



MIDDLEWARE CIE PER MAC OSx
MANUALE UTENTE
27/11/18

SOMMARIO

1. Middleware CIE – a cosa serve	3
2. Sistemi operativi supportati	3
3. Installazione del Middleware CIE	3
4. Rimozione del Middleware CIE	7
5. Primo utilizzo della CIE con il Middleware	7
6. Accesso ad un servizio online mediante il browser e la CIE	8
6.1 Safari e Chrome	9
6.2 Firefox	10
7. Gestione del PIN utente	18
7.1 Dov'è il PIN utente?.....	18
7.2 Cambio	19
7.3 Sblocco	20

1. Middleware CIE – a cosa serve

Il Middleware CIE è un software che consente di utilizzare la Carta di Identità elettronica per l'accesso sicuro in rete ai servizi web erogati dalle PP.AA.

Lo scenario di utilizzo tipico è l'accesso ad un servizio web di una P.A. (ad esempio all'area riservata dell'Agenzia delle Entrate) mediante il browser del computer (Safari, Chrome, Firefox, ecc.) in modo sicuro. In tale scenario il middleware CIE interagisce con il browser per realizzare, in maniera del tutto sicura e trasparente all'utente, la comunicazione con il microchip della CIE tramite il lettore di smart card.

All'utente è richiesto esclusivamente di inserire il PIN che ha ricevuto al momento della richiesta della CIE (1° parte) e della consegna di quest'ultima (2° parte) per autorizzare l'utilizzo della chiave crittografica presente all'interno del microchip della CIE, autorizzazione necessaria a completare il processo di autenticazione tra il browser e il servizio web.

2. Sistemi operativi supportati

La versione attuale del Middleware CIE può essere installata ed utilizzata su sistemi operativi Mac OS-X 10.12 o successivi.

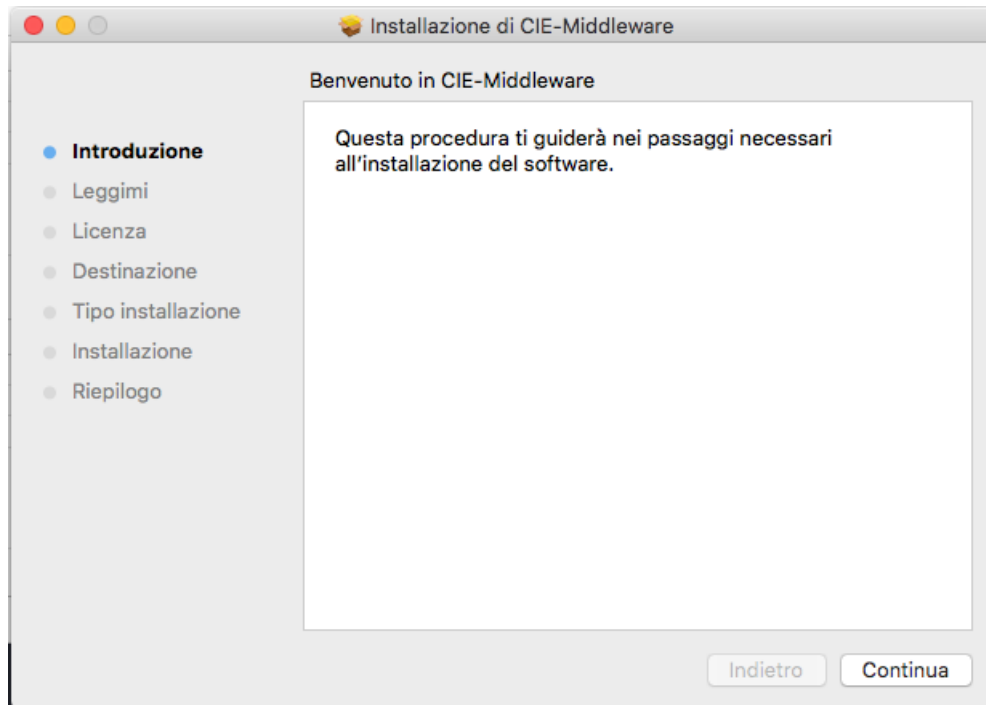
3. Installazione del Middleware CIE

Per installare il Middleware CIE è necessario disporre di un account con privilegi di amministratore. È necessario effettuare il download dell'ultima versione del middleware dal Portale CIE, www.cartaidentita.interno.gov.it, sezione "Servizi", sotto sezione "Software CIE" oppure dal sito developers.italia.it, sezione "CIE" nel caso in cui si sia interessati alle ultime versioni "beta" del software o al codice sorgente.

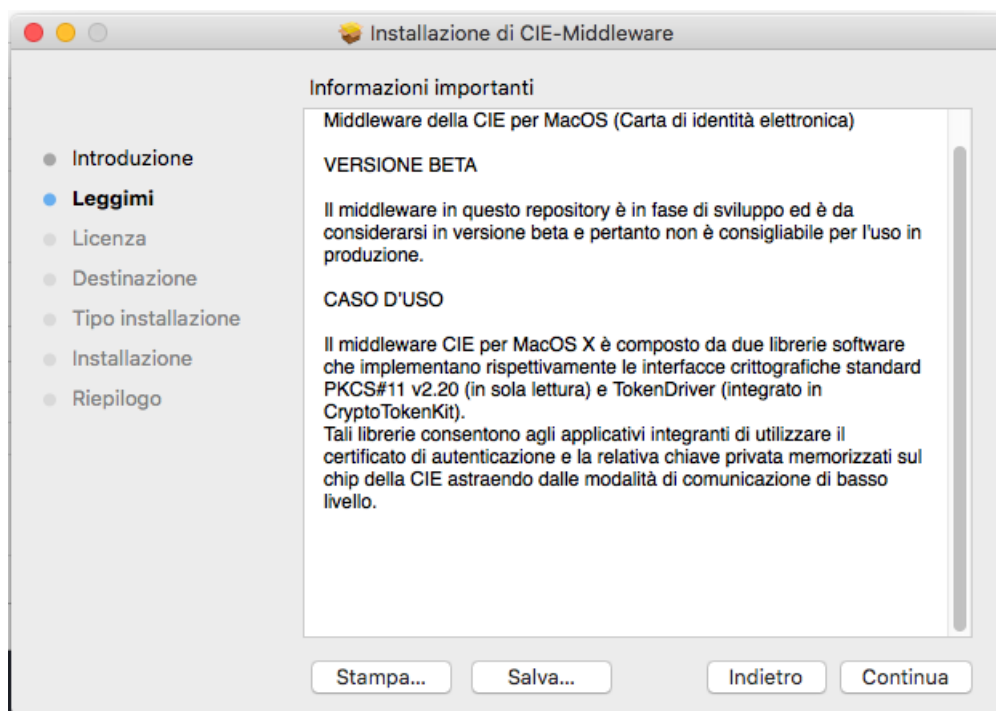
Terminato il download del pacchetto, effettuare un doppio click sul file "CIE-Middleware-<VERSIONE>.pkg" scaricato.



