Consolle Avvocato® e Consolle CTU®

Configurazione firma digitale su sistema operativo MAC OS

OPEN Dot Com S.p.A.

Sede: Corso Francia, 121 D – 12100 Cuneo

Tel. 0171 700700 – Fax 800 136814

www.opendotcom.it – pct@opendotcom.it

1 Premesse operative

Per poter utilizzare Consolle Avvocato® o Consolle CTU è sempre necessario che il dispositivo di firma digitale, ***previamente installato sul computer in uso***, sia fisicamente collegato alla postazione (inserito nella porta USB).

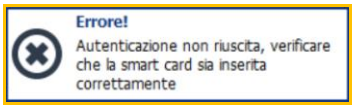
Ai fini della installazione in locale dei driver di utilizzo di ciascun dispositivo di firma digitale, si rimanda a quanto indicato nei siti web dei rispettivi enti certificatori. Di seguito, le indicazioni afferenti i dispositivi di maggior utilizzo:

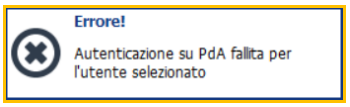
- **Infocert** – https://www.firma.infocert.it/installazione/
- **Aruba** - https://www.pec.it/download-software-driver.aspx
- **Namirial** - https://www.firmacerta.it/download.php
- **Digital DNAkey -** https://www.card.infocamere.it/infocard/pub/token-digital-dna_11345

Si ricorda, inoltre, di verificare **sempre** la compatibilità del dispositivo di firma digitale acquistato con il sistema operativo installato sulla postazione di utilizzo.

2 Operazioni di configurazione di Consolle Avvocato®/CTU

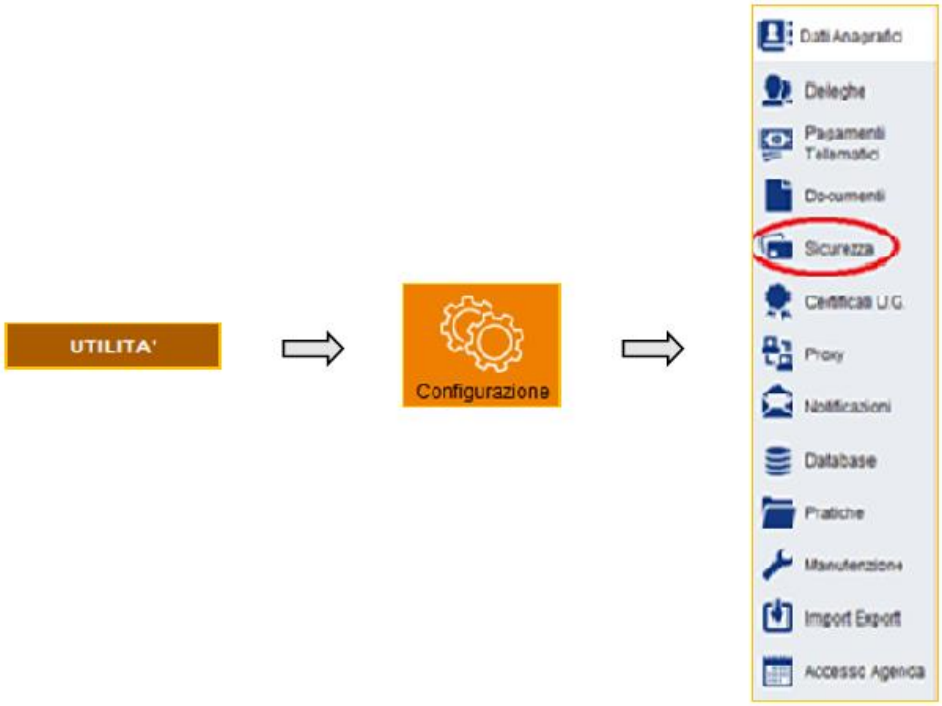
Al primo utilizzo di Consolle Avvocato®/ CTU, è necessario procederne alla configurazione affinchè vi sia una corretta interazione col dispositivo di firma digitale in uso. L'attività di configurazione, inoltre, potrebbe costituire strumento di risoluzione di eventuali errori di autenticazione al programma





oppure di mancata richiesta del codice PIN all'avvio.

