

Il presente documento ha lo scopo di fornire alcune informazioni sulla CNS, (Carta Nazionale dei Servizi), necessaria per la presentazione della domanda sul portale INVITALIA

La Carta Nazionale dei Servizi o CNS è un dispositivo (ovvero una Smart Card o una chiavetta USB) che contiene un “certificato digitale” di autenticazione personale ed un “certificato digitale” atto all’apposizione della firma digitale su un documento informatico:

1. Cos’è il certificato di autenticazione CNS?

È un “certificato digitale” di autenticazione personale. È uno strumento informatico che consente l’identificazione certa dell’utente in rete e permette di accedere ai servizi della pubblica amministrazione e/o consultare i dati personali resi disponibili dalle pubbliche amministrazioni direttamente su sito web. Il certificato digitale, contenuto all’interno della CNS, è l’equivalente elettronico di un documento d’identità (come il passaporto o la carta d’identità) e identifica in maniera digitale una persona fisica o un’entità. Viene emesso da un’apposita Autorità di certificazione (Certification Authority - CA) riconosciuta secondo standard internazionali, la quale garantisce la validità delle informazioni riportate nel certificato. Come i documenti cartacei, anche il certificato digitale ha una validità temporale al di fuori della quale risulterà scaduto.
(tutorial)

2. Come si usa il certificato di autenticazione CNS?

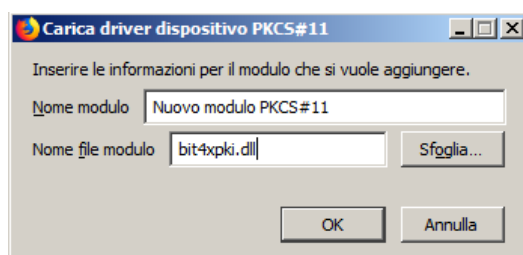
Il certificato CNS va importato nel browser che si utilizza per la navigazione, in modo tale che, al momento dell’accesso con autenticazione, il sistema riconosca le informazioni relative al soggetto che sta entrando e consenta l’accesso all’area protetta e ai servizi di consultazione o creazione di pratiche per la Pubblica Amministrazione.

L’operazione di importazione dei certificati nel browser varia a seconda dell’ente certificatore che ha rilasciato il dispositivo. È consigliabile verificare con il proprio gestore le modalità di configurazione del browser per il proprio dispositivo. È possibile consultare l’elenco esaustivo degli enti certificatori sul portale [Agid](#).

- ✓ Nella maggior parte dei casi è possibile procedere con la configurazione del browser installando l’eleggibile: **Bit4id**
- ✓ Dopo aver lanciato l’eleggibile del programma, si dovrà aprire il browser e collegarsi al sito di interesse. Al momento dell’accesso, il sistema, se l’importazione è avvenuta con successo, chiederà il pin del dispositivo per procedere con l’autenticazione

Attenzione! Se si utilizza come browser Mozilla Firefox, l’importazione dei certificati dovrà avvenire manualmente dalla sezione delle opzioni di Privacy e Sicurezza:

- ✓ cliccando alla voce Certificati --> Dispositivi di sicurezza.
- ✓ Nel box che verrà aperto, cliccando alla voce Carica, dovrà essere compilata a mano la sezione nome file modulo:

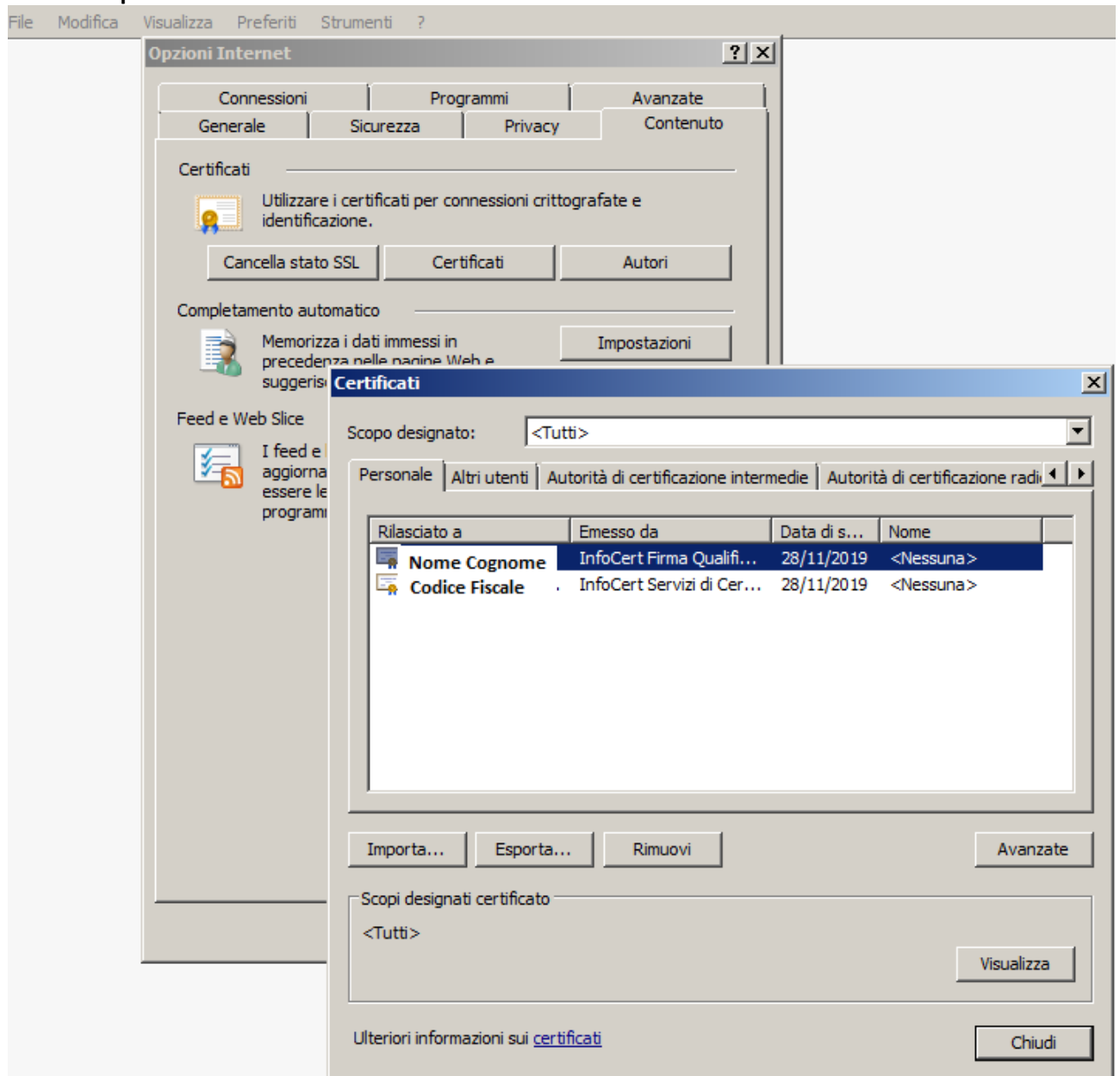




3. Come posso verificare la corretta installazione dei certificati di autenticazione CNS nel browser?

Una volta installati, i certificati saranno visibili all'interno del browser **quando il dispositivo è inserito**, con percorsi diversi a seconda del browser utilizzato per la navigazione:

Internet Explorer:





Mozilla Firefox:

The screenshot shows the Mozilla Firefox settings page with the 'Gestione certificati' (Certificate Manager) dialog box open. The dialog box displays a list of certificates under the 'Certificati personali' tab. The background settings are dimmed, showing options for privacy, security, and certificates.

Gestione certificati

Certificati personali | Persone | Server | Autorità | Altro

Sono presenti certificati rilasciati dalle seguenti organizzazioni che attestano la propria identità

Nome certificato	Dispositivo di sicurezza	Numero seriale	Termina il
INFOCERT SPA			
Codice Fiscale	/742010160004... CNS	08:81:80	giovedì 28 novembre 2019
Nome e Cognome	CNS	2D:8B:D1	giovedì 28 novembre 2019

Visualizza... Salva... Salva tutto... Importa... Elimina...