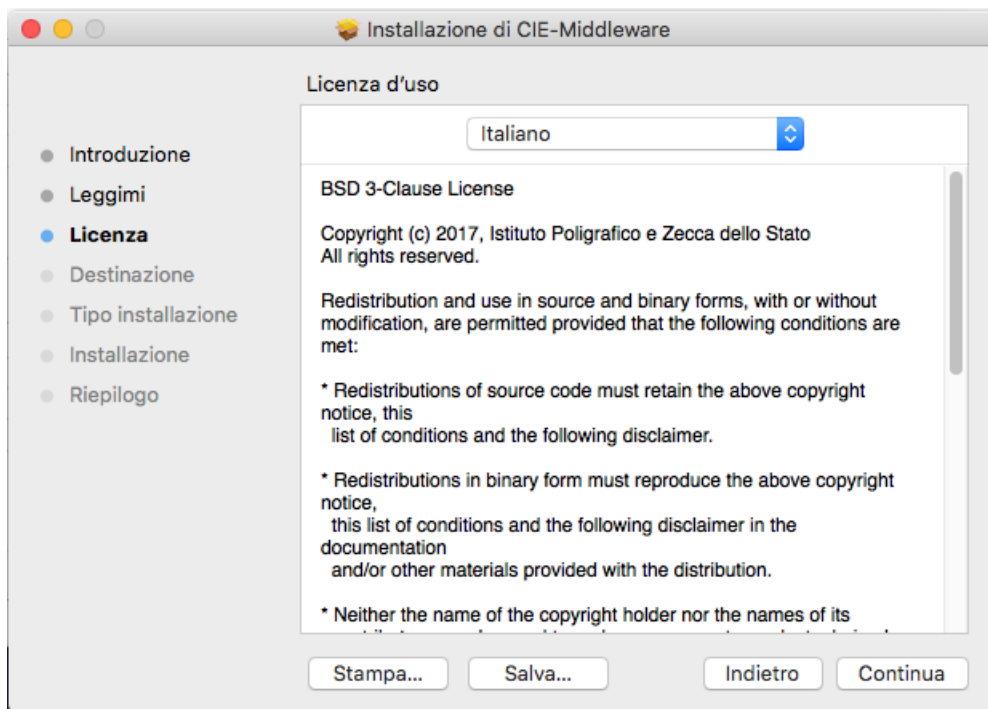
Comparirà la seguente schermata:



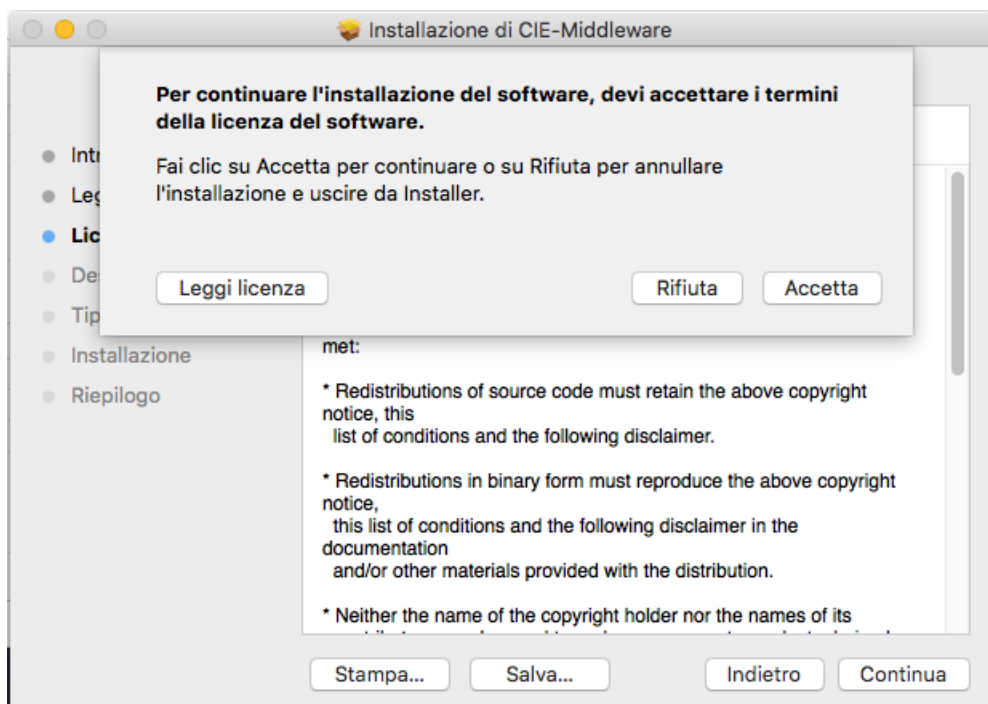
Cliccare sul tasto "Continua". Comparirà quindi la finestra di informazioni sul middleware della CIE che si sta installando.



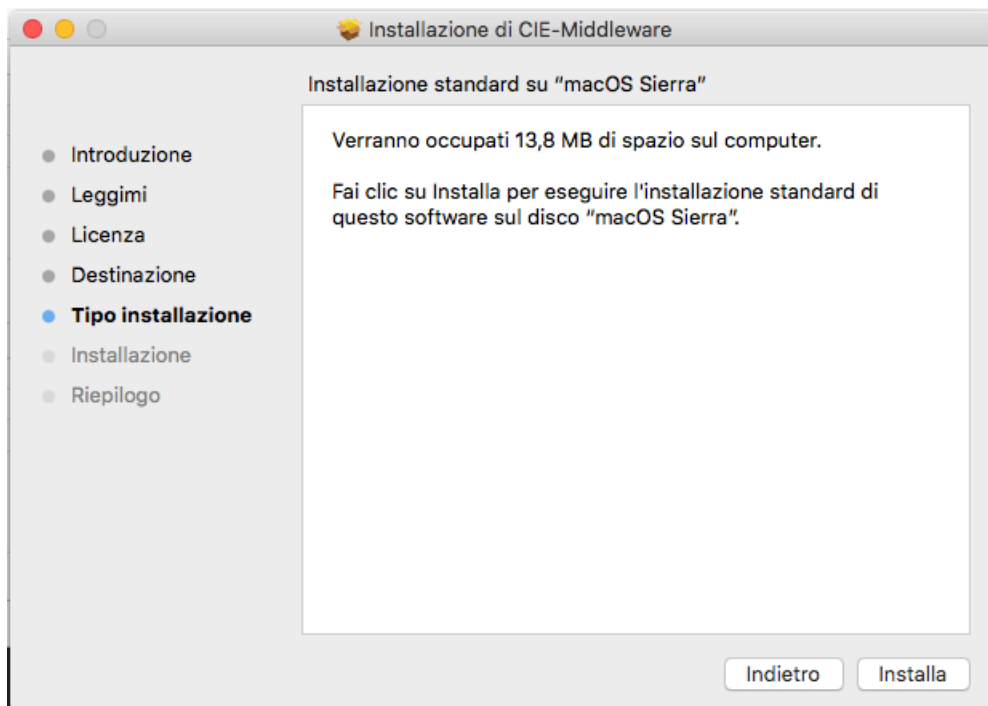
Cliccare sul tasto "Continua" per proseguire nella sezione "Licenza".



Leggere la licenza d'uso e Cliccare sul tasto "Continua".



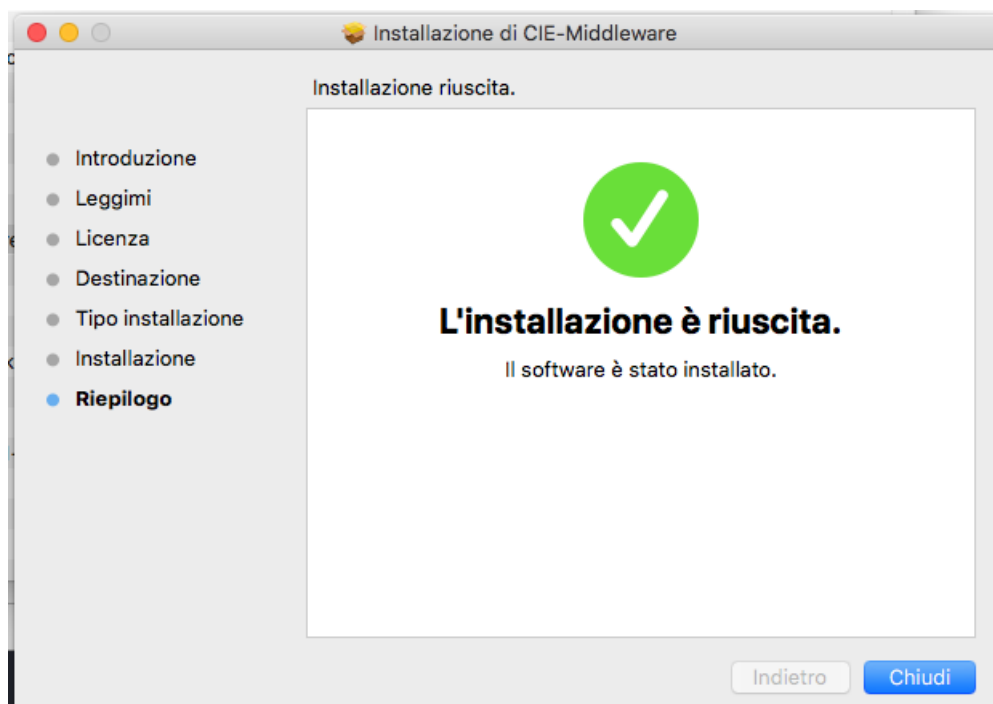
Cliccare su "Accetta" per proseguire con l'installazione.



