Guida all'installazione e all'uso delle funzionalità della CNS

Versione MAC OS X

Indice

1 Prerequisiti

Di seguito sono descritti i prerequisiti Hardware e Software che deve possedere il PC su cui viene installata ed utilizzata la CNS.

1.1 Caratteristiche del lettore smart card

Il Lettore smart card da utilizzare con la funzionalità CNS deve garantire la totale compatibilità con i seguenti standard di mercato:

- ISO 7816 part 1-2-3-4-6-8-9
- CCID
- PC/SC
- RoHS, WEEE
- USB 2.0 full speed, USB 1.1
- Plug&Play and Hot Swapping tramite porta USB

1.2 Caratteristiche Software del PC

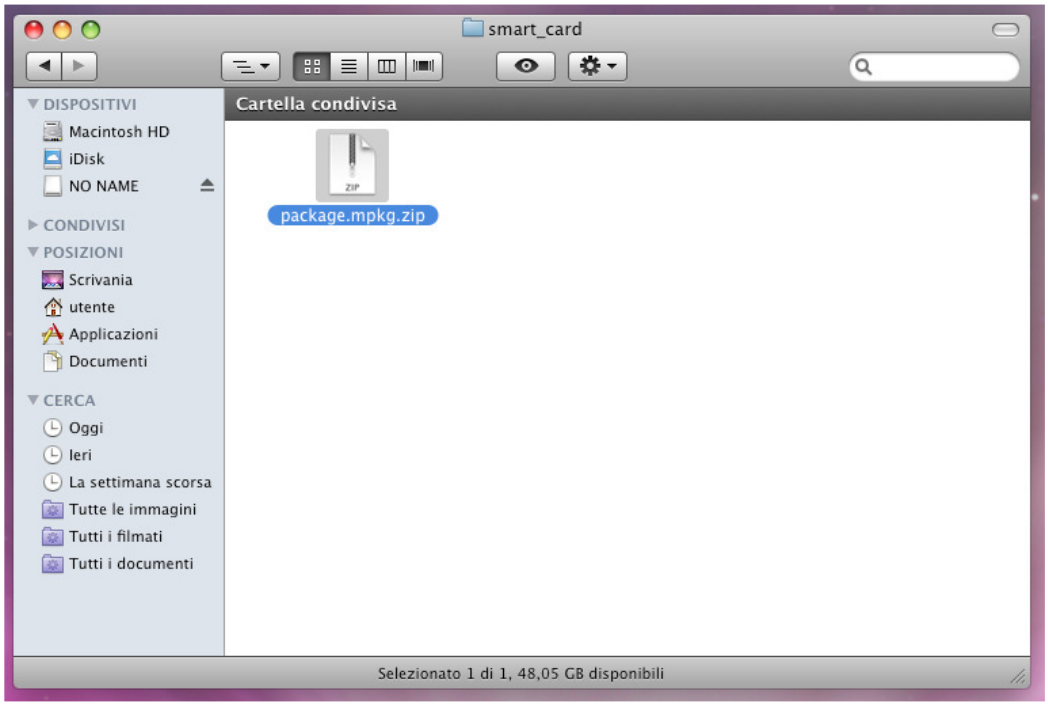
Versioni MAC OS X supportate:

