Premessa

Il presente documento è finalizzato a descrivere la corretta modalità d'installazione e configurazione dei nuovi dispositivi di firma digitale e CNS rilasciati da Infocert S.p.A..

E' consigliabile avvalersi di un tecnico e/o sistemista informatico di fiducia per la corretta configurazione dei Vs. dispositivi.

Lo Studio Eureka, in quanto rivenditore di servizi Infocert S.p.A., non è tenuta a fornire supporto tecnico e/o sistemistico nel caso in cui la presente guida non permetta di configurare e/o utilizzare i Vs. dispositivi CNS.

Possono essere presenti e/o subentrare problematiche di funzionamento dei dispositivi qualora i PC siano configurati con particolari restrizioni a livello di policy, driver di sistema e software antivirus.

Requisiti hardware

Per permettere il corretto funzionamento ed utilizzo dei dispositivi Infocert S.p.A., sono necessari i seguenti requisiti hardware:

Microsoft Windows:

- PC o notebook con sistema operativo:
    - Windows 10 Home
    - Windows 10 Professional
    - Windows 11 Home
    - Windows 11 Professional
- Almeno 4GB di RAM.
- Almeno 10GB di spazio di archiviazione libero.
- 1 presa USB 2.0 e/o USB 3.0 correttamente funzionante.
- Smart card e/o Business Key attivata correttamente.
- 1 lettore di smart card di recente produzione, in grado di poter leggere e/o gestire chip di ultima generazione con CA3 (necessario nel caso in cui si sia in possesso di una smart card).
  Fortemente consigliata l'adozione del lettore di smart card certificato Bit4id MiniLector EVO, acquistabile direttamente dallo Studio Eureka o tramite canali web.
  (https://www.bit4id.com/dispositivi/lettore-di-smart-card-minilector-evo/)

MacOS:

- PC o notebook con sistema operativo:
    - MacOS High Sierra (10.13.6) – *non certificato*
    - MacOS Mojave (10.14.6 e precedenti)
    - MacOS Catalina (10.15.7 e precedenti)
    - MacOS Big Sur (11.7.1 e precedenti)
    - MacOS Monterey (12.6.1 e precedenti)
    - MacOS Ventura (13.0.1) – *in fase di test e adattamento software*

- Almeno 4GB di RAM.
- Almeno 10GB di spazio di archiviazione libero.
- 1 presa USB 2.0 e/o USB 3.0 correttamente funzionante (per MacBook Air, MacBook Pro e notebook in generale, è altamente consigliato l'utilizzo di adattatori USB-C to USB originali Apple).
- Smart card e/o Business Key attivata correttamente.
- 1 lettore di smart card recente, in grado di poter leggere e/o gestire chip di ultima generazione con CA3 (necessario nel caso in cui si sia in possesso di una smart card)
- Fortemente consigliata l'adozione del lettore di smart card certificato Bit4id MiniLector EVO, acquistabile direttamente dallo Studio Eureka o tramite canali web.
- (https://www.bit4id.com/dispositivi/lettore-di-smart-card-minilector-evo/)

Requisiti software

Per permettere il corretto funzionamento ed utilizzo dei dispositivi Infocert S.p.A., sono necessari i seguenti requisiti software:

Microsoft Windows:

- Sistema operativo correttamente aggiornato ad ultima release software Microsoft.
- Servizio “Smart Card” di Windows in esecuzione e configurato in modalità “esecuzione automatica”.
- Utente di accesso con permessi di amministratore locale di sistema (nel caso di configurazioni in dominio AD).
- In caso di presenza di un’utenza di dominio AD, l’utente stesso non deve essere soggetto a policy di dominio che ne limiti l’attività, l’esecuzione e la scrittura di file di sistema e/o software.
- Driver porte USB aggiornati ad ultima versione software disponibile.
- Software antivirus configurato ad hoc per inibire scansione e/o controllo e/o restrizioni e/o qualsiasi attività su dispositivo e/o lettore USB collegato.
- Software driver lettore smart card correttamente installato ed aggiornato ad ultima versione disponibile:

  https://www.bit4id.com/assistenza-clienti/minilector-evo-2/

- Software GoSign Desktop correttamente installato ed aggiornato ad ultima versione disponibile:

  https://www.firma.infocert.it/installazione/

- Browser Mozilla Firefox aggiornato ad ultima versione disponibile.