OK

Generale
 Avvisa se un sito web cerca di installare un componente aggiuntivo **Eccezioni...**

Ricerca
 Impedisci ai servizi di accessibilità di accedere al browser **Ulteriori informazioni**

Privacy e sicurezza

Raccolta e utilizzo dati di Firefox
Cerchiamo di garantire agli utenti la possibilità di migliorare Firefox per tutti. Chiediamo il tuo permesso prima di raccogliere dati. **Ulteriori informazioni**

Consenti a Firefox di inviare a Mozilla i dati di utilizzo di Firefox
 Consenti a Firefox di inviare a Mozilla i dati di utilizzo di Firefox

Sicurezza

Protezione contro contenuti dannosi
 Blocca contenuti a rischio e ingannevoli
 Blocca download a rischio
 Avvisa in caso di software indesiderati

Certificati
Quando un sito web richiede il certificato personale:
 Selezionane uno automaticamente
 Chiedi ogni volta
 Interroga risponditori OCSP per confermare la validità attuale dei certificati **Mostra certificati...**

Supporto a Firefox **Dispositivi di sicurezza...**



Google Chrome:

Impostazioni

Cerca nelle impostazioni

- Continua da dove eri rimasto
- Apri una pagina specifica o un insieme di pagine

Avanzate

Privacy e sicurezza

Certificati

Scopo designato: <Tutti>

Personale | Altri utenti | Autorità di certificazione intermedie | Autorità di certificazione radi

Rilasciato a	Emesso da	Data di s...	Nome
Nome e Cognome	InfoCert Firma Qualifi...	28/11/2019	<Nessuna>
Codice Fiscale	InfoCert Servizi di Cer...	28/11/2019	<Nessuna>

Importa... | Esporta... | Rimuovi | Avanzate

Scopi designati certificato: <Tutti> Visualizza

Ulteriori informazioni sui [certificati](#) | Chiudi

Gestisci certificati
Gestisci certificati e impostazioni HTTPS/SSL

Impostazioni contenuti
Consentono di stabilire quali contenuti possono mostrarti i siti web e quali informazioni possono utilizzare

Cancella dati di navigazione
Cancella i cookie e la cronologia di navigazione, svuota la cache e molto altro.

igazione. Se preferisci,

gli indirizzi

elle pagine per

li

4. Cos'è la Firma Digitale?

La firma digitale è l'equivalente informatico di una firma autografa apposta su carta ed ha il suo stesso valore legale. La sua funzione è quella di garantire autenticità, integrità e validità di un documento: tramite l'apposizione della firma digitale, infatti, è possibile sottoscriverne il contenuto, assicurarne la provenienza e garantire l'inalterabilità delle informazioni in esso contenute.

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare.

La chiave privata è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento. Viceversa, la chiave da rendere pubblica è usata per verificare l'autenticità della firma.

Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza visto che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata.

La firma digitale conferisce al documento informatico le seguenti caratteristiche:

- ✓ autenticità: la firma digitale garantisce l'identità del sottoscrittore del documento
- ✓ integrità: la firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione
- ✓ non ripudio: la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore

5. Come si usa la Firma Digitale?

Per utilizzare il dispositivo di Firma Digitale occorre una dotazione hardware e software: se si dispone di un dispositivo token usb l'hardware e il software sono integrati, se abbiamo una smart card occorre un dispositivo hardware compatibile con il proprio sistema operativo (lettore smart card), e un software: esistono diversi tipi di software di firma digitale a seconda dell'ente certificatore che ha rilasciato il dispositivo. Tutti i software devono essere in grado di leggere e far funzionare qualsiasi tipo di firma digitale secondo il principio dell'interoperabilità. Una volta in possesso di tutta la strumentazione informatica, e completata, laddove necessaria, l'installazione delle componenti hardware, sarà possibile procedere ad operazioni di apposizione di firma digitale e verifica di documenti firmati.

L'elenco completo degli enti accreditati al rilascio delle firme digitali è presente sul sito dell'[Agid](#).

6. Come verifico l'avvenuta apposizione della Firma Digitale sul documento prodotto?

Aperto un file dal software che utilizziamo per apporre la firma digitale, sarà possibile verificare i dati relativi al soggetto che ha apposto la firma, e la validità del certificato con cui è stata eseguita l'operazione, per essere valida infatti la firma dovrà essere apposta con un certificato non scaduto, la durata dei certificati di firma è di 2 anni

Le ricordiamo che può trovare tutte le informazioni sui requisiti per l'accesso alla predisposizione dell'istanza sul sito www.mise.gov.it.