- MAC OS X 10.5.4 PPC
- MAC OS X 10.6.x
- MAC OS X 10.7.x
- MAC OS X 10.8.x

2 Installazione del software

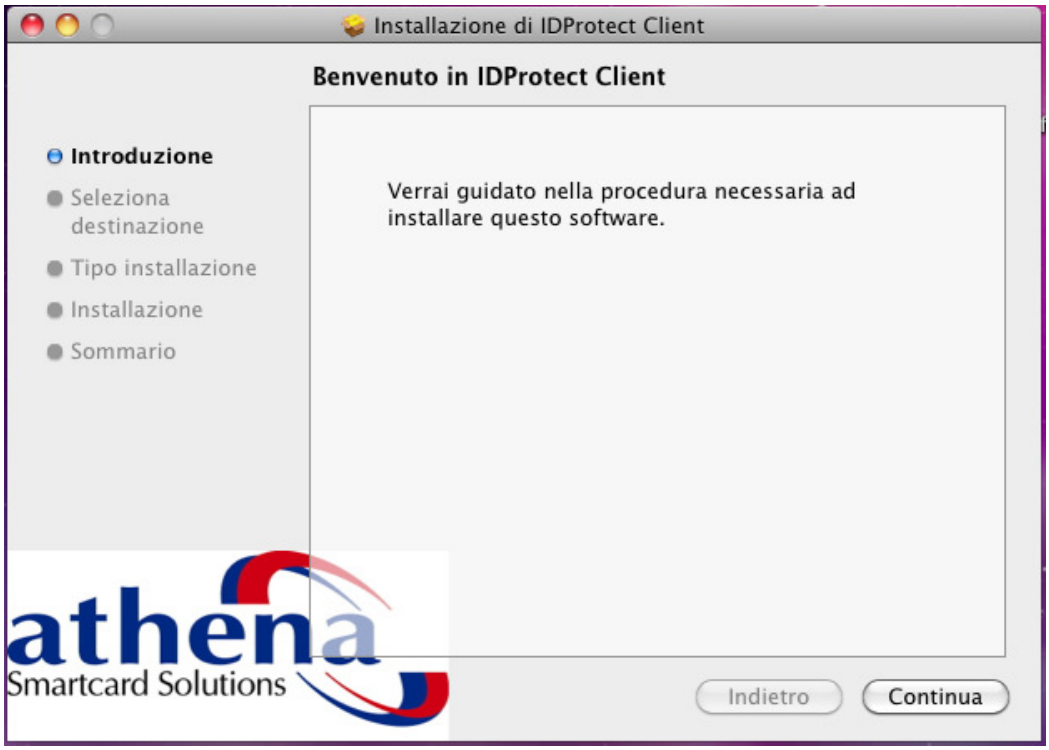
Installazione del software

1. Aprire il file Idprotect Client `6.08.mpkg`;



a. Avviare l'installar facendo doppio-clic sull'icona `IDProtect Client Installer` appena creata;

b. Apparirà la seguente finestra;



A questo punto, continuare seguendo le istruzioni a video e accettando le impostazioni proposte.

Durante l'installazione può essere richiesto l'inserimento di Username e Password di un'utenza amministrativa del Mac.
Al termine dell'installazione può essere richiesto il riavvio del Mac.

Il pacchetto installa i seguenti componenti:

- **PIN Tool** (utility per la gestione dei PIN della carta, nella cartella "Applicazioni")
