Ministero dell'Interno

Istruzioni operative

Stazione Appaltante

Si.Ce.Ant.

Documentazione necessaria per lo *START UP*

Attività tecnica necessaria per lo start up

Certificazione della postazione UTENTE (smart card virtuale).

Prima di procedere con la certificazione della postazione occorre precisare quanto segue ***:***

- L'operazione di certificazione è possibile solo se in possesso delle credenziali rilasciate dalla Prefettura*;*
- La postazione presenta la seguente configurazione*:*
    - S.O.Windows 7
    - Browser Internet Explorer 9 o 10

  Nel caso di IE11 è necessario accedere in modalità compatibilità.

  Il browser IE deve essere a 32 bit.
- L'utente deve essere necessariamente **amministratore** della macchina sulla quale verranno scaricati il certificato digitale e il client della VPN*;*
- È necessario inserire "**certbdna**" tra i siti attendibili (Fig.1);
- Si consiglia di **abbassare al minimo le protezioni del browser** per i siti attendibili (Fig. 1);
- si sottolinea, che alcuni tipi di antivirus potrebbero bloccare il download del pacchetto, quindi potrebbe essere necessario **disabilitare temporaneamente il sistema antivirus** o aggiungere un' eccezione per permettere il corretto download

Configurazione IE

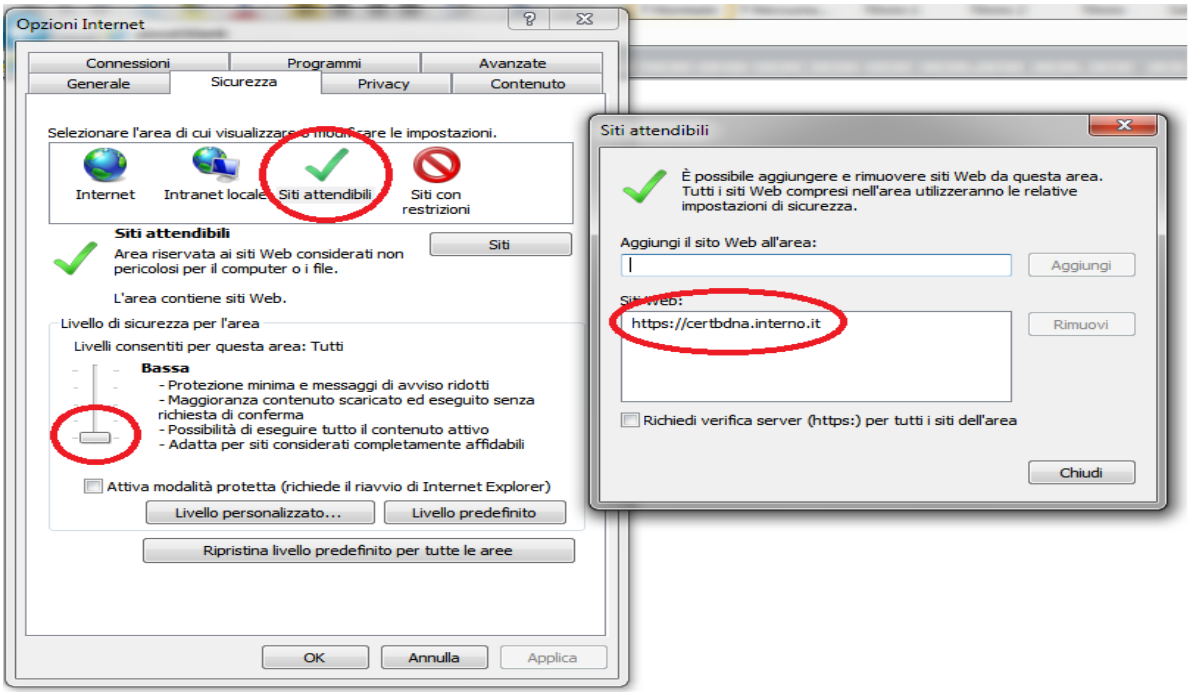


Fig. 1

- L'utente deve disinstallare la VPN se già presente sul proprio pc e procedere con l'installazione della nuova VPN;
- Poiché alcuni tipi di antivirus potrebbero bloccare il download di questo pacchetto, potrebbe essere necessario disabilitare temporaneamente il sistema antivirus o aggiungere un'eccezione per permettere il corretto download.

La **certificazione della postazione** richiede:

1) **Installazione VPN**

I. indicazioni per l'abilitazione delle **porte per la VPN**:

a) TCP 443

b) ip 212.14.141.11

II. indicazioni per l'abilitazione delle **porte per certbdna**:

a) TCP 443

b) ip 212.14.141.87

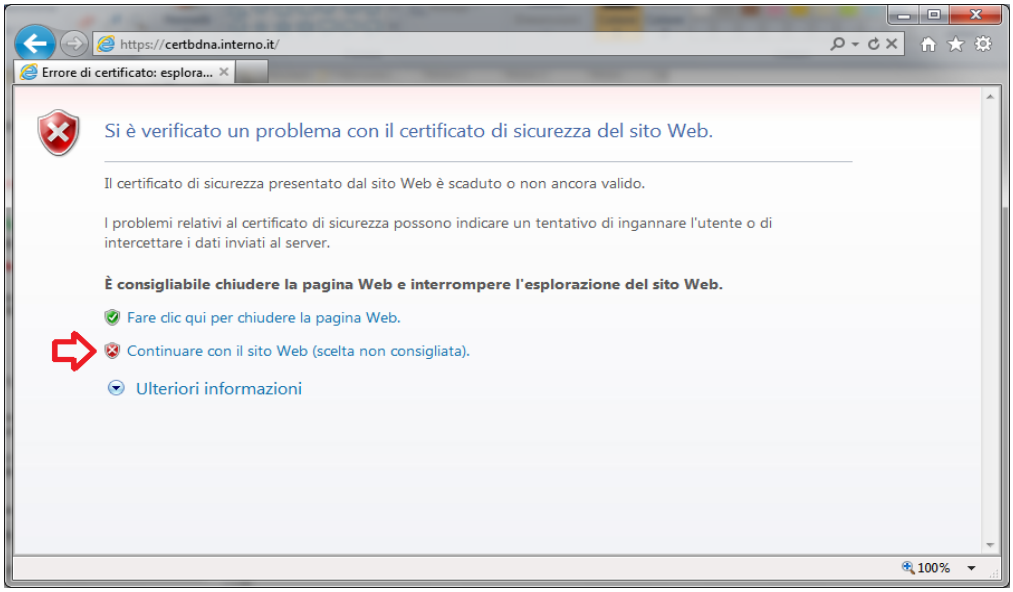
III. Disinstallare la precedente VPN (se presente) e collegarsi all'indirizzo: **http://www.prefettura.it/FILES/Siceant/AnyConnect.zip**;

