

WPanel

Manuale configurazione client per VPS Zero Trust Desktop e Smart Card

Versione 1.0

11 dicembre 2023

Copyright © 2023 WPanel – Tutti i diritti riservati

Indice

1. Guida all'acquisto	4
1.1 Sicurezza avanzata nella gestione dei VPS acquistati.....	5
2. Accesso al desktop via browser (solo serie Zero Trust Desktop)	6
2.1 Visualizzazione del desktop a tutto schermo	9
2.2 Upload di un file tramite browser web	10
2.3 Download di un file tramite browser web.....	13
2.4 Cambio password utente Administrator da WPanel.....	17
3. Creazione del primo certificato di accesso al VPS	18
3.1 Creazione di un certificato all'interno di un TPM.....	19
3.2 Creazione di un certificato per smart card o token USB	36
4. Pannello servizi del VPS	38
5. Pannello funzioni speciali del VPS	39
6. Configurazione del proprio PC tramite procedura automatica	40
7. Primo accesso al VPS (VPN, desktop remoto e condivisioni di rete)	45
7.1 Apertura del tunnel VPN	45
7.2 Connessione al Desktop Remoto.....	47
7.3 Accesso alle condivisioni di rete.....	49
8. Cifratura della partizione dati con BitLocker	50
8.1 Cifratura della partizione dati con BitLocker tramite dispositivo sicuro	50
8.2 Blocco dell'accesso alla partizione cifrata con BitLocker	55
8.3 Nuovo accesso alla partizione cifrata con BitLocker	57
8.4 Aggiunta di una seconda smart card per l'accesso alla partizione BitLocker.....	59
9. Creazione di una nuova condivisione di rete	62
10. Rimozione di una condivisione di rete	65
11. Elenco dei certificati emessi e creazione di un nuovo certificato	68
12. Creazione manuale della Virtual Smart Card per TPM	70

13. Cambio del PIN e riattivazione del dispositivo sicuro tramite PUK	73
14. Creazione manuale dei certificati	75
15. Mappatura degli UPN agli utenti del VPS	78
16. Configurazione manuale per Windows 11	84
16.1 Configurazione autenticazione Kerberos	84
16.2 Installazione del certificato CA	85
16.3 Creazione della connessione VPN	90
17. Configurazione manuale per Windows 10	97
17.1 Note preliminari	97
17.2 Creazione della connessione VPN	98
18. Accesso al VPS con una password	104
19. Disabilitazione accesso sicuro al sito WPanel	106
20. Accesso al sito WPanel in caso di smarrimento del dispositivo sicuro	108
21. Revoca dei certificati	110
22. Estensione della partizione BitLocker dopo un upgrade	111

1. Guida all'acquisto

Il presente manuale si riferisce ai VPS delle linee Zero Trust Desktop e Smart Card gestite dal sito WPanel del vostro fornitore.

- I VPS della **linea Smart Card** permettono l'accesso al desktop remoto e ad alle risorse in modalità passwordless (senza password) attraverso una smart card o una Smart Card Virtuale Microsoft (solo per PC dotati di dispositivo hardware TPM). **Si ricorda che il dispositivo TPM è presente su tutti i PC con sistema operativo Windows 11.**

I VPS della linea Smart Card godono delle seguenti caratteristiche:

- **Accesso con VPN:** per migliorarne la sicurezza, i VPS della linea Smart Card sono protetti da una VPN di tipo SSTP con autenticazione passwordless, già integrata in tutti i sistemi operativi Microsoft;
- **Crittografia con BitLocker:** in fase di acquisto è possibile optare per la creazione di una seconda partizione disco da dedicare alla memorizzazione dei dati. È possibile cifrare tale partizione attraverso la tecnologia Microsoft BitLocker (già integrata nel VPS) utilizzando direttamente la smart card. In questo modo il processo di crittografia sarà di gran lunga più affidabile rispetto all'utilizzo delle tradizionali password e l'accesso ai dati sarà garantito al solo possessore della smart card.
- I VPS della linea **Zero Trust Desktop** includono tutte le caratteristiche della linea Smart Card con l'aggiunta dell'accesso al desktop via browser web, quindi in precarie condizioni di sicurezza (zero trust security). L'accesso via browser avviene con nome utente e password quindi può essere effettuato con i dispositivi mobile (smartphone o tablet).

I VPS della linea Zero Trust Desktop godono inoltre delle seguenti caratteristiche:

- **Utilizzo del VPS anche in assenza di smart card:** in fase di acquisto è possibile configurare i VPS della linea Zero Trust Desktop per l'accesso con la classica combinazione nome utente e password, quindi senza l'utilizzo di una smart card, cliccando semplicemente il tasto di colore nero **Non usare i certificati**:

Prodotto	Taglia	Canone	vCPU	RAM (GB)	Storage (GB)
<input checked="" type="radio"/> WINZTD/WP-WNAT.S	Size S	€ 9,90	4	8	50
<input type="radio"/> WINZTD/WP-WNAT.M	Size M	€ 14,90	4	8	100
<input type="radio"/> WINZTD/WP-WNAT.L	Size L	€ 19,90	6	12	200

Non è ancora stato emesso alcun certificato per smart card

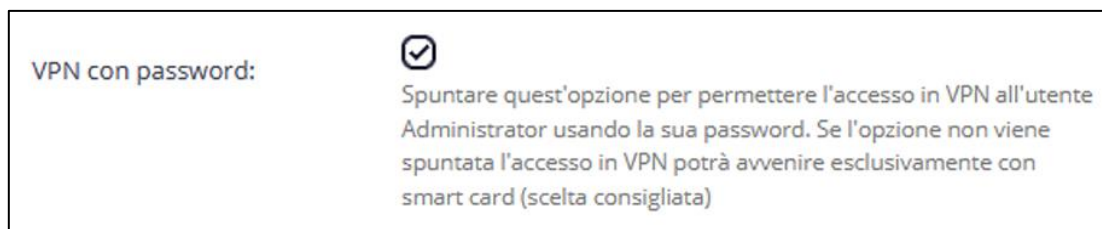
Non è ancora stato emesso alcun certificato per smart card. Per poter accedere (ed acquistare) un VPS della serie "Smart Card" è necessario inserire nella smart card il primo certificato.

 Manuale PKI
 + Crea il primo certificato per la smart card
 Non usare i certificati



- **Accesso VPN con nome utente e password:** in fase di acquisto è possibile configurare i VPS della linea Zero Trust Desktop per consentire l'accesso in VPN anche con la modalità nome utente e password. Tale modalità non esclude l'accesso VPN tramite smart card.

ATTENZIONE! Se il VPS è stato acquistato cliccando il tasto nero **Non usare i certificati** allora questa opzione è impostata automaticamente e non è deselezionabile dall'acquirente.



1.1 Sicurezza avanzata nella gestione dei VPS acquistati

Il sito WPanel supporta l'accesso tramite smart card o Smart Card Virtuale Microsoft per rendere sicura la gestione dei VPS acquistati:



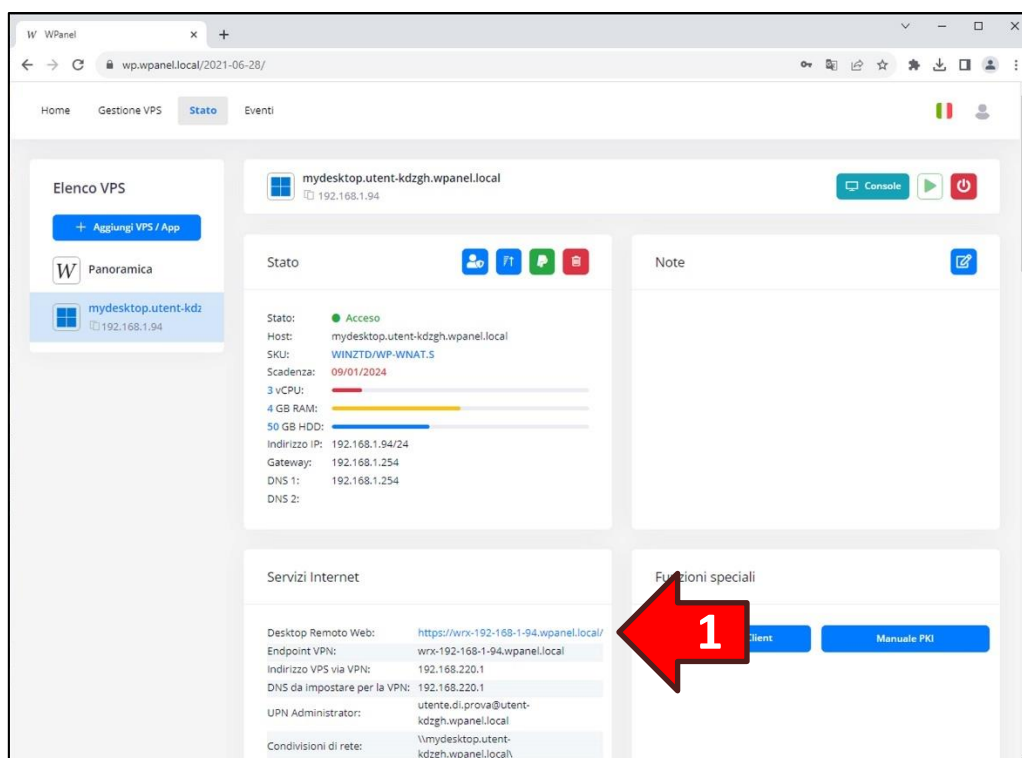
ATTENZIONE! In caso di smarrimento della smart card è possibile ripristinare l'accesso solo attraverso i codici contenuti nel **Foglio per il recupero dell'account** inviato in fase di registrazione cliente.

ATTENZIONE! Con il browser Firefox non è possibile accedere al sito WPanel tramite Smart Card Virtuale Microsoft. Invece il browser Firefox supporta l'accesso con smart card fisica.

2. Accesso al desktop via browser (solo serie Zero Trust Desktop)

I VPS della serie Zero Trust Desktop permettono l'accesso al desktop anche tramite browser web. Sempre tramite browser è possibile inserire o prelevare i vari file verso e dal VPS.

L'indirizzo web (URL) per accedere al desktop è indicato sia nel sito WPanel del vostro fornitore nella sezione **Servizi Internet (1)** che nell'email contenente le credenziali del VPS (2).



Modalità di accesso al VPS mydesktop.utent-kdzgh.wpanel.local

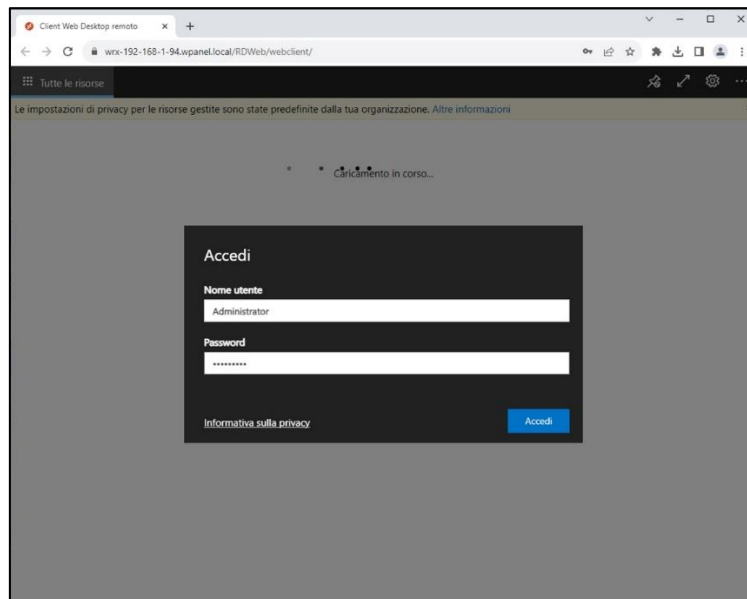
La informiamo che il VPS in oggetto è stato attivato con il sistema operativo Windows ed è già stato preconfigurato.

Può accedere al desktop remoto del suo VPS attraverso un qualunque browser web utilizzando le seguenti informazioni:

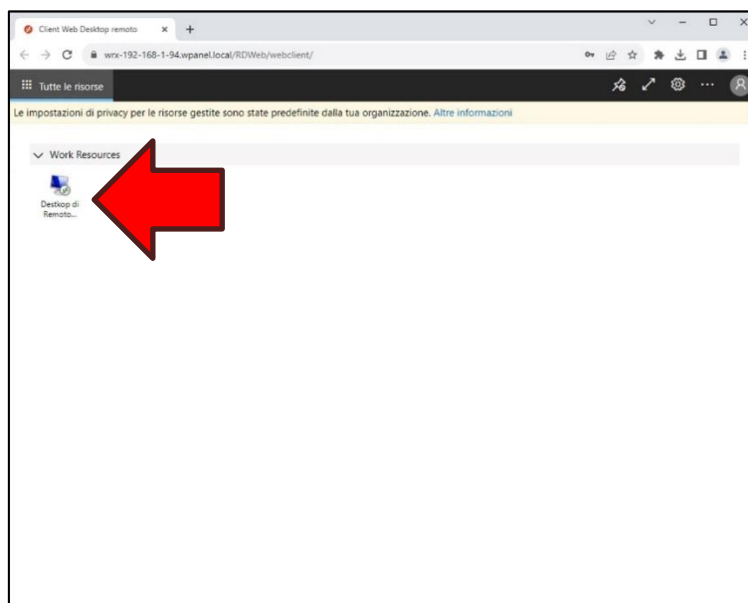
- Indirizzo web desktop remoto: <https://wrx-192-168-1-97.wpanel.local:22071/>
- Nome utente: **Administrator**
- Password: **MCUb77iuRE,,H2LV**

2

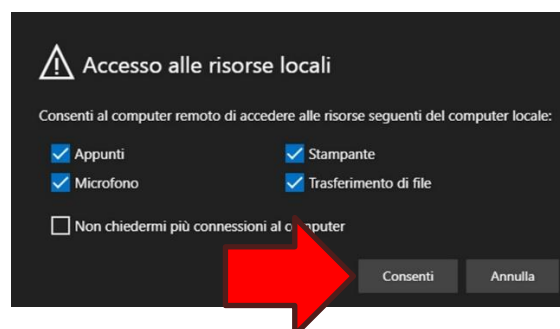
Una volta visualizzata la pagina web di accesso inserire le credenziali e cliccare sul tasto **Accedi**:



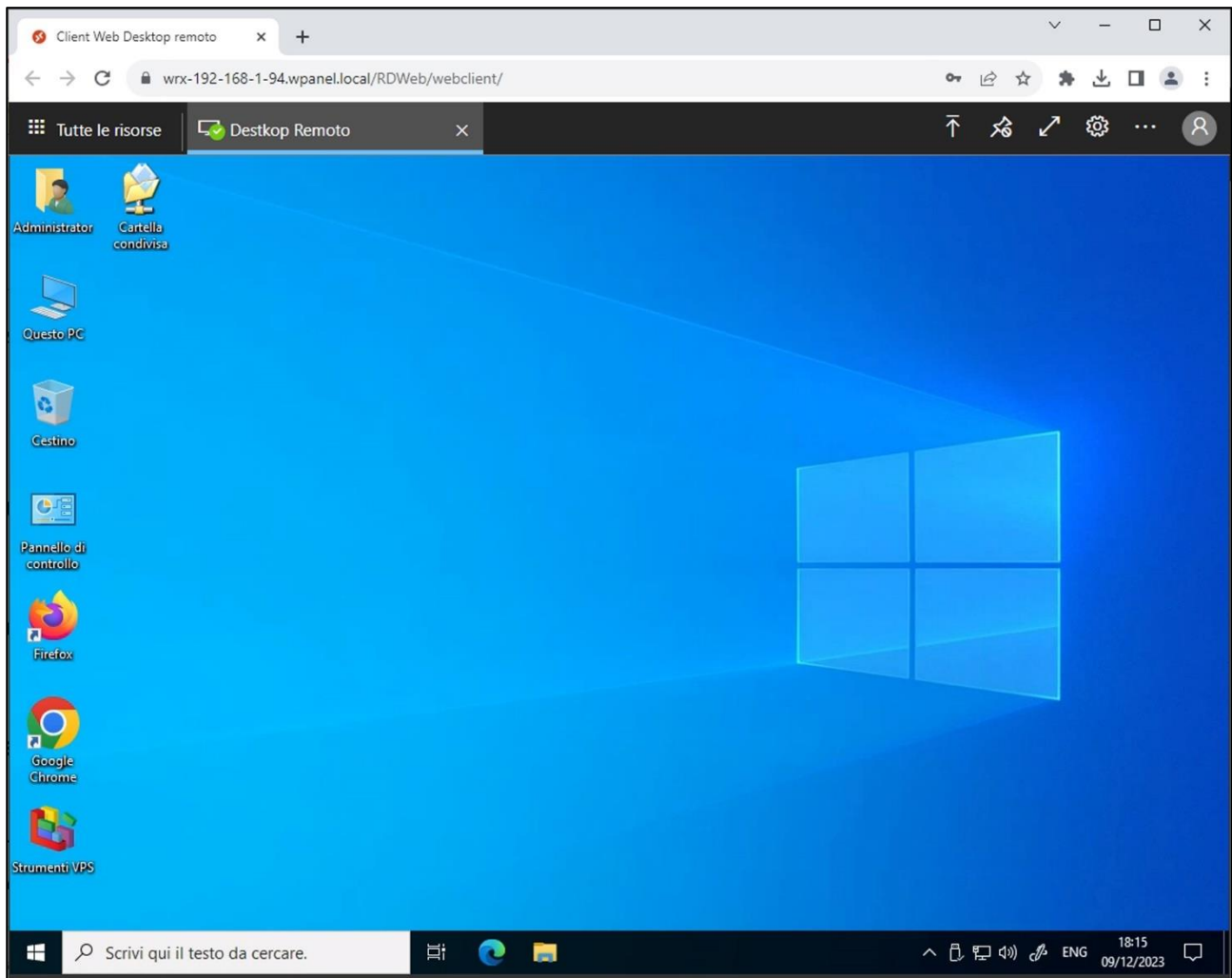
Successivamente dalla sezione *Work Resources* cliccare sull'icona **Desktop di Remoto...**:



Apparirà il riquadro con le opzioni di trasporto delle risorse locali sul VPS. **Tale operazione non costituisce alcun problema di sicurezza né per il PC che si sta utilizzando e né per il VPS**, quindi cliccare il tasto **Consenti**.

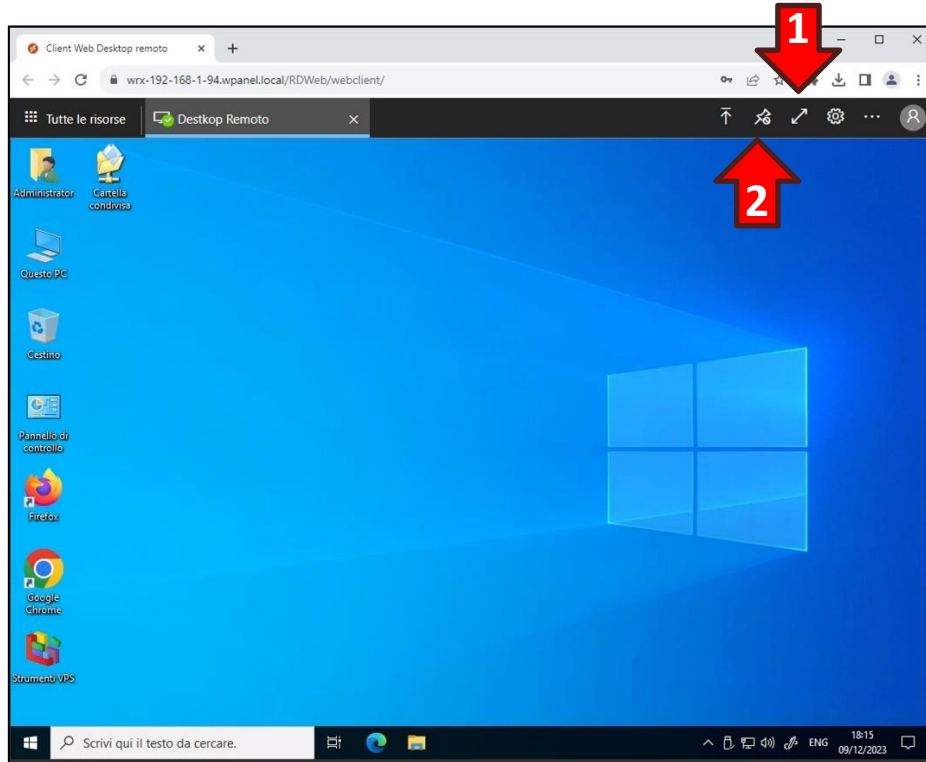


Verrà quindi visualizzato il desktop del VPS:

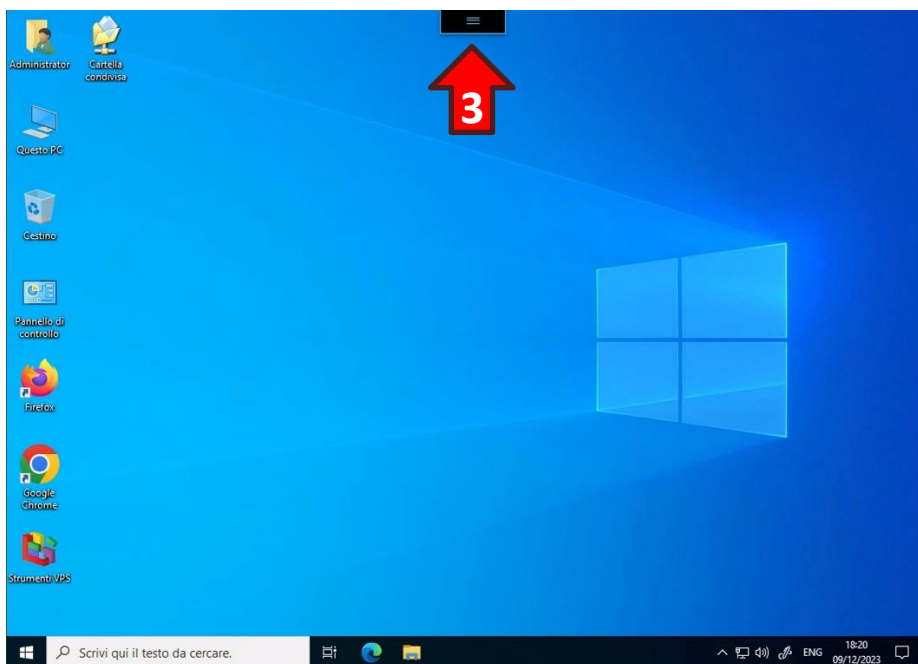


2.1 Visualizzazione del desktop a tutto schermo

Dalla *dashboard* del desktop del VPS cliccare prima il **tasto delle due frecce contrapposte (1)** e poi il **tasto della puntina metallica (2)**:



Il desktop del VPS si adatterà automaticamente alle dimensioni del monitor del PC client. In alto al centro comparirà una **linguetta (3)** per visualizzare nuovamente la dashboard del desktop remoto.

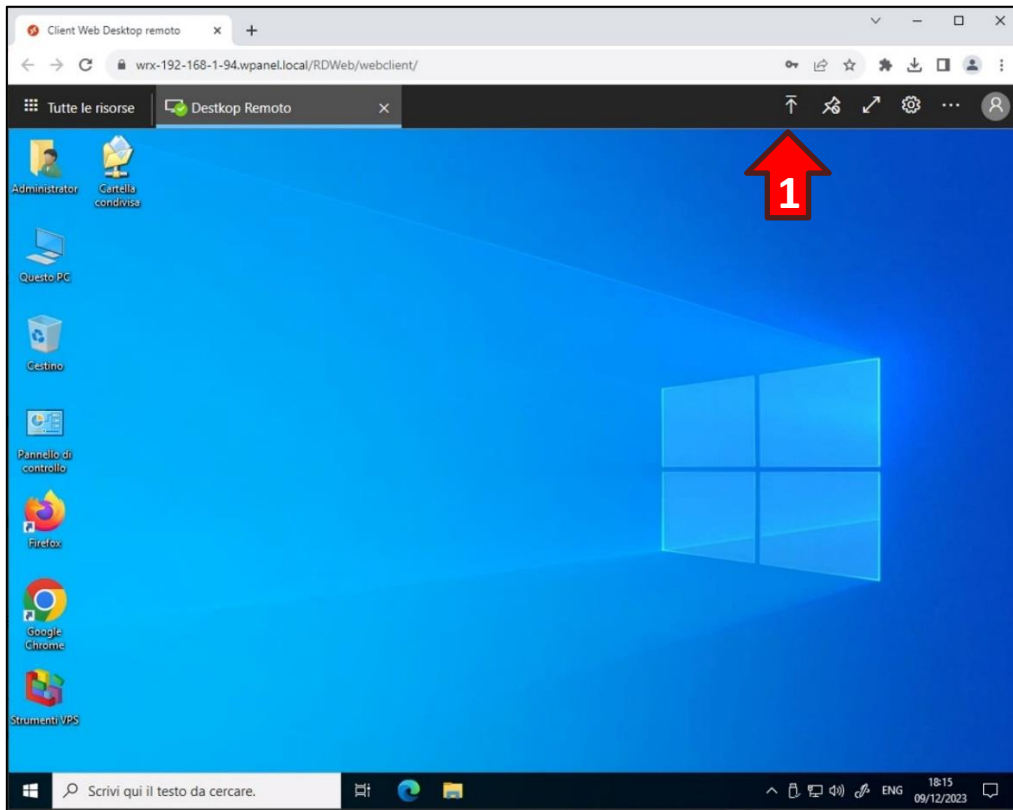


ATTENZIONE! Per uscire dalla modalità a schermo intero premere il tasto **ESC** della tastiera oppure cliccare sulla linguetta e successivamente cliccare sull'**icona delle due frecce contrapposte**.

