



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



Istruzioni operative per l'accesso alla macchina virtuale

versione 3.1

ottobre 2016

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 la precedente versione, installare un client VPN sul proprio computer.

La postazione utente viene ora resa virtuale e il relativo certificato digitale, necessario per l'accesso, sarà posto nella directory dell'utente.

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

Nel "Glossario" che segue sono elencati e **ri-definiti** dei termini che nel corso dell'evoluzione dell'applicativo BDNA hanno avuto versioni diverse.

Lo scopo della **ri-definizione** è quello di assumere una terminologia comune, chiara e univoca.



GLOSSARIO :

UTENZA O USERNAME O ACCOUNT

I termini sono sinonimi che indicano il “*nome*” con il quale l'utente viene riconosciuto dall'applicativo.

PASSWORD APPLICATIVA

Con il termine **PASSWORD APPLICATIVA**, che sostituirà il termine generico **PASSWORD**, si intende la “*sequenza di caratteri alfanumerici*” che si imposta al primo accesso in sostituzione di quella “*scaduta*” rilasciata dalla Prefettura.

Ha una durata di 90 giorni e può essere rinnovata come indicato al punto 5) di questo Manuale.

La gestione della **PASSWORD APPLICATIVA** è a cura dell'utente che può, all'interno dell'applicativo per la certificazione della postazione di lavoro (CertBdna) modificarla o reimpostarla in caso di smarrimento

CERTIFICATO DIGITALE

Il **CERTIFICATO DIGITALE** è un documento elettronico, un file, con una **validità temporale limitata** ed è usato per garantire l'identità di un soggetto.

SMART CARD

La **SMART CARD** è un “contenitore” che protegge il **CERTIFICATO DIGITALE**. La **SMART CARD** è dotata di una “**PASSWORD SMART CARD**”, che consente di accedere al **CERTIFICATO DIGITALE**.

PASSWORD SMART CARD

Con il termine **PASSWORD SMART CARD**, che sostituirà nell'esposizione i termini “*PIN*”, “*ON LINE PASSWORD*” e “*PASSWORD DEL CERTIFICATO*” che sono stati usati in precedenza anche nelle schermate della procedura, si intende la “*sequenza di caratteri alfanumerici*” **creata dall'utente** per la protezione della *smart card* che contiene il certificato digitale.



L'immagine che segue sintetizza i concetti di
SMART CARD - PASSWORD SMART CARD - CERTIFICATO DIGITALE



il **CERTIFICATO DIGITALE** ha una "SCADENZA TEMPORALE" che ne determina la validità (1 anno).

Invece, la **SMART CARD**, che protegge il CERTIFICATO DIGITALE, ha una "**CHIAVE DI ACCESSO**" che chiameremo **PASSWORD SMART CARD**.

La **PASSWORD SMART CARD** viene ideata dall'utente al momento dello scarico del certificato.

La sua composizione deve sottostare a delle regole precise che vengono descritte nel manuale.

Può essere modificata quando l'utente lo ritiene opportuno per ragioni di sicurezza.

Se viene **dimenticata** o **perduta** l'assistenza attiverà, dietro richiesta dell'utente, la funzione di "*Password smart card dimenticata*" nel menù "*Lista delle operazioni*" permettendo all'utente di idearne una nuova.

Se viene **bloccata** per digitazione errata e/o superamento del numero dei tentativi consentiti, l'assistenza provvederà, dietro richiesta dell'utente, al suo sblocco e l'utente **potrà continuare ad utilizzarla senza la necessità di cambiarla**.



In questo manuale è possibile trovare informazioni su

1. ATTIVITÀ TECNICA NECESSARIA PER LO START UP
 - 1a Generalità sulla PASSWORD APPLICATIVA
 - 1b Abilitazione della postazione UTENTE (Citrix plug-in)
 - 1c Installazione del PLUGIN di connessione alla postazione virtuale
2. INFORMAZIONI SULLE ICONE PRESENTI SUL PORTALE DI ACCESSO
3. **CERTIFICAZIONE DELL'UTENTE**
4. CAMBIO POSTAZIONE DI LAVORO
5. CAMBIO PASSWORD APPLICATIVA
6. CAMBIO PASSWORD SMART CARD
7. PASSWORD SMART CARD DIMENTICATA
8. PASSWORD SMART CARD BLOCCATA
9. RICHIESTA RINNOVO CERTIFICATO DIGITALE
10. ACCESSO ALLA BDNA

APPENDICI

- 1) MESSAGGI DI ERRORE
- 2) FUNZIONALITÀ DI STAMPA E SALVATAGGIO DEL PDF
- 3) MODELLI



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 APPLICATIVA

La password è sempre legata allo username rilasciato 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 APPLICATIVA**".

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

La **PASSWORD APPLICATIVA** deve avere le seguenti caratteristiche:

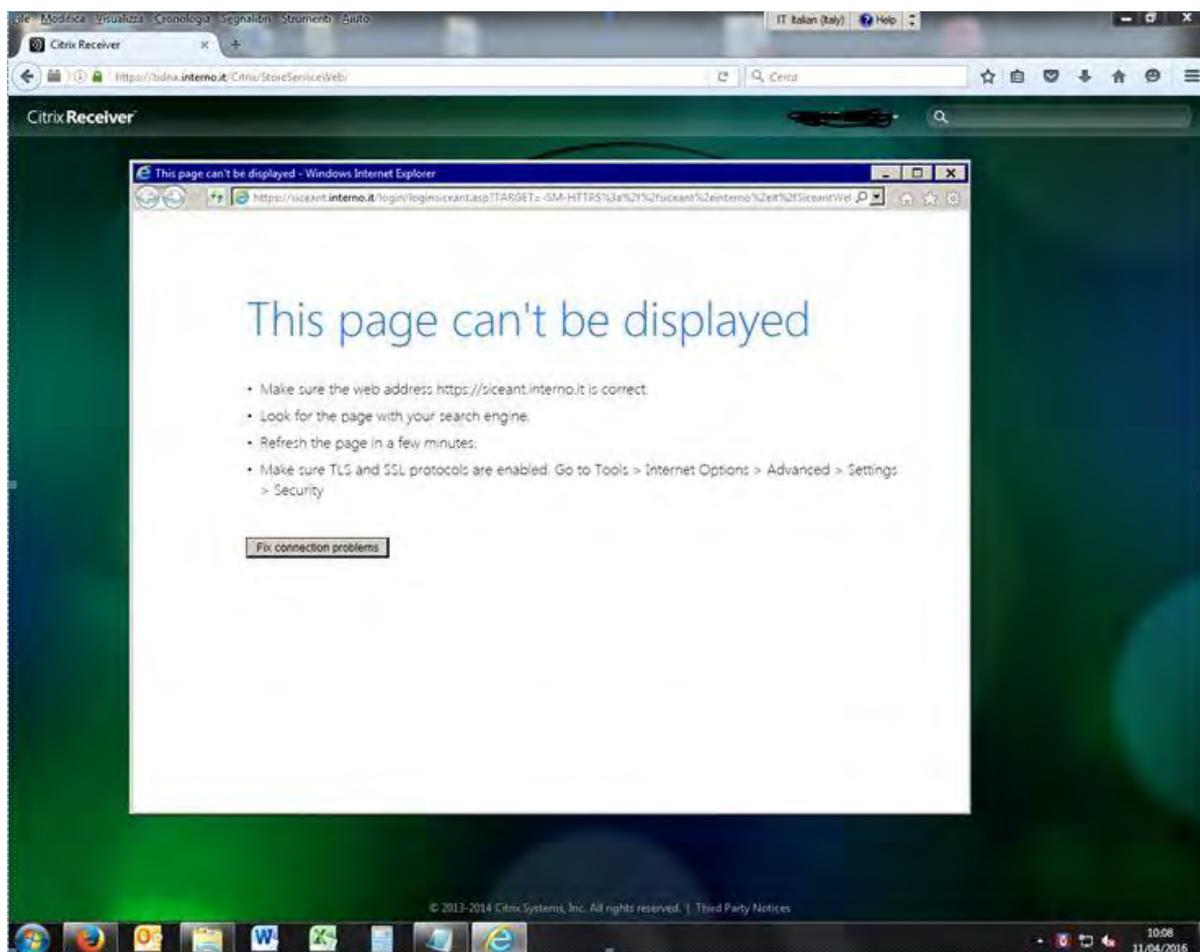
- . non deve contenere il cognome o il nome o parti di essi
- . deve contenere da un minimo di 10 a un massimo di 14 caratteri.
E' necessario rispettare il limite massimo.
- . deve contenere almeno 1 lettera MAIUSCOLA e almeno 6 lettere minuscole
- . deve contenere almeno 1 NUMERO
- . deve contenere almeno 1 carattere speciale
- . deve essere diversa dalle ultime 2 password utilizzate

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



AVVISO

Al momento della creazione della Password applicativa è necessario fare attenzione a non superare i 14 caratteri per evitare di ottenere la seguente segnalazione di errore:





Abilitazione della postazione UTENTE (Citrix plug-in).

Premesse all'installazione

Il plug-in Citrix è compatibile con i sistemi operativi Windows, 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.gov.it> (se STAZIONE APPALTANTE)

<https://bdna.dipp.interno.it> (se PREFETTURA)

La prima schermata proposta dopo il collegamento è la seguente.





Digitare nelle rispettive caselle lo USERNAME e la PASSWORD APPLICATIVA rilasciati dalla Prefettura.

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

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

Inserire una sequenza alfanumerica composta secondo i criteri esposti nelle *"generalità sulla password applicativa"*, **annotarla e conservarla con cura.**

Additional Information Required

Please type your response below.

Password Expired. Please enter a new password.

Submit

ATTENZIONE

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

Please log on to continue.

User name

Password

Incorrect credentials. Try again.

Log On



Altrimenti viene richiesta la conferma della password applicativa appena inserita. Confermarla digitandola nuovamente.

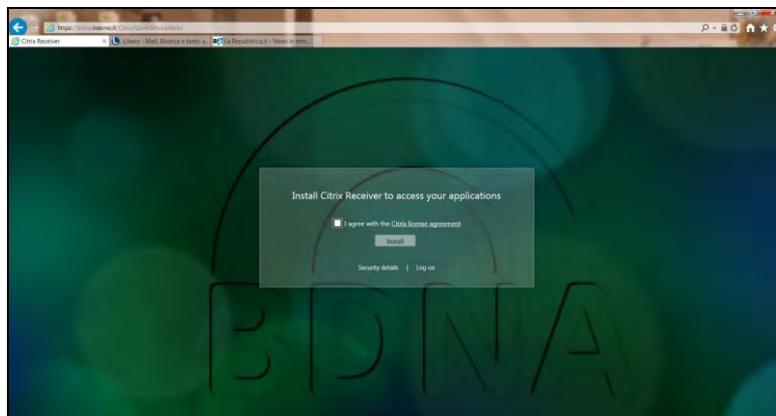
A screenshot of a blue web form titled "Additional Information Required". On the left is a white padlock icon with a keyhole. The text reads: "Additional Information Required", "Please type your response below:", "Please confirm password", followed by a white input field, and a "Submit" button at the bottom.

In caso di digitazione errata viene segnalato l'errore.

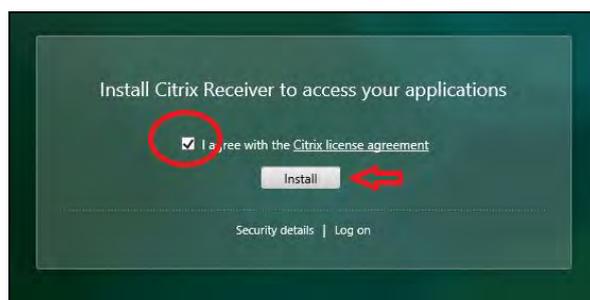
A screenshot of a blue web form titled "Please log on to continue.". On the left is a white padlock icon with a keyhole. The text reads: "Please log on to continue.", "User name" with a white input field, "Password" with a white input field, a red "X" icon followed by "Incorrect credentials. Try again.", and a "Log On" button at the bottom.

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

Dopo aver effettuato l'inserimento delle credenziali e il primo cambio password si procede con il download e l'installazione del Citrix Receiver (**solo per utenti che non hanno già installato Citrix Receiver**).

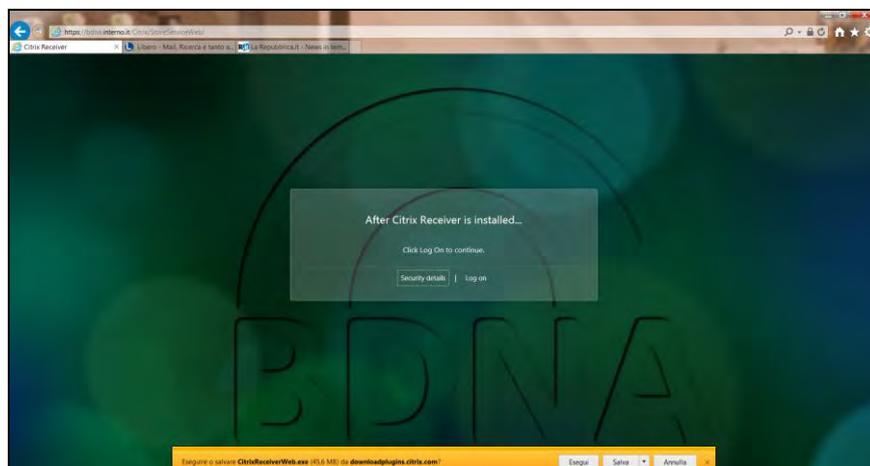


Alla richiesta di installazione del Citrix Receiver accettare le condizioni della licenza cliccando nel check e poi su INSTALL



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:



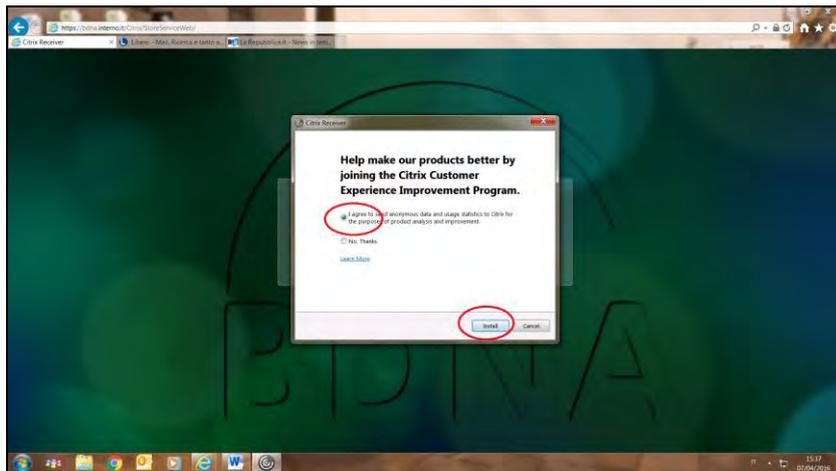
Selezionare **Start**



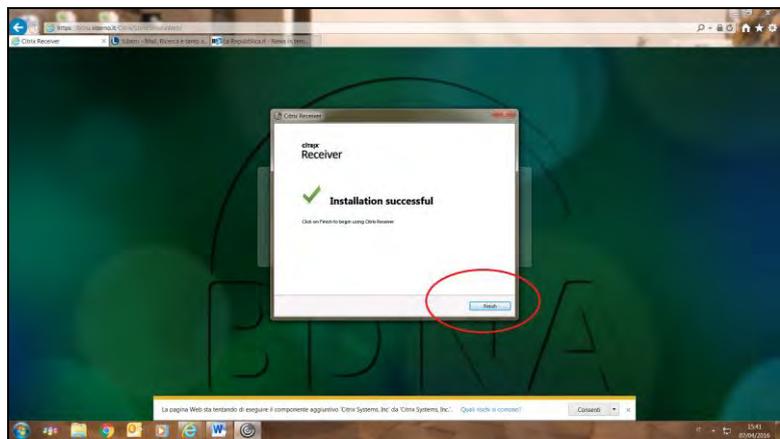
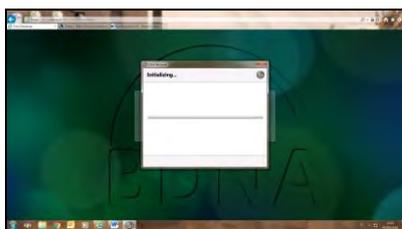
Accettare le condizioni e continuare con **Next**



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.