IV. effettuare il **download** del file eseguibile e procedere alla installazione della VPN.

2) Certificazione della postazione UTENTE

I. L'utente, dalla propria postazione, si collega all'indirizzo: **https://certbdna.interno.it**

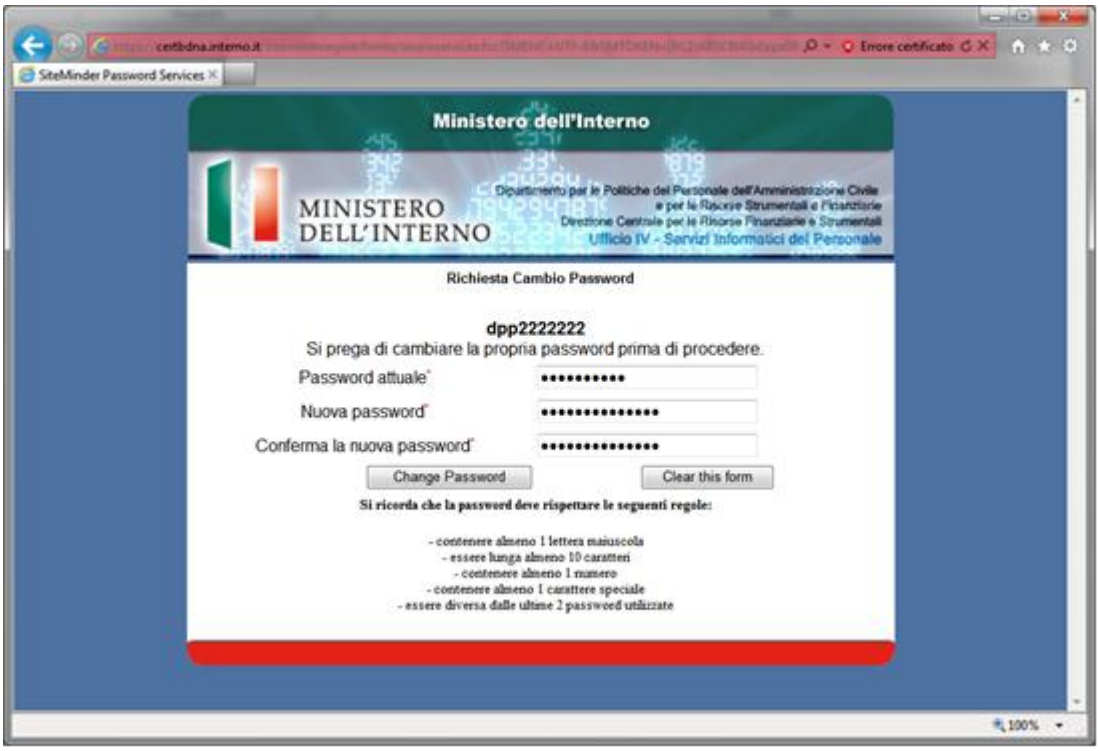
Si sottolinea che è necessario utilizzare, come browser, Internet Explorer in quanto le operazioni rinvenibili sul sopraindicato portale richiedono l'impiego della tecnologia Active X.



II. Cliccando sulla opzione "**Continua con il sito (scelta non consigliata**)", si accede alla maschera riportata di seguito per l'inserimento delle credenziali ricevute (n.b.: Username è fornito dalla Prefettura e Password viene inviata via e-mail);

III. Inserite le credenziali, il sistema propone la maschera del cambio password (obbligatorio al 1° accesso);

Effettuare il cambio password rispettando le regole sulla pagina; in particolare, si precisa che la password deve contenere almeno un carattere speciale tranne '*' e '£'.



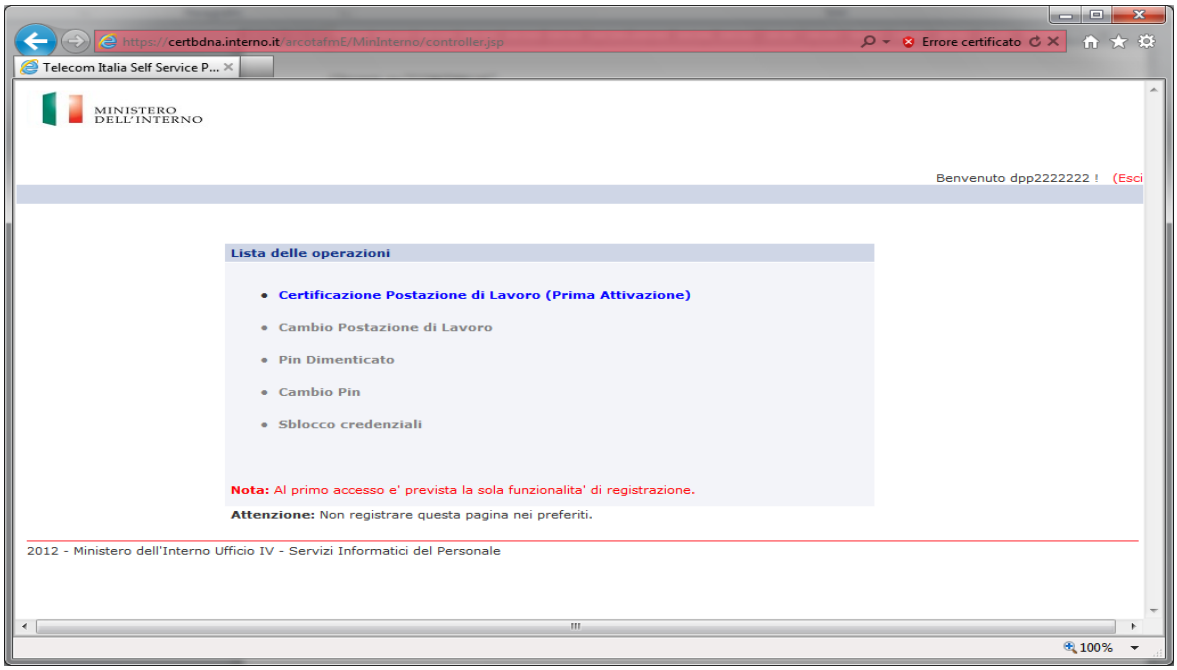
Si ricorda che la password ha una validità di 90 giorni e, al termine di tale periodo, l'account dell'utente sarà sospeso in attesa di cambiare la password.

E' possibile effettuare il **cambio password** accedendo all'indirizzo https://certbdna.interno.it e cliccando sul link "Password dimenticata/Cambio Password".