Il middleware deve necessariamente essere installato sull'hard disk principale, non è possibile scegliere un disco secondario/esterno. Cliccare quindi su "Continua" per proseguire.

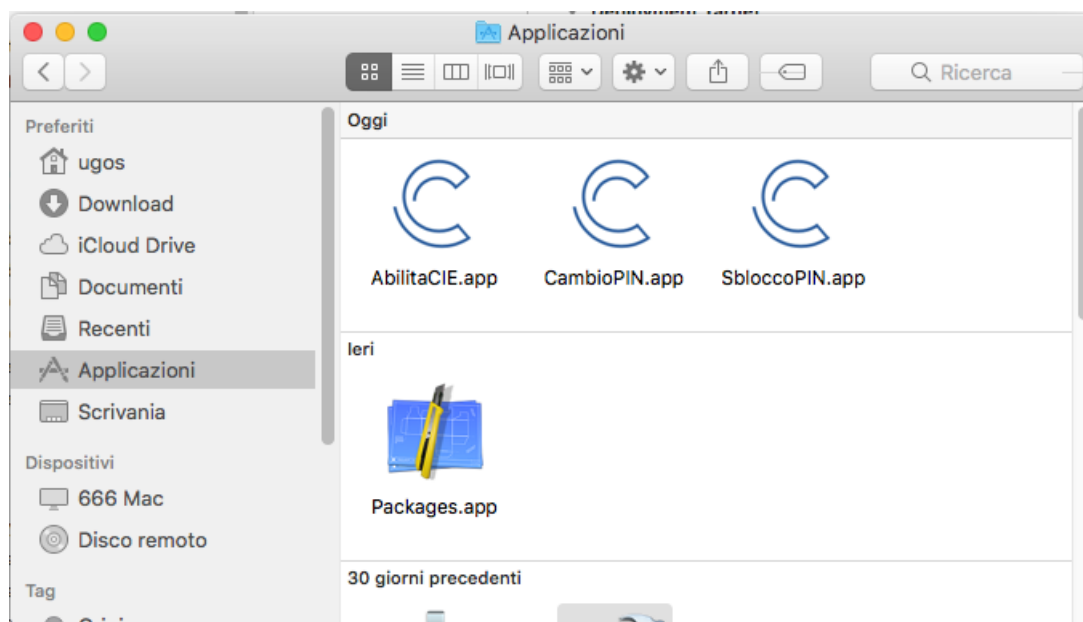
Cliccare su "Installa" per completare il processo di installazione. A questo punto verrà richiesta la password di un utente amministratore. Inserire la password e premere su "Installa Software".

Attendere il completamento dell'installazione, al termine della quale verrà mostrata la finestra di installazione riuscita.



Cliccare su "Chiudi" per terminare l'installazione.

In seguito all'installazione, nella cartella "Applicazioni" saranno presenti tre nuove app: "AbilitaCIE", "Cambio PIN" e "Sblocco PIN".



4. Rimozione del Middleware CIE

- Per rimuovere il software "CIE Middleware" è necessario rimuovere le app "AbilitaCIE", "Sblocco PIN" e "Cambio PIN" dalla cartella "Applicazioni" e il file `/Library/ipzs/libcie-pkcs11.dylib`.

5. Primo utilizzo della CIE con il Middleware

Al primo utilizzo di una CIE, "CIE Middleware" richiede che venga effettuato un processo di verifica per assicurarsi che la carta sia valida e i dati contenuti in essa siano corretti. Questo processo viene eseguito solo una volta; al successivo utilizzo non sarà necessario ripetere questa operazione. Durante il processo è necessario inserire il PIN per esteso.

La procedura viene avviata, lanciando l'app "AbilitaCIE" presente sotto la cartella "Applicazioni". Viene presentata una schermata come quella di seguito. Lasciando la CIE posizionata sul lettore, digitare il PIN e premere "Abilita".



Attenzione! In fase di abilitazione verranno richieste tutte le 8 cifre del PIN. Successivamente, durante il normale utilizzo sarà necessario inserire solo le ultime 4 cifre.

Viene quindi avviata la procedura di controllo. Al termine, la CIE sarà abilitata all'uso e verrà visualizzato il messaggio di CIE abilitata. Cliccare su "Annulla" per terminare.

6. Accesso ad un servizio online mediante il browser e la CIE

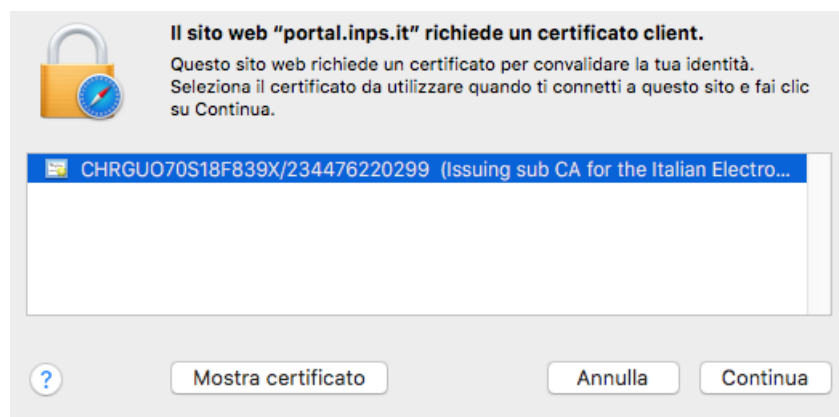
La CIE può essere utilizzata per accedere ai servizi online erogati dalle Pubbliche Amministrazioni, che accettano la modalità di autenticazione mediante Carta di identità elettronica.

La procedura di autenticazione richiede sempre l'inserimento del PIN e, sulla base del browser utilizzato può richiedere delle operazioni di configurazione aggiuntiva, come descritto nei paragrafi seguenti.

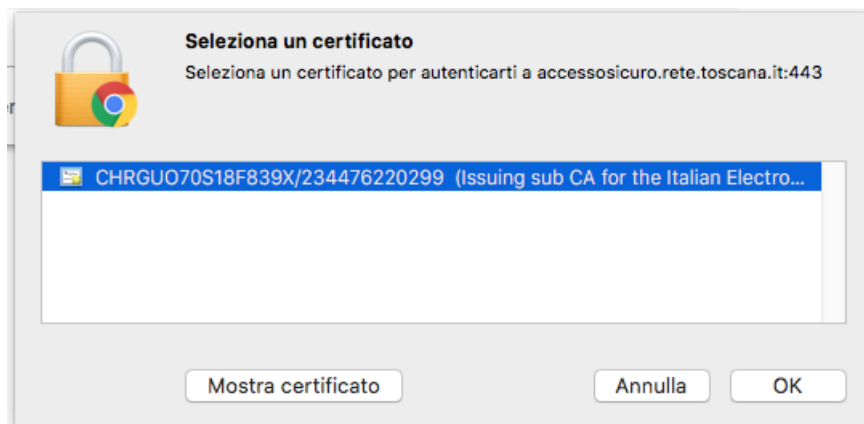
6.1 Safari e Chrome

L'autenticazione tramite CIE su Safari e Chrome non richiede alcuna operazione di configurazione aggiuntiva a quanto descritto nei paragrafi precedenti.

