Configurazione del Browser per l'utilizzo con il dispositivo di firma

Verifica libreria utilizzata dal dispositivo di firma

Aprire InfoCert Dike 6. Cliccare sul menu Configurazione 🔅 e successivamente su Dispositivi:



Nel menu **Dispositivi** (Punto 1) scegliere il dispositivo da gestire (Punto 2) e selezionare **InfoCert Key 0**. Quindi cliccare sull'icona **"i"** (Punto 3).

Verificare il nome della Libreria (inp11lib):

🗘 Generale	2	Sono stati rilevati 2 dispositivi. Scegliere il dispositivo da gestire: 3 InfoCert Key 0
🎯 Marcatura Tempo	orale	Attivazione dispositivo
🕘 Firma Remota	(8) Informazio	Cambio PIN ni sul dispositivo
Connessione	Lettore: ATR:	InfoCert Key 0
🖞 Dispositivi	Libreria: Produttore:	inp11lib T Incard
Cronologia Certifi	Modello: Seriale:	CNS
K Licenza PRO ed E	Chiudi	



Il middleware corretto per l'importazione dei certificati dei dispositivi 7028[...] è il **SafeDive2** scaricabile dal sito Infocert SpA al link:

- <u>https://www.firma.infocert.it/software/SafeDive2_setup.zip</u>

Al termine dell'installazione riavviare il sistema.



1.2 Configurazione

1. Avviare il browser e selezionare la voce "Opzioni".



2. Selezionare la funzione "**Avanzate**" dall'elenco posto sulla sinistra dello schermo e, successivamente la sezione "**Certificati**".

🛱 Opzioni	× +	
Firefox about:pre	ferences#advanced	☆ 自 ♥ ↓ ♠ ♥ 〓
0 Generale	Avanzate	
Q Ricerca	Generale Condivisione dati Rete Aggiornamenti Certificati	
Applicazioni	Richieste Quando un sito web richiede il certificato personale:	
Sicurezza	Selezionane uno automaticamente Shiedi ogni volta	
🌒 Sync	✓ Interroga risponditori <u>Q</u> CSP per confermare la validità attuale dei certificati	
	Mostra certificati Dispositivi di sicurezza	

- 3. All'interno della sezione "Certificati"
 - Verificare l'attivazione dell'opzione "Selezionane uno automaticamente"
 - Cliccare su "Dispositivi di Sicurezza"
 - Cliccare su "**Carica**" dopo aver verificato l'inserimento del dispositivo digitale che contiene il certificato di autenticazione.

Moduli e dispositivi di sicurezza	Dettagli	Valore	Accedi
NSS Internal PKCS #11 Module			Esci
Servizi crittografici generici Disp. di sicurezza software			Cambia <u>p</u> assword
Modulo radice predefinito			<u>C</u> arica
Builtin Object Token			<u>C</u> arica
			Attiva <u>F</u> IPS

N.B. : Verranno visualizzati SOLO i certificati compatibili con l'indirizzo e-mail dell'account selezionato.

Inserire le informazioni per il modu	ulo che si vuole aggiunger
Nome modulo: Nuovo modulo	PKCS#11
Nome <u>f</u> ile modulo:	Sf <u>og</u> lia
	OK Annulla

5. Inserire nel campo "**Nome modulo**" un nome a proprio piacimento che identifichi il tipo di dispositivo utilizzato. E' anche possibile lasciare il valore di default che compare a video.

6.Nel campo "**Nome file modulo**" inserire uno dei seguenti valori in base al numero di serie della smart card utilizzata:

- inp11lib.dll per smartcard: 7028..
- ipmpki32.dll per smartcard: 1201..., 1202..., 1203...
- bit4ipki.dll per smartcard: 7420.., 1204.., 1205.., 6090...
- bit4opki.dll per smart card Oberthur: 170.., 190..
- cvP11_M4.dll per smartcard: 16..
- si_pkcs11.dll per smartcard: 1401.., 1402.., 1501.., 1502..
- cmp11.dll per smart card: 1503...

P.S. Nel nostro caso "inp11lib.dll"

7.Cliccare su "OK"

Verrà richiesta una conferma, cliccare su "**OK**" Verrà visualizzato un messaggio che conferma l'installazione del modulo, cliccare su "**OK**" Cliccare su OK per chiudere "**Dispositivi di Sicurezza**"

11.Tornare alla pagina delle funzioni **Avanzate**, cliccare su "**Mostra certificati**" e inserire il **PIN** del dispositivo.

?	Inserire la password principale per CNS.
	•••••
	OK Annulla

Sono presenti certificati su file che identificano	le seguenti autorità di certificazione:	
Nome certificato	Dispositivo di sicurezza	E.
🔺 (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim G	δũν	<u>^</u>
 A-Trust Ges. f. Sicherheitssysteme im elektr. I A-Trust-nQual-03 AC Camerfirma S.A. Chambers of Commerce Root - 2008 	Dat Builtin Object Token Builtin Object Token	
Global Chambersign Root - 2008 AC Camerfirma SA CIF A82743287 Visualizza Modifica attendibilità	Builtin Object Token mpo <u>r</u> ta Esp <u>o</u> rta <u>E</u> limina o considera i	nattendibile

12.Selezionare la sezione "Autorità"

- Prima di procedere alla configurazione del software di autenticazione con Firefox V.41.0 è necessario importare i certificati della Certification Authority InfoCert all'interno del sistema operativo.
 E' quindi necessario eseguire il download dei Certificati della C.A. InfoCert preventivamente dal sito:
 - o https://www.firma.infocert.it/installazione/certificato.php

alla voce: (certificato CA InfoCert Servizi di Certificazione) e salvarlo su una qualsiasi directory del proprio P.C.

13.Cliccare su "Importa".

- 14.Selezionare la directory in cui sono stati scaricati i certificati root
- 15.Selezionare il certificato InfoCert_Servizi_di_Certificazione.cer e cliccare su "Apri"

ownload certifi	cato				×
È stato richies	o di dare fiducia a	a una nuova autorità	di certificazione	(CA).	
Considerare at	ttendibile "InfoCer	rt Servizi di Certificazi	one" per i segue	enti utilizzi?	
🔽 Dai fiducia	a questa CA per l	l'identificazione di sit	i web.		
👿 Dai fiducia	a questa CA per l	l'identificazione di ut	enti di posta.		
🔽 Dai fiducia	a questa CA per l	l'identificazione di pr	oduttori softwar	e.	
Prima di dare le politiche e p	fiducia a questa C procedure da essa	A per un qualsiasi sc adottate (se disponit	opo, è consigliat vili).	oile esaminare i	l suo certificato,
Visualizza	Esamina certific	ato CA			
17				ОК	Annulla

16.Selezionare ora "Dai fiducia a questa CA" per tutti gli scopi indicati e poi clicca su "OK"

17.Cliccare su "OK" per chiudere la "Gestione Certificati"

18.Cliccare su "OK" per chiudere la finestra "Opzioni"

19. Ripetere le operazioni dal punto **15** al punto **18** per il certificato **InfoCert_Servizi_di_Certificazione 2.cer**.