IV. Cliccando sul tasto "**Change Password"**, il sistema propone la maschera sotto riportata;

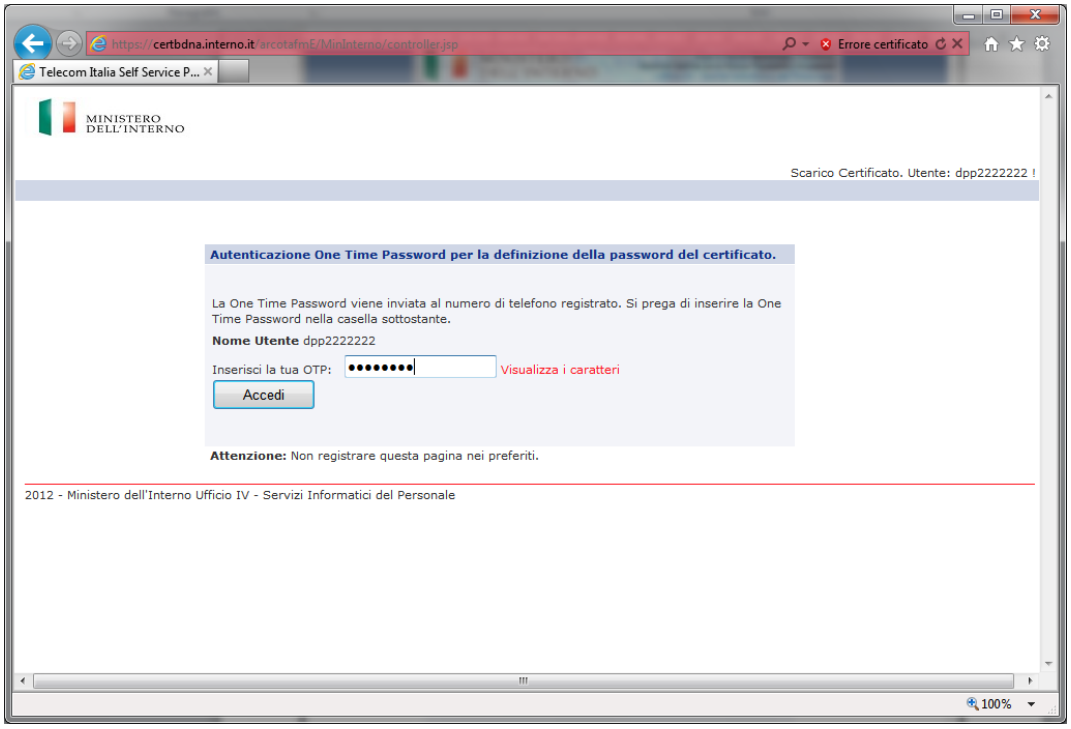
V. Con la maschera sopra riportata si sono concluse le operazioni di cambio password. Ora si prosegue con la procedura di certificazione della postazione di lavoro che consente di generare il certificato digitale pubblico e scaricare il software di sicurezza per la protezione dello stesso. Durante questa fase, si rammenta che l'utente deve avere i privilegi di **amministratore** della postazione e deve essere collegato con le credenziali che in seguito utilizzeranno il certificato. Cliccare sul tasto "**Continua**".

VI. Cliccare sulla opzione "**Certificazione Postazione di Lavoro (Prima attivazione)**";

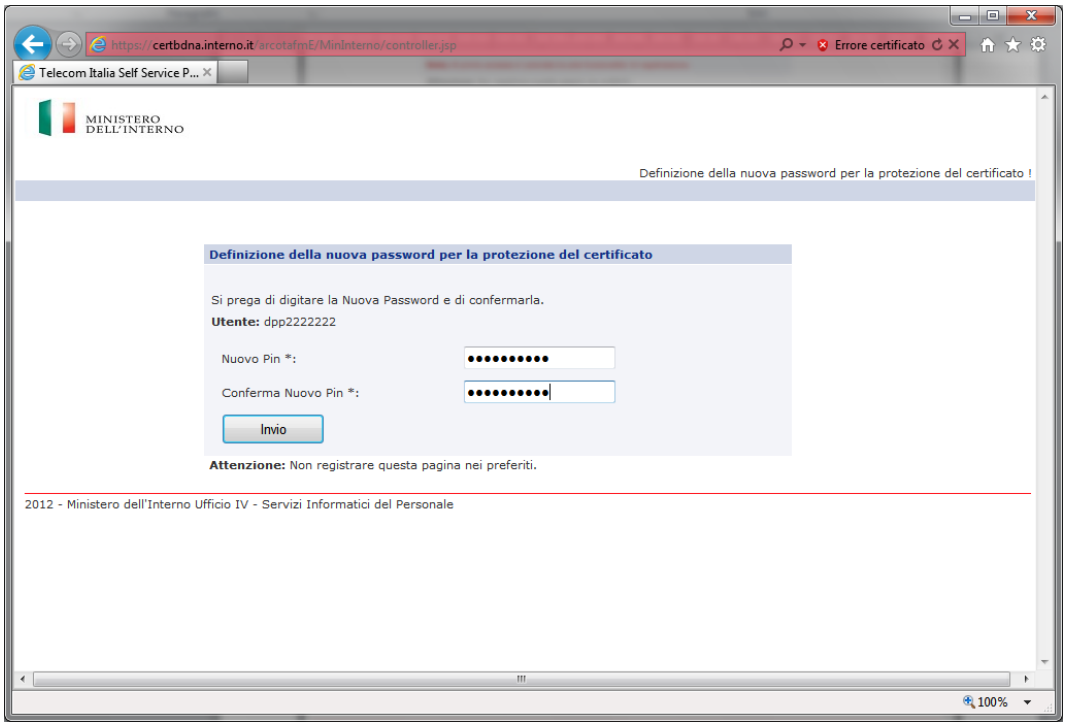


L'utente riceve via SMS una OTP (sequenza numerica di 8 caratteri) sul numero di cellulare indicato nel modello sottoscritto per la "registrazione utente";

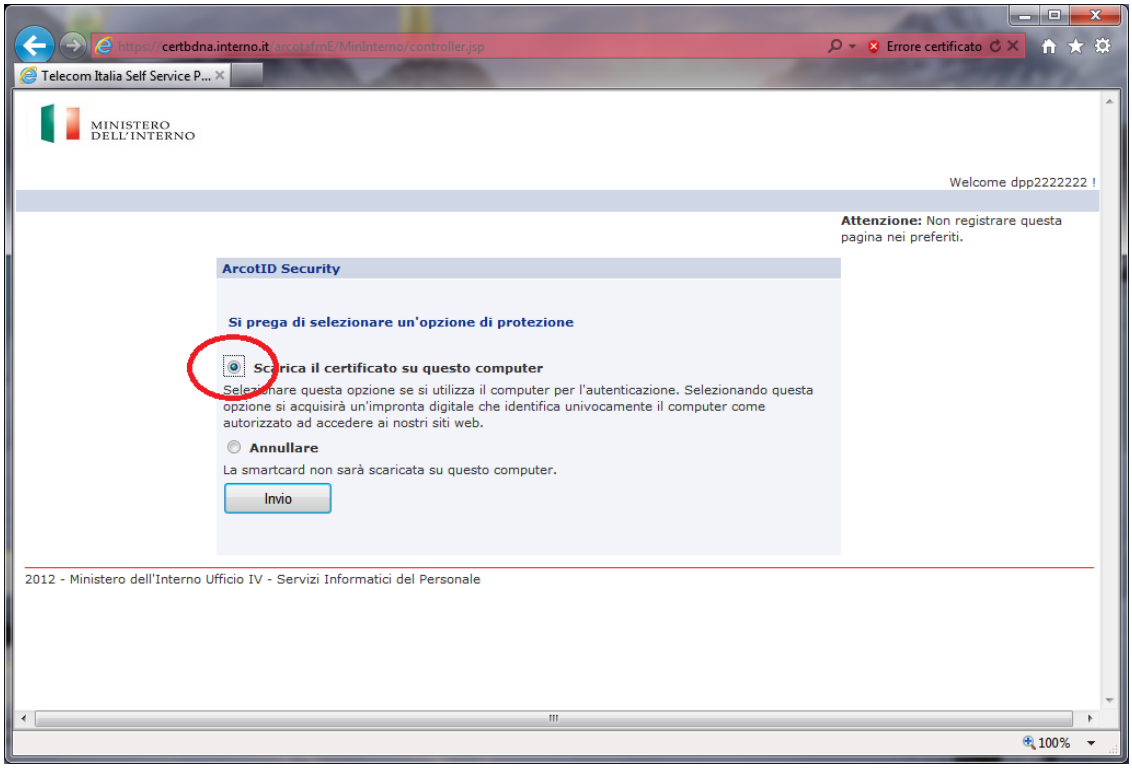
VII. L'utente deve digitare a video la OTP ricevuta. Inserita l'OTP, cliccare sul tasto "**Accedi**";



