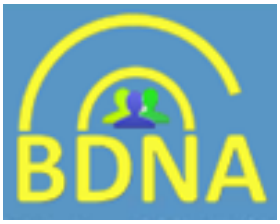
Ministero dell'Interno

DIPARTIMENTO PER LE POLITICHE DEL PERSONALE DELL'AMM. CIVILE E PER LE RISORSE STRUMENTALI E FINANZIARIE

DIREZIONE CENTRALE RISORSE FINANZIARIE E STRUMENTALI

UFFICIO IV - INNOVAZIONE TECNOLOGICA PER L'AMMINISTRAZIONE GENERALE



Nuove istruzioni operative di accesso

Stazioni Appaltanti e Prefetture

Premessa

Con l'avvio della BDNA è stata realizzata una nuova modalità di accesso tramite la quale non sarà più necessario, come succedeva con il vecchio applicativo Siceant, installare una VPN sul proprio computer.

La postazione utente viene ora virtualizzata e il certificato digitale, necessario per l'accesso, andrà installato una sola volta.

Per gli utenti già certificati con la vecchia modalità sarà necessario effettuare il cambio postazione di lavoro al primo accesso.

In questo manuale è possibile trovare informazioni su

1. Attività tecnica necessaria per lo start up
   - 1a Generalità sulla PASSWORD (PASSWORD DELL'APPLICATIVO)
   - 1b Abilitazione della postazione UTENTE (Citrix plug-in
   - 1c Installazione del PLUGIN di connessione alla postazione virtualizzata
2. Informazioni sui pulsanti presenti sul Portale di accesso
3. Certificazione dell'UTENTE
4. Cambio postazione di lavoro
5. Cambio PASSWORD DELL'APPLICATIVO
6. Cambio PIN (PASSWORD DEL CERTIFICATO)
7. PIN (PASSWORD DEL CERTIFICATO) DIMENTICATO
8. PIN (PASSWORD DEL CERTIFICATO) BLOCCATO
9. Accesso alla BDNA
10. Funzionalità di stampa e salvataggio del PDF

1 Attività tecnica necessaria per lo start up

Nota bene (**solo per le stazioni appaltanti**): L'operazione di abilitazione è possibile solo dopo aver ricevuto le credenziali rilasciate dalla Prefettura.

Generalità sulla PASSWORD (PASSWORD DELL'APPLICATIVO)

La password è sempre legata allo username rilasciata dalla prefettura ed è necessaria per accedere all'applicativo e alla certificazione della postazione di lavoro. Nell'esposizione di questo manuale, questa password sarà identificata come "**PASSWORD DELL'APPLICATIVO**".

Si ricorda che la password inviata in posta elettronica dalla prefettura di competenza, nasce "*scaduta*" e DEVE essere modificata al primo accesso.

La password (**PASSWORD DELL'APPLICATIVO*)*** deve avere le seguenti caratteristiche:

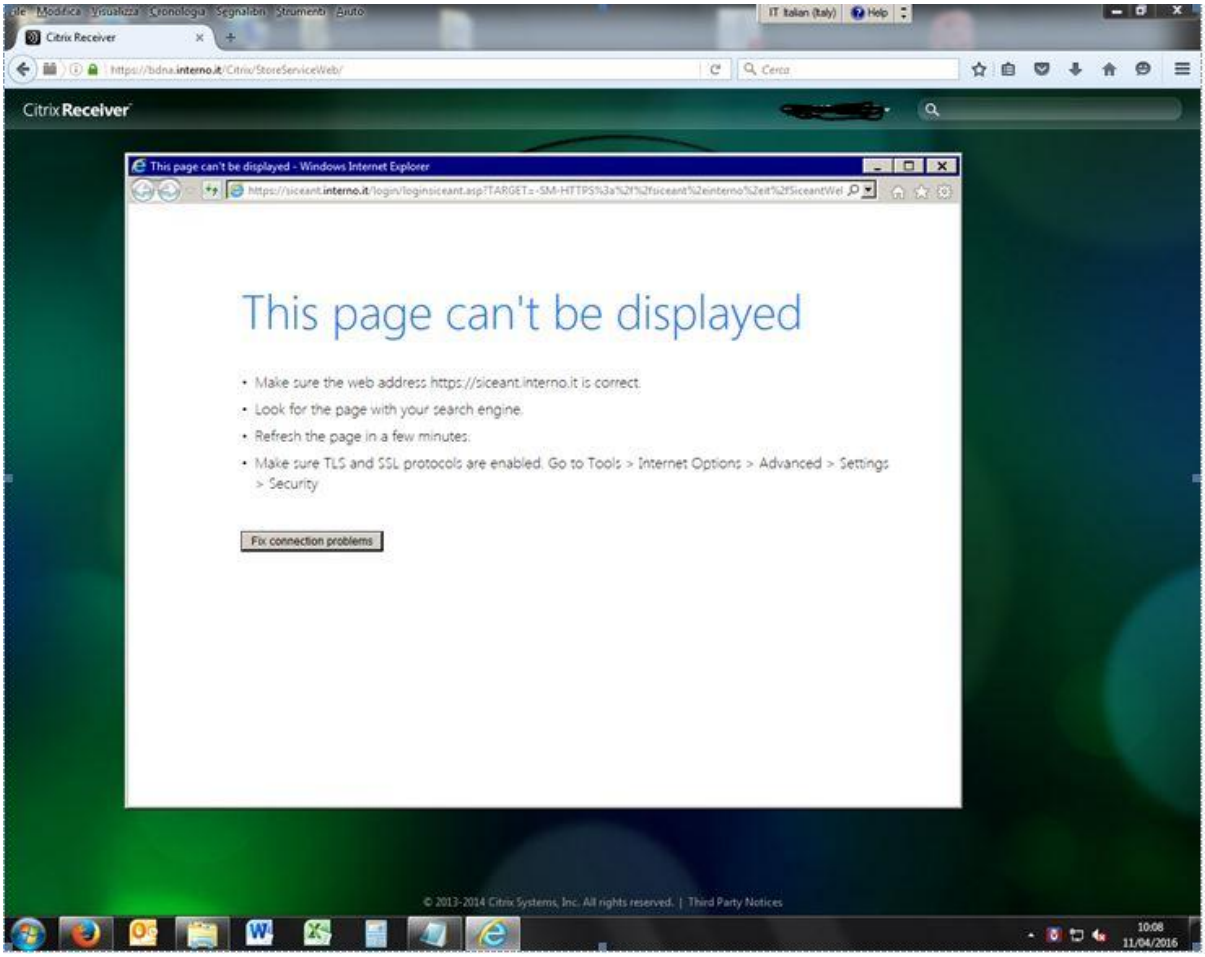
. deve essere diversa dalle ultime 2 password utilizzate
. non deve contenere il cognome o il nome o parti di essi
. deve contenere da un minimo di 10 a un massimo di 14 caratteri.
E' necessario rispettare il limite massimo.
. deve contenere almeno 1 lettera maiuscola e almeno 6 caratteri alfabetici tra maiuscole e minuscole
. deve contenere almeno 1 numero
. deve contenere almeno 1 carattere speciale **esclusi * £ $ € & !**

i caratteri speciali consigliati perché verificati sono

. (punto)
@ (at)

AVVISO

Al momento della creazione della Password dell'applicativo è necessario fare attenzione a non superare i 14 caratteri perché sono comunque accettati, ma al momento dell'utilizzo verrà segnalato l'errore con la seguente schermata:



Abilitazione della postazione UTENTE (Citrix plug-in).

Premesse all'installazione

Il plug-in Citrix è compatibile con i sistemi operativi Windows successivi a XP e con i sistemi operativi Mac e Linux.

Se sulla postazione che si deve utilizzare è presente Windows XP si deve controllare che sia la versione XP SP3 e in questo caso per l'installazione si può scaricare la versione compatibile al seguente indirizzo:

https://www.citrix.it/downloads/xendesktop/legacy-client-software/receiver-for-windows-401.html

Se il plug-in è già presente sul computer l' attività di installazione non sarà necessaria e si potrà passare direttamente alla certificazione dell'utente.

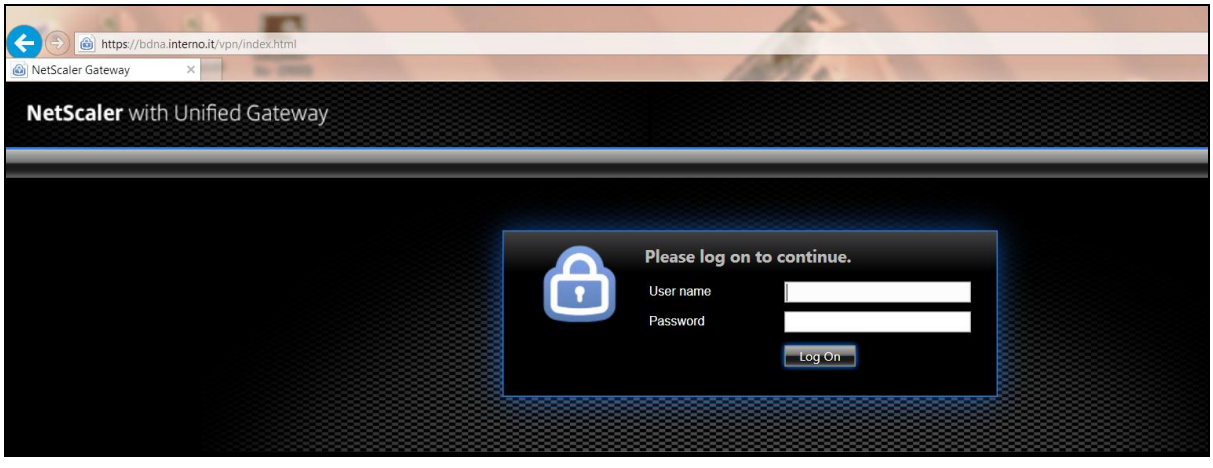
Installazione del PLUGIN di connessione alla postazione virtualizzata

Aprire il browser utilizzato abitualmente sulla postazione
(Internet Explorer, Chrome, Firefox, Safari) e connettersi all'indirizzo:

https://bdna.interno.it (se STAZIONE APPALTANTE)
(username diverso "dppxxxxxxx")

https://bdna.dippp.interno.it (se PREFETTURA)
(username che inizia con "dpp")

La prima schermata proposta dopo il collegamento è la seguente.

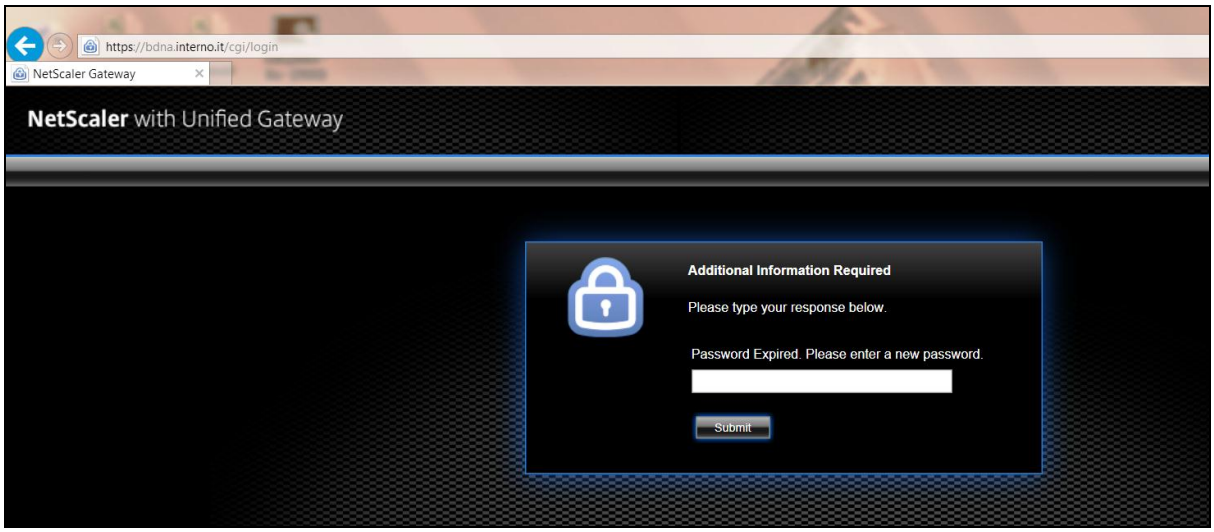


Digitare nelle rispettive caselle lo USERNAME e la PASSWORD ricevuti in Prefettura.

Come già detto nelle *"generalità sulla password (*PASSWORD DELL'APPLICATIVO*)"* la password inviata in posta elettronica dalla prefettura di competenza, nasce "*scaduta*" e DEVE essere modificata al primo accesso.

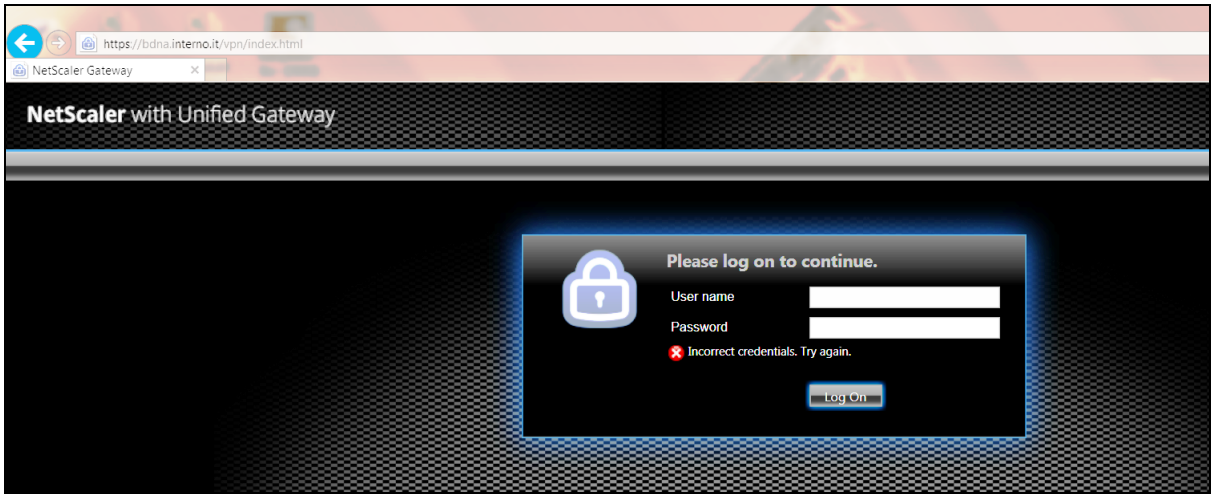
Viene quindi proposta la maschera per il "*primo cambio password"* .

Inserire una password composta secondo i criteri esposti nelle "*generalità sulla password (password dell'applicativo)"*, annotarla e conservarla con cura.



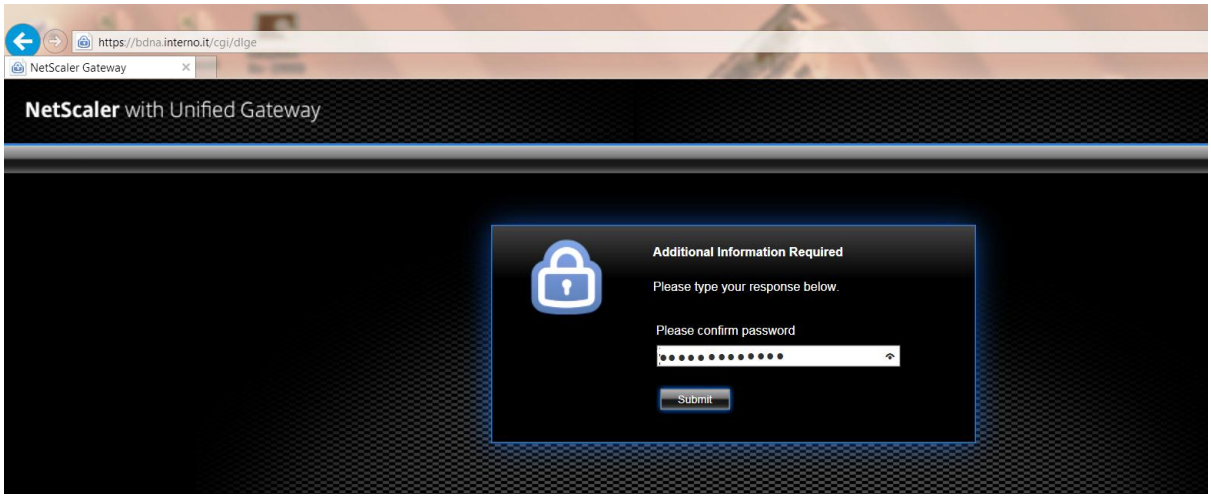
ATTENZIONE

Se la composizione della password NON rispetta i criteri precedentemente indicati verrà segnalato l'errore

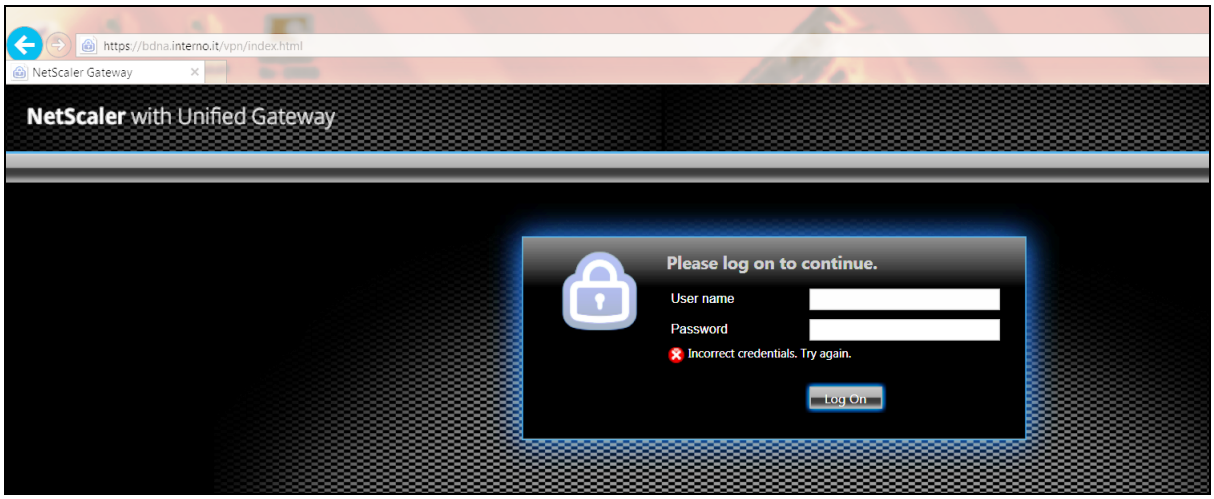


Altrimenti viene richiesta la conferma della password appena inserita.