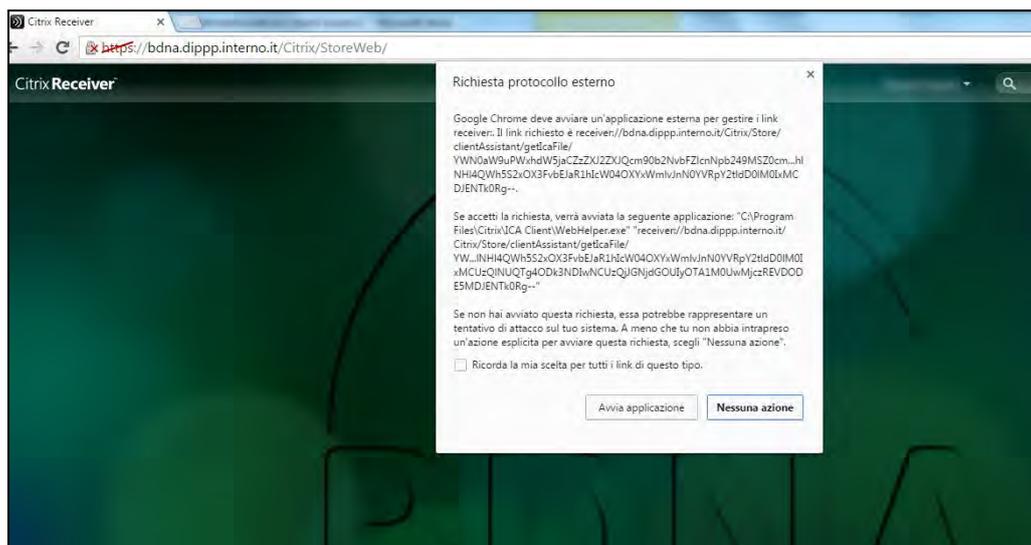
Completata quindi l'installazione del PLUGIN passare alla certificazione della postazione utente.



Controllare che tra una eventuale modifica della PASSWORD APPLICATIVA relativa all'utenza o username e la certificazione dell'utente **siano trascorsi 10 minuti** per avere la certezza del buon esito dell'operazione.

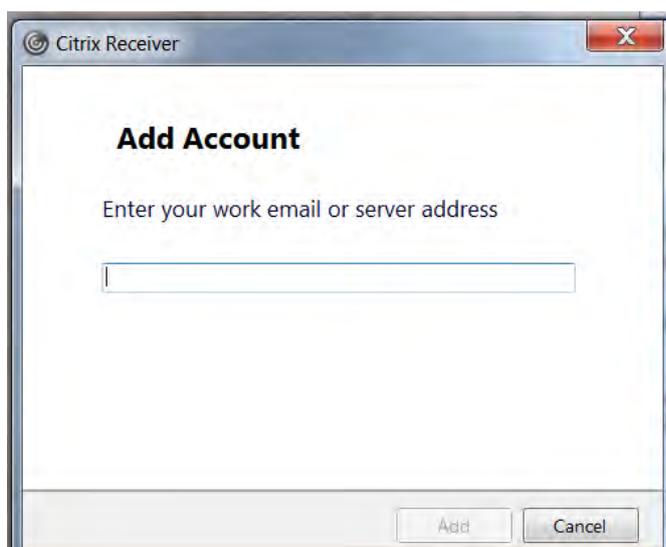
Terminata l'attesa procedere all'accesso.

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 3 pulsanti che identificano tre sezioni distinte della procedura

BDNA

che permette le seguenti funzioni:

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

CERTBDNA

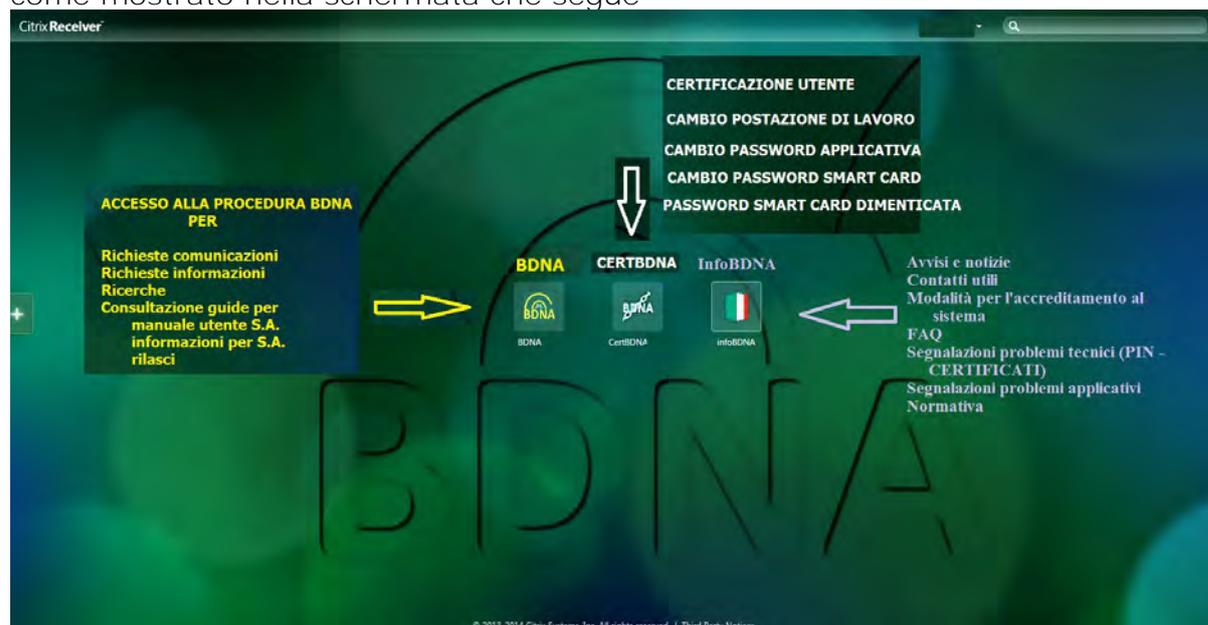
che permette le seguenti funzioni:

- certificazione utente**
- cambio postazione lavoro**
- cambio password applicativa**
- cambio password smart card**
- password smart card dimenticata**

InfoBDNA

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

come mostrato nella schermata che segue





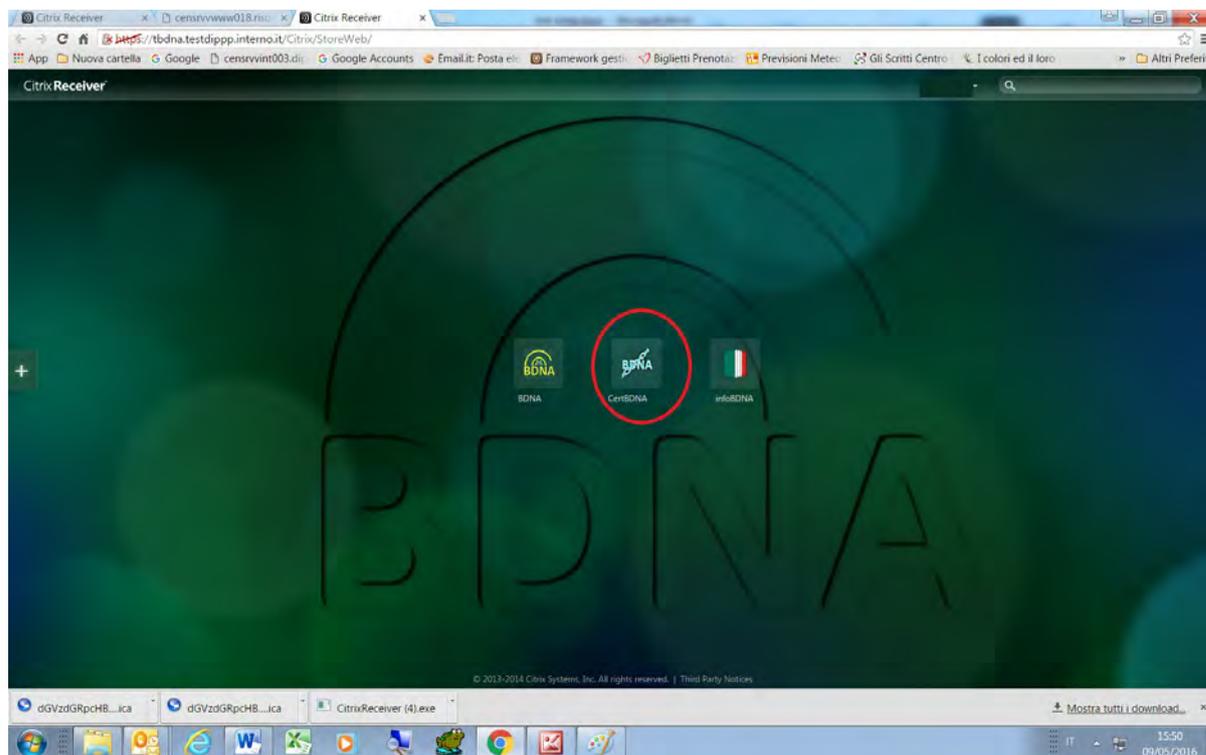
3) CERTIFICAZIONE DELL'UTENTE

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

"CertBdna" verrà utilizzato per

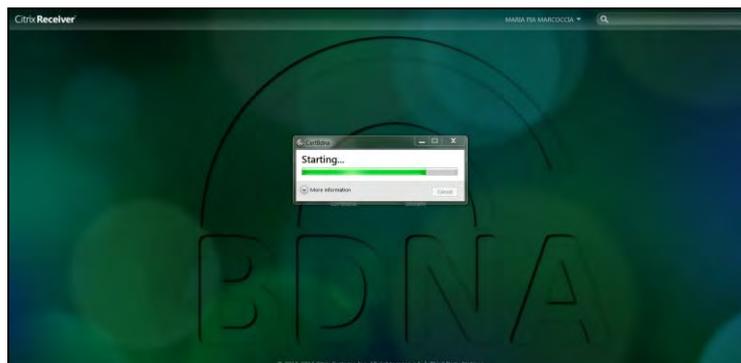
- certificare i nuovi utenti o per ri-certificare utenti il cui certificato è scaduto (ogni certificato scaricato ha la validità di 1 anno)
- eseguire la funzione "*cambio postazione di lavoro*" da parte di coloro che già in passato accedevano alla procedura Si.Ce.Ant tramite la VPN.

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 APPLICATIVA (**la nuova generata in sostituzione di quella già scaduta ricevuta dalla Prefettura**)



Verrà 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)"** (se non è attiva questa funzione selezionare **"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, **entro 2 minuti dalla ricezione**, 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, deselegionandola, i caratteri digitati saranno criptati.



La successiva maschera permetterà di impostare la PASSWORD SMART CARD

Anche se sulla maschera proposta l'indicazione recita "Nuova Password smart card" non si tratta di "aggiornamento di Password smart card esistente", ma di **prima creazione della Password smart card.**

Questo termine, "**Password smart card**", sostituisce, come già esposto nel "GLOSSARIO" le precedenti definizioni ("PIN" o "Online Password" o "Password del certificato"). Mentre il termine "PIN" può evocare un codice numerico come quello, per esempio, del bancomat, la "**Password smart card**" consiste di una **sequenza alfanumerica** che deve rispettare delle regole.

La **PASSWORD SMART CARD** deve avere le seguenti caratteristiche:

- . 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 lettere minuscole
- . deve contenere almeno 1 NUMERO
- . deve contenere almeno 1 carattere speciale **esclusi * £ \$ € & !**
- . deve essere diversa dalle ultime 2 password utilizzate



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

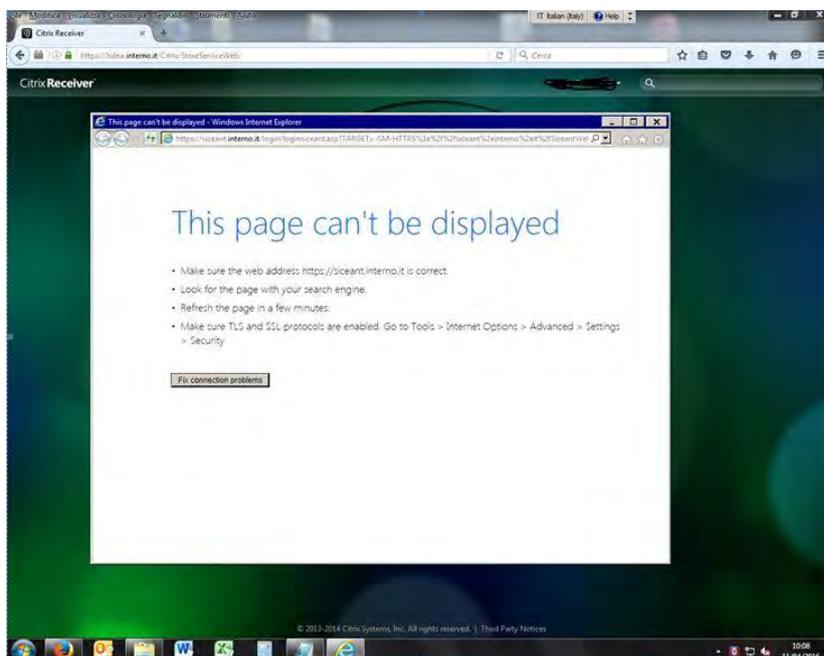
Comporre quindi con le regole suddette la PASSWORD SMART CARD, **annotarla e conservarla con cura.**

E' molto importante annotarla e conservarla con cura perché in caso di digitazioni errate della stessa verrà applicato un blocco e verrà negato l'accesso al sistema.

