



MINISTERO
DELL'INTERNO



POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO



CARTA
DI IDENTITÀ
ELETTRONICA

MIDDLEWARE CIE
MANUALE UTENTE
01/11/18

SOMMARIO

1. Middleware CIE – a cosa serve.....	3
2. Sistemi operativi supportati.....	3
3. Installazione del Middleware CIE.....	3
4. Rimozione del Middleware CIE.....	5
5. Primo utilizzo della CIE con il Middleware.....	7
6. Accesso ad un servizio mediante il browser e la CIE.....	8
6.1 MS Internet Explorer, MS Edge, Chrome e Opera.....	10
6.2 Firefox.....	13
7. Gestione del PIN utente.....	20
7.1 Dov'è il PIN utente?.....	20
7.2 Cambio.....	21
7.3 Sblocco.....	23

1. Middleware CIE – a cosa serve

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

L'esempio di utilizzo più frequente è l'accesso ad un servizio di una P.A. (ad esempio Agenzia delle Entrate) mediante il browser del computer (Internet Explorer, Firefox, Opera ecc.) in modo sicuro per il tramite della CIE: il middleware CIE interagisce con il browser per realizzare, in maniera del tutto sicura e trasparente all'utente, la comunicazione fra il lettore di smart card e il microprocessore della CIE.

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 sbloccare l'utilizzo della chiave e portare a termine il processo di autenticazione.

2. Sistemi operativi supportati

La versione attuale del Middleware CIE può essere installata ed utilizzata su sistemi operativi Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10 e su Linux (con pacchettizzazione per Debian/Ubuntu). I seguenti screenshot sono stati catturati dalle schermate per Windows, su Linux il contenuto informativo è il medesimo ma il look&feel delle finestre potrebbe essere diverso a seconda della distribuzione.

3. Installazione del Middleware CIE

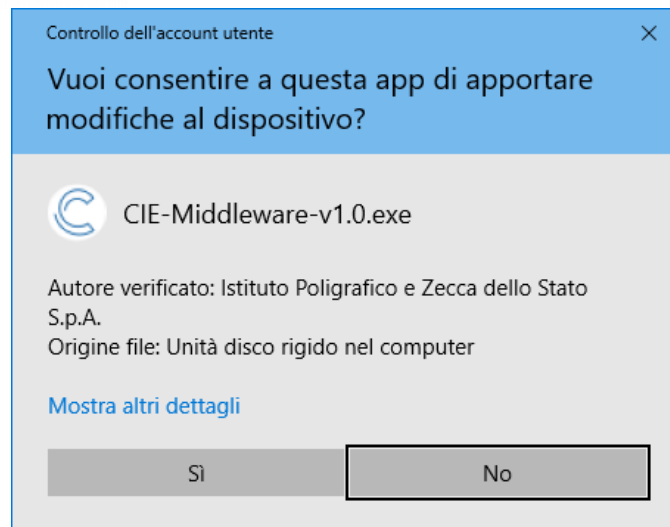
WINDOWS

Per installare il Middleware CIE è necessario disporre di un account con privilegi di amministratore. Effettuare il download del middleware dal Portale CIE, www.cartaidentita.interno.gov.it, sezione "La carta", sotto sezione "Il Microprocessore" oppure dal sito developers.italia.it, sezione "CIE".

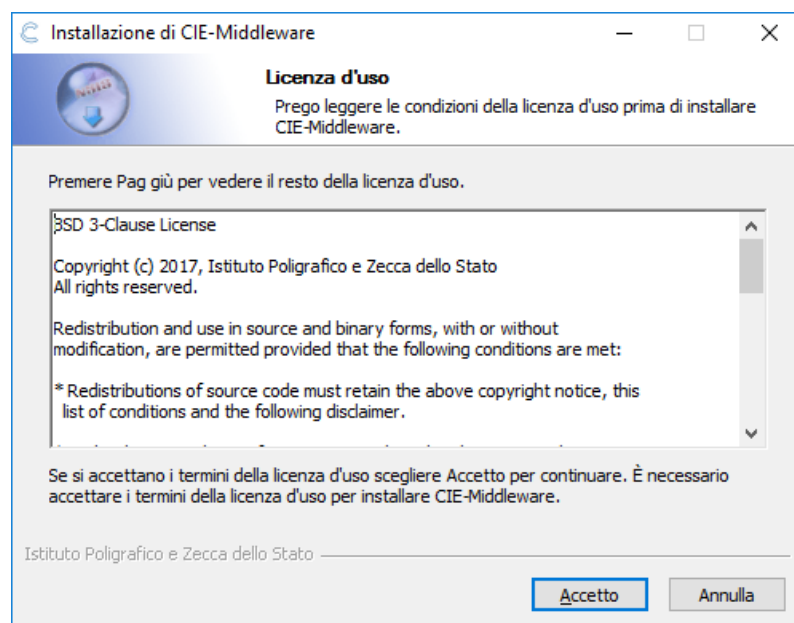
Effettuare un doppio click sul file "CIE-Middleware-<VERSIONE>.exe" scaricato. Nel caso sia abilitato il Controllo Account Utente (UAC) di Microsoft, verrà visualizzata la seguente schermata. È necessario cliccare su "SI":



MINISTERO
DELL'INTERNO



Comparirà la seguente schermata:



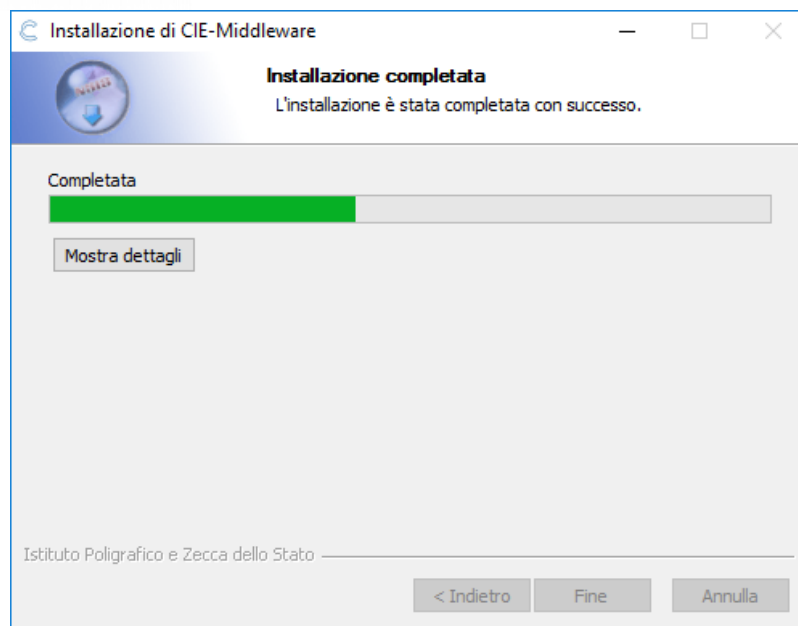
Cliccare sul tasto Accetto e attendere il completamento dell'installazione



MINISTERO
DELL'INTERNO

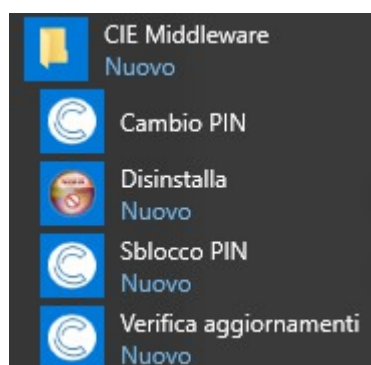


POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO



Cliccare su Fine per terminare l'installazione.