Per procedere alla configurazione, è necessario accedere all'area *Sicurezza* che si raggiunge dal pannello di *Modifica Configurazione Utente* di Consolle:



Per settare il corretto driver di lettura del dispositivo di firma digitale ed iniziare il relativo iter, si dovrà quindi indicare - qualora non rilevato in autonomia - il percorso della *Directory extra*, selezionando l'icona dedicata e raffigurante una cartella di sistema:

Di seguito vengono riportate istruzioni utili alla configurazione dei più diffusi dispositivi di firma digitale.

2.1 INFOCERT BusinessKey e Smart Card

I dispositivi Infocert, siano essi BusinessKey oppure Smart Card, possono essere configurati in Consolle secondo due diverse modalità: tramite puntamento al software interno (cd. *portable*) oppure tramite puntamento al software Dike installato in locale sul computer.

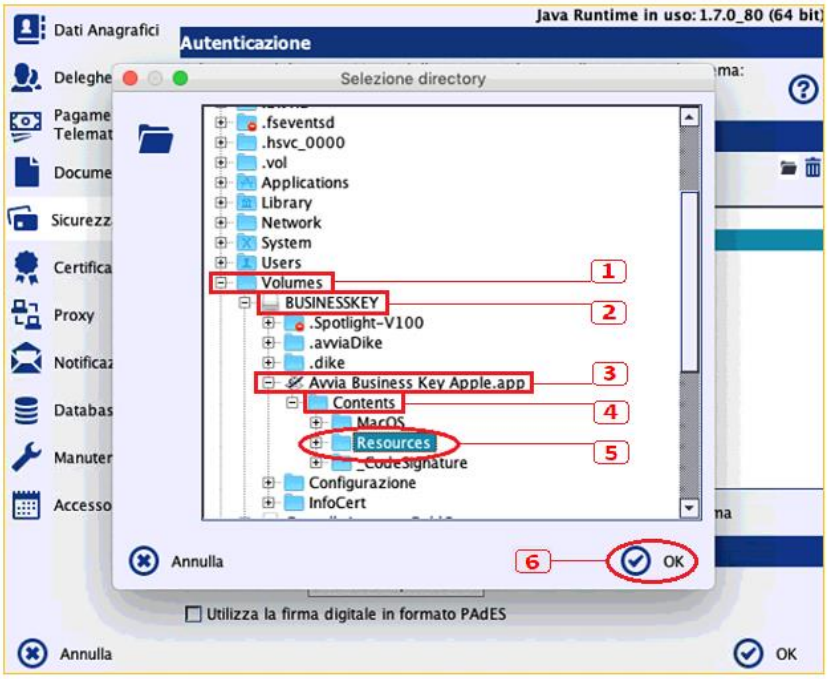
➔ Per effettuare la prima tipologia di configurazione (puntamento al software *portable*) è necessario:

1. collegare il dispositivo alla postazione in uso, mediante inserimento fisico nella porta USB od eventuale adattatore del MAC;
2. avviare Consolle Avvocato®/CTU;

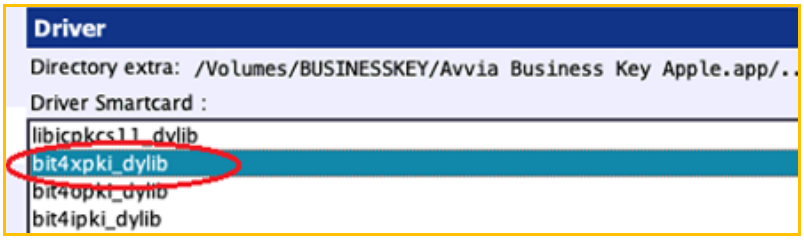
3. impostare la Directory extra di Consolle col seguente percorso:

Volumes (1) -> BUSINESSKEY (2) -> Avvia Business Key Apple.app (3) -> Contents (4) -> (selezionare senza aprire la cartella) Resources (5) -> OK (6).

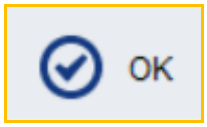
Il tutto, come da immagine che segue:



Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Bit4xpki_dylib**:



Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.