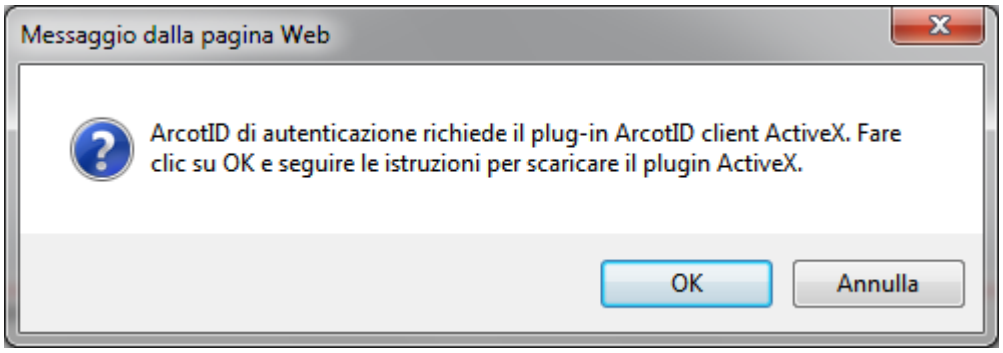
VIII. Se l'OTP digitato è corretto, il sistema propone all'utente la maschera per impostare il PIN **(*)** della propria smart card virtuale per connettersi alla VPN. Il PIN deve essere almeno di 10 caratteri, contenere almeno 1 lettera maiuscola, 1 carattere speciale e 1 numero (come la Password).Si precisa infine che il PIN per accedere alla VPN deve essere diverso dalla password di accesso all'applicativo.



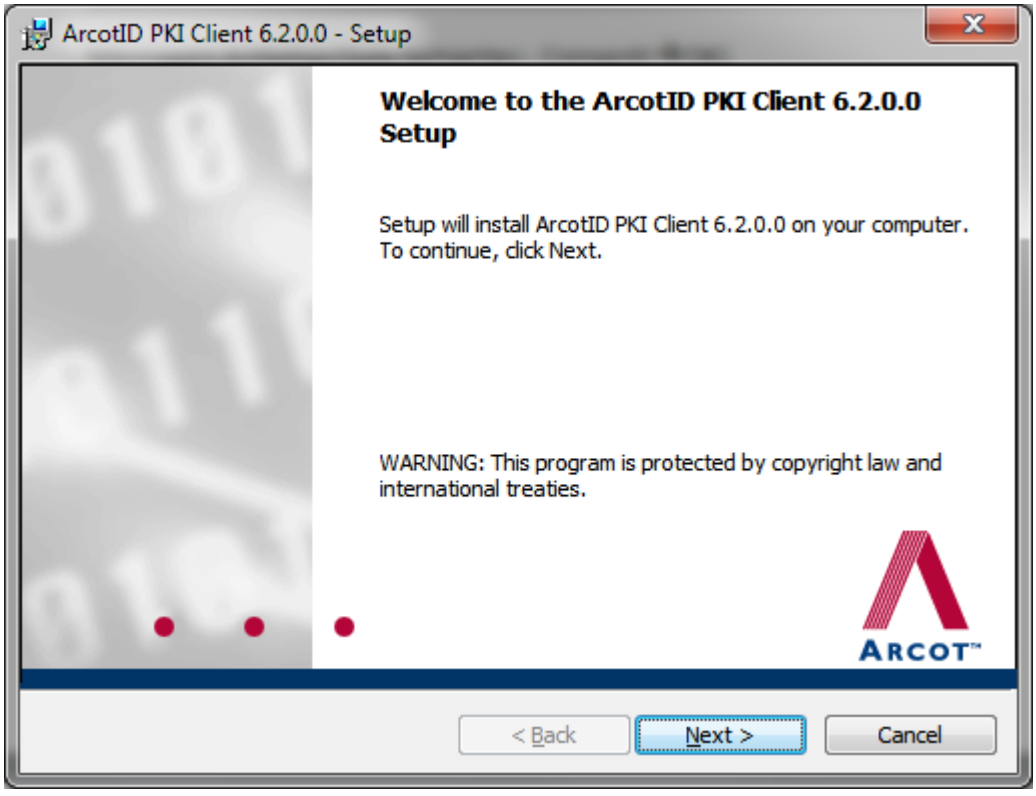
IX. Selezionare l'opzione "**Scarica il certificato su questo computer"** e cliccare su **Invio**