Appoggiare la CIE sul lettore smart card e digitare l'indirizzo del servizio a cui si vuole accedere nella barra degli indirizzi del browser. Nel caso si sia già effettuata la procedura di primo utilizzo della CIE o dopo averla in ogni caso completata, verrà richiesto quale certificato utilizzare per l'autenticazione. Selezionare il certificato CIE, riconoscibile dal codice fiscale del titolare, e premere OK.

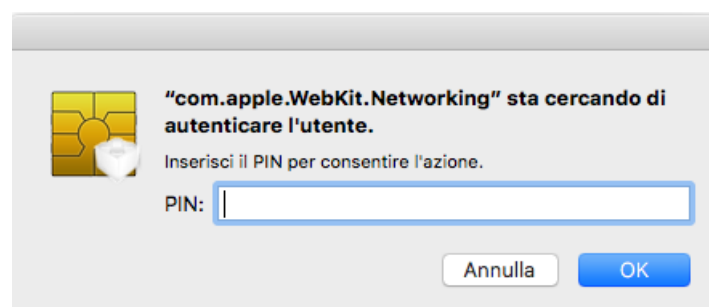


Su Chrome la finestra di selezione del certificato è la seguente:

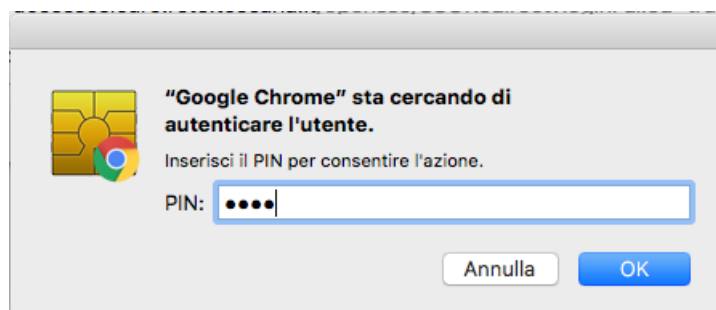


Confermato il certificato da utilizzare, verrà richiesto di immettere il PIN della CIE.

Su Safari:



Su Chrome:



Digitare le ultime 4 cifre del PIN, premere su OK e attendere qualche secondo (la finestra di richiesta PIN non scompare immediatamente). L'applicazione dovrebbe riconoscere correttamente l'utente e consentire l'accesso al servizio.

Nel caso in cui venga inserito un PIN errato viene mostrata nuovamente la finestra di inserimento PIN.

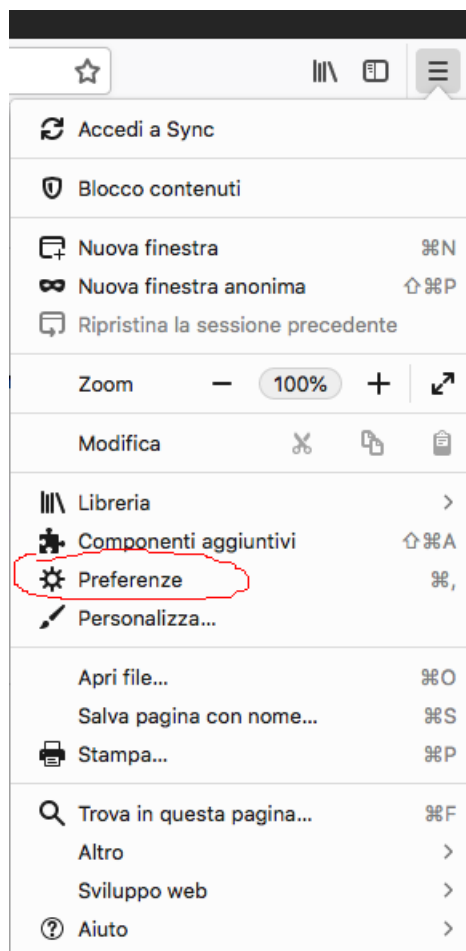
Se il PIN viene digitato in modo errato per 3 volte consecutive quest'ultimo viene bloccato per sicurezza. Per sbloccarlo sarà necessario lanciare l'app "Sblocca PIN" nella cartella "Applicazioni".

Consultare il paragrafo §7.3 Sblocco per ulteriori dettagli in merito alla procedura di sblocco PIN.

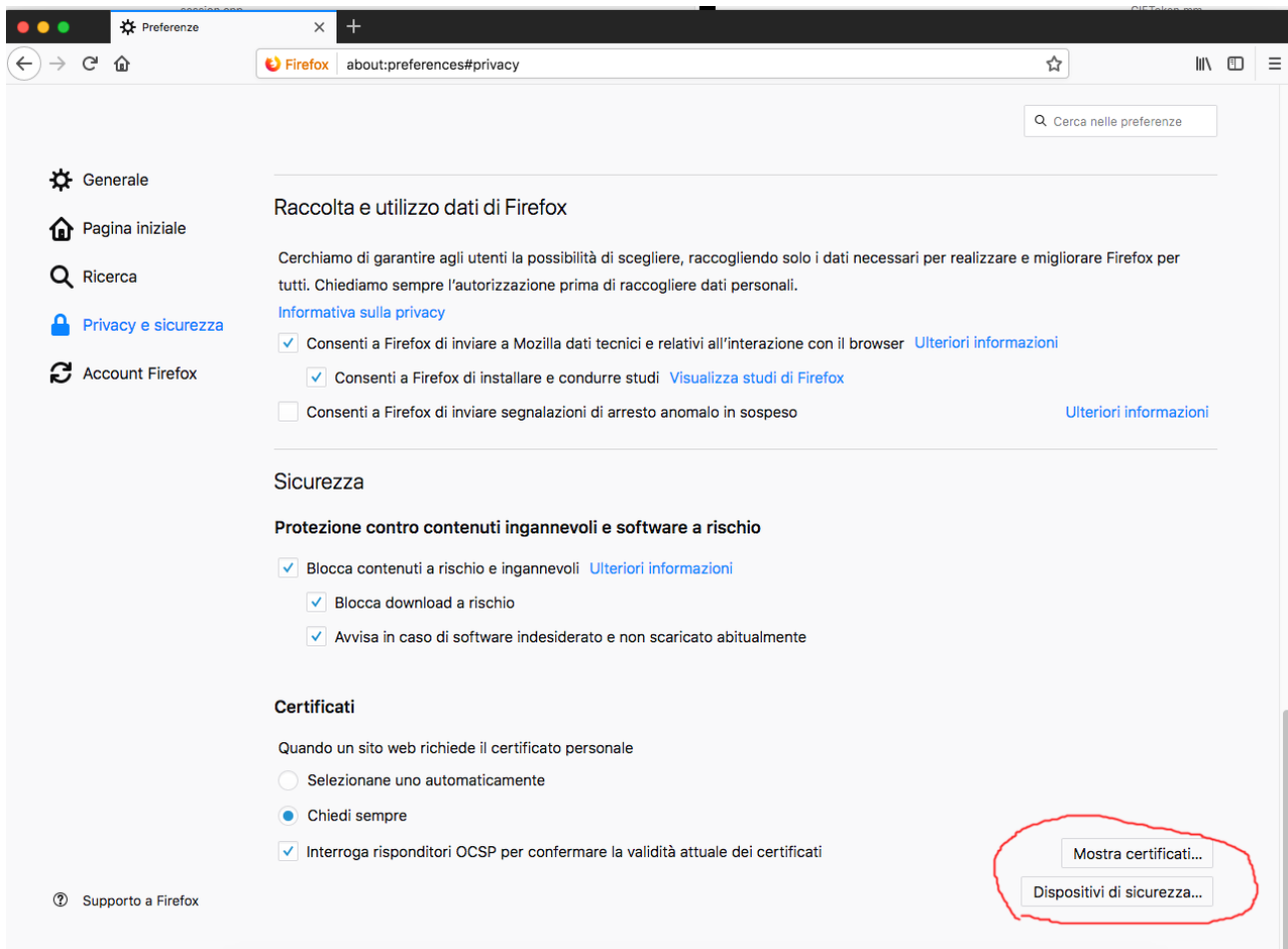
6.2 Firefox

Per utilizzare la CIE con il browser Firefox è necessario apportare a quest'ultimo una configurazione diversa, attenendosi ai passi sottostanti.