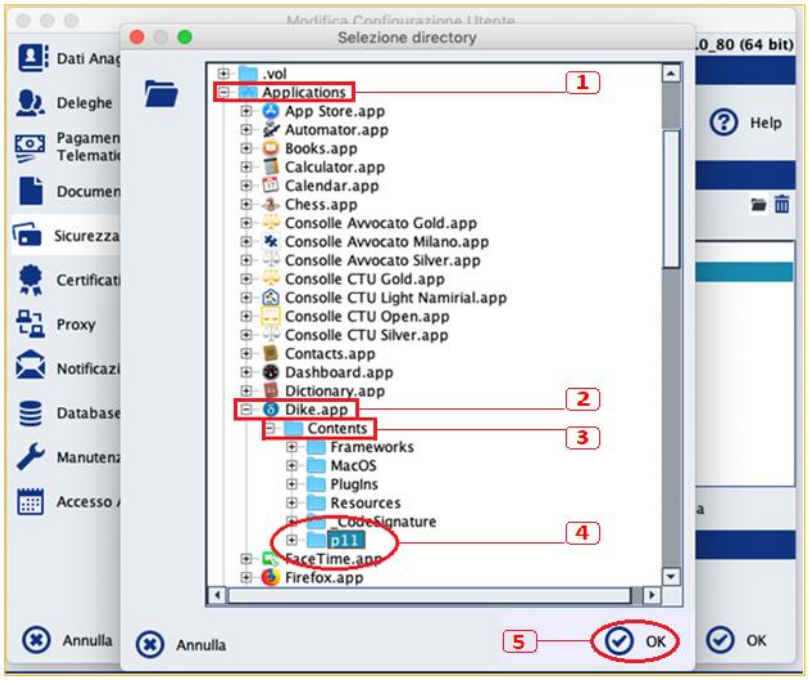


➔ Per effettuare la seconda tipologia di configurazione (puntamento al software Dike) è necessario:

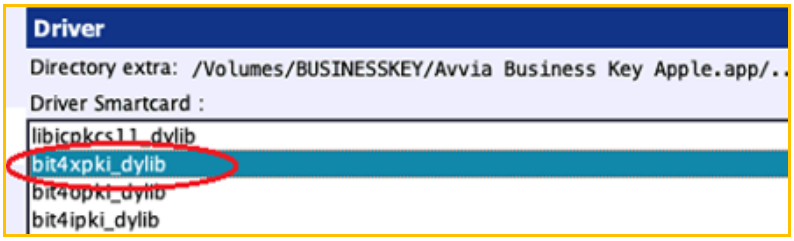
1. Scaricare dal sito del fornitore Infocert (https://www.firma.infocert.it/installazione/) ed installare il software *Dike*, avendo cura di scegliere la versione dedicata ai sistemi operativi MAC OS;
2. avviare Consolle Avvocato®/CTU;
3. impostare la Directory extra di Consolle col seguente percorso:

Applications (1) -> Dike.app [oppure GoSign] (2) -> Contents (3) -> (selezionare senza aprire la cartella) p11 (4) -> OK (5).

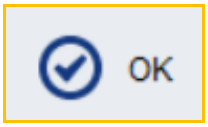
Il tutto, come da immagine che segue:



Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Bit4xpki_dylib**:



Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.



2.2 INFOCERT WIRELESSKEY

In caso di utilizzo di dispositivo Infocert WirelessKey, è necessario procedere con la configurazione che prevede il puntamento della Directory extra alla cartella "p11" del software Dike escludendo, pertanto, l'installazione in locale del software interno del dispositivo e, dunque, delle componenti wireless del dispositivi di firma digitale.

Ai fini della configurazione, si rimanda alla pagina 5 del presente vademecum.

