A4PASiope+
A4HealthSiope+

GUIDA ALL'INSTALLAZIONE DEI PROGRAMMI

CODICE MIF3.UB
REV. 03
11/04/2024

ARGENTEA Srl
Società soggetta
all'attività di direzione e
coordinamento di
Zucchetti Hospitality Srl

Via Ragazzi del '99, nr. 13
I-38123 Trento (TN)
T +39 0461 381666

R.I. TN | CF | PI 02260390220
R.E.A. C.C.I.A.A. TN nr. 211447
Cap. Soc. Euro 200.000,00 i.v.
PEC argentea@pec.gpi.it
info@argentea.it

argentea.it

SOMMARIO

1. PREMESSA

Il manuale fornisce le indicazioni operative per eseguire l'installazione di A4PASiope+ e A4HealthSiope+. L'archivio contiene i software necessari per consentire l'accesso al sistema tramite dispositivi di firma digitale InfoCert. L'ultima sezione è dedicata alla configurazione del browser Firefox ESR, variabile a seconda del dispositivo di firma utilizzato.

2. REQUISITI MINIMI RICHIESTI PER IL FUNZIONAMENTO DEL PROGRAMMA

- **Sistema Operativo a 64 bit**:
  Ubuntu 22.04.1 o successive

- **Browser**[1]:
  - Firefox ESR (Versione 102.2.0 o successive);
  - Firefox (Versione 104.0.2 o successive) solo per l'accesso tramite credenziali;
  - Google Chrome (Versione 105.0.5195.102 o successive) solo per l'accesso tramite credenziali;

- **Connessione Internet** (connessione minima ADSL);

- Gli eventuali **apparati di sicurezza** interposti al collegamento internet (firewall – proxy) devono permettere il transito del protocollo TCP/IP con le porte 80 e 443 (SSL), in particolare devono essere opportunamente configurati affinché il client possa accedere al servizio esposto dalla Certification Authority che ha emesso il certificato HTTPS dei server **ordinativo-pre.argentea.it** e **ordinativo.argentea.it** per stabilirne attraverso lo scaricamento della CRL o attraverso l'API OCSP, lo stato di revoca.

- **Dispositivo di firma digitale**[2]
  InfoCert - Smart Card o Business Key nei modelli 1205, 1206, 1207, 1208, 1209, 7420 e 1702;

  Altri dispositivi di firma digitale CNS, ArubaKey - CNS, Smart Card con certificato di autenticazione CNS, PosteKey, Smart Card rilasciate dalle Camere di Commercio, etc. L'utilizzo di queste carte è vincolato all'installazione del corretto driver della carta, fornito dai diversi produttori.

- **Firma Remota InfoCert**[3]
  Gli utenti abilitati alla firma possono apporla anche mediante un certificato residente su server remoto (HSM). In questo caso l'autenticazione avverrà tramite credenziali oppure con certificato browser. Al momento l'unico provider utilizzabile per questa modalità è InfoCert.

---

[1] Si consiglia l'utilizzo di browser con ultimi aggiornamenti installati al fine di evitare rischi per la sicurezza.
[2] Solo per utenti che utilizzano il dispositivo di firma digitale per accedere e/o firmare.
[3] Servizio accessorio.

2.1 DETTAGLIO DELL'INSTALLAZIONE

Scaricare ed estrarre il file compresso ***Ordinativo_Ubuntu_V1.zip***

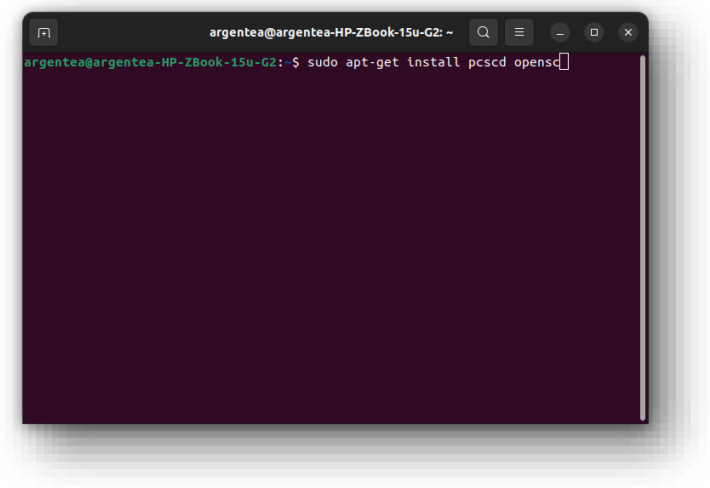
L'archivio contiene i seguenti file:

- *4identity_2.3.5_uniit_p11.run*
- *Librerie*

2.1.1 INSTALLAZIONE

Si consiglia di chiudere tutte le applicazioni attive prima di procedere con l'installazione.

Come prima operazione è necessario installare i pacchetti relativi al supporto dei dispositivi di firma (Smart Card e Business Key) eseguendo dal terminale di Ubuntu il comando:




```
sudo apt-get install pcscd opensc
```

Successivamente estrarre l'archivio "***Ordinativo_Ubuntu_V1.zip***" in un percorso sicuro a piacimento. I file all'interno della cartella "***Librerie***" non dovranno essere cancellati. Per la configurazione delle librerie presenti nell'archivio verificare il paragrafo "**Configurazione di Firefox ESR**"

INSTALLAZIONE 4IDENTITY

Solo per utenti firmatari che utilizzano dispositivi di firma (Smart Card o Business Key)

Aprire il terminale e spostarsi nella cartella dove è stato scaricato il file *4identity_2.3.5_uniit_p11.run*

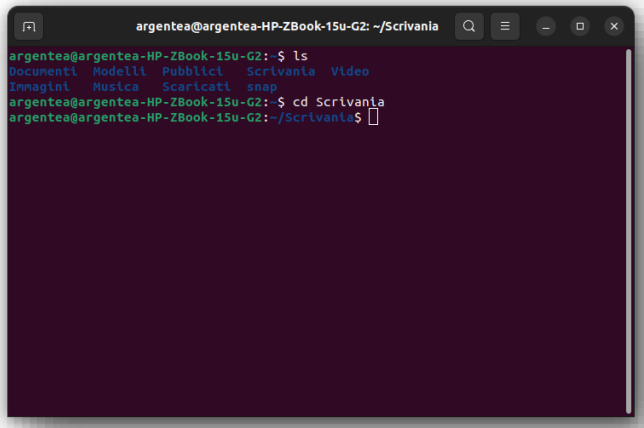
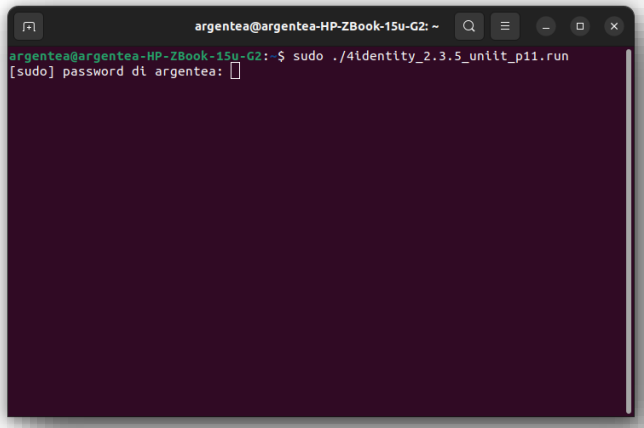


Immagine di esempio

Lanciare il comando ***sudo chmod +x 4identity_2.3.5_uniit_p11.run*** per rendere eseguibile il file ***.run*** e digitare la password utente.

Lanciare il comando **sudo *./4identity_2.3.5_uniit_p11.run*** per eseguire il *file* ***.run*** digitando anche la password utente.