Confermarla digitandola nuovamente.

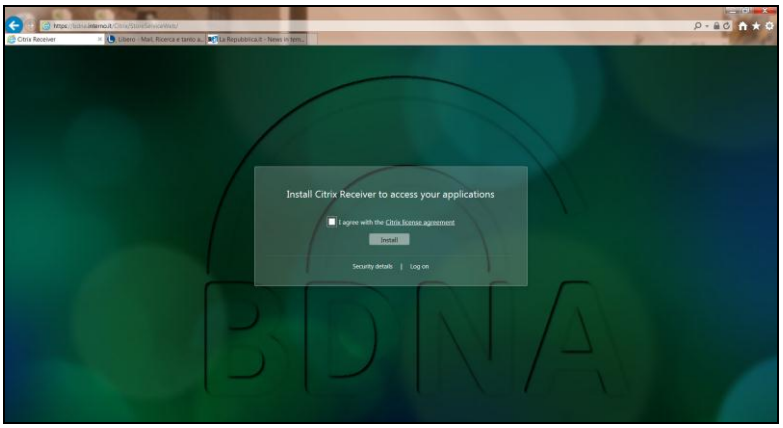


In caso di digitazione errata viene segnalato l'errore.

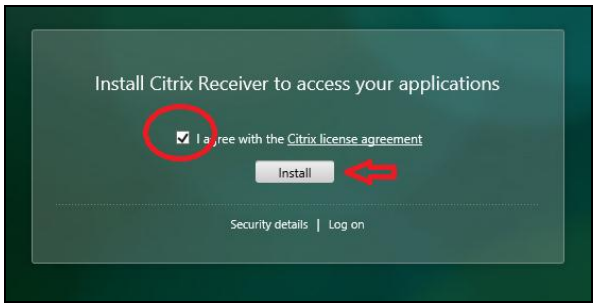


Ripetere l'inserimento ripartendo dalla digitazione dello USERNAME e la PASSWORD ricevuti in Prefettura.

Dopo aver effettuato l'inserimento delle credenziali e il primo cambio password si procede con il download e l'installazione di Citrix

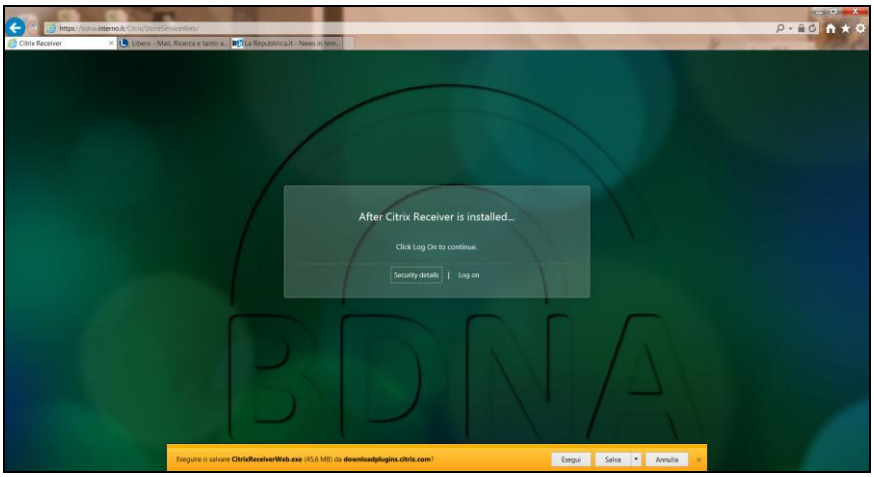


Alla richiesta di installazione del Citrix Receiver accettare le condizioni della licenza cliccando nel check e poi su INSTALL



Inizierà il download del plug-in di Citrix che chiederà l'autorizzazione per proseguire.

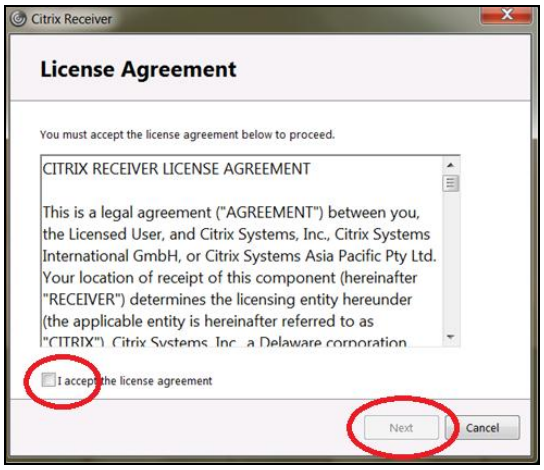
Cliccare, quindi, su ESEGUI (o Install se viene usata una versione in inglese) e attendere il completamento del download.



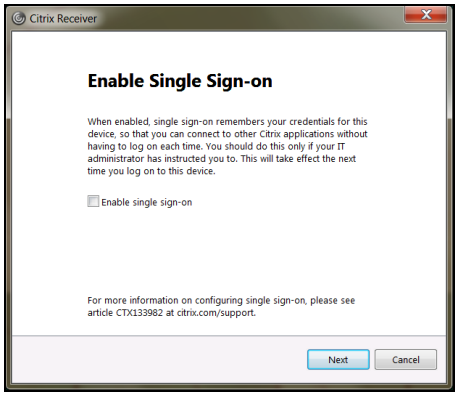
Al termine del download di CitrixReceiver.exe cliccare su ESEGUI (o Install se viene usata una versione in inglese).

L'installazione presenterà una successione di maschere alle quali è necessario rispondere come di seguito indicato:

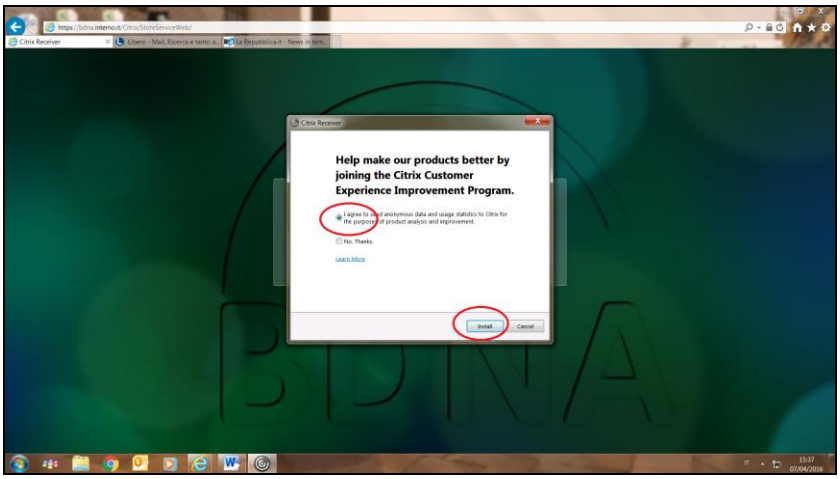
Selezionare **Start**



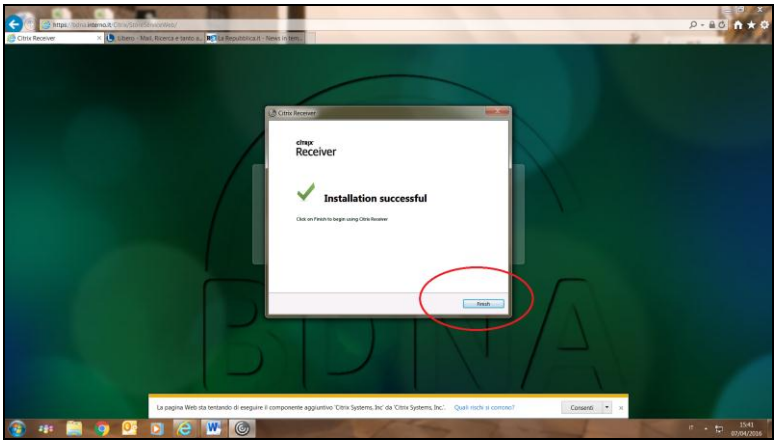
Accettare le condizioni e continuare con **Next**



continuare con **Next**

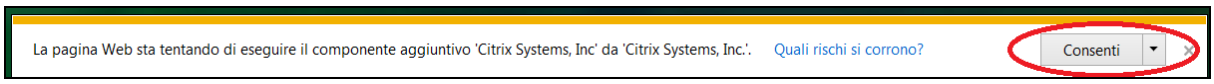


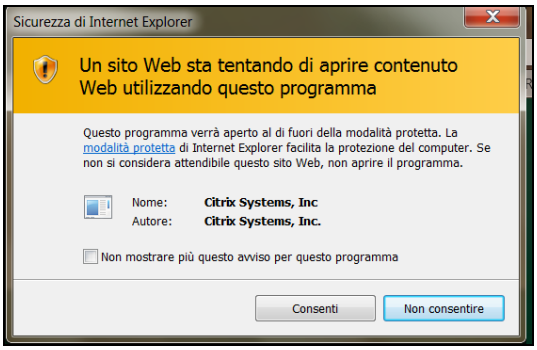
continuare con **Install**

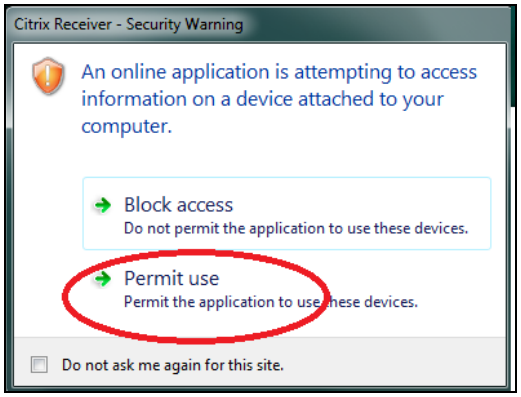


Al termine dell'installazione selezionare **Finish**

Il plugin "Citrix Receiver" potrebbe, in base alle impostazioni e al tipo di browser, richiedere a video delle autorizzazioni. Cliccare su **PERMIT** o **Consenti** (a seconda della versione che viene mostrata) per attivare la componente software appena scaricata e autorizzarne l'esecuzione.



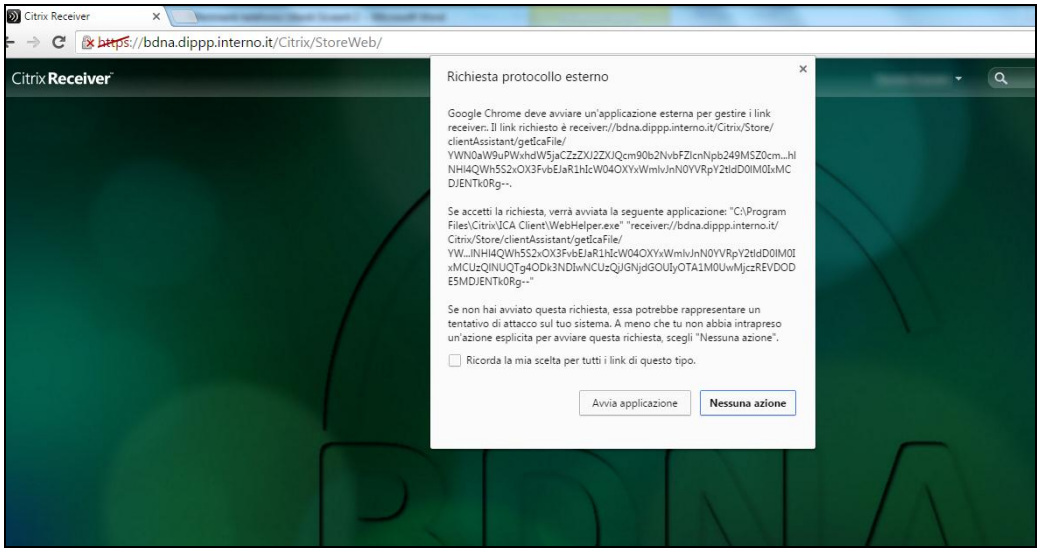




Completata quindi l'installazione del PLUGIN passare alla certificazione della postazione utente.

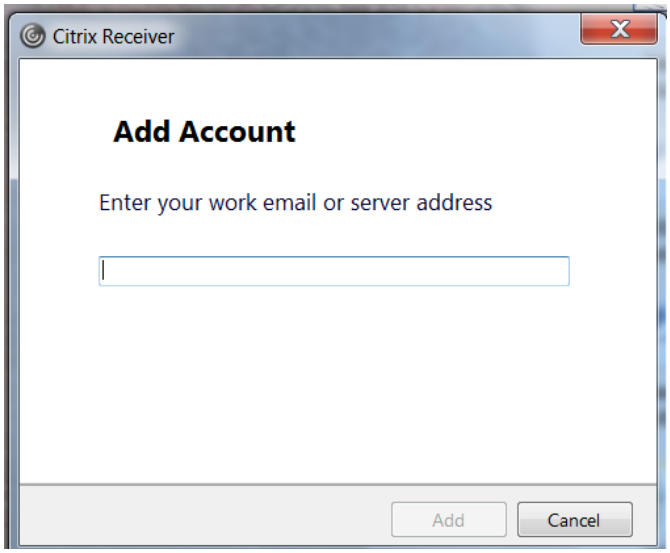
Controllare che tra una eventuale modifica della password (PASSWORD DELL'APPLICATIVO) relativa all'utenza (username) e la certificazione dell'utente **siano trascorsi 10 minuti** per avere la certezza del buon esito dell'operazione. Terminata l'attesa procedere all'accesso.

N.B. Nel caso di utilizzo di browser diversi da Internet Explorer potrebbe essere necessario, come nell'esempio sottostante, fornire ulteriori autorizzazioni all'esecuzione del plug-in.



AVVISO

A seguito dell'installazione di Citrix all'accensione del PC verrà proposta la seguente schermata



La richiesta non va presa in considerazione, quindi selezionare "*Cancel*" o chiudere la finestra per continuare.