2.3 ARUBAKEY (TOKEN ARUBA)

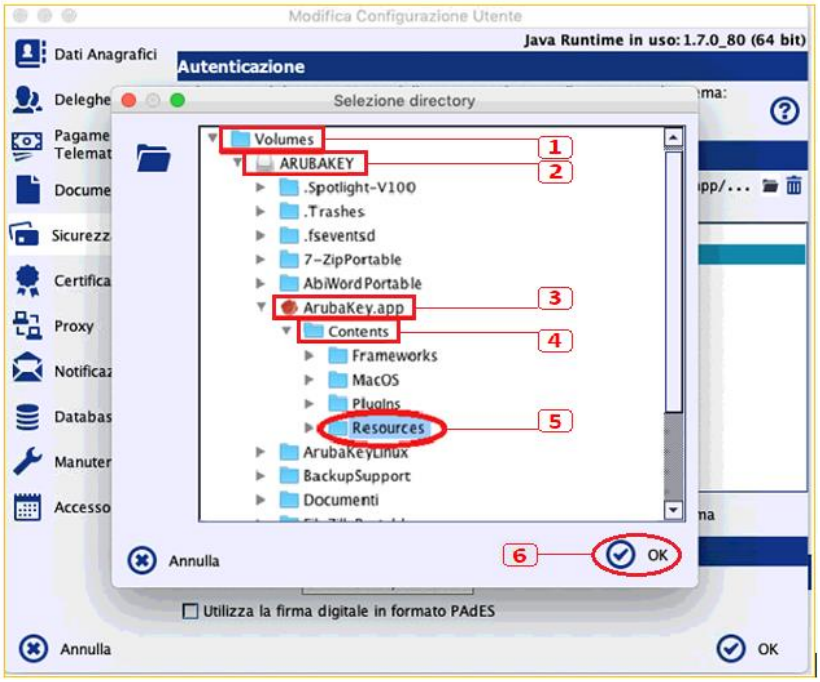
Analogamente a quanto indicato per i dispositivi Infocert, anche i dispositivi Aruba possono essere configurati in Consolle secondo due diverse modalità: tramite puntamento al software interno (cd. portable) oppure tramite puntamento al software Dike installato in locale sul computer.

➔ Per effettuare la prima tipologia di configurazione (puntamento al software *portable*) è necessario:

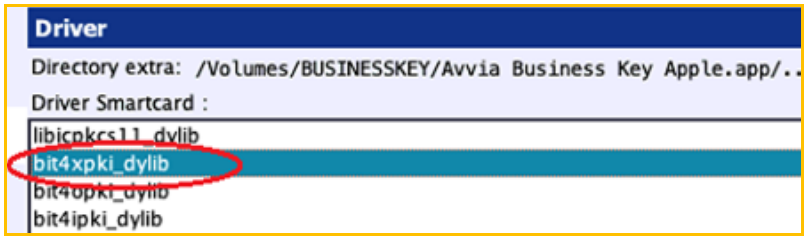
1. collegare il dispositivo alla postazione in uso, mediante inserimento fisico nella porta USB od eventuale adattatore del MAC;
2. avviare Consolle Avvocato®/CTU;
3. impostare la Directory extra di Consolle col seguente percorso:

Volumes (1) -> ARUBAKEY (2) -> ArubaKey.app (3) -> Contents (4) -> (selezionare senza aprire la cartella) Resources (5) -> OK (6)

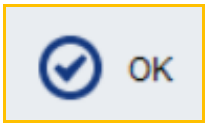
come da immagine seguente:



Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Bit4xpki_dylib**:



Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.

