

# STATO MAGGIORE DELLA DIFESA Comando C4 Difesa

## **Autenticazione CNS**

Configurazione del browser Microsoft Internet Explorer e Mozilla Firefox 33.1.1

## Sommario

Ca	rta Nazionale dei Servizi	3
Premessa		3
		4
1.	<b>€</b> Internet Explorer	4
2.	Firefox	Δ

#### Carta Nazionale dei Servizi

Il Ministero della Difesa nella figura dello Stato Maggiore della Difesa - Comando C4 Difesa - fornisce, attraverso un centro tecnico denominato Centro di Certificazione PKI Difesa, il servizio di certificazione a chiavi pubbliche.

Dal mese di settembre 2014 il Centro di Certificazione della Difesa rilascia, al personale militare e civile dell'Amministrazione della Difesa, una nuova Carta Multiservizi della Difesa denominata CMD2, una smart-card che contiene, oltre al certificato di Firma Digitale e di Cifra, anche un **certificato di Autenticazione CNS** (Carta Nazionale dei Servizi).

Tale Carta Multiservizi, rilasciata ai sensi del DPR 851/1967, del DPCM 24 maggio 2010 e del DPCM 10 maggio 2012, ha anche valore di tessera di riconoscimento elettronico (Mod. ATe).

#### L'utilizzo del **certificato di Autenticazione CNS** consente:

- come privati cittadini, di collegarsi ai siti web delle Pubbliche Amministrazioni, autenticarsi telematicamente ai portali e, quindi, poter accedere ed usufruire di tutti i servizi esposti.
  E' possibile, ad esempio, autenticarsi al portale ed usufruire dei servizi dell'INPS/INPDAP (www.inps.it) della GIUSTIZIA (pst.giustizia.it) e dell'AGENZIA DELLE ENTRATE (www.agenziaentrate.gov.it).
- di autenticarsi ai portali web per l'accesso telematico ai servizi offerti dall'Amministrazione della Difesa (futura implementazione);

Ulteriori informazioni relative all'Autenticazione CNS sono reperibili sul sito dell'Agenzia per l'Italia Digitale (Ag.I.D.) - <a href="http://www.agid.gov.it/identita-digitali/carta-nazionale-servizi">http://www.agid.gov.it/identita-digitali/carta-nazionale-servizi</a>

#### Premessa

Qualunque sia il browser utilizzato è necessario installare i certificati di Root delle Certification Authority.

Tale operazione, che risulta indispensabile per l'utilizzo della CMD, viene eseguita durante l'installazione sul proprio PC della suite di Firma "PKIDesk", seguendo le istruzioni del "Manuale Utente PKI Desk" a corredo del pacchetto di installazione pubblicato sul sito del Centro Sistemi Informatici dell'Esercito (Ce.S.I.E) e del Centro di Certificazione PKI Difesa il cui download è disponibile al seguente link:

http://c4d.difesa.it/Sicurezza/PKI-Firma-Digitale/Software/PKIDesk.zip

### Configurazione dei principali browser per l'accesso ai servizi con Autenticazione CNS

Il **browser** è il programma che consente di accedere ai portali Web dell'Amministrazione Difesa e delle Pubbliche Amministrazioni e di poter usufruire dei servizi esposti.

Prima di procedere è necessario verificare che sia stata installata la suite di firma PKI Desk comprendente:

- CMD API 3.5 (versione per i S.O. a 32 bit e versione per i S.O. a 64 bit);
- Client di firma ATOS PKI Desk 3.5.1;
- Certificati di Root delle Certification Authority;
- PDFCreator-0.9.8;
- "Manuale Utente PKI Desk".

La procedura di configurazione è diversa a seconda del browser utilizzato:

## 1. Finternet Explorer

Per utilizzare il browser IE di Microsoft per la navigazione SSL, è necessario importare il certificato di autenticazione CNS nello store Microsoft. Questa operazione avviene durante la prima Autenticazione, su qualsiasi sito web in protocollo https, grazie alle CMD Api installate sul PC.

In sintesi non sono necessarie ulteriori configurazioni e installazioni se non quelle precedentemente descritte nel documento e relative all'installazione della suite di Firma "PKI Desk".

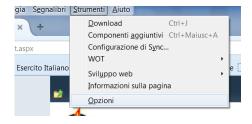
**NOTA:** su Internet Explorer 10 e successivi è necessario accedere a **Opzioni Internet/Avanzate/Impostazioni** e disabilitare le opzioni TLS 1.1 e TLS 1.2.

Lasciare abilitata unicamente l'opzione TLS 1.0.