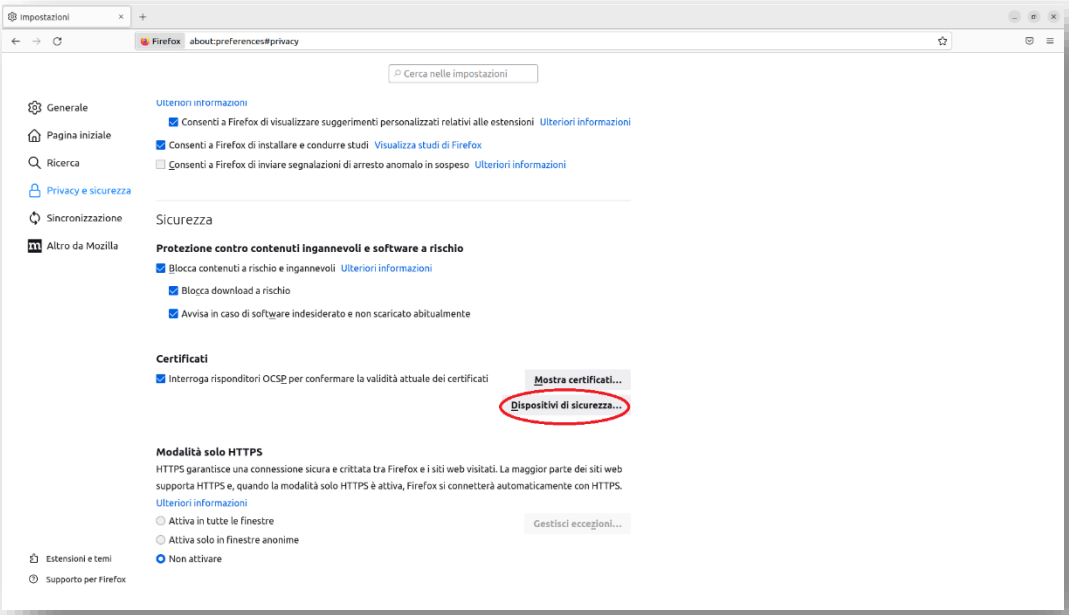


CONFIGURAZIONE DI FIREFOX ESR

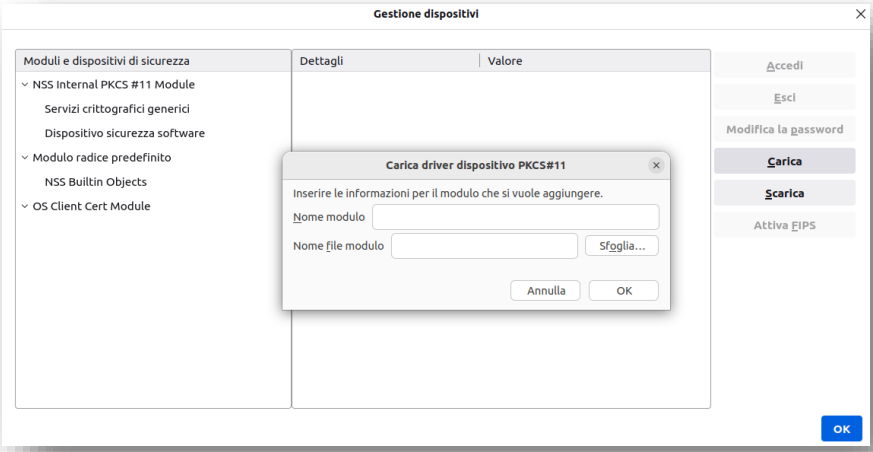
Avviare il browser Firefox ESR

Dal menu selezionare "***Preferenze***" e cliccare su "***Privacy e sicurezza***", in alternativa incollare nella barra degli indirizzi il seguente link about:preferences#privacy.