Per ripristinare il normale accesso sarà necessario inviare un modulo di richiesta SBLOCCO PASSWORD SMART CARD, firmato dal dirigente dell'ufficio, a assistenza.antimafia@interno.it che provvederà all'eliminazione del blocco applicato.

AVVISO

Al momento della creazione della PASSWORD SMART CARD è necessario fare attenzione a **non superare i 14 caratteri** per evitare di ottenere la seguente schermata:





Impostare la PASSWORD SMART CARD scelta **inserendo i caratteri** nella casella denominata "Nuova Password smart card" e poi riscriverlo nella casella denominata "Conferma Nuova Password smart card".

Selezionare quindi **Invio**.

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Definizione della nuova Password Smart Card per la protezione del certificato

Si prega di digitare la Nuova Password Smart Card e di confermarla

Utente:

Nuovo Password Smart Card

Conferma Nuovo Password Smart Card

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Il certificato riservato all'utente deve essere scaricato. Procedere quindi con la seguente maschera, selezionando la voce "Scarica il certificato." e **Invio**.

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

DOWNLOAD DEL CERTIFICATO !

Si prega di selezionare un'opzione di protezione

Scarica il certificato
Selezionare questa opzione se si utilizza il computer per l'autenticazione. Selezionando questa opzione si acquisirà un'impronta digitale che identifica univocamente il computer come autorizzato ad accedere ai nostri siti web.

Annullare
La smartcard non sarà scaricata.

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



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



Selezionando la voce evidenziata in rosso **(home)** si potrà procedere con il login alla BDNA.

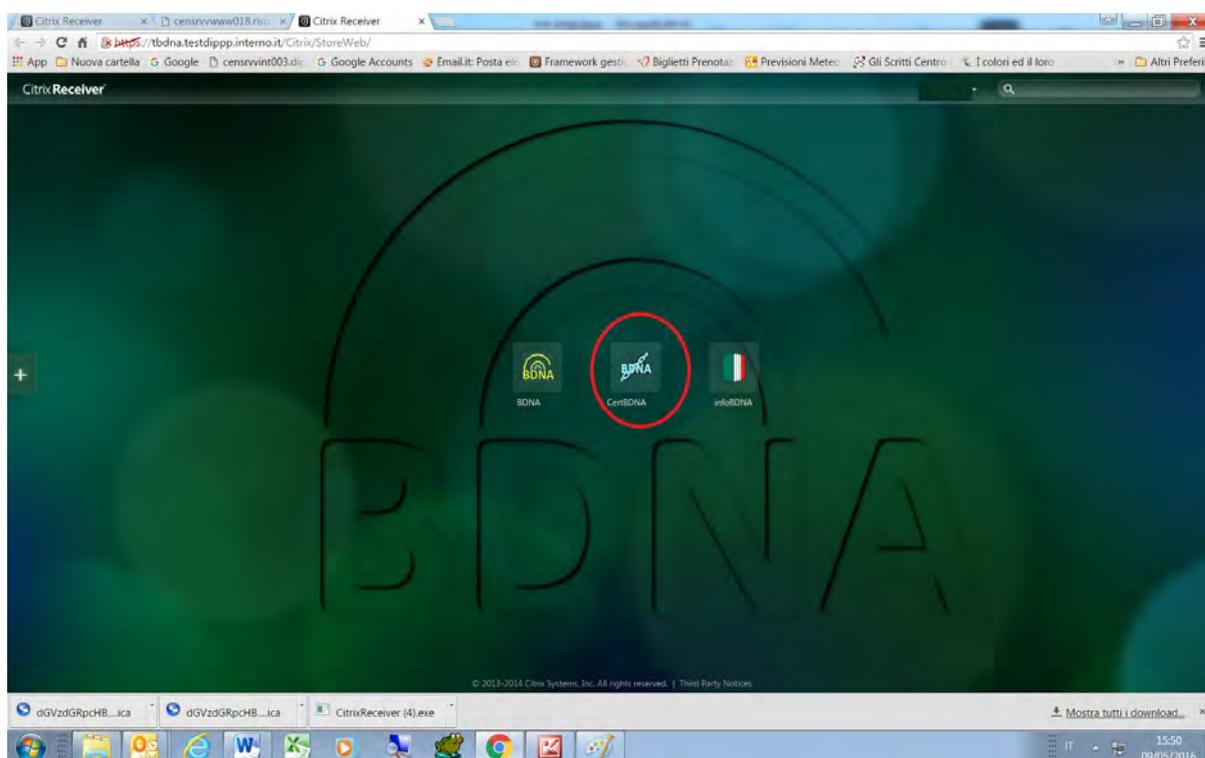


4) CAMBIO POSTAZIONE DI LAVORO

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 APPLICATIVA



Viene proposto il menù delle funzioni.

Sono attive due funzioni:

- . Cambio Postazione di Lavoro
- . Cambio Password smart card

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!

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*"



MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Benvenuto [nome] (Esci)

Lista delle operazioni

- Certificazione Postazione di Lavoro (Prima Attivazione)
- [Cambio Postazione di Lavoro](#)
- Password smart card dimenticata
- [Cambio Password smart card](#)
- Sblocco credenziali

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Sul cellulare arriverà un sms contenente la OTP (One Time Password) cioè un codice numerico utilizzabile solo una volta che dovrà essere digitato, **entro 2 minuti dalla ricezione**, 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, deselegionandola, i caratteri digitati saranno criptati.

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Scarico Certificato. Utente: [nome] !

Autenticazione One Time Password per la definizione della password del certificato.

La One Time Password viene inviata al numero di telefono registrato. Si prega di inserire la One Time Password nella casella sottostante.

Nome Utente dpp1043537

Inserisci la tua OTP: [Visualizza i caratteri](#)

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



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

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

DOWNLOAD DEL CERTIFICATO !
Username: [input field]

Si prega di selezionare un'opzione di protezione

Scarica il certificato
Selezionare questa opzione se si utilizza il computer per l'autenticazione. Selezionando questa opzione si acquisirà un'impronta digitale che identifica univocamente il computer come autorizzato ad accedere ai nostri siti web.

Annullare
La smartcard non sarà scaricata.

[Conferma]

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

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

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Certificato scaricato correttamente.
[Torna alla home](#)

Il certificato è stato scaricato correttamente sul vostro sistema.

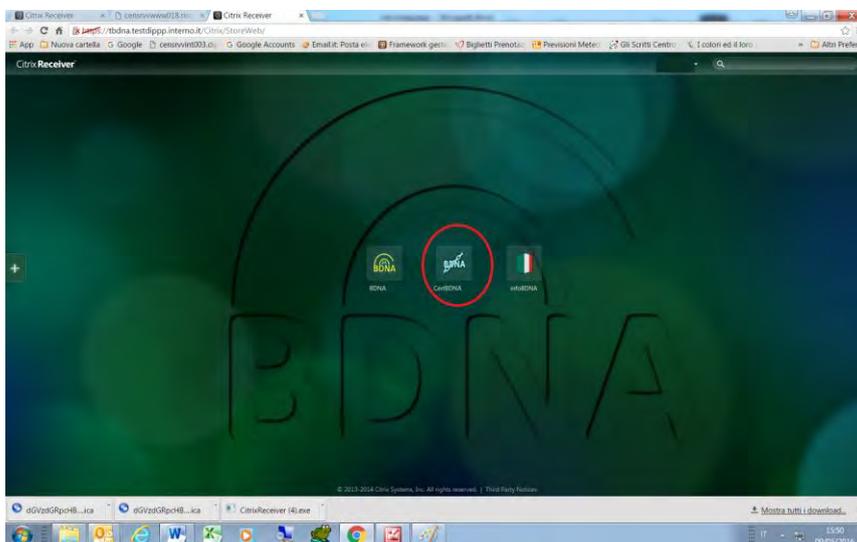
a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Selezionando la voce evidenziata in rosso (**home**) si potrà procedere con il login alla BDNA.



5) CAMBIO PASSWORD APPLICATIVA

Cliccare sull'icona **CertBdna**



Si ricorda che la PASSWORD APPLICATIVA 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.

E' possibile effettuare il **cambio password** cliccando sul link

"Password applicativa dimenticata/Cambio Password applicativa"

senza digitare le credenziali.





Verrà richiesto di digitare **l'indirizzo email accreditato** e cliccare
SU

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Reset Password applicativa
Si prega di inserire il vostro indirizzo email.
Verrà inviata una One Time Password al numero di telefono registrato.

Indirizzo email:

Attenzione: Non salvare questo link nei favoriti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Successivamente sul proprio cellulare arriverà un sms con una OTP.

Digitare nella casella la **OTP** ricevuta via SMS **entro 2 minuti dalla ricezione.**

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Reset della password per l'utente con email:
email@interno.it!

Verifica Utente per il Reset della password applicativa

La One Time Password è stata inviata al vostro numero di telefono registrato.
Indirizzo email: email@interno.it

Inserire la OTP ricevuta via SMS: [Visualizza OTP](#)

Attenzione: Non salvare questo link nei favoriti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Selezionando **"Visualizza OTP"** si può controllare quanto digitato.



Presentare

Per continuare il cambio password cliccare sul pulsante che presenterà la maschera del cambio password.

MINISTERO DELL'INTERNO

PORTALE DI ACCESSO SERVIZI APPLICATIVI

Reset Password applicativa !

Reset Password applicativa

Si prega di fornire la Nuova Password e la conferma.
Indirizzo email: email@interno.it

Nuova Password applicativa:

Conferma Nuova Password applicativa:

Continua >>

Attenzione: Non salvare questo link nei favoriti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

La **PASSWORD APPLICATIVA** deve avere le seguenti caratteristiche:

- . 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 lettere minuscole
- . deve contenere almeno 1 NUMERO
- . deve contenere almeno 1 carattere speciale
- . deve essere diversa dalle ultime 2 password utilizzate

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

Digitare la nuova password applicativa e ripeterla nella casella successiva per conferma e concludere con il pulsante

Continua >>



Nella successiva schermata l'avvenuto cambiamento della password applicativa 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 applicativa perché la stessa potrebbe contenere la segnalazione di un errore e conseguentemente la NON registrazione della nuova password applicativa come nell'esempio seguente



MINISTERO DELL'INTERNO

PORTALE DI ACCESSO SERVIZI APPLICATIVI



Errore durante il reset Password

L'utente inserito e' sbagliato o non e' presente nell'elenco

I dati inseriti non sono attualmente disponibili nel nostro sistema.
Si prega di contattare la prefettura di riferimento per il supporto.

[Continua >>](#)

Attenzione: Non salvare questo link nei favoriti.



a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



6) **CAMBIO PASSWORD SMART CARD**

(ex Pin ex Online password ex Password del certificato)

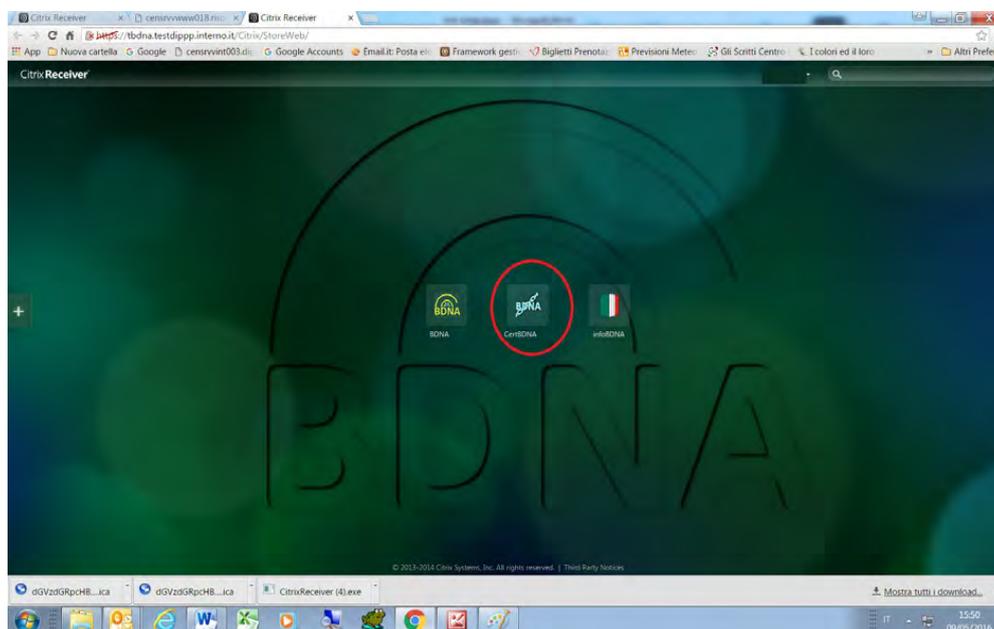
La **PASSWORD SMART CARD** (che è stata chiamata anche *Online password o Pin o Password del certificato*) è una password **distinta** dalla password applicativa ed è **strettamente e univocamente legata alla protezione della smart card virtuale che contiene il "Certificato digitale"**.

(vedi spiegazione nel glossario all'inizio del manuale)

Mentre la PASSWORD SMART CARD può essere cambiata a discrezione dell'utente, **il Certificato, invece, ha una scadenza annuale.**

Alla scadenza del Certificato dovrà, necessariamente, essere impostata una nuova PASSWORD SMART CARD

Per accedere a questa funzione cliccare sull'icona **CertBdna**





Selezionare la funzione "Cambio password smart card"

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Benvenuto [nome] (Esci)

Lista delle operazioni

- Certificazione Postazione di Lavoro (Prima Attivazione)
- [Cambio Postazione di Lavoro](#)
- Password smart card dimenticata
- [Cambio Password smart card](#) ←
- Sblocco credenziali

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Il sistema invia un sms sul cellulare dell'utente con una OTP che deve essere digitata, **entro 2 minuti dalla ricezione**, nella casella "Inserisci la tua OTP"

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Scarico Certificato. Utente: [nome]!

Autenticazione One Time Password per la definizione della password del certificato.

La One Time Password viene inviata al numero di telefono registrato. Si prega di inserire la One Time Password nella casella sottostante.

Nome Utente [nome]

Inserisci la tua OTP: [Visualizza i caratteri](#)

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



Verrà proposta la seguente maschera nella quale deve essere inserita l'attuale PASSWORD SMART CARD.

