



Berna, agosto 2017

Informazione

Passaggio dal certificato GluePKI* al certificato AdminPKI* per la trasmissione in NCTS

* GluePKI e AdminPKI sono infrastrutture che mettono a disposizione i certificati necessari per la comunicazione con i server della dogana

Indice

1	Introduzione	2
1.1	Scadenario (i termini sono stati aggiornati)	2
2	Principali cambiamenti	2
3	Informazioni importanti per l'applicazione	2
3.1	Invio di notifiche	2
3.2	Firma e codificazione	3
3.3	Comunicazione degli indirizzi e-mail	3
3.4	Certificati di server dell'AFD	3
3.5	Istruzioni e manuali	3
4	Passaggio dal certificato GluePKI a quello di AdminPKI e impiego parallelo	5
4.1	Invio di notifiche	5
4.2	Risposte	5
4.3	Certificati GluePKI differenti a seconda dell'ambiente NCTS	5
4.4	Correzioni	6
4.5	Risposte e notifiche dello stato	6

Passaggio al certificato AdminPKI in NCTS

1 Introduzione

In e-dec Importazione ed Esportazione sono già state bloccate le prime trasmissioni di dichiarazioni doganali con numero di spedizioniere/TIN. Il prossimo passo programmato dall'Amministrazione federale delle dogane (AFD) sarà il blocco in NCTS delle prime trasmissioni di dichiarazioni doganali con numero di spedizioniere/TIN. A partire da tale momento la trasmissione di dichiarazioni doganali sarà possibile soltanto con il numero d'identificazione delle imprese (IDI).

In futuro per la comunicazione tecnica in NCTS verrà impiegato il certificato AdminPKI, che sostituisce il certificato GluePKI finora utilizzato. Il presente documento contiene le principali informazioni per il passaggio al certificato AdminPKI in NCTS.

1.1 Scadenario (i termini sono stati aggiornati)

Blocco numero di spedizioniere

A partire dal 1° febbraio 2018, le prime trasmissioni in NCTS potranno essere effettuate esclusivamente con l'IDI. Il sistema respinge le prime trasmissioni con il numero di spedizioniere.

Blocco certificati GluePKI

Il 31 maggio 2018 verranno disattivati tutti i certificati GluePKI, anche quelli con un termine di validità più lungo. Da tale momento non sarà più possibile effettuare correzioni con il numero di spedizioniere.

Anche in NCTS le dichiarazioni doganali devono essere trasmesse con AdminPKI a partire dalla [Gestione dei clienti della dogana](#) (GCD) e dai dati di comunicazione registrati nella GCD. Pertanto il certificato AdminPKI è valido sia per e-dec sia per NCTS.

2 Principali cambiamenti

- In NCTS (analogamente a e-dec) si passa al certificato AdminPKI.
- Il certificato (private key) va richiesto e scaricato nell'ambiente di produzione dell'applicazione GCD, compresi i nuovi certificati (vedi punto 3.5).
- Per l'ambiente test e di produzione (NCTS) rimane ancora un solo certificato utente, proveniente dall'ambiente di produzione GCD. Il numero IDI viene tuttavia registrato a seconda dell'ambiente GCD (produzione, test), nel quale viene archiviato il ruolo di base per il carico nonché i dichiaranti.
- I clienti che utilizzano sia e-dec sia NCTS hanno lo stesso certificato per entrambe le applicazioni per via del ruolo di base per il carico e pertanto, secondo il set di dati di comunicazione, anche gli stessi indirizzi e-mail.

3 Informazioni importanti per l'applicazione

3.1 Invio di notifiche

Dopo la registrazione nella GCD e il passaggio all'IDI, le notifiche NCTS munite di IDI vanno inviate ai seguenti indirizzi server:

NCTS produzione: transit_uid@ncts.ezv.admin.ch

NCTS test: transit_uid@nctstest.ezv.admin.ch

A seconda dell'ambiente, per la codificazione della notifica all'invio e per la verifica della firma alla ricezione occorre scaricare e installare il certificato AdminPKI del server (public key) dal [sito dell'AFD](#).