MacOS:

- Sistema operativo correttamente aggiornato ad ultima release software Apple.
- Utente di accesso con permessi di amministratore locale di sistema.
- In caso di presenza di un’utenza di dominio AD, l’utente stesso non deve essere soggetto a policy di dominio che ne limiti l’attività, l’esecuzione e la scrittura di file di sistema e/o software.
- Software antivirus, se presente, configurato ad hoc per inibire scansione e/o controllo e/o restrizioni e/o qualsiasi attività su dispositivo e/o lettore USB collegato.
- Software driver lettore smart card correttamente installato ed aggiornato ad ultima versione disponibile:

  https://www.bit4id.com/assistenza-clienti/minilector-evo-2/

- Software GoSign Desktop correttamente installato ed aggiornato ad ultima versione disponibile:

  https://www.firma.infocert.it/installazione/

- Browser Mozilla Firefox aggiornato ad ultima versione disponibile.

Verifica presenza software installato

Prima di procedere con l'installazione del software necessario, è fondamentale verificare se all'interno del sistema operativo siano presenti vecchie versioni delle stesse, utili al funzionamento e all'utilizzo dei vecchi dispositivi CNS.

La presenza di più versioni del medesimo software causano il mancato corretto funzionamento e riconoscimento dei dispositivi CNS.

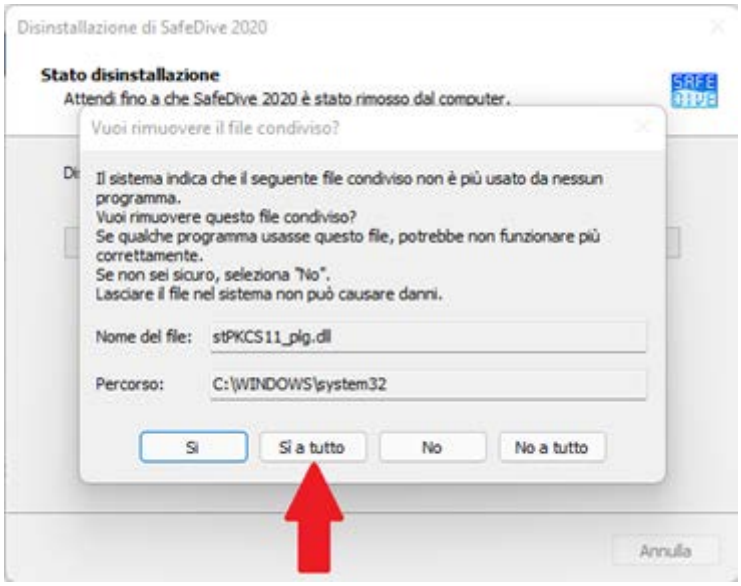
Per fare ciò, attenersi alla seguente procedura, differente in base al sistema operativo in uso:

Microsoft Windows:

1. Dal pannello di controllo di Windows accedere alla sezione di disinstallazione dei software.

2. Individuare la presenza di versioni precedenti del software Bit4id (Bit4id - Universal MW 1.4.x.x) e di SafeDive (SafeDive 2020, SafeDive 2.1, ecc.).

3. Procedere con la disinstallazione manuale, avendo l'accortezza di acconsentire ad eventuali richieste di eliminazione file temporanei e/o cartelle di sistema.



4. Riavviare il sistema operativo.

MacOS:

1. Dalla barra dei menù, accedere all'elenco delle applicazioni installata all'interno del sistema.

2. Individuare la presenza di versioni precedenti del software Bit4id e di SafeDive e trascinarli all'interno del cestino di sistema.