Accedere alla sezione "Preferenze" del browser:



Selezionare la scheda “Privacy e Sicurezza”



The screenshot shows the Firefox Preferences window, specifically the 'Privacy e sicurezza' (Privacy and Security) section. The 'Raccolta e utilizzo dati di Firefox' (Firefox Data Collection and Use) section is expanded, showing three checkboxes: 'Consenti a Firefox di inviare a Mozilla dati tecnici e relativi all'interazione con il browser' (checked), 'Consenti a Firefox di installare e condurre studi' (checked), and 'Consenti a Firefox di inviare segnalazioni di arresto anomalo in sospeso' (unchecked). The 'Sicurezza' (Security) section is also expanded, showing 'Protezione contro contenuti ingannevoli e software a rischio' (Protection against deceptive content and risky software) with three checkboxes: 'Blocca contenuti a rischio e ingannevoli' (checked), 'Blocca download a rischio' (checked), and 'Avvisa in caso di software indesiderato e non scaricato abitualmente' (checked). The 'Certificati' (Certificates) section is expanded, showing 'Quando un sito web richiede il certificato personale' (When a website requests a personal certificate) with three radio buttons: 'Selezionane uno automaticamente' (selected), 'Chiedi sempre' (unchecked), and 'Interroga risponditori OCSP per confermare la validità attuale dei certificati' (checked). A red circle highlights the 'Mostra certificati...' (Show certificates...) button in the bottom right corner.

Preferenze

about:preferences#privacy

Cerca nelle preferenze

Generale

Pagina iniziale

Ricerca

Privacy e sicurezza

Account Firefox

Raccolta e utilizzo dati di Firefox

Cerchiamo di garantire agli utenti la possibilità di scegliere, raccogliendo solo i dati necessari per realizzare e migliorare Firefox per tutti. Chiediamo sempre l'autorizzazione prima di raccogliere dati personali.

[Informativa sulla privacy](#)

- ☒ Consenti a Firefox di inviare a Mozilla dati tecnici e relativi all'interazione con il browser [Ulteriori informazioni](#)
- ☒ Consenti a Firefox di installare e condurre studi [Visualizza studi di Firefox](#)
- ☐ Consenti a Firefox di inviare segnalazioni di arresto anomalo in sospeso [Ulteriori informazioni](#)

Sicurezza

Protezione contro contenuti ingannevoli e software a rischio

- ☒ Blocca contenuti a rischio e ingannevoli [Ulteriori informazioni](#)
- ☒ Blocca download a rischio
- ☒ Avvisa in caso di software indesiderato e non scaricato abitualmente

Certificati

Quando un sito web richiede il certificato personale

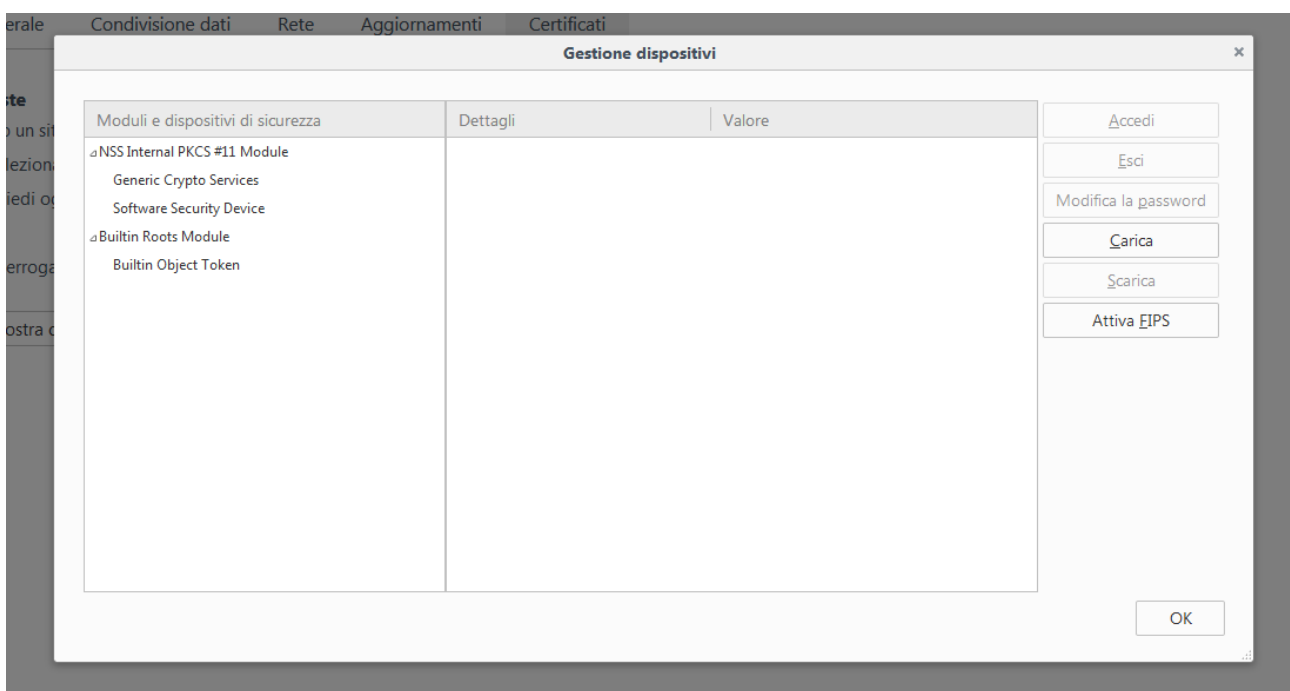
- ☐ Selezionane uno automaticamente
- ☒ Chiedi sempre
- ☒ Interroga risponditori OCSP per confermare la validità attuale dei certificati

Supporto a Firefox

Mostra certificati...

Dispositivi di sicurezza...

Cliccare su "Dispositivi di sicurezza".



The screenshot shows the 'Gestione dispositivi' (Device Management) window. It has a tabbed interface with 'Certificati' (Certificates) selected. The main area is divided into two columns: 'Moduli e dispositivi di sicurezza' (Security Modules and Devices) and 'Dettagli' (Details). The 'Moduli e dispositivi di sicurezza' column lists the following items: 'NSS Internal PKCS #11 Module', 'Generic Crypto Services', 'Software Security Device', 'Builtin Roots Module', and 'Builtin Object Token'. The 'Dettagli' column is empty. The 'Valore' (Value) column is also empty. On the right side, there are several buttons: 'Accedi' (Access), 'Esci' (Exit), 'Modifica la password' (Change password), 'Carica' (Load), 'Scarica' (Download), and 'Attiva EIPS' (Activate EIPS). An 'OK' button is located at the bottom right.