Passaggio al certificato AdminPKI in NCTS

3.2 Firma e codificazione

Le notifiche con AdminPKI possono essere firmate e codificate oppure firmate e non codificate. Di conseguenza, la firma (per l'identificazione del mittente) è imperativa, mentre la codificazione è auspicata ma non richiesta.

Invio: il dichiarante (spedizioniere) deve firmare la notifica con il proprio certificato (private key) e può codificarla con il certificato di server fornito dall'AFD.

Ricezione: il dichiarante (spedizioniere) deve decodificare la notifica con il proprio certificato e può verificare la firma dell'AFD mediante il certificato di server della dogana.

Risposta da parte di AdminPKI: le notifiche vengono rinviate sempre firmate E codificate.

3.3 Comunicazione degli indirizzi e-mail

Nei dati di comunicazione della GCD vanno registrati gli indirizzi e-mail:

E-mail del certificato: il certificato viene rilasciato per questo indirizzo, di cui viene controllata l'unicità.

E-mail ricezione: la risposta dell'applicazione per le merci viene inviata per e-mail a questo indirizzo dell'ambiente di produzione.

E-mail test ricezione: vedi «E-mail ricezione» (ambiente di produzione), solo per l'ambiente test.

E-mail invio: l'autenticazione del cliente doganale, quando comunica per e-mail con una delle applicazioni per le merci, avviene mediante questo indirizzo e-mail. Ciò significa che il cliente deve imperativamente inviare la sua comunicazione da questo indirizzo e-mail; ambiente di produzione.

E-mail test invio: vedi «E-mail invio» (ambiente di produzione), solo per l'ambiente test.

Ulteriori dettagli sono desumibili dal manuale «6. Dati di comunicazione e certificato» (punti 1.1 e 2: registrazione del set di dati di comunicazione).

3.4 Certificati di server dell'AFD

I certificati di server rimangono validi fino al 9 giugno 2019. La public key del nuovo certificato è disponibile sul [sito dell'AFD](#). I certificati di server dell'ambiente di produzione e di quello di test sono differenti e per ciascun certificato di server viene creata una propria public key.

3.5 Istruzioni e manuali

- Documentazione GCD

[6. Dati di comunicazione e certificati](#) (punti 1.1 e 2: registrazione del set di dati di comunicazione)

Fonte: <https://www.ezv.admin.ch/ezv/it/home/documentazione/pubblicazioni/pubblicazioni-gestione-dei-clienti-della-dogana---idi/manuali.html>

Passaggio al certificato AdminPKI in NCTS

4. Registrare i dati di comunicazione

Fonte: <https://www.ezv.admin.ch/ezv/it/home/dichiarazione-doganale/dichiarazione-da-parte-di-ditte/zollkundenverwaltung-uid/istruzioni-in-breve-gcd-per-nuovi-clienti.html>

- Documentazione tecnica NCTS

Comunicazione (punto 1.5 «Fehlermeldungen» del documento tedesco)

Fonte: <https://www.ezv.admin.ch/ezv/it/home/dichiarazione-doganale/dichiarazione-da-parte-di-ditte/ncts---transito-nazionale/documentazione-ncts---transito-nazionale.html>

Passaggio al certificato AdminPKI in NCTS

4 Passaggio dal certificato GluePKI a quello di AdminPKI e impiego parallelo

4.1 Invio di notifiche

Per il passaggio da numero di spedizioniere/GluePKI a IDI/AdminPKI è previsto un impiego parallelo. Ciò significa che durante una fase transitoria è possibile ricorrere a entrambe le procedure; le notifiche possono essere inviate sia con numero di spedizioniere/GluePKI o IDI/AdminPKI. Da osservare:

Identificazione	Certificato	Indirizzo e-mail
Numero di spedizioniere	Certificato GluePKI	transit@ncts.ezv.admin.ch
IDI	Certificato GluePKI (possibile solo se nel certificato è stato registrato l'IDI)	transit@ncts.ezv.admin.ch
IDI	Certificato AdminPKI	transit_uid@ncts.ezv.admin.ch

Indipendentemente dal certificato, l'invio di notifiche con il numero di spedizioniere all'indirizzo transit_uid@ncts.ezv.admin.ch non è supportato.