- **libASEP11** (modulo PKCS#11, nella cartella \Libreria\Application Support\.....)
- **ASE.tokend** (modulo di supporto per l'Accesso Portachiavi e per il browser Safari).

N.B. se si presenta un errore " tecnologia Powerpc non supportata" alla fine dell'installazione di IDprotect Client Vi preghiamo di ignorarlo abbiamo già preso contatto con il fornitore per eliminarle Alert.

3 Configurazione per l'utilizzo con Firefox

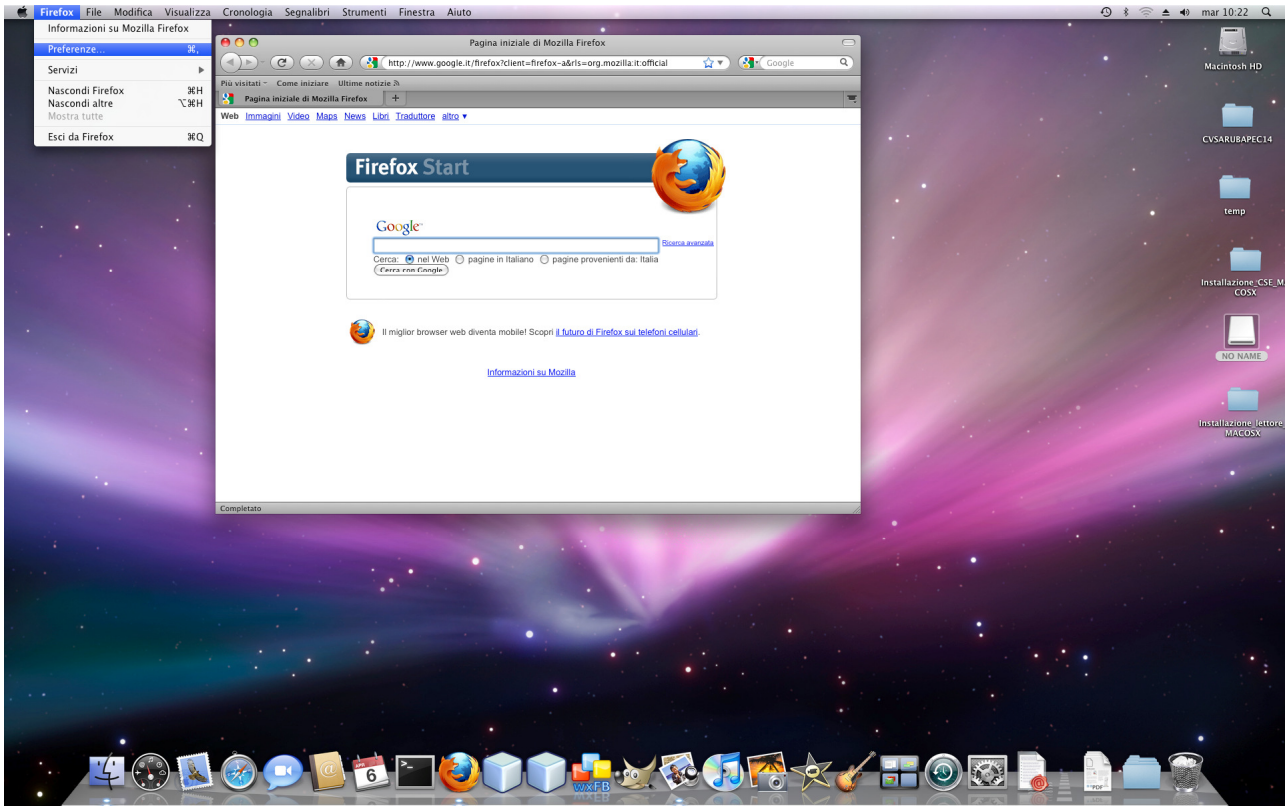
Il pacchetto di installazione cerca di configurare *automaticamente* il browser Firefox per l'uso delle carte Athena CNS. Tuttavia, in alcune circostanze la configurazione automatica può fallire (es. quando il lettore di smartcard è scollegato, quando il browser è aperto, ecc) per motivi non riconducibili a difetti del middleware Athena.