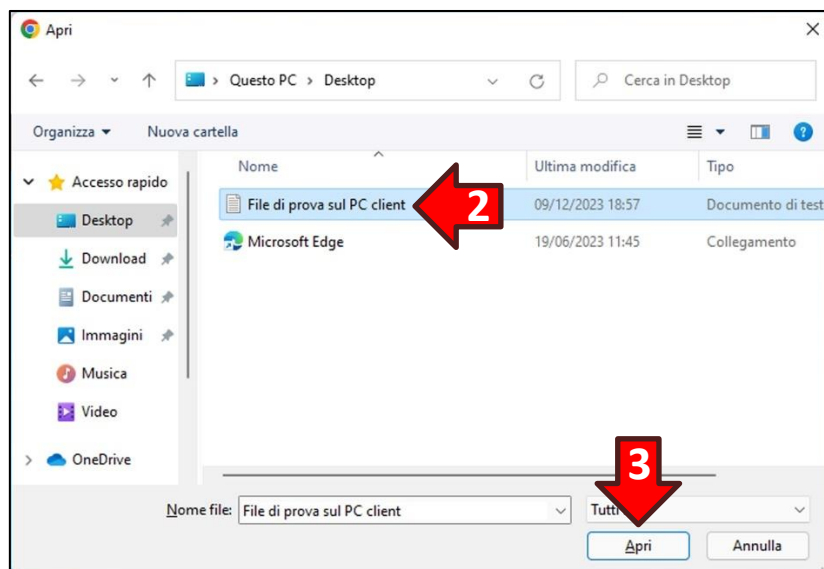
2.2 Upload di un file tramite browser web

ATTENZIONE! La maggior parte dei browser supporta il caricamento dei file attraverso la funzione di trascinamento. Identificare un file di prova all'interno del proprio PC e provare a trascinarlo all'interno della finestra del browser per verificare se è possibile utilizzare questa modalità di upload. In tutti i casi i file caricati finiranno nella cartella **Caricamenti** come indicato di seguito.

Dalla *dashboard* del desktop del VPS cliccare il **tasto della freccia rivolta verso l'alto (1)**:



Si aprirà la *finestra di selezione file*. Scegliere il **file da caricare dal proprio PC (2)** e cliccare il **tasto Apri (3)**:

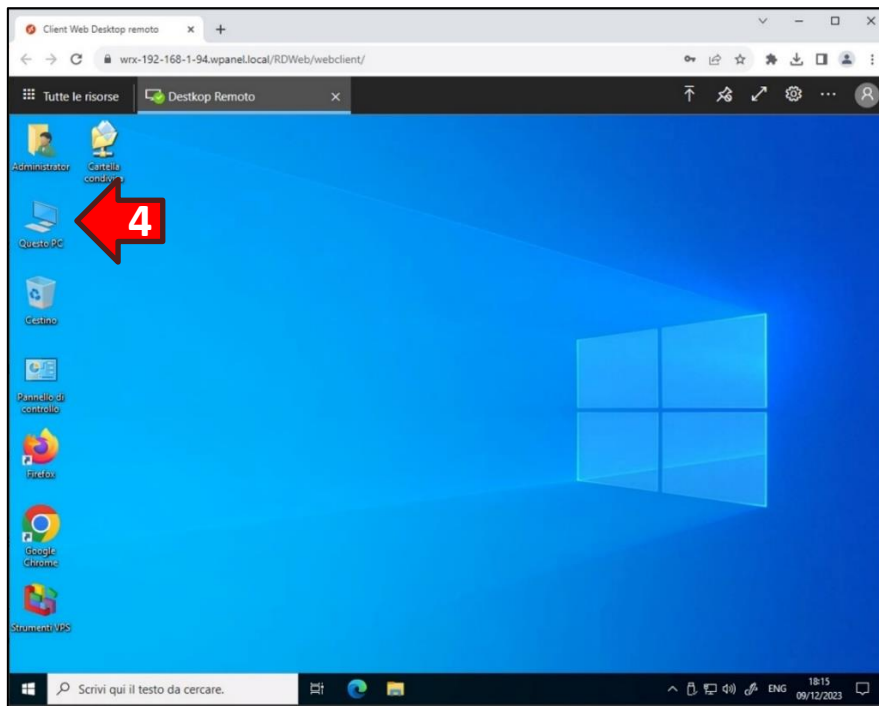


ATTENZIONE! I file caricati non compaiono sul desktop del VPS.

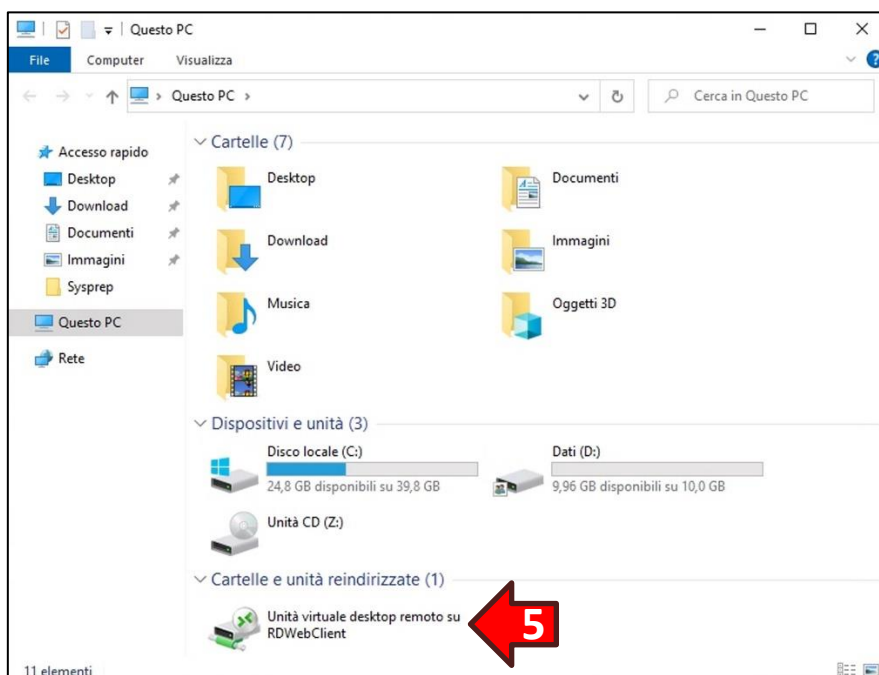
Per ragioni di sicurezza i file caricati vengono posizionati in una cartella speciale accessibile al seguente percorso:

\\tsclient\Unità virtuale desktop remoto\Caricamenti

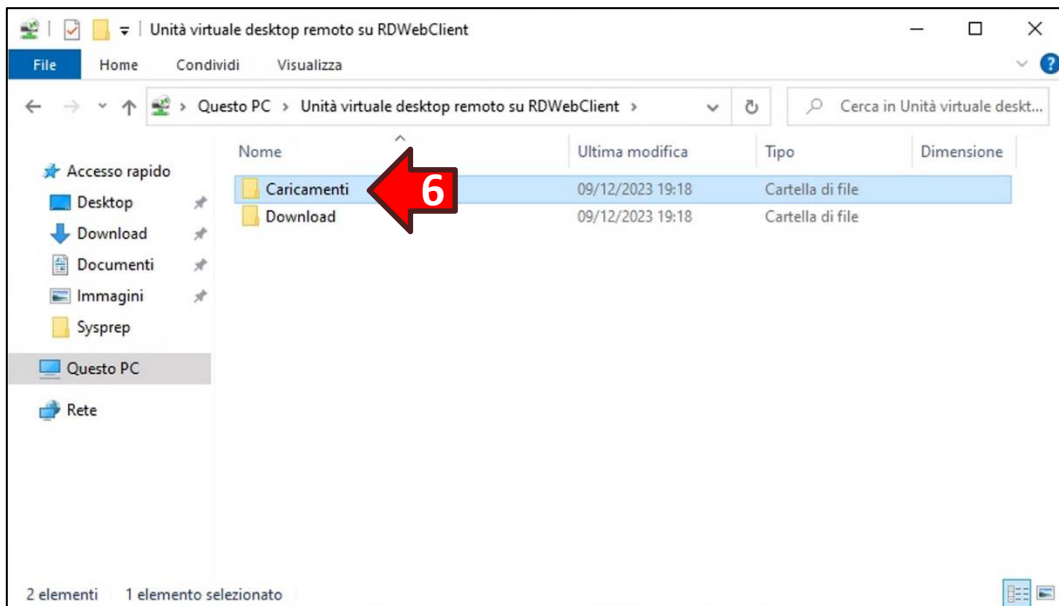
In alternativa è possibile accedere alla cartella attraverso l'icona **Questo PC (4)**, posizionata sul desktop del VPS:



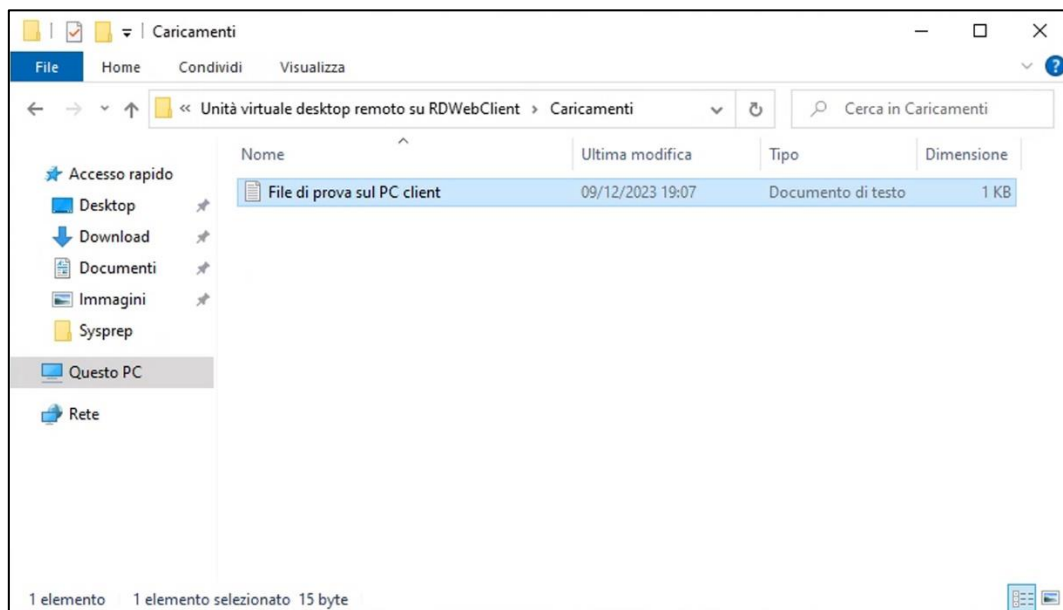
Cliccare sull'icona **Unità virtuale desktop remoto su RDWebClient (5)**:



Cliccare poi sulla cartella **Caricamenti (6)**:



Infine spostare il file caricato nella cartella desiderata all'interno del VPS:

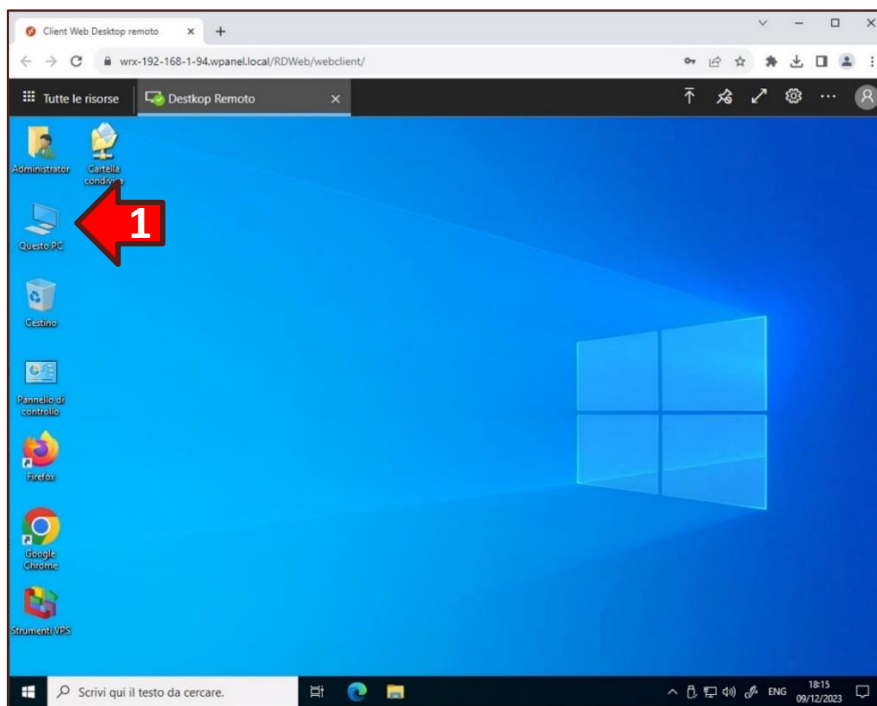


2.3 Download di un file tramite browser web

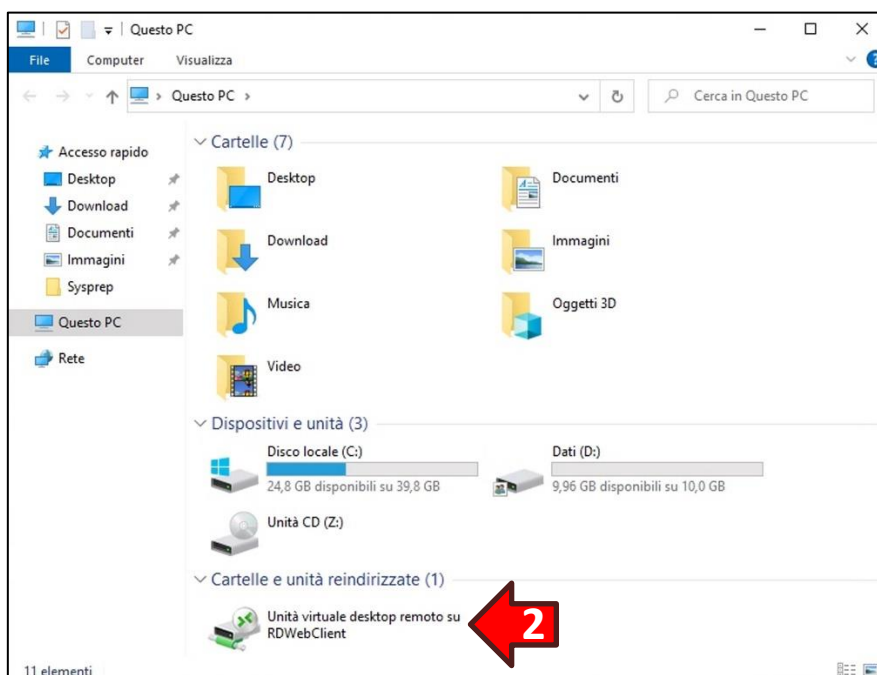
I file che si desidera scaricare dal VPS devono essere copiati in una cartella speciale accessibile al seguente percorso:

\\tsclient\Unità virtuale desktop remoto\Download

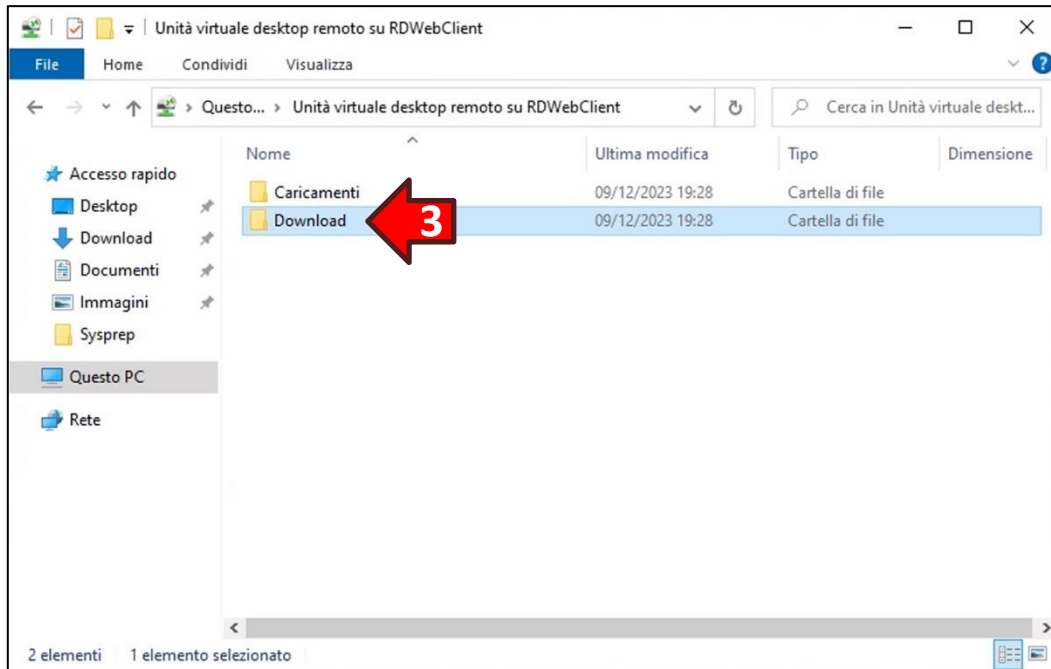
In alternativa è possibile accedere alla cartella attraverso l'icona **Questo PC (1)**, posizionata sul desktop del VPS:



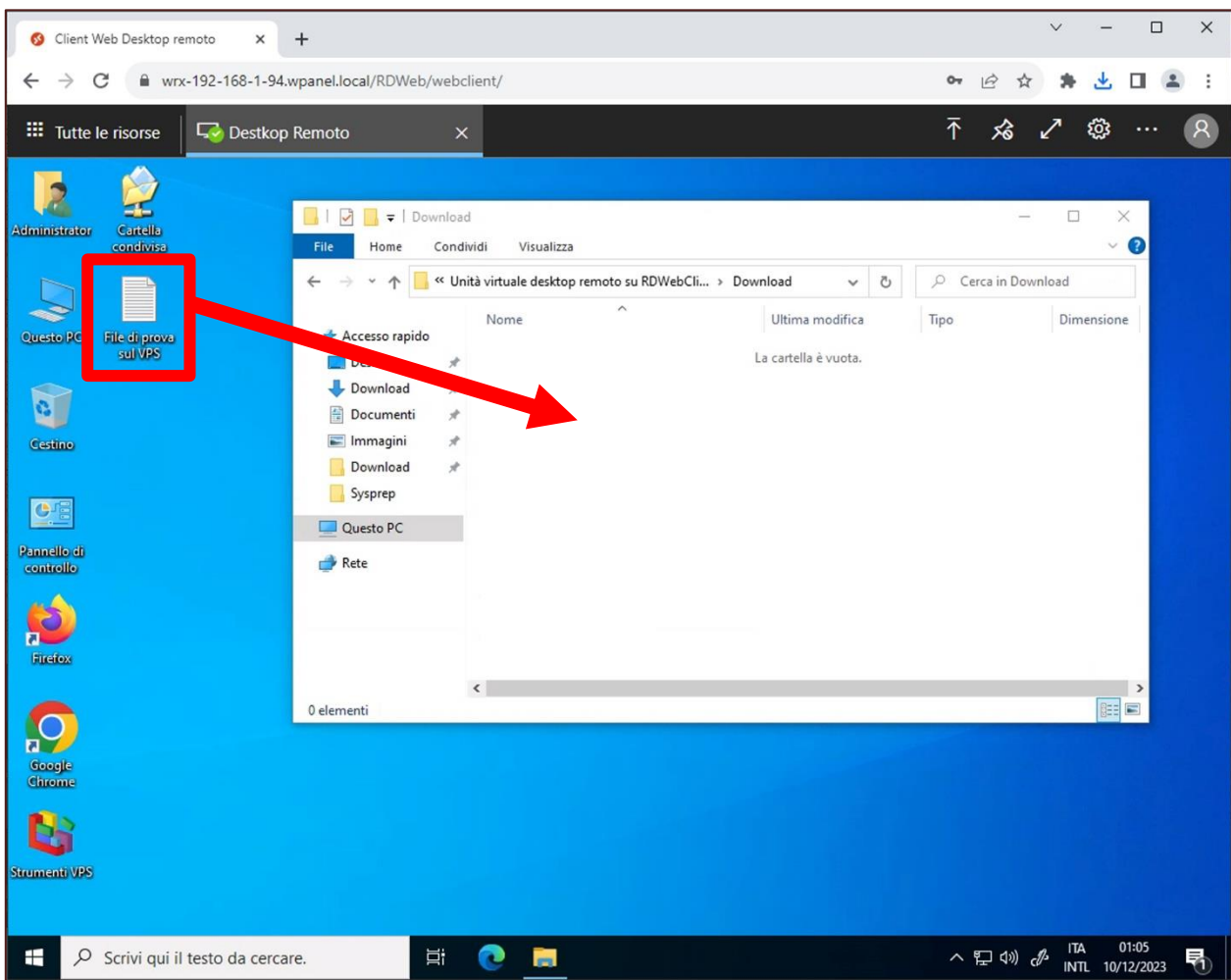
Cliccare sull'icona **Unità virtuale desktop remoto su RDWebClient (2)**:



Cliccare poi sulla cartella **Download (3)**:

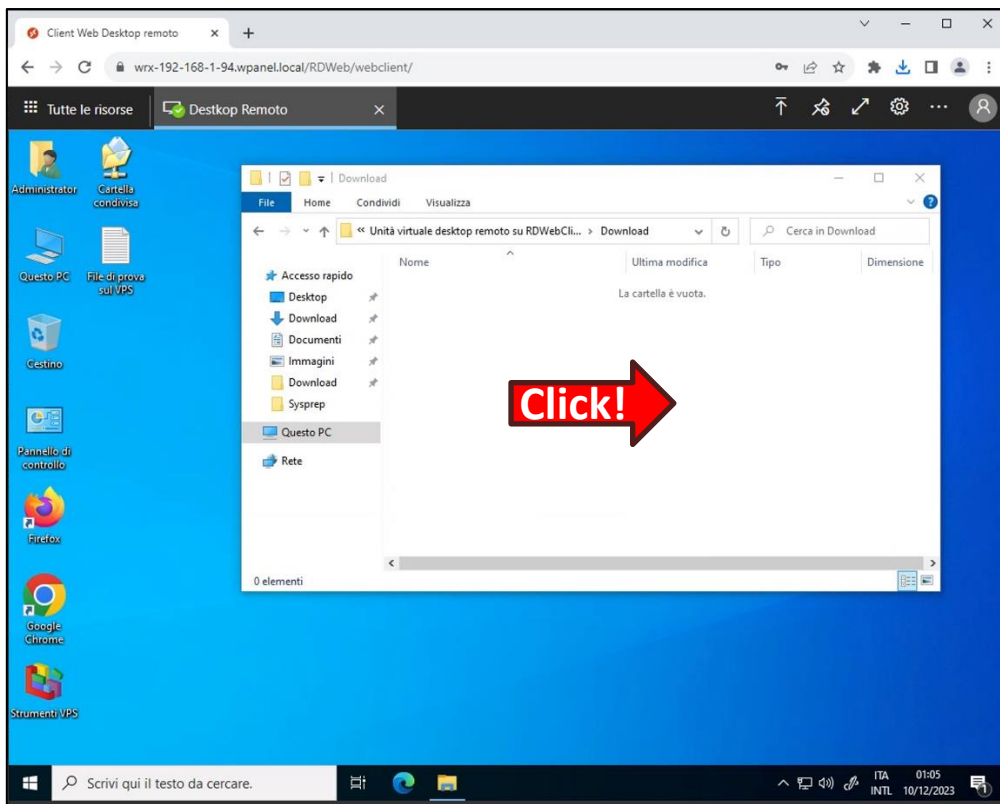


Ora **trascinare** il file o i file desiderati all'interno della cartella *Download*:

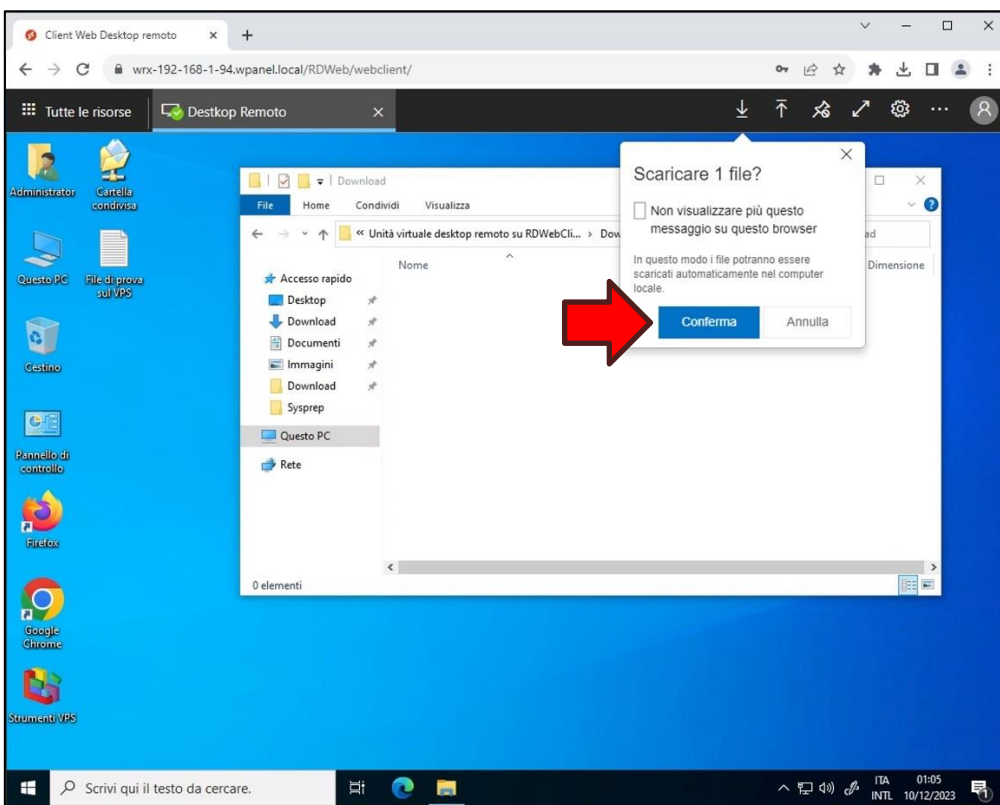


ATTENZIONE! Terminato il trascinamento cliccare all'interno della finestra **Download**.