In seguito all'installazione sarà presente nel menu avvio un nuovo gruppo di programmi chiamato "CIE Middleware":



LINUX

Su Debian/Ubuntu è necessario, dopo aver scaricato il pacchetto .deb dal link XXX, installare il middleware con la seguente procedura da riga di comando, tutte come utente root (oppure aggiungendo all'inizio **sudo** se è installato), assumendo che il pacchetto deb sia nella directory corrente:

Su Debian 8 (jessie):

se non si ha il repository jessie-backports, agiungerlo tra le sorgenti con il seguente comando:

```
echo "deb http://ftp.debian.org/debian/ jessie-backports main contrib" >> /etc/apt/sources.list
```

apt-get update

apt-get install libccid libnss3-tools pcscd

apt-get install -t jessie-backports libssl1.0.0

dpkg -i ./libciepki_1.0-1_amd64.deb

(il ./ davanti al file è importante, oppure se il file non è nella directory corrente inserire il path completo fino al file .deb). Sostituire '_amd64' con '_i386' in caso di sistema a 32 bit.

Al termine dell'installazione saranno copiati nella directory degli eseguibili le utility 'cieunlockpin' e 'ciechangePIN', oltre alla libreria che gestisce la CIE.

Su Debian 9 (stretch):

apt-get install libccid libnss3-tools pcscd

dpkg -i ./libciepki_1.0-1_amd64.deb

(il ./ davanti al file è importante, oppure se il file non è nella directory corrente inserire il path completo fino al file .deb). Sostituire '_amd64' con '_i386' in caso di sistema a 32 bit.

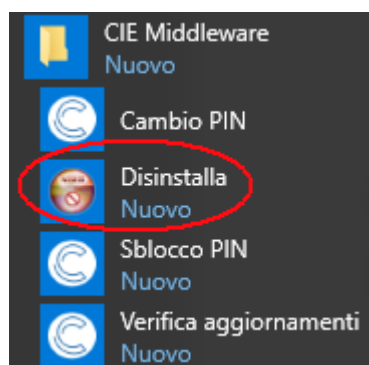
Al termine dell'installazione saranno copiati nella directory degli eseguibili le utility 'cieunlockpin' e 'ciechangePIN', oltre alla libreria che gestisce la CIE.

4. Rimozione del Middleware CIE

WINDOWS

Per rimuovere il software “CIE Middleware” è necessario utilizzare un account amministratore.

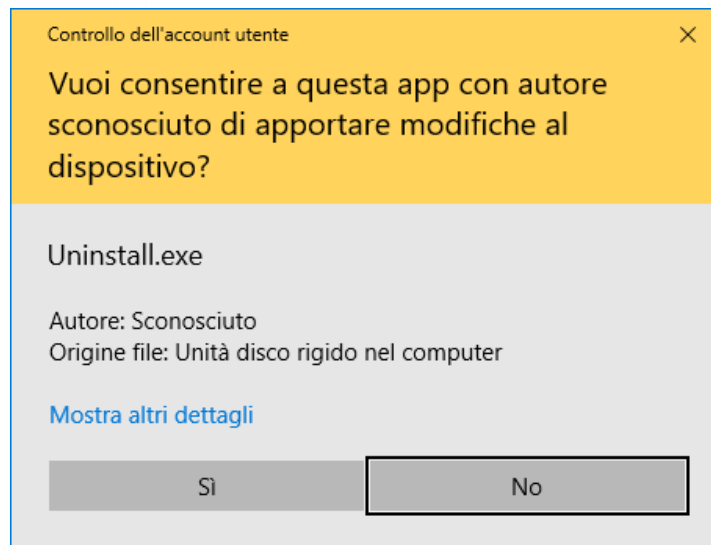
Selezionare il collegamento Disinstalla nel gruppo di programmi CIE Middleware.



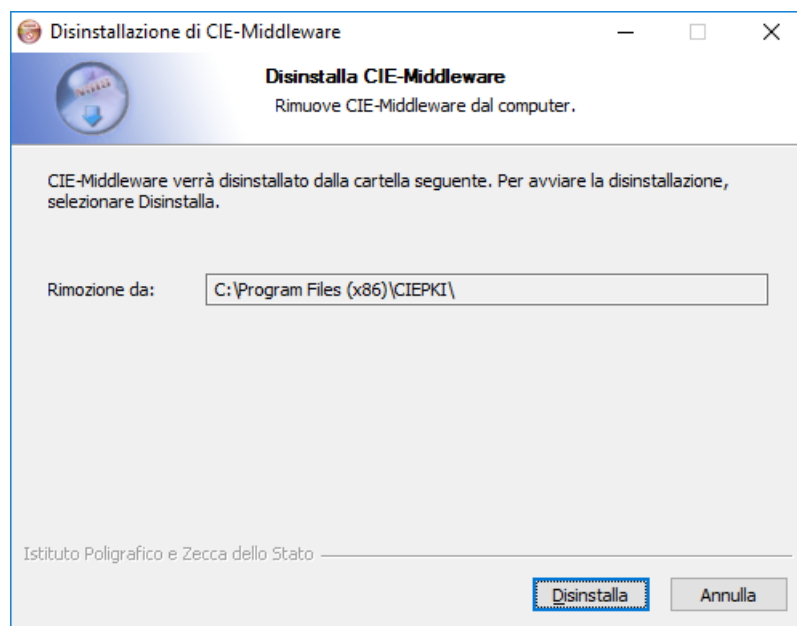
Nel caso sia abilitato il Controllo Account Utente (UAC) verrà visualizzata la seguente schermata. Confermare cliccando su “Sì”.



MINISTERO
DELL'INTERNO



Confermare la rimozione cliccando su Disinstalla



Attendere il termine della rimozione.

