

ARUBA

INSTALLAZIONE CERTIFICATI ARUBA KEY

2. Import dei certificati sul proprio PC

Per effettuare l'import è necessario collegare l'ArubaKEY e far partire il programma di Firma come descritto nelle sezioni "Collega la tua Aruba Key" o "Avvia il programma di firma"

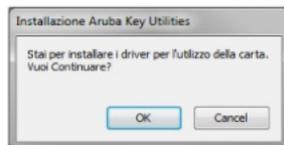
1. Seleziona il menu Utilities



2. Clicca su Import Certificato



3. Accetta e completa l'installazione



RIAVVIARE IL COMPUTER AL TERMINE DELL'INSTALLAZIONE

INSTALLAZIONE CERTIFICATI ARUBA (SMART CARD)

SCARICARE ED INSTALLARE IL DRIVER "CARD produttore Incard e Oberthur" DAL SEGUENTE LINK:

<https://www.pec.it/download-software-driver.aspx>

RIAVVIARE IL COMPUTER AL TERMINE DELL'INSTALLAZIONE.

IMPORTAZIONE CERTIFICATI SU FIREFOX

A. Apri Firefox. Apri il menù in alto a destra e scegli "Opzioni".

- B. Scegli la scheda "Privacy e sicurezza" e poi premi sul pulsante "Dispositivi di sicurezza" (si trova in fondo alla pagina)
- C. Clicca su "Carica" e poi su "Sfoggia" per scegliere il file da caricare
- D. Scegli il file "bit4xpki.dll" nella cartella C:\windows\system32 e clicca su "Apri".

INFOCERT

INSTALLAZIONE CERTIFICATI INFOCERT

SCARICARE ED INSTALLARE I DUE CERTIFICATI DAL SEGUENTE LINK:

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

NELLA SEZIONE CERTIFICATI VANNO INSTALLATI ENTRAMBI I CERTIFICATI "certificato CA InfoCert Servizi di Certificazione 2" - "certificato CA InfoCert Certification Services CA 3"

Qualsiasi sia il browser o il programma di posta elettronica utilizzato è necessario:

1. Scaricare il certificato root della Certification Authority InfoCert 2
[certificato CA InfoCert Servizi di Certificazione 2 \[CER\]](#)
2. Scaricare il certificato root della Certification Authority InfoCert 3
[certificato CA InfoCert Certification Services CA 3 \[CER\]](#)
[Consulta la guida per importare correttamente i certificati](#)
3. Aver installato GoSign (vedere sezione [GoSign](#))
4. Se utilizzi una smart card, aver installato i driver del lettore (vedere sezione [Lettore](#))
5. Configurare opportunamente il programma:
 - browser Internet
 - client di posta elettronica

RIAVVIARE IL COMPUTER AL TERMINE DELLA PROCEDURA.

QUALORA FOSSE UNA SMART CARD OLTRE ALLA PROCEDURA SOPRA INDICATA, BISOGNA CLICCARE AL PUNTO 5 "BROWSER INTERNET" - "INTERNET EXPLORER" E SCARICARE IL FILE IN BASE AL NUMERO DI SERIE DELLA SMART CARD CHE E' INDICATO PROPRIO SOPRA LA TESSERA.

Le attività variano in funzione del browser utilizzato:

 Internet Explorer

Internet Explorer permette la navigazione SSL (autenticazione sicura, firma su moduli online...) a patto di aver installato il modulo CSP (Cryptographic Service Provider, cioè il software che consente l'importazione del certificato di autenticazione nello store Microsoft).