Poi comporre la nuova PASSWORD SMART CARD che dovrà anche essere confermata.

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

cambiare la password del Certificato

Username:

Inserisci la vecchia password.

Password Smart Card Certificato:

Nuova Password Smart Card *:

Conferma Nuova Password Smart Card *:

ArcotID activex Client 6.2.0.0 ready.
Attenzione: Non registrare questa pagina nei prefetti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

La PASSWORD SMART CARD deve avere le seguenti caratteristiche:

- . 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 lettere minuscole
- . deve contenere almeno 1 NUMERO
- . deve contenere almeno 1 carattere speciale **esclusi * £ \$ € & !**
- . deve essere diversa dalle ultime 2 password utilizzate



Comporre quindi con le regole suddette la PASSWORD SMART CARD.

Annotarla e conservarla con cura.

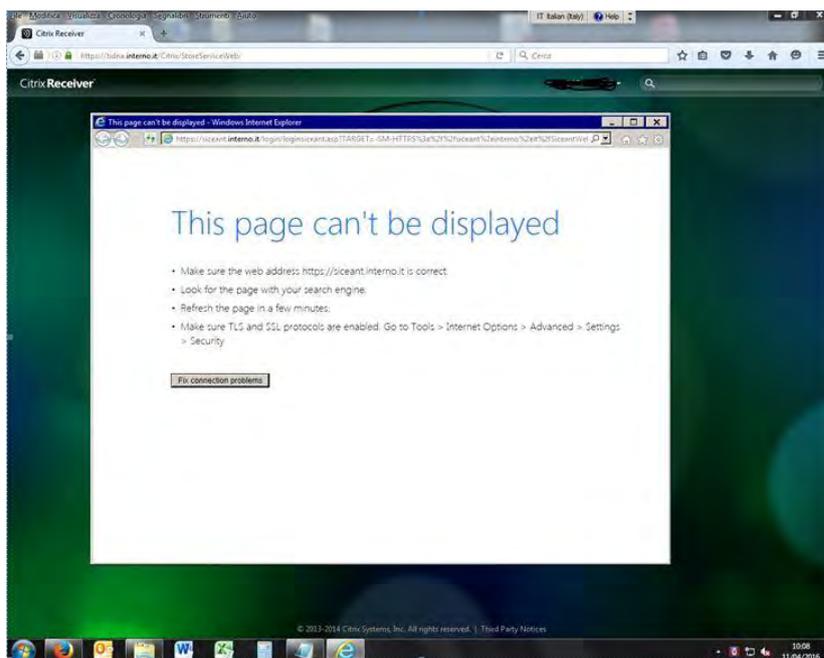
.... (Come già detto nella sezione di certificazione dell'utente)

E' molto importante annotarla e conservarla con cura perché in caso di digitazioni errate della stessa verrà applicato un blocco e verrà negato l'accesso al sistema.

Per ripristinare il normale accesso sarà necessario inviare un modulo di richiesta SBLOCCO PASSWORD SMART CARD, firmato dal dirigente dell'ufficio, a assistenza.antimafia@interno.it che provvederà all'eliminazione del blocco applicato.

AVVISO

Al momento della creazione della PASSWORD SMART CARD è necessario fare attenzione a **non superare i 14 caratteri** per evitare di ottenere la seguente schermata:





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**) si potrà procedere con il login alla BDNA.



7) PASSWORD SMART CARD DIMENTICATA

Nel caso in cui non si ricordi la PASSWORD SMART CARD impostata durante la **certificazione dell'utente** si deve inoltrare una richiesta alla casella di posta assistenza.antimafia@interno.it

Le istruzioni su come inoltrare la richiesta si possono reperire

A) sul portale della Prefettura-Utg di competenza



B) sul portale della BDNA nella sezione InfoBDNA



Le informazioni della sezione BDNA sono reperibile anche sul sito del *Dipartimento per le politiche del personale dell'Amministrazione civile e per le risorse strumentali e finanziarie* all'indirizzo

<http://politichepersonale.interno.it>



MINISTERO DELL'INTERNO

Accessibilità

Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie

Home | Ministero

Ministero dell'Interno

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

Il Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie svolge le funzioni e i compiti spettanti al Ministero di seguito indicati:

politiche del personale e gestione delle risorse umane dell'amministrazione civile;
organizzazione delle strutture centrali e periferiche dell'amministrazione civile;
sviluppo delle attività formative per il personale dell'amministrazione civile;
documentazione generale e statistica a sostegno dell'attività di amministrazione generale del Ministero e delle Prefetture-Uffici territoriali del Governo;
coordinamento dei sistemi informativi automatizzati, promozione e impiego delle tecnologie informatiche;
gestione delle risorse finanziarie e strumentali per le esigenze generali del Ministero.

Il Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie è diretto da un Capo Dipartimento e ad esso sono assegnati un vice Capo Dipartimento per l'esplicitamento delle funzioni un altro vice Capo Dipartimento al quale è anche affidata la responsabilità della Direzione centrale per le risorse umane. Il Capo del Dipartimento può delegare ai vice capi, di volta in volta o in via generale, specifiche attribuzioni.

Dipartimento si avvale del supporto qualificato degli Uffici di diretta collaborazione.

Gli Uffici di diretta collaborazione con il Capo Dipartimento

Ufficio I - Gabinetto del Capo Dipartimento
Ufficio II - Studi, analisi, affari legislativi e parlamentari
Ufficio III - Pianificazione, programmazione e controllo di gestione
Ufficio IV - Relazioni sindacali
Ufficio V - Valutazione
Ufficio VI - Innovazione e organizzazione
Commissione per la progressione in carriera

Il Dipartimento è articolato nelle seguenti direzioni:

Direzione centrale per le risorse umane
Direzione centrale per le risorse finanziarie e strumentali

Dal Dipartimento per le politiche del personale dell'amministrazione civile e per le risorse strumentali e finanziarie dipende la Scuola Superiore dell'Amministrazione dell'Interno (S.S.A.I.), quale istituto di formazione, quale aggiornamento del personale dell'Amministrazione civile dell'Interno. Con l'entrata in vigore del G.P.R. 24 novembre 2009 e 210 per il comma 3, la Scuola assicura anche la funzione di documentazione generale e di statistica dell'attività di amministrazione generale del Ministero e delle prefetture - Uffici territoriali del Governo. Alla Scuola sono altresì attribuiti compiti di analisi e ricerca su tematiche socio-economiche emergenti sul territorio.

Le Direzioni centrali
Gli Uffici di diretta collaborazione
L.T.G.A.
Accordi sindacali
Circolari
Circolari Personale Amministrazione Civile
Provvidenze Straordinarie
Atti normativi
Carriera Prefettizia
Comitato unico di garanzia
Dirigenti Contrattualizzati Amministrazione Civile
Interno
Gare ed appalti
Molteplicità sessuali
Amministrazione trasparente
Borse di studio
Convenzioni
Banca dati nazionale antimafia
In evidenza

A) ISTRUZIONI CONTENUTE SUL PORTALE DELLA PREFETTURE-UTG DI COMPETENZA

Collegarsi sul portale della Prefettura nella sezione

1. **B.D.N.A. Banca dati nazionale unica antimafia, SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)**

Verrà mostrata la pagina che segue

3.0 SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)

In questa sezione sono elencate le tipologie di problemi di natura tecnica che si possono presentare:

Password smart card bloccata e/o Password smart card dimenticata
(Password smart card = ex PIN = ex PASSWORD ON LINE = ex PASSWORD DEL CERTIFICATO)
Account sospeso / Riattivazione utenza
Certificato scaduto /Prima attivazione

Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente. Il modello deve essere allegato ad una mail da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.
L'oggetto della mail deve indicare la **tipologia del problema** e la **sigla della provincia**.
La tipologia del problema sarà riportata automaticamente scegliendo una delle tipologie di seguito indicate mentre la sigla della provincia deve essere scritta manualmente.

Password smart card bloccata
 Password smart card dimenticata **3**
 Account sospeso
 Riattivazione utenza
 Certificato scaduto Stazione Appaltante
 Certificato scaduto Prefettura-U.T.G.
 Prima attivazione

Il contatto può avvenire esclusivamente via email.
Il messaggio deve contenere obbligatoriamente:

- username
- il nominativo
- il recapito telefonico
- l'indirizzo mail personale del richiedente per eventuali contatti da parte degli operatori dell'ASSISTENZA TECNICA
- la descrizione della problematica

Nei moduli predisposti richiedenti la firma del Dirigente si fa presente che la firma deve essere in originale e che non potranno, per ovvi motivi di sicurezza, essere prese in considerazione richieste avanzate con moduli non corretti.

Documenti scaricabili

Modulo per la richiesta della riattivazione dell'utenza in caso di account sospeso
 Modulo per la richiesta di sblocco della Password smart card o generazione di una nuova Password smart card se precedente dimenticata **2**
 Richiesta nuova certificazione per Prefettura- U.T.G.
 Richiesta nuova certificazione per Stazione Appaltante



- 4) Scaricare il modulo "Modulo per la richiesta di sblocco/reset password smart card" se precedente dimenticata

Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome e Cognome Dirigente	
Tipo di operazione (scegliere SOLO una operazione)	Sblocco Password Smart card <input type="checkbox"/> Password Smart card dimenticata <input type="checkbox"/>

Firma del Dirigente
.....

Compilare tutti i dati richiesti.

E' importante scegliere una sola operazione tra le due proposte, in questo caso "Password smart card dimenticata".

Il modulo deve essere firmato dal dirigente dell'ufficio.

Eseguire la scansione del modulo per poterlo allegare la email di cui al punto successivo.

- 3) Tornare sulla pagina del portale e selezionare la voce "Password smart card dimenticata" per ottenere una email con l'indirizzo e l'oggetto predisposti oppure inviare una email al seguente indirizzo assistenza.antimafia@interno.it specificando nell'oggetto la dicitura "Password smart card dimenticata - SIGLA PROVINCIA"

Nel corpo della email è necessario indicare i seguenti dati:

USERNAME
NOMINATIVO
RECAPITO TELEFONICO
INDIRIZZO EMAIL PERSONALE

Allegare il modulo compilato e firmato dal dirigente.



B) ISTRUZIONI CONTENUTE SUL PORTALE BDNA

Verrà mostrata la pagina che segue:

The screenshot shows the 'infoBDNA' portal with a navigation menu on the left and a main content area. The main content area is titled 'SEGNALEZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)' and contains instructions for reporting technical issues. A red arrow points to the 'Allegati' link at the bottom of the page.

Cliccare sul collegamento agli allegati e scegliere

**Modulo richiesta ripristino PASSWORD SMART CARD
Password smart card dimenticata)**



Scaricare il modulo "Modulo per la richiesta ripristino Password smart card"



 **MINISTERO DELL'INTERNO**

Dipartimento Pubblica Amministrazione Civile e per le Risorse Strumentali e Finanziarie
Direzioni Centrali Risorse Finanziarie e Strumentali
URBIS IV - Innovazione tecnologica per l'amministrazione pubblica

**MODULO RICHIESTA SBLOCCO/RESET
PASSWORD SMART CARD BDNA**

Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome e Cognome Dirigente	
Tipo di operazione <i>(scegliere SOLO una operazione)</i>	Sblocco <input type="checkbox"/> Password Smart card <input type="checkbox"/> Password Smart card dimenticata <input type="checkbox"/>

Firma del Dirigente
.....

Compilare tutti i dati richiesti.

E' importante scegliere una sola operazione tra le due proposte

Il modulo deve essere firmato dal dirigente dell'ufficio.

Eseguire la scansione del modulo per poterlo allegare alla email di cui al punto successivo.

Selezionare nel menù "*facsimile email per Password smart card dimenticata*" per vedere come compilare la email da inviare all'indirizzo

assistenza.antimafia@interno.it

Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente.

Il modello deve essere allegato ad una mail (tra gli allegati sono presenti i facsimili delle mail) da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.

L'oggetto della mail deve indicare la tipologia del problema e la sigla della provincia :

facsimile mail per password smart card bloccata

facsimile mail per password smart card dimenticata



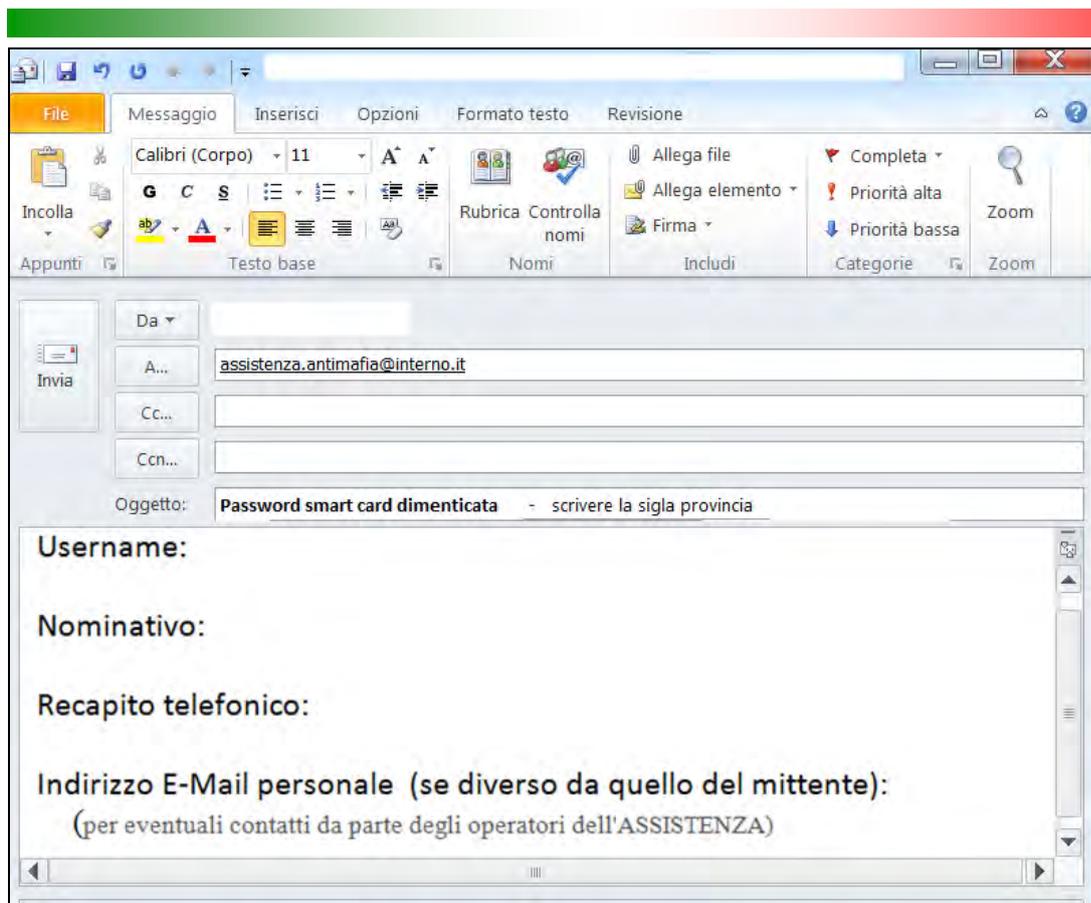
facsimile mail per Account sospeso

facsimile mail per Riattivazione utenza

facsimile mail per Certificato scaduto Stazione Appaltante

facsimile mail per Certificato scaduto Prefettura-U.T.G.

facsimile mail per Prima attivazione



Compilare la email come indicato, allegare il modulo firmato dal dirigente e spedire.