LINUX

Da riga di comando digitare, come root oppure con **sudo**, se installato:

apt-get purge libciepki1

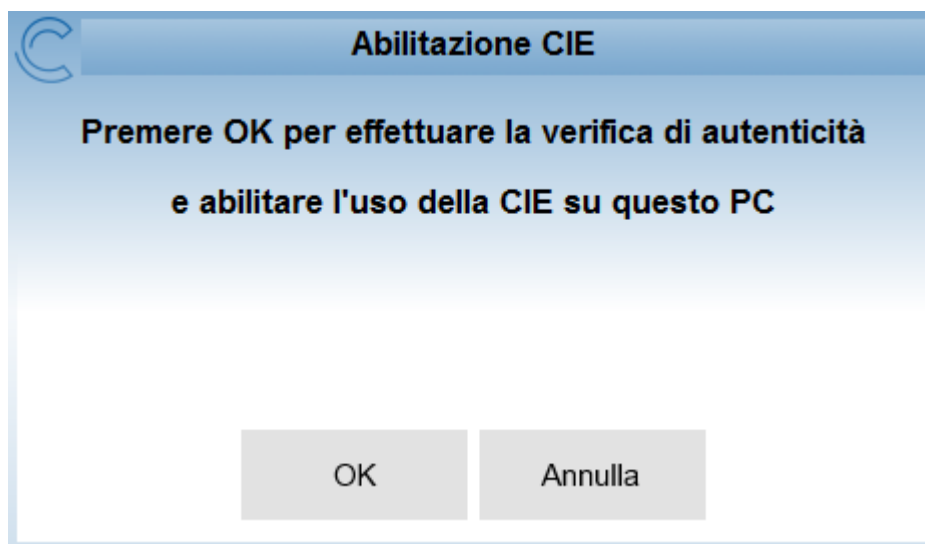
Attendere il termine della rimozione. Nel caso si sia aggiunto il middleware a Chrome tramite modutil, eliminarlo con il seguente comando da shell, come utente dal quale si era fatta l'installazione del modulo all'inizio:

modutil -dbdir ~/.pki/nssdb -delete CIEPKI

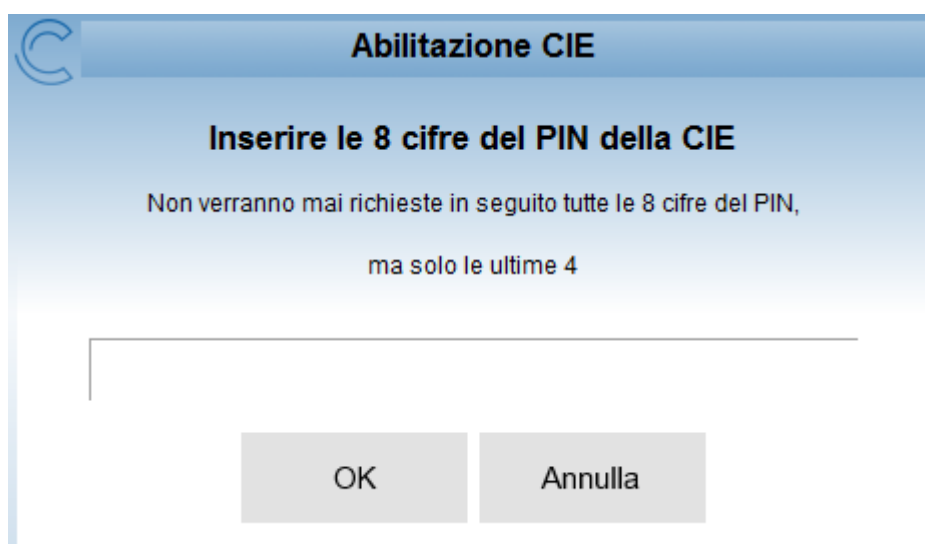
5. Primo utilizzo della CIE con il Middleware

Al primo utilizzo di una CIE, "CIE Middleware" richiede di effettuare 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 la prima volta che si tenta di utilizzare la CIE per autenticarsi ad un servizio in rete attraverso il browser. Viene presentata una schermata come quella di seguito. Lasciando la CIE posizionata sul lettore, premere OK.



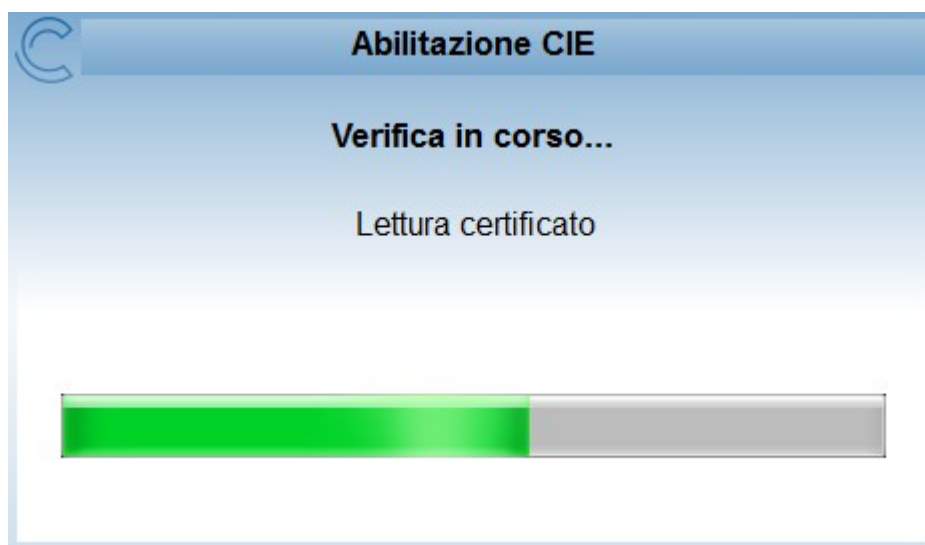
Viene richiesto di digitare il PIN. Procedere e premere OK.



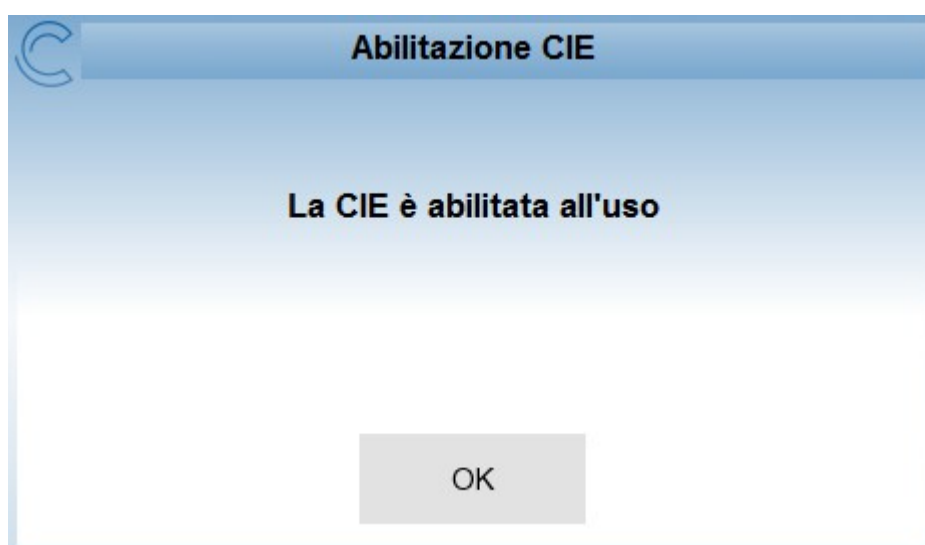


Attenzione! In fase di abilitazione verranno richieste tutte le 8 cifre del PIN. Successivamente, durante il normale utilizzo sarà necessario inserire solo le ultime 4 cifre.