2) Informazioni sui pulsanti presenti sul Portale di accesso

Sul portale sono presenti 2 pulsanti che identificano due rami distinti della procedura

CERTBDNA che permette le seguenti funzioni:

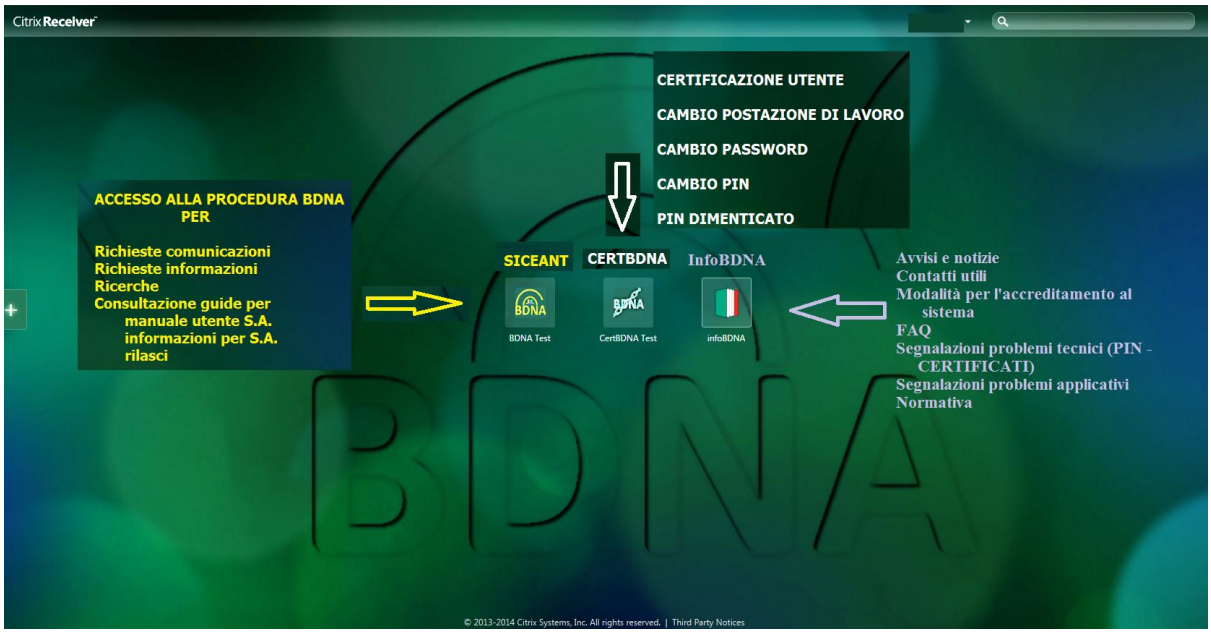
certificazione utente
cambio postazione lavoro
cambio password
cambio pin
pin dimenticato

SICEANT che permette le seguenti funzioni:

ricerche comunicazioni
ricerche informazioni
ricerche
consultazione guide per manuale utente S.A.
informazioni S.A.
rilasci

InfoBDNA che permette di consultare gli avvisi, la documentazione, le FAQ, le modalità di segnalazione problemi tecnici e applicati, la normativa di riferimento

come mostrato nella schermata che segue



3) Certificazione dell'UTENTE

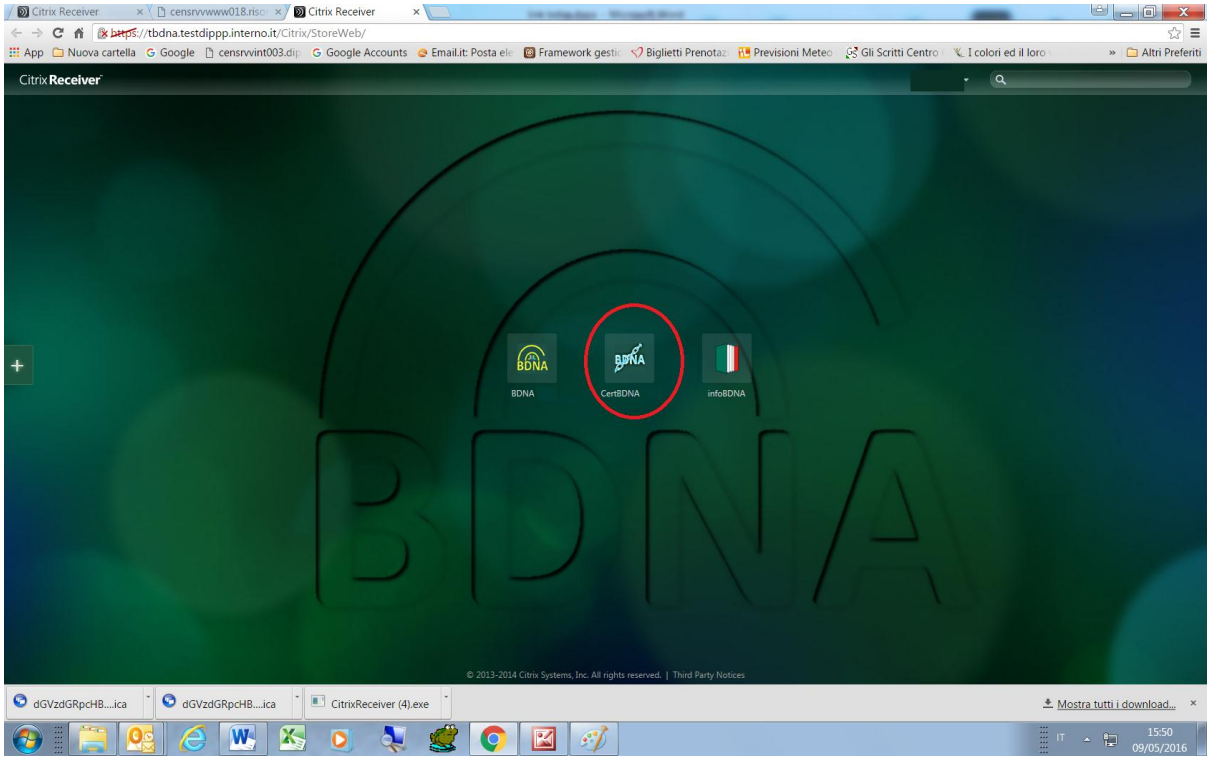
L'operazione di certificazione dell'utente è necessaria per scaricare il certificato digitale intestato all'utente BDNA sulla postazione virtuale.

Il portale "**CertBdna"** verrà utilizzato per

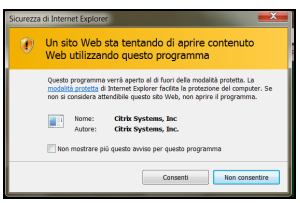
. certificare i nuovi utenti o per ri-certificare utenti il cui certificato è scaduto (ogni certificato scaricato ha la validità di 1 anno)

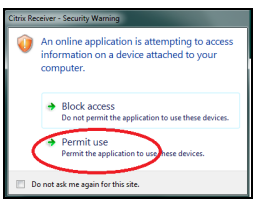
. eseguire la funzione "*cambio postazione di lavoro*" da parte di coloro che già in passato accedevano alla procedura Siceant tramite la VPN.

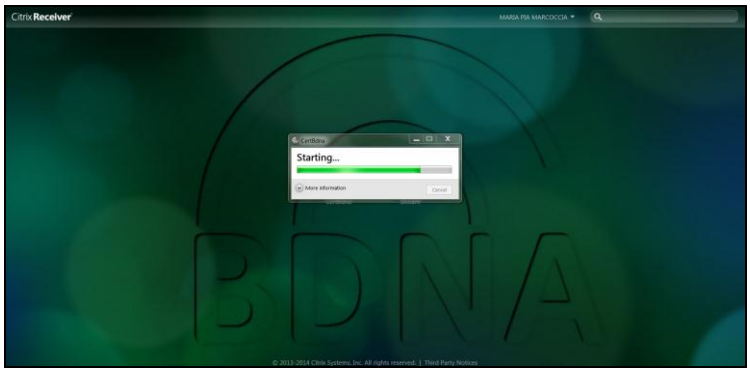
Cliccare sull'icona **CertBdna**



E' possibile che vengano richieste autorizzazioni a procedere come già descritto in precedenza. Continuare con **consenti** o **permit**





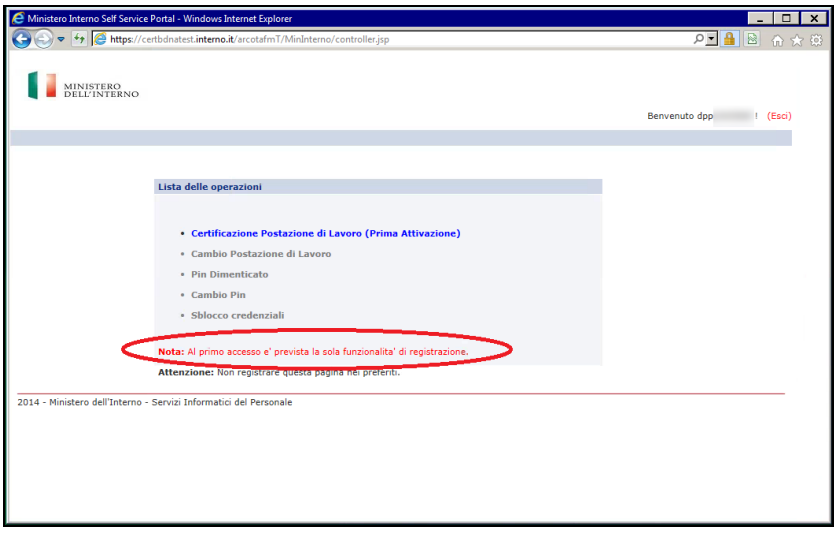


All'apertura della finestra di accesso digitare le proprie credenziali , ossia lo USERNAME (consegnato dalla Prefettura) e la PASSWORD DELL'APPLICATIVO (la nuova generata in sostituzione di quella già scaduta ricevuta dalla Prefettura)

Viene proposto il menù delle funzioni. Quelle in blu sono attive mentre quelle grigie non lo sono.
Per ovvi motivi di sicurezza sulla maschera è stato posto un avviso nel quale si prescrive di non registrare questa pagina nei preferiti. **Rispettare l'indicazione.**

Come evidenziato in rosso sulla maschera, al primo accesso è attiva solo la funzione di "*Certificazione Postazione di lavoro (Prima Attivazione)*"

Assicurarsi di avere a portata di mano il cellulare il cui numero è stato fornito al momento dell'accreditamento in Prefettura.
Per la certificazione della postazione di lavoro sarà necessario interagire con il cellulare.
Selezionare quindi "*Certificazione Postazione di lavoro (Prima Attivazione)*"



Sul cellulare arriverà un sms contenente la OTP (One Time Password) cioè un codice numerico utilizzabile solo una volta che dovrà essere digitato nella casella con l'indicazione "*Inserisci la tua OTP"*
A fianco della casella viene proposto di selezionare la funzione "Visualizza i caratteri". Selezionandola si può controllare quanto si sta digitando, altrimenti, o deselezionandola, i caratteri digitati saranno criptati.

La successiva maschera permetterà di impostare il PIN (PASSWORD DEL CERTIFICATO).
Il PIN (PASSWORD DEL CERTIFICATO) deve avere le seguenti caratteristiche:

. deve essere diversa dalle ultime 2 password utilizzate
. non deve contenere il cognome o il nome o parti di essi
. deve contenere da un minimo di 10 a un massimo di 14 caratteri
E' necessario rispettare il limite massimo.
. deve contenere almeno 1 lettera maiuscola e almeno 6 caratteri alfabetici tra maiuscole e minuscole
. deve contenere almeno 1 numero
. deve contenere almeno 1 carattere speciale **esclusi * £ $ € & !**

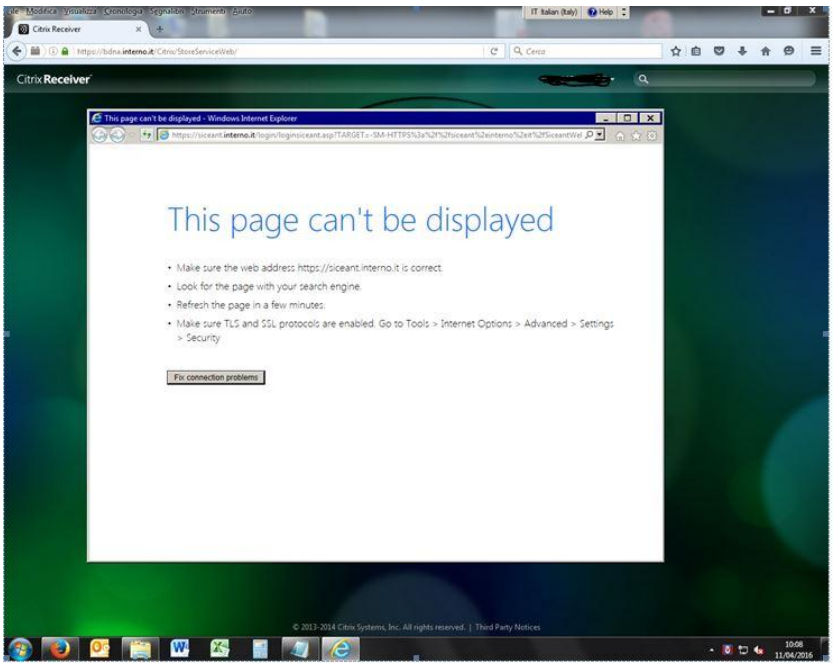
i caratteri speciali consigliati perché verificati sono

. (punto)
@ (at)

Comporre quindi con le regole suddette il PIN (PASSWORD DEL CERTIFICATO), **annotarlo e conservarlo con cura**.

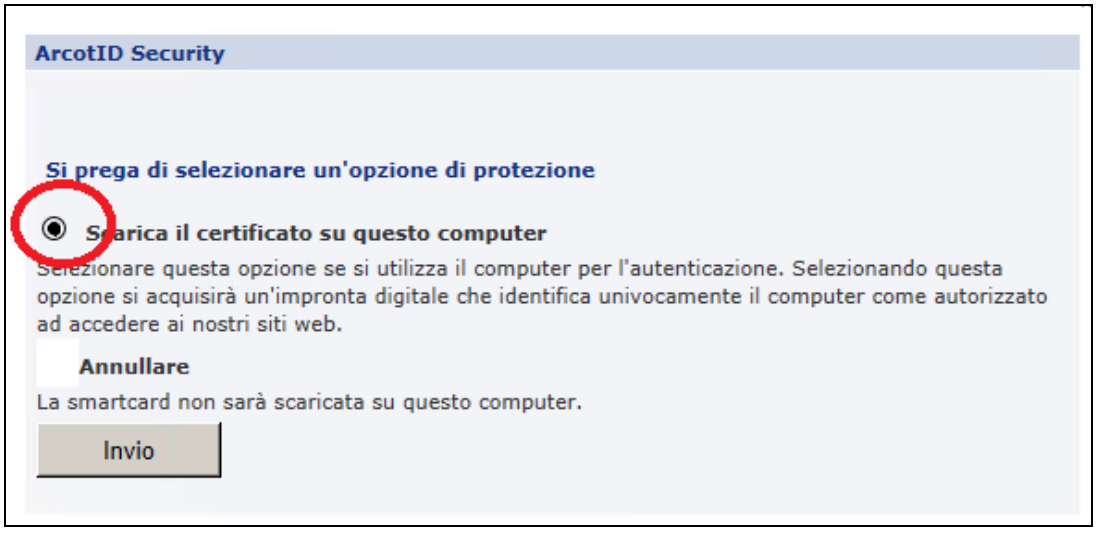
AVVISO

Al momento della creazione della Password del certificato (PIN) è necessario fare attenzione a non superare i 14 caratteri perché sono comunque accettati, ma al momento dell'utilizzo verrà segnalato l'errore con la seguente schermata:

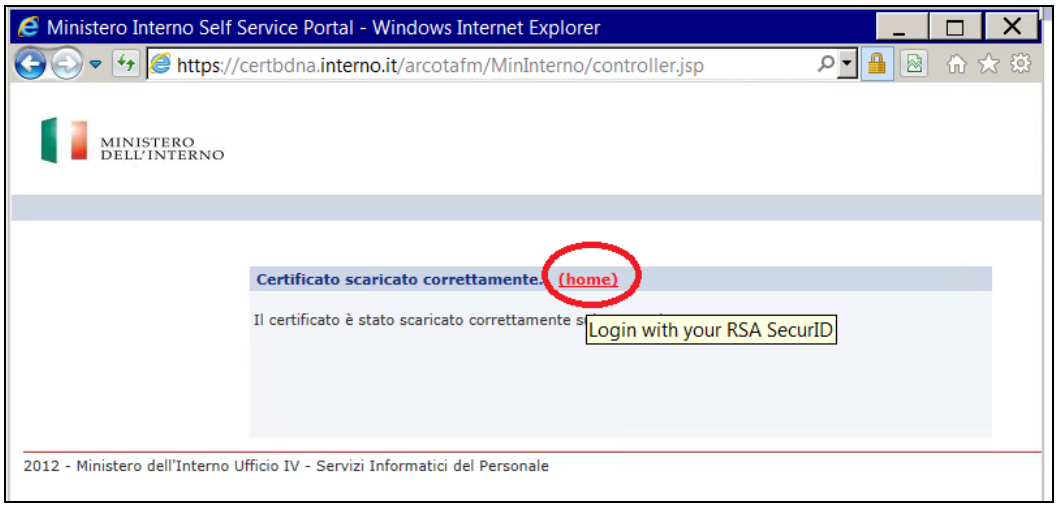


Inserire il PIN (PASSWORD DEL CERTIFICATO) nella casella denominata "*Nuovo Pin*" e poi riscriverlo nella casella denominata "*Conferma Nuovo Pin*".
Selezionare quindi **Invio**.

Il certificato riservato all'utente deve essere scaricato sulla macchina virtuale. Procedere quindi con la seguente maschera, selezionando la voce "*Scarica il certificato su questo computer*" e il successivo **Invio**.



Il sistema comunica che il certificato è stato scaricato correttamente presentando la maschera che segue.