Dopo aver ricevuto la email, l'Assistenza tecnica provvederà ad attivare la funzione "*Password smart card dimenticata*" della Lista delle operazioni che potrà essere utilizzata al successivo accesso sul portale **BDNA** cliccando sull'icona **CERTBDNA**





MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Benvenuto [nome] (Esci)
Lista delle operazioni

- Certificazione Postazione di Lavoro (Prima Attivazione)
- Cambio Postazione di Lavoro
- [Password smart card dimenticata](#)
- Cambio Password smart card
- Sblocco credenziali

Attenzione: La funzione di reset della password e' stata attivata su richiesta. Le altre funzioni torneranno disponibili dopo il reset e al prossimo accesso.

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Selezionando questa funzione il sistema invia un sms sul cellulare dell'utente con una OTP che deve essere, **entro 2 minuti dalla ricezione**, digitata nella casella "Inserisci la tua OTP"

MINISTERO DELL'INTERNO PORTALE DI ACCESSO SERVIZI APPLICATIVI

Scarico Certificato. Utente: [nome] !
Autenticazione One Time Password per la definizione della password del certificato.

La One Time Password viene inviata al numero di telefono registrato. Si prega di inserire la One Time Password nella casella sottostante.

Nome Utente [nome]
Inserisci la tua OTP: [Visualizza i caratteri](#)

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016

Propone quindi la maschera nella quale si potrà inserire una nuova PASSWORD SMART CARD e poi confermarla.



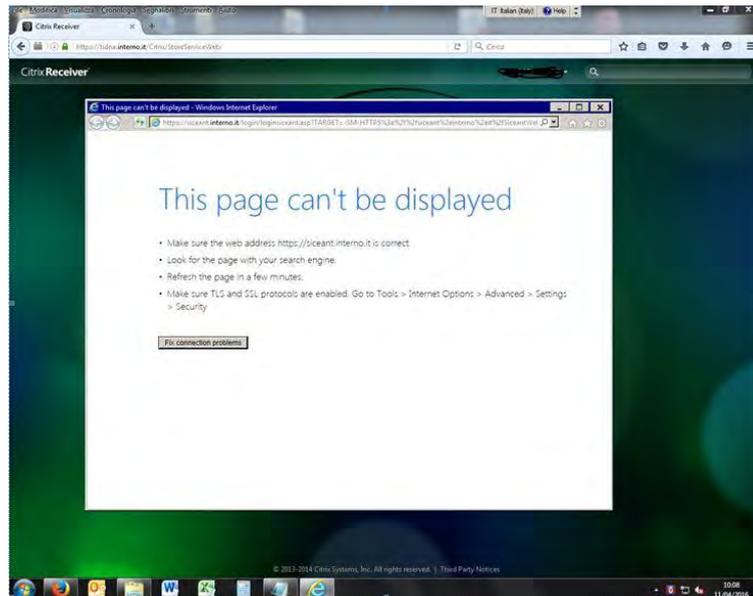
La PASSWORD SMART CARD deve avere le seguenti caratteristiche:

- . 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 lettere minuscole
- . deve contenere almeno 1 NUMERO
- . deve contenere almeno 1 carattere speciale **esclusi * £ \$ € & !**
- . deve essere diversa dalle ultime 2 password utilizzate

Comporre quindi con le regole suddette la PASSWORD SMART CARD,
annotarla e conservarla con cura.

AVVISO

Al momento della creazione della PASSWORD SMART CARD è necessario fare attenzione a **non superare i 14 caratteri** per evitare di ottenere la seguente schermata:



Impostare la PASSWORD SMART CARD scelta **inserendo i caratteri** nella casella denominata **"Nuova Password smart card"** e poi riscriverlo nella casella denominata **"Conferma Nuova Password smart card"**.

MINISTERO DELL'INTERNO

PORTALE DI ACCESSO SERVIZI APPLICATIVI

Definizione della nuova password smart card

Si prega di digitare la Nuova Password e di confermarla.

Utente:

Nuova Password smart card * :

Conferma Nuova Password smart card * :

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



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**) si potrà procedere con il login alla BDNA.



8) **PASSWORD SMART CARD BLOCCATA**

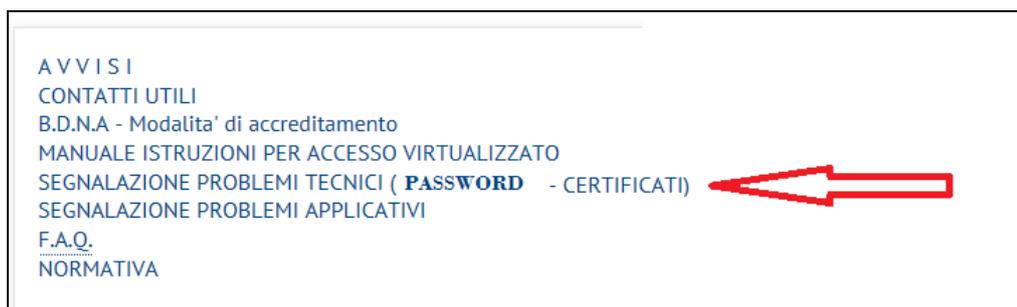
La Password smart card risulterà bloccata a seguito di una delle seguenti operazioni:

- . per 3 volte è stata digitata erroneamente la OTP ricevuta sul cellulare
- . per 3 volte è stato digitata sul tastierino numerico una Password smart card errata

Quando si riceve la segnalazione di PASSWORD SMART CARD BLOCCATA si deve inoltrare una richiesta alla casella di posta assistenza.antimafia@interno.it seguendo le istruzioni.

Le istruzioni su come inoltrare la richiesta si possono reperire

A) sul portale della Prefettura-Utg di competenza



B) sul portale della BDNA nella sezione InfoBDNA





A) ISTRUZIONI CONTENUTE SUL PORTALE DELLA PREFETTURE-UTG DI COMPETENZA

Collegarsi sul portale della Prefettura nella sezione

1. **B.D.N.A. ▶ Banca dati nazionale unica antimafia ▶ SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)**

Verrà mostrata la pagina che segue

3.0 SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)

In questa sezione sono elencate le tipologie di problemi di natura tecnica che si possono presentare:

Password smart card bloccata e/o Password smart card dimenticata
(Password smart card = ex PIN = ex PASSWORD ON LINE = ex PASSWORD DEL CERTIFICATO)
Account sospeso / Riattivazione utenza
Certificato scaduto /Prima attivazione

Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente.

Il modello deve essere allegato ad una mail da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.

L'oggetto della mail deve indicare la **tipologia del problema** e la **sigla della provincia**.

La tipologia del problema sarà riportata automaticamente scegliendo una delle tipologie di seguito indicate mentre la sigla della provincia deve essere scritta manualmente

Password smart card bloccata
Password smart card dimenticata
Account sospeso
Riattivazione utenza
Certificato scaduto Stazione Appaltante
Certificato scaduto Prefettura-U.T.G.
Prima attivazione

Il contatto può avvenire **esclusivamente** via email.

Il messaggio deve contenere **obbligatoriamente** :

username
il nominativo
il recapito telefonico
l'indirizzo mail personale del richiedente per eventuali contatti da parte degli operatori dell'ASSISTENZA TECNICA
la descrizione della problematica

Nei moduli predisposti richiedenti la firma del Dirigente si fa presente che la firma deve essere in originale e che non potranno, per ovvi motivi di sicurezza, essere prese in considerazione richieste avanzate con moduli non corretti.

Documenti scaricabili

Modulo per la richiesta della riattivazione dell'utenza in caso di account sospeso

Modulo per la richiesta di sblocco della Password smart card o generazione di una nuova Password smart card se precedente dimenticata

Richiesta nuova certificazione per Prefettura- U.T.G.

Richiesta nuova certificazione per Stazione Appaltante



Scaricare il modulo "Modulo per la richiesta di sblocco/reset Password smart card" per Password smart card dimenticata

 MINISTERO DELL'INTERNO <small>Dipartimento Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie Direzione Centrale Risorse Finanziarie e Strumentali Ufficio IV - Innovazione tecnologica per l'amministrazione generale</small>	
MODULO RICHIESTA SBLOCCO/RESET PASSWORD SMART CARD BDNA	
Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome e Cognome Dirigente	
Tipo di operazione <i>(scegliere SOLO una operazione)</i>	Sblocco Password Smart card <input type="checkbox"/> Password Smart card dimenticata <input type="checkbox"/>
Firma del Dirigente	

Compilare tutti i dati richiesti.

E' importante scegliere una sola operazione tra le due proposte, in questo caso "Sblocco PASSWORD SMART CARD"

Il modulo deve essere firmato dal dirigente dell'ufficio.

Eeguire la scansione del modulo per poterlo allegare la email di cui al punto successivo.

2) Tornare sulla pagina del portale e selezionare la voce "Password smart card dimenticata" per ottenere una email con l'indirizzo e l'oggetto predisposti oppure inviare una email al seguente indirizzo assistenza.antimafia@interno.it specificando nell'oggetto la dicitura "Password smart card bloccata - SIGLA PROVINCIA"

Nel corpo della email è necessario indicare i seguenti dati:

USERNAME
NOMINATIVO
RECAPITO TELEFONICO
INDIRIZZO EMAIL PERSONALE

Allegare il modulo compilato e firmato dal dirigente.



B) ISTRUZIONI CONTENUTE SUL PORTALE BDNA

Verrà mostrata la pagina che segue:

Ministero Dell'Interno - Windows Internet Explorer
http://infobdna.dippp.interno.it/gruppoWWW/ita/index.php?IdMat=1&IdSot=11&IdSottomatDirif=11

MINISTERO DELL'INTERNO

infoBDNA - il portale di riferimento per chi opera con la BDNA

Home

Avvisi e notizie

Contatti utili

Modalità per l'accreditamento al sistema

FAQ

Segnalazione problemi tecnici (password - CERTIFICATI)

Segnalazione problemi applicativi

Normativa

Manuali

infoBDNA

SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)

Problematiche tecniche

In questa sezione sono elencate le tipologie di problemi di natura tecnica che si possono presentare:

Password smart card bloccata / password smart card dimenticata (PASSWORD SMART CARD = EX PIN = EX PASSWORD ON LINE = EX PASSWORD DEL CERTIFICATO)
Account sospeso / Riattivazione utenza
Certificato scaduto /Prima attivazione

Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente.
Il modello deve essere allegato ad una mail (tra gli allegati sono presenti i facsimili delle mail) da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.
L'oggetto della mail deve indicare la tipologia del problema e la sigla della provincia :

[facsimile mail per password smart card bloccata](#)
[facsimile mail per password smart card dimenticata](#)
[facsimile mail per Account sospeso](#)
[facsimile mail per Riattivazione utenza](#)
[facsimile mail per Certificato scaduto Stazione Appaltante](#)
[facsimile mail per Certificato scaduto Prefettura-U.T.G.](#)
[facsimile mail per Prima attivazione](#)

Il contatto può avvenire esclusivamente via email.
Il messaggio deve contenere obbligatoriamente:
username
il nominativo
il recapito telefonico
l'indirizzo mail personale del richiedente per eventuali contatti da parte degli operatori dell'ASSISTENZA TECNICA
la descrizione della problematica

Nei moduli predisposti richiedenti la firma del Dirigente si fa presente che la firma deve essere in originale e che non potranno, per ovvi motivi di sicurezza, essere prese in considerazione richieste avanzate con moduli non corretti.

Ufficio IV Innovazione Tecnologica dell'Amministrazione Generale -Sezione Centrale

Allegati

© Pagine realizzate a cura dell'Ufficio IV - Innovazione tecnologica per l'amministrazione generale

Cliccare sul collegamento agli allegati e scegliere

**Modulo richiesta ripristino PASSWORD SMART CARD
Password smart card dimenticata)**





Scaricare il modulo "Modulo per la richiesta di sblocco/reset Password smart card"


MINISTERO DELL'INTERNO
Dipartimento Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie
Direzionale Centrale Risorse Finanziarie e Strumentali
Ufficio IV - Innovazione tecnologica per l'amministrazione generale

**MODULO RICHIESTA SBLOCCO/RESET
PASSWORD SMART CARD BDNA**

Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome e Cognome Dirigente	
Tipo di operazione (scegliere SOLO una operazione)	Sblocco Password Smart card <input type="checkbox"/> Password Smart card dimenticata <input type="checkbox"/>

Firma del Dirigente
.....

Compilare tutti i dati richiesti.

E' importante scegliere una sola operazione tra le due proposte, in questo caso "Sblocco PASSWORD SMART CARD"

Il modulo deve essere firmato dal dirigente dell'ufficio.

Eseguire la scansione del modulo per poterlo allegare la email di cui al punto successivo.