Condivisione dati

Rete

Aggiornamenti

Certificati

Gestione dispositivi

Moduli e dispositivi di sicurezza	Dettagli	Valore
NSS Internal PKCS #11 Module		
Generic Crypto Services		
Software Security Device		
Builtin Roots Module		
Builtin Object Token		

Accedi

Esci

Modifica la password

Carica

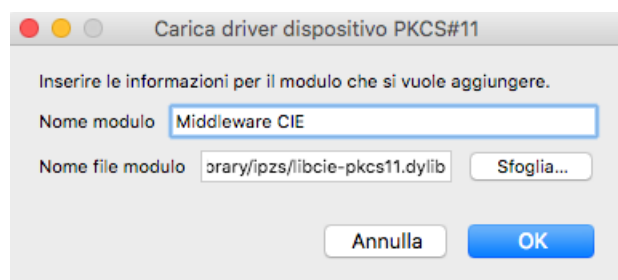
Scarica

Attiva EIPS

OK

Cliccare su “Carica” e inserire le seguenti informazioni:

- Nome modulo: Middleware CIE
- Nome file modulo: /Library/ipzs/libcie-pkcs11.dylib



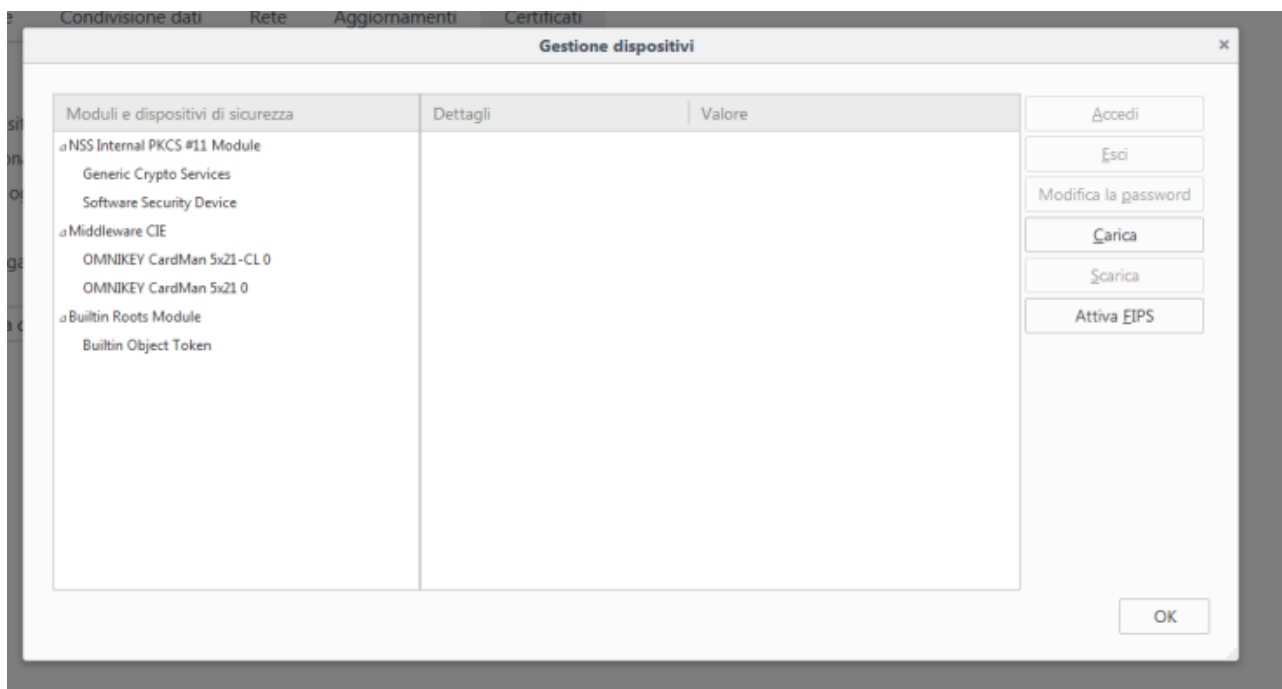
Carica driver dispositivo PKCS#11

Inserire le informazioni per il modulo che si vuole aggiungere.

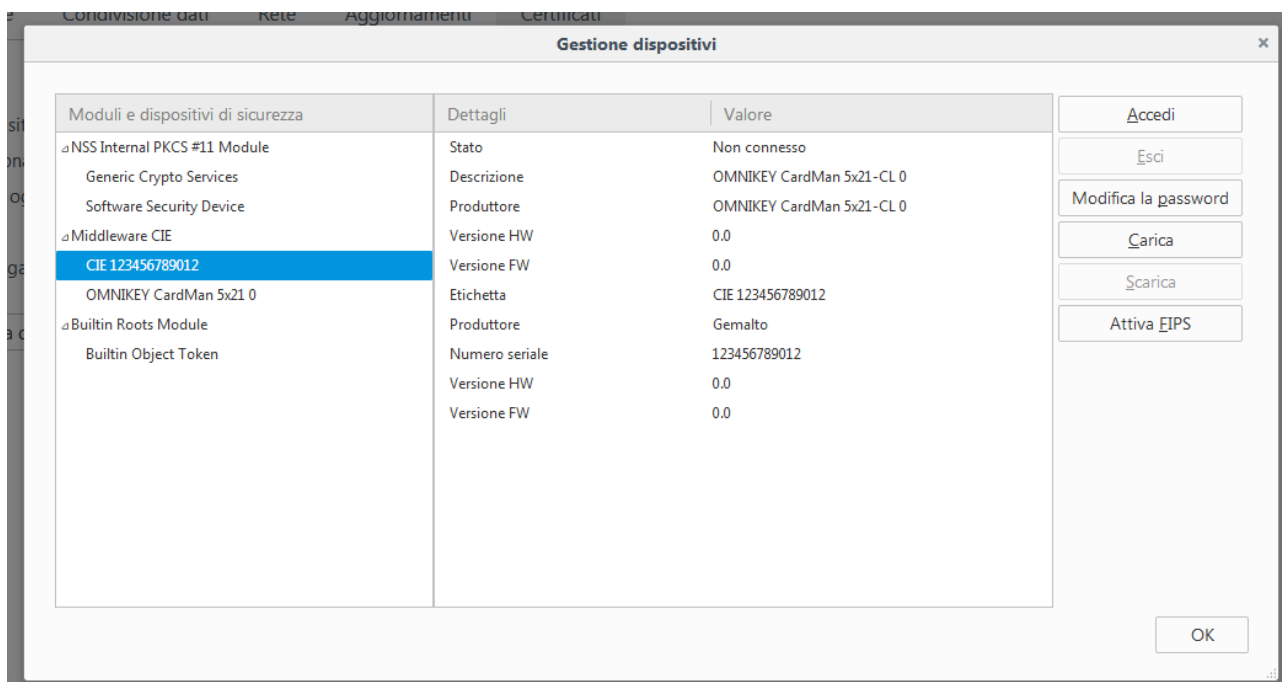
Nome modulo

Nome file modulo

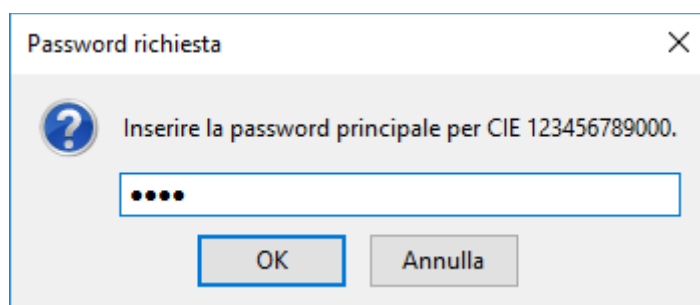
Se è la prima volta che si utilizza la CIE, sarà necessario completare preventivamente la procedura di prima registrazione riportata nel paragrafo 5. Se tutto va a buon fine, il modulo comparirà nella lista di sinistra, con l'elenco dei lettori di smart card installati sul computer:



Appoggiando la CIE sul lettore questa verrà riconosciuta dal browser e verranno visualizzate delle informazioni.



Per verificare la corretta installazione tornare alla scheda “Avanzate”, e, lasciando la CIE appoggiata sul lettore, cliccare su “Certificati”. Verrà richiesto il PIN della CIE. Digitare le ultime 4 cifre del PIN e premere su OK.