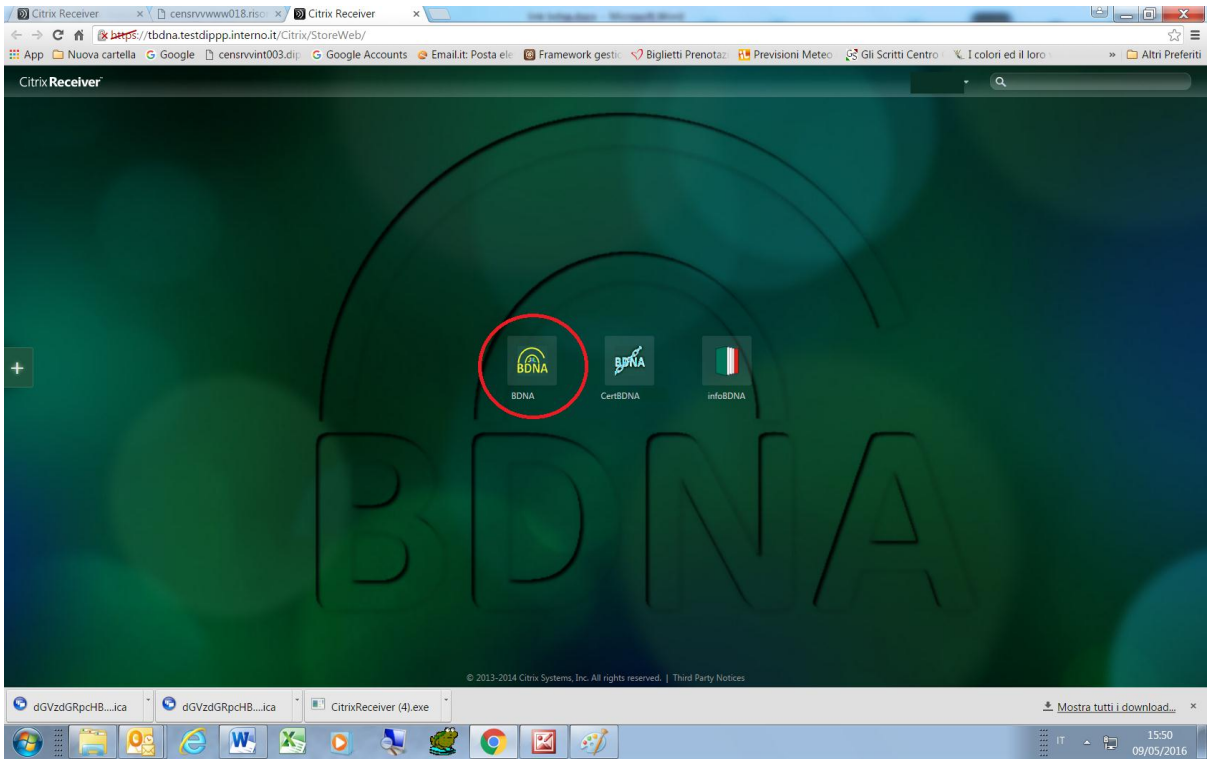
Selezionando la voce evidenziata in rosso **(home),** come avverte il messaggio, si potrà procedere con il login alla BDNA con il proprio certificato di sicurezza.

4) Cambio postazione di lavoro

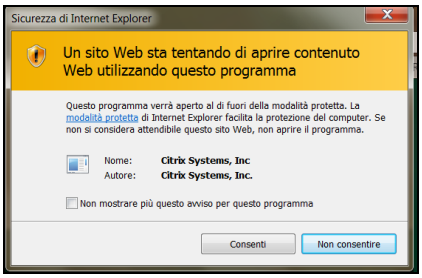
La funzione "**Cambio postazione di lavoro**" permette:

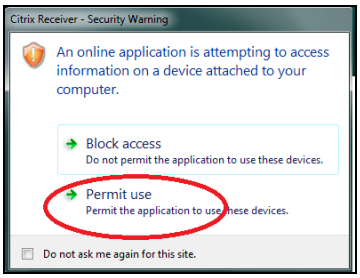
. di scaricare il certificato digitale su una nuova postazione di lavoro (quindi, per chi lavora con la vecchia macchina virtuale VPN, di passare alla nuova macchina virtuale Citrix)

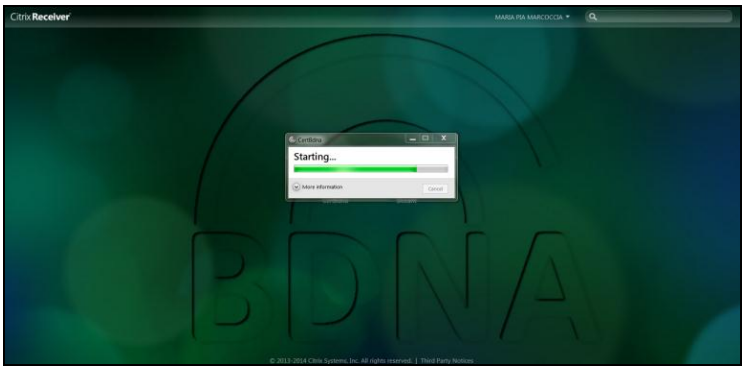
Cliccare sull'icona **CertBdna**



E' possibile che vengano richieste autorizzazioni a procedere come già descritto in precedenza. Continuare con **consenti** o **permit**







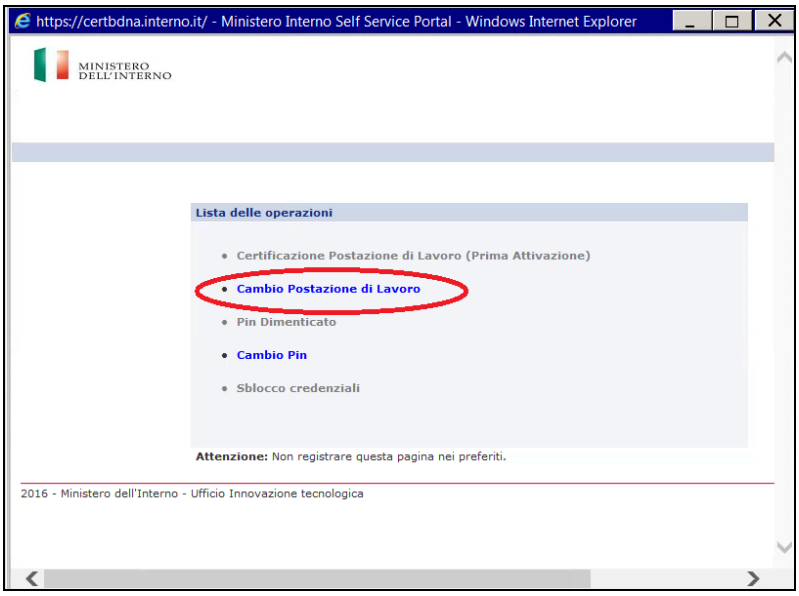
All'apertura della finestra di accesso digitare le proprie credenziali , ossia lo USERNAME e la PASSWORD DELL'APPLICATIVO

Per ovvi motivi di sicurezza sulla maschera è stato posto un avviso nel quale si prescrive di non registrare questa pagina nei preferiti. **Rispettare l'indicazione.**

Viene proposto il menù delle funzioni.
Sono attive due funzioni:
. Cambio Postazione di Lavoro
. Cambio Pin

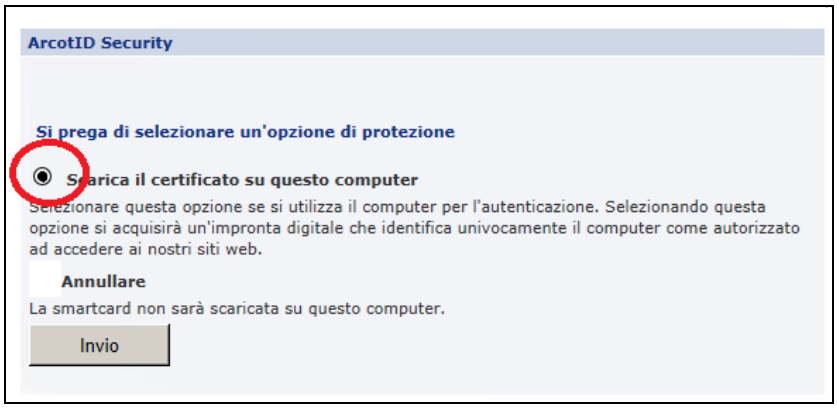
Assicurarsi di avere a portata di mano il cellulare il cui numero è stato fornito al momento dell'accreditamento in Prefettura.
Per la certificazione della postazione di lavoro sarà necessario interagire con il cellulare.

Selezionare quindi "*Cambio Postazione di Lavoro*"

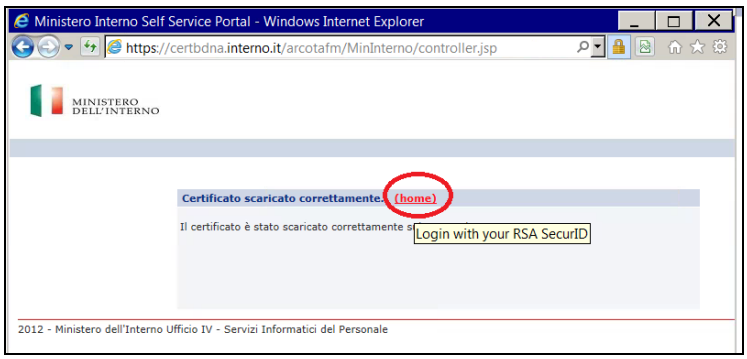


Sul cellulare arriverà un sms contenente la OTP (One Time Password) cioè un codice numerico utilizzabile solo una volta che dovrà essere digitato nella casella con l'indicazione "*Inserisci la tua OTP"*
A fianco della casella viene proposto di selezionare la funzione "Visualizza i caratteri". Selezionandola si può controllare quanto si sta digitando, altrimenti, o deselezionandola, i caratteri digitati saranno criptati.

Procedere quindi con la seguente maschera, selezionando la voce "*Scarica il certificato su questo computer*" e il successivo **Invio**.



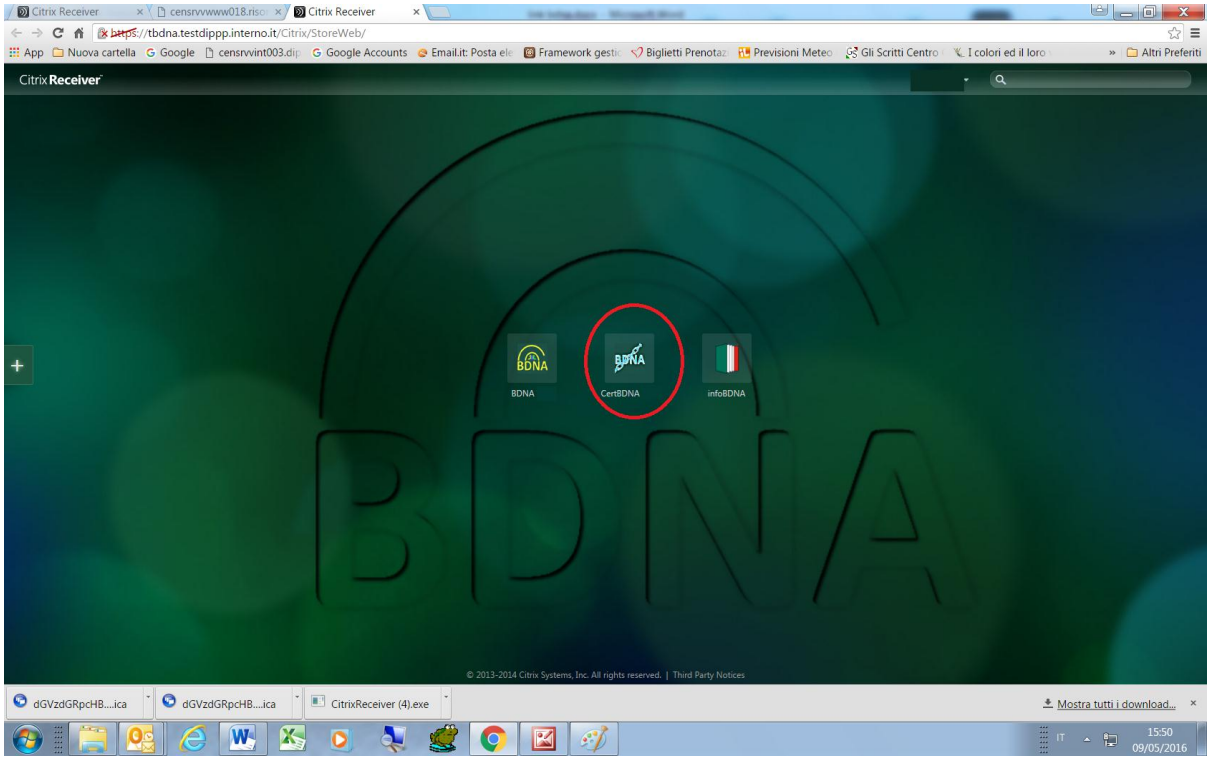
Il sistema comunica che il certificato è stato scaricato correttamente presentando la maschera che segue.



Selezionando la voce evidenziata in rosso **(home),** come avverte il messaggio, si potrà procedere con il login alla BDNA con il proprio certificato di sicurezza.

5) Cambio PASSWORD DELL'APPLICATIVO

Per accedere a questa funzione è necessario accedere nel portale Citrix nel ramo **CERTBDNA**



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

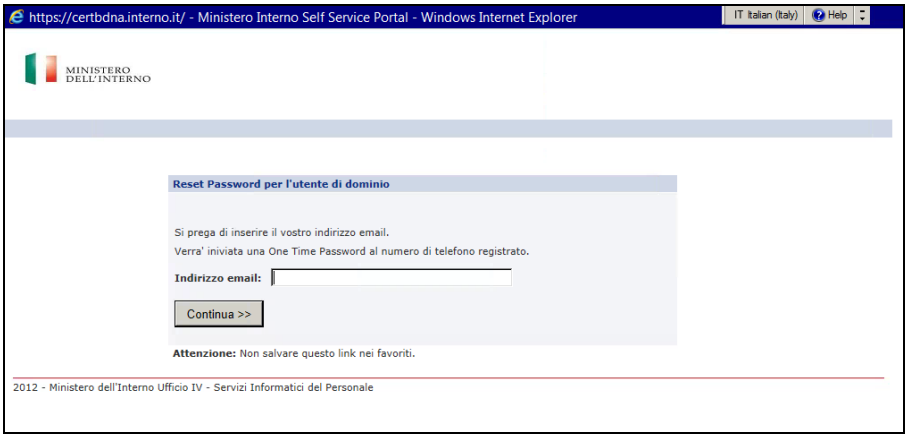
N.B. Solo le S.A. possono usare la funzione cambio password.

Per le Prefetture la password è la stessa del dominio.

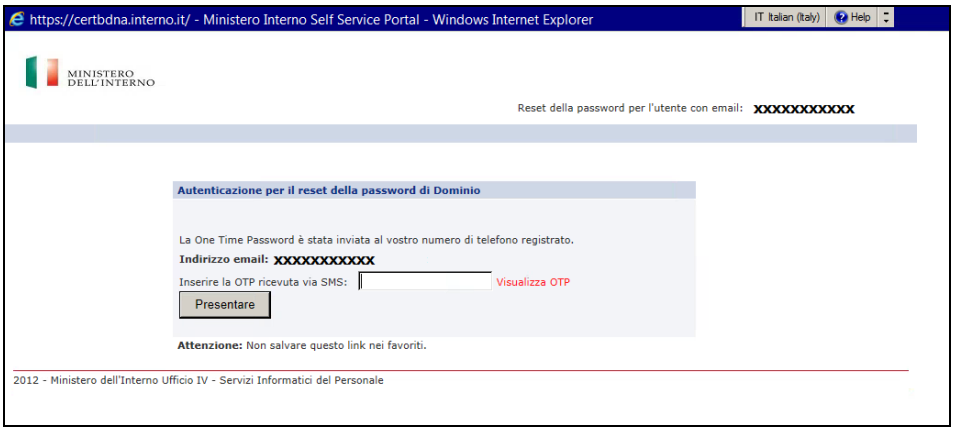
E' possibile effettuare il **cambio password** cliccando sul link "Password dimenticata/Cambio Password" **senza digitare le credenziali**.

Verrà richiesto di digitare l'indirizzo email accreditato e cliccare su Continua >>

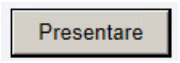
Successivamente sul proprio cellulare arriverà un sms con una OTP.



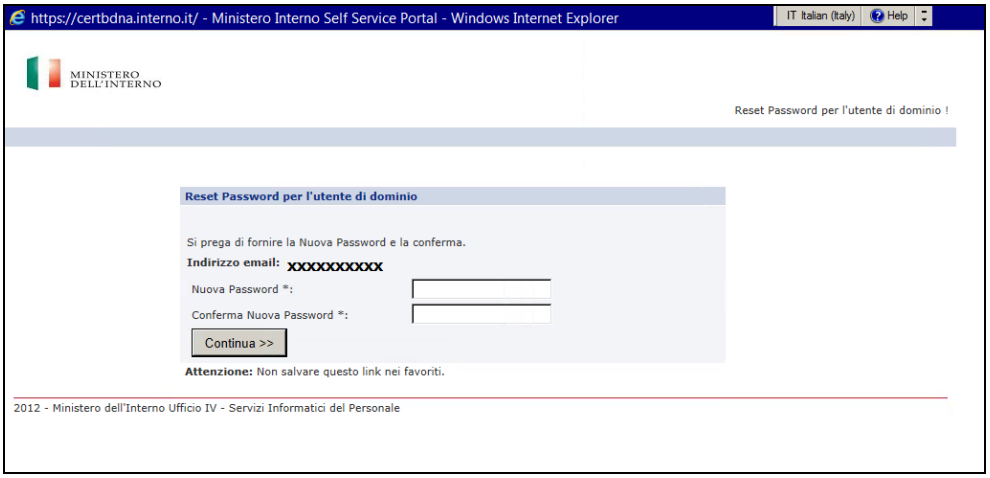
Digitare nella casella la OTP ricevuta via SMS.



Selezionando "Visualizza OTP" si può controllare quanto digitato.

Per continuare il cambio password cliccare sul pulsante 

che presenterà la maschera del cambio password.