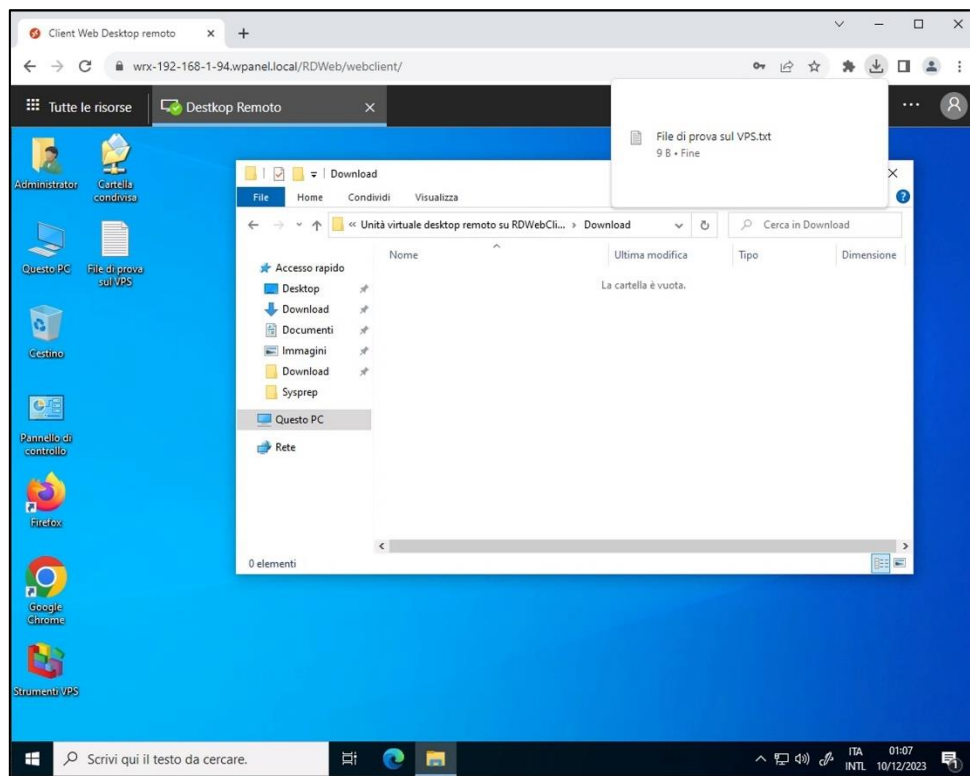
ATTENZIONE! Il file trascinato potrebbe non comparire nella finestra della cartella **Download**.



Cliccare il tasto **Conferma** nella richiesta di download del file:

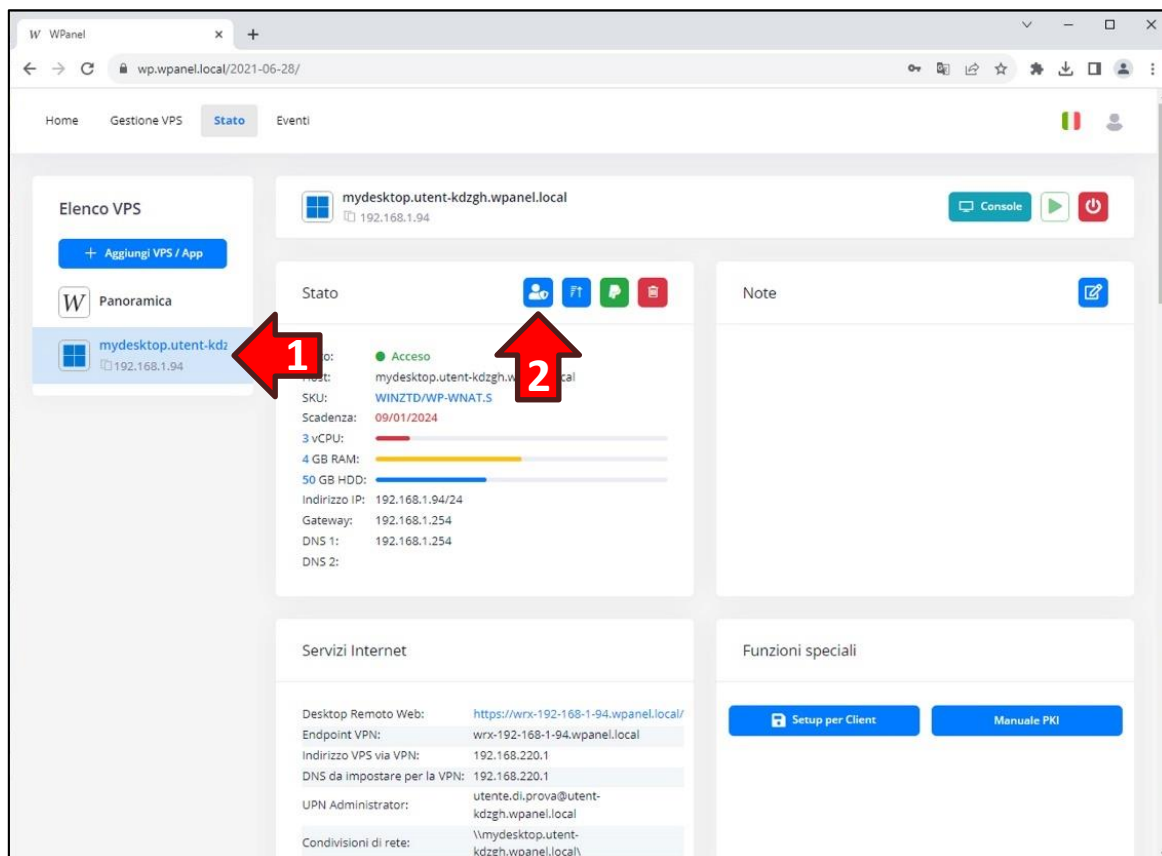


Successivamente il file verrà scaricato all'interno del proprio PC:

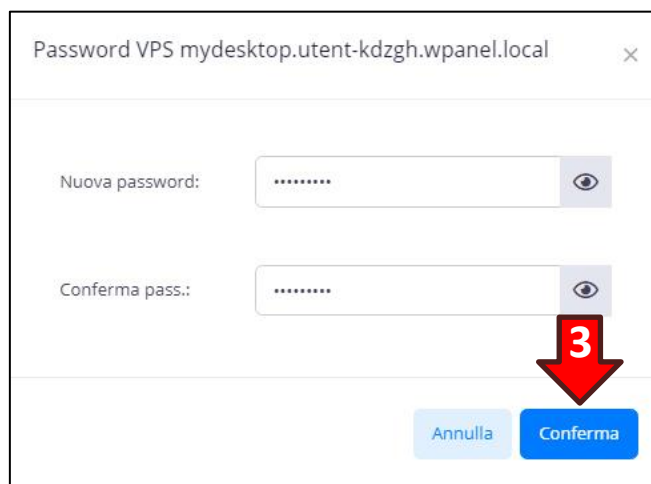


2.4 Cambio password utente Administrator da WPanel

Per creare una password per l'utente Administrator accedere al sito WPanel del vostro fornitore, poi entrare nello **stato del VPS (1)** e dal *Pannello stato* cliccare il tasto con l'**icona dell'utente con lo scudo (2)**:



Impostare la password nel pannello *Password VPS* e confermare l'operazione cliccando il tasto **Conferma (3)**:



ATTENZIONE! La password deve avere una lunghezza minima di 8 caratteri e deve contenere almeno una lettera minuscola, almeno una lettera maiuscola, almeno un numero e almeno un simbolo.

3. Creazione del primo certificato di accesso al VPS

I VPS della linea Smart Card sono accessibili esclusivamente tramite dispositivo sicuro (smart card, token USB o TPM) per cui prima di effettuare l'acquisto è indispensabile dotarsi di uno di questi dispositivi e inserire un certificato all'interno di essi.

ATTENZIONE! Se sul proprio PC è preinstallato Windows 11 allora nel computer è presente il dispositivo sicuro TPM (Trusted Platform Module) quindi non è necessario acquistare una smart card o un token USB.

ATTENZIONE! Per massimizzare le policy di sicurezza non viene fornita alcuna password all'utente Administrator. È comunque possibile creare una password per manutenzioni straordinarie ed eliminare tale password al termine delle operazioni.

Se non è ancora stato emesso alcun certificato la procedura di acquisto ne proporrà l'emissione invitando a avviare l'apposita procedura guidata:

WPanel

wp.wpanel.local/2021-06-28/

Home Gestione VPS **Aggiungi VPS / Appliance**

Selezionare un sistema operativo o un'appliance:

- Windows Remote Experience
- Windows Server 2022
- Windows Smart Card**
- Windows SSTP VPN
- Windows OpenVPN

Selezionare un'offerta:

Prodotto	Taglia	Canone	vCPU	RAM (GB)	Storage (GB)
<input checked="" type="radio"/> WINSC/WP-WNAT,S	Size S	€ 9,90	3	4	50
<input type="radio"/> WINSC/WP-WNAT,M	Size M	€ 14,90	4	8	100
<input type="radio"/> WINSC/WP-WNAT,L	Size L	€ 19,90	6	12	200

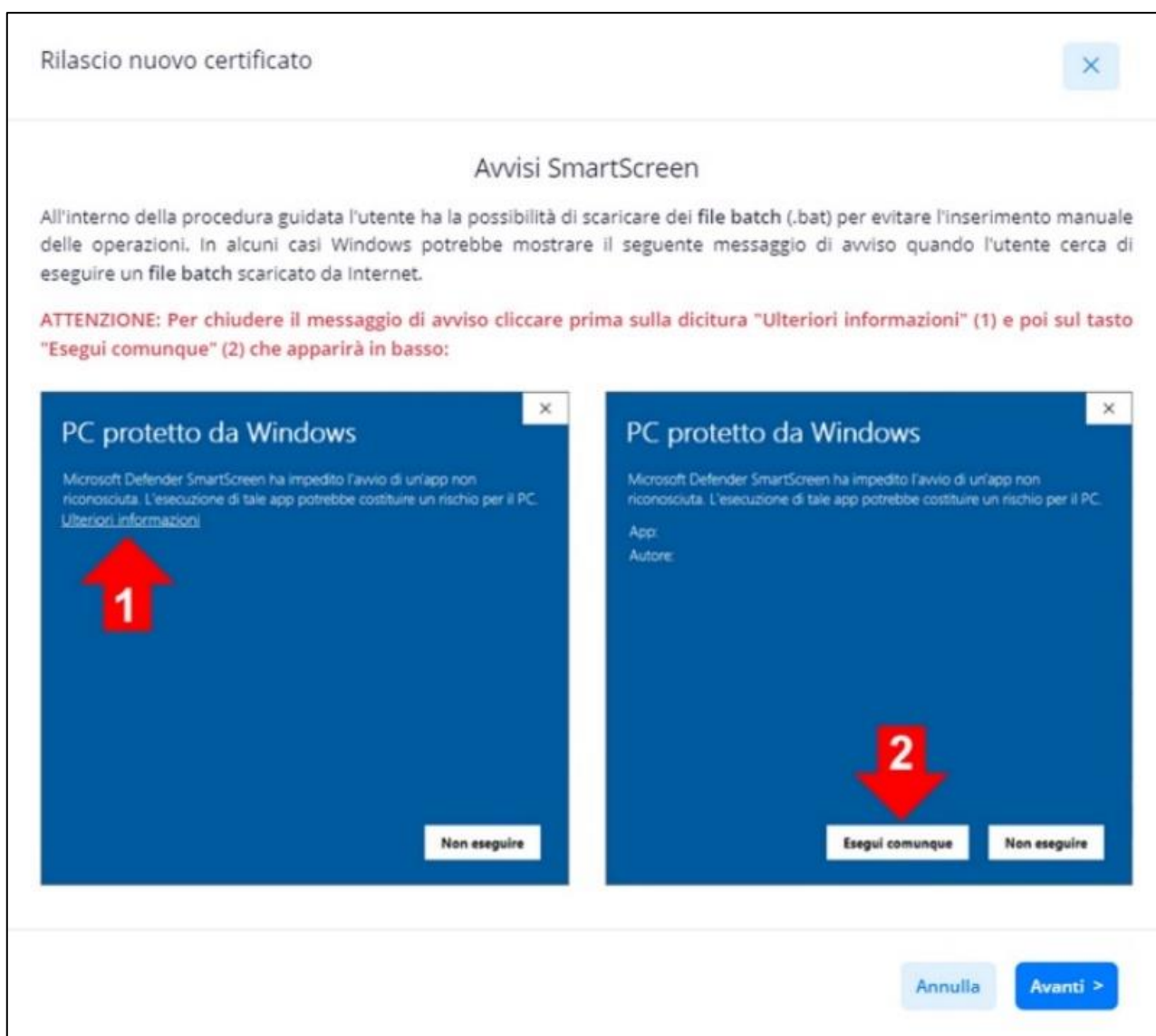
Non è ancora stato emesso alcun certificato per smart card. Per poter accedere (ed acquistare) un VPS della serie "Smart Card" è necessario inserire nella smart card il primo certificato.

[Manuale PKI](#) [+ Crea il primo certificato per la smart card](#)

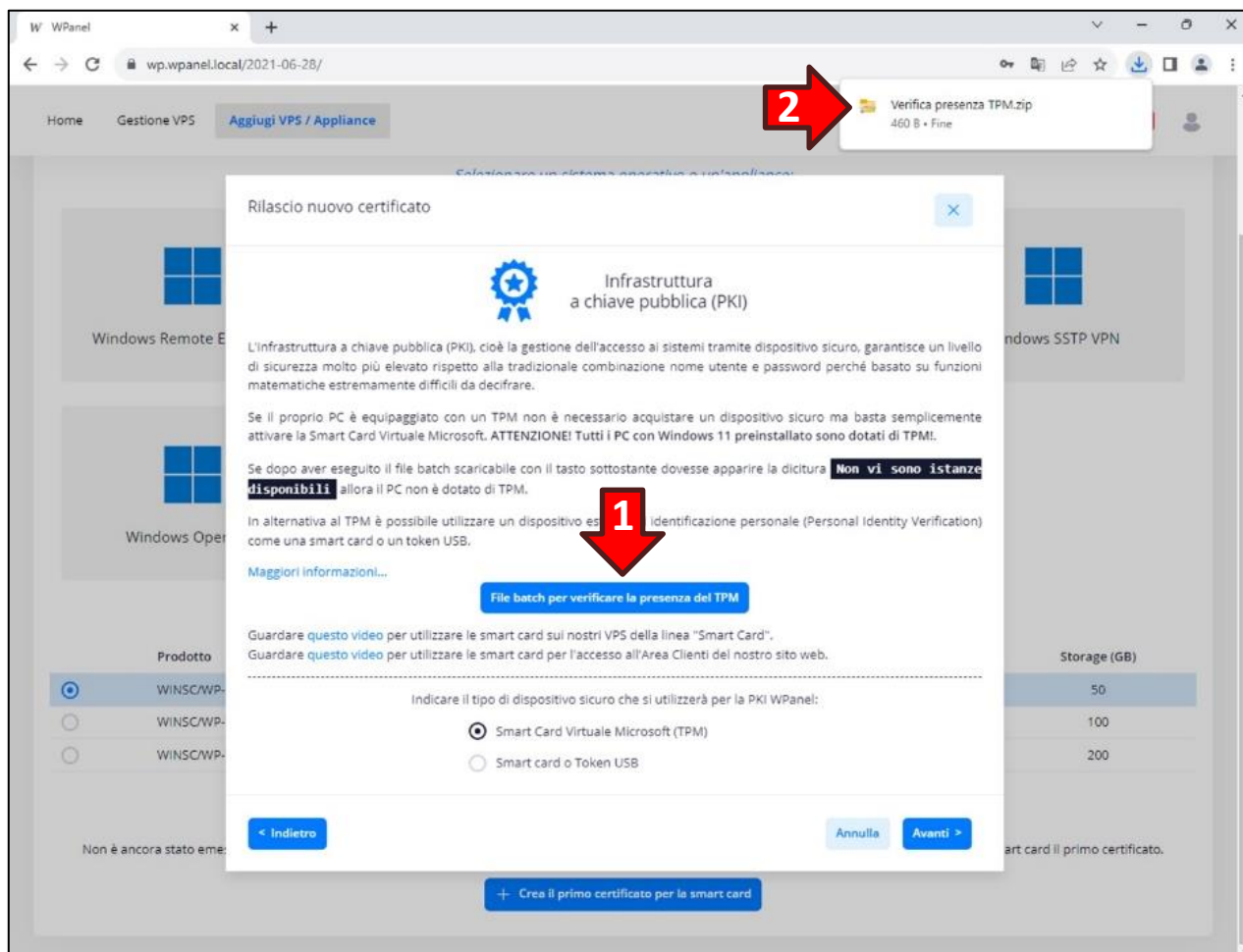
3.1 Creazione di un certificato all'interno di un TPM

La procedura guidata permetterà di scaricare degli appositi file batch, da eseguire all'interno del proprio PC, per semplificare l'emissione del certificato. È possibile che al momento dell'esecuzione di ogni file batch appaia il messaggio di avviso *SmartScreen*.

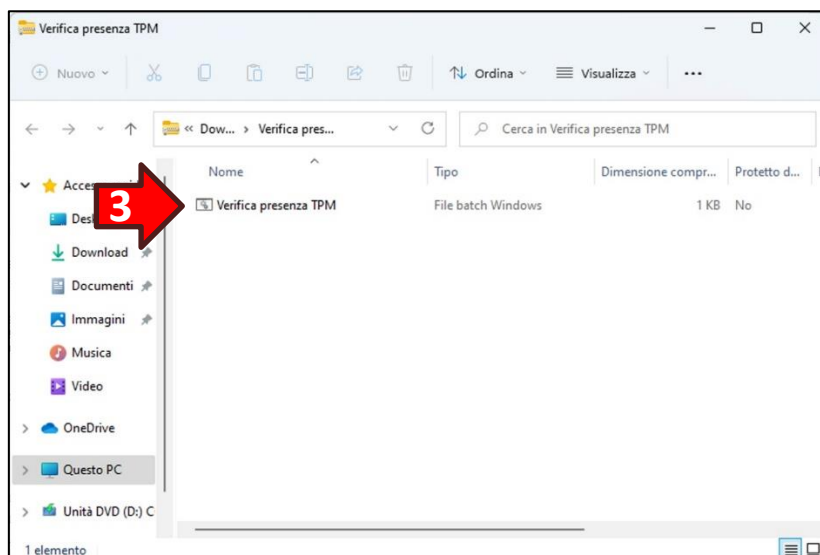
ATTENZIONE! Per superare il messaggio di avviso *SmartScreen* cliccare sulla dicitura **Ulteriori informazioni (1)** e successivamente il tasto **Esegui comunque (2)** che apparirà in basso.



La seconda pagina della procedura guidata permetterà di scegliere il tipo di dispositivo sicuro da utilizzare (TPM oppure smart card/token USB). Per accertarsi che sul proprio PC sia presente un TPM cliccare il tasto **File batch per verificare la presenza del TPM (1)**. Verrà scaricato sul PC il file **Verifica presenza TPM.zip (2)**:



Aprire il file zip e fare doppio click sul file **Verifica presenza TPM (3)**:

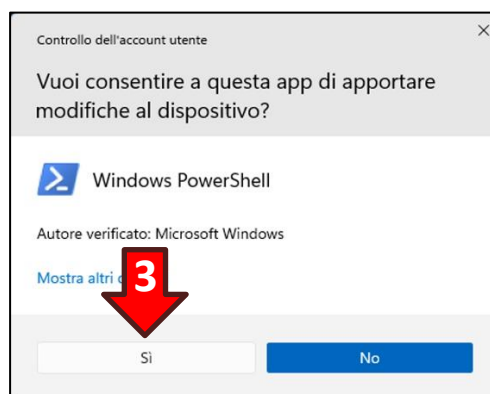


È probabile che compaia il messaggio di avviso *SmartScreen*. Per superarlo cliccare sulla dicitura **Ulteriori informazioni (1)** e poi il tasto **Esegui comunque (2)** che apparirà in basso:

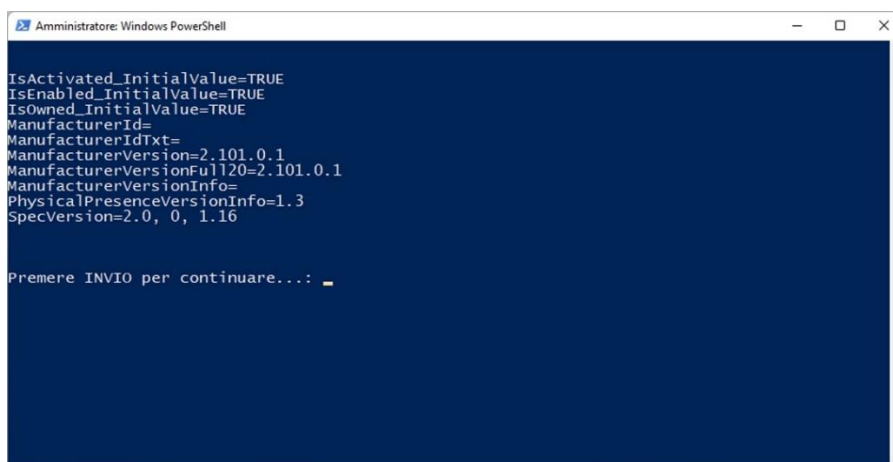


Per qualche secondo apparirà una finestra con lo sfondo nero, poi apparirà la finestra Controllo dell'account utente. Cliccare il tasto **Sì (3)**:

ATTENZIONE! La procedura di verifica della presenza del TPM non apporta alcuna modifica al PC.