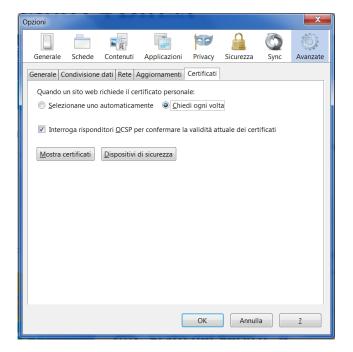
# 2. Firefox

Le istruzioni che seguono portano alla corretta configurazione del browser Mozilla Firefox vers. 33.1.1, per l'utilizzo dei certificati di Autenticazione CNS:

a. Avviare il browser Mozilla Firefox e selezionare la voce "Opzioni" dal menù "Strumenti"

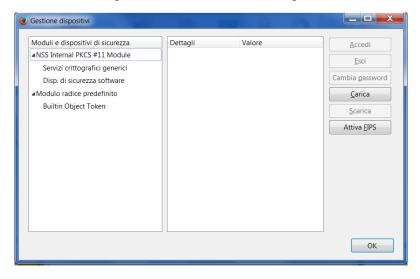


b. Selezionare "Avanzate" Avanz

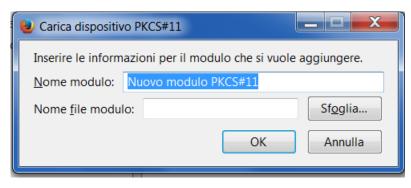


Nel pannello "Certificati" verificare che sia configurato come mostrato nell'immagine.

c. Cliccare su "Dispositivi di sicurezza" e compare la finestra "Gestione dispositivi"



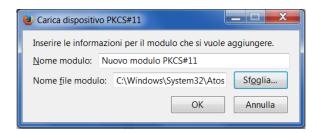
d. Cliccare su "Carica" e compare la finestra "Carica dispositivo PKCS#11



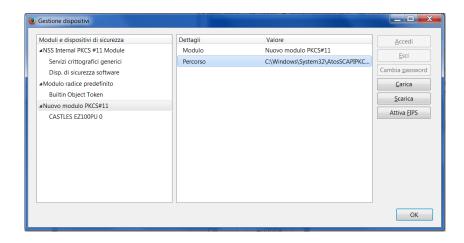
e. Cliccare su "Sfoglia..." e selezionare il percorso per raggiungere la libreria "AtosSCAPIPKCS11.dll" sotto C:\Windows\System32. Cliccare su "Apri".



f. Cliccare su "OK"

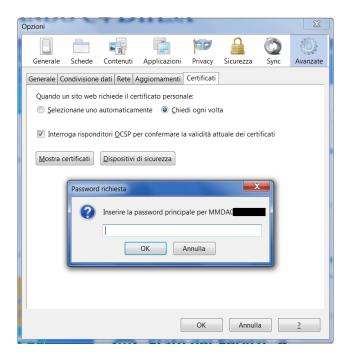


Nell'immagine che segue è visibile il modulo PKCS#11 configurato

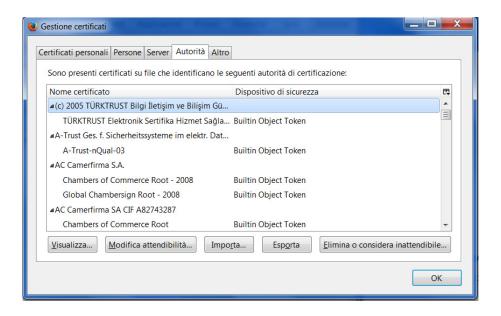


Cliccare su "OK" per chiudere "Gestione dispositivi".

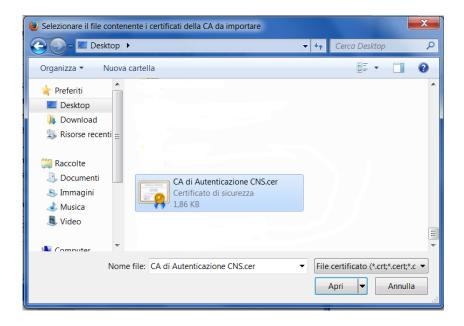
g. Inserire la CMD2 nel lettore smart-card, attendere che termini la lettura della CMD e cliccare su mostra certificati. Verrà richiesta la password (PIN Carta) per accedere alla CMD2. Inserire il PIN Carta e cliccare su "OK".



h. Comparirà la finestra "Gestione certificati". Cliccare su "Autorità" e su "Importa" per importare il certificato di Root della CA di Autenticazione CNS. Il certificato di Root della CA di Autenticazione CNS è reperibile sia nella cartella "Certificati" della Suite di Firma (vedi installazione Suite di Firma "PKIDesk" precedentemente descritta) e sia nello store Microsoft (Internet Explorer -> Opzioni Internet -> Contenuto -> Certificati -> Autorità di certificazione radice attendibili -> Esporta) in quanto installati durante l'installazione della Suite di Firma



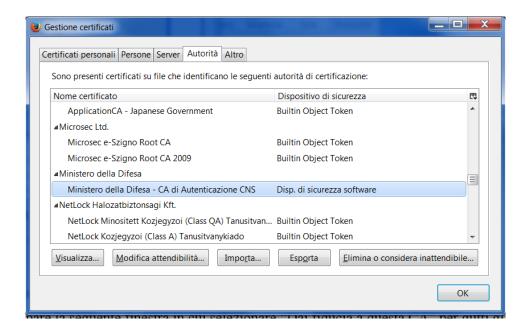
#### Selezionare il Certificato e cliccare su "Apri"



Compare la seguente finestra in cui selezionare "Dai fiducia a questa CA....." per gutti gli utilizzi indicati e cliccare su "OK"



Nell'immagine che segue è visibile il certificato importato. Cliccare su "OK" e su "OK della finestra "Opzioni"



Accedere ai servizi offerti dall'Amministrazione Difesa e dalle Pubbliche Amministrazioni.