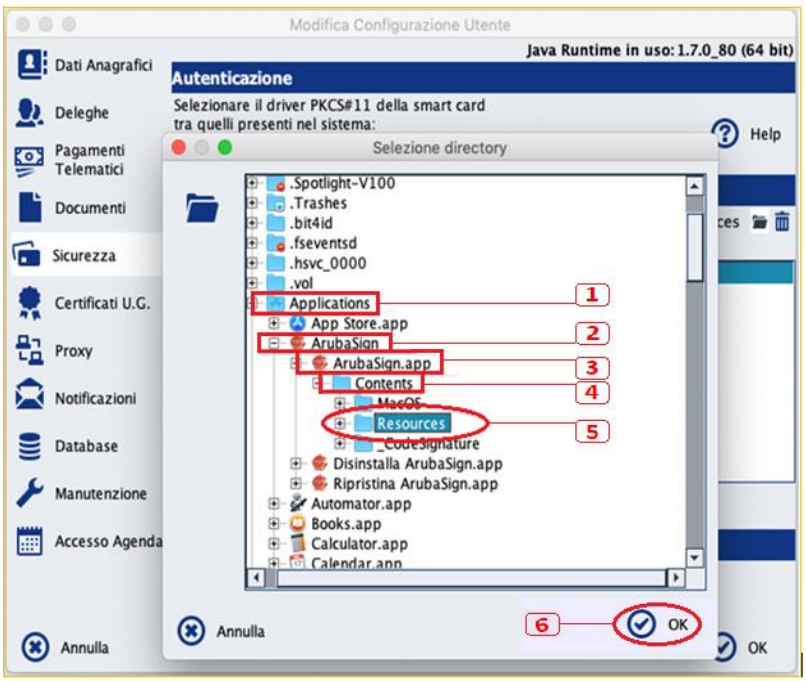


➔ Per effettuare la seconda tipologia di configurazione (puntamento al software ArubaSign) è necessario:

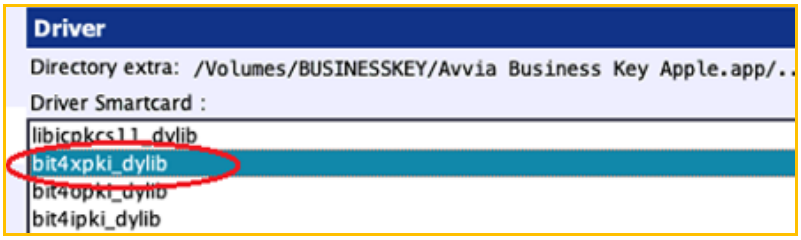
4. Scaricare dal sito del fornitore Aruba (https://www.pec.it/download-software-driver.aspx) ed installare il software *ArubaSign*, avendo cura di scegliere la versione dedicata ai sistemi operativi MAC OS;
5. avviare Consolle Avvocato®/CTU;
6. impostare la Directory extra di Consolle col seguente percorso:

Applications (1) -> ArubaSign (2) -> Aruba Sign.app (3) -> Contents (3) -> (selezionare senza aprire la cartella) Resoruces (4) -> OK (5).

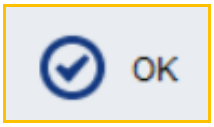
come da immagine seguente:



Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Bit4xpki_dylib**:



Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.



2.4 NAMIRIAL

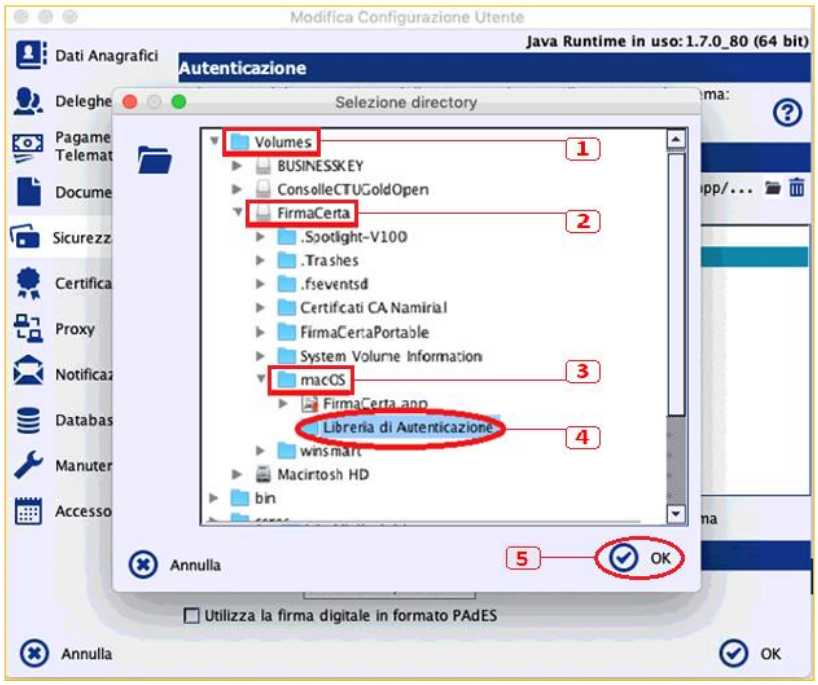
Analogamente a quanto indicato per i dispositivi precedenti, anche i dispositivi Namirial possono essere configurati in Consolle secondo due diverse modalità: tramite puntamento al software interno (cd. portable) oppure tramite puntamento al software Dike installato in locale sul computer.