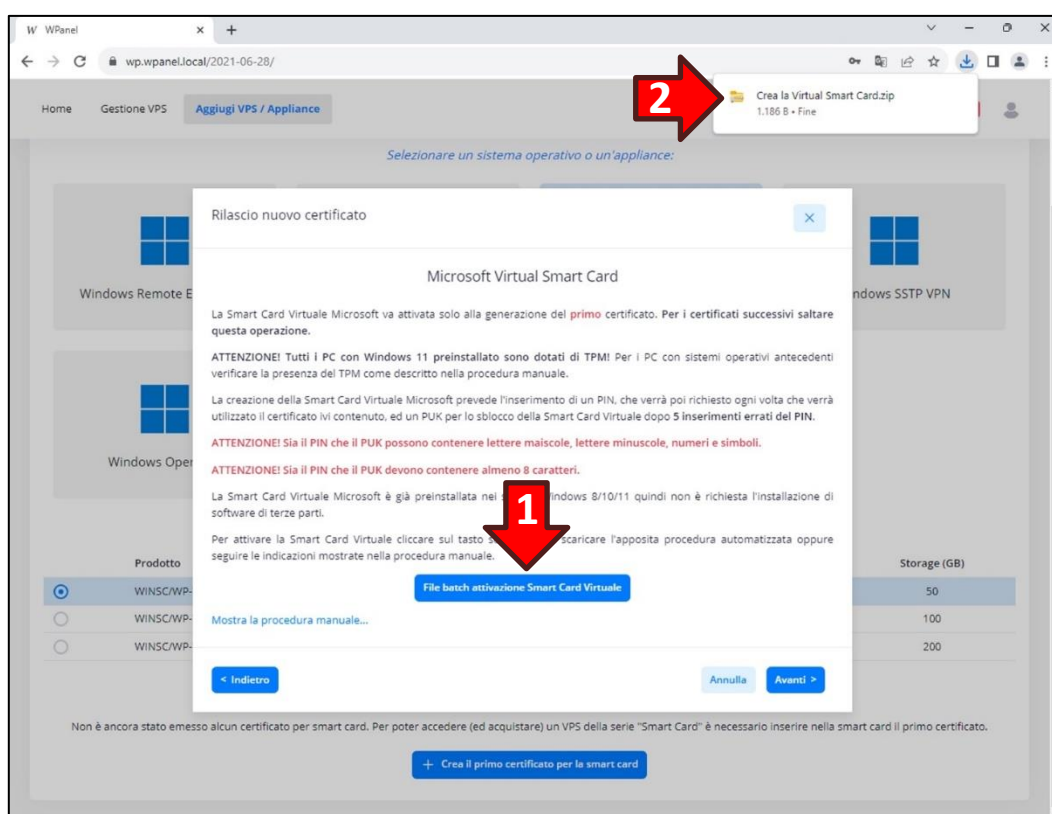
Se nella finestra di PowerShell con sfondo blu scuro appariranno una lista di valori allora il PC è dotato di TPM:



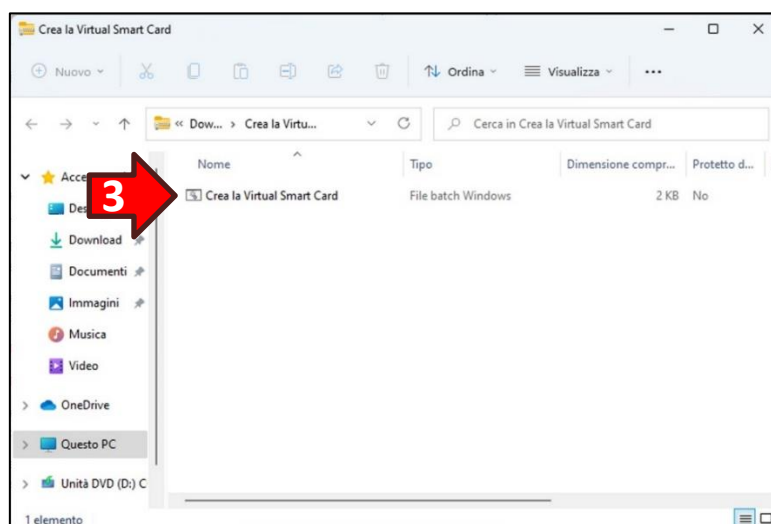
La terza pagina della procedura guidata proporrà la creazione della *Microsoft Virtual Smart Card*. Prima di inserire un certificato nel TPM del proprio PC è necessaria una procedura intermedia affinché il TPM possa emulare una smart card.

ATTENZIONE! La procedura di creazione della *Microsoft Virtual Smart Card* va eseguita una sola volta per ogni PC per cui se è già stata eseguita passare alla quarta pagina della procedura guidata.

Se la procedura non è mai stata eseguita nel PC cliccare il tasto **File batch attivazione Smart Card Virtuale (1)**. Verrà scaricato sul PC il file **Crea la Virtual Smart Card.zip (2)**:

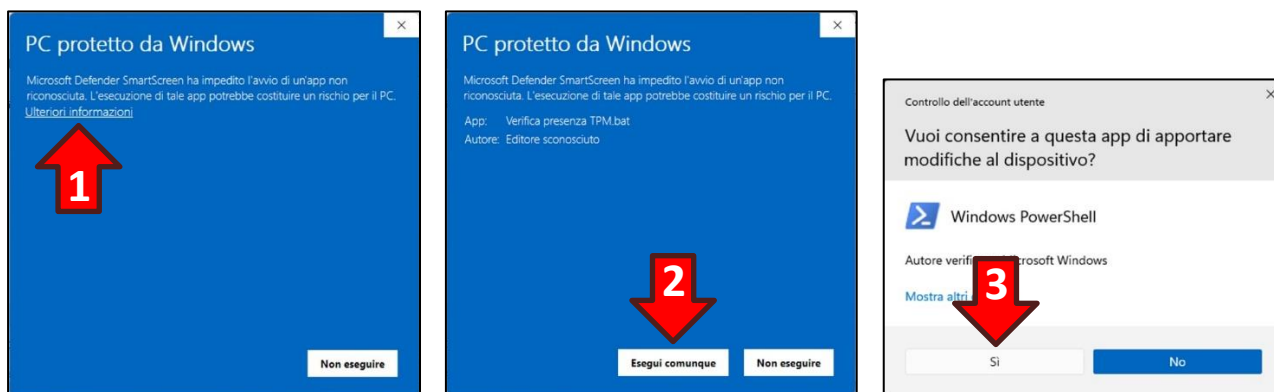


Aprire il file zip e fare doppio click sul file **Crea la Virtual Smart Card (3)**:



Se dovesse apparire il messaggio *SmartScreen* cliccare sulla dicitura **Ulteriori informazioni (1)** e poi il tasto **Esegui comunque (2)** che apparirà in basso.

Poi confermare l'apporto di modifiche al dispositivo cliccare il tasto **Sì (3)** nella finestra Controllo dell'account utente:



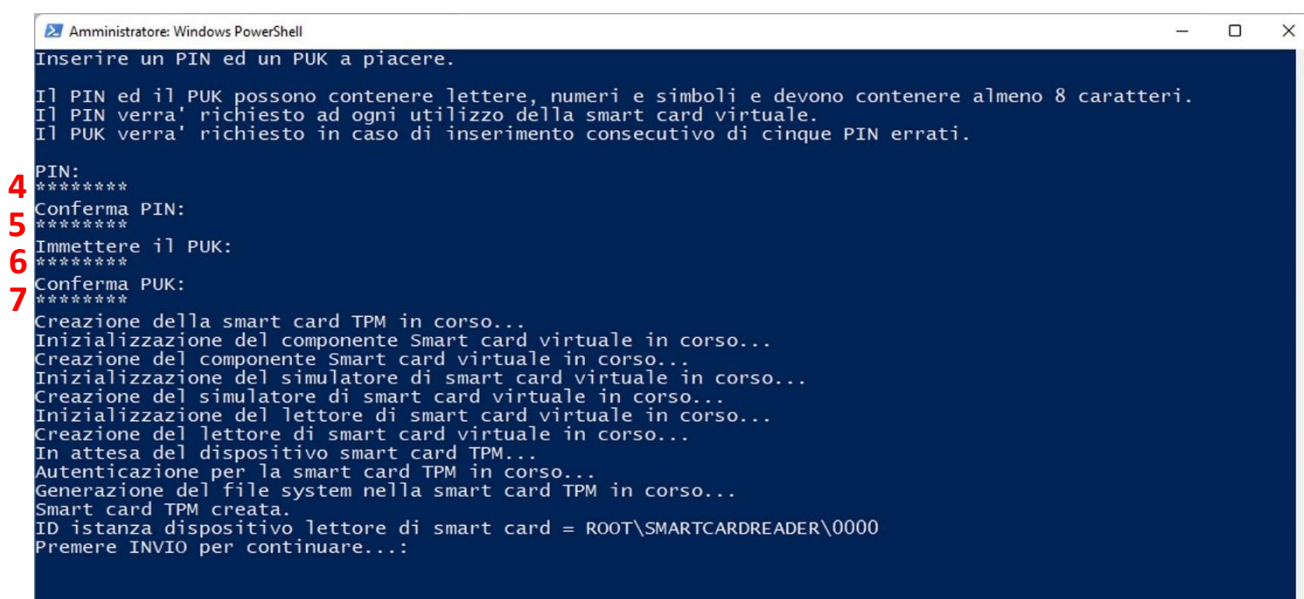
Si aprirà una finestra PowerShell in cui verrà richiesto l'inserimento sia di un **nuovo PIN (4)** che di un nuovo PUK.

Il PIN deve avere una lunghezza minima di 8 caratteri e, oltre ai numeri, può contenere anche lettere e simboli al pari di una comune password.

Il PIN deve essere digitato una seconda volta per **conferma (5)**.

Dopo il PIN verrà chiesto l'inserimento di un **nuovo PUK (6)** indispensabile per sbloccare l'utilizzo della *Smart Card Virtuale* dopo 5 inserimenti errati del PIN. Anche il PUK deve avere una lunghezza minima di 8 caratteri e può contenere sia lettere che simboli.

Anche il PUK deve essere digitato una seconda volta per **conferma (7)**.



Nella quarta pagina della procedura guidata verrà chiesto un nome da assegnare al certificato per riconoscerlo in caso di utilizzo di più certificati sullo stesso PC. Se non si ha intenzione di utilizzare più certificati lasciare il valore predefinito:

Rilascio nuovo certificato
×

Nome del certificato

Il nome identificativo (Common Name) è utile per distinguere più certificati contenuti nella stessa smart card oppure più certificati utilizzati per accedere allo stesso VPS della linea "Smart Card".

Inserire un nome identificativo per il certificato

Nome:

< Indietro
Annulla
Avanti >

Nella quinta pagina verrà chiesto se il certificato può essere usato per cifrare la partizione dati di un VPS attraverso la tecnologia Microsoft BitLocker. In questo modo l'accesso alla partizione diventerà molto più sicuro rispetto ad una trazionale password.

Se non si hanno particolari esigenze aziendali lasciare l'impostazione predefinita:

Rilascio nuovo certificato
×

Cifratura BitLocker con certificato

BitLocker è una tecnologia integrata in Microsoft Windows per la cifratura delle partizioni disco e solitamente gli utenti creano una password per accedere ai dati.

Su tutti i VPS della linea "Smart Card" è possibile utilizzare una o più smart card invece della password, aumentando così il livello di protezione dei dati.

ATTENZIONE! Si raccomanda caldamente di memorizzare su una penna USB o stampare la chiave BitLocker come illustrato in [questo video](#).

ATTENZIONE! La modifica delle policy di Windows relative a BitLocker potrebbe consentire l'uso di certificati con scopi generici, quindi se si intende utilizzare questo flag per fini di sicurezza accertarsi che utenti inaffidabili possano accedere al VPS con i diritti di amministratore.

È possibile sbloccare un'unità cifrata con BitLocker con più di una smart card. Ciò potrebbe rendersi necessario, ad esempio, se l'utente si ha abilitato la Virtual Smart Card Microsoft su due notebook e quindi accede al VPS con due differenti certificati.

[Mostra come sbloccare un'unità BitLocker con più di una smart card...](#)

Si desidera abilitare il certificato per l'utilizzo con BitLocker?

Sì, abilita il certificato all'uso di BitLocker
 No, non abilitare il certificato per BitLocker

< Indietro
Annulla
Avanti >

Nella sesta pagina della procedura guidata verrà chiesto di inserire un nome utente (c.d. User Principal Name) che fungerà da identità digitale e sarà l'unico attributo del certificato ad essere mappato sugli utenti dei vari VPS.

In questo modo è possibile utilizzare più dispositivi sicuri (o più PC, nel caso dei TPM) con certificati diversi ed effettuare il login in più VPS con la medesima identità digitale.

ATTENZIONE! Per ragioni di sicurezza il dominio associato dell'UPN è univoco per utente del sito WPanel e non può essere modificato.

Se non si ha intenzione di utilizzare più identità digitali lasciare il valore predefinito:

Rilascio nuovo certificato
✕

User Principal Name

Per l'accesso ai VPS della linea "Smart Card" è indispensabile configurare un nominativo da associare all'utente Administrator o altri utenti configurati nella foresta Active Directory del singolo VPS.

Infatti su ogni VPS della linea "Smart Card" viene preconfigurato un dominio Active Directory univoco per ogni cliente WPanel. Il cliente a sua volta può creare nuovi utenti all'interno della foresta Active Directory ed associarli ai certificati da inserire nelle smart card attraverso l'attributo userPrincipalName.

In questo modo il cliente WPanel può distribuire le smart card ai dipendenti della propria organizzazione per accedere ai VPS della linea "Smart Card" con diritti limitati o comunque non di amministrazione.

Se si sta emettendo un certificato per la prima volta si consiglia di lasciare l'impostazione predefinita.

[Mostra come associare un UPN ad un utente da Prompt dei comandi...](#)

Inserire un'entità utente per l'accesso ai VPS della linea "Smart Card" oppure lasciare l'entità predefinita

UPN: @utente-kdzhg.wpanel.local

< Indietro
Annulla
Avanti >

Nella settima pagina verranno riassunti i dati che verranno inseriti nel certificato:

Rilascio nuovo certificato
✕

Richiesta emissione certificato (CSR)

Il sistema PKI prevede la generazione di una richiesta di emissione del certificato affinché l'Autorità di certificazione possa associare i dati dell'utente alla chiave segreta generata all'interno del dispositivo hardware sicuro.

Nella pagina successiva sarà possibile scaricare il file batch per la creazione automatica della richiesta o in alternativa è possibile visualizzare la procedura manuale da questa pagina.

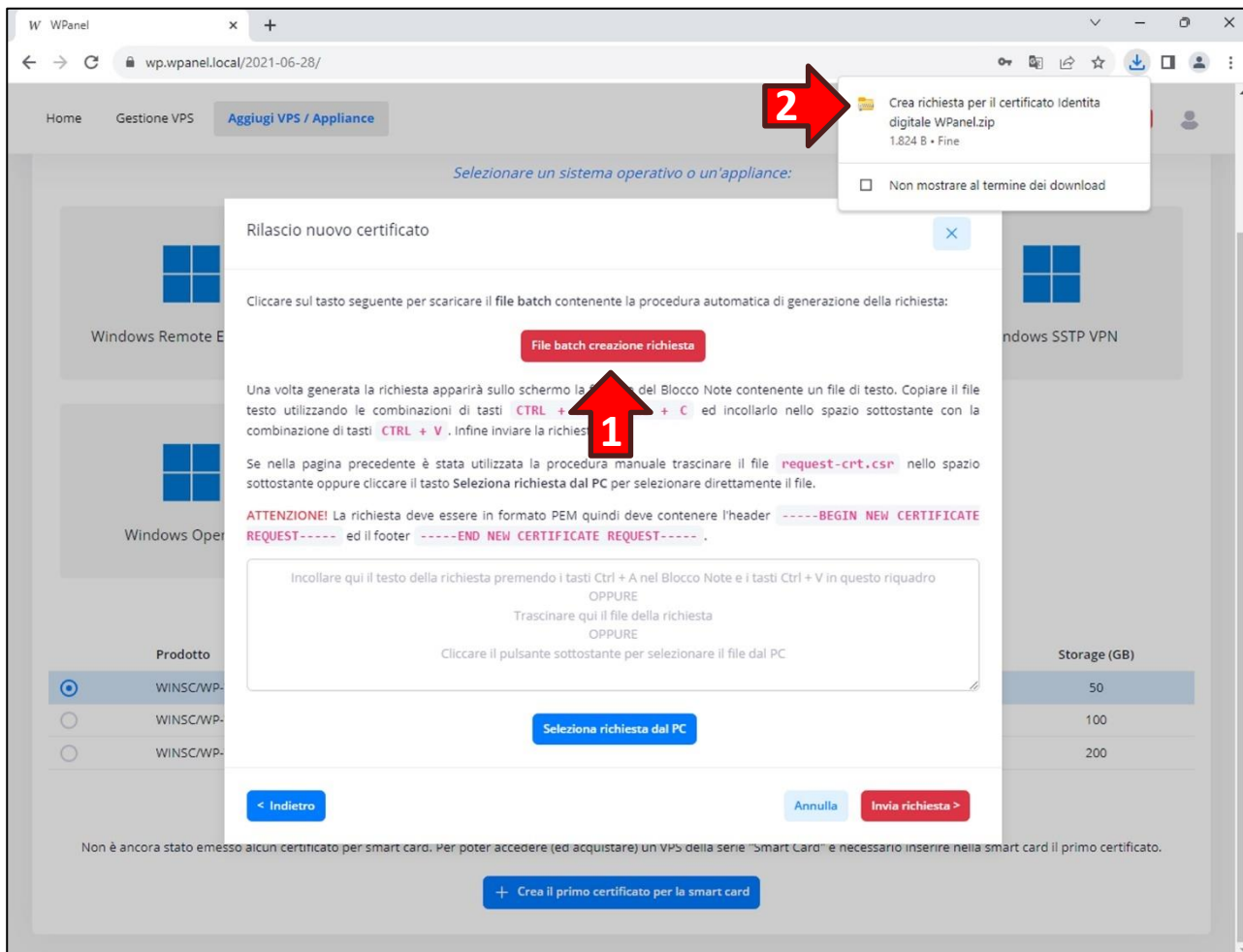
Il certificato verrà emesso utilizzando i dati seguenti:

Nome identificativo:	Identità digitale WPanel
Nome distintivo:	CN=Identità digitale WPanel,O=Azienda di prova,G=Di Prova,SN=Utente,E=utente.di.prova@wpanel.local,STREET=123,L=Prova,S=AG,C=IT
Login sito:	Si
BitLocker:	Si
UPN (login VPS):	utente.di.prova@utente-kdzhg.wpanel.local

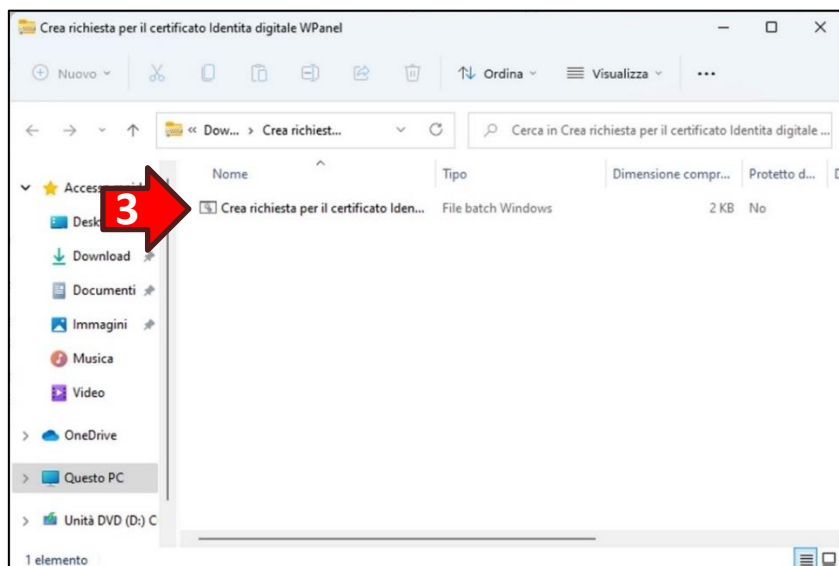
[Mostra la procedura manuale...](#)

< Indietro
Annulla
Avanti >

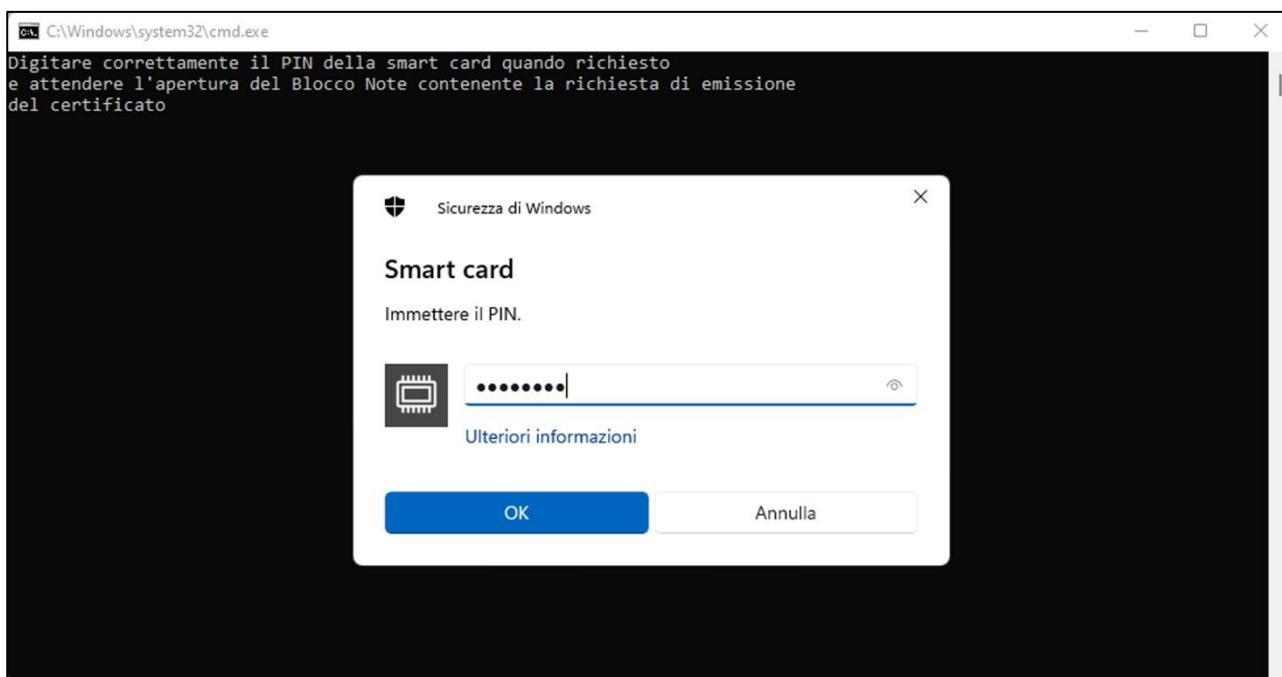
Dall'ottava pagina sarà necessario scaricare la procedura di creazione della coppia di chiavi per crittografia asimmetrica all'interno del dispositivo sicuro il cliccando il tasto **File batch creazione richiesta (1)**. Verrà scaricato sul PC il file **Crea richiesta per il certificato <nome certificato>.zip (2)**:



Aprire il file zip e fare doppio click sul file **Crea richiesta per il certificato <nome certificato> (3)**:

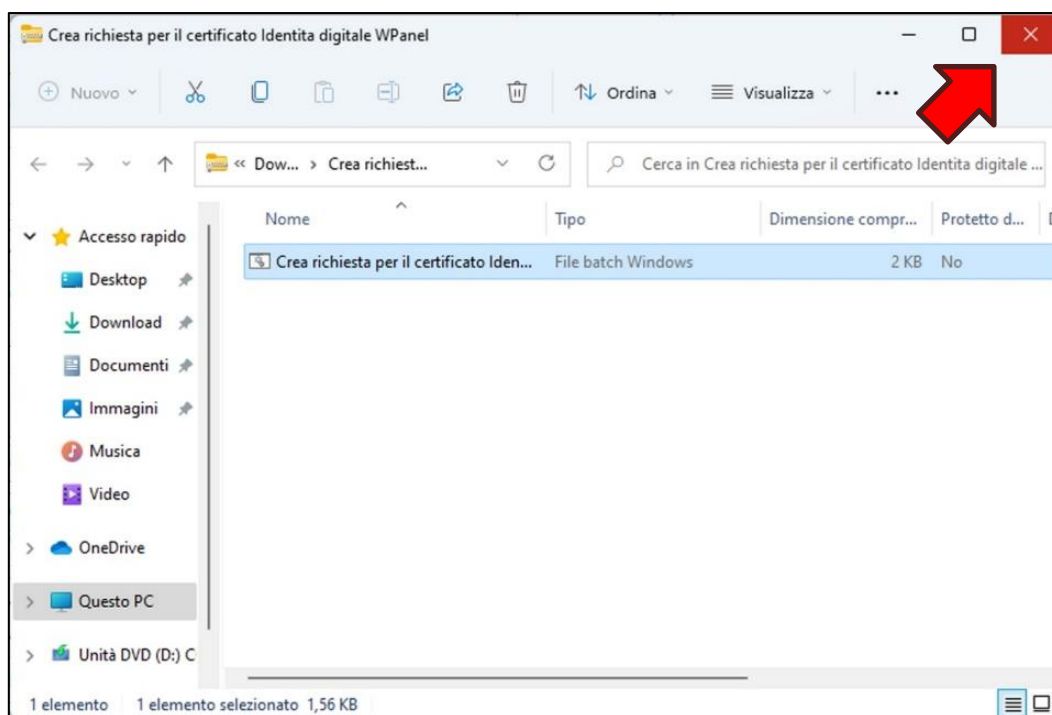


Si aprirà una finestra del *Prompt dei comandi* e dopo diversi secondi verrà richiesto l'inserimento del PIN del dispositivo sicuro:

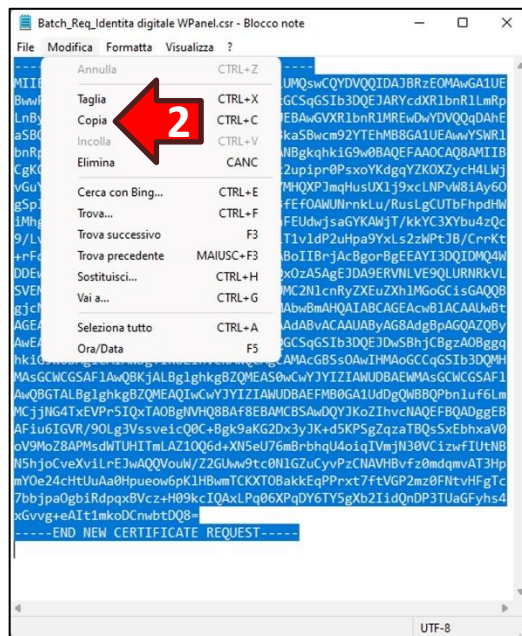
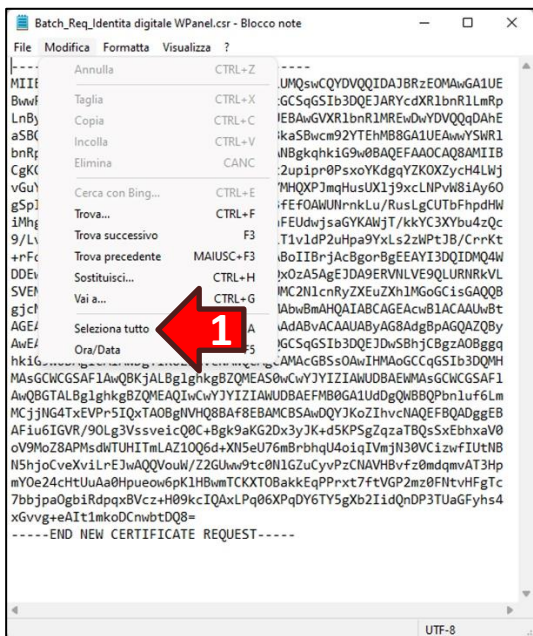


Trascorsi altri secondi la finestra del *Prompt dei comandi* si chiuderà automaticamente e nel mentre si aprirà una finestra del *Blocco Note* contenente un lungo insieme di caratteri.

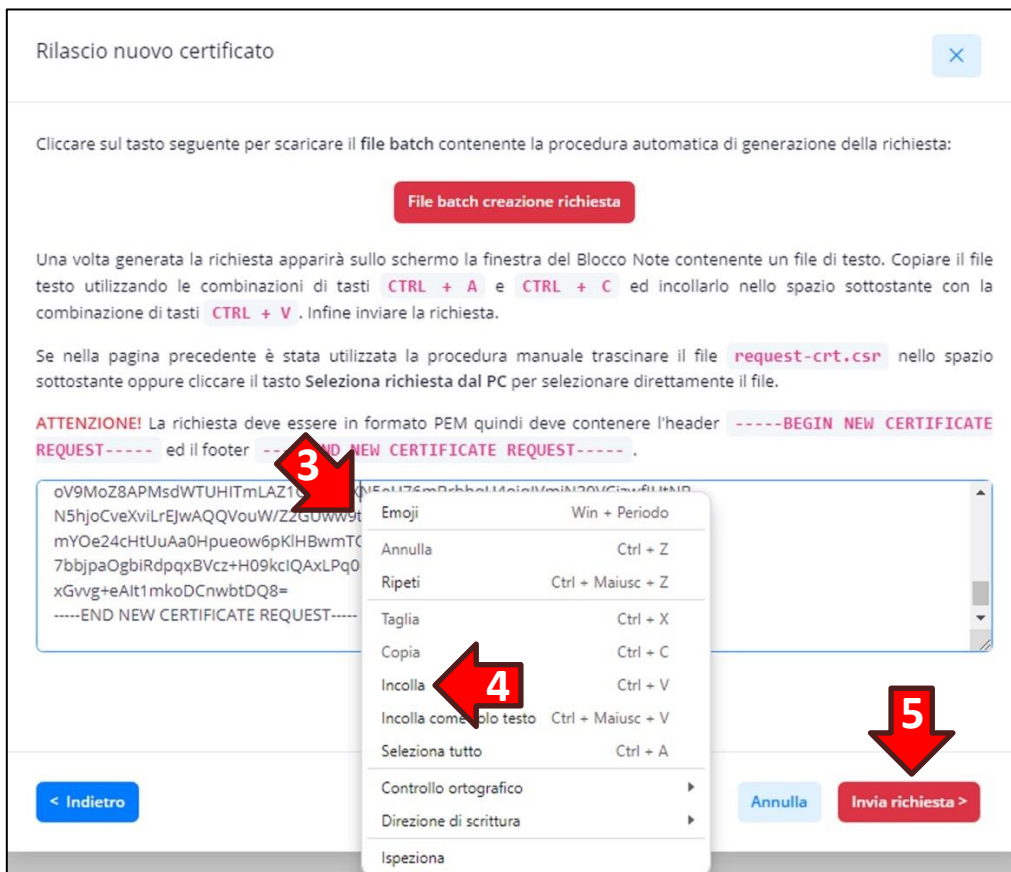
ATTENZIONE! La finestra del *Blocco Note* potrebbe essere nascosta dalla finestra contenente *Crea richiesta per il certificato <nome certificato>*. Chiudere quest'ultima finestra per visualizzare il *Blocco Note*:



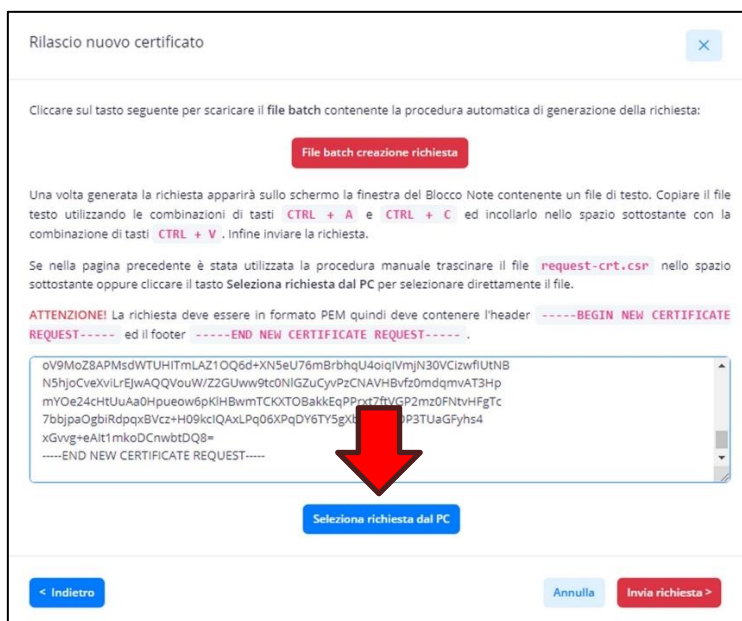
Dalla finestra del *Blocco Note* aprire il menù **Modifica** e cliccare sull'opzione **Seleziona tutto** (1) in modo da evidenziare tutto il testo. Successivamente riaprire il menù **Modifica** e cliccare sull'opzione **Copia** (2):



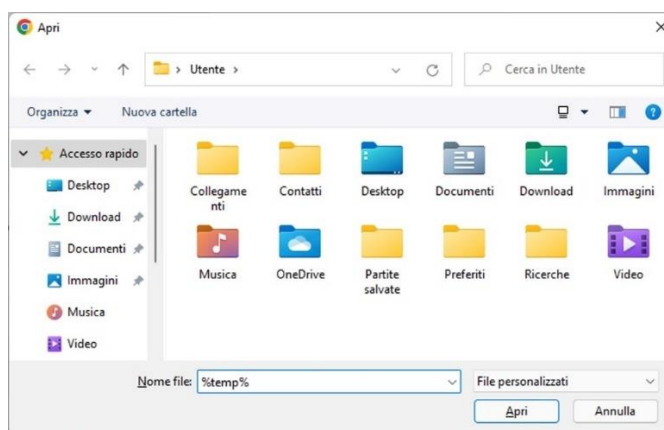
Ritornare sul sito WPanel e con il tasto destro del mouse cliccare all'interno dell'area di testo (3) poi dal menù popup selezionare l'opzione **Incolla** (4). Poi cliccare il tasto **Invia richiesta** (5):



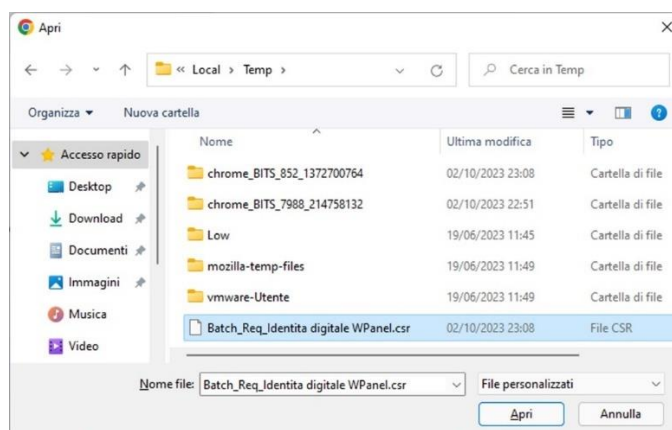
ATTENZIONE! Se si sono riscontrare difficoltà nella procedura di copia del file di testo dal Blocco Note al sito WPanel è possibile utilizzare il tasto Seleziona richiesta dal PC:



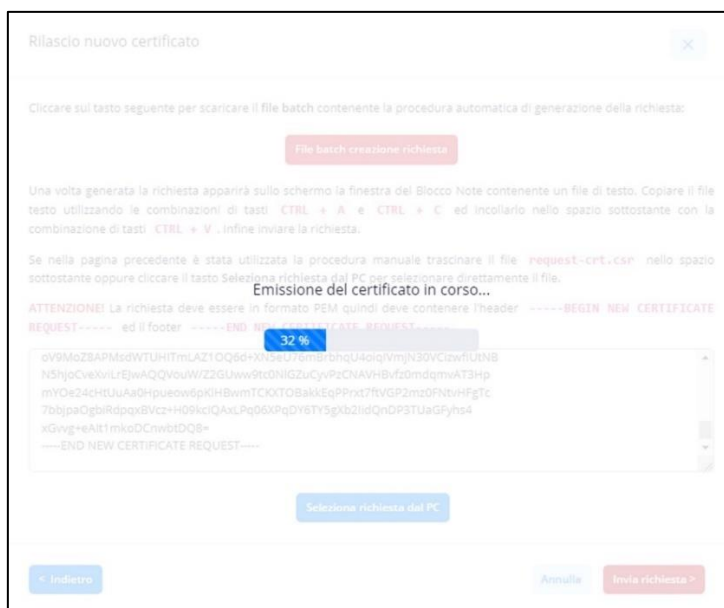
In *Nome file* della finestra *Apri* digitare **%temp%** e poi premere il tasto **Invio**:



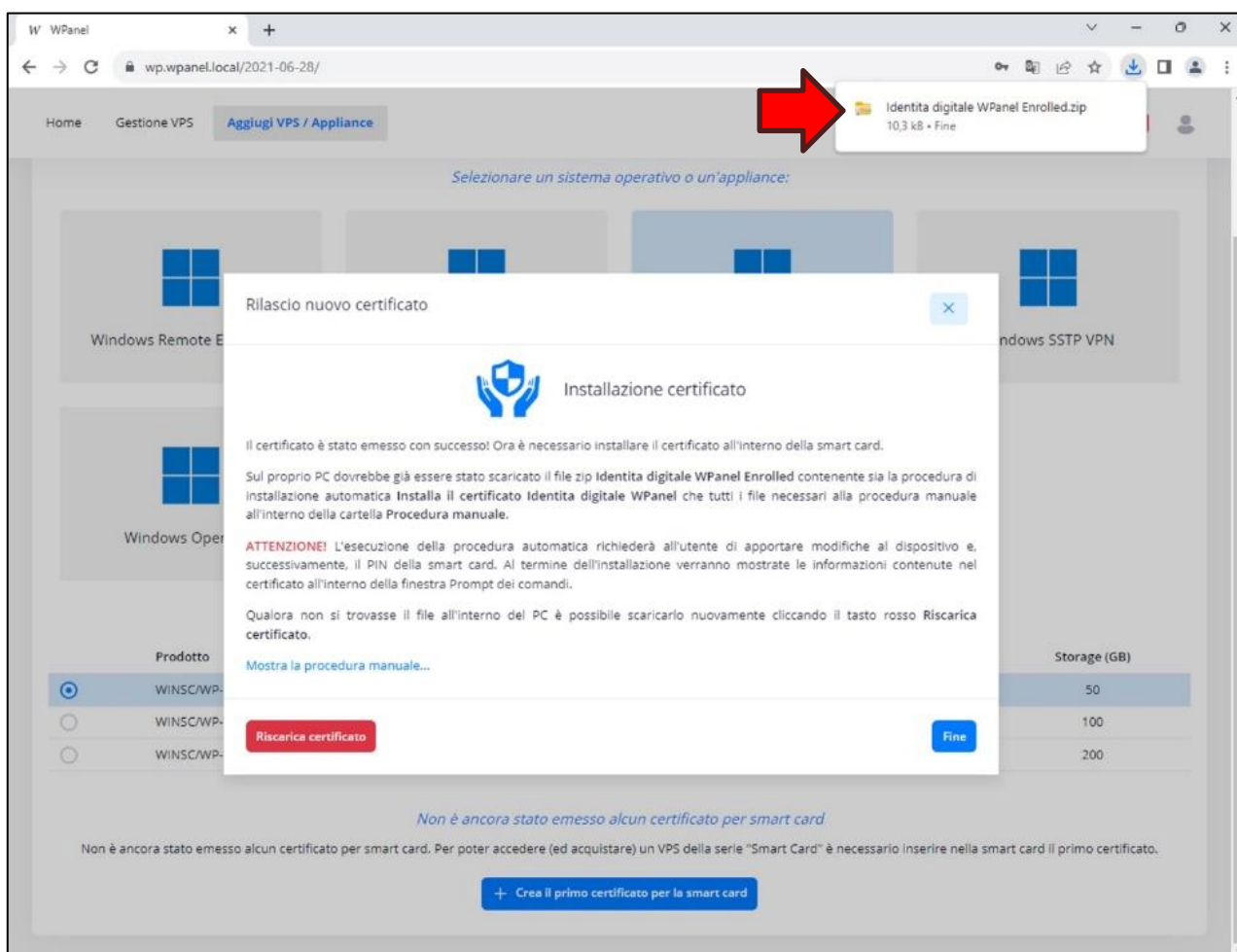
Poi nella lista dei file temporanei selezionare **Batch_Req_<nome del certificato>.csr**:



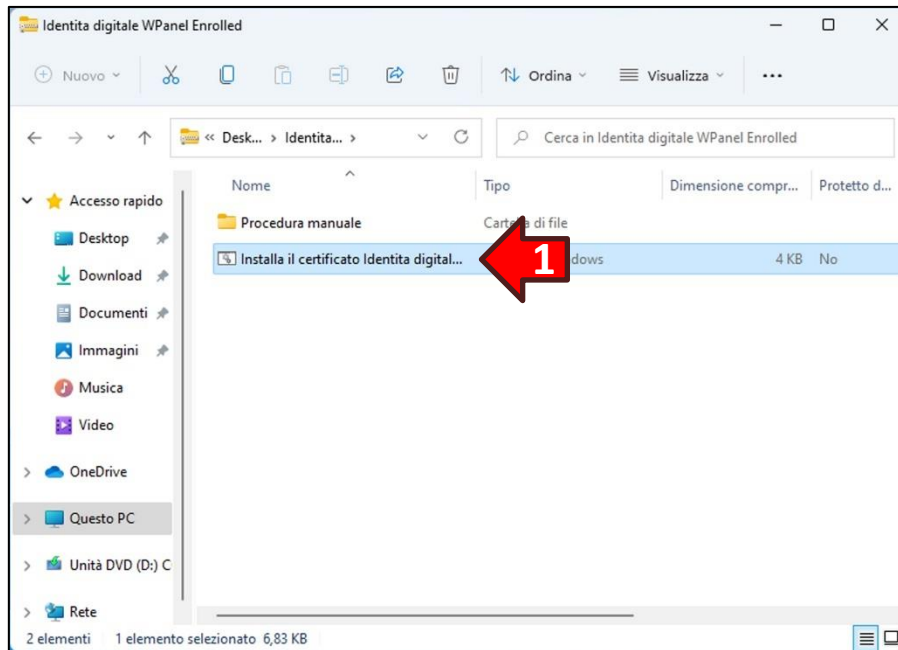
All'invio della richiesta il sito WPanel procederà all'emissione del certificato da inserire nel dispositivo sicuro:



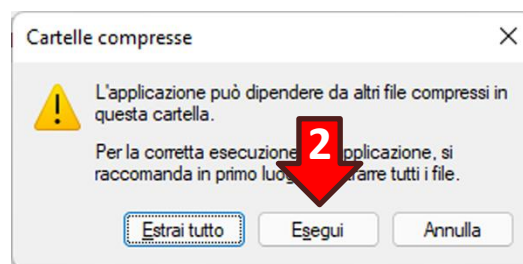
Terminata la fase di emissione il file con il certificato verrà scaricato sul proprio PC:



Aprire il file zip e fare doppio click sul file **Installa il certificato <nome certificato> (1)**:

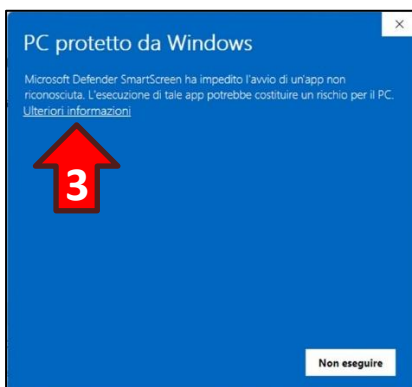


Nella finestra *Cartelle compresse* cliccare il tasto **Esegui (2)**:

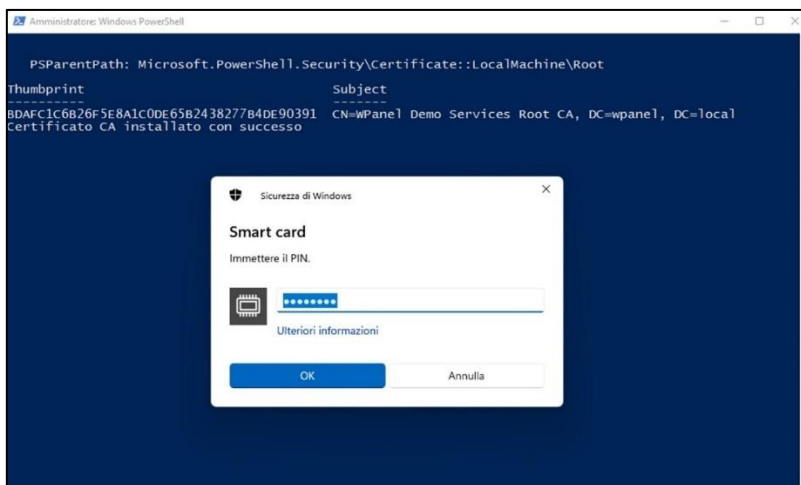


Se dovesse apparire il messaggio *SmartScreen* cliccare sulla dicitura **Ulteriori informazioni (3)** e poi il tasto **Esegui comunque (4)** che apparirà in basso.

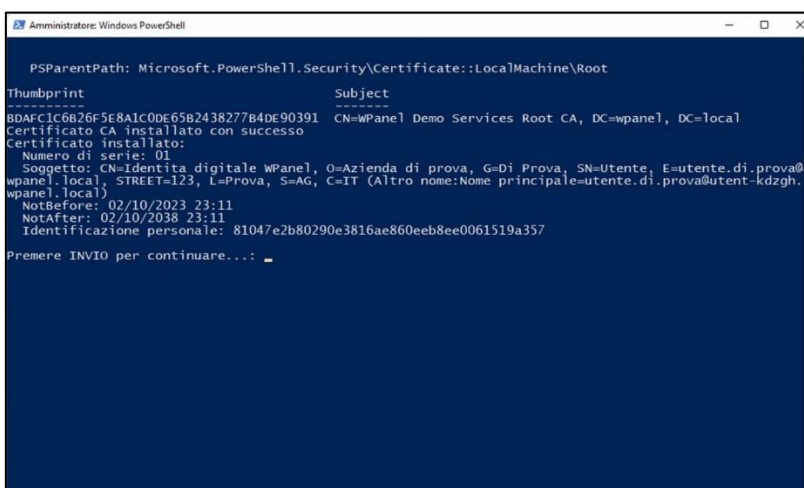
Poi confermare l'apporto di modifiche al dispositivo cliccare il tasto **Sì (5)** nella finestra Controllo dell'account utente:



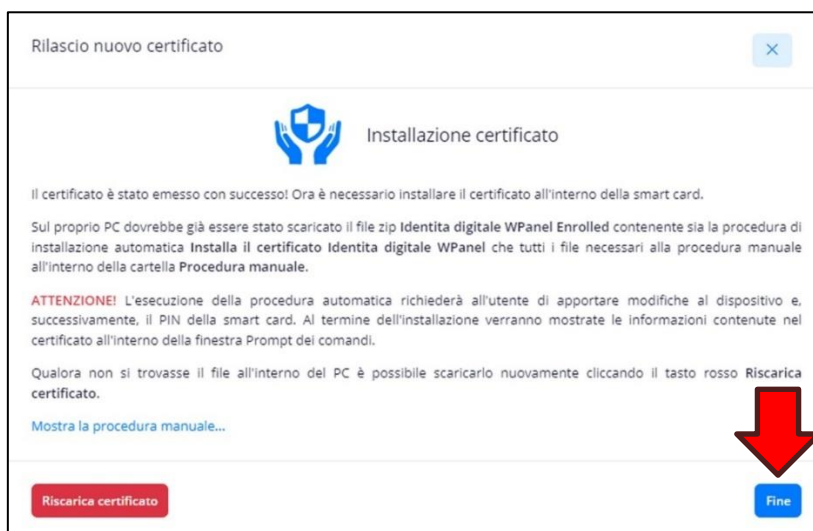
Si aprirà una finestra PowerShell e dopo alcuni secondi verrà richiesto il PIN del dispositivo sicuro:



Una volta inserito il PIN il certificato verrà inserito nel dispositivo sicuro e potrà essere utilizzato:



Ritornare sul sito WPanel e cliccare il tasto **Fine** della procedura guidata:



Una volta emesso il primo certificato è possibile utilizzare il dispositivo sicuro anche per accedere al sito WPanel del vostro fornitore. In questo modo la password associata al nome utente verrà eliminata rendendo l'accesso estremamente sicuro.