3. Riavviare il sistema operativo.

Verifica dati dispositivo CNS

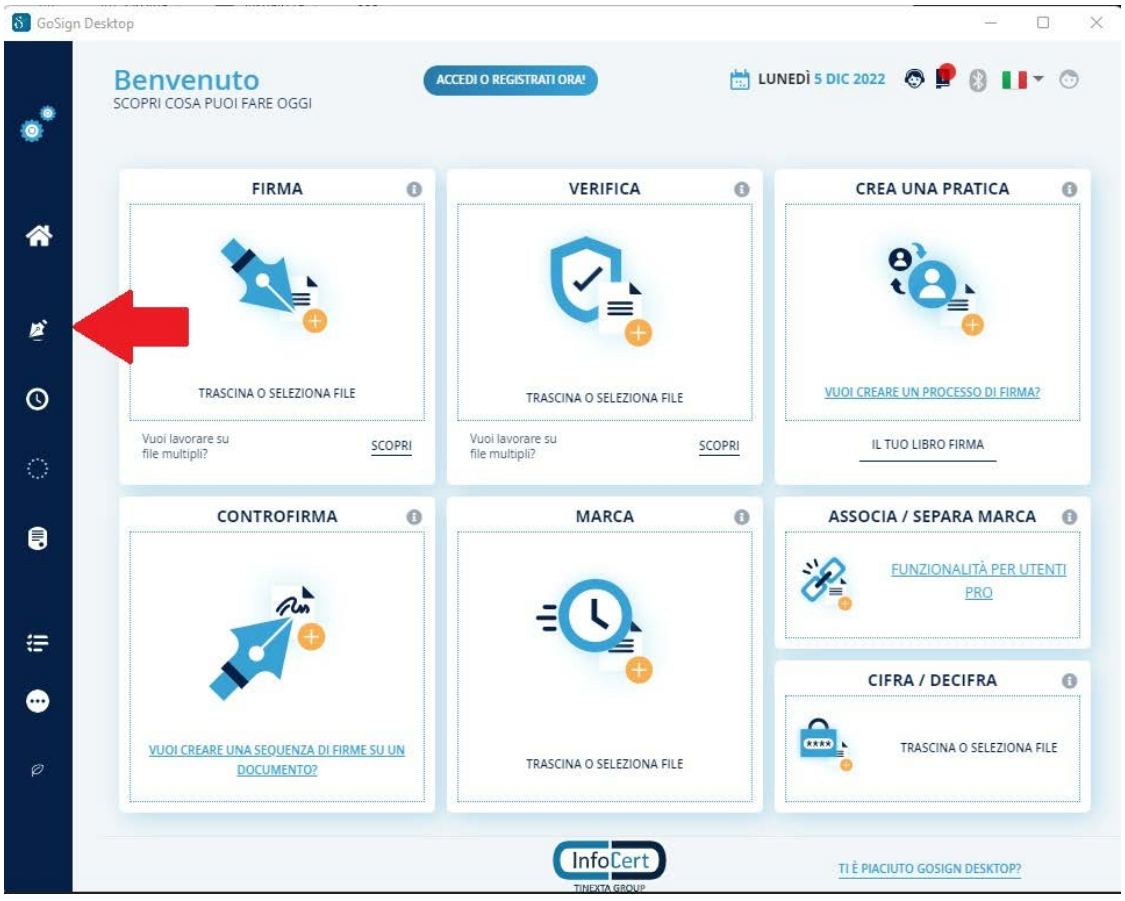
Al fine di installare il software driver corretto per la smart card e/o token USB di cui si è in possesso, è necessario identificarne con certezza la tipologia ed i relativi dati.

Per fare ciò procedere con i seguenti passaggi:

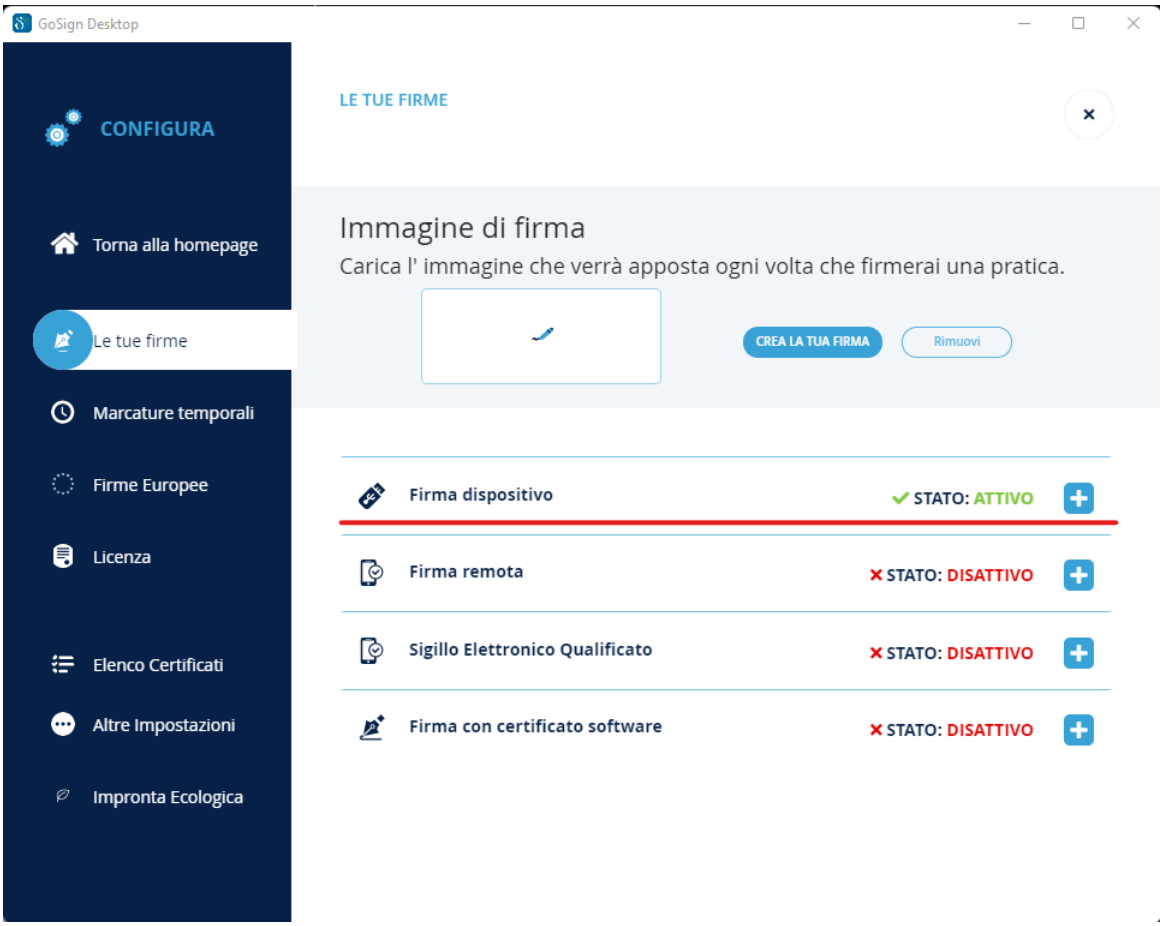
1. Collegare il proprio dispositivo al computer in uso ed attendere il tempo necessario affinchè il sistema lo identifichi.

2. Avviare il software GoSign Desktop ed attenderne l'apertura. I tempi di apertura del software dipendono dalle prestazioni del computer in uso (generalmente pochi secondi).