Pertanto, di seguito, viene descritta la **configurazione manuale**.

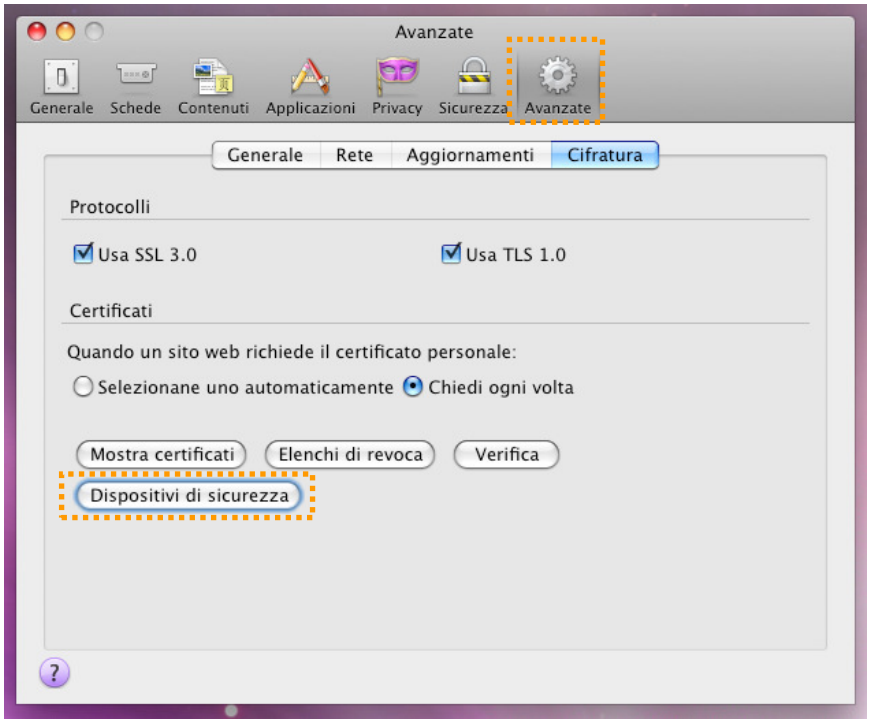
Per procedere alla configurazione di Firefox per l'utilizzo delle funzionalità della propria CNS attenersi alle indicazioni riportate di seguito:

1. Assicurarsi che il lettore sia collegato al PC ed inserire il propria CNS prima di procedere;

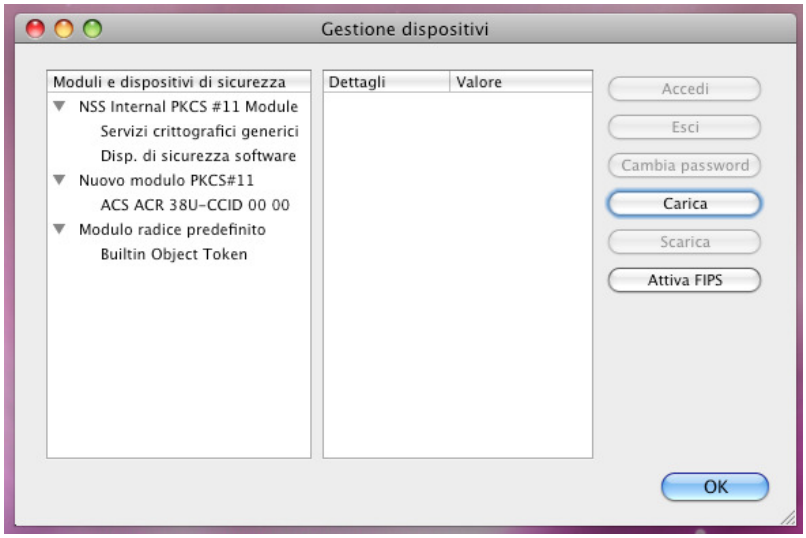
2. Avviare Firefox e selezionare quindi *Firefox → Preferenze* (vedi figura seguente);