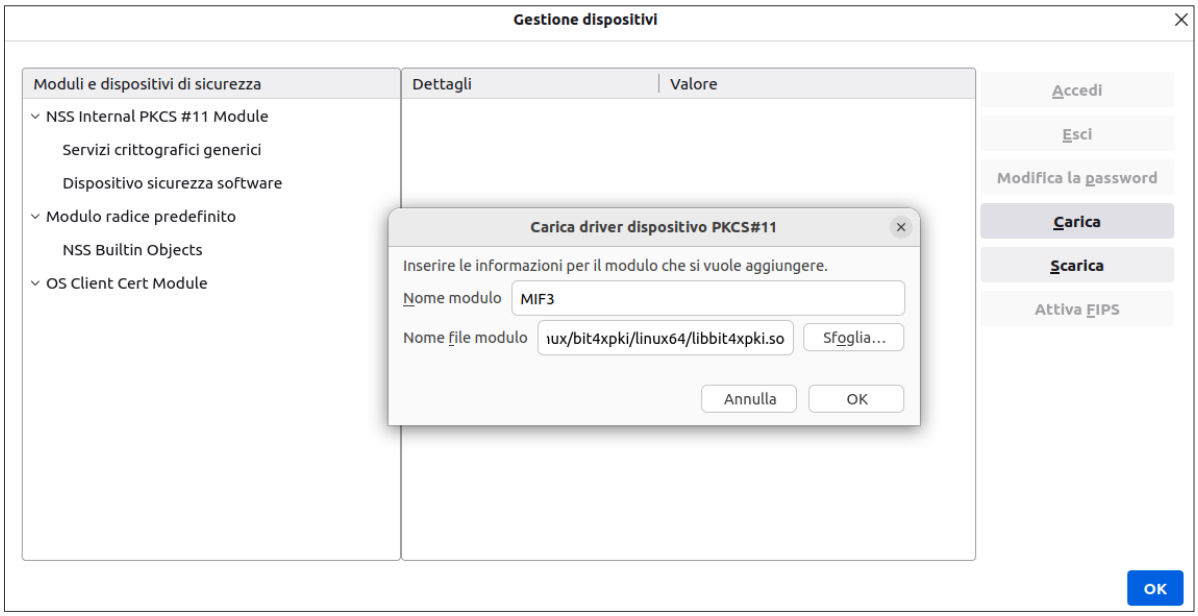
Scorrere la pagina fino alla sezione "***Certificati***" e cliccare su "***Dispositivi di sicurezza***".



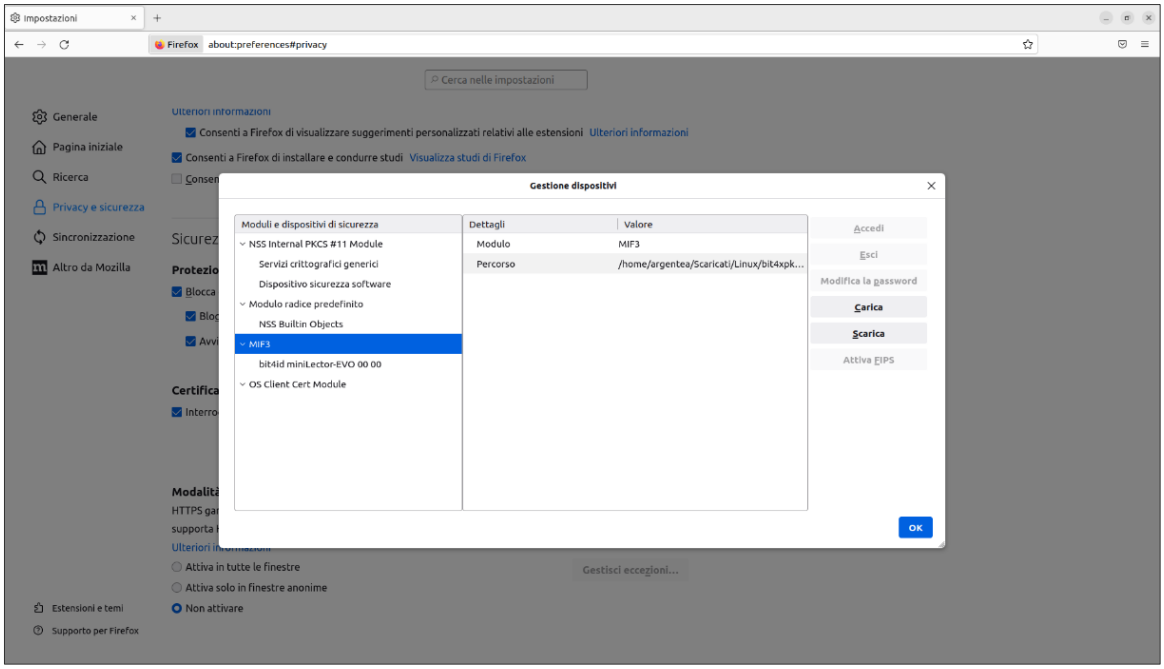
Nella finestra “Gestione dispositivi”, cliccare su “**Carica**”.
Si aprirà la finestra “***Carica driver dispositivo PKCS#11***”