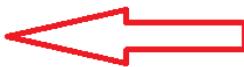
Selezionare nel menù "facsimile email per Password smart card bloccata" per vedere come compilare la email da inviare all'indirizzo assistenza.antimafia@interno.it



Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente.
Il modello deve essere allegato ad una mail (tra gli allegati sono presenti i facsimili delle mail) da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.
L'oggetto della mail deve indicare la tipologia del problema e la sigla della provincia :

facsimile mail per [password smart card bloccata](#)

facsimile mail per [password smart card dimenticata](#)



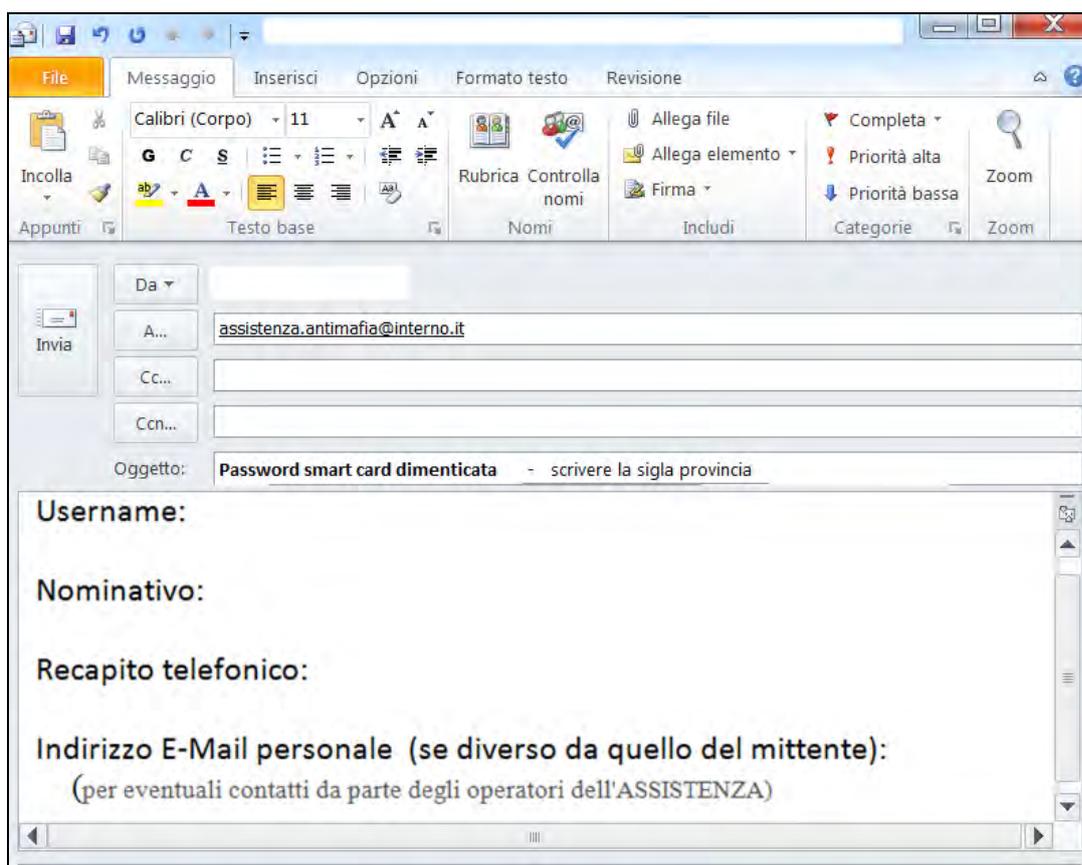
facsimile mail per [Account sospeso](#)

facsimile mail per [Riattivazione utenza](#)

facsimile mail per [Certificato scaduto Stazione Appaltante](#)

facsimile mail per [Certificato scaduto Prefettura-U.T.G.](#)

facsimile mail per [Prima attivazione](#)



Compilare la email come indicato, allegare il modulo firmato dal dirigente e spedire.

Dopo aver ricevuto la email l'Assistenza tecnica provvederà a sbloccare la Password smart card **è la renderà di nuovo operativa senza la necessità di crearne una nuova.**



9) Richiesta rinnovo certificato digitale

Il certificato digitale ha validità di 1 anno dalla sua emissione.

A partire da una settimana prima della data di scadenza è possibile chiederne il rinnovo.

a) Modalità richiesta tramite portale della Prefettura

Nella sezione "Segnalazione problemi tecnici", tra i documento scaricabili sono disponibili 2 moduli:

3.0 SEGNALAZIONE PROBLEMI TECNICI (PASSWORD - CERTIFICATI)

In questa sezione sono elencate le tipologie di problemi di natura tecnica che si possono presentare:

Password smart card bloccata e/o Password smart card dimenticata
(Password smart card = ex PIN = ex PASSWORD ON LINE = ex PASSWORD DEL CERTIFICATO)
Account sospeso / Riattivazione utenza
Certificato scaduto

Per ogni tipologia è presente un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzato con firma del dirigente.
Il modello deve essere allegato ad una mail da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it.
L'oggetto della mail deve indicare la **tipologia del problema** e la **sigla della provincia**.
La tipologia del problema sarà riportata automaticamente scegliendo una delle tipologie di seguito indicate mentre la sigla della provincia deve essere scritta manualmente.

Password smart card bloccata
Password smart card dimenticata
Account sospeso
Riattivazione utenza
Certificato scaduto Stazione Appaltante
Certificato scaduto Prefettura-U.T.G.

Il contatto può avvenire **esclusivamente** via email.
Il messaggio deve contenere **obbligatoriamente** :
username
il nominativo
il recapito telefonico
l'indirizzo mail personale del richiedente per eventuali contatti da parte degli operatori dell'ASSISTENZA TECNICA
la descrizione della problematica

Nel moduli predisposti richiedenti la firma del Dirigente si fa presente che la firma deve essere in originale e che non potranno, per ovvi motivi di sicurezza, essere prese in considerazione richieste avanzate con moduli non corretti.

Ufficio IV Innovazione Tecnologica dell'Amministrazione Generale - Sezione Centrale
Ultima modifica il 23/06/2016 alle 10:58

Documenti scaricabili

- Modulo per sblocco o reset della password smart card
- Modulo per la richiesta della riattivazione dell'utenza in caso di account sospeso
- Richiesta nuova certificazione per Prefettura-U.T.G.
- Richiesta nuova certificazione per Stazione Appaltante

- . Richiesta nuova certificazione per Prefettura – U.T.G.
- . Richiesta nuova certificazione per Stazione appaltante

Selezionare il modello adatto, scaricarlo, compilarlo in tutte le sue parti.

Spedire una mail a assistenza.antimafia@interno.it allegando il modello firmato e scansionato.

Il corpo della mail si può ottenere selezionando, nel menù della sezione, la voce "Certificato scaduto Prefettura-U.T.G." o "Certificato scaduto Stazione appaltante".



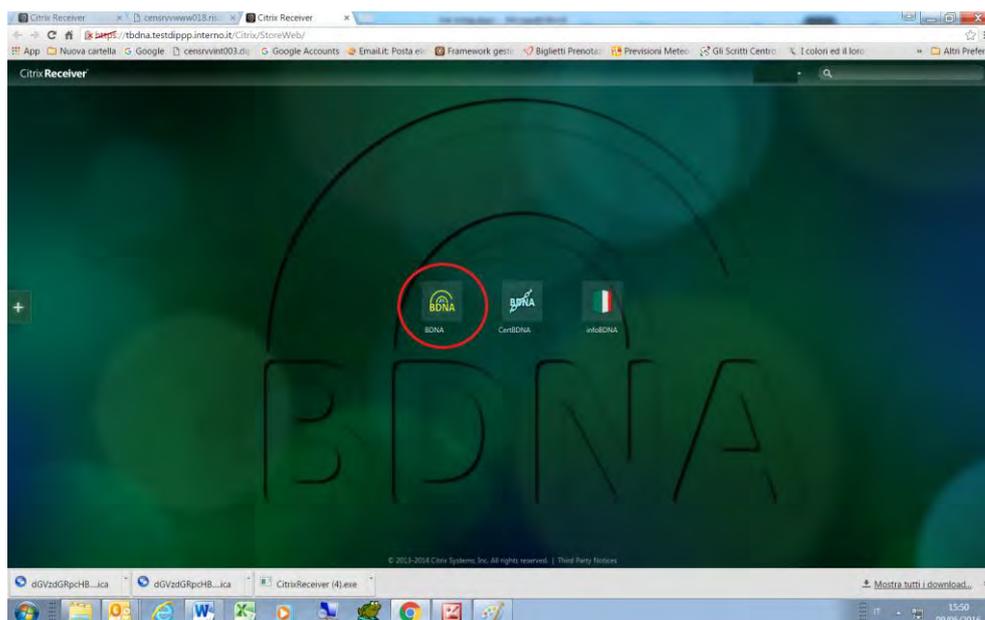
10) Accesso alla B.D.N.A.

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

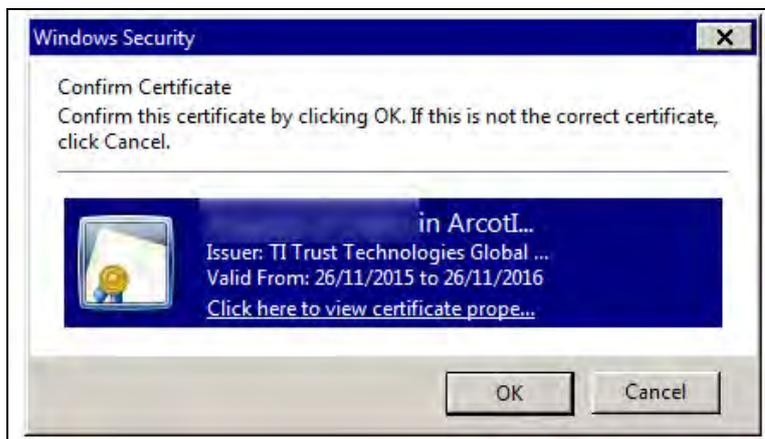
1. Aprire il browser utilizzato sulla propria postazione e connettersi all'indirizzo **<https://bdna.interno.gov.it>** (se STAZIONE APPALTANTE)
<https://bdna.dipp.interno.it> (se PREFETTURA)
2. Eseguire il login digitando nelle rispettive caselle USERNAME e la PASSWORD APPLICATIVA



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

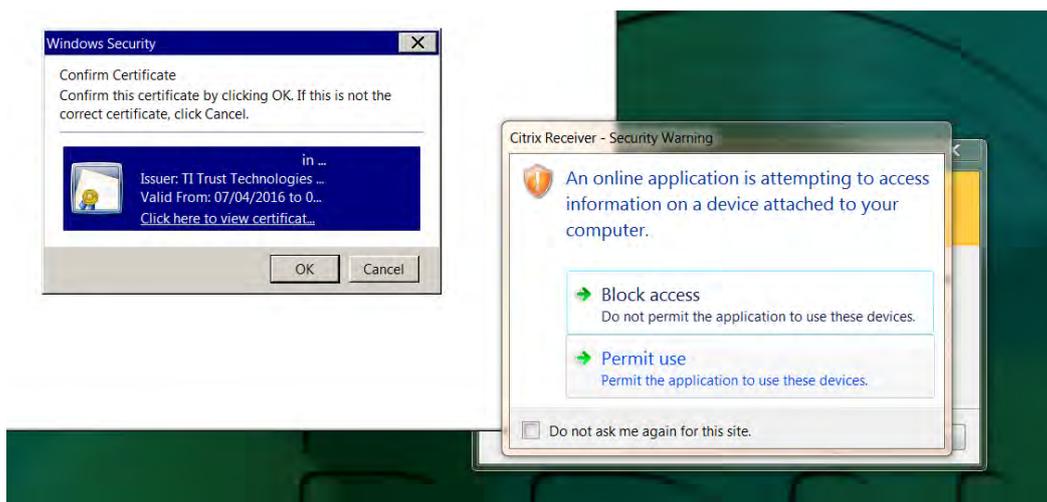


4. All'apertura di una nuova finestra del browser verificare che il certificato digitale riporti il proprio nome e cliccare su OK



Se non si è fatto al momento dello scarico del certificato annotare ora la validità per poter controllare la scadenza. Il rinnovo del certificato potrà essere chiesto una settimana prima della scadenza con le modalità descritte nel punto 9) del presente manuale

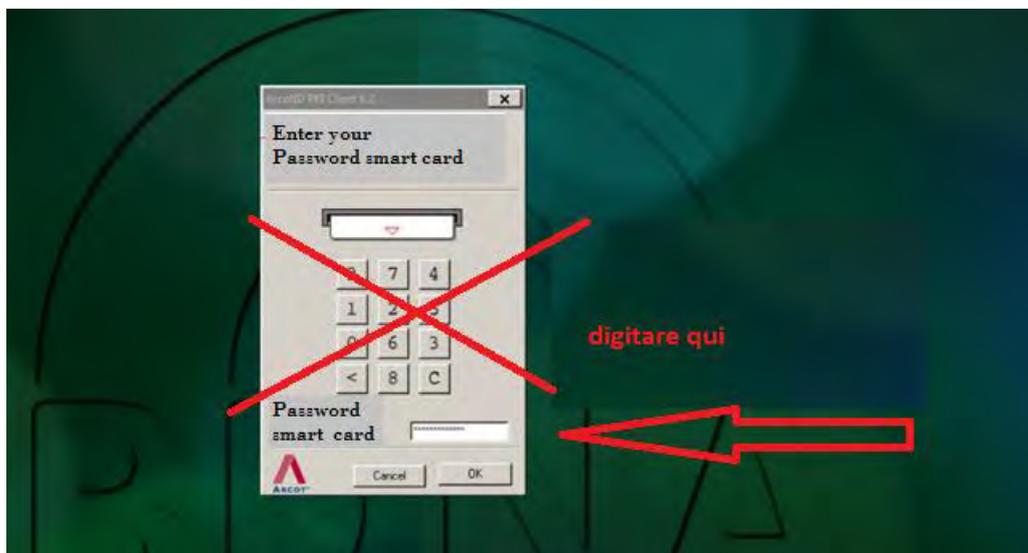
Potrebbe verificarsi che insieme alla visualizzazione dei dati del certificato venga anche richiesta una autorizzazione, come mostrato nella prossima maschera



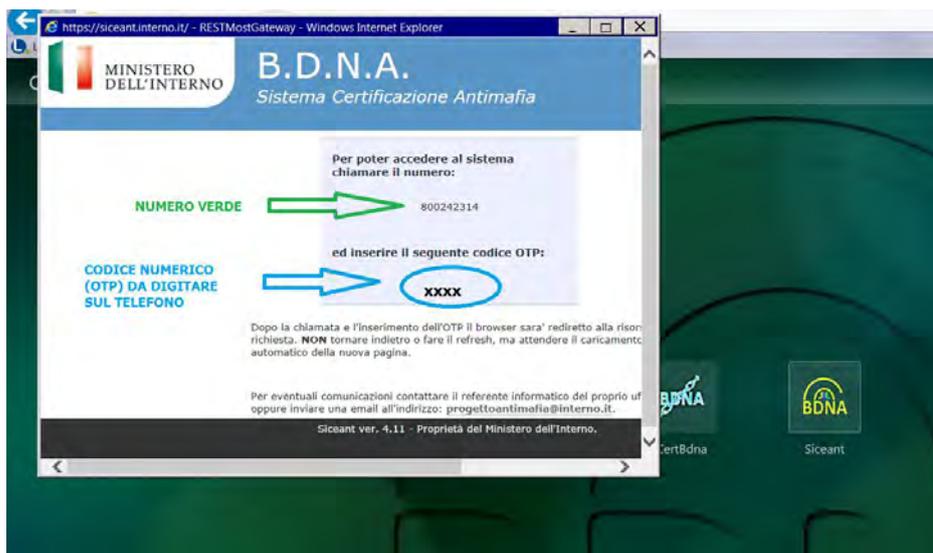
In questo caso cliccare su "Permit" o "Consenti" per continuare.