Viene quindi avviata la procedura di controllo e validazione e viene mostrata la schermata in figura:



Al termine, la CIE sarà abilitata all'uso e verrà visualizzata la seguente schermata. Cliccare su OK per terminare.



6. Accesso ad un servizio 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.

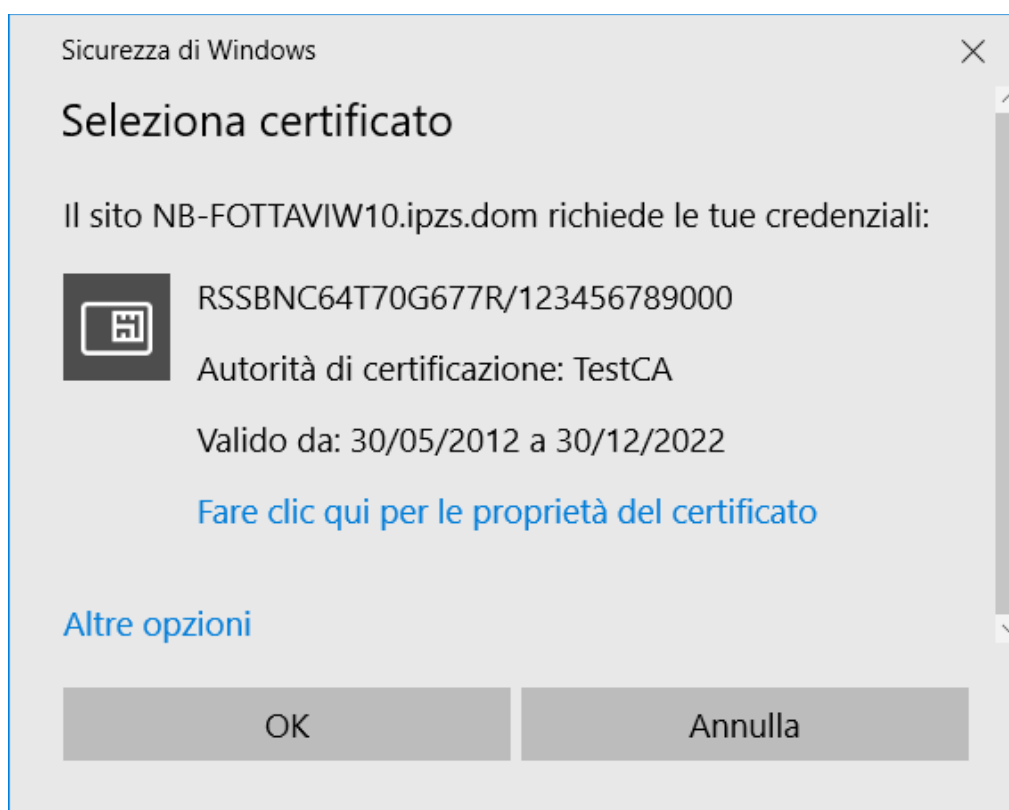
La procedura di autenticazione richiede sempre l'inserimento del PIN e, sulla base del browser utilizzato può richiedere delle operazioni di configurazione aggiuntiva, come descritto nei paragrafi seguenti.

6.1 MS Internet Explorer, MS Edge, Chrome e Opera

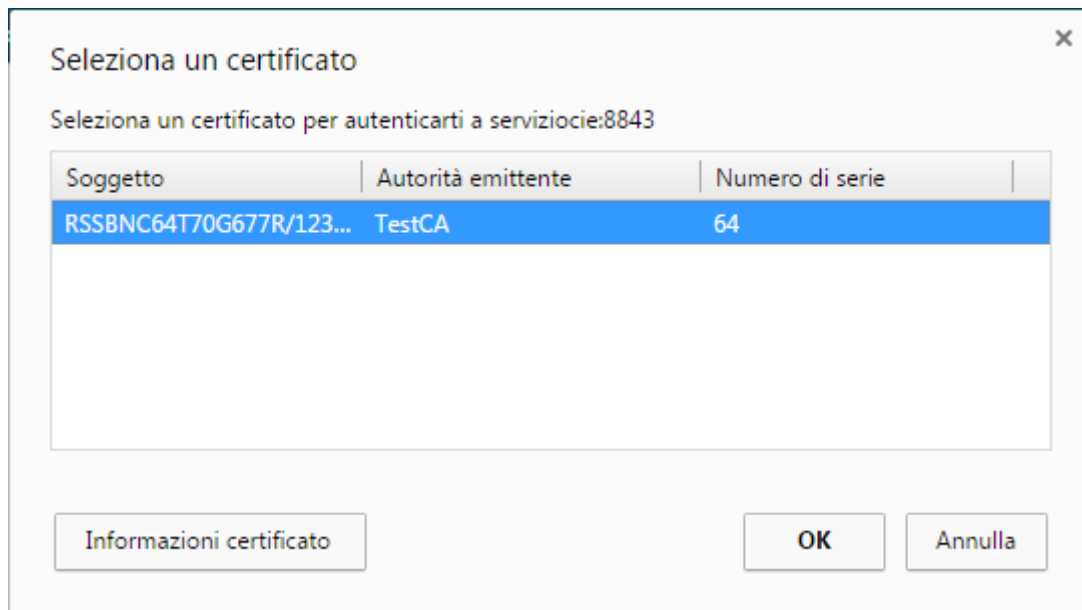
WINDOWS

L'autenticazione tramite CIE su Internet Explorer (fino alla versione 11 e Edge), su Chrome e su Opera non richiede alcuna operazione di configurazione aggiuntiva a quanto descritto nei paragrafi precedenti.

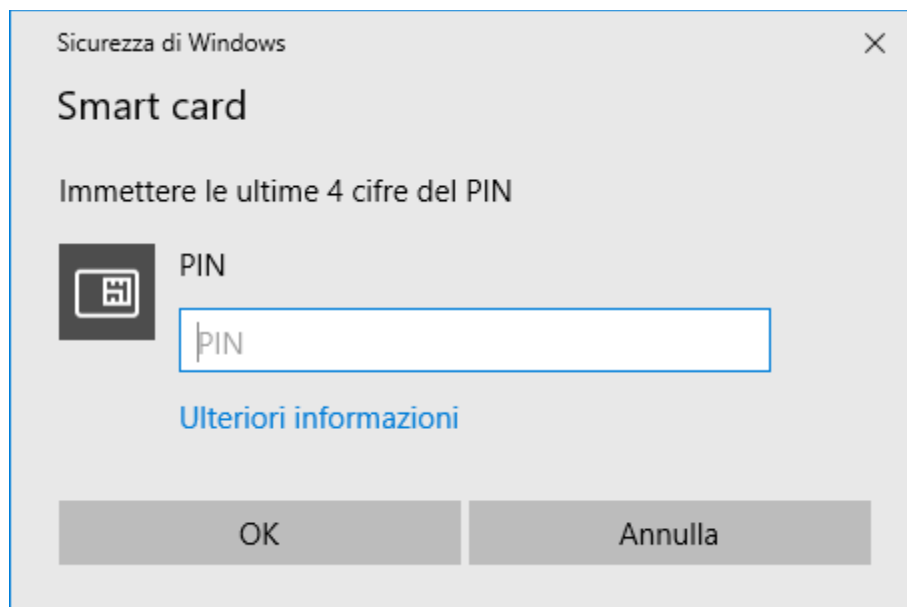
Appoggiare la CIE sul lettore smart card e digitare l'indirizzo del servizio a cui si vuole accedere nella barra degli indirizzi del browser. Se è la prima volta che si procede all'utilizzo della CIE con il browser, verrà avviata la procedura descritta nel paragrafo 5. Nel caso si sia già effettuata 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 e Opera la finestra di selezione del certificato è la seguente:



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




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 visualizzata una finestra di errore in cui è specificato il numero rimanente di tentativi di inserimento PIN prima del blocco:

Sicurezza di Windows

Smart card

Immettere le ultime 4 cifre del PIN

 PIN

[Ulteriori informazioni](#)

Il PIN inviato alla smart card non è corretto. Numero di tentativi rimasti: 2


OK Annulla

Se il PIN viene sbagliato per 3 volte consecutive quest'ultimo viene bloccato per sicurezza.

Sicurezza di Windows

Smart card

Immettere le ultime 4 cifre del PIN

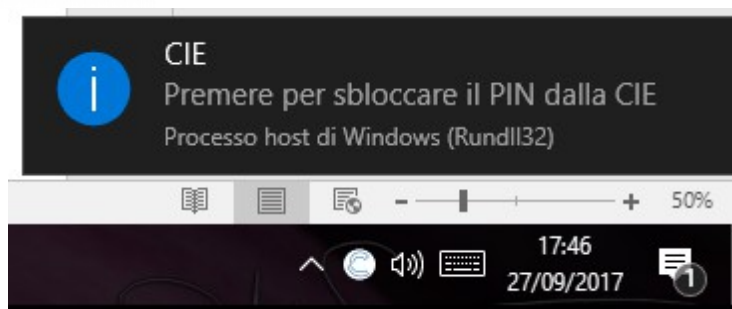
 PIN

[Ulteriori informazioni](#)

Smart card bloccata

OK Annulla

In tal caso, è possibile procedere al suo sblocco utilizzando il PUK e cliccando sull'avviso che compare nell'area di notifica in basso a destra.



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

LINUX

Il browser Opera al momento non è supportato. Per configurare Chrome è necessario impartire i seguenti comando da shell, come utente dal quale si intende lanciare il browser (di solito è l'utente con cui si esegue il login al Desktop):

se non esiste la directory `~/.pki/nssdb` digitare i seguenti tre comandi:

```
mkdir -p ~/.pki/nssdb
```

```
chmod 700 ~/.pki/nssdb
```

```
certutil -d ~/.pki/nssdb -N --empty-password
```

a questo punto è possibile aggiungere il middleware CIE tra i moduli NSS:

```
modutil -dbdir ~/.pki/nssdb -add CIEPKI -libfile /usr/lib/libciepki.so
```

con la smartcard appoggiata sul lettore collegato al pc, digitare:

```
modutil -dbdir ~/.pki/nssdb -list
```

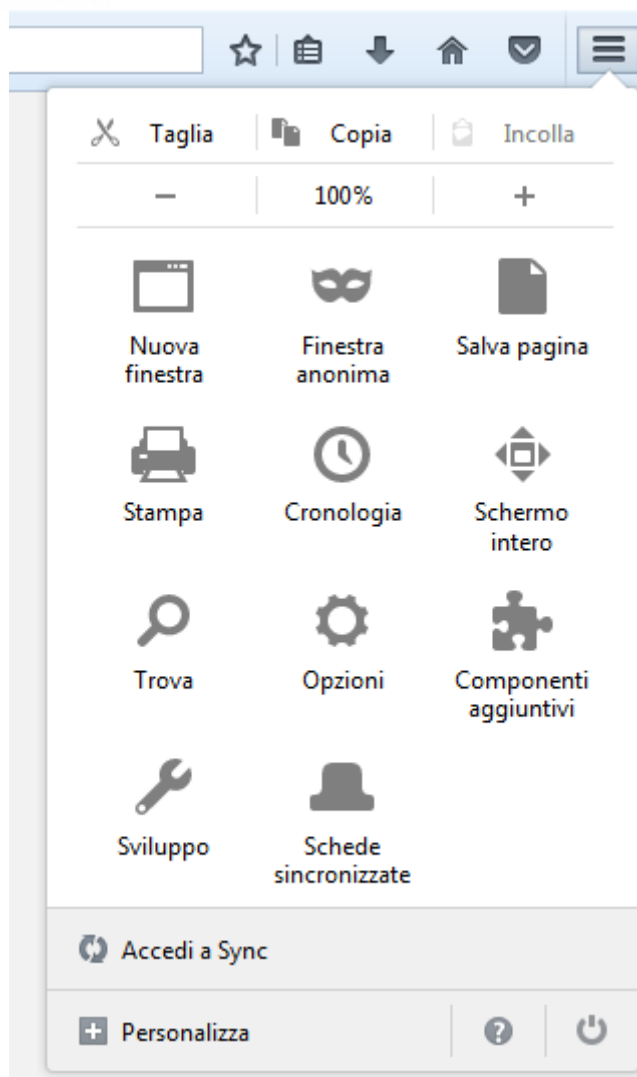
se è la prima volta che si usa la CIE, la smartcard verrà inizializzata con le stesse modalità descritte nel paragrafo 5. E' ora possibile controllare che il certificato sia stato importato correttamente in Chrome, dal menù Impostazioni->Avanzate->Gestisci Certificati->I tuoi certificati. E' possibile che vengano richieste le ultime 4 cifre del PIN della CIE.