3. All'interno della finestra *Preferenze* spostarsi sulla sezione *Avanzate*, selezionare l'opzione *Cifratura* e quindi cliccare il pulsante *Dispositivi di sicurezza* (vedi figura seguente);

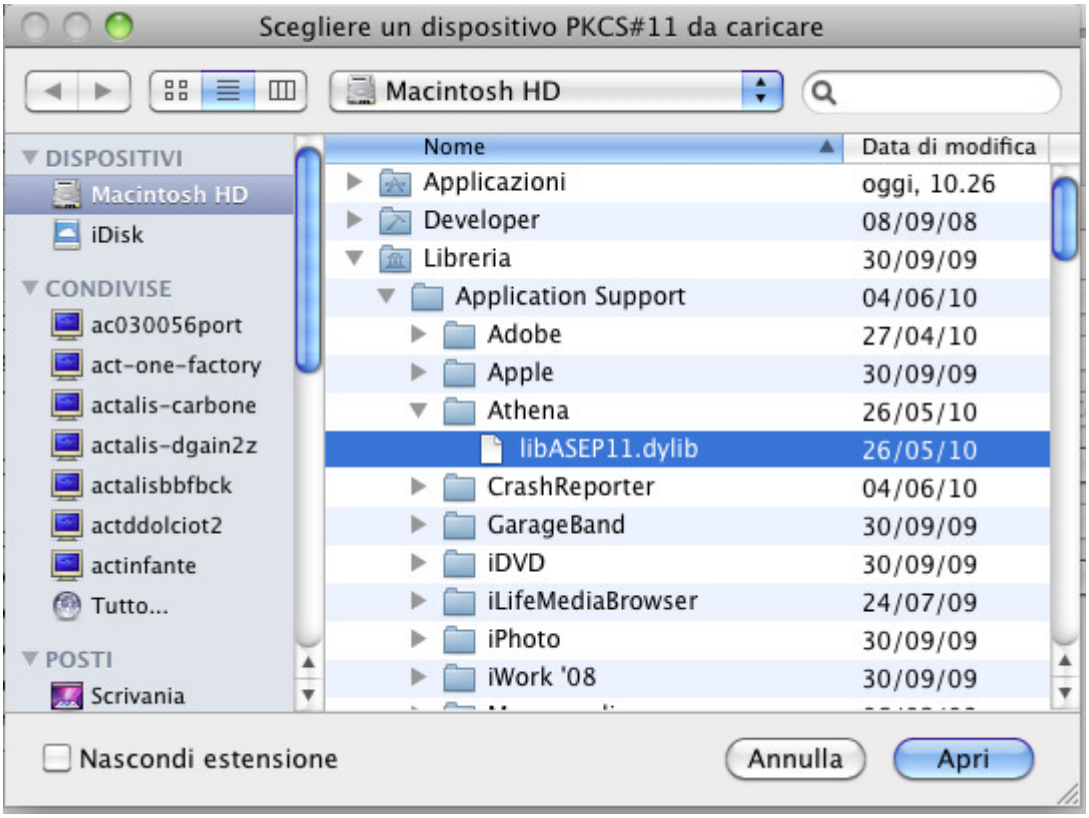


4. All'interno della finestra *Gestioni dispositivi* cliccare il pulsante *Carica* (vedi figura seguente);

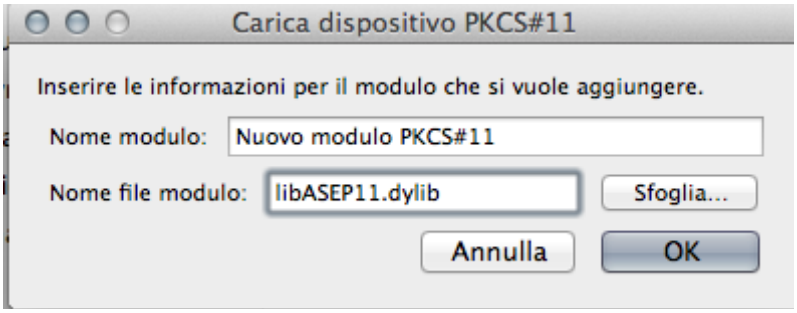


5. All'interno della finestra *Carica dispositivo PKCS#11* eseguire le seguenti operazioni:

   a. Nel campo *Nome modulo* inserire una stringa descrittiva che serva ad identificare successivamente la carta ogni qualvolta dovrà essere richiamata dall'utente (ad esempio specificare Athena CNS;
   b. Nel campo *Nome file modulo* cliccare il pulsante "Sfoglia" per selezionare il modulo PKCS#11; apparirà la seguente finestra:

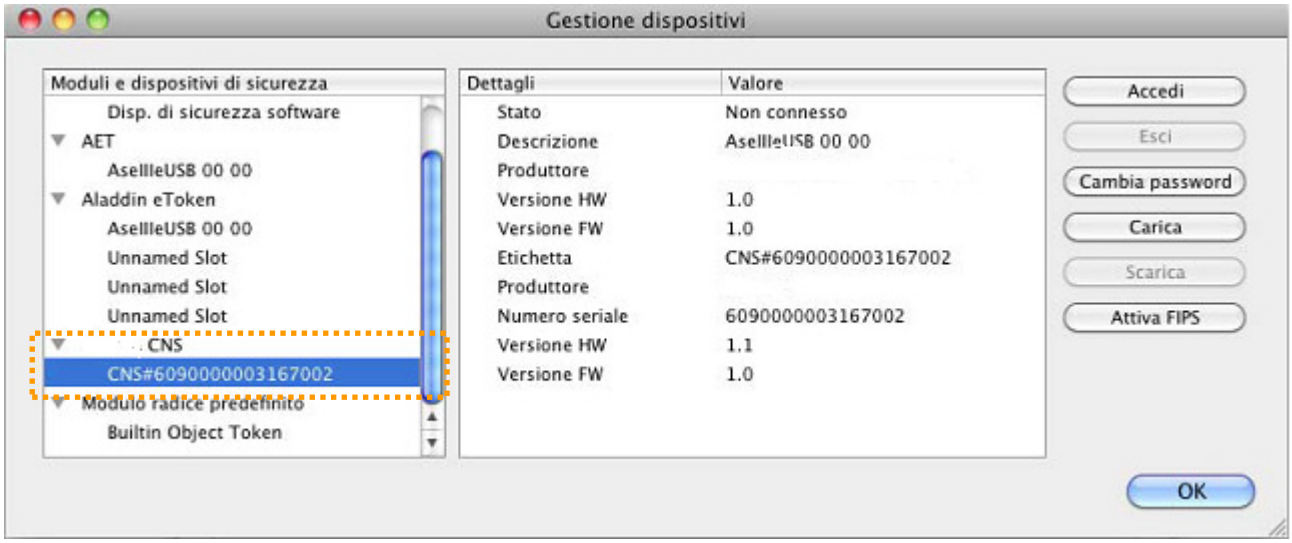


Inserire nel form “nome file modulo” la libreria “libASEP11.dylib” e cliccare sul pulsante “Ok” (digitare solo il nome delle libreria come è rafffigurato nell’immagine sottostantesenza cliccare sul pulsante Sfoglia)



6. Cliccare su *OK*

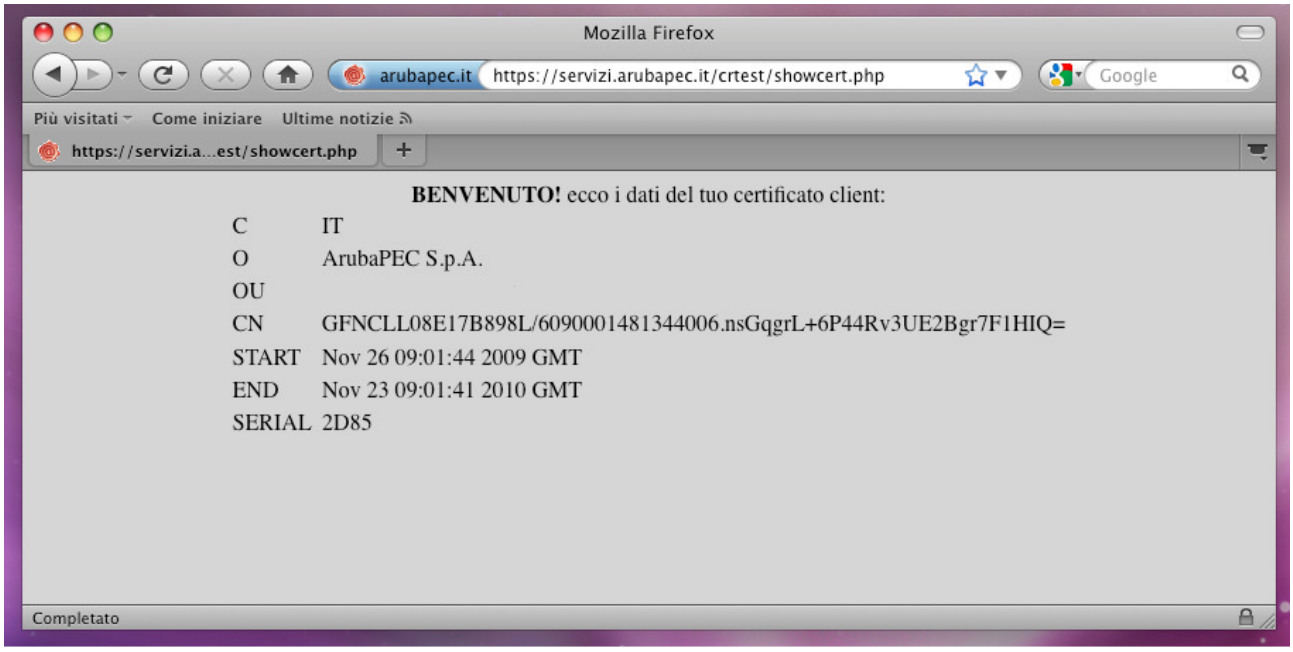
7. Verificare che all'interno della finestra *Gestioni dispositivi* compaia il nuovo modulo appena aggiunto e cliccare su *OK* (vedi figura seguente);