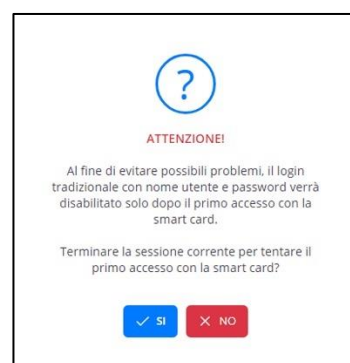
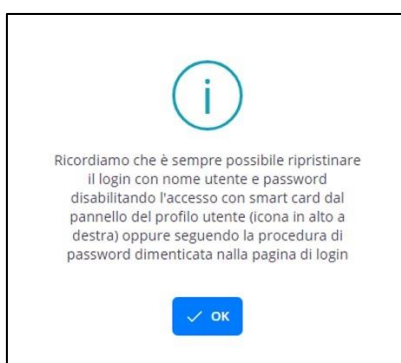
ATTENZIONE! La password associata al nome utente verrà eliminata solo dopo la riuscita del primo accesso con dispositivo sicuro. ABILITARE L'ACCESSO CON DISPOSITIVO SICURO DAL SITO NON ELIMINERÀ LA PASSWORD.

ATTENZIONE! È possibile abilitare l'accesso con dispositivo sicuro anche se ci si è registrati al sito tramite un provider OpenID Connect (Es. Google, LinkedIn, GitHub, ecc.). In ogni caso l'accesso con OpenID verrà disabilitato al primo accesso riuscito con dispositivo sicuro.

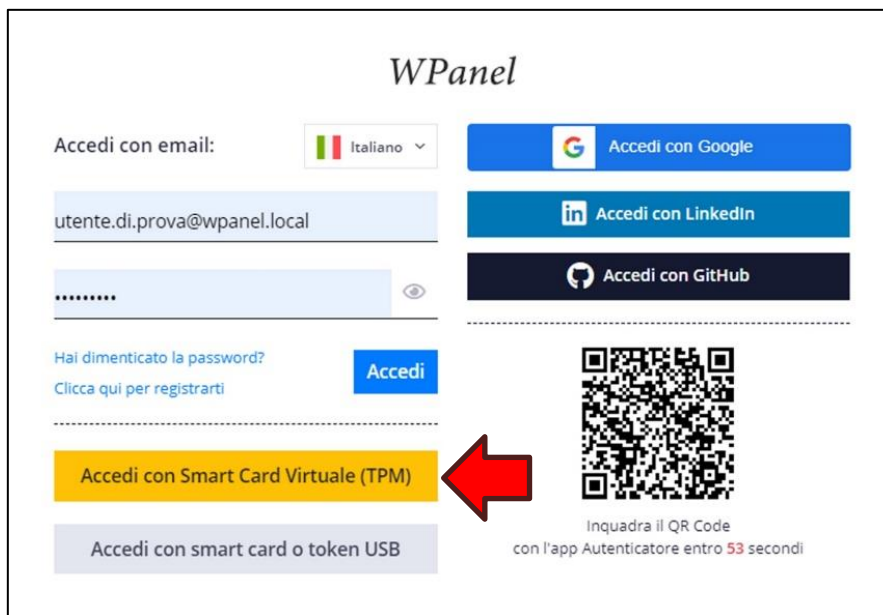
ATTENZIONE! Una volta effettuato l'accesso con il dispositivo sicuro è possibile disabilitarlo dal menù laterale del profilo.

ATTENZIONE! Se si è smarrito il dispositivo sicuro è **sempre** possibile ripristinare l'accesso al sito tramite la procedura di recupero password. Tale procedura è valida anche se si è registrati al sito tramite provider OpenID Connect.

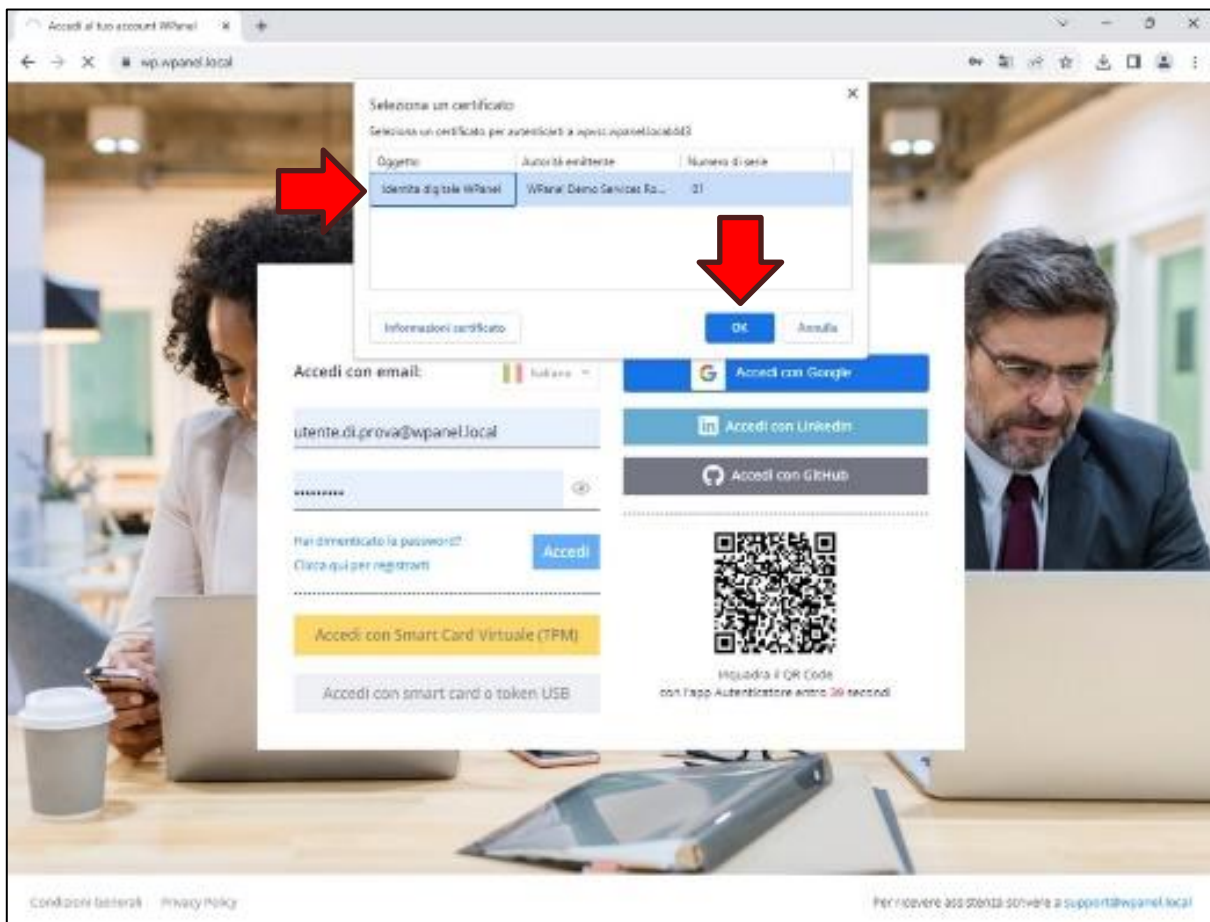
Terminata l'emissione del primo certificato verrà quindi proposto all'utente di abilitare l'accesso tramite dispositivo sicuro. Se si ha questa necessità seguire le indicazioni contenute nei vari messaggi di richiesta:



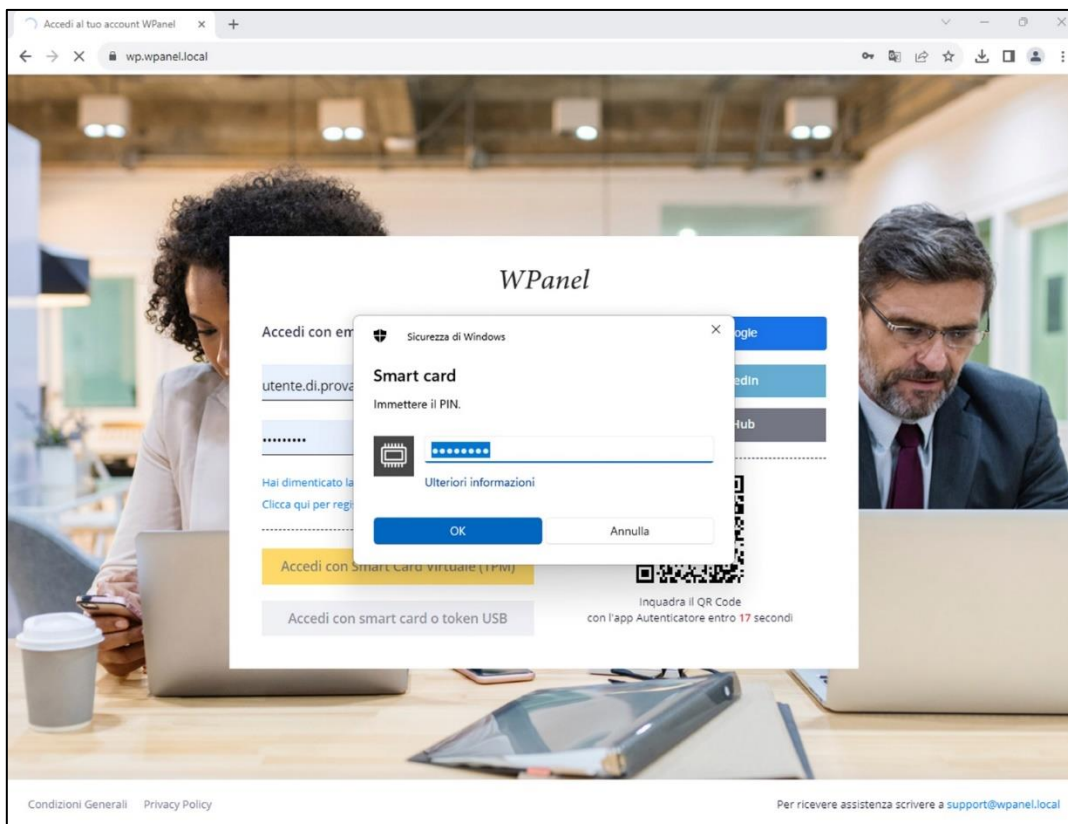
Una volta effettuata la disconnessione e ritornati al modulo di accesso cliccare il tasto **Accedi con Smart Card Virtuale (TPM)**:



A quel punto il browser mostrerà l'elenco dei certificati validi per l'accesso. Se è stato emesso un solo certificato la lista dovrebbe contenere un solo elemento:

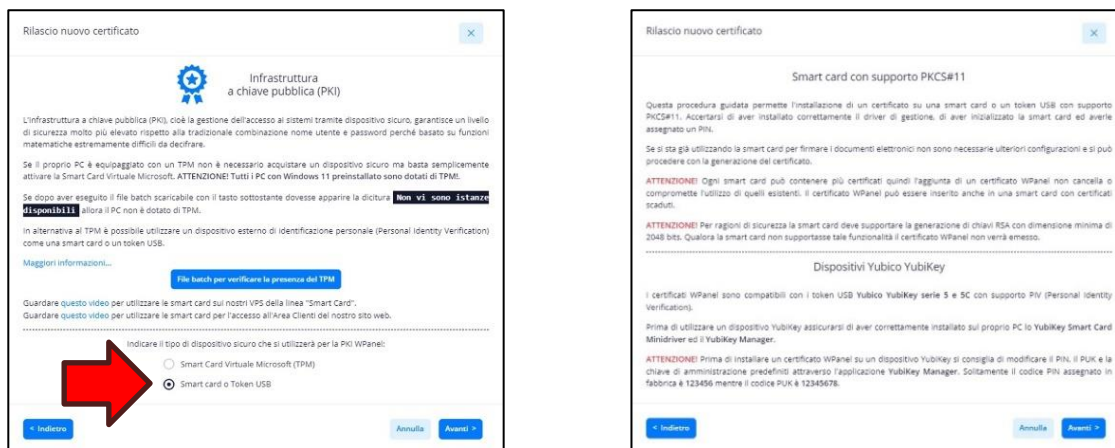


Una volta confermato il certificato da utilizzare verrà richiesto il PIN per completare l'accesso:



3.2 Creazione di un certificato per smart card o token USB

La procedura per l'emissione di un certificato destinato ad una smart card o ad un token USB è sostanzialmente identica a quella utilizzata per il TPM. Semplicemente all'utente non viene proposta la creazione della Smart Card Virtuale perché non pertinente.



ATTENZIONE! Prima di iniziare la procedura di emissione del certificato assicurarsi che nel PC sia già stato installato il driver (c.d. middleware) PKCS#11 del dispositivo e, se necessario, il driver del lettore di smart card.

Se si sta utilizzando un token USB Yubico YubiKey è possibile scaricare i driver da questo indirizzo:

<https://www.yubico.com/support/download/smart-card-drivers-tools/>

Per effettuare l'accesso a WPanel con questi dispositivi è necessario utilizzare il tasto **Accedi con smart card o token USB** dalla form di login:



ATTENZIONE! I dispositivi Yubico YubiKey 5 e Yubico YubiKey 5 FIPS con funzione smart card (PIV) possono essere utilizzati direttamente per l'accesso ai VPS della serie Smart Card.

ATTENZIONE! Per tutti gli altri dispositivi è necessario installare il middleware all'interno del VPS. Per effettuare questa operazione:

- creare una password temporanea per l'utente Administrator (*fare riferimento al **Capitolo 5. Pannello funzioni speciali del VPS***);
- effettuare il collegamento VPN, anche tramite il dispositivo sicuro;
- accedere al desktop del VPS con la password temporanea;
- installare il middleware del dispositivo sicuro;
- chiudere la connessione Desktop Remoto;
- ripristinare l'accesso esclusivo via dispositivo sicuro (*fare riferimento al **Capitolo 5. Pannello funzioni speciali del VPS***);
- accedere al desktop del VPS con il dispositivo sicuro per verificare il corretto funzionamento.

4. Pannello servizi del VPS

Nel dettaglio del VPS, all'interno del sito WPanel del vostro fornitore, è presente un riquadro denominato **Servizi Internet**. Da notare all'interno del riquadro:

- l'indirizzo di accesso al server via VPN (Endpoint VPN);
- l'indirizzo IP del VPS assegnato nel tunnel VPN;
- l'indirizzo DNS da associare al tunnel VPN;
- il percorso delle condivisioni di rete (accessibili via Kerberos).

The screenshot displays the WPanel interface for a VPS. The main content area is titled 'Stato' (Status) and includes a 'Note' section. Below this, the 'Servizi Internet' (Internet Services) section is highlighted with a red box, containing the following information:

Endpoint VPN:	wrx-192-168-1-92.wpanel.local:22001
Indirizzo VPS via VPN:	192.168.222.1
DNS da impostare per la VPN:	192.168.222.1
UPN Administrator:	utente.di.prova@utent-kdzh.wpanel.local
Condivisioni di rete:	\\mydesktop.utent-kdzh.wpanel.local\

Other visible sections include 'Elenco VPS' (VPS List) with an 'Aggiungi VPS / App' button, 'Panoramica' (Overview) for the selected VPS, and 'Funzioni speciali' (Special Functions) with buttons for 'Setup per Client', 'Manuale PKI', 'Imposta password Administrator', and 'Login solo con smart card'.

5. Pannello funzioni speciali del VPS

Nel dettaglio del VPS, all'interno del sito WPanel del vostro fornitore, è presente un riquadro denominato **Funzioni speciali**. Da notare all'interno del riquadro:

- il download della procedura automatica di setup per un computer che deve accedere al VPS;
- il download di questo manuale;
- l'impostazione di una password per l'utente Administrator (per le operazioni di manutenzione);
- la cancellazione della password per l'utente Administrator (al termine delle operazioni di manutenzione).

The screenshot displays the WPanel interface for a VPS. The main content area is titled 'mydesktop.utent-kdzh.wpanel.local' with IP address 192.168.1.92. The 'Stato' (Status) section shows the VPS is 'Acceso' (Accessed) with various system metrics like CPU, RAM, and HDD usage. The 'Servizi Internet' (Internet Services) section lists VPN endpoint and other network details. The 'Funzioni speciali' (Special Functions) section, highlighted with a red box, contains four buttons: 'Setup per Client', 'Manuale PKI', 'Imposta password Administrator', and 'Login solo con smart card'.

6. Configurazione del proprio PC tramite procedura automatica

All'interno del sito WPanel del vostro fornitore è possibile scaricare una procedura (file batch) per la configurazione automatica del tunnel VPN, della connessione al **Desktop Remoto** e dell'accesso alle **condivisioni di rete** del vostro VPS.

La procedura non è un file eseguibile quindi può essere ispezionata dall'utente più diffidente tramite il **Blocco Note**. La procedura non contiene e non installa alcun software eseguibile nel PC dell'utente ma si limita ad inserire i dati e le icone necessarie per interagire con il VPS.

ATTENZIONE! La velocità della connessione VPN potrebbe risultare rallentata nei 10 minuti successivi alla creazione del VPS.

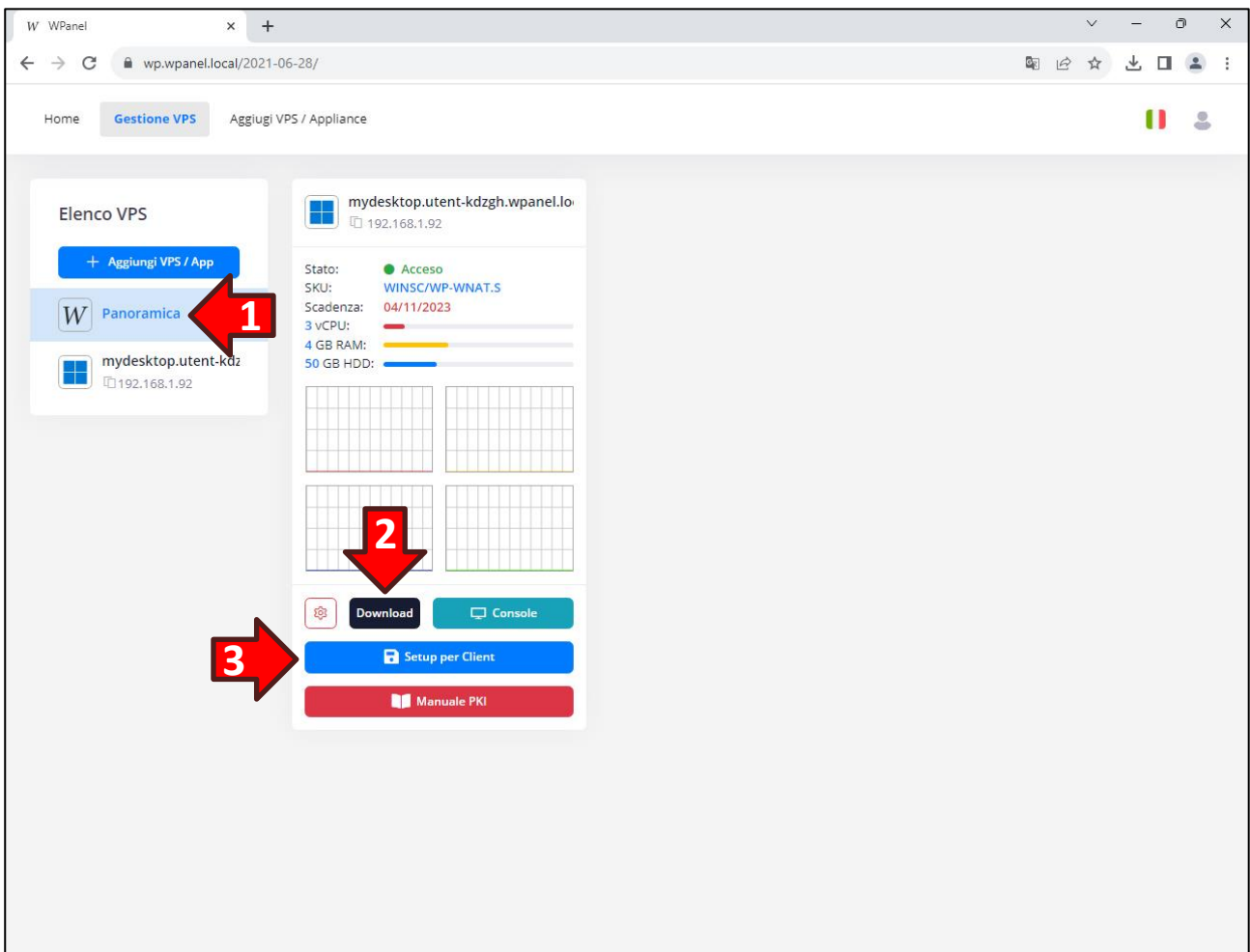
ATTENZIONE! Il sito WPanel non memorizza alcuna credenziale, per cui, una volta effettuata la configurazione del client, le password dovranno essere inserite manualmente facendo riferimento all'email inviata in fase di acquisto del VPS.

ATTENZIONE! La procedura di configurazione viene scaricata automaticamente come file ZIP sul PC dell'utente in fase di creazione del VPS:

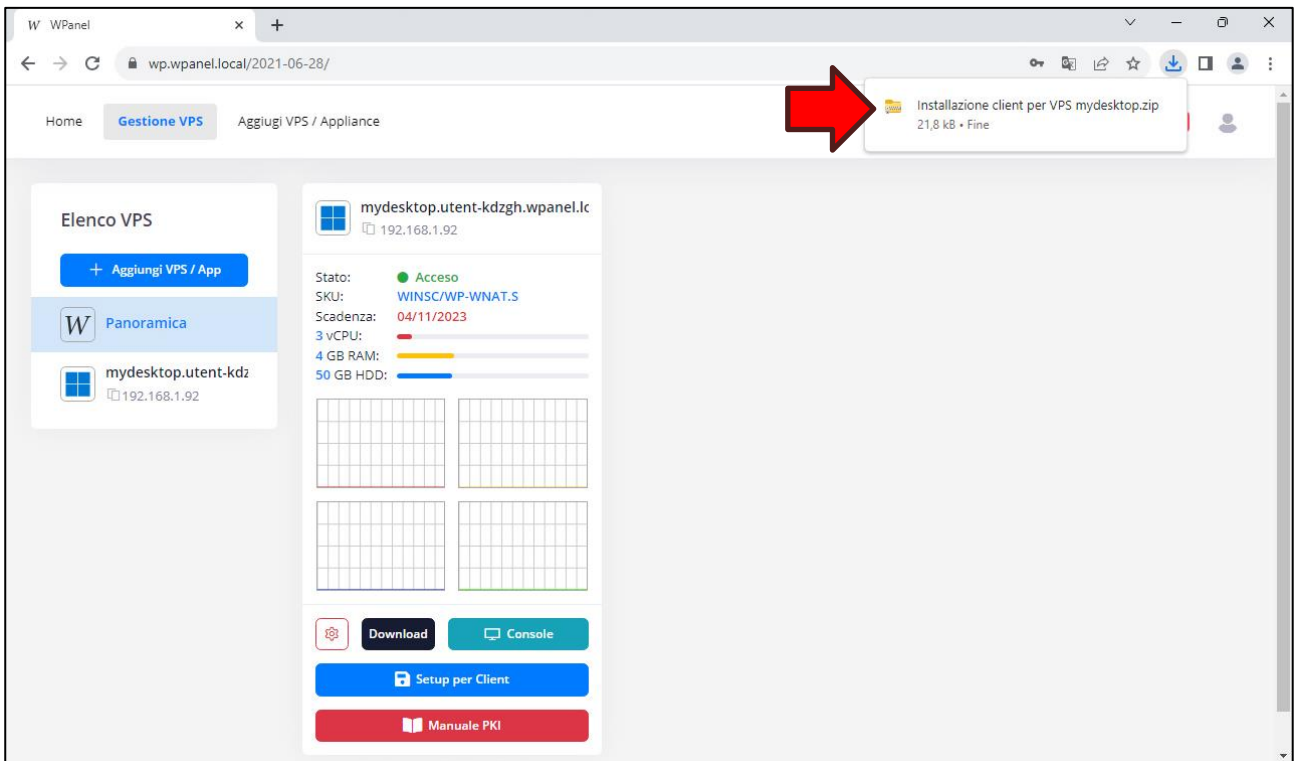
The screenshot shows a web browser window with the URL `wp.wpanel.local/2021-06-28/`. A download notification for "Installazione client per VPS mydesktop.zip" (21,8 kB) is visible in the top right, with a red arrow pointing to it. Below the notification, a "Download setup per client" section contains instructions and a warning: "ATTENZIONE: Per chiudere il messaggio cliccare prima sulla dicitura 'Ulteriori informazioni!' (1) e poi sul tasto 'Esegui comunque' (2) che apparirà in basso:". Two "PC protetto da Windows" warning boxes are shown. The first box has a red arrow labeled "1" pointing to the "Ulteriori informazioni" link. The second box has a red arrow labeled "2" pointing to the "Esegui comunque" button. At the bottom of the page, there are buttons for "Scarica di nuovo" and "Torna alla gestione dei VPS".