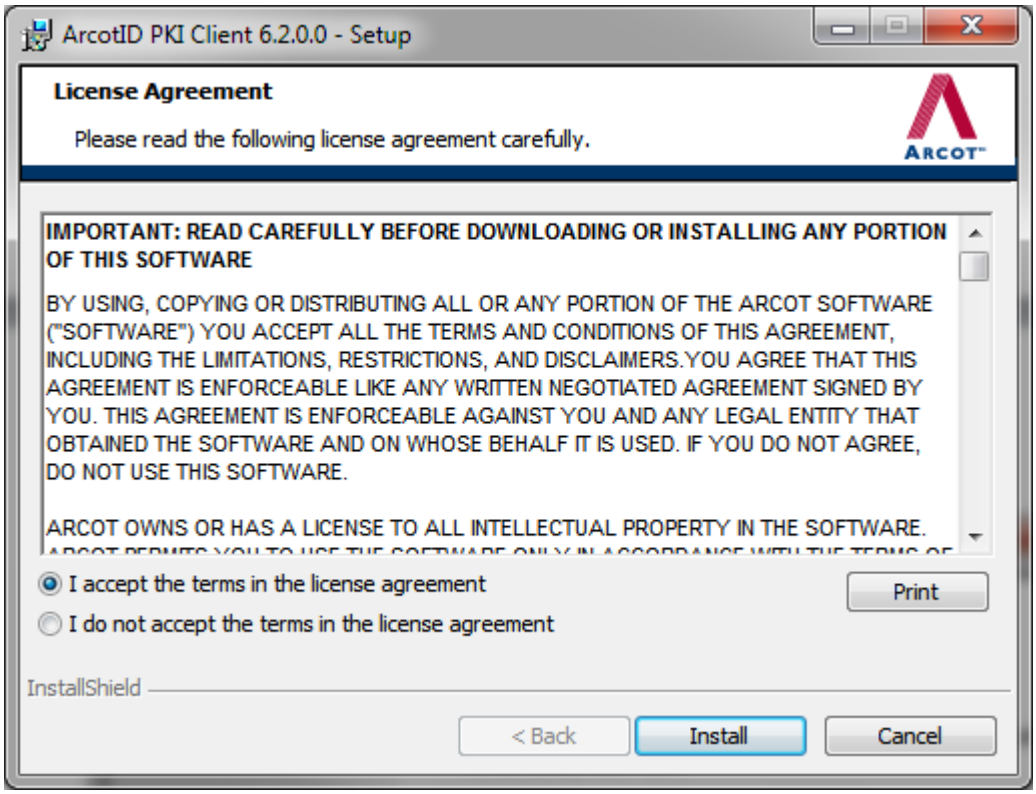


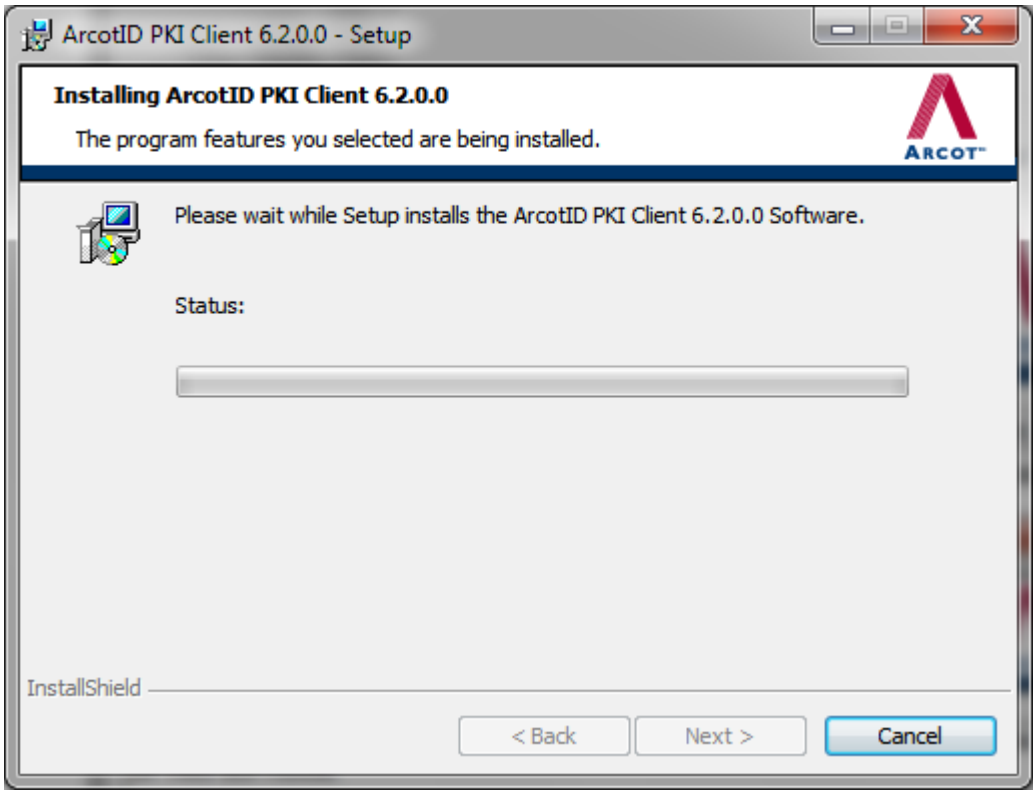
X. Il sistema propone il messaggio sotto riportato; cliccare su **Ok** e attendere;