La password (**PASSWORD DELL'APPLICATIVO*)* deve avere le seguenti caratteristiche:

. deve essere diversa dalle ultime 2 password utilizzate
. non deve contenere il cognome o il nome o parte di essi
. deve contenere da un minimo di 10 a un massimo di 14 caratteri
  E' necessario rispettare il limite massimo.
. deve contenere almeno 1 lettera maiuscola e almeno 6 caratteri alfabetici tra maiuscole e minuscole
. deve contenere almeno 1 numero
. deve contenere almeno 1 carattere speciale **esclusi * £ $ € & !**

i caratteri speciali consigliati perché verificati sono

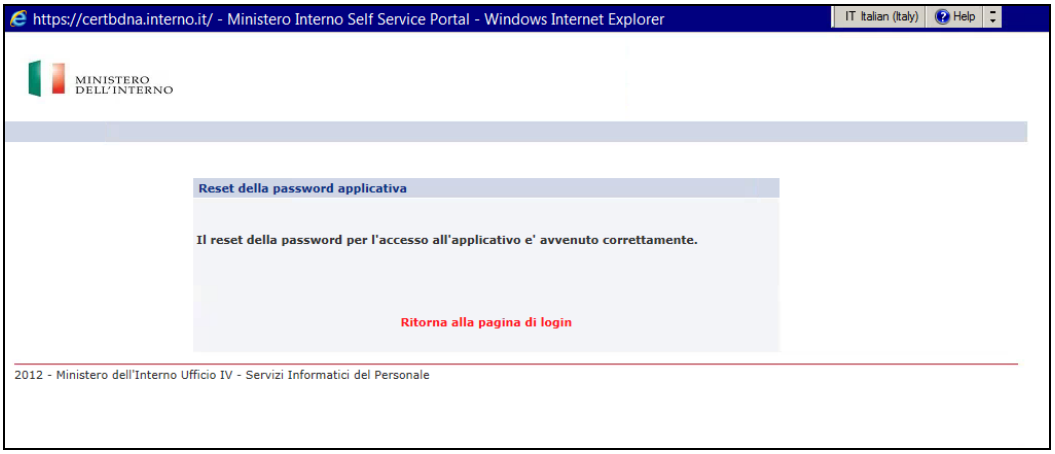
. (punto)
@ (at)

Digitare la nuova password e ripeterla nella casella successiva per conferma e

concludere con il pulsante 

Nella successiva schermata l'avvenuto cambiamento della password viene confermato con l'indicazione

Il reset della password per l'accesso all'applicativo e' avvenuto correttamente.



Selezionando **Ritorna alla pagina di login** si ritorna alla schermata di inserimento credenziali.

ATTENZIONE

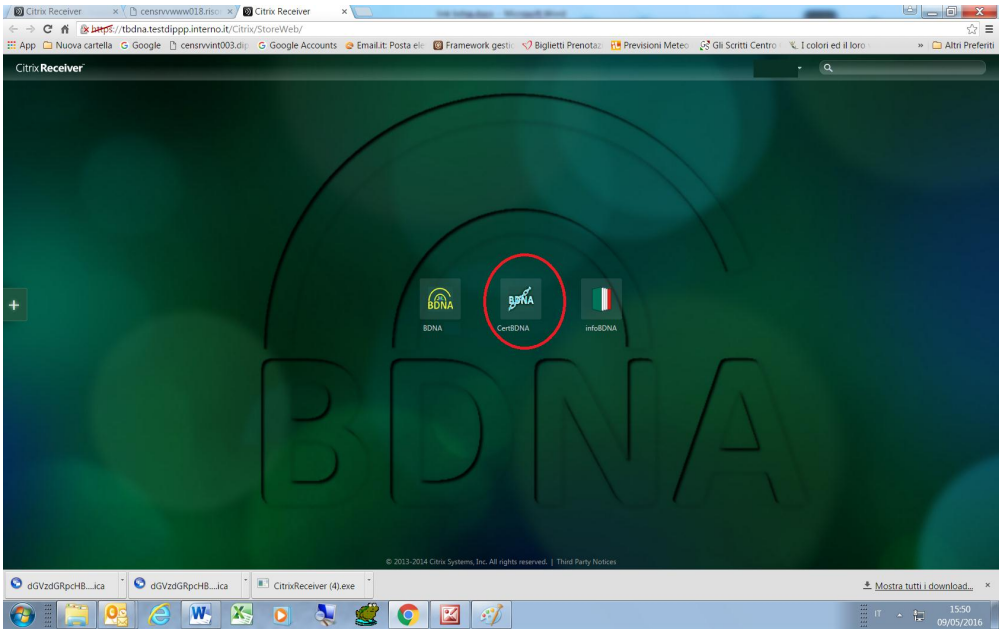
Verificare "la risposta" dell'ultima maschera del cambio password perché la stessa potrebbe contenere la segnalazione di un errore e conseguentemente la NON registrazione della nuova password come nell'esempio seguente

6) Cambio PIN (PASSWORD DEL CERTIFICATO)

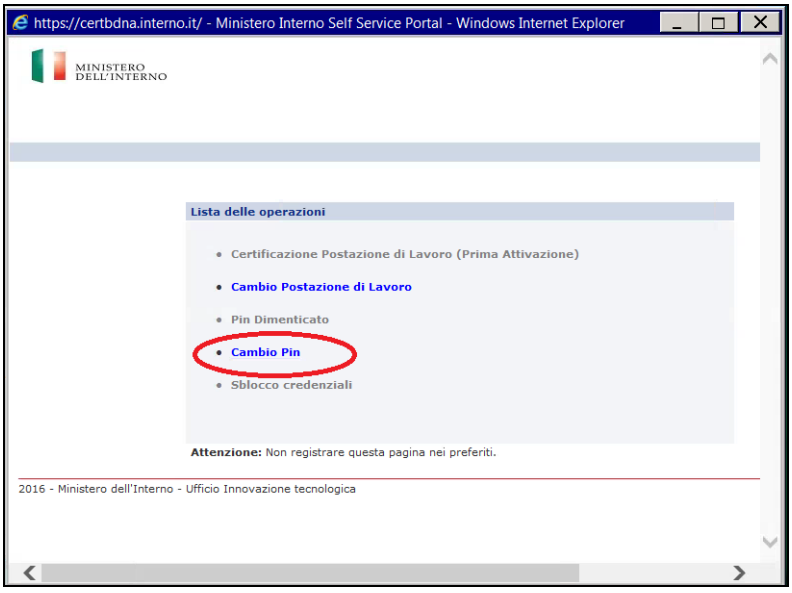
Il PIN (PASSWORD DEL CERTIFICATO) (in alcune maschere è chiamato anche Online password) è una password distinta dalla password dell'applicativo ed è strettamente legata alla smart card virtuale anche detta "*Certificato digitale".*

Mentre il PIN (PASSWORD DEL CERTIFICATO) non ha una scadenza e può essere cambiato a discrezione dell'utente, il Certificato, invece, ha una scadenza annuale. Alla scadenza del Certificato dovrà, necessariamente essere impostato un nuovo PIN (PASSWORD DEL CERTIFICATO).

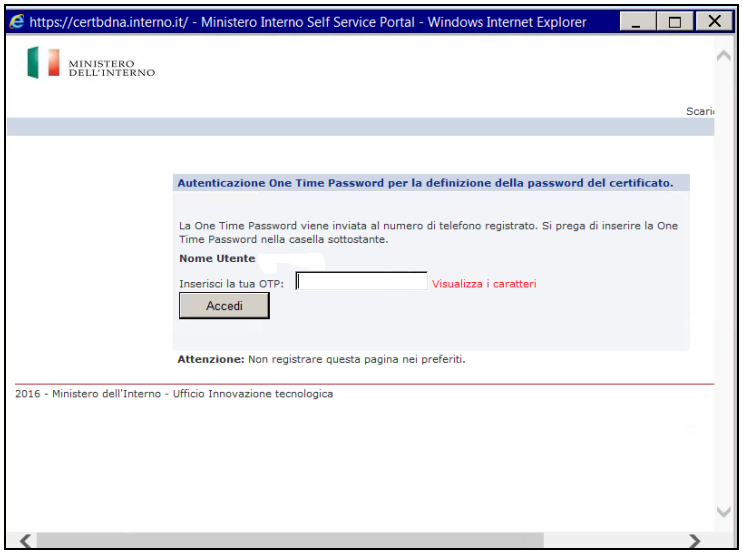
Per accedere a questa funzione è necessario accedere nel portale Citrix nel ramo **CERTBDNA**



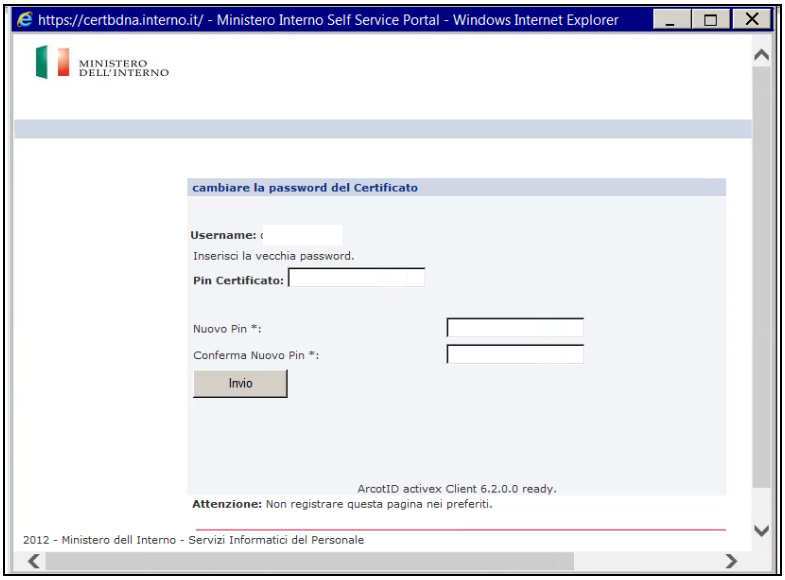
Selezionare la funzione "*Cambio Pin*"



Il sistema invia un sms sul cellulare dell'utente con una OTP che deve essere digitata nella casella "*Inserisci la tua OTP*"



Verrà proposta la seguente maschera nella quale deve essere inserito l'attuale PIN (PASSWORD DEL CERTIFICATO), il nuovo PIN che dovrà anche essere confermato.



Il PIN (PASSWORD DEL CERTIFICATO) deve avere le seguenti caratteristiche:

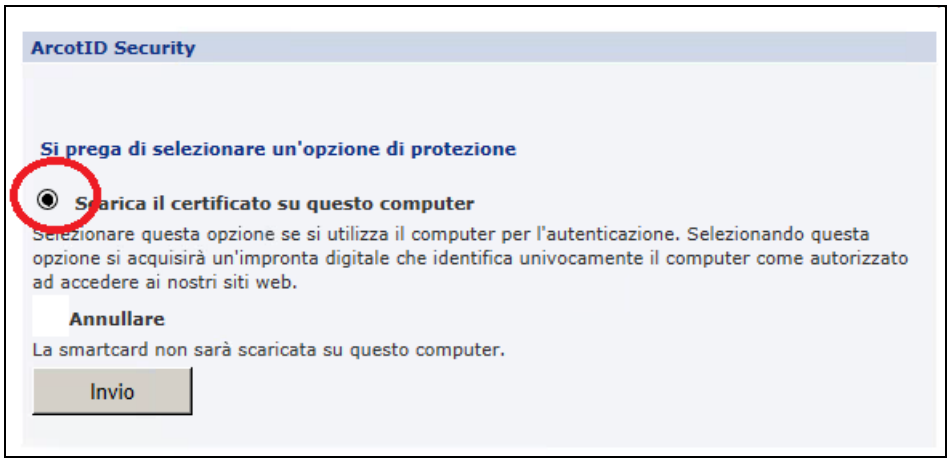
. deve essere diversa dalle ultime 2 password utilizzate
. non deve contenere il cognome o il nome o parte di essi
. deve contenere da un minimo di 10 a un massimo di 14 caratteri
  E' necessario rispettare il limite massimo
. deve contenere almeno 1 lettera maiuscola e almeno 6 caratteri alfabetici tra maiuscole e minuscole
. deve contenere almeno 1 numero
. deve contenere almeno 1 carattere speciale **esclusi * £ $ € & !**

i caratteri speciali consigliati perché verificati sono

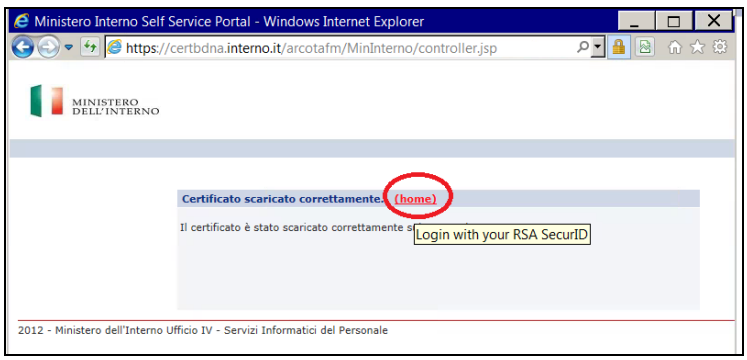
. (punto)
@ (at)

Comporre quindi con le regole suddette il PIN (PASSWORD DEL CERTIFICATO), **annotarlo e conservarlo con cura**.

Dopo aver inserito le informazioni il sistema chiederà la conferma per lo scarico del certificato.
Selezionare la voce indicata nella maschera che segue.



Il sistema comunica che il certificato è stato scaricato correttamente presentando la maschera che segue.



Selezionando la voce evidenziata in rosso **(home),** come avverte il messaggio, si potrà procedere con il login alla BDNA con il proprio certificato di sicurezza.

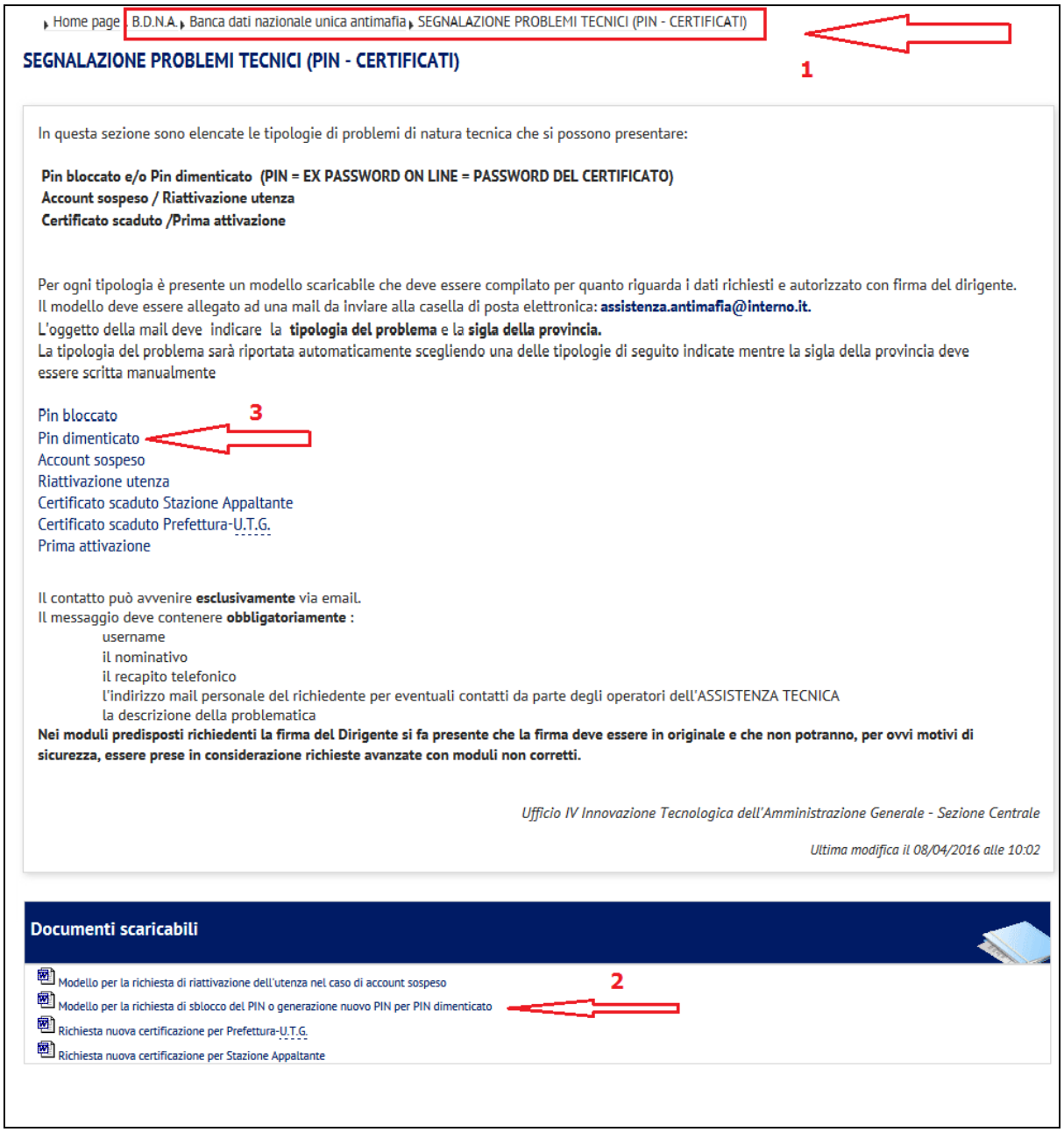
7) PIN (PASSWORD DEL CERTIFICATO) DIMENTICATO

Nel caso in cui non si ricordi il PIN (PASSWORD DEL CERTIFICATO) impostati durante la certificazione dell'utente si deve procedere nel seguente modo:

1. Collegarsi sul portale della Prefettura nella sezione

   B.D.N.A. ▸ Banca dati nazionale unica antimafia ▸ SEGNALAZIONE PROBLEMI TECNICI (PIN - CERTIFICATI)

   Verrà mostrata la pagina che segue



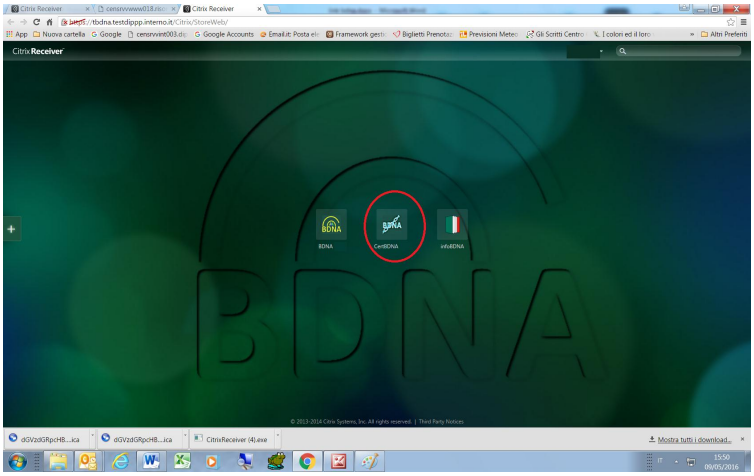
2. Scaricare il modulo "*Modello per la richiesta di sblocco del PIN o generazione nuovo PIN per PIN dimenticato*"

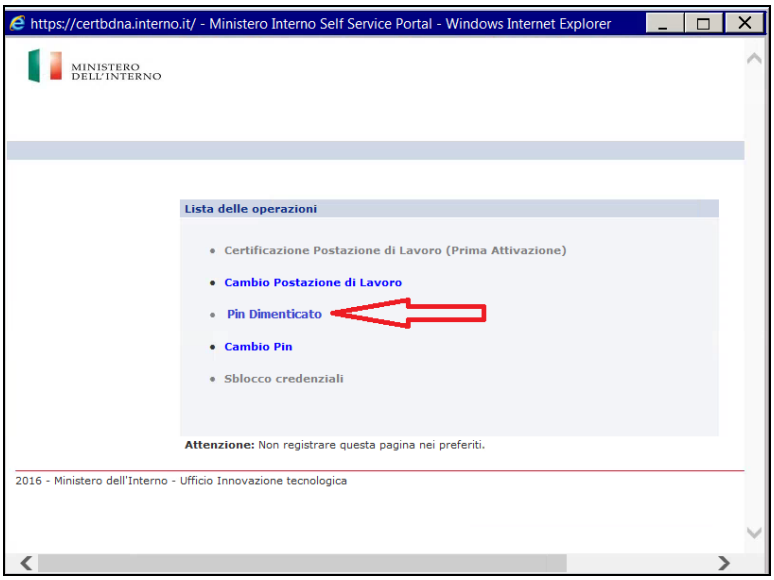
3. Selezionare la voce "*Pin dimenticato*" per ottenere una mail predisposta oppure inviare una mail al seguente indirizzo assistenza.antimafia@interno.it specificando nell'oggetto la dicitura "*Pin dimenticato - SIGLA PROVINCIA*" , indicando nel corpo della mail i seguenti dati:

   USERNAME
   NOMINATIVO
   RECAPITO TELEFONICO
   INDIRIZZO MAIL PERSONALE

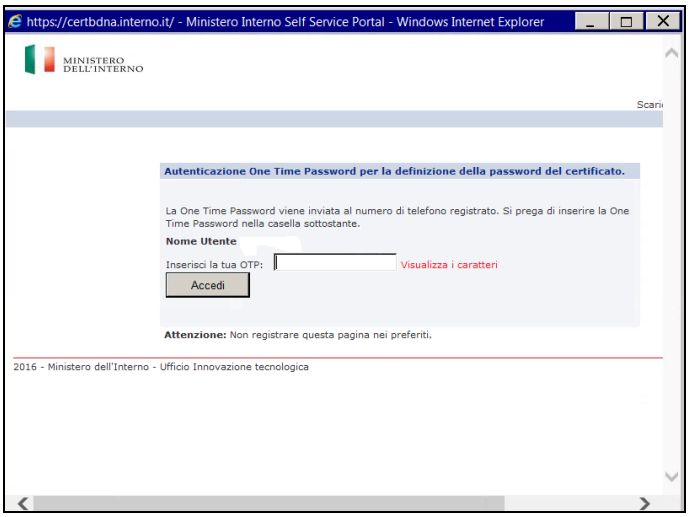
   e allegando il modulo compilato e firmato dal dirigente.

   L'Assistenza tecnica provvederà ad attivare la voce del menù "*Pin dimenticato*" al quale si può accedere collegandosi al portale Citrix nel ramo **CERTBDNA**



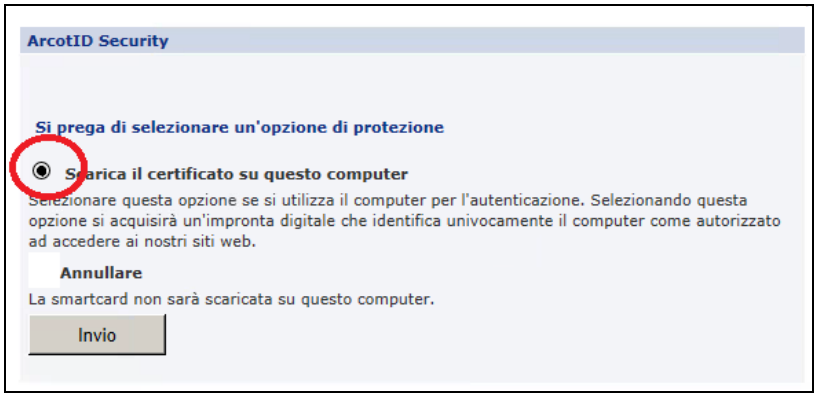


   Selezionando questa funzione il sistema invia un sms sul cellulare dell'utente con una OTP che deve essere digitata nella casella "*Inserisci la tua OTP*"

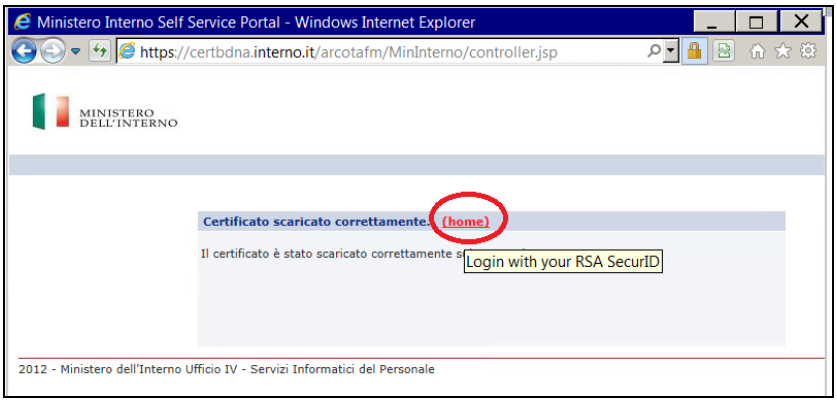


Propone quindi la maschera nella quale si potrà inserire un nuovo PIN e poi confermarlo.

Dopo aver inserito le informazioni il sistema chiederà la conferma per lo scarico del certificato.
Selezionare la voce indicata nella maschera che segue.



Il sistema comunica che il certificato è stato scaricato correttamente presentando la maschera che segue.



Selezionando la voce evidenziata in rosso **(home),** come avverte il messaggio, si potrà procedere con il login alla BDNA con il proprio certificato di sicurezza.

8) PIN (PASSWORD DEL CERTIFICATO) BLOCCATO

Il PIN (PASSWORD DEL CERTIFICATO) risulterà bloccato a seguito delle seguenti operazioni:

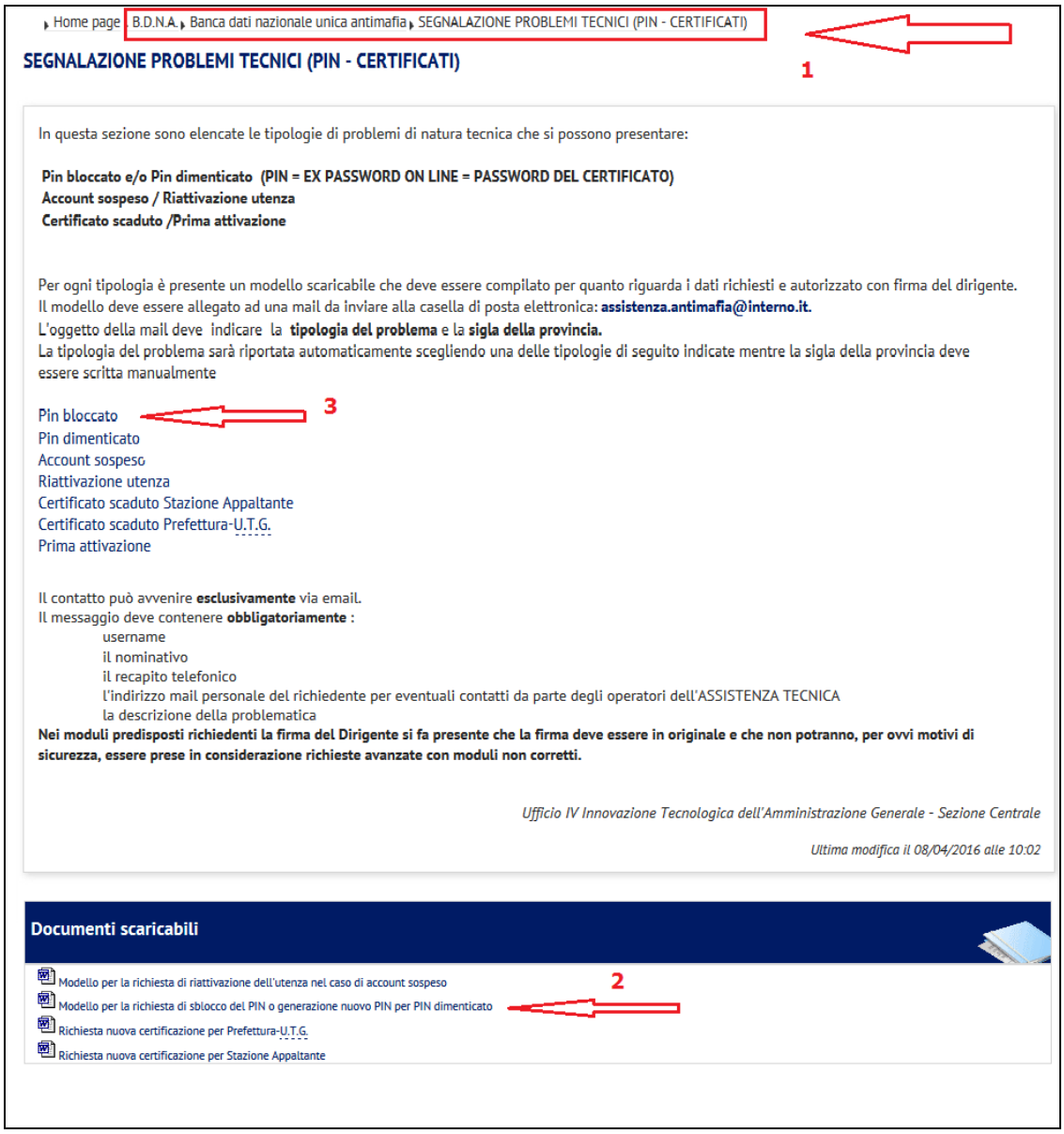
. per 3 volte è stata digitata erroneamente la OTP ricevuta sul cellulare
. per 3 volte è stato digitato sul tastierino numerico un PIN errato

Quando si riceve la segnalazione di PIN BLOCCATO si deve procedere nel seguente modo:

1. Collegarsi sul portale della Prefettura nella sezione

B.D.N.A. ▸ Banca dati nazionale unica antimafia ▸ SEGNALAZIONE PROBLEMI TECNICI (PIN - CERTIFICATI)

Verrà mostrata la pagina che segue



2. Scaricare il modulo "*Modello per la richiesta di sblocco del PIN o generazione nuovo PIN per PIN dimenticato*"

3. Selezionare la voce "*Pin bloccato*" per ottenere una mail predisposta oppure inviare una mail al seguente indirizzo assistenza.antimafia@interno.it specificando nell'oggetto la dicitura "*Pin bloccato - SIGLA PROVINCIA*" , indicando nel corpo della mail i seguenti dati:

   USERNAME
   NOMINATIVO
   RECAPITO TELEFONICO
   INDIRIZZO MAIL PERSONALE

   e allegando il modulo compilato e firmato dal dirigente.

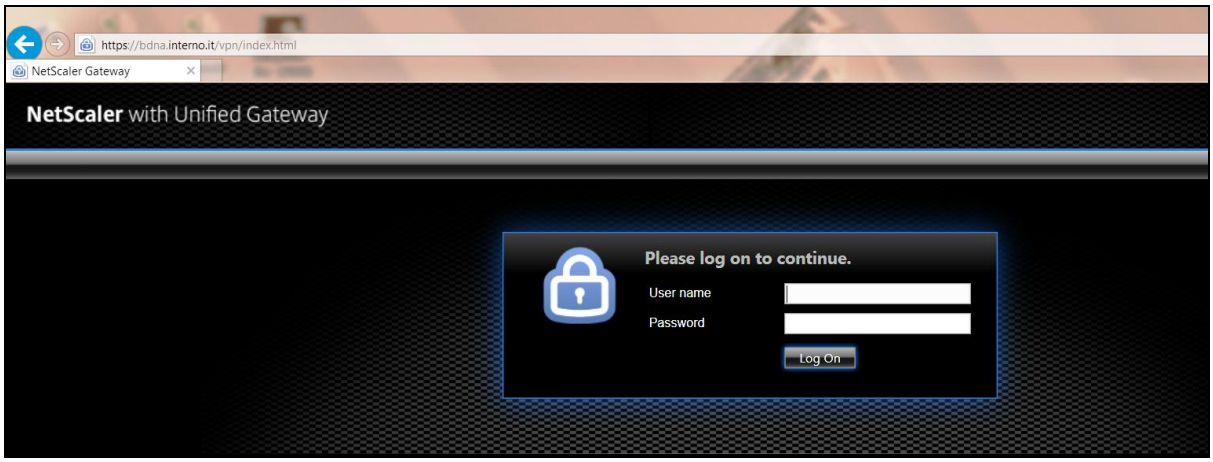
   L'Assistenza tecnica provvederà a sbloccare il PIN (PASSWORD DEL CERTIFICATO) che sarà di nuovo disponibile.

9) Accesso alla B.D.N.A.

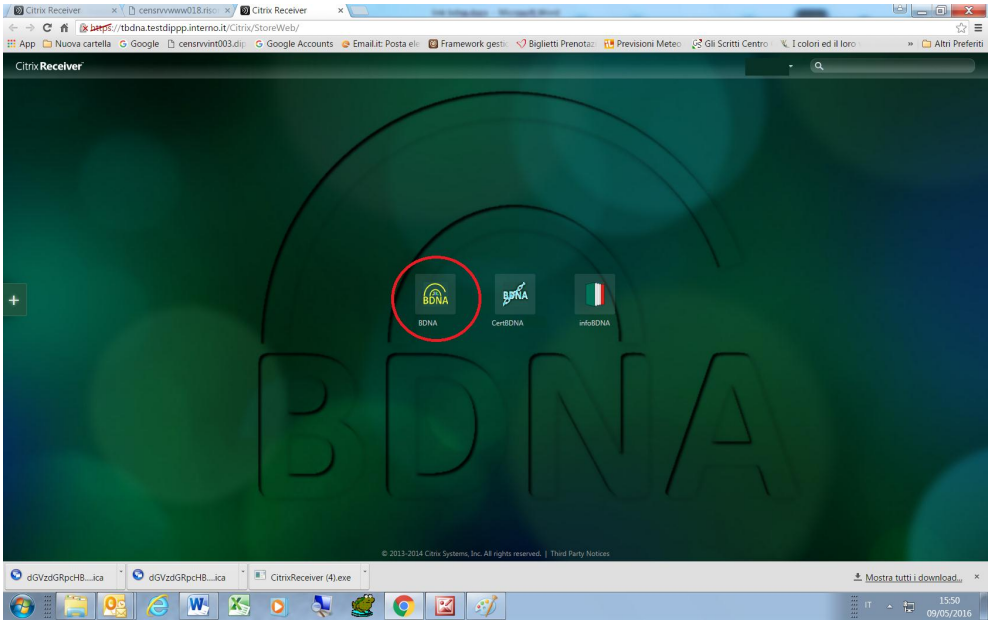
Di seguito si riportano le operazioni per accedere all'applicativo **B.D.N.A.**

1. Aprire il browser utilizzato sulla propria postazione e connettersi all'indirizzo
   https://bdna.interno.it (se STAZIONE APPALTANTE)
   https://bdna.dippp.interno.it (se PREFETTURA)