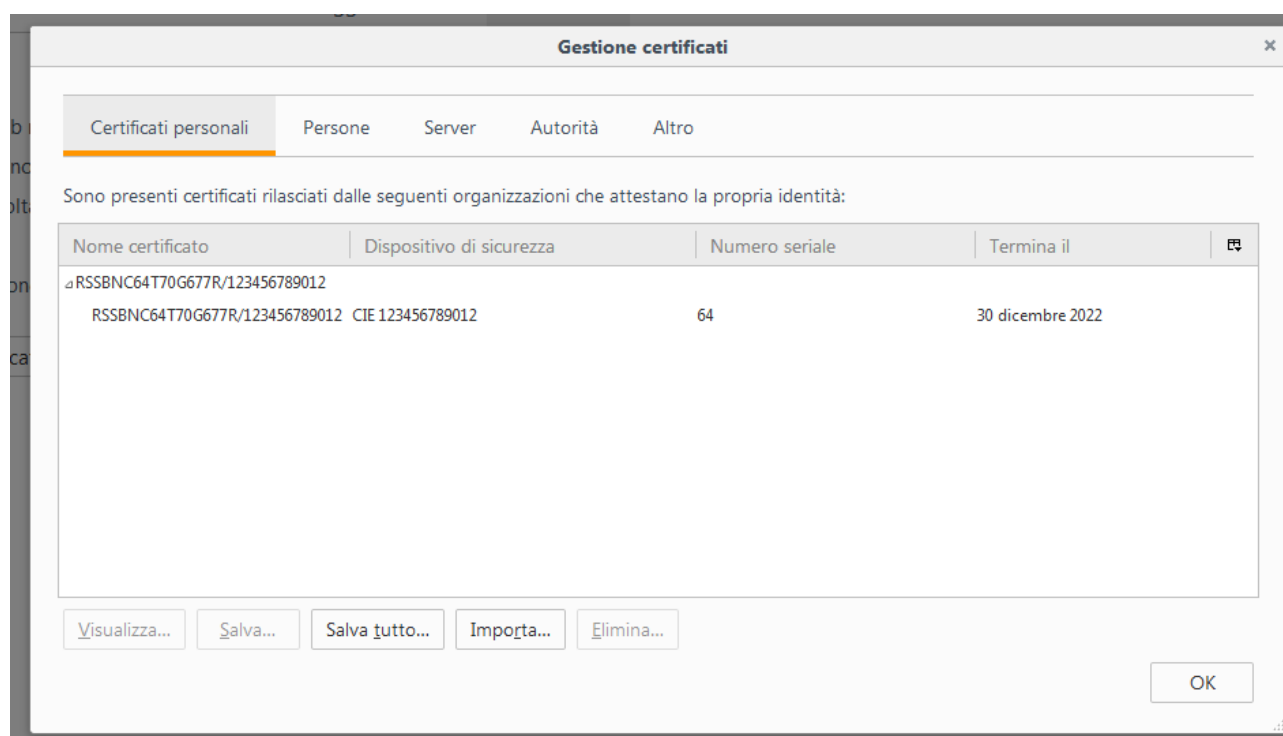
Password richiesta

Inserire la password principale per CIE 123456789000.

••••

OK Annulla

Nella scheda “Certificati Personali” comparirà il certificato di autenticazione dell’utente, riconoscibile dal codice fiscale.



Gestione certificati

Certificati personali Persone Server Autorità Altro

Sono presenti certificati rilasciati dalle seguenti organizzazioni che attestano la propria identità:

Nome certificato	Dispositivo di sicurezza	Numero seriale	Termina il
RSSBNC64T70G677R/123456789012	RSSBNC64T70G677R/123456789012 CIE 123456789012	64	30 dicembre 2022

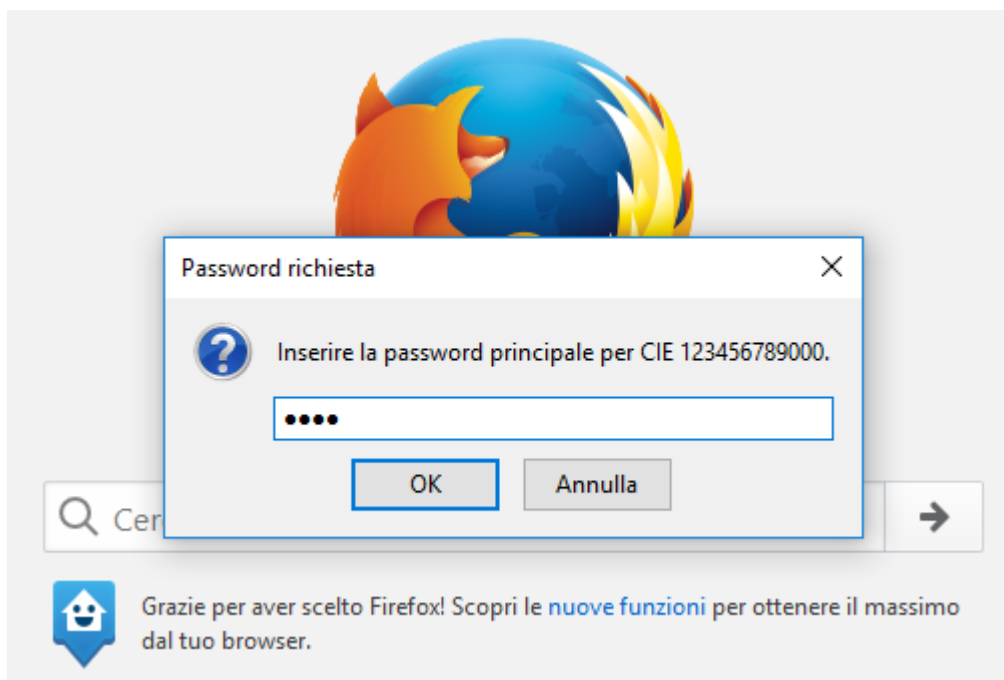
Visualizza... Salva... Salva tutto... Importa... Elimina...

OK

La configurazione a questo punto è stata eseguita correttamente. All’avvio successivo di Firefox non sarà necessario ripetere questa operazione.

Per utilizzare la CIE nell’accesso ad un servizio erogato da una Pubblica Amministrazione, appoggiare la carta sul lettore smart card e digitare l’indirizzo del servizio a cui si vuole accedere nella barra degli indirizzi del browser Firefox.

All'avvio della connessione verrà richiesto il PIN della CIE. Inserire le ultime 4 cifre del PIN.



Verrà poi richiesto di selezionare il certificato da utilizzare per l'autenticazione client. Selezionare il certificato CIE, riconoscibile dal codice fiscale del titolare, e premere OK.



Richiesta identificazione utente

Questo sito richiede che ci si identifichi tramite un certificato:
localhost:443
Organizzazione: ""
Rilasciato da: ""

Scegliere un certificato da presentare come identificativo:
RSSBNC64T70G677R/123456789000 [64]

Dettagli del certificato selezionato:

Rilasciato a: serialNumber=IDCIT-CA00000AA,CN=RSSBNC64T70G677R/123456789000,givenName=BIANCA,SN=ROSSI,C=IT
Numero seriale: 64
Valido dal mercoledì 30 maggio 2012, 00:00:00 al venerdì 30 dicembre 2022, 00:00:00
Ambiti di utilizzo della chiave: Firma
Rilasciato da: C=IT,CN=TestCA

☒ Ricorda questa scelta

OK Annulla

L'applicazione dovrebbe riconoscere correttamente l'utente e consentire l'accesso al servizio desiderato.

Attenzione: nel caso in cui venga inserito un PIN errato o il PIN sia bloccato, Firefox non restituisce alcun messaggio d'errore all'utente, ma ripropone la finestra di inserimento PIN. Verificare accuratamente il PIN inserito per evitare il blocco accidentale della CIE.

Consultare il paragrafo §7.3 Sblocco per ulteriori dettagli in merito alla procedura di sblocco PIN.

7. Gestione del PIN utente

7.1 Dov'è il PIN utente?

I codici PIN e PUK vengono comunicati al titolare della CIE in due parti. La prima parte durante la richiesta del documento presso gli uffici comunali. La seconda parte si trova sul foglio di accompagnamento a cui è attaccata la CIE, all'interno della busta sigillata che il cittadino riceve a casa o ritira al Comune.