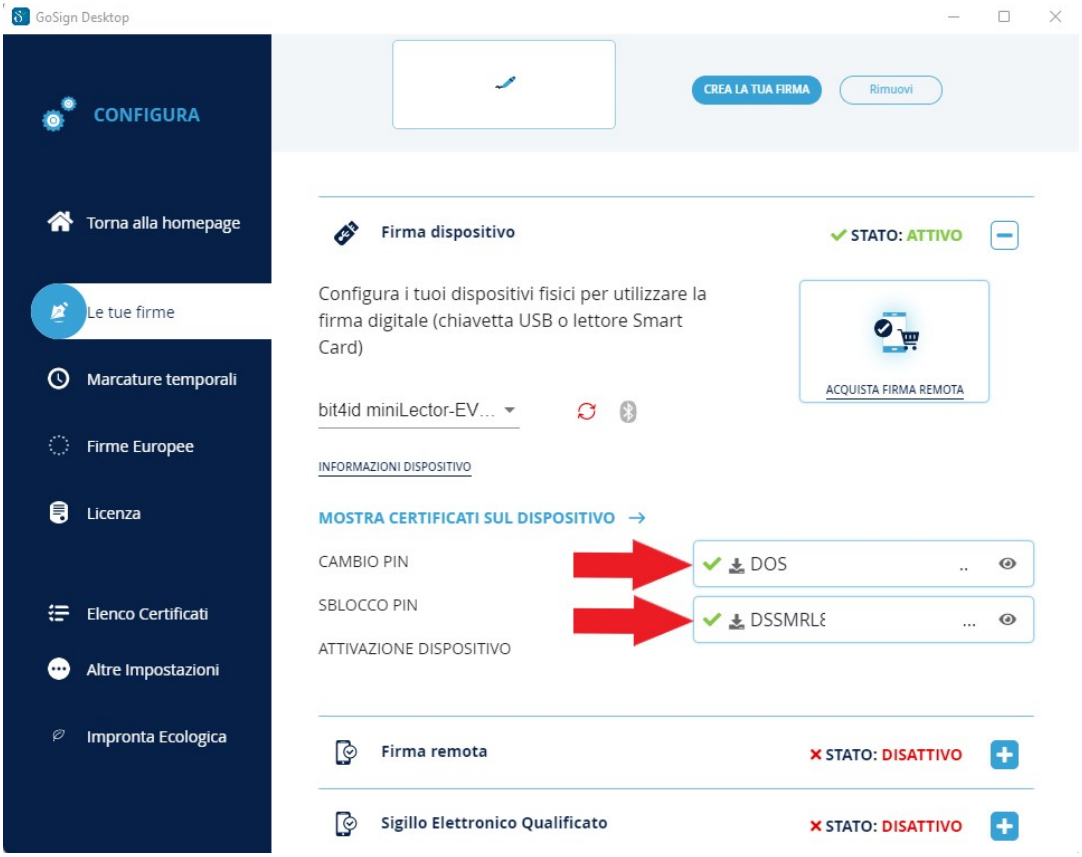
3. Con il puntatore del mouse spostarsi sul lato sinistro della finestra aperta a video e cliccare sul simbolo evidenziato nell'immagine sottostante:



4. Verificare che, la voce "Firma Dispositivo" risulti come stato "Attivo".

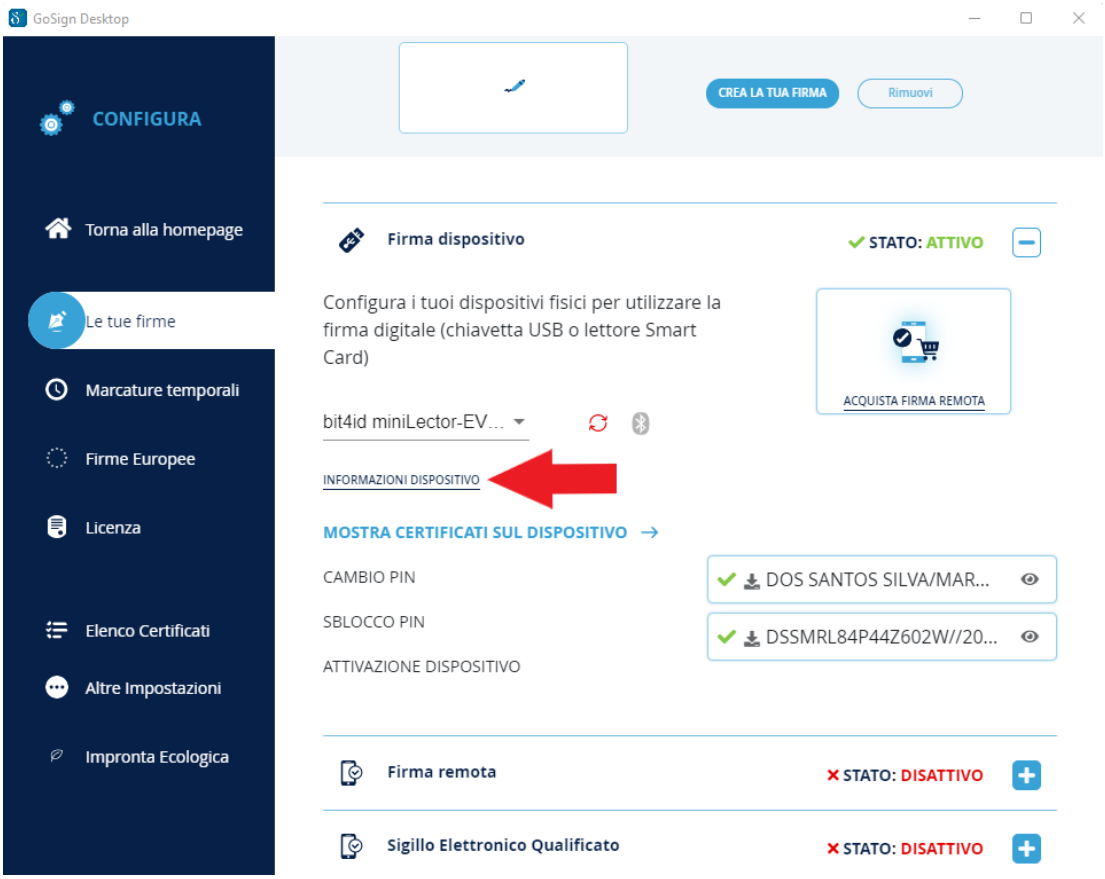


5. Se il software driver del lettore è correttamente installato, cliccando sul pulsante  verranno visualizzati i certificati di firma e di autenticazione.

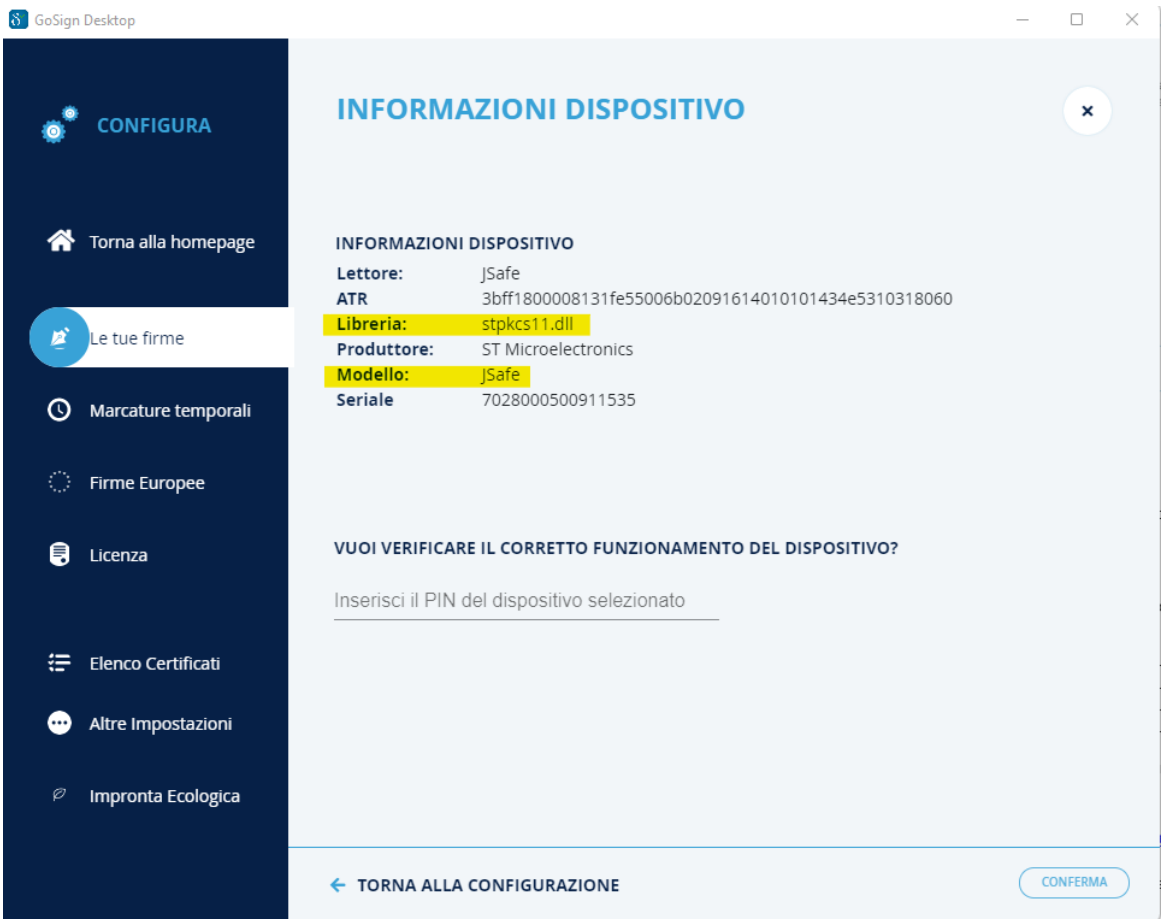


Nel caso in cui all'interno della schermata sopra sia presente esclusivamente un certificato, il Vs. dispositivo potrebbe **non** essere una CNS e/o potrebbero non essere stati installati correttamente i driver del lettore. In caso di prima installazione degli stessi, potrebbe essere necessario procedere con un riavvio preventivo del sistema operativo.

