligo.

I servizi disponibili sono **interattivi** (U2S User to System) con l'accesso dell'operatore all'**area riservata** del Portale Unico Agenzia Dogane e Monopoli (PUDM) tramite un browser internet; o di tipo **web service** (S2S System to System) per l'**interoperabilità** della stazione di lavoro con il server dell'Agenzia delle Dogane

Per ciascuna delle modalità di accesso è prevista l'acquisizione di credenziali che permettono agli operatori o alla stazione di lavoro di interagire con l'Agenzia delle Dogane.

L'Azienda utente deve comunque preliminarmente dotare tutti gli operatori che saranno coinvolti nella gestione del DAS Elettronico di una **Carta Nazionale** dei **Servizi** (CNS) abilitata.
Al successivo Capitolo 1 sono indicate le modalità di inserimento nel PUDM del **gestore** e degli **operatori delegati** alla emissione del DAS Elettronico e all'accesso ai **servizi interattivi** collegati.

Per l'utilizzo della modalità **web service** l'Azienda deve acquisire un **Certificato** di **Autenticazione** (CA) rilasciato dall'Agenzia delle Dogane che consenta di attivare l'**interoperabilità** tra la stazione di lavoro (Client) e l'Agenzia delle Dogane (Server).
Al successivo Capitolo 2 sono indicate le modalità di acquisizione, creazione e download, del Certificato di Autenticazione (CA).

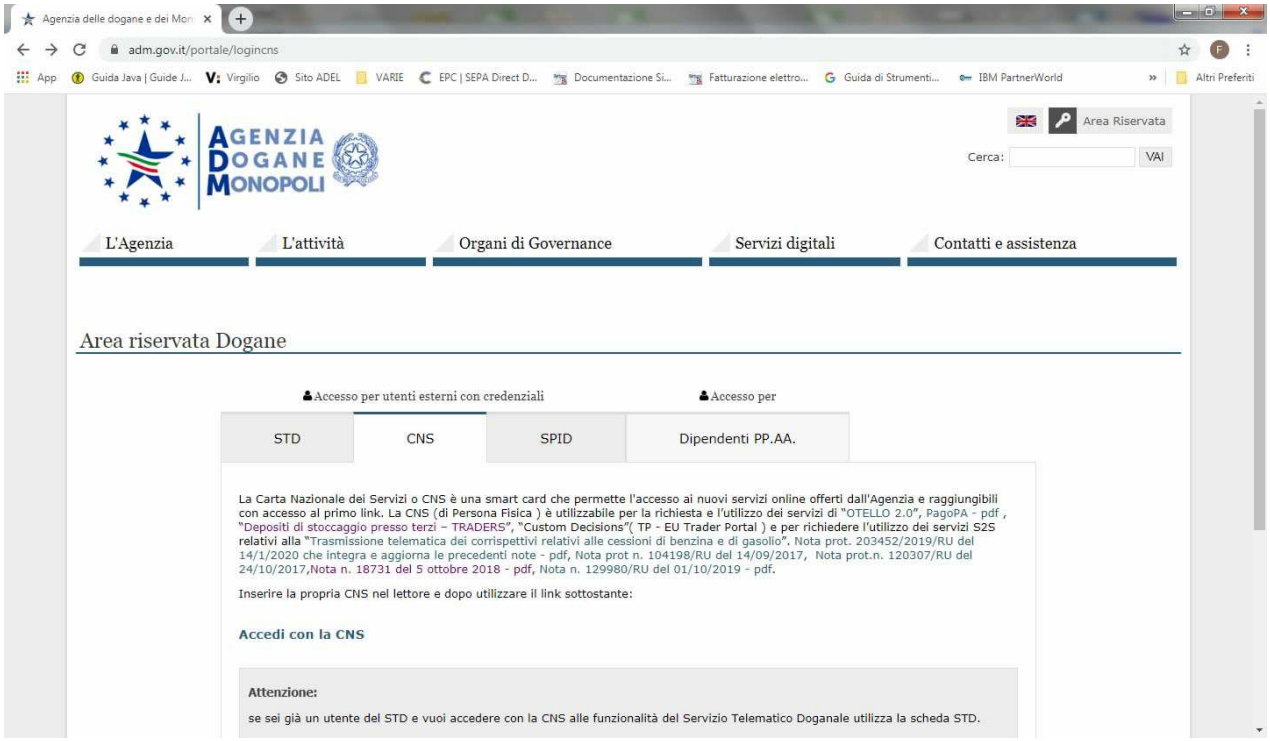
Infine per poter apporre la **firma digitale** ai **messaggi** relativi al DAS Elettronico inviati dalla stazione di lavoro all'Agenzia delle Dogane tutti gli **operatori delegati** devono essere in possesso di un file di firma digitale **XADES-BES** rilasciato da un ente autorizzato.
Al successivo Capitolo 3 sono riportate le regole stabilite dall'Agenzia delle Dogane sulle firme digitali valide.