➔ Per effettuare la prima tipologia di configurazione (puntamento al software portable) è necessario:

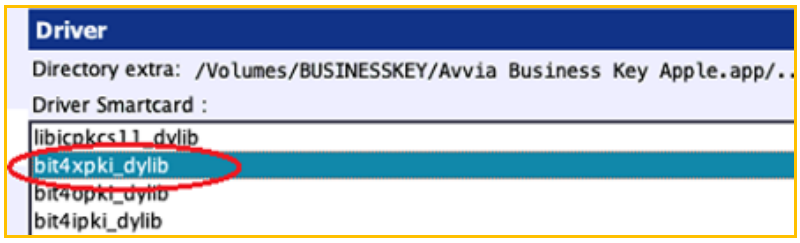
1. collegare il dispositivo alla postazione in uso, mediante inserimento fisico nella porta USB od eventuale adattatore del MAC;
2. avviare Consolle Avvocato®/CTU;
3. impostare la Directory extra di Consolle col seguente percorso:

Volumes (1) -> Firmacerta (2) -> MacOs (3) -> (selezionare senza aprire la cartella) Libreria di autenticazione (4) -> OK (5).

come da immagine seguente:



Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Bit4xpki_dylib**:



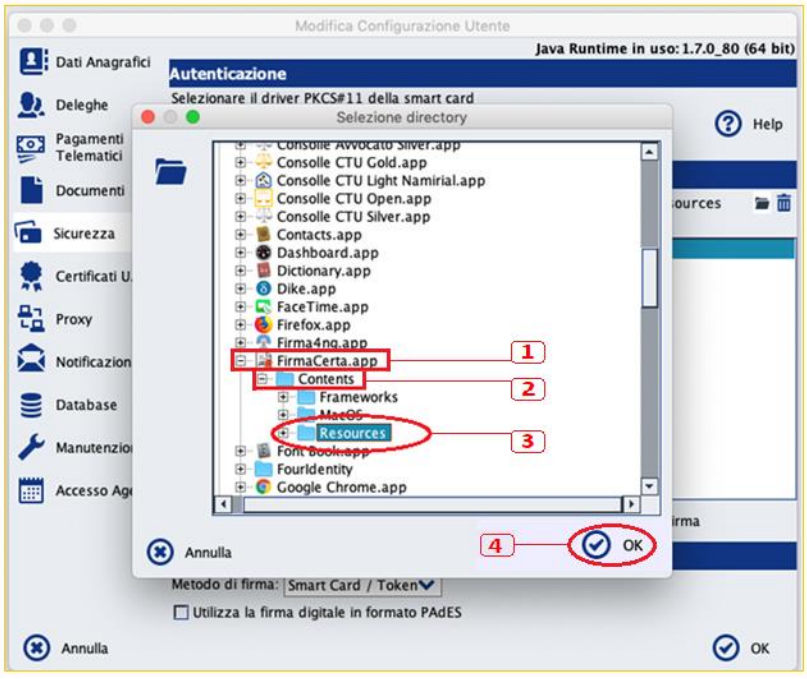
Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.

➔ Per effettuare la seconda tipologia di configurazione (puntamento al software Firmacerta) è necessario:

1. Scaricare dal sito del fornitore Namirial (https://www.firmacerta.it/software-firma-digitale.php) ed installare il software *Firma Certa*, avendo cura di scegliere la versione dedicata ai sistemi operativi MAC OS;
2. Inserire il dispositivo di firma digitale nell'apposita porta USB del computer;
3. avviare Consolle Avvocato®/CTU;
4. impostare la Directory extra di Consolle col seguente percorso, partendo dalle Applications:

FirmaCerta.app (1) -> Contents (2) -> (selezionare senza aprire la cartella) Resoruces (3) -> OK (4)

come da immagine seguente:



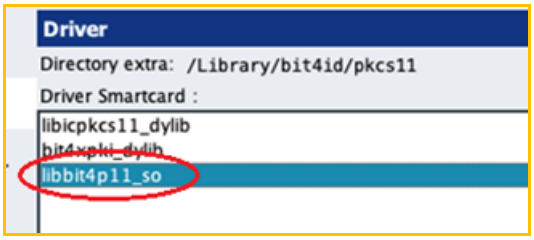
2.5 DigitalDNA KEY

Per configurare un dispositivo DigitalDNA Key è necessario:

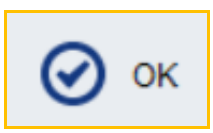
1. Inserire il dispositivo di firma digitale nell'apposita porta USB del computer;
2. avviare Consolle Avvocato®/CTU;
3. impostare la Directory extra di Consolle col seguente percorso, partendo dalle Applications:

Library -> bit4id -> (selezionare senza aprire la cartella) pkcs11 -> OK.