8. Chiudere la finestra *Preferenze;*
9. Collegarsi al seguente link tramite Firefox: https://servizi.arubapec.it/crtest/showcert.php;
10. Quando richiesto inserire il PIN della carta e cliccare su *OK* (vedi figura seguente);

11. Nella finestra di *Richiesta identificazione utente* selezionare il certificato di CNS e cliccare su *OK* (vedi figura seguente);

12. Verificare che, dopo l'inserimento del PIN, si riesca ad accedere ad una pagina contenente i dati del proprio certificato CNS (vedi figura seguente);

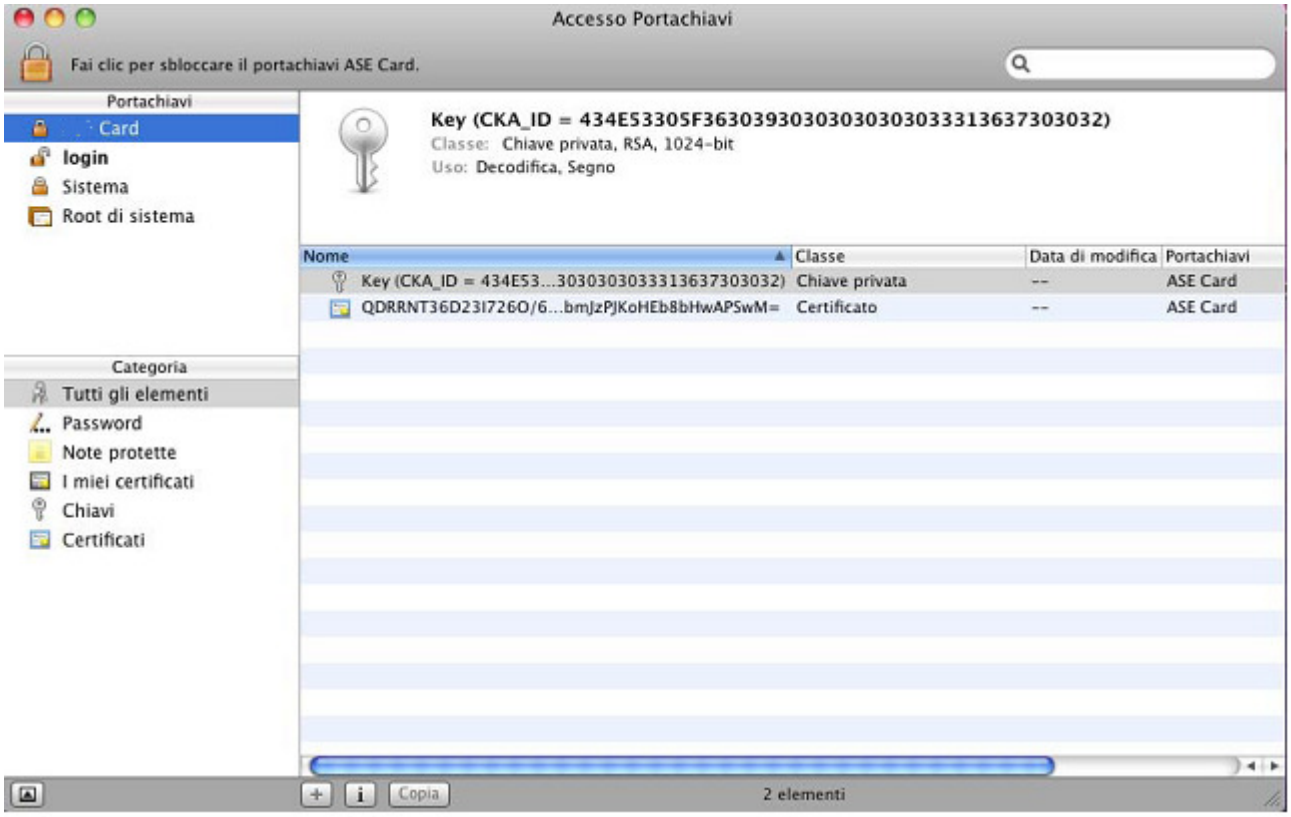


Se si riesce a visualizzare la pagina di benvenuto la funzionalità CNS e Firefox risultano correttamente configurati ed operativi.

4 Accesso portachiavi e Safari

Affinché la carta CNS sia utilizzabile anche dal browser Safari (vedere oltre) è necessario che essa risulti visibile dall'utility standard "Accesso Portachiavi". Questo dipende dal corretto funzionamento del componente ASE.tokend (vedere Paragrafo 2 "Installazione del software").

Per verificare la configurazione, lanciare "Accesso Portachiavi", quindi inserire la CNS nel lettore e attendere qualche istante: dovrebbe comparire un portachiavi di nome **"CNS Card"** nella parte in alto a sinistra della finestra, come mostrato nella figura seguente:



Cliccando poi sul portachiavi "ASE Card", nella parte destra della finestra dovrebbero comparire due righe che indicano la presenza, sulla carta, di una chiave privata e di un certificato.

Se compaiono queste due informazioni, ciò indica il regolare funzionamento del tokend.
A questo punto è possibile usare la carta CNS per autenticarsi sui siti web che lo richiedono, mediante il browser Safari o altre applicazioni basate sull'Accesso Portachiavi.

4.1 Autenticazione online con Safari

Quando il sito web che si sta “navigando” richiede l’autenticazione mediante CNS, il browser Safari visualizza una finestra del tipo seguente:

In questa finestra, con “password del portachiavi” si deve intendere il PIN della carta CNS.

Inserendo il PIN della carta e poi cliccando su OK, il browser eseguirà l’autenticazione on-line usando il certificato presente sulla CNS.

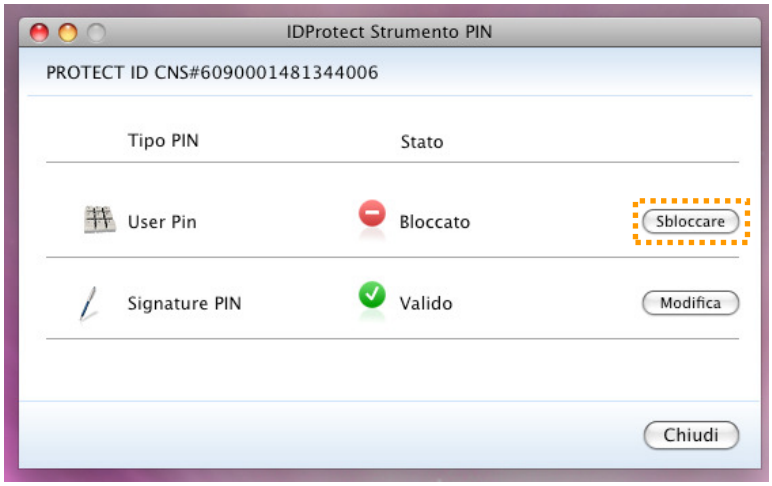
5 Sblocco della funzionalità CNS

Se, a seguito di un ripetuto inserimento di Pin non corretti, la propria CNS venga bloccata, è sufficiente seguire gli step descritti di seguito per procedere allo sblocco:

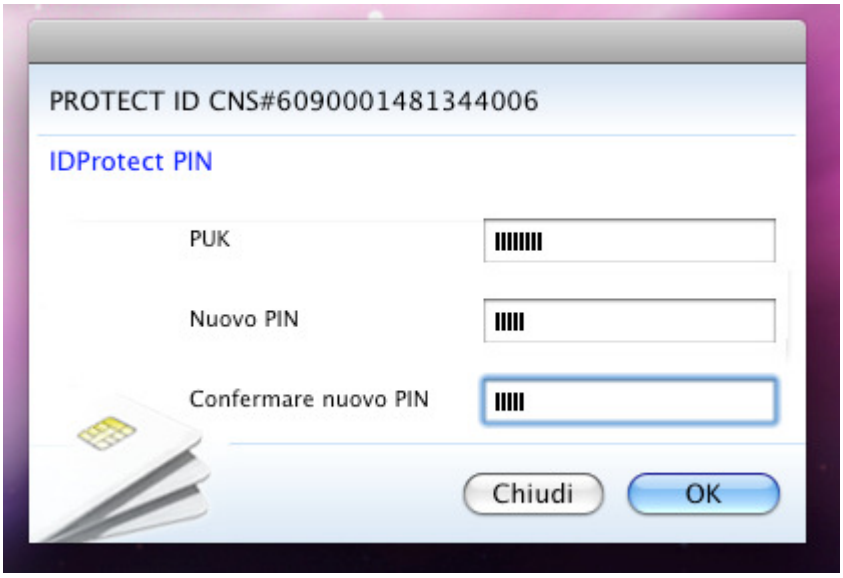
1. Assicurarsi che il lettore sia collegato al PC ed inserire la propria CNS prima di procedere;

2. Avviare il programma di gestione della CNS situato in: *Applicazioni → PIN Tool*

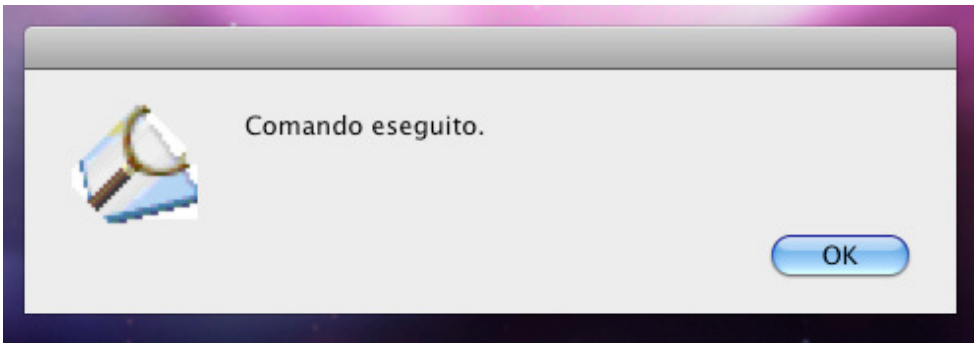
3. Assicurarsi che sia riportata lo stato di blocco del Pin e cliccare sulla voce Sbloccare (vedi figura seguente):



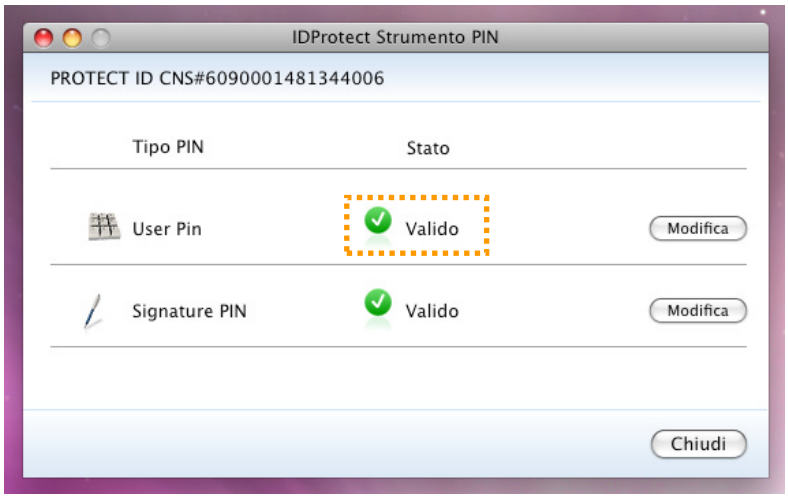
4. Inserire nel campo **PUK** il PUK della propria CNS e nei campi **Nuovo PIN** e **Conferma PIN** il nuovo PIN che s'intende assegnare alla carta (vedi figura seguente):



5. Cliccare sul pulsante OK ed attendere che venga mostrato il messaggio di avvenuto sblocco della carta (vedi figura seguente);



6. Verificare che la finestra di gestione del PIN riporti ora lo stato **Valido**;



7. CNS sbloccata con successo, chiudere il la finestra di gestione del PIN;

6 Risoluzione dei problemi più comuni

Puà capitare che la carta risulti “invisibile” dal browser Firefox e/o dalla utility “Accesso Portachiavi”, per motivi non riconducibili a difetti del middleware. I questi casi, spesso il problema si risolve in uno dei modi seguenti:

- estrarre la carta, quindi inserirla nuovamente ed attendere qualche istante;
- riavviare il Mac, assicurandosi che il lettore di smartcard sia sempre collegato.

Si raccomanda di tenere il lettore di smartcard sempre collegato al Mac, perché il suo scollegamento può determinare l’arresto di componenti di sistema operativo necessarie per l’uso della CNS.