Nel campo “*Nome modulo*” inserire “**Ordinativo Informatico**” o “**MIF3**” e in prossimità del campo “*Nome file modulo*” cliccare sul tasto “Sfoglia” e selezionare la libreria “**libbit4xpki.so”** contenuta nella cartella “Librerie” presente all’interno dell’archivio *Ordinativo_Ubuntu_V1.zip* estratto in precedenza.



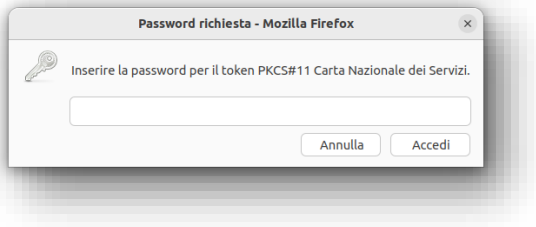
Ad inserimento avvenuto confermare cliccando sul pulsante "***OK***".
Nell'elenco apparirà la voce appena inserita.



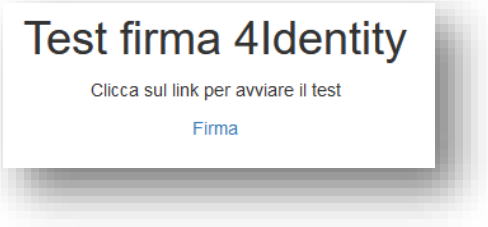
2.1.2 TEST DI FIRMA PER ORDINATIVO INFORMATICO

Per verificare la corretta configurazione del client tramite dispositivi di firma digitale esegui questo test:

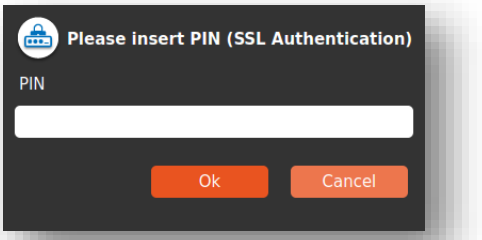
1. Inserire una **Smart Card**;
2. **Collegarsi** al link https://testfirma.argentea.it/4Identity;
3. Quando richiesto digitare il codice **PIN** della Smart Card, e confermare cliccando su "***Accedi***";



4. Cliccare su "***Firma***";

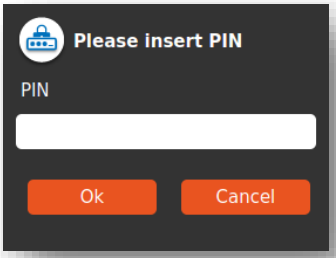


5. Digitare il **PIN** e confermare cliccando sul pulsante "***Ok*** ";
6.



7. Selezionare il certificato di **firma** e cliccare sul pulsante "***OK***";

8. Digitare il **PIN** e confermare su "***OK***";



9. L'**esito** positivo del test verrà notificato dal messaggio "***Firma avvenuta correttamente***".

CUSTOMER SERVICE DESK

Tutti i giorni lavorativi dalle ore **9:00** alle ore **17:00**

Telefono: **199.20.60.29**

Email: **supporto.pa@argentea.it**