Nell'area della finestra dedicata all'elenco dei *Driver Smartcard* comparirà un'elencazione all'interno della quale dovrà essere scelta la voce **Blibbit4p11_so**:



Terminare l'attività di configurazione selezionando il pulsante *Ok* presente in basso a sinistra della finestra.



3 Verifica PIN e Verifica Firma

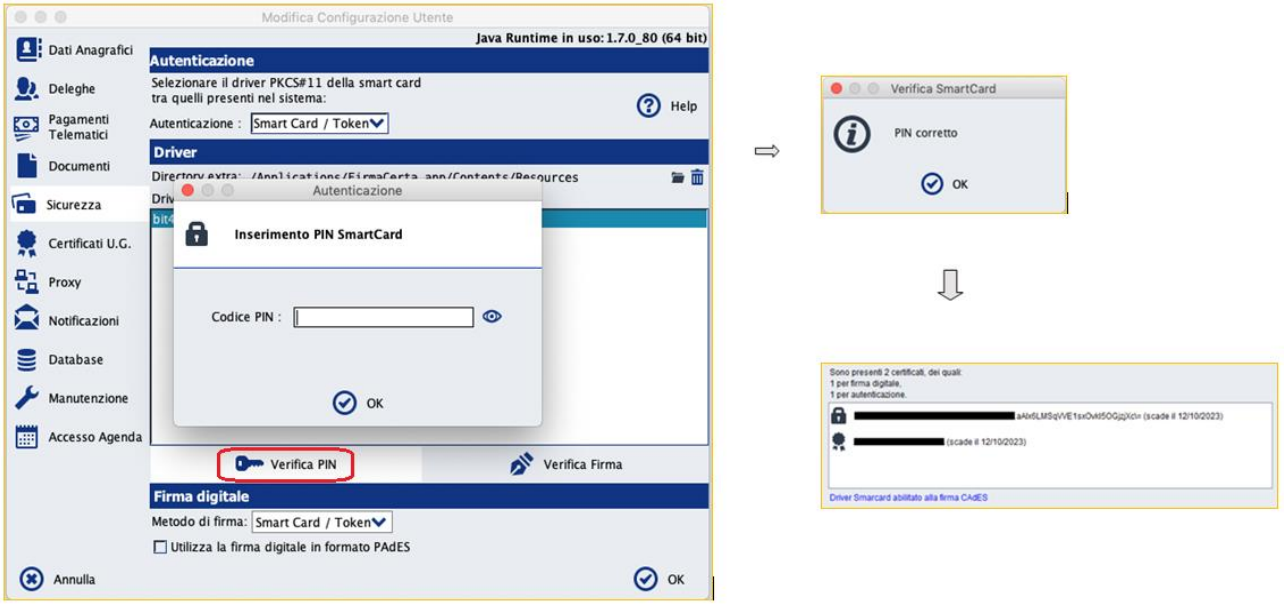
Le funzioni di *Verifica PIN* e *Verifica Firma* consentono di verificare la corretta configurazione del programma, ovverosia se il driver selezionato nell'apposita area costituisca quello corretto sia ai fini della procedura di autenticazione, che ai fini della procedura di apposizione della firma: ***entrambe le verifiche devono avere esito positivo***. In caso contrario (es: viene a presentarsi una finestra di errore oppure viene mostrato solo uno dei due certificati cristallizzati nel dispositivo), il driver selezionato dovrà essere cambiato scegliendone uno fra gli altri proposti (per la corretta individuazione del driver, si vedano i paragrafi precedenti).