6.2 Firefox

WINDOWS

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

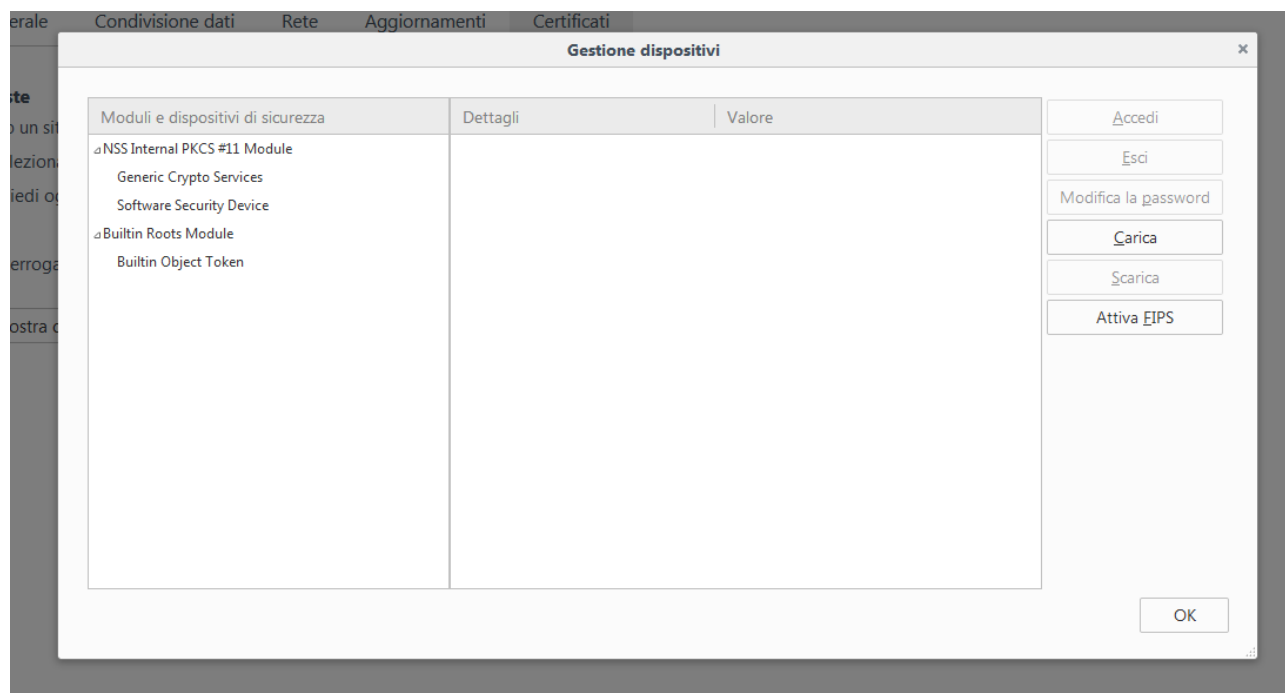
Accedere alla sezione "Opzioni" del browser:



Selezionare la scheda “Avanzate”, quindi la scheda “Certificati”

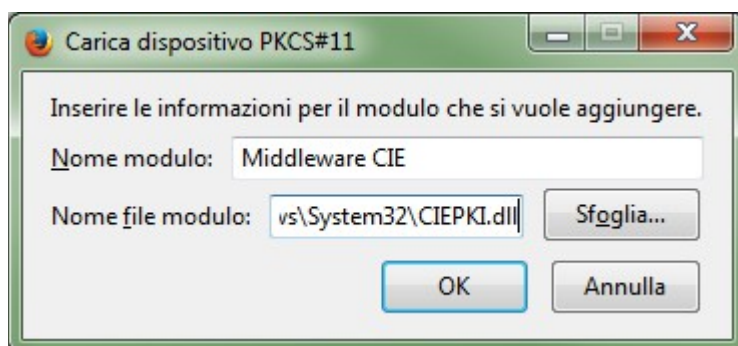


Cliccare su “Dispositivi di sicurezza”.

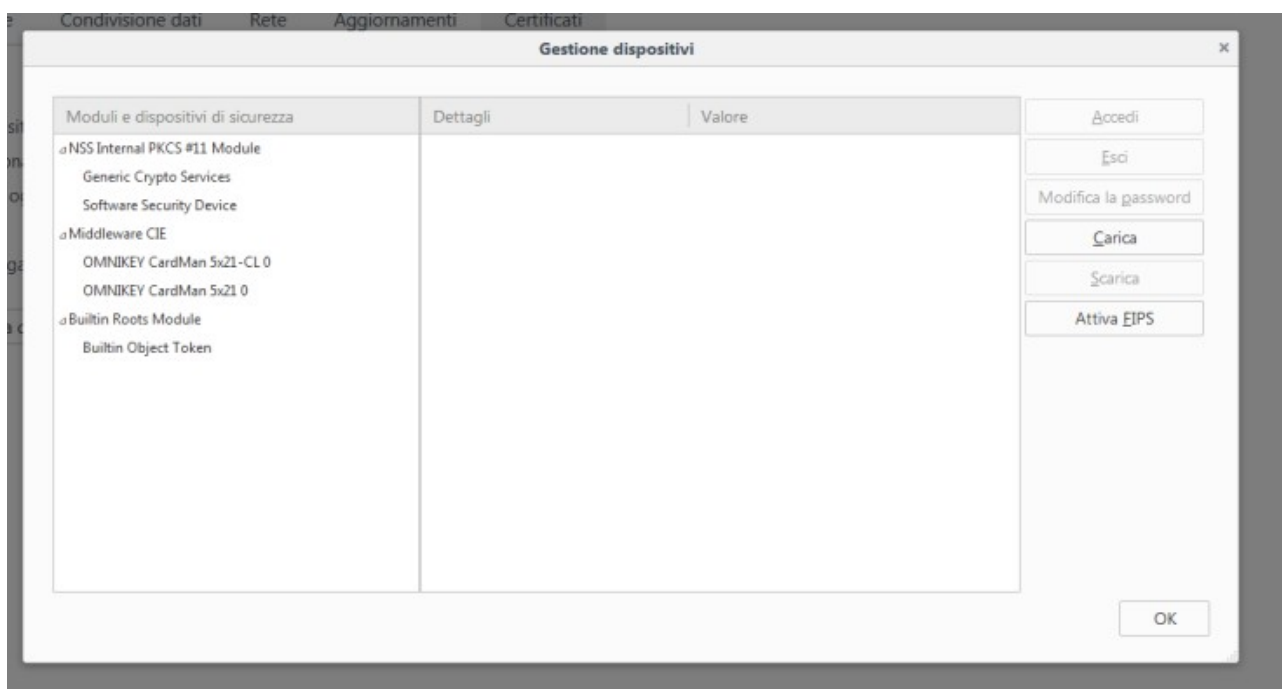


Cliccare su “Carica” e inserire le seguenti informazioni:

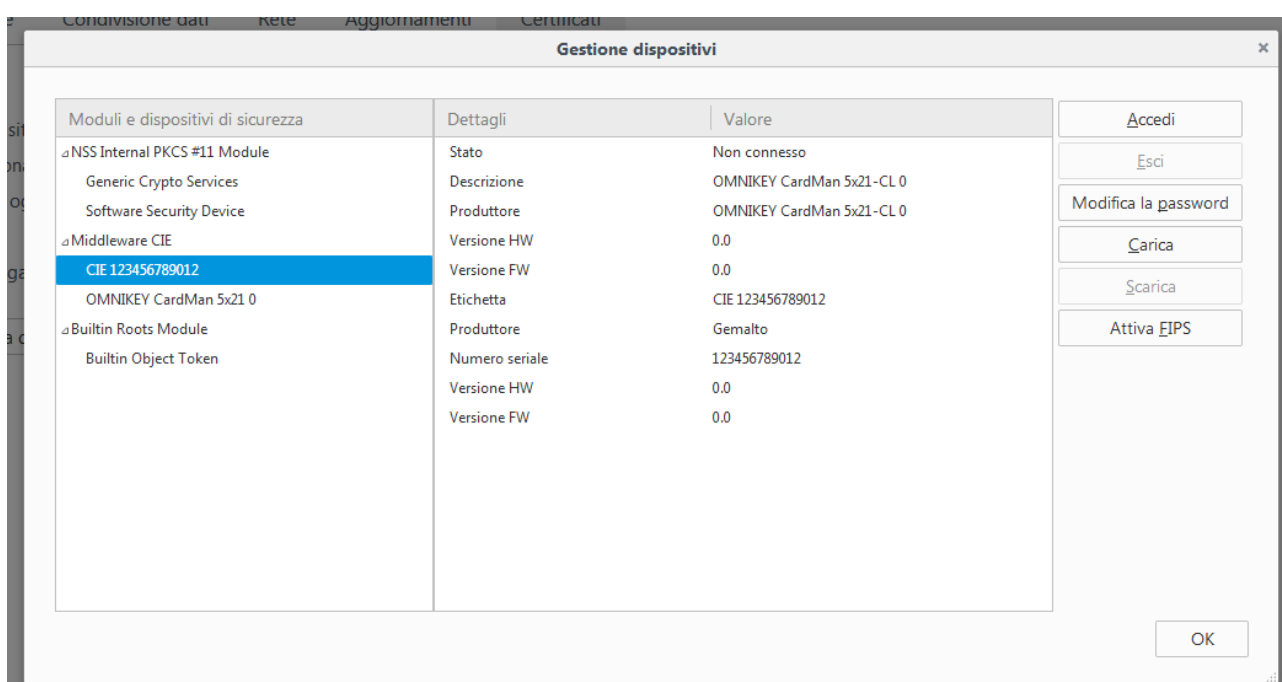
- Nome modulo: Middleware CIE
- Nome file modulo: C:\Windows\System32\CIEPKI.dll



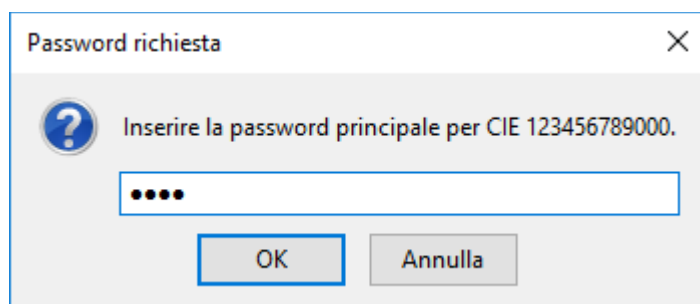
Se è la prima volta che si utilizza la CIE, verrà richiesto di completare la procedura di prima registrazione riportata nel paragrafo 5. Se tutto va a buon fine, il modulo comparirà nella lista di sinistra, con l'elenco dei lettori di smart card installati sul computer:



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

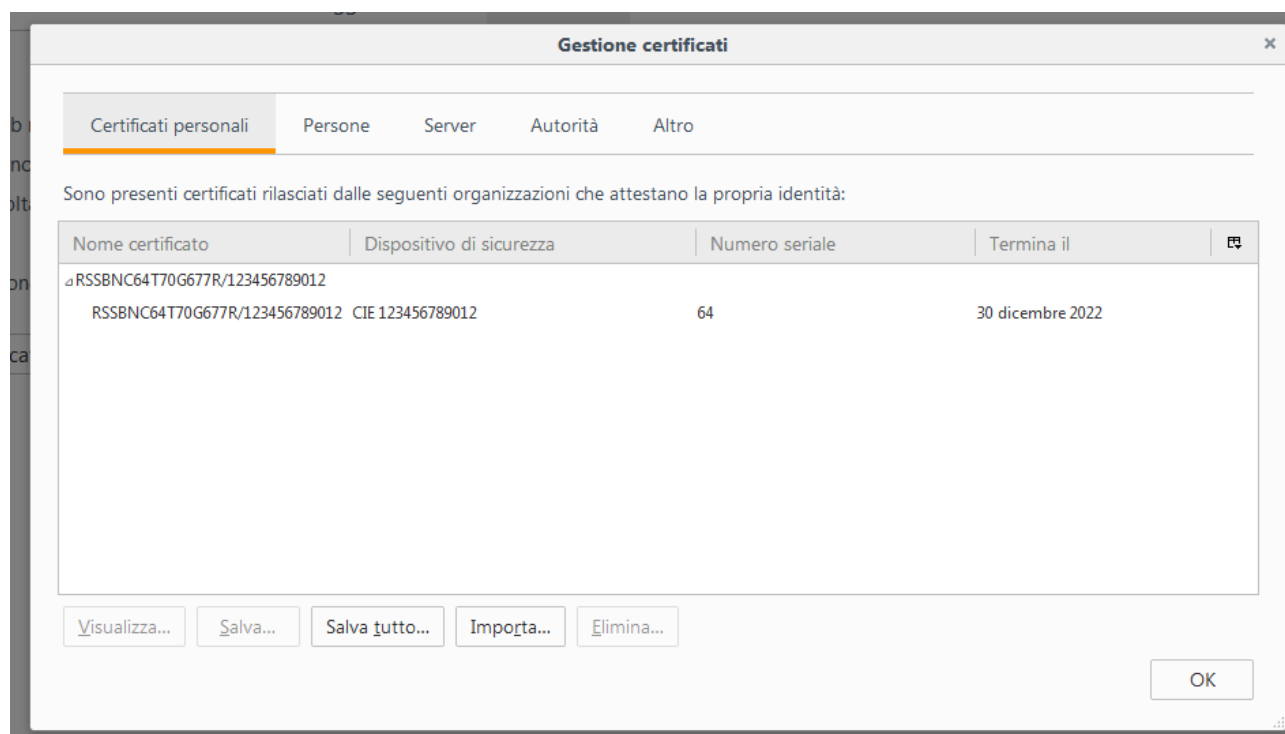
?