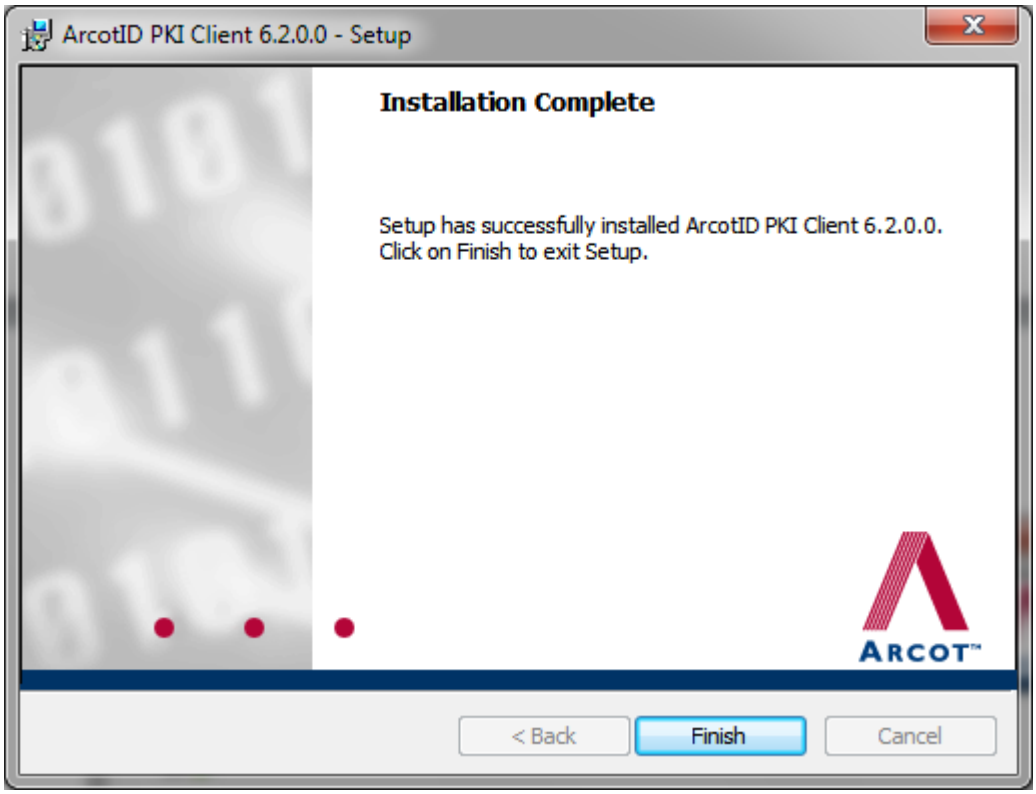


XI. Si procede con la installazione sulla postazione del certificato digitale ArcotID;

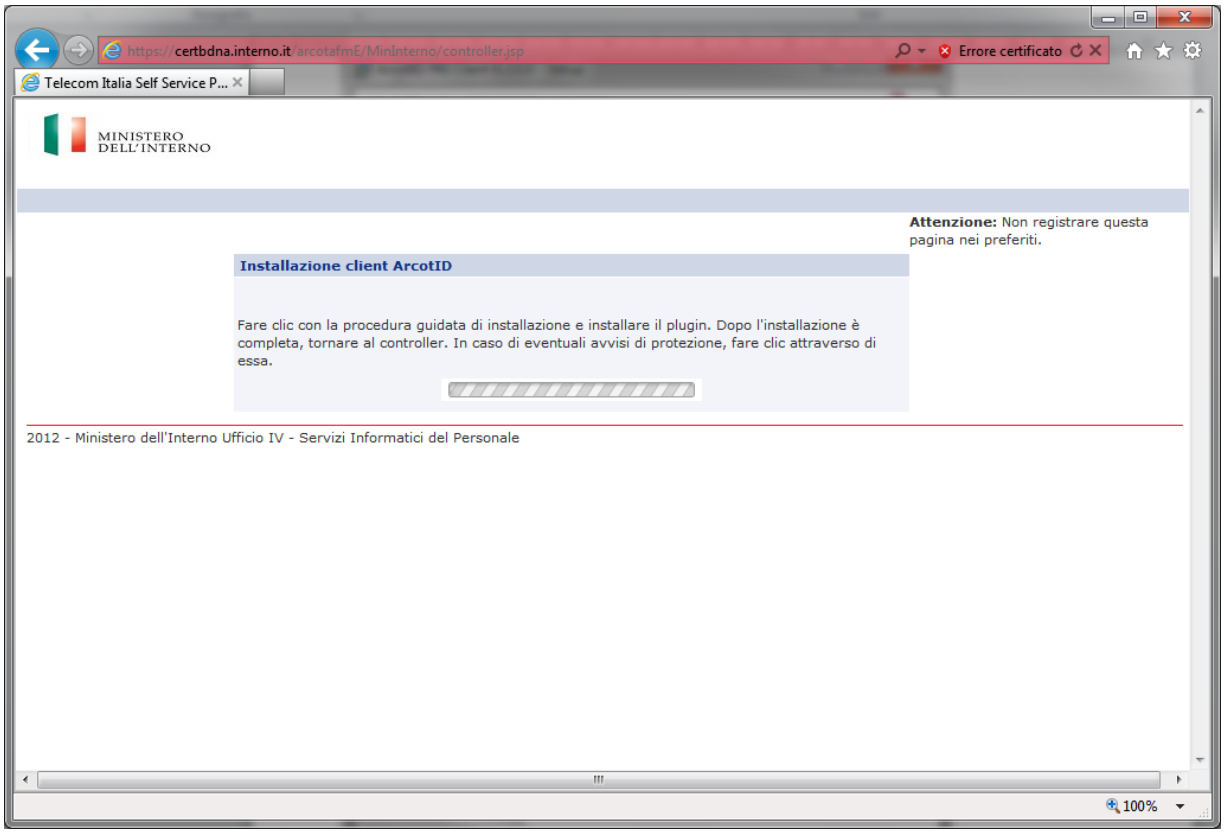



ArcotID PKI Client 6.2.0.0 - Setup
License Agreement
Please read the following license agreement carefully.
ARCOT
IMPORTANT: READ CAREFULLY BEFORE DOWNLOADING OR INSTALLING ANY PORTION OF THIS SOFTWARE
BY USING, COPYING OR DISTRIBUTING ALL OR ANY PORTION OF THE ARCOT SOFTWARE ("SOFTWARE") YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING THE LIMITATIONS, RESTRICTIONS, AND DISCLAIMERS.YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. THIS AGREEMENT IS ENFORCEABLE AGAINST YOU AND ANY LEGAL ENTITY THAT OBTAINED THE SOFTWARE AND ON WHOSE BEHALF IT IS USED. IF YOU DO NOT AGREE, DO NOT USE THIS SOFTWARE.
ARCOT OWNS OR HAS A LICENSE TO ALL INTELLECTUAL PROPERTY IN THE SOFTWARE.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Install
Cancel

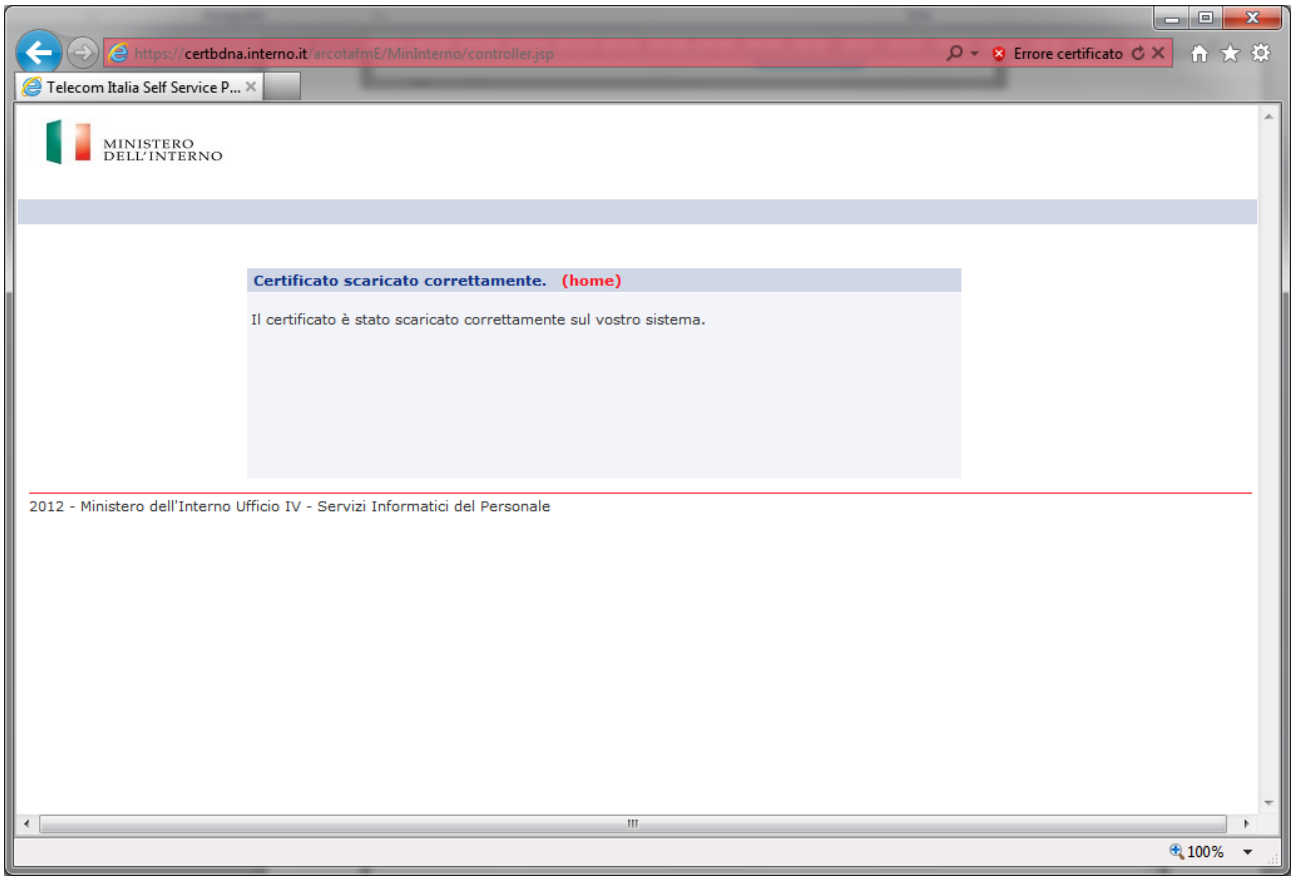

ArcotID PKI Client 6.2.0.0 - Setup
Installing ArcotID PKI Client 6.2.0.0
The program features you selected are being installed.
ARCOT
Please wait while Setup installs the ArcotID PKI Client 6.2.0.0 Software.
Status:
InstallShield
< Back
Next >
Cancel


ArcotID PKI Client 6.2.0.0 - Setup
Installation Complete
Setup has successfully installed ArcotID PKI Client 6.2.0.0.
Click on Finish to exit Setup.
ARCOT
< Back
Finish
Cancel

Attendere


https://certbdna.interno.it/arcotafmE/MinInterno/controller.jsp
Errore certificato
Telecom Italia Self Service P...
MINISTERO DELL'INTERNO
Attenzione: Non registrare questa pagina nei preferiti.
Installazione client ArcotID
Fare clic con la procedura guidata di installazione e installare il plugin. Dopo l'installazione è completa, tornare al controller. In caso di eventuali avvisi di protezione, fare clic attraverso di essa.
2012 - Ministero dell'Interno Ufficio IV - Servizi Informatici del Personale
100%

XII. Se le operazioni di installazione del certificato si sono concluse con esisto positivo, il sistema propone la finestra sotto indicata;



XIII. l'utente può effettuare l'uscita dal sistema di certificazione della postazione, selezionando "**home**".

N.B:Per controllare che il certificato sia stato scaricato con successo, verificare che la lunghezza del file **.aid** presente nella cartella **C:\Users*USERNAME*\AppData\Roaming\arcot\ids** sia di circa 9k.