Qualora si fosse smarrito tale file ZIP è possibile scaricarlo nuovamente **una volta completata la creazione del VPS** seguendo i passaggi indicati di seguito.

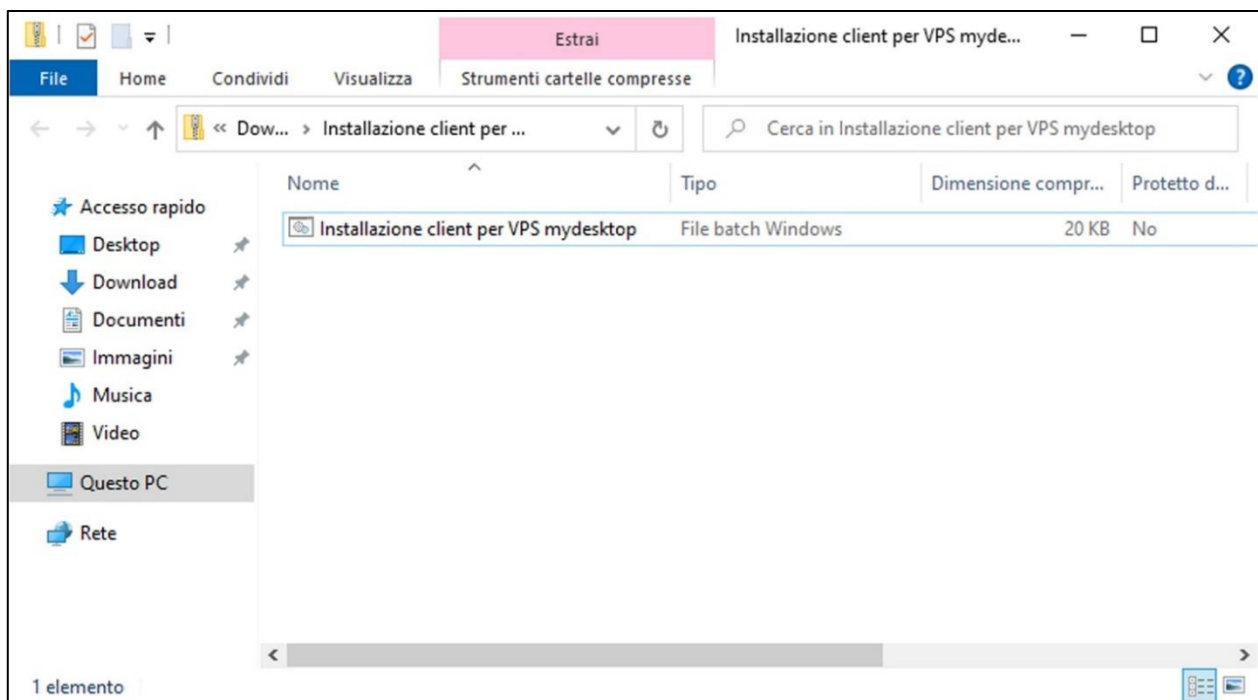
Accedere al sito WPanel del vostro fornitore, cliccare sull'opzione **Panoramica (1)** dalla sezione Elenco VPS, individuare il VPS appena creato e cliccare il tasto **Download (2)**. Dall'elenco di tasti che verrà mostrato cliccare il tasto **Setup per Client (3)**:



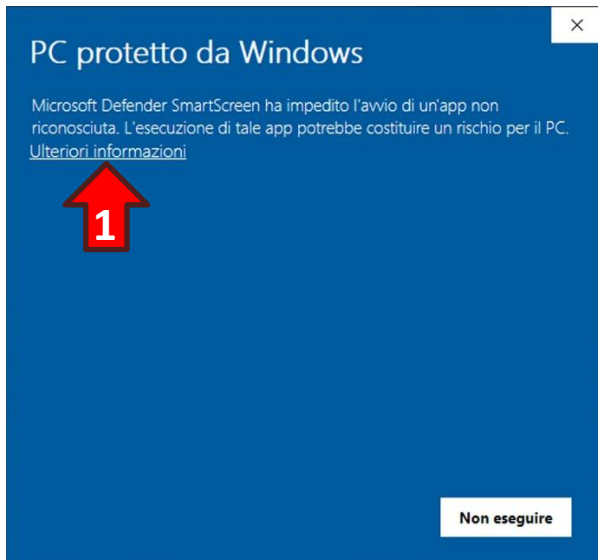
Quindi aprire il file ZIP appena scaricato cliccando sul nome del file mostrato nel riquadro del browser:



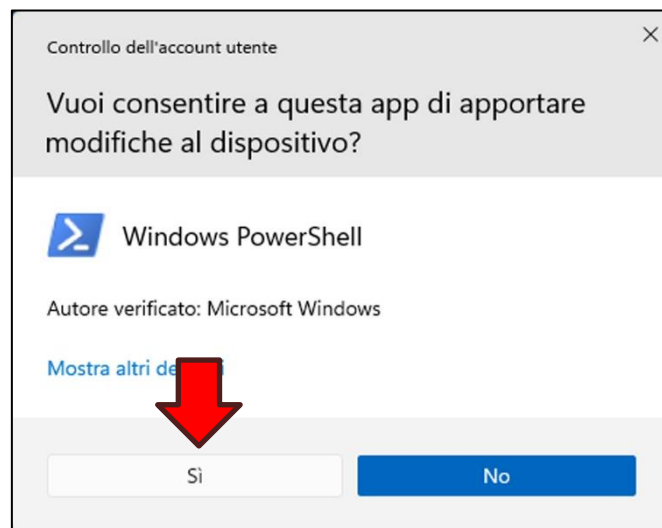
Poi fare doppio click sulla procedura **Installazione client...** contenuta nel file ZIP:



Se nel PC è attivo il sistema *SmartScreen* potrebbe apparire una finestra con sfondo blu con il messaggio che l'applicazione non è stata riconosciuta da Windows. Quindi cliccare sulla scritta **Ulteriori informazioni (1)** e successivamente il tasto **Esegui comunque (2)**:



Confermare le modifiche al dispositivo, se richiesto, cliccando il tasto **Sì**:

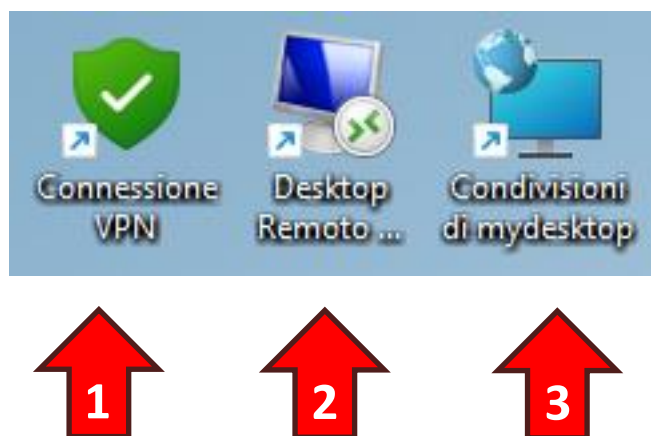


Al termine della configurazione verrà visualizzato l'elenco delle modifiche apportate:

```
C:\Windows\system32\cmd.exe
Consentire le modifiche al dispositivo se e quando richiesto
Creazione connessione VPN effettuata
Creazione icona per connessione VPN effettuata
Creazione icona per connessione Desktop Remoto effettuata
Creazione del link delle risorse di rete del VPS effettuata
Certificato CA già installato
Configurazione Kerberos già presente
Associazione IP VPS nel file hosts effettuata con successo
Premere un tasto per continuare . . .
```

Inoltre sul desktop saranno comparse le icone per:

- 1) L'apertura del tunnel VPN;
- 2) La connessione al desktop del VPS;
- 3) L'accesso alle condivisioni di rete attivate sul VPS.



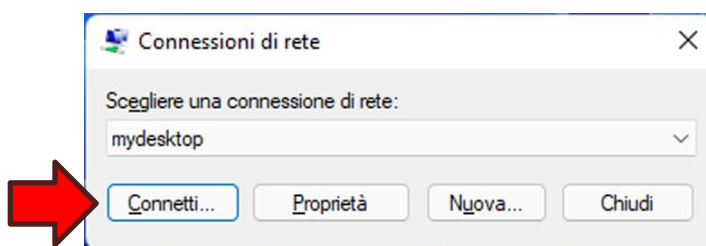
7. Primo accesso al VPS (VPN, desktop remoto e condivisioni di rete)

7.1 Apertura del tunnel VPN

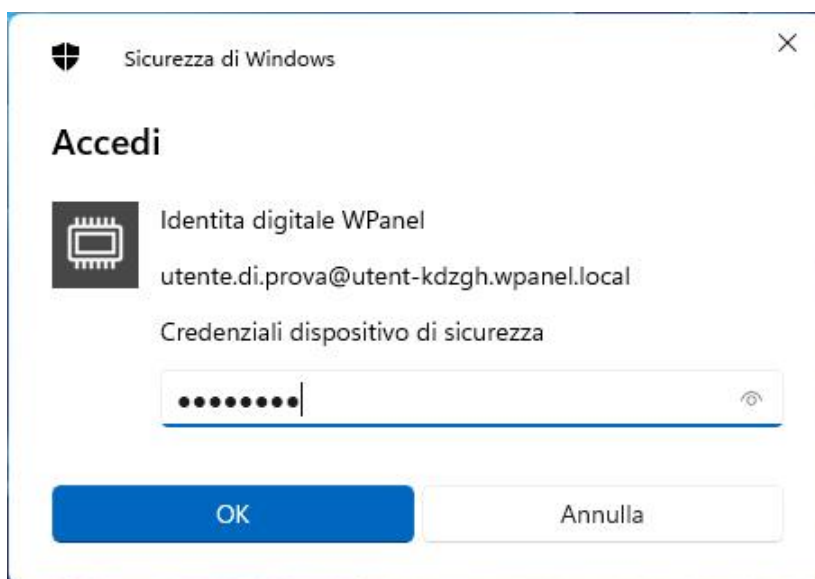
Il VPS da voi acquistato è protetto da una connessione VPN quindi prima di poter accedere a qualunque risorsa (desktop remoto, condivisioni di rete, risorse web, ecc.) è necessario aprire il tunnel VPN facendo doppio click sull'icona **Connessione VPN** nel desktop:



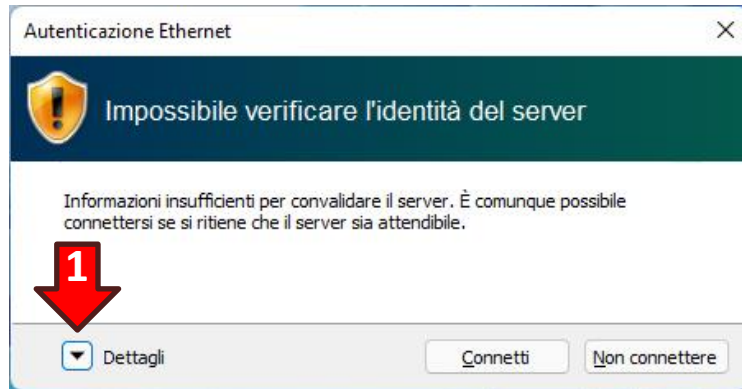
Dalla finestra di selezione della VPN accertarsi che il VPS a cui si intende connettersi sia quello indicato (Esempio: **midesktop**) dopodiché cliccare il tasto **Connetti...**:



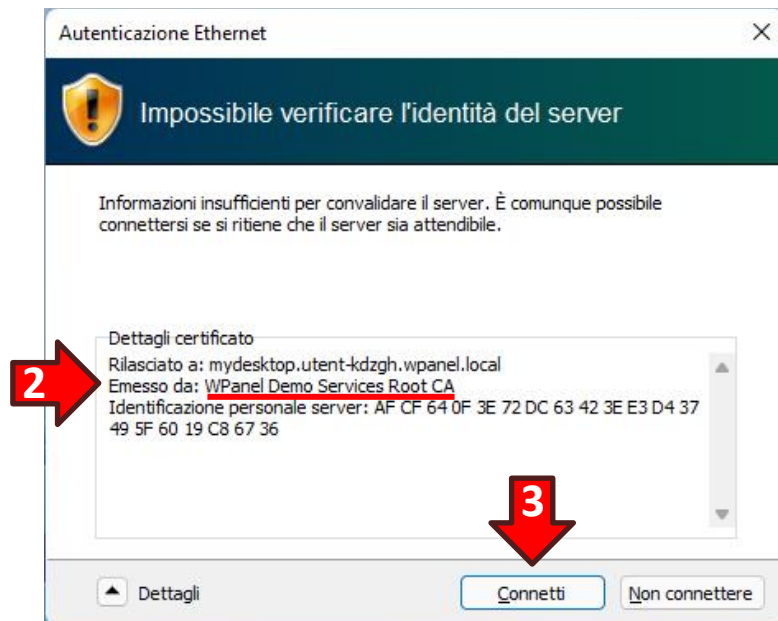
Verrà richiesto il PIN del dispositivo sicuro:



Alla prima connessione, e solo alla prima connessione, apparirà la finestra *Autenticazione Ethernet*. Poiché per ragioni di sicurezza il vostro fornitore non mantiene online il server per l'Autorità di Certificazione, la verifica del certificato di tale autorità deve essere effettuata dall'utente. Cliccare quindi il tasto con la **freccia verso il basso (1)** per mostrare i dettagli del certificato di connessione:



Nella sezione **Dettagli certificato** verificare che il certificato sia stato emesso dal **vostro fornitore (2)** e poi cliccare il tasto **Connetti (3)**:



Se non appaiono messaggi di errore il tunnel VPN è attivo.

7.2 Connessione al Desktop Remoto

Una volta aperto il tunnel VPN è possibile collegarsi sia al Desktop Remoto che accedere alle condivisioni di rete del VPS.

La procedura di configurazione del client crea automaticamente due nuove icone sul desktop del computer denominate **Condivisioni in <nome del vostro VPS>** (Esempio: **Condivisioni in mydesktop**) e **Desktop di <nome del vostro VPS>** (Esempio: **Desktop di mydesktop**).

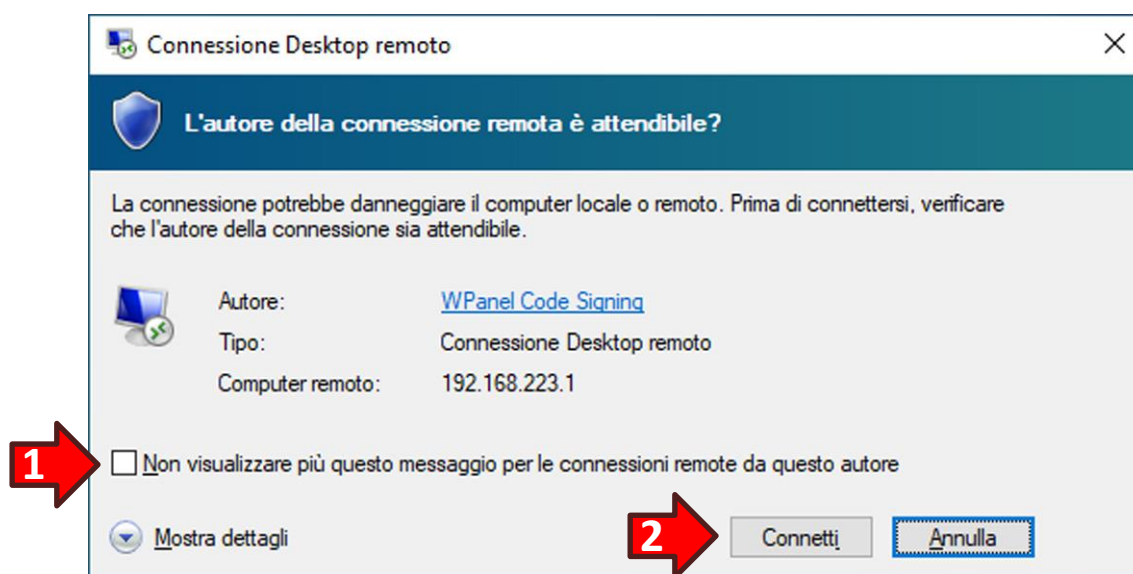
Icone in Windows 11



Icone in Windows 10

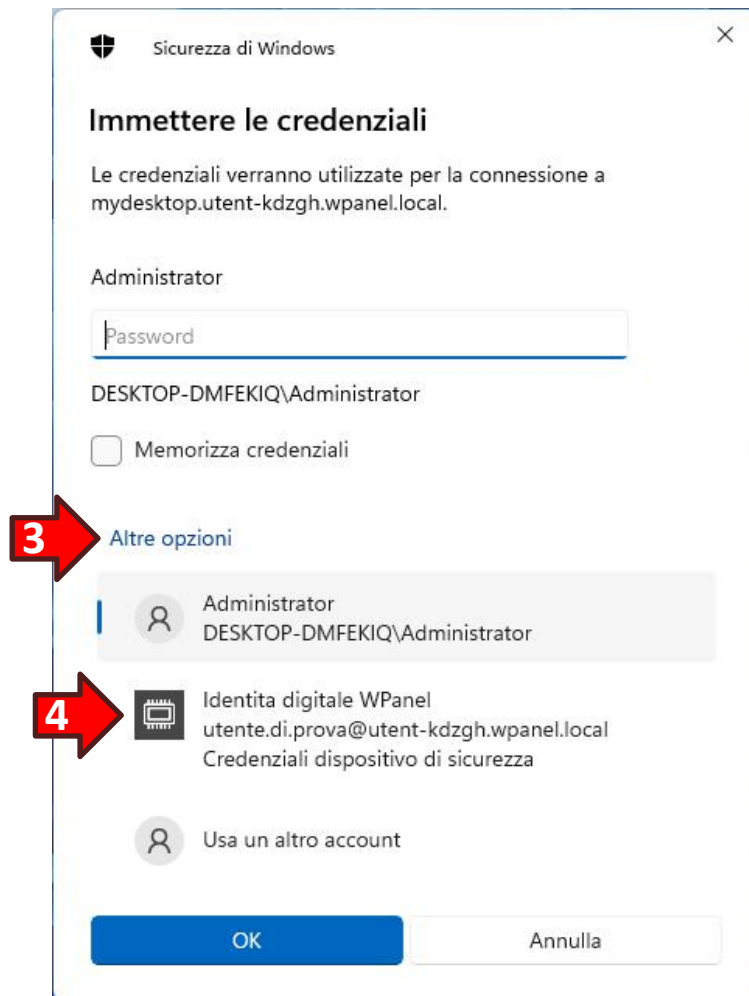


Facendo doppio click sull'icona **Desktop di <nome del vostro VPS>** apparirà la finestra di conferma dell'autore del file di configurazione. Per evitare la visualizzazione del messaggio ad ogni nuovo collegamento spuntare l'opzione **Non visualizzare più questo messaggio...** (1), poi cliccare il tasto **Connetti** (2):



Successivamente verranno richieste le credenziali di accesso al desktop del VPS.

Se venisse richiesta la password dell'utente Administrator è necessario cliccare sulla dicitura azzurra **Altre opzioni (3)** e selezionare il **certificato/identità digitale (4)** da utilizzare per la connessione:



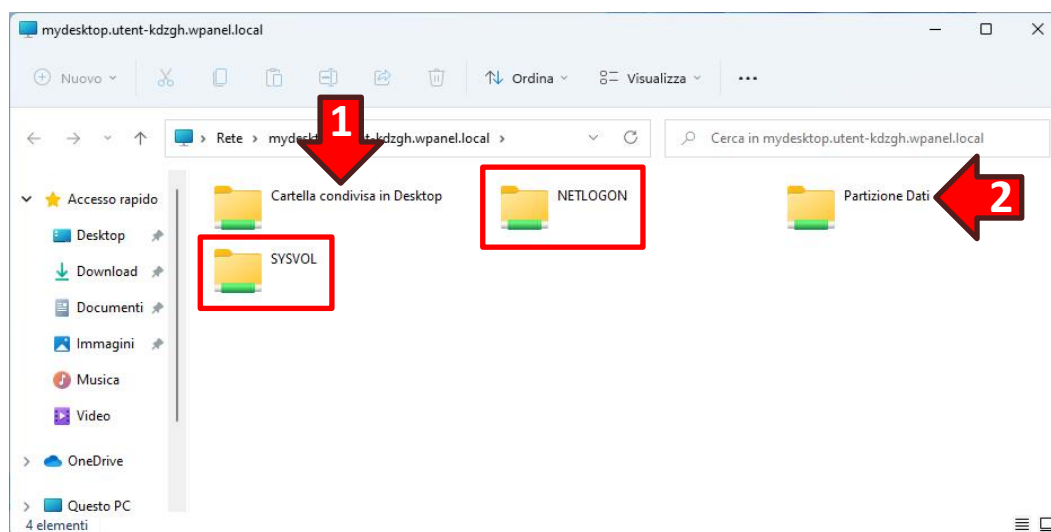
7.3 Accesso alle condivisioni di rete

Il VPS viene consegnato con una cartella sul desktop dell'utente *Administrator*, denominata **Cartella condivisa (1)**, già condivisa in rete con la definizione **Cartella condivisa in Desktop (1)**.



Se in fase di acquisto del VPS si è scelto di creare anche una partizione dati questa verrà automaticamente condivisa con la definizione **Partizione Dati (2)**.

Facendo doppio click sull'icona **Condivisioni in <nome del vostro VPS>** sul desktop del proprio PC sarà possibile accedere automaticamente alle cartelle condivise attivate all'interno del vostro VPS:



ATTENZIONE! Nell'elenco delle cartelle condivise appariranno anche le voci **NETLOGON** e **SYSVOL**. Queste voci devono essere ignorate in quanto condivisioni tecniche dei domini Windows.

8. Cifratura della partizione dati con BitLocker

Se in fase di acquisto si è scelto di creare una partizione dati questa può essere cifrata con BitLocker.

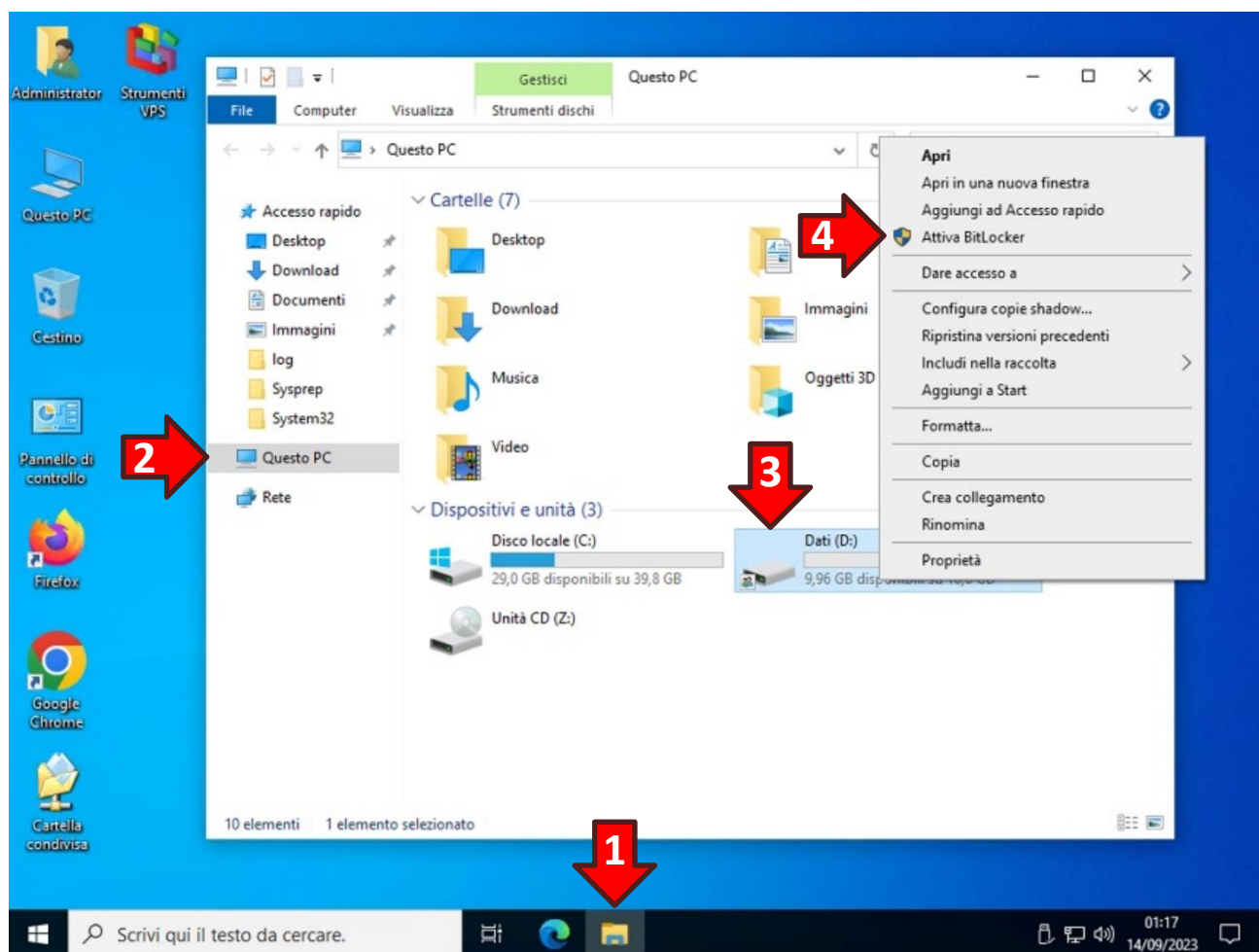
ATTENZIONE! Per effettuare questa operazione in assoluta sicurezza procurarsi una Penna USB dove conservare la Chiave di ripristino BitLocker.