4.2 Risposte

Dopo la prima trasmissione in NCTS con il certificato AdminPKI, il flag AdminPKI è impostato nel set di dati di comunicazione della GCD.

Criteri per determinare quale certificato utilizzare per l'invio delle risposte da parte dell'AFD:

- **Risposta contiene un numero IDI**
 - Se il flag AdminPKI è impostato nel set di dati di comunicazione della GCD: l'AFD effettua l'invio dall'indirizzo transit_uid@ezv.admin.ch con il certificato AdminPKI secondo l'IDI, la firma va verificata con il certificato AdminPKI secondo l'IDI.
 - Se il flag AdminPKI non è impostato nel set di dati di comunicazione della GCD: l'AFD effettua l'invio dall'indirizzo transit@ncts.ezv.admin.ch con il certificato GluePKI secondo l'indirizzo e-mail registrato nel set di dati di comunicazione NCTS, la firma va verificata con il certificato GluePKI.
- **Risposta contiene un numero di spedizioniere**
 - l'AFD effettua l'invio dall'indirizzo transit@ncts.ezv.admin.ch con il certificato GluePKI secondo l'indirizzo e-mail registrato nel set di dati di comunicazione NCTS, la firma va verificata con il certificato GluePKI.

4.3 Certificati GluePKI differenti a seconda dell'ambiente NCTS

Il certificato GluePKI è differente a seconda dell'ambiente NCTS. In pratica un certificato GluePKI vale solo per l'ambiente test di NCTS e un altro per l'ambiente di produzione. Pertanto sono determinanti gli indirizzi e-mail transit@nctstest.ezv.admin.ch (private key ambiente test) e transit@ncts.ezv.admin.ch (private key ambiente produzione).

Se il flag AdminPKI è impostato nel set di dati di comunicazione della GCD e le notifiche sono state trasmesse con lo stesso certificato AdminPKI nell'ambiente test e in quello di produ-

Passaggio al certificato AdminPKI in NCTS

zione di NCTS, per il flusso di dati valgono gli indirizzi transit_uid@nctstest.ezv.admin.ch e transit_uid@ncts.ezv.admin.ch.

Prima di utilizzare la prima volta il certificato AdminPKI nell'ambiente di produzione si raccomanda di fare una prova nell'ambiente test.

4.4 Correzioni

Una notifica inviata con numero di spedizioniere e certificato GluePKI (secondo la vecchia procedura) e che necessita in seguito di una correzione deve essere inviata anche per la correzione con il numero di spedizioniere e il certificato GluePKI (anche se è già avvenuto il passaggio a IDI e al certificato AdminPKI [secondo la nuova procedura]).

4.5 Risposte e notifiche dello stato

Di regola le procedure NCTS durano circa un mese (incl. risposte e notifiche dello stato) e in casi rari fino a tre mesi. In via assolutamente eccezionale le notifiche possono rimanere in sospenso per anni.

- ⇒ Il dichiarante (spedizioniere) deve garantire per un certo periodo un impiego parallelo.
- ⇒ Le risposte e le notifiche dello stato con il certificato GluePKI possono essere effettuate anche se il certificato non è più valido. All'invio non viene controllata la validità del certificato GluePKI.
- ⇒ I dichiaranti (spedizionieri) che non ricevono più notifiche munite del certificato GluePKI possono rivolgersi al Centro di servizio TIC. Qui è possibile elaborare le notifiche allo schermo e sostituire il numero di spedizioniere con l'IDI e rinviarle. (Dato che lo spedizioniere ha già effettuato il passaggio al certificato AdminPKI, nel set di dati di comunicazione della GCD è già inserito il flag AdminPKI. Di conseguenza, la notifica dello stato viene inviata con il certificato AdminPKI.)