I moduli CSP sono diversi, a seconda del **dispositivo di firma** utilizzato:

- per la **Business Key** fare clic su "Utilizza la BUSINESS KEY con le applicazioni del tuo PC" della voce "IMPOSTAZIONI" del menu del BK Manager
- per **Smart Card** con numero di serie **1203...**, **1204...**, **1205...**, **6090...**, **7420..** scaricare il file [KIT_CSP_1.3.5.0.zip](#) [ZIP 8 MB]
- per **SmartCard/Token** con numero di serie **120513...**, **1206..** scaricare il file [SafeDive Lib p11](#)
- per **Smart Card/Token** con numero di serie **1401...**, **1402...**, **1501...**, il CSP viene installato con il CARDOS API 2.2 (vedere sezione GoSign, su questa pagina)
- per **Smart Card** con numero di serie **1601...**, scaricare il file [KIT_INSTALL_CSP_CV.zip](#) [ZIP - 6,70 MB] e seguire le indicazioni illustrate nel file [leggimi.pdf](#)

[Consulta la guida di configurazione di Internet Explorer per l'accesso sicuro ai siti web](#)

NAMIRIAL

INSTALLAZIONE CERTIFICATI NAMIRIAL (FIRMA CERTA)

SCARICARE ED INSTALLARE I DRIVER IN BASE AL NUMERO DI SERIE DELLA SMART CARD CHE E' INDICATO PROPRIO SOPRA LA TESSERA.

<https://www.firmacerta.it/download.php#drivertoken>

Driver per l'utilizzo di Token usb CNS e Smart Card CNS

Middleware per Windows

Il primo passo da effettuare, per l'utilizzo della firma digitale, è l'installazione del Driver:

1. **BIT4ID**: Per i dispositivi di firma con numero di serie 2201... 2205... 2302... 2304...70000030 e 2444024...70000035
2. **SwitchService**: Per i dispositivi Token che riscontrano il messaggio d'errore "Smart Card non presente".
3. **INCARD**: Per i dispositivi di firma con numero di serie 2204... e 2203...
 - a. **SAFEDIVE 32 bit**
 - b. **SAFEDIVE 64 bit**
4. **OBERTHUR**: Per i dispositivi di firma con numero di serie 2302... 2304...

Middleware per Mac

- **Bit4ID**: Per i dispositivi di firma con numero di serie 2201... 2205... 2302... 2304...70000030 e 2444024...70000035
Nota Bene: consigliamo di seguire le istruzioni per l'installazione del software firmacerta per Mac OS > [Link](#)

RIAVVIARE IL COMPUTER AL TERMINE DELLA PROCEDURA.

DOPO IL RIAVVIO, AL SEGUENTE LINK, CI SARA' INDICATA LA PROCEDURA DA EFFETTUARE IN BASE AL DRIVER INSTALLATO IN PRECENDEZA "BIT4ID" OPPURE "SAFEDIVE"

<https://download.firmacerta.it/pdf/manualeIE.pdf>

QUALORA I DRIVER FOSSERO INSTALLATI CORRETTAMENTE, OVVERO NELLA FASE DI AUTENTICAZIONE VENGA PROPOSTA LA SCELTA DEL CERTIFICATO E L'INSERIMENTO DEL CODICE PIN, POTREBBE DIPENDERE DALL'ANTIVIRUS INSTALLATO SUL COMPUTER.

POSSIBILI PROBLEMATICHE LEGATE ALL'ANTIVIRUS

PER ESPERIENZA SOLITAMENTE I DUE ANTIVIRUS CHE POSSONO CAUSARE PROBLEMI SONO:

- AVAST - potrebbe interferire sull'installazione dei driver delle firme, solitamente disattivandolo temporaneamente, selezionando la voce "disattiva fino al riavvio del computer", e procedendo con l'installazione non dovrebbero esserci problemi.

Al termine dell'installazione riavviando il computer l'antivirus tornerà attivo in automatico.

- KASPERSKY - potrebbe bloccare l'accesso nonostante venga richiesta la scelta del certificato e del codice PIN. Facendo vari tentativi si può risolvere in tre modi:
 1. Disattivando l'antivirus fino al riavvio del computer;
 2. Inserendo il sito nell'elenco dei siti sicuri dell'antivirus;
 3. Se non dovesse funzionare seguendo i due punti sopra indicati, potrebbe dipendere da una spunta da togliere sul controllo delle connessioni crittografate. (personalmente faccio fare sempre una prova per dar contezza al professionista che in questo modo funziona tutto).