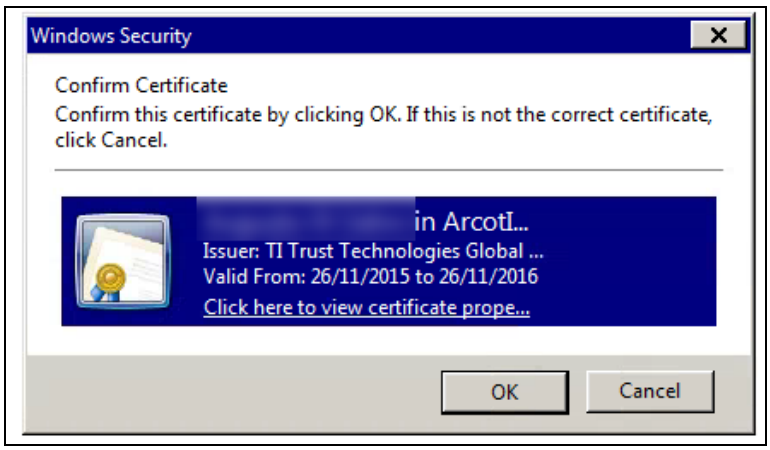
2. Eseguire il login digitando nelle rispettive caselle USERNAME e la PASSWORD DELL'APPLICATIVO



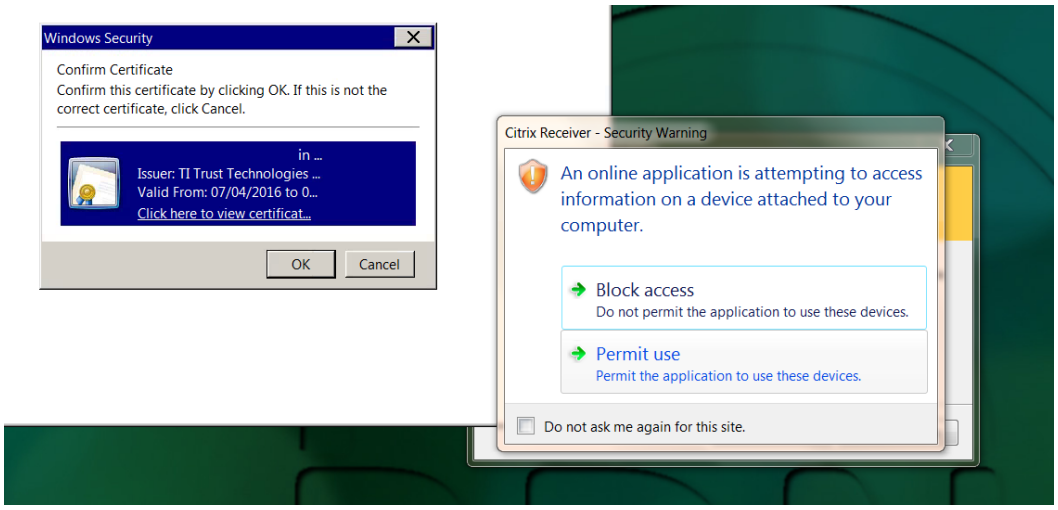
3. Una volta effettuato il Login cliccare sull'icona BDNA.



4. All'apertura di una nuova finestra del browser verificare che il certificato digitale riporti il proprio nome e cliccare su OK

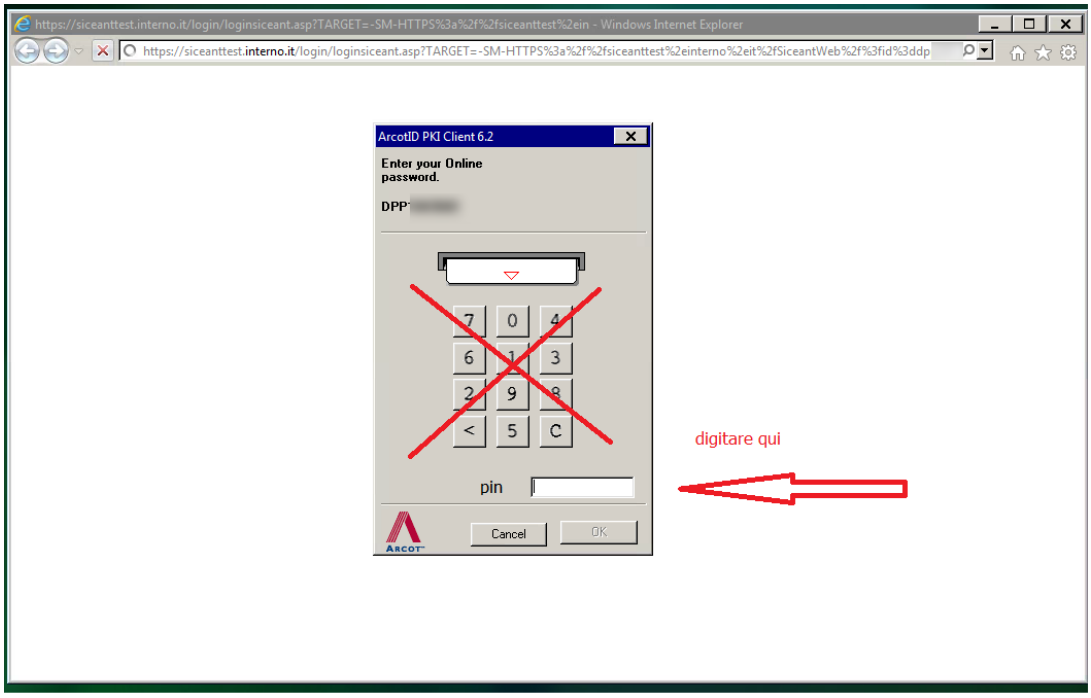


Potrebbe verificarsi che insieme alla visualizzazione dei dati del certificato venga anche richiesta una autorizzazione, come mostrato nella prossima maschera

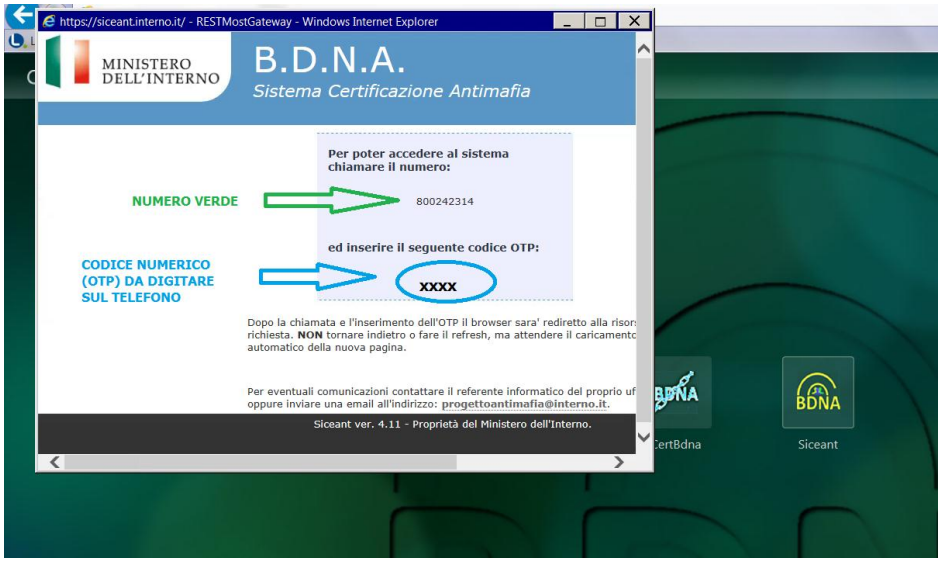


In questo caso cliccare su "*Permit*" o "*Consenti*" per continuare.

5. Accettato il certificato viene richiesto di digitare il PIN (PASSWORD DEL CERTIFICATO).
   Attenzione **NON UTILIZZARE I PULSANTI DELLA TASTIERINA NUMERICA, MA SCRIVERE NELLA CASELLA VUOTA I CARATTERI DELLA PASSWORD DEL CERTIFICATO (PIN)**

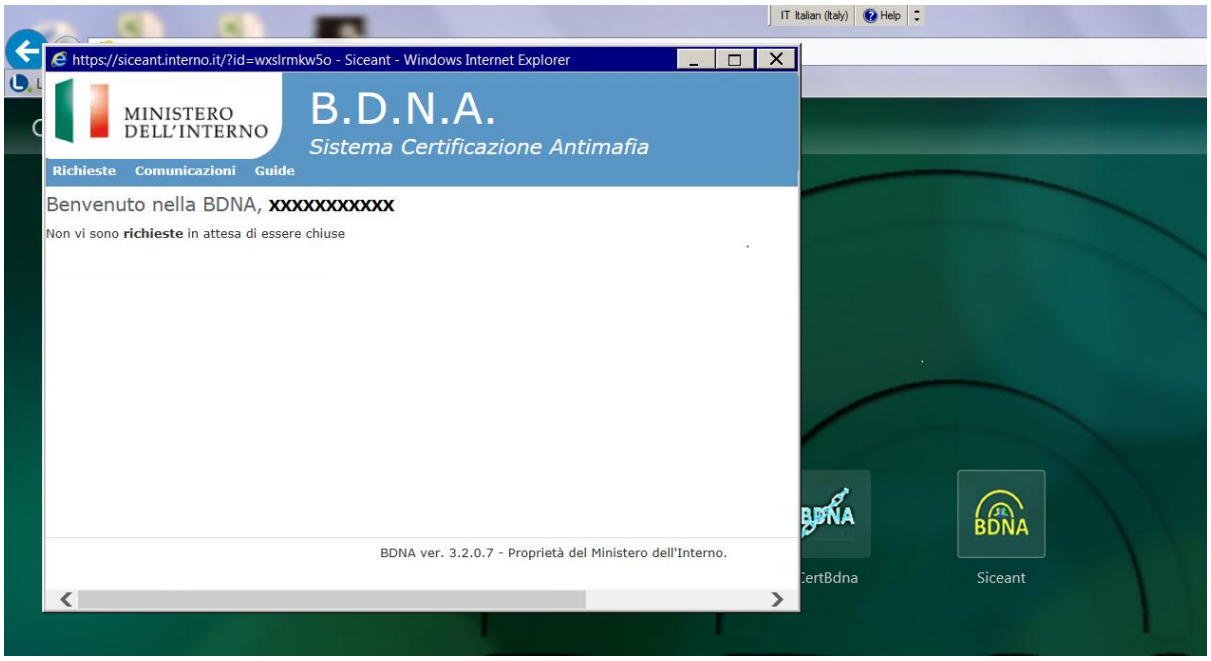


6. Il sistema una volta verificata la correttezza del PIN (PASSWORD DEL CERTIFICATO) e accettato il certificato digitale presenterà a video un codice numerico di 4 cifre (OTP) ed un numero verde gratuito da contattare.



7. Con il cellulare accreditato contattare il "***NUMERO VERDE***" e, alla risposta, digitare il "*codice numerico (OTP)*" indicato a video.

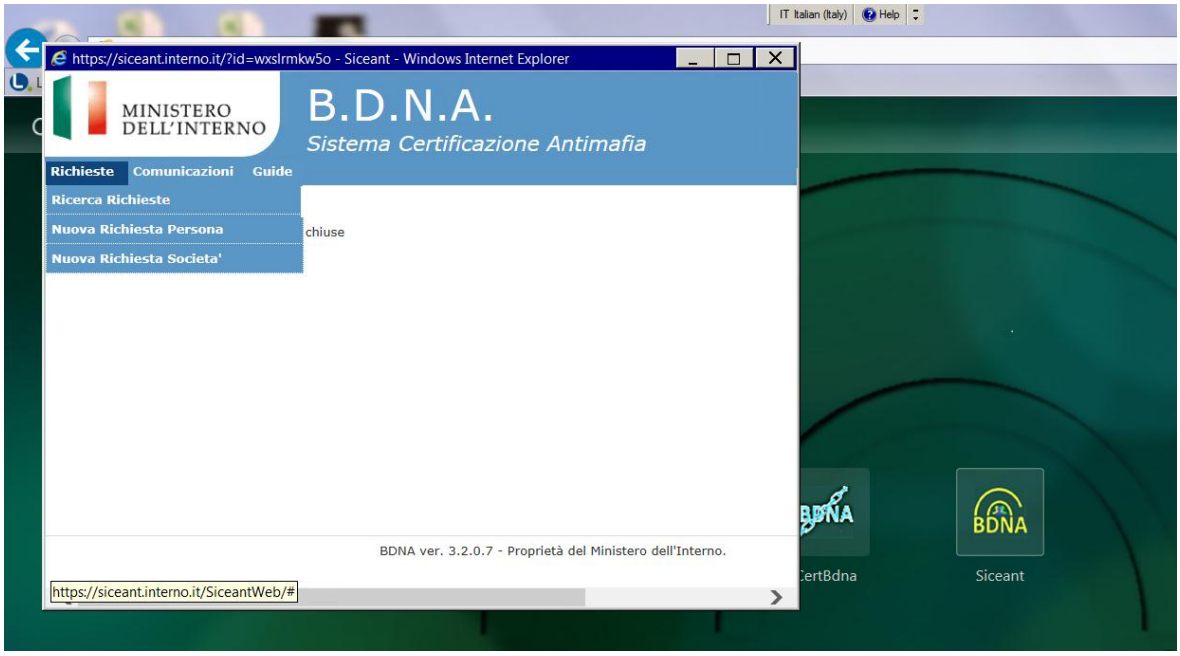
8. Se l'operazione viene eseguita con successo, l'utente di S.A. accede alla schermata applicativa principale della **B.D.N.A.** e potrà navigare tra i menù proposti.
   Le funzioni dell'applicativo sono descritte nel manuale
   SICEANT_2.0_-_manuale_utente_stazione_appaltante
   reperibile nel menù Guide.

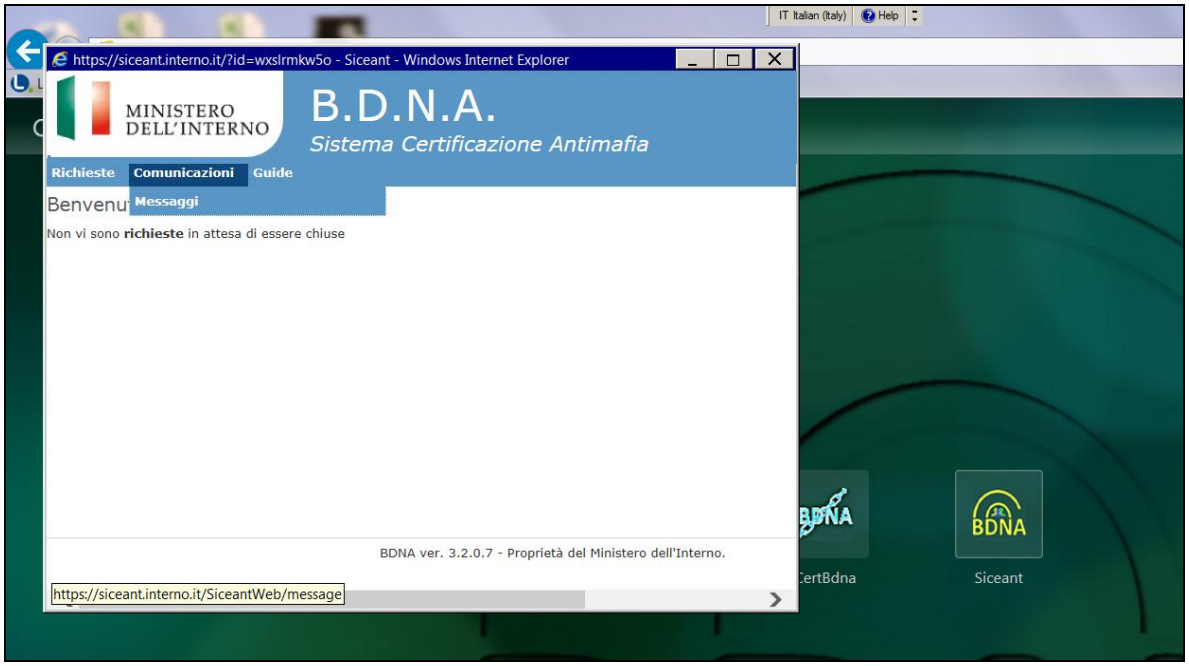


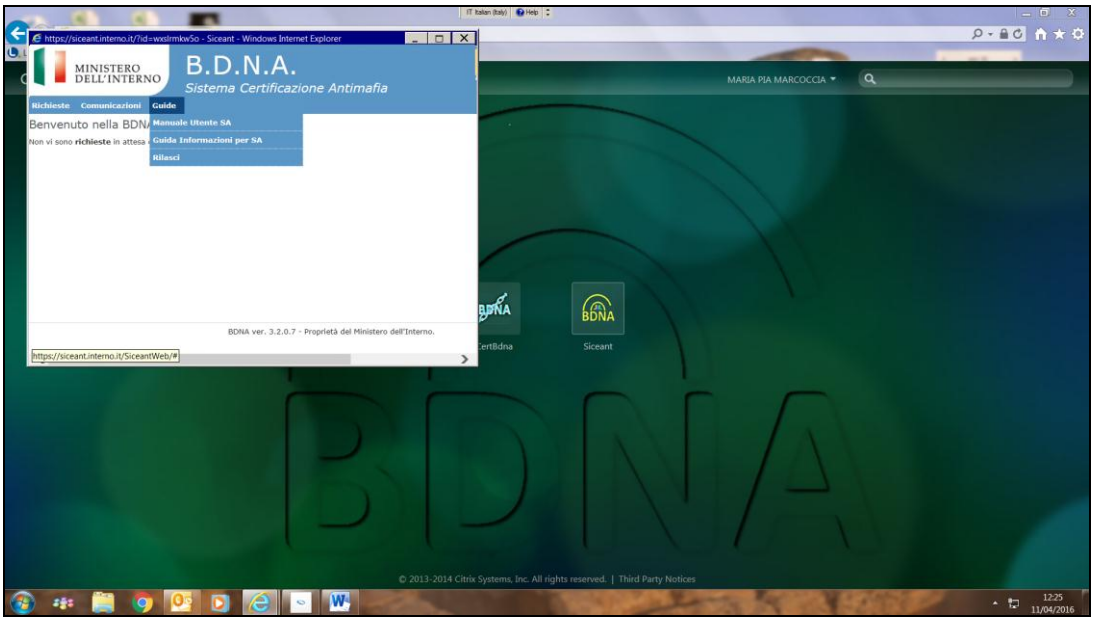
Nel caso di utente di Prefettura, se non gli è stato assegnato il profilo di "Utente Prefettura", vedrà una schermata senza menù:

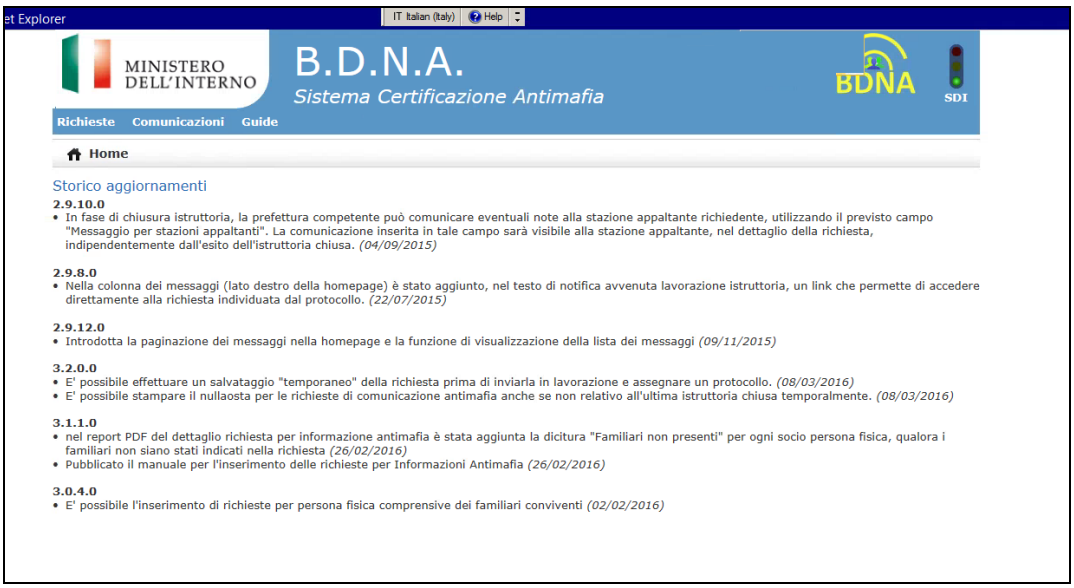
E' necessario che gli venga assegnato il profilo "utente Prefettura" e poi potrà eseguire di nuovo l'accesso.

Le maschere che seguono mostrano le estensioni del menù





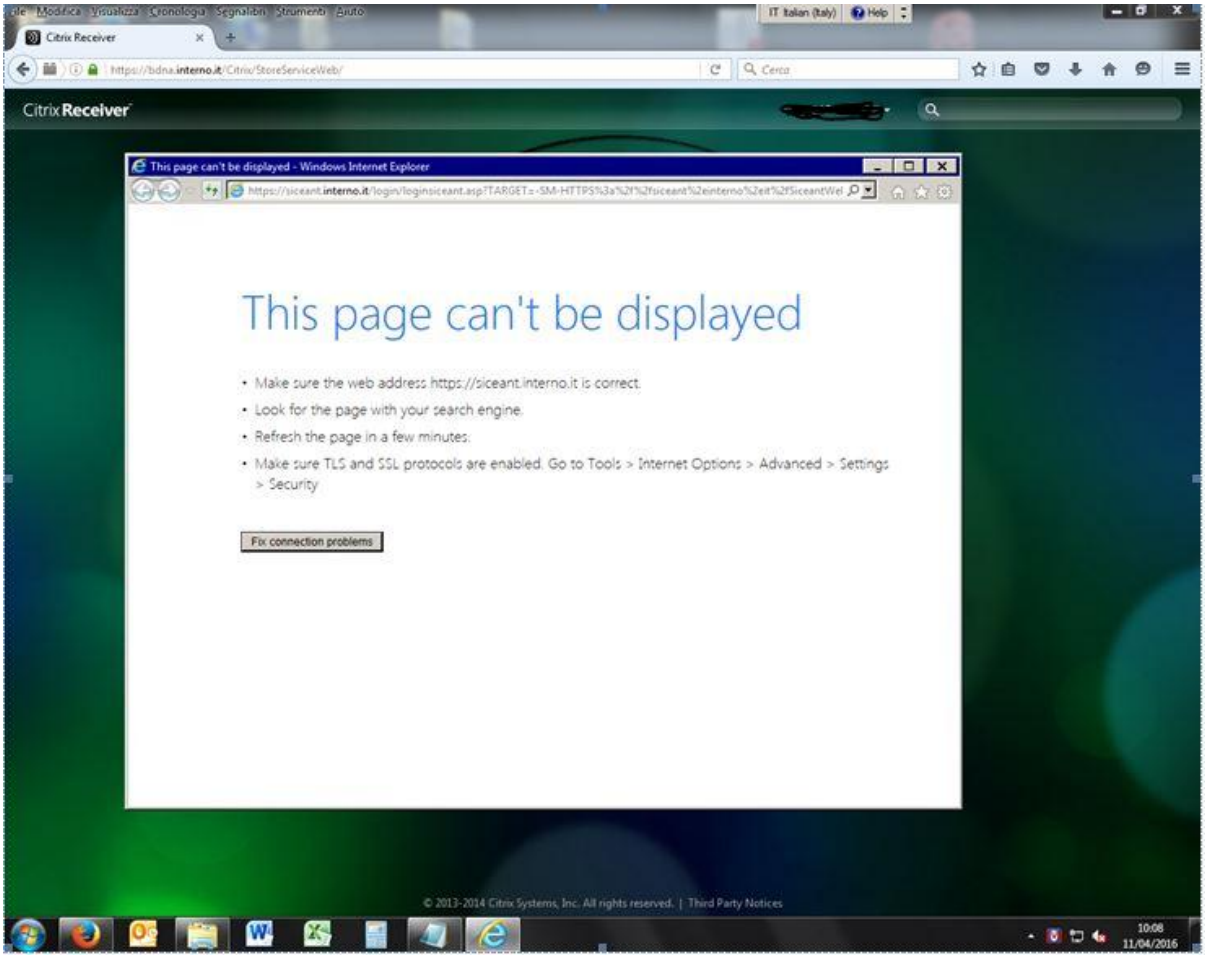

B.D.N.A.
Sistema Certificazione Antimafia
MINISTERO DELL'INTERNO
Richieste
Comunicazioni
Guide
Manuale Utente SA
Guida Informazioni per SA
Rilasci
BDNA ver. 3.2.0.7 - Proprietà del Ministero dell'Interno.
MARIA PIA MARCOCCIA
Siceant
© 2013-2014 Citrix Systems, Inc. All rights reserved. | Third Party Notices


IT Italian (Italy)
Help
MINISTERO DELL'INTERNO
B.D.N.A.
Sistema Certificazione Antimafia
BDNA
SDI
Richieste
Comunicazioni
Guide
Home
Storico aggiornamenti
2.9.10.0
In fase di chiusura istruttoria, la prefettura competente può comunicare eventuali note alla stazione appaltante richiedente, utilizzando il previsto campo "Messaggio per stazioni appaltanti". La comunicazione inserita in tale campo sarà visibile alla stazione appaltante, nel dettaglio della richiesta, indipendentemente dall'esito dell'istruttoria chiusa. (04/09/2015)
2.9.8.0
Nella colonna dei messaggi (lato destro della homepage) è stato aggiunto, nel testo di notifica avvenuta lavorazione istruttoria, un link che permette di accedere direttamente alla richiesta individuata dal protocollo. (22/07/2015)
2.9.12.0
Introdotta la paginazione dei messaggi nella homepage e la funzione di visualizzazione della lista dei messaggi (09/11/2015)
3.2.0.0
E' possibile effettuare un salvataggio "temporaneo" della richiesta prima di inviarla in lavorazione e assegnare un protocollo. (08/03/2016)
E' possibile stampare il nullaosta per le richieste di comunicazione antimafia anche se non relativo all'ultima istruttoria chiusa temporalmente. (08/03/2016)
3.1.1.0
nel report PDF del dettaglio richiesta per informazione antimafia è stata aggiunta la dicitura "Familiari non presenti" per ogni socio persona fisica, qualora i familiari non siano stati indicati nella richiesta (26/02/2016)
Pubblicato il manuale per l'inserimento delle richieste per Informazioni Antimafia (26/02/2016)
3.0.4.0
E' possibile l'inserimento di richieste per persona fisica comprensive dei familiari conviventi (02/02/2016)

Possibili messaggi di errore.

ERRORE 1

La seguente segnalazione di errore appare quando è impostata una Password dell'applicativo o una Password del certificato (PIN) con un numero di caratteri superiori a 14.

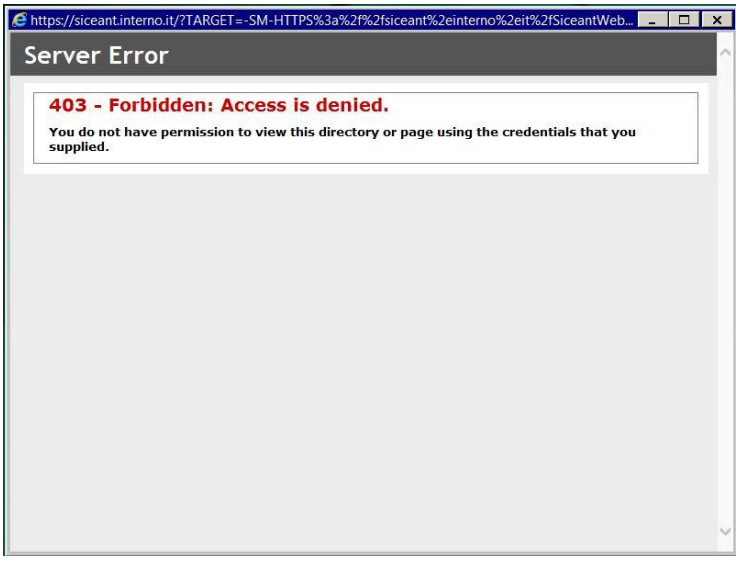


ERRORE 2

Gli utenti del precedente applicativo SICEANT che utilizzano un certificato emesso prima dell' 1/4/2015 potrebbero ricevere un messaggio di errore come quello riportato qui accanto. In questo caso occorre procedere come per una nuova attivazione.

ERRORE 3

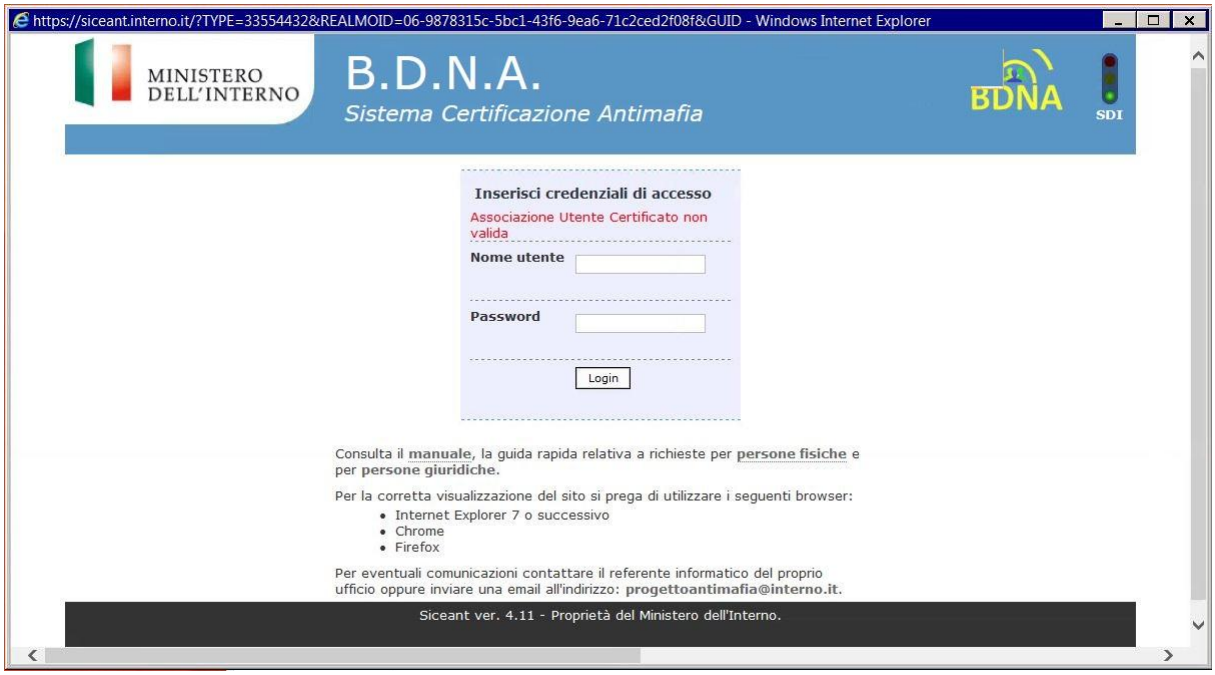
Quando il certificato non è installato compare il messaggio qui accanto. In questo caso occorre procedere alla certificazione dell'utente.



ERRORE 4

Durante l'attività è possibile che si venga disconnessi.

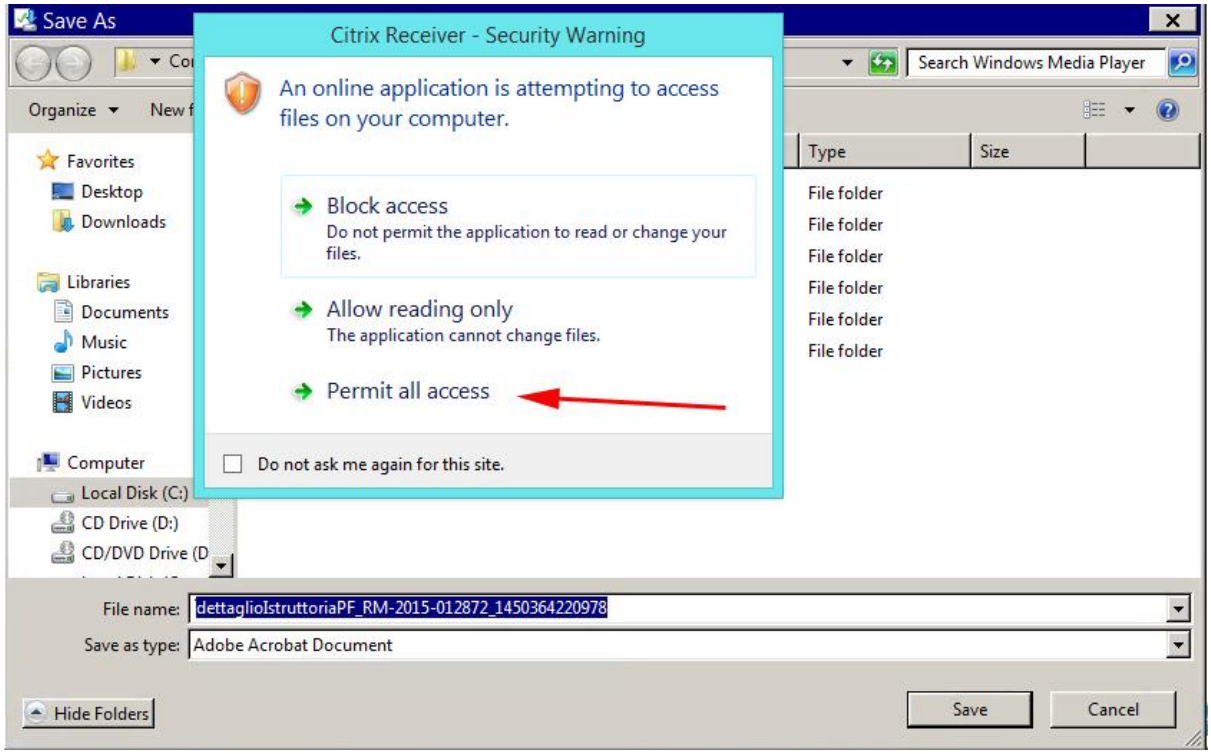
In questo caso non inserire subito le credenziali per riconnettersi, altrimenti si riceverà il messaggio di errore "Associazione Utente Certificato non valido" come nella maschera qui accanto. Prima di riconnettersi è necessario chiudere tutte le finestre del browser e quindi ricominciare nuovamente tutta la procedura per la connessione (apertura del browser, inserimento credenziali, PIN, numero verde…..).



10) Funzionalità di stampa e salvataggio del PDF

Se si intende salvare il PDF o stamparlo in un secondo momento è possibile selezionare "Save as" quando richiesto (come nell'esempio sottostante)

In caso di "security warning" selezionare "permit all access"



infine scegliere sempre il disco "Local Disk (C: on *nomepc*)"