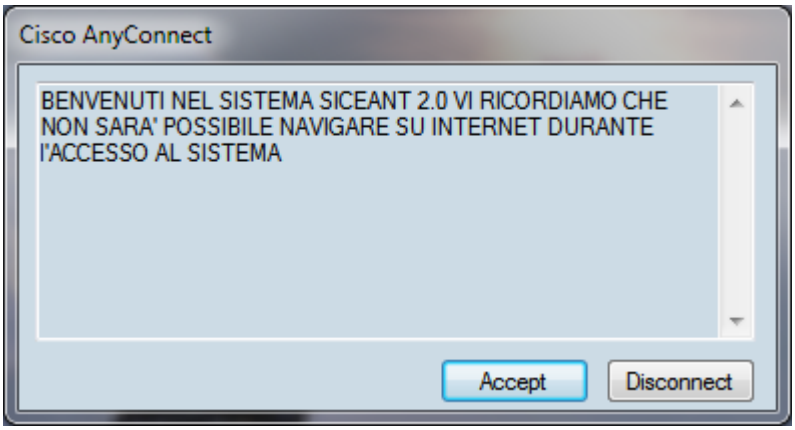
Accesso al Si.ce.ant.

Di seguito si riportano le operazioni per accedere all'applicativo Si.ce.ant.:

1. L'utente attiva il collegamento alla VPN usando il PIN del certificato digitale (vedi punto VIII del paragrafo precedente Certificazione della postazione UTENTE).
   Si ricorda che attivata la VPN non è più possibile la navigazione nel browser. In particolare occorre:
   a. Attivare "Cisco AnyConnect Secure Mobility Client";
   b. digitare il seguente indirizzo: vpnciv-gateway-i.interno.it;
   c. Cliccare su "Connect";

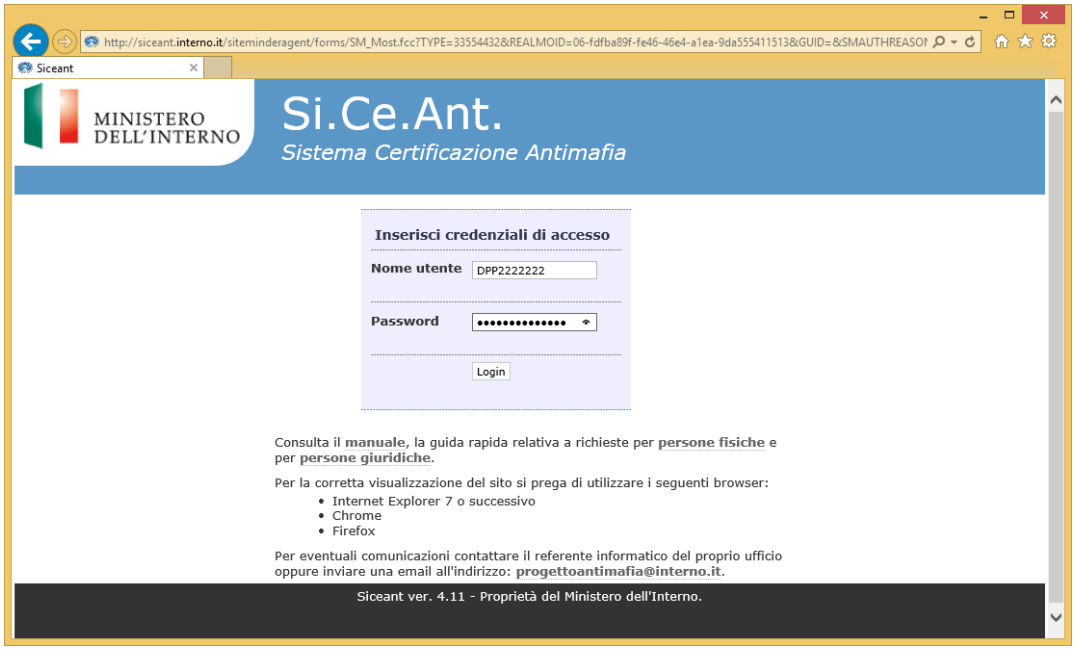
   d. Inserire il PIN del certificato digitale e cliccare su **OK**;

Viene visualizzato il messaggio sotto indicato;

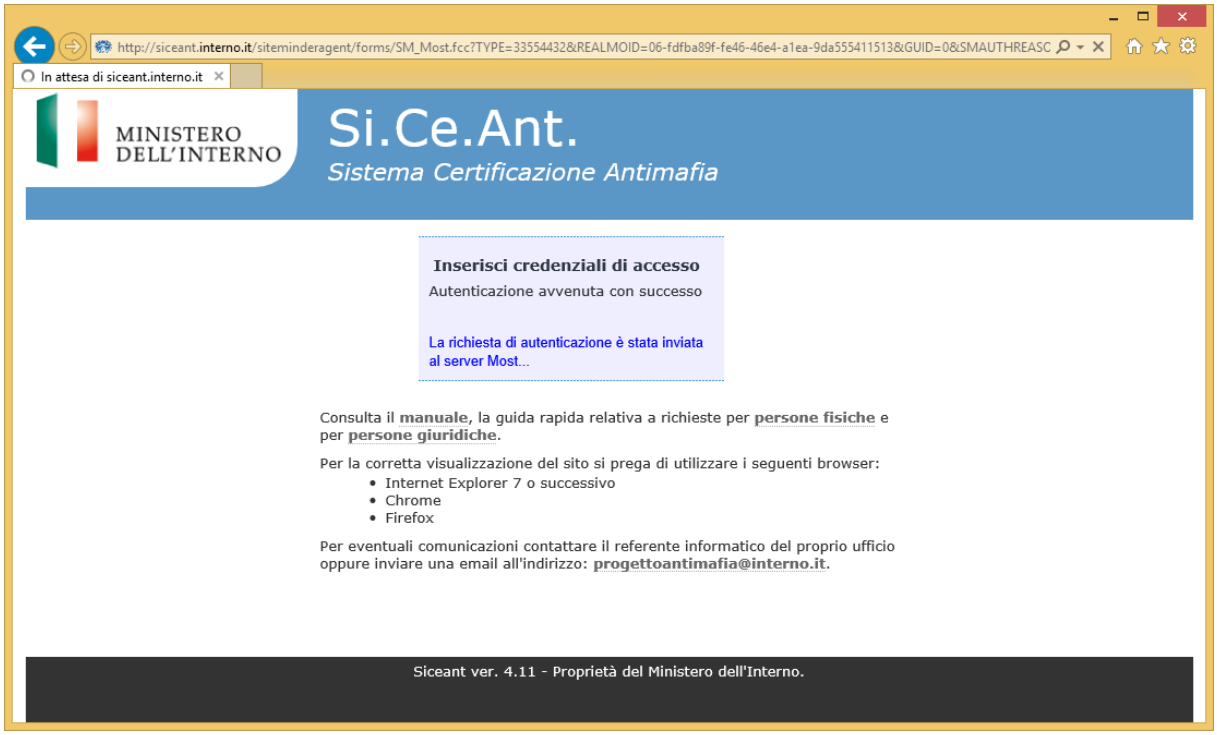


Per verificare che AnyConnect sia collegato correttamente controllare che sia presente l'icona con il lucchetto.