6. Cliccare sul link "informazioni dispositivo".



7. Verificare, nella finestra a video, oltre al produttore anche il campo libreria.



I dispositivi rilasciati, possono essere di due produttori e tipologie diverse:

- **Produttore Bit4ID e libreria bit4idxpki.dll**
- **Produttore ST Microelectronics e libreria stpkcs11.dll**

8. A seconda del dispositivo di cui si è in possesso, è necessario procedere con l'installazione del driver corretto:

Produttore	Libreria	Software Driver
Bit4ID	bit4idxpki.dll	Bit4id Universal MW 1.4.X.X
ST Microelectronics	Stpkcs11.dll	SafeDive

Entrambi i software, sono disponibili per il download direttamente dal sito ufficiale Infocert, alla voce "*Driver e componenti aggiuntivi*". Di seguito il link:

https://www.firma.infocert.it/installazione/#menuid3

9. Completato il download e la relativa installazione, procedere con il riavvio del sistema operativo per applicare le modifiche.

Configurazione browser – Mozilla Firefox

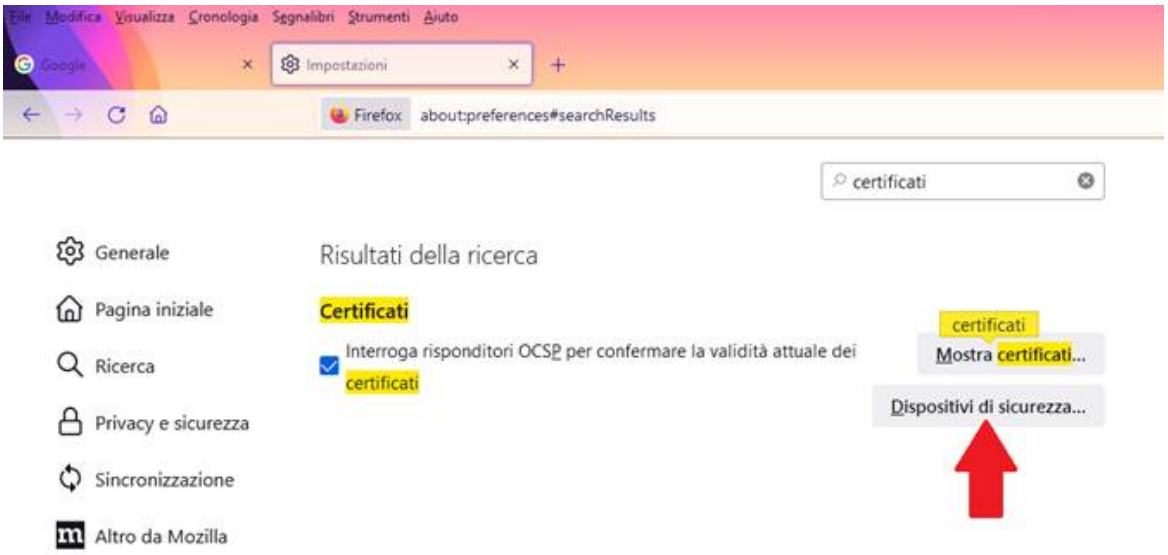
Per poter sfruttare la funzionalità di autenticazione, con il medesimo certificato, è obbligatorio l'utilizzo di Mozilla Firefox come browser predefinito per la navigazione.

Tale browser è, al momento, **l'unico** certificato per il corretto funzionamento dell'intero processo di autenticazione e gestione certificati di autenticazione.