Durante lo svolgimento di ciascuna verifica - la quale, beninteso, presuppone che il dispositivo di firma digitale sia collegato alla postazione -, il sistema richiederà l'inserimento del codice PIN del dispositivo di firma digitale di cui l'utente deve già essere in possesso.

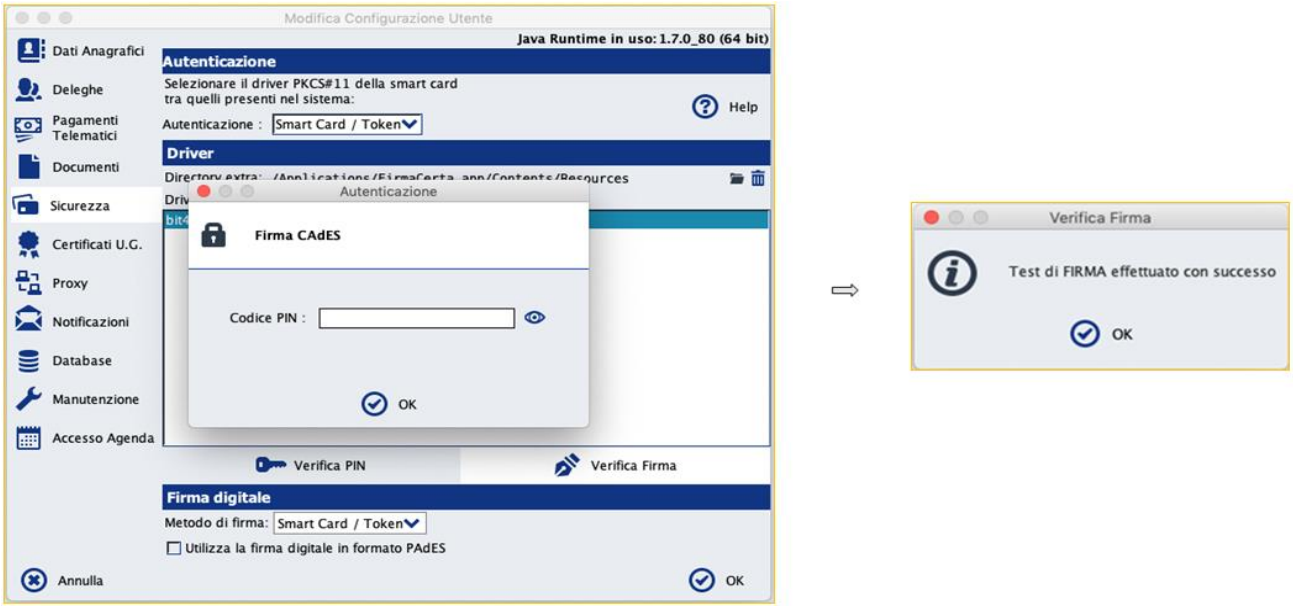
N.B.: il codice PIN, unitamente al codice PUK, del dispositivo di firma digitale viene consegnato dal fornitore al titolare al momento dell'acquisto e/o ritiro dello stesso.

Per operare le verifiche in esame è previamente necessario selezionare il driver di riferimento presente nella sovrastante area di *Driver Smartcard*. Selezionato il driver, sarà sufficiente cliccare sul pulsante di verifica – rispettivamente "Verifica PIN" e "Verifica Firma" – e, come detto, inserire il codice PIN del dispositivo all'interno della apposita finestra che verrà visualizzata dal sistema.

Di seguito i passaggi riferiti a ciascuna tipologia di verifica.



***


Modifica Configurazione Utente
Java Runtime in uso: 1.7.0_80 (64 bit)
Dati Anagrafici
Deleghe
Pagamenti Telematici
Documenti
Sicurezza
Certificati U.G.
Proxy
Notificazioni
Database
Manutenzione
Accesso Agenda
Autenticazione
Selezionare il driver PKCS#11 della smart card tra quelli presenti nel sistema:
Autenticazione : Smart Card / Token
Help
Driver
Autenticazione
Firma CAdES
Codice PIN :
OK
Verifica PIN
Verifica Firma
Firma digitale
Metodo di firma: Smart Card / Token
Utilizza la firma digitale in formato PAdES
Annulla
OK
Verifica Firma
Test di FIRMA effettuato con successo
OK