Prima parte del PIN:






Prima metà del PIN

1234

Prima metà del PUK

8765

Seconda parte del PIN:

	MINISTERO DELL'INTERNO		CARTA DI IDENTITÀ ELETTRONICA
<p>Le invio, allegata alla presente, la Carta di Identità Elettronica che costituisce documento di identificazione e, salva l'indicazione "NON VALIDA PER L'ESPATRIO", anche di viaggio in tutti gli Stati membri dell'Unione Europea ed in quelli che hanno aderito a specifici accordi con lo Stato Italiano.</p>			
			
		PIN	5678
		PUK	4321

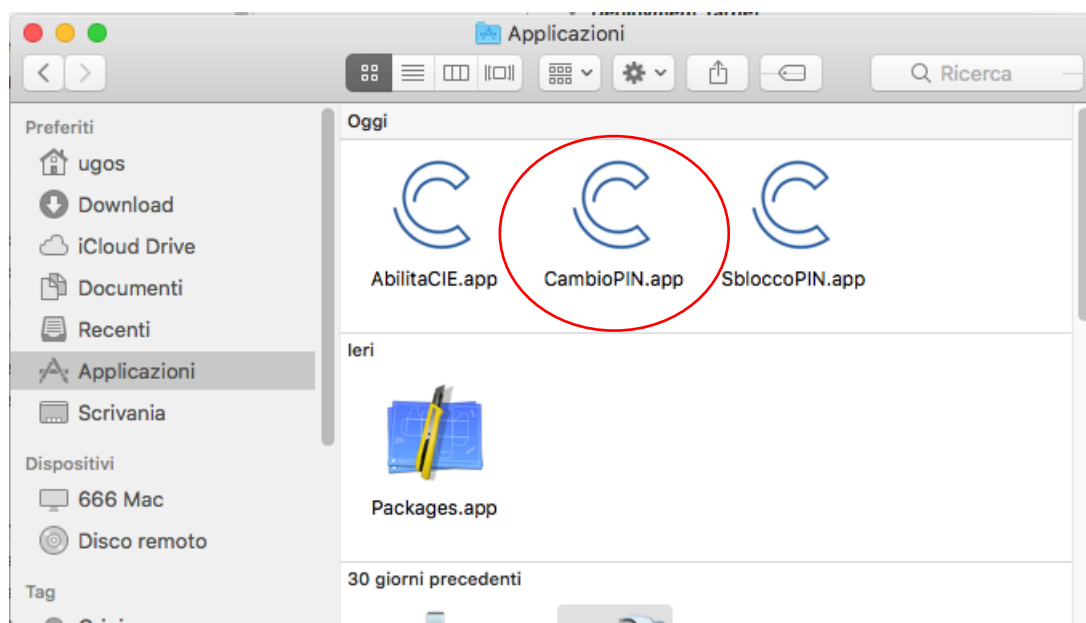
In questo caso il PIN completo è **12345678** e il PUK è **87654321**.

In seguito all'abilitazione verranno sempre richieste **solo le ultime 4 cifre del PIN**. Nel caso in esempio **5678**.

7.2 Cambio

Il PIN della CIE può essere modificato per intero (tutte e 8 le cifre) con un nuovo PIN che il titolare può ricordare più facilmente. Non è possibile impostare valori facilmente intelligibili (es. un PIN di tutte cifre uguali o di cifre consecutive)

Per cambiare il PIN, appoggiare la CIE sul lettore di smart card e avviare l'app "Cambio PIN" nella cartella "Applicazioni":



Inserire le 8 cifre del PIN attuale della CIE, Inserire quindi due volte le 8 cifre del nuovo PIN rispettivamente nei campi "Nuovo PIN" e "Conferma" (per evitare che, a causa di errori di digitazione, il PIN venga impostato ad un valore diverso da quello desiderato):

A screenshot of a 'Cambio PIN' (Change PIN) dialog box. The title bar says 'Cambio PIN'. On the left, there is a logo for 'CARTA DI IDENTITÀ ELETTRONICA' (Electronic Identity Card). The main text says: 'Per cambiare il PIN digitare il PIN corrente, il nuovo PIN e la conferma del nuovo PIN'. There are three input fields: 'PIN Corrente' (Current PIN), 'Nuovo PIN' (New PIN), and 'Conferma Nuovo PIN' (Confirm New PIN). At the bottom, there are two buttons: 'Cambia' (Change) and 'Annulla' (Cancel).

Nel caso in cui la seconda digitazione del PIN non corrisponda alla prima l'applicazione avverte l'utente dell'errore. Se il PIN iniziale è invece digitato correttamente per due volte, avviene il cambio e viene mostrata una finestra di conferma.

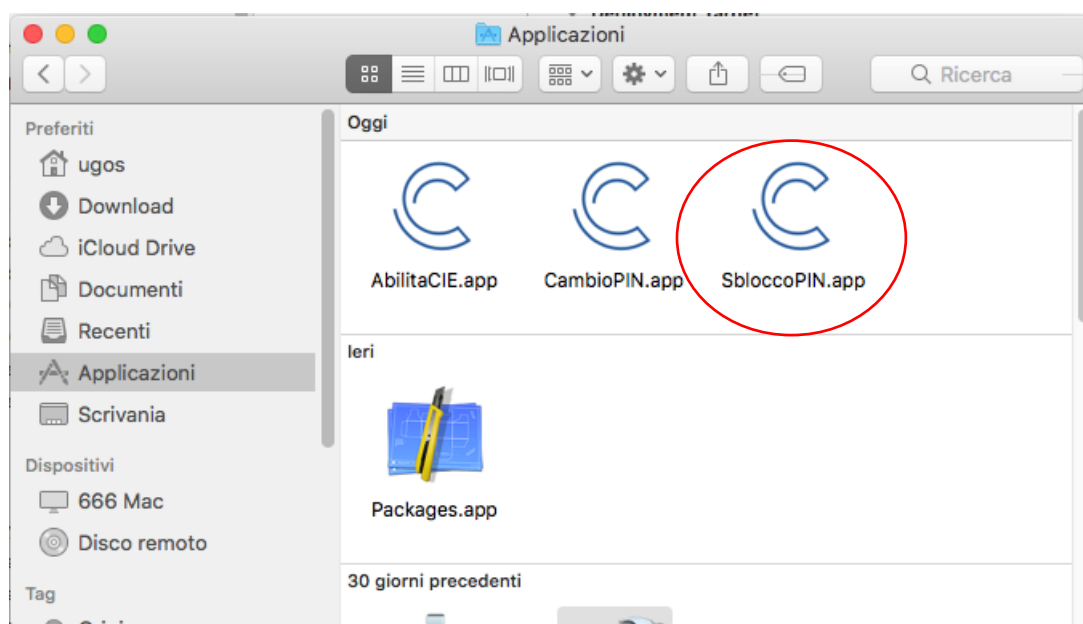
Se il PIN iniziale non corrisponde a quello digitato verrà visualizzata una schermata di errore in cui è specificato il numero di tentativi rimanenti prima di bloccare il PIN.

In caso di blocco del PIN è necessario procedere allo sblocco tramite il PUK. Consultare il paragrafo §7.3 Sblocco per ulteriori dettagli in merito alla procedura di sblocco PIN.

7.3 Sblocco

In caso di blocco del PIN questo deve essere sbloccato e reimpostato inserendo il PUK.

Per sbloccare il PIN appoggiare la CIE sul lettore di smart card e avviare l'app "Sblocco PIN" dalla cartella "Applicazioni":



Digitare il PUK della CIE, digitare le 8 cifre del nuovo PIN. Inserire il nuovo PIN e premere OK. Il nuovo PIN deve essere digitato 2 volte per evitare che a causa di errori di digitazione esso venga impostato ad un valore diverso da quello desiderato:



Nel caso in cui la seconda digitazione del PIN non corrisponda alla prima, l'applicazione avvisa l'utente con un apposito messaggio.

Se il PUK iniziale è stato digitato correttamente, il PIN viene sbloccato e impostato al nuovo valore. All'utente viene mostrata una finestra di conferma.

Se il PUK non corrisponde a quello digitato, viene visualizzata una schermata di errore in cui è specificato il numero di tentativi rimanenti prima di bloccare il PUK.

ATTENZIONE: In caso di blocco del PUK non sarà possibile procedere né al suo sblocco né a quello del PIN.