I file contenenti il **Certificato** di **Autenticazione** (CA) e le **firme digitali** degli operatori delegati dovranno essere installati sulla stazione di lavoro che dovrà anche essere dotata di **lettore smart-card** per l'utilizzo della **Carta Nazionale** dei **Servizi** (CNS).

1 - Servizio interattivo online

Il servizio interattivo online consente ad un operatore, autorizzato dal titolare dell'azienda o dal gestore di visualizzare i DAS Elettronici, eventualmente stamparli, visionare le notifiche dell'Agenzia ed inserire il **Rapporto di Ricezione** dei prodotti (messaggio DE818) e i **Cambi di Destinazione** (messaggio DE813).

L'operatore deve essere in possesso delle credenziali **SPID** o della **CNS** (Carta Nazionale dei Servizi) del legale rappresentante dell'Azienda da utilizzarsi per l'accesso al servizio.



Con le credenziali del legale rappresentante dell'Azienda si accede alla pagina:

- **Servizi Online => Interattivi => Accise => DAS Elettronico**

Una volta entrati è possibile definire il **gestore** e gli **operatori delegati** abilitati ai servizi per conto dell'Azienda titolare del Codice Ditta.

Tutti gli **operatori delegati** all'invio delle richieste di emissione dei DAS Elettronici devono essere in possesso della **Carta Nazionale dei Servizi**.

2 - Web Service di scambio messaggi

Per l'utilizzo del **Web Service** per lo scambio dei messaggi relativi al DAS Elettronico l'Azienda utente deve essere in possesso di un **Certificato di Autenticazione** rilasciato dall'Agenzia delle Dogane.

Le modalità di accreditamento sono descritte nel documento: ***PROGETTO WEB SERVICES DOGANE - "SERVIZIO ACQUISIZIONE INFORMAZIONI INTEROPERABILITÀ" - MOVIMENTAZIONI DAS*** - Versione del 3 luglio 2020.

Il documento è disponibile sul sito dell'Agenzia delle Dogane, ma per facilitare gli utenti nel seguito sono richiamate la parte specifica relativa alle procedure di accreditamento.

2.2. MODALITA' DI ACCREDITAMENTO

Nell'ambito della sicurezza e delle modalità di accreditamento, per usufruire dei servizi è necessario essere in possesso delle credenziali SPID (Sistema Pubblico di Identità Digitale) di livello 2 (permette 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 dedicata) o CNS (Carta Nazione dei Servizi).
Per ulteriori informazioni sull'ottenimento di tali credenziali si rimanda ai rispettivi fornitori del servizio di Identity Management.
Gli utenti in possesso delle suddette credenziali accedono al Portale Unico Dogane per richiedere le autorizzazioni tramite MAU (Modello Autorizzativo Unico), autenticandosi attraverso la pagina di login disponibile nella seguente sezione:

"Area riservata" > "Dogane" > "Accesso per utenti esterni con credenziali" > "SPID".

Nell'ambito della sicurezza e delle modalità di accreditamento, l'accesso ai servizi cooperativi si articola in due fasi ben distinte, **autenticazione** ed **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;
- 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.
Da Portale Unico Dogane in "Area Riservata" > "Dogane" > "Servizi online" > "Interattivi" > "Gestione Certificato" è possibile generare il certificato utile all'autenticazione.

Il Certificato così generato permetterà l'utilizzo del servizio di Web Service e andrà, in forma di file, collocato sulla stazione di lavoro (PC Windows 10 o Windows 7 64-bit) utilizzata per lo scambio telematico dei messaggi DAS Elettronico.

Si presume che i **Certificati di Autenticazione** siano distinti tra **ambiente di addestramento** e **ambiente reale**,, nella procedura di creazione l'utente ricordi che è opportuno generarli e scaricarli entrambi.

3 - Certificato di firma digitale degli operatori

Considerato che i messaggi inviati al Web Service debbono essere **firmati digitalmente**, gli operatori incaricati dell'emissione del DAS Elettronico devono essere dotati di una **firma digitale** rilasciata da un ente autorizzato.
La firma digitale è personale e associata al **Codice Fiscale** dell'operatore, pertanto tutti gli **operatori delegati** all'invio delle richieste di emissione dei DAS Elettronici devono essere in possesso della **firma digitale** da apporre ai messaggi inviati al PUDM.

La tipologia della firma richiesta è dettagliata nel documento in precedenza citato, anche in questo caso di seguito è richiamato il paragrafo che ne descrive le caratteristiche.

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:
(....)
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

Anche i file contenenti la **firma digitale** degli **operatori delegati** devono risiedere sulla stazione di lavoro (PC Windows 10 o Windows 7 64-bit) utilizzata per lo scambio telematico dei messaggi DAS Elettronico.

Si raccomanda alle Aziende utenti di provvedere rapidamente agli adempimenti richiamati e a comunicarlo al Servizio Software in modo che possa essere avviata una fase di addestramento all'utilizzo e test della procedura.

= = = = = = = = =
Fine documento
= = = = = = = = =