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

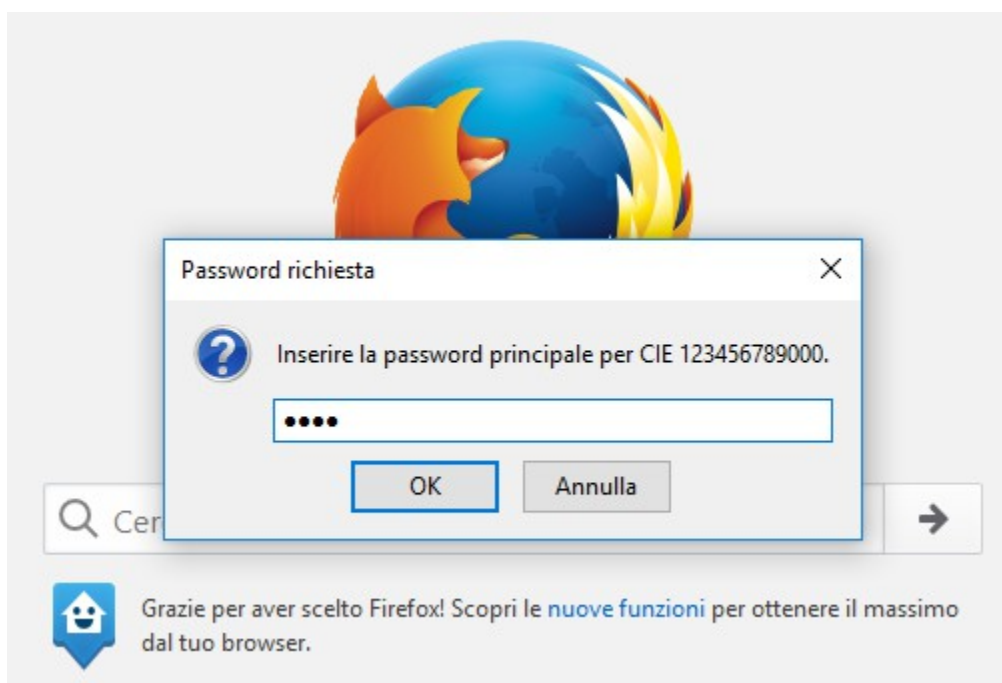
Visualizza... Salva... Salva tutto... Importa... Elimina...

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 quale certificato utilizzare per l'autenticazione client. Selezionare il certificato CIE, riconoscibile dal codice fiscale del titolare, e premere OK.



MINISTERO
DELL'INTERNO



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.

LINUX

La procedura è la medesima di quella di Windows descritta poco sopra, con l'unica eccezione di sostituire alla DLL di windows la shared library di linux che si trova in `/usr/lib/libciepki.so`.

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:

 <p>MINISTERO DELL'INTERNO</p>	 <p>CARTA DI IDENTITÀ ELETTRONICA</p>
<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**.

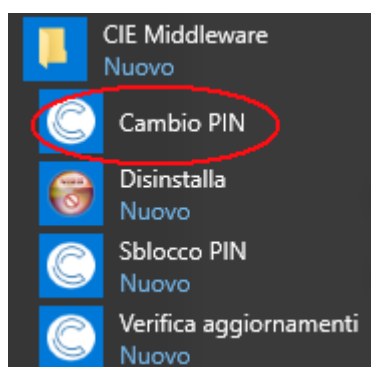
In seguito all'abilitazione verranno sempre richieste **solo le ultime 4 cifre del PIN**. Nel caso in esempio **5678**.

7.2 Cambio

WINDOWS

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.

Per cambiare il PIN appoggiare la CIE sul lettore di smart card e selezionare Cambio PIN dal menu avvio:



Inserire le ultime 4 cifre del PIN attuale della CIE e confermare cliccando su OK.

A screenshot of a dialog box titled 'Cambio PIN'. The dialog has a blue header bar with a circular icon on the left. Below the header, the text 'Inserire le 8 cifre del PIN della CIE' is displayed. There is a large, empty rectangular input field for the PIN. At the bottom of the dialog, there are two buttons: 'OK' and 'Annulla'.

Inserire quindi le ultime 4 cifre del nuovo PIN e confermare. Quest'ultimo deve essere digitato 2 volte per evitare che, a causa di errori di digitazione, il PIN venga impostato ad un valore diverso da quello desiderato:



Cambio PIN

Inserire le 8 cifre del nuovo PIN

OK Annulla

Nel caso in cui la seconda digitazione del PIN non corrisponda alla prima l'applicazione si blocca con un avviso all'utente. Se il PIN iniziale è invece digitato correttamente per due volte, avviene il cambio e viene mostrata la finestra di conferma seguente.

Cambio PIN

Il PIN è stato cambiato correttamente

OK

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.

LINUX

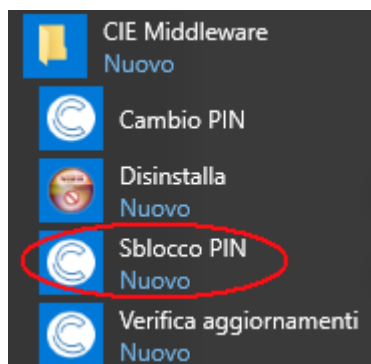
L'eseguibile del cambio PIN viene lanciato digitando da shell il comando '*ciechangePIN*'. La procedura è del tutto identica a quella per Windows descritta poco sopra.

7.3 Sblocco

WINDOWS

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 selezionare Sblocco PIN dal menu avvio:



Inserire il PUK della CIE e premere su OK.



Sblocco PIN

Inserire le 8 cifre del PUK della CIE

.....

OK Annulla

Verranno chieste tutte le 8 cifre di un 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:



Sblocco PIN

Inserire le 8 cifre del nuovo PIN

.....

.....

OK Annulla

Nel caso in cui la seconda digitazione del PIN non corrisponda alla prima, l'applicazione si blocca con un avviso all'utente:



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



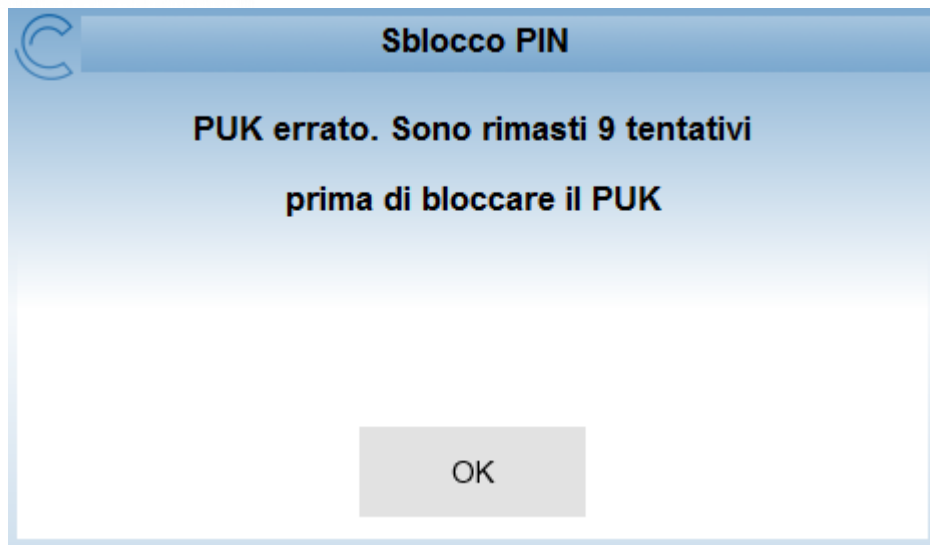
Se il PUK non corrisponde a quello digitato, viene visualizzata una schermata di errore in cui è specificato il numero di tentativi rimanenti prima di bloccare il PUK.



MINISTERO
DELL'INTERNO



POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO



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

LINUX

L'eseguibile dello sblocco PIN viene lanciato digitando da shell il comando '**cieunlockpin**'. La procedura è del tutto identica a quella per Windows descritta poco sopra.