5. Accettato il certificato viene richiesto di digitare la PASSWORD SMART CARD.
- 6.

Attenzione NON UTILIZZARE I PULSANTI DELLA TASTIERINA NUMERICA, MA SCRIVERE NELLA CASELLA VUOTA I CARATTERI DELLA PASSWORD SMART CARD



7. Il sistema una volta verificata la correttezza della PASSWORD SMART CARD e accettato il certificato digitale presenterà a video un codice numerico di 4 cifre (OTP) ed un numero verde gratuito da contattare.



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



9. 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.



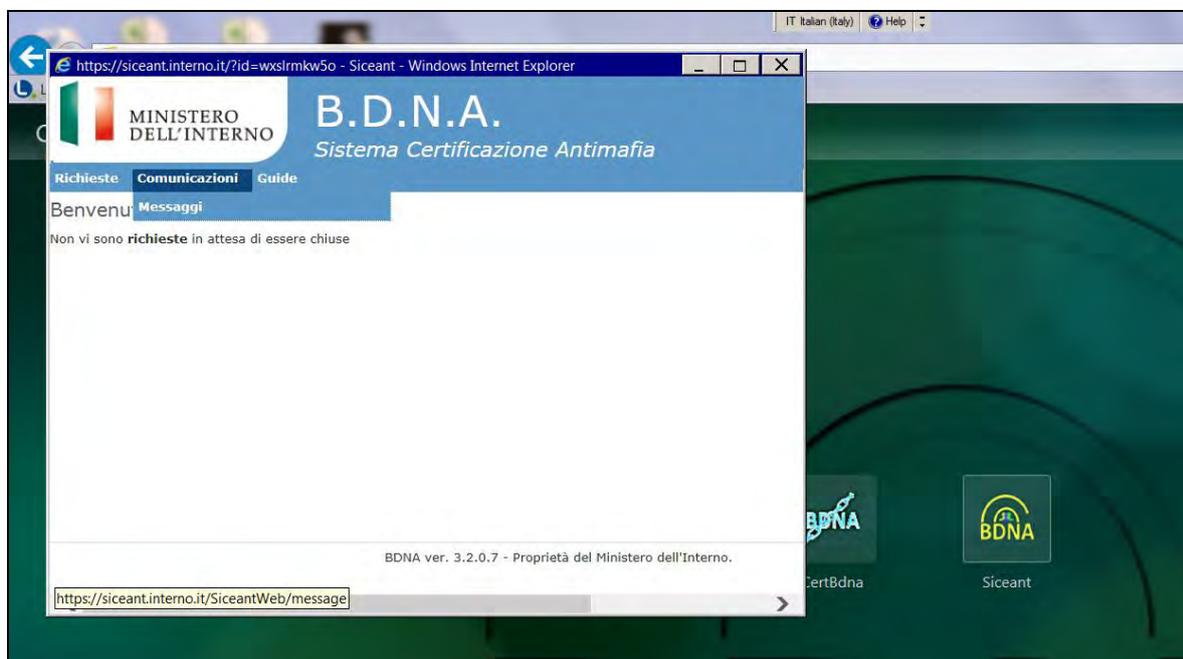
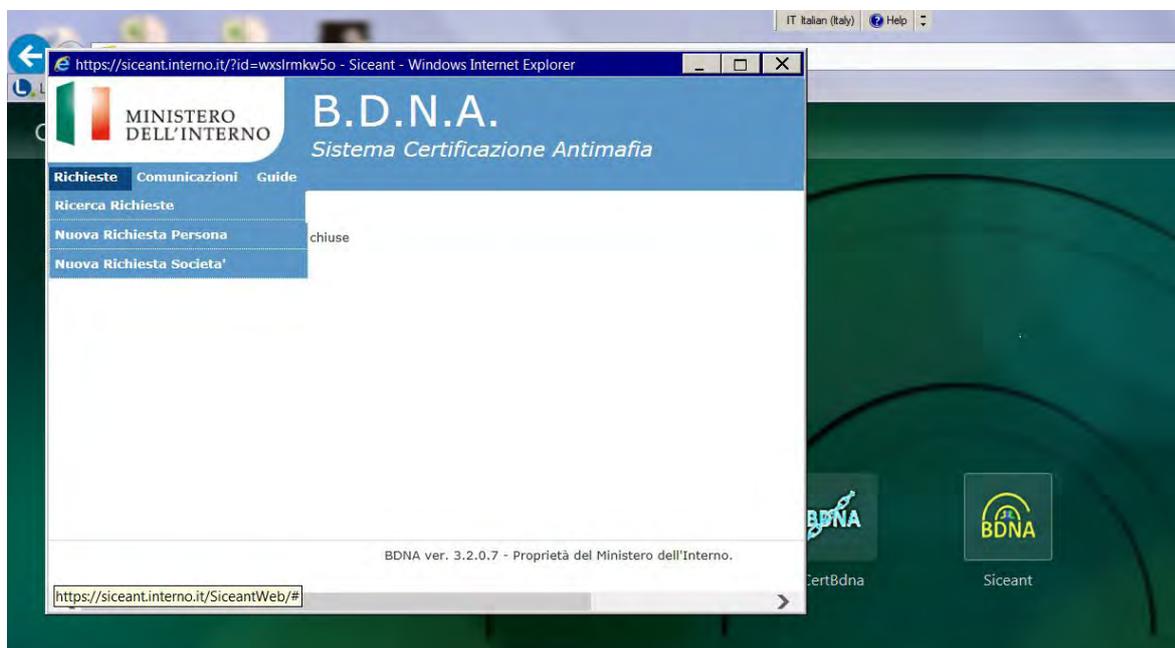
Nel caso di utente di Prefettura, se non gli è stato assegnato il profilo di "Utente Prefettura", vedrà una schermata senza menù:

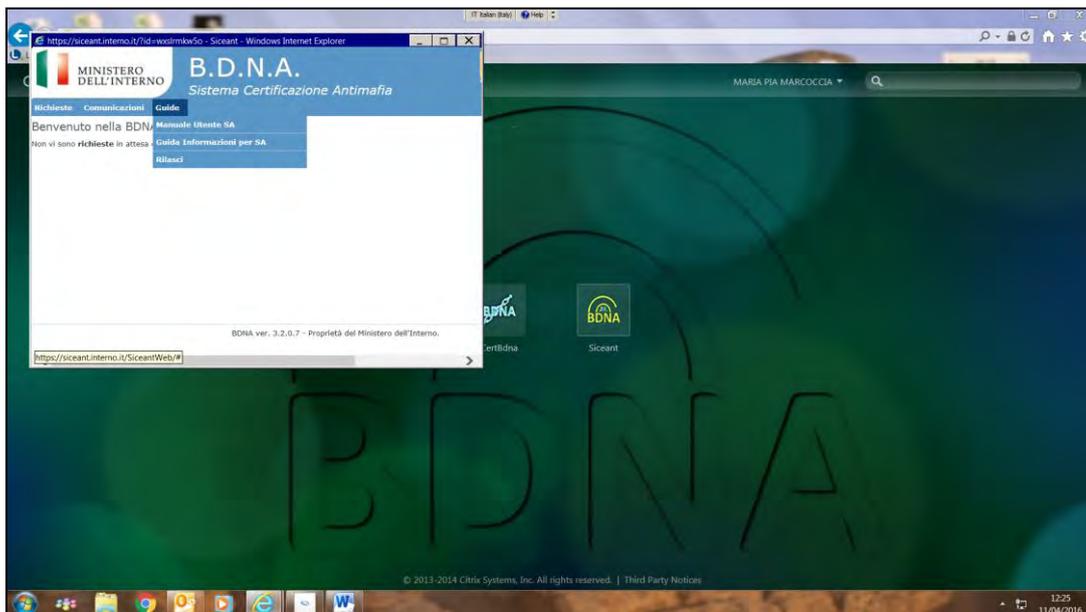


E' necessario che gli venga assegnato il profilo "utente Prefettura" e poi potrà eseguire di nuovo l'accesso.



Le maschere che seguono mostrano le estensioni del menù





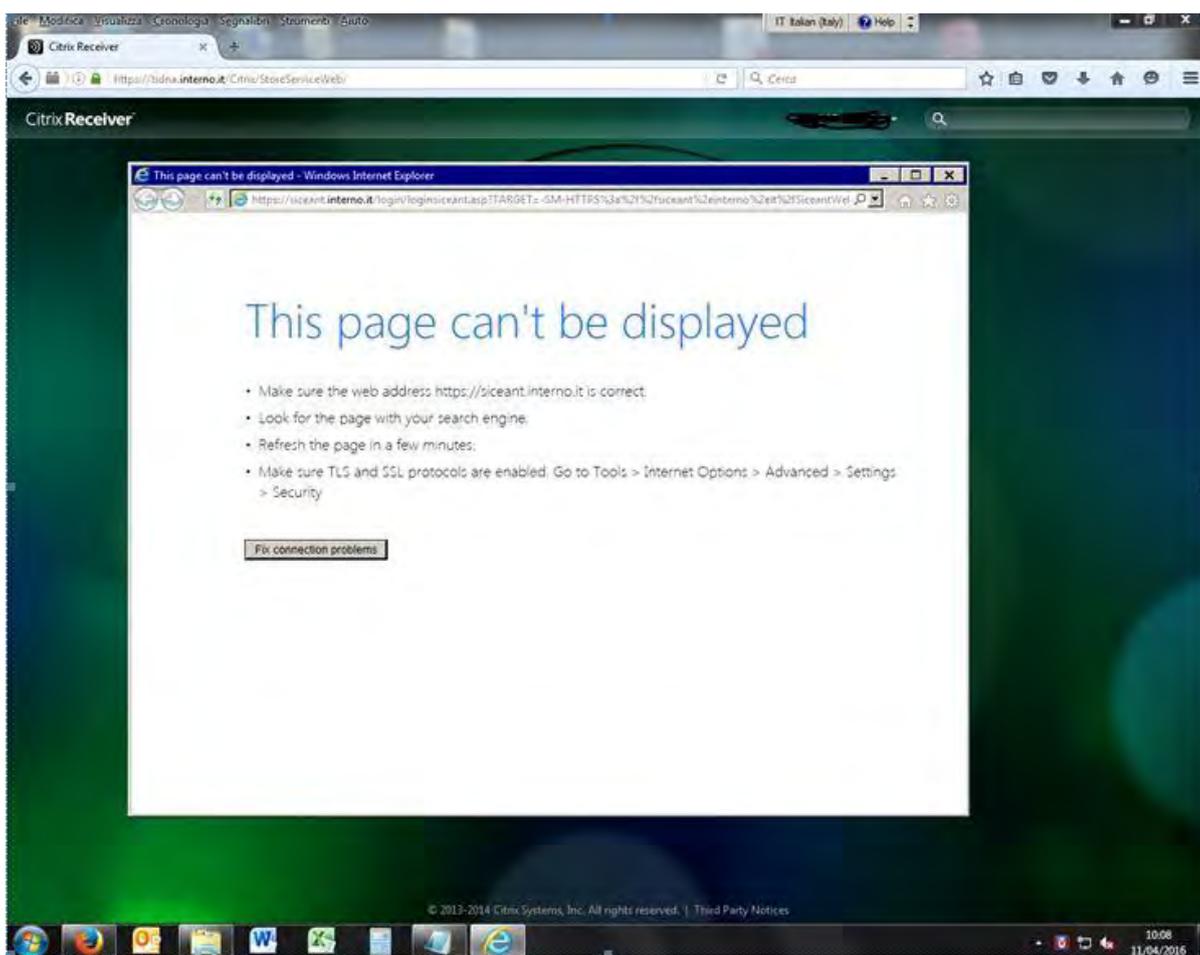


APPENDICE 1

Possibili messaggi di errore.

ERRORE 1

La seguente segnalazione di errore appare quando è impostata una Password applicativa o una Password smart card 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 richiedere lo sblocco del serial number alla casella di posta assistenza.antimafia@interno.it

Inserisci credenziali di accesso

Il campo -serial Number- per questo utente risulta vuoto.

Nome utente

Password

Login

ERRORE 3

Quando il certificato è scaduto oppure 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, password, numero verde.....).





ERRORE 5

La schermata seguente viene proposta quando è stata digitata una OTP diversa da quella inviata sul telefono cellulare.

Digitare correttamente la **otp inviata con il successivo sms**.

MINISTERO DELL'INTERNO

PORTALE DI ACCESSO SERVIZI APPLICATIVI

Scarico Certificato. Utente: dpp1043537 !

Autenticazione One Time Password per la definizione della password del certificato.

La One Time Password viene inviata al numero di telefono registrato. Si prega di inserire la One Time Password nella casella sottostante.

La OTP inserita non è corretta. (Dopo più tentativi errati l'accesso verrà inibito).

Nome Utente dpp1043537

Inserisci la tua OTP: Visualizza i caratteri

Accedi

Attenzione: Non registrare questa pagina nei preferiti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



ERRORE 6

La schermata seguente viene proposta quando la digitazione della Password smart card di conferma è diversa da quella digitata in precedenza.

E' possibile ripetere la digitazione della Password smart card e della sua conferma

The screenshot shows a web portal for the Italian Ministry of the Interior. The header includes the Italian flag, the text 'MINISTERO DELL'INTERNO', and 'PORTALE DI ACCESSO SERVIZI APPLICATIVI'. The main content area features a futuristic blue background with a grid pattern and floating screens. The central text reads: 'Definizione della nuovo pin per la protezione del certificato'. Below this, it says 'Si prega di digitare il Nuovo Pin e di confermarlo.' followed by 'Utente: [masked]'. A red error message states 'Password e Conferma password non corrispondono.' There are two input fields: 'Nuova Password smart card *:' and 'Conferma Nuova Password smart card *:'. An 'Invio' button is located below the second field. At the bottom, a small note says 'Attenzione: Non registrare questa pagina nei preferiti.' The footer of the page reads 'a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016'.



ERRORE 7

La seguente maschera viene proposta quando è stato digitato un indirizzo email per il recupero della Password applicativa diverso da quello registrato.

Selezionando il bottone "Continua" si può tornare alla digitazione dell'indirizzo email.

MINISTERO DELL'INTERNO

PORTALE DI ACCESSO SERVIZI APPLICATIVI

Errore durante il reset Password

L'utente inserito e' sbagliato o non e' presente nell'elenco

I dati inseriti non sono attualmente disponibili nel nostro sistema.
Si prega di contattare la prefettura di riferimento per il supporto.

[Continua >>](#)

Attenzione: Non salvare questo link nei favoriti.

a cura dell'Ufficio IV - Innovazione Tecnologica per l'Amministrazione Generale © 2016



ERRORE 8

La seguente schermata viene proposta quando si è scelto di NON scaricare il certificato digitale durante la prima attivazione.