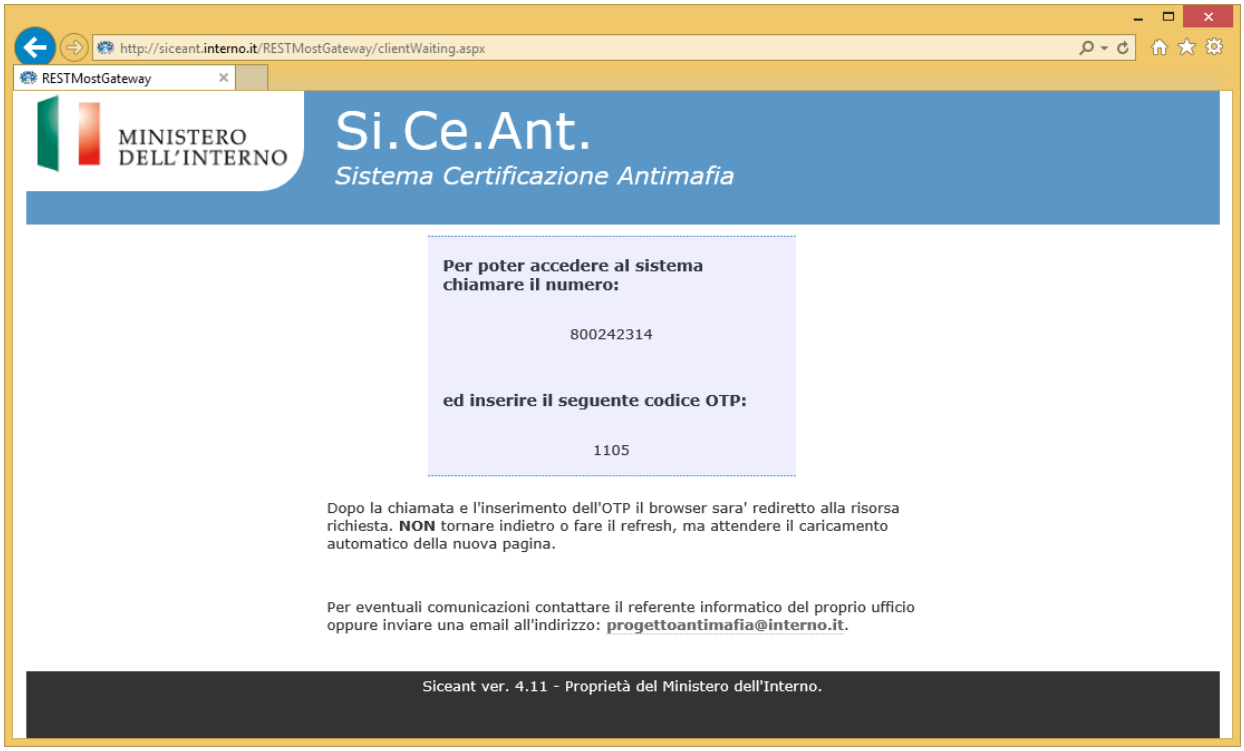
2. L'utente si collega all'indirizzo:
   http://siceant.interno.it
3. Digita le credenziali di accesso alla procedura Si.ce.ant(n.b: il **Nome utente** è lo Username fornito dalla Prefettura e la Password è quella ricevuta via e-mail e cambiata al primo accesso)



Cliccare su **Login** ed attendere…..



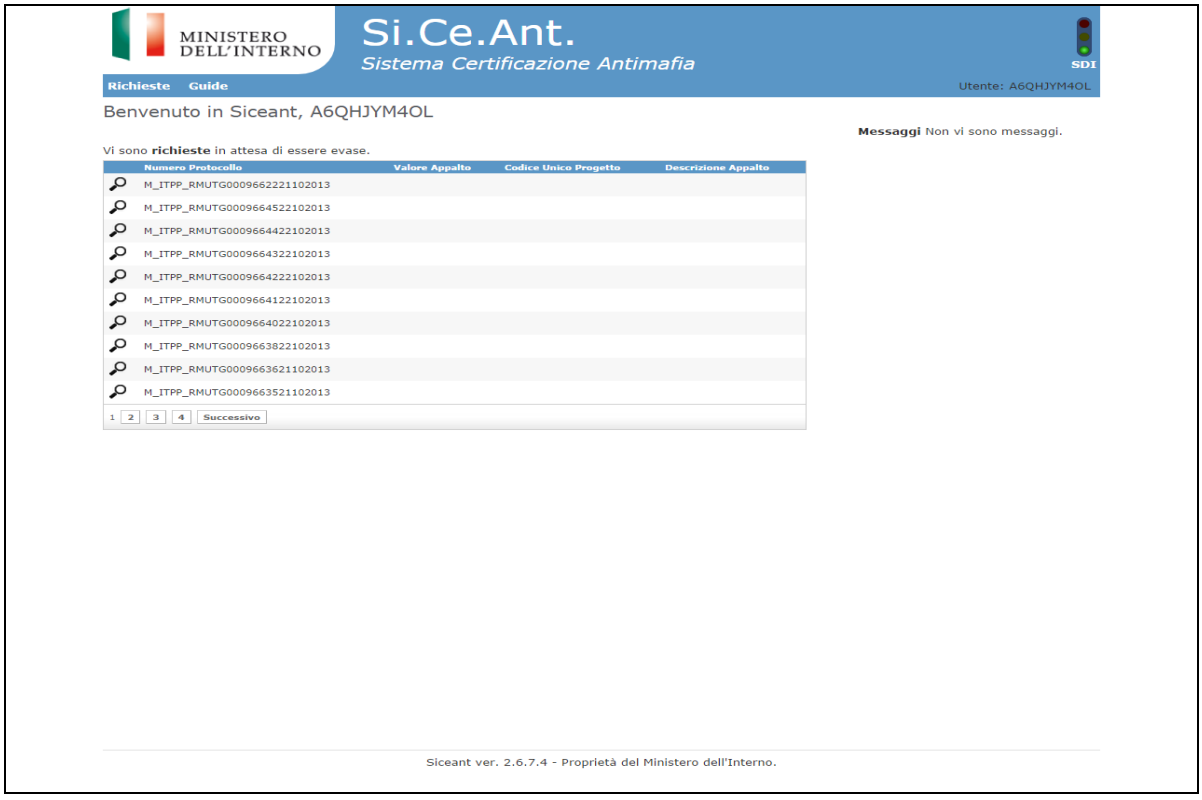
4. Se le credenziali sono corrette, verrà visualizzata la pagina di seguito riportata con il numero verde e una OTP:



5. L'utente deve contattare il numero verde indicato e digitare la OPT visualizzata a video;

6. Se l'operazione viene eseguita con successo, l'utente accede alle funzionalità del Si.ce.ant.

Accesso effettuato

7. 

ATTENZIONE

L'utente che accede al Si.Ce.Ant. può verificare se il collegamento con il servizio SDI è attivo, tramite il semaforo collocato in alto a destra sullo schermo, che deve indicare il colore verde. In caso contrario (colore rosso), la richiesta, se inoltrata, rimarrà nello stato di lavorazione, fino al momento in cui sarà ripristinato il collegamento con lo SDI.