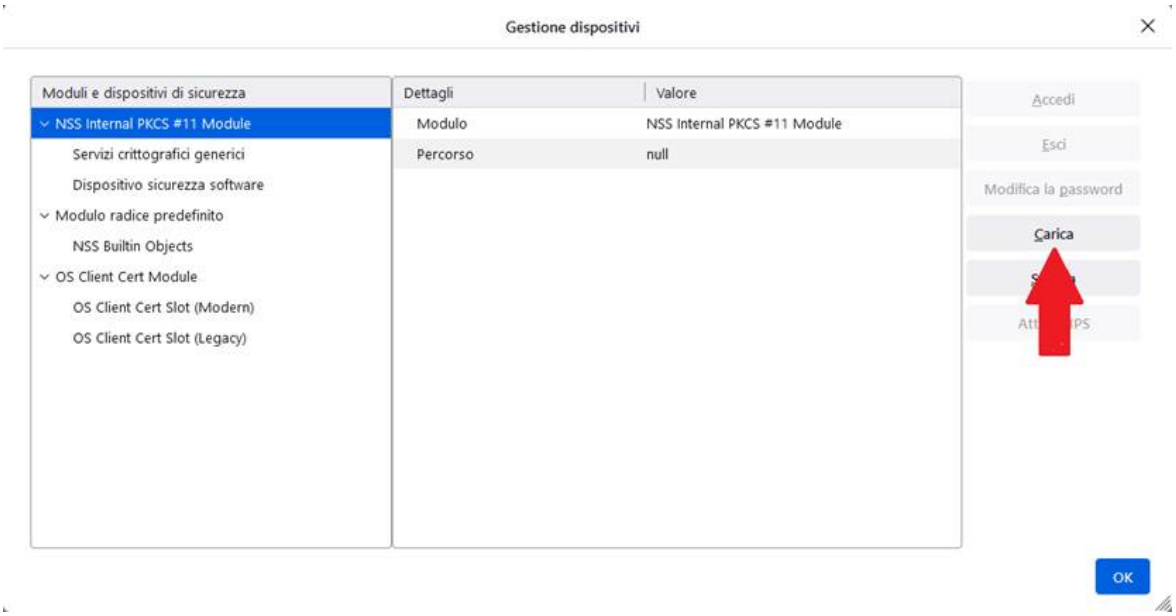
Procedere alla configurazione del software seguendo i seguenti punti:

1. Avviare Firefox ed entrate all'interno delle impostazioni del browser.

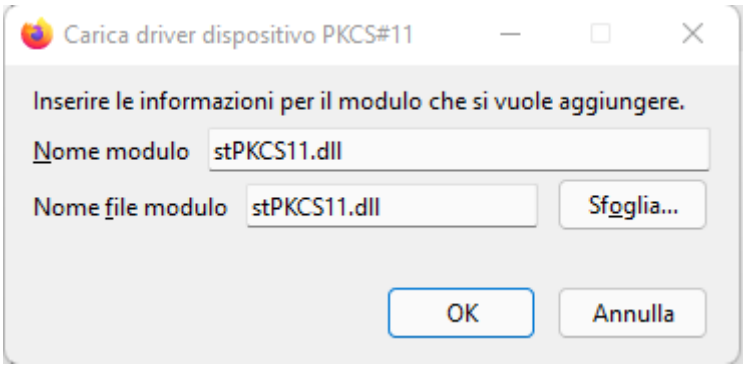
2. Nel campo di ricerca, digitare la parola "certificati" e, successivamente, cliccare sulla voce "Dispositivi di sicurezza".



3. All'interno della finestra che si è aperta, dopo aver selezionato la voce "NSS Internal PKCS#11 Module", cliccare sul pulsante "Carica".



4. Inserire sia nel campo "Nome modulo" che nel campo "Nome file modulo", la voce **stPKCS11.dll** o la voce **bit4idxpki.dll,** a seconda si sia in possesso di una smart card e/o token USB **JSIGN** o **Bit4id** (vedi tabella al punto 7 del paragrafo "Verifica dati dispositivo CNS".



5. Cliccare sul pulsante “OK” per confermare l’operazione.
6. Per verificare che il computer sia correttamente configurato per l’utilizzo, individuare nell’elenco a sinistra all’interno della finestra “Gestione dispositivi” di Firefox, la nuova voce che si è venuta a creare (corrisponde al nome modulo precedentemente inserito).

7. Cliccare sul pulsante “Accedi” ed inserire il PIN della Vs. CNS.
8. A questo punto, se la procedura è stata eseguita correttamente, lo stato del dispositivo corrisponde a “Connesso”.

9. Procedere con l’accesso a portali web (INPS, Agenzia delle Entrate e/o altri) per verificarne il corretto funzionamento.