E' necessario chiudere la schermata e iniziare di nuovo dal login





ERRORE 9

La seguente schermata viene proposta quando si è superato il numero massimo (5) di tentativi permessi per la digitazione delle credenziali durante il login.



E' necessario inviare una email, secondo le indicazioni descritte nella sezione Infobdna alla casella assistenza.antimafia@interno.it :

InfoBDNA

3.0 AVVISI E NOTIZIE	3.0 portale Infobdna
3.0 Contatti utili	SEGNALAZIONE PROBLEMI TECNICI (PIN - CERTIFICATI)
3.0 Modalità per l'accredimento al sistema	Problematiche tecniche
3.0 Segnalazione problemi tecnici (Password - Certificati)	In questa sezione sono elencate le tipologie di problemi di natura tecnica che si possono presentare:
3.0 Segnalazione problemi tecnici (Password - Certificati) per sito dpp	<ul style="list-style-type: none"> Password smart card bloccata e/o Password smart card dimenticata Account sospeso / Riattivazione utenza Certificato scaduto / Pressa attivazione
3.0 Segnalazione problemi applicativi	<p>Per ogni tipologia è previsto un modello scaricabile che deve essere compilato per quanto riguarda i dati richiesti e autorizzate con firma del dirigente. Il modello deve essere allegato ad una mail (tra gli allegati sono presenti i facsimili delle mail) da inviare alla casella di posta elettronica: assistenza.antimafia@interno.it. L'oggetto della mail deve indicare la tipologia del problema e la sigla della provincia.</p> <ul style="list-style-type: none"> facsimile mail per Password smart card bloccata facsimile mail per Password smart card dimenticate facsimile mail per Account sospeso facsimile mail per Riattivazione utenza facsimile mail per Certificato scaduto Stazione Appaltante facsimile mail per Certificato scaduto Prefettura-U.T.G.
3.0 FAQ	
3.0 Manuali	
3.0 Modelli	

Il canale di servizio è esclusivamente via email.
Il messaggio deve contenere obbligatoriamente:
 - cognome
 - il nominativo
 - il recapito telefonico
 - l'indirizzo mail personale del richiedente per eventuali contatti da parte degli operatori dell'ASSISTENZA TECNICA
 - la descrizione della problematica.

Nei modelli predisposti richiesti la firma del Dirigente, si fa presente che la firma deve essere in originale e che non potranno, per ogni motivo di sicurezza, essere prese in considerazione richieste avanzate con modalità diverse.

Facsimile email da inviare

FACSIMILE MAIL PER ACCOUNT SOSPESO

Destinatario mail : assistenza.antimafia@interno.it

Oggetto mail : Account sospeso - scrivere la sigla della provincia del mittente

Corpo della mail:

Username:

Nominativo:

Recapito telefonico:

Indirizzo mail personale (se diverso da quello del mittente) per eventuali contatti da parte degli operatori dell'Assistenza



ERRORE 10

La schermata seguente viene proposta quando la password è scaduta e deve essere reimpostata.

La Password rilasciata dalla Prefettura **"nasce scaduta"** e deve essere cambiata al primo accesso.

The screenshot shows a blue dialog box with a white padlock icon on the left. The text inside the dialog box reads: "Additional Information Required", "Please type your response below.", "Password Expired. Please enter a new password.", followed by a white text input field and a "Submit" button.



ERRORE 11

La seguente schermata viene proposta quando sono state digitate delle credenziali errate.

Si può ripetere la digitazione, ma è necessario fare attenzione a non superare i 5 tentativi perché in questo caso l'account sarà bloccato.

(vedi ERRORE 9)





APPENDICE 2

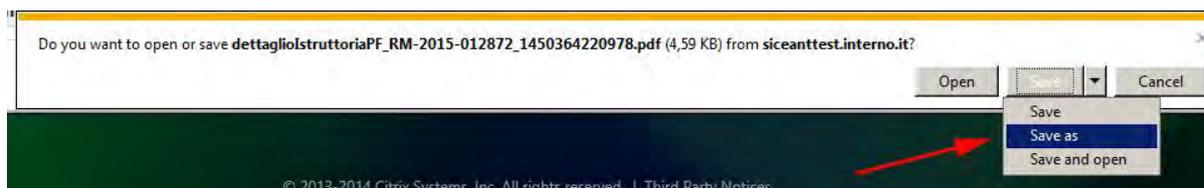
Funzionalità di stampa e salvataggio del PDF

Con l'utilizzo di una macchina virtuale è necessario **ricordare sempre** che le operazioni che si eseguono avvengono **SEMPRE** sul server che ospita la macchina.

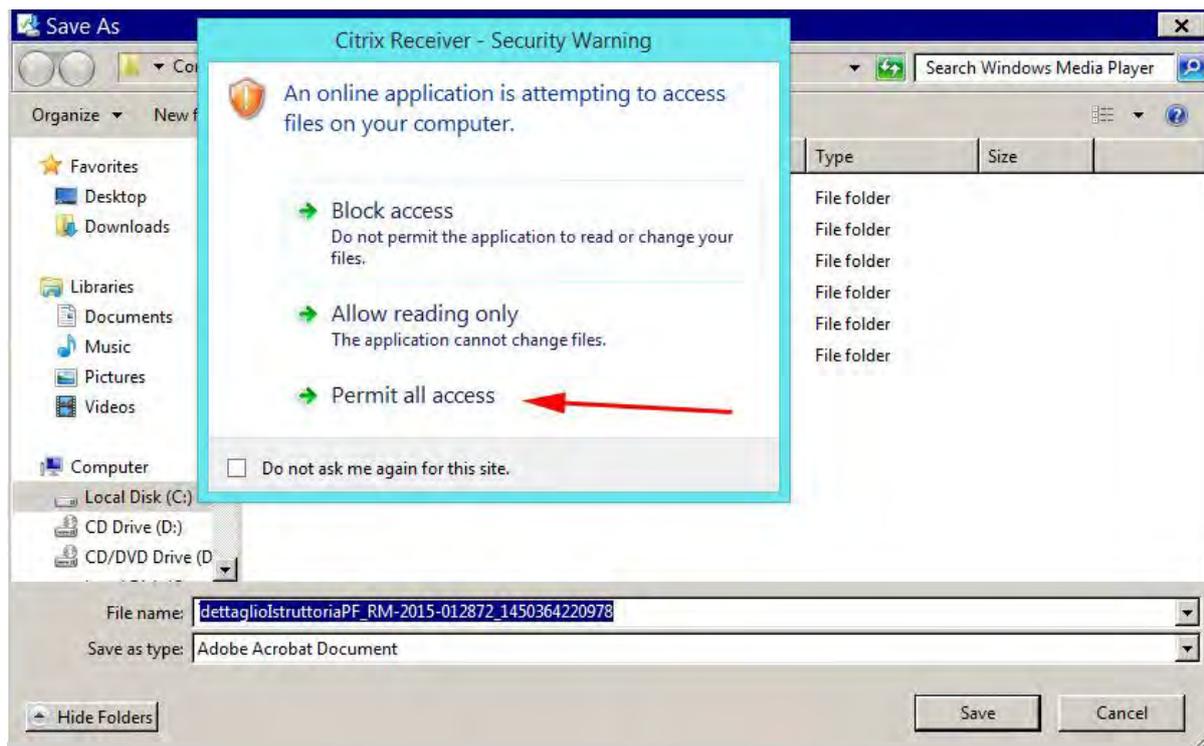
Quindi, nel caso in cui si voglia salvare un PDF prodotto dall'applicativo per utilizzarlo in un momento successivo, non si può **semplicemente** eseguire un "Salva" o "Save" perché il documento sarebbe memorizzato sul server che ospita la macchina Citrix.

Le istruzioni che seguono permetteranno di salvare il documento sul proprio PC.

Utilizzando la funzione proposta "Save as" potremo indicare su quale dispositivo intendiamo salvare il documento.



Può darsi che la macchina ci chieda l'autorizzazione per procedere con il salvataggio. In questo caso selezionare "Permit" .





Nel riquadro a sinistra è necessario selezionare **DOVE** si vuole salvare il documento. Vengono presentati i dispositivi collegati al computer di lavoro. Nell'esempio proposto possiamo vedere che vengono indicati 4 dispositivi:



Local Disk (C:) indica il disco del server che ospita la macchina virtuale Citrix

CD Drive (D:) in questo esempio indica un lettore CD

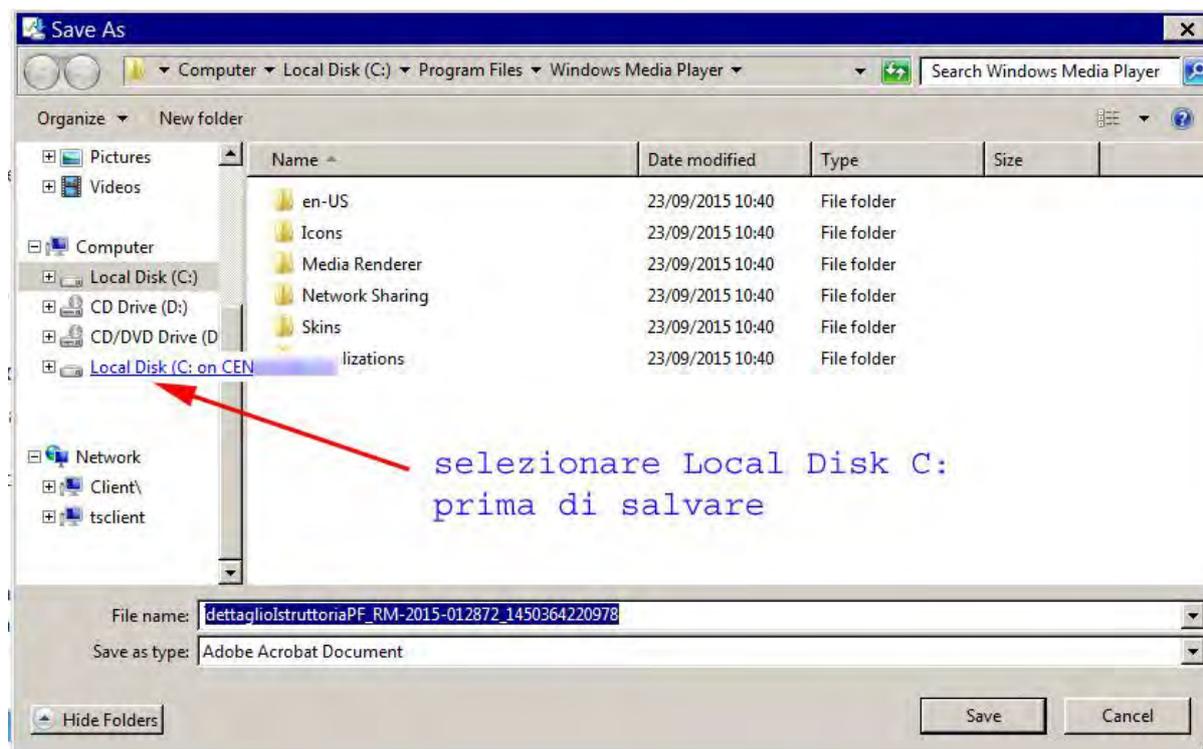
CD/DVD DRIVE (D) in questo esempio indica un lettore di DVD

Possono esserci altri drivers diversi, quello che ci interessa è il seguente

Local Disk (C: on xxxxxxxxxxxxxxxxxxxx) dove xxxxxxxxxxxxxxxxxxxx

indica il nome del computer sul quale vogliamo salvare il documento.

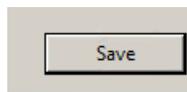
Selezionare, quindi, questa opzione. "Local Disk (C: on *nome del nostro pc*)"





Ora che siamo sicuri di salvare il documento sul nostro computer di lavoro

possiamo proseguire con la selezione di :





APPENDICE 3

Modelli

Richiesta nuovo certificato per Stazione Appaltante

Modello richiesta nuovo certificato S.A.

Carta intestata della Stazione Appaltante richiedente

(La richiesta deve essere trasmessa all'indirizzo di posta elettronica assistenza.antimafia@interno.it)

Richiesta di emissione nuovo certificato digitale per accesso alla Banca Dati Nazionale unica per la documentazione Antimafia (B.D.N.A.)

Il/La sottoscritto/a _____
in qualità di responsabile dell'Amministrazione _____
Struttura di riferimento _____
Codice Fiscale della Struttura di riferimento _____
Ufficio _____
Indirizzo _____
Cap _____
Posta Elettronica Certificata (PEC) _____

CHIEDE

sotto la propria personale responsabilità l'abilitazione alla richiesta di un nuovo certificato digitale B.D.N.A per il seguente personale:

TOTALE NUMERO UTENTI (IN CIFRE E IN LETTERE): _____

COGNOME	NOME	LUOGO DI NASCITA	DATA DI NASCITA	COD. FISCALE	NUMERO UTENZA TEL. MOBILE

Luogo e data _____

Firma del Responsabile



Richiesta nuovo certificato per Prefettura- U.T.G.

Modello richiesta nuovo certificato U.T.G.

(La richiesta deve essere trasmessa all'indirizzo di posta elettronica assistenza.antimafia@interno.it)

Richiesta di emissione nuovo certificato digitale per accesso alla Banca Dati Nazionale unica per la documentazione Antimafia (B.D.N.A.)

Il/La sottoscritto/a _____

in qualità di responsabile dell'Ufficio Antimafia della Prefettura-UTG di _____

CHIEDE

sotto la propria personale responsabilità l'abilitazione alla richiesta di un nuovo certificato digitale B.D.N.A per il seguente personale:

COGNOME	NOME	DPP

Luogo e data _____

Firma del Responsabile dell'Ufficio Antimafia



Richiesta riattivazione utenza



Dipartimento Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie
Divisione Centrale Risorse Finanziarie e Strumentali
Ufficio IV - Innovazione tecnologica per l'amministrazione generale

MODULO RICHIESTA RIATTIVAZIONE UTENZA BDNA

Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome Cognome Dirigente	

Firma del Dirigente

.....



Richiesta sblocco/reset password smart card



Dipartimento Politiche del Personale dell'Amministrazione Civile e per le Risorse Strumentali e Finanziarie
Direzione Centrale Risorse Finanziarie e Strumentali
Ufficio IV - Innovazione Identificata per l'Amministrazione generale

**MODULO RICHIESTA SBLOCCO/RESET
PASSWORD SMART CARD BDNA**

Data	
Nome Cognome	
Utenza/Username/Account	
Email	
Ente Appartenenza	
Nome e Cognome Dirigente	
Tipo di operazione <i>(scegliere SOLO una operazione)</i>	Sblocco Password Smart card <input type="checkbox"/> Password Smart card dimenticata <input type="checkbox"/>

Firma del Dirigente

.....