ATTENZIONE! Collegare la Penna USB al proprio PC **non prima** di quando indicato nelle istruzioni.

8.1 Cifratura della partizione dati con BitLocker tramite dispositivo sicuro

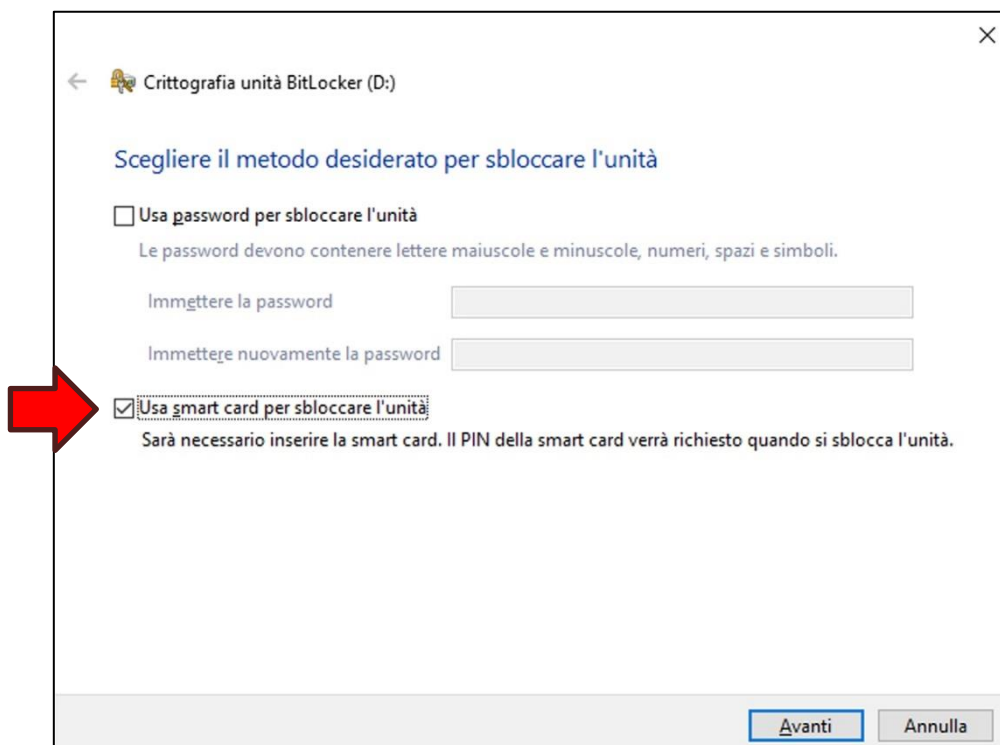
Per cifrare la partizione dati entrare nel desktop del VPS e **solo successivamente** collegare la Penna USB al proprio PC.

Dal desktop del VPS cliccare sull'icona **Esplora Risorse (1)**. Quindi selezionare l'opzione **Questo PC (2)** dalla lista a destra e cliccare con il tasto destro del mouse sull'icona della partizione dati (3). Infine dal menù pop-up scegliere l'opzione **Attiva BitLocker (4)**:

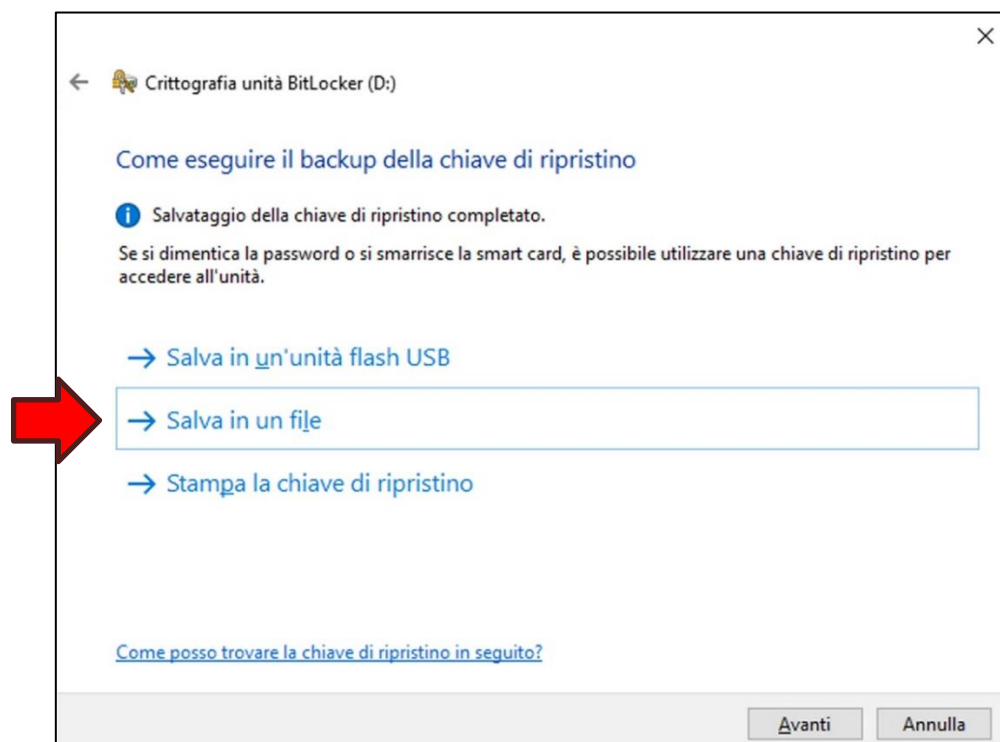


Nella finestra *Scegliere il metodo desiderato per sbloccare l'unità* spuntare l'opzione **Usa smart card per sbloccare l'unità (1)**.

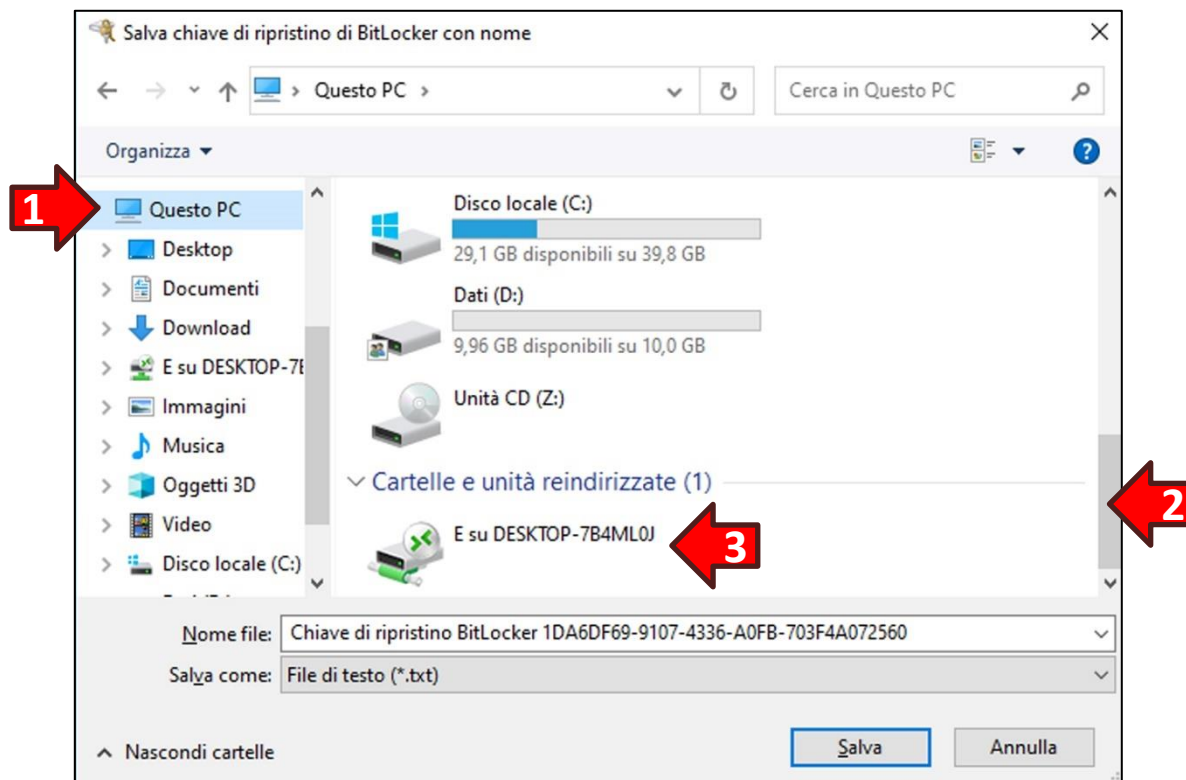
ATTENZIONE! Il dispositivo sicuro o la smart card verranno rilevati da BitLocker solo se in fase di emissione del certificato è stato autorizzato l'utilizzo con BitLocker.



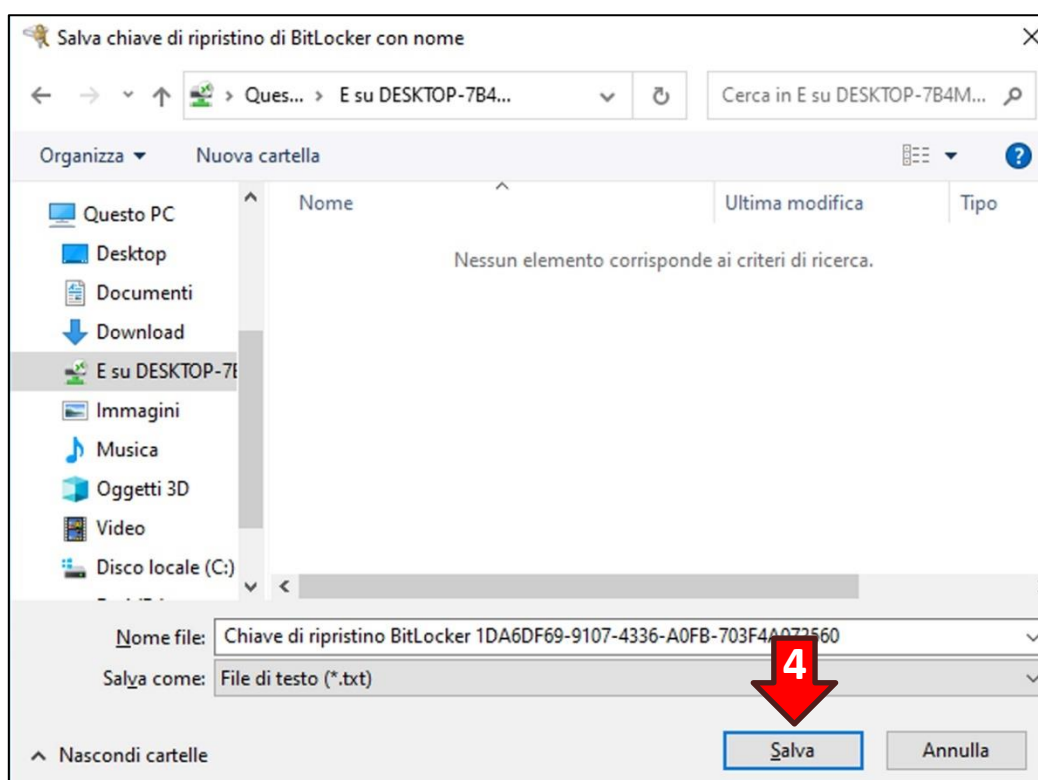
Dalla finestra *Come eseguire il backup della chiave di ripristino* cliccare sull'opzione **Salva in un file:**



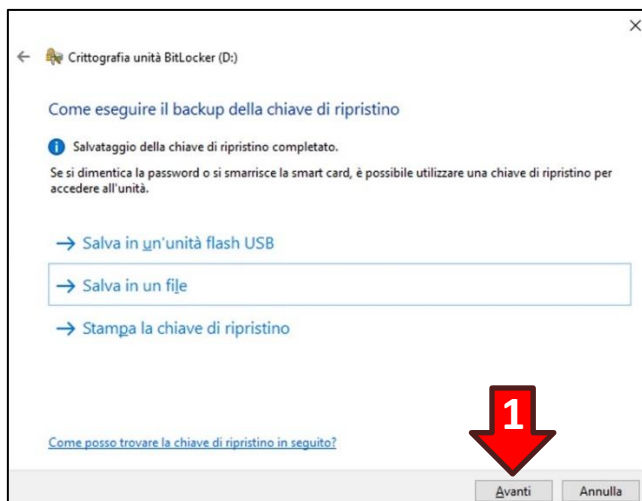
Si aprirà la finestra *Salva chiave di ripristino di BitLocker con nome*. Nell'albero di sinistra cliccare sulla voce **Questo PC (1)** poi scorrere la **sezione di destra fino in fondo (2)** e **fare doppio click sull'Unità E (3)** nella sezione *Cartelle e unità reindirizzate*:



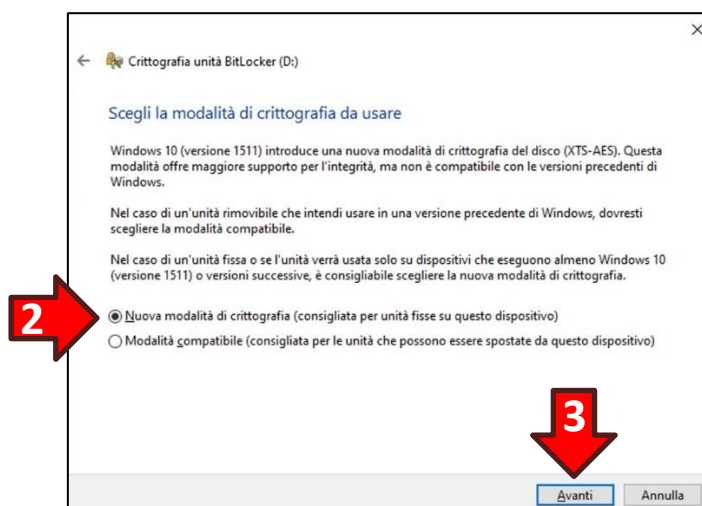
Quindi una volta impostato il salvataggio nell'**Unità E** cliccare il tasto **Salva (4)**:



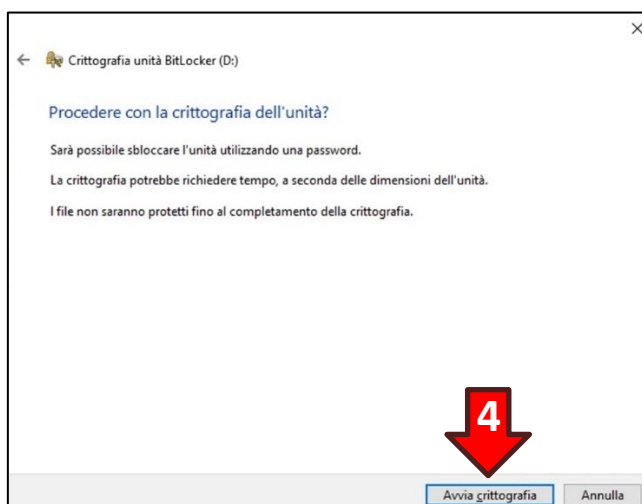
Dopo aver salvato la chiave di ripristino cliccare il tasto **Avanti (1)**:



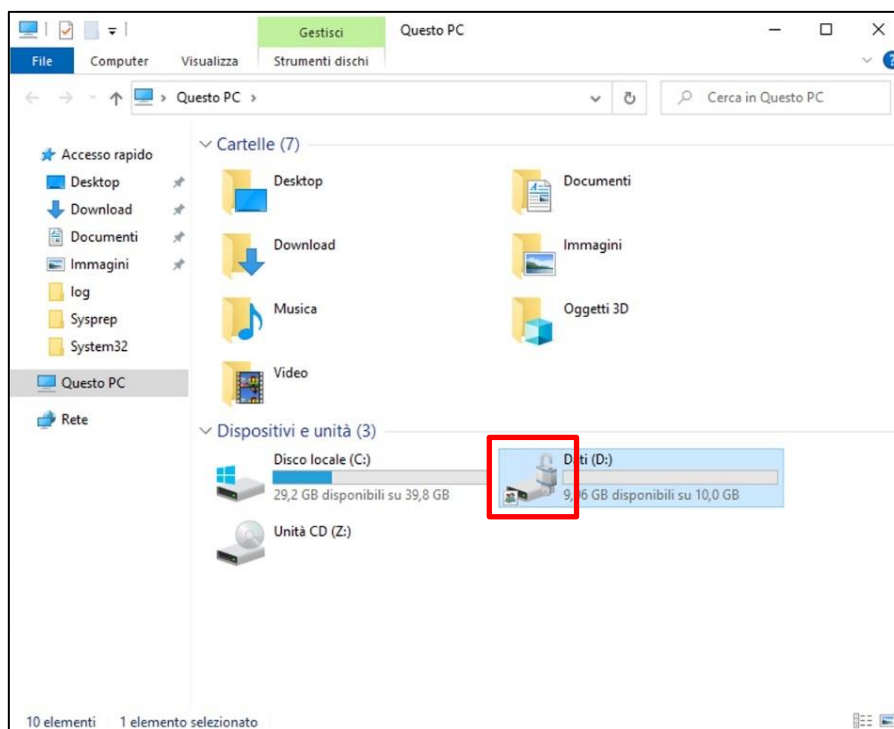
Nella finestra successiva accertarsi che sia spuntata l'opzione **Nuova modalità di crittografia...** (2) quindi cliccare il tasto **Avanti (3)**:



Infine nell'ultima finestra cliccare il tasto **Avvia crittografia (4)**:



Trascorso qualche istante sull'icona della partizione Dati apparirà un lucchetto grigio in posizione aperta:



ATTENZIONE! Prima di utilizzare la partizione dati cifrata con BitLocker è fortemente consigliato di bloccare la partizione (Paragrafo 8.2 Blocco dell'accesso alla partizione cifrata con BitLocker) e bloccare nuovamente la partizione (Paragrafo 8.3 Nuovo accesso alla partizione cifrata con BitLocker) per verificare il corretto funzionamento del dispositivo sicuro.

ATTENZIONE! Se si dispone di una stampante è preferibile conservare la *Chiave di ripristino BitLocker* su carta invece che su un dispositivo digitale. Si ricorda che la *Chiave di ripristino BitLocker* è un file di testo ispezionabile anche con il Blocco Note.

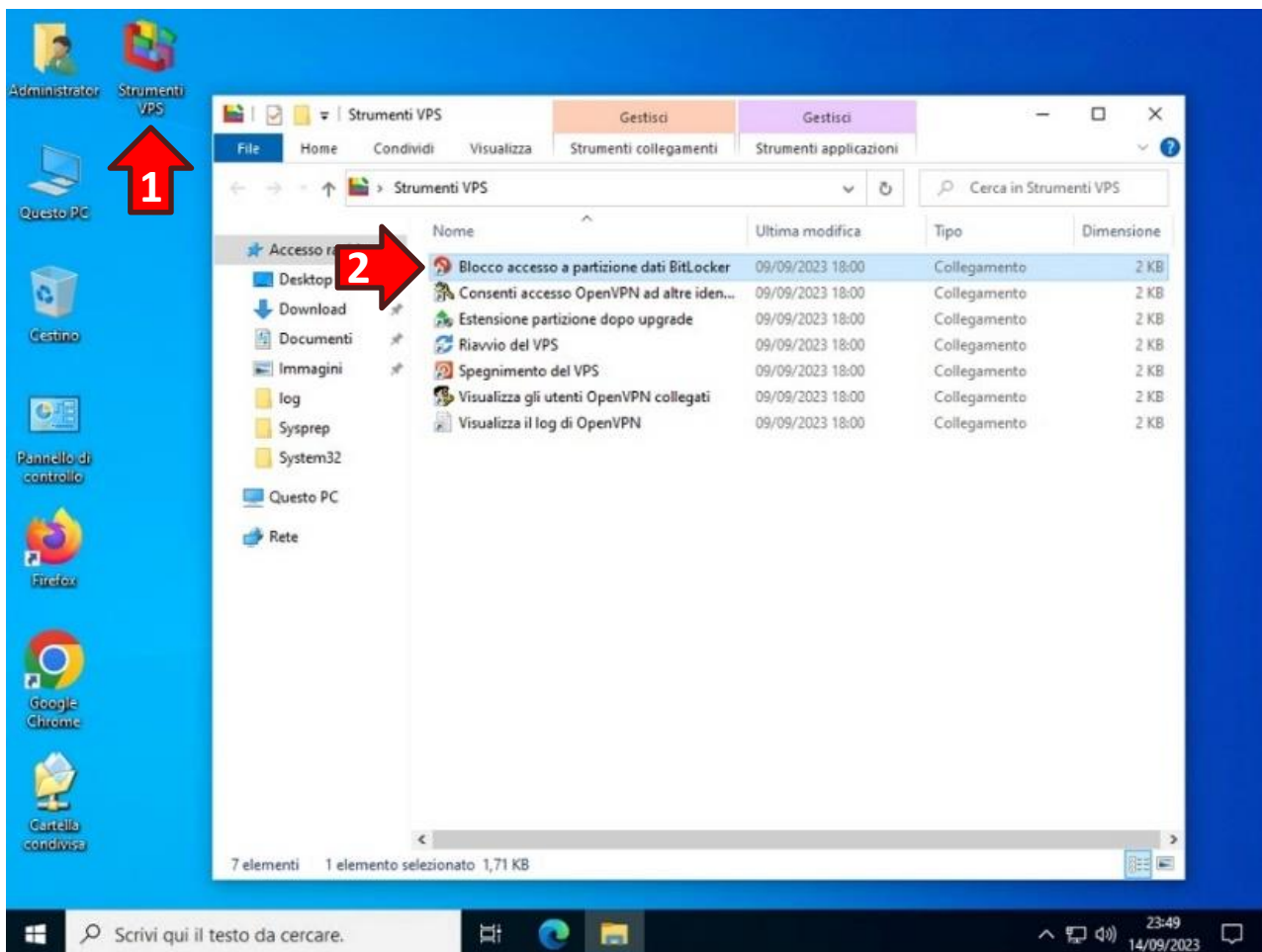
ATTENZIONE! La *Chiave di ripristino BitLocker* è indispensabile in caso di smarrimento della password di accesso all'unità BitLocker quindi conservarla in un luogo sicuro.

ATTENZIONE! In caso di smarrimento sia della password di accesso all'unità BitLocker che della *Chiave di ripristino BitLocker* neppure il fornitore del vostro VPS non sarà in grado di recuperare i dati contenuti nella partizione cifrata e questi dovranno essere considerati definitivamente perduti.

8.2 Blocco dell'accesso alla partizione cifrata con BitLocker

Una volta effettuata la copia sicura dei dati sensibili è consigliabile bloccare l'accesso alla partizione cifrata finché non sarà necessario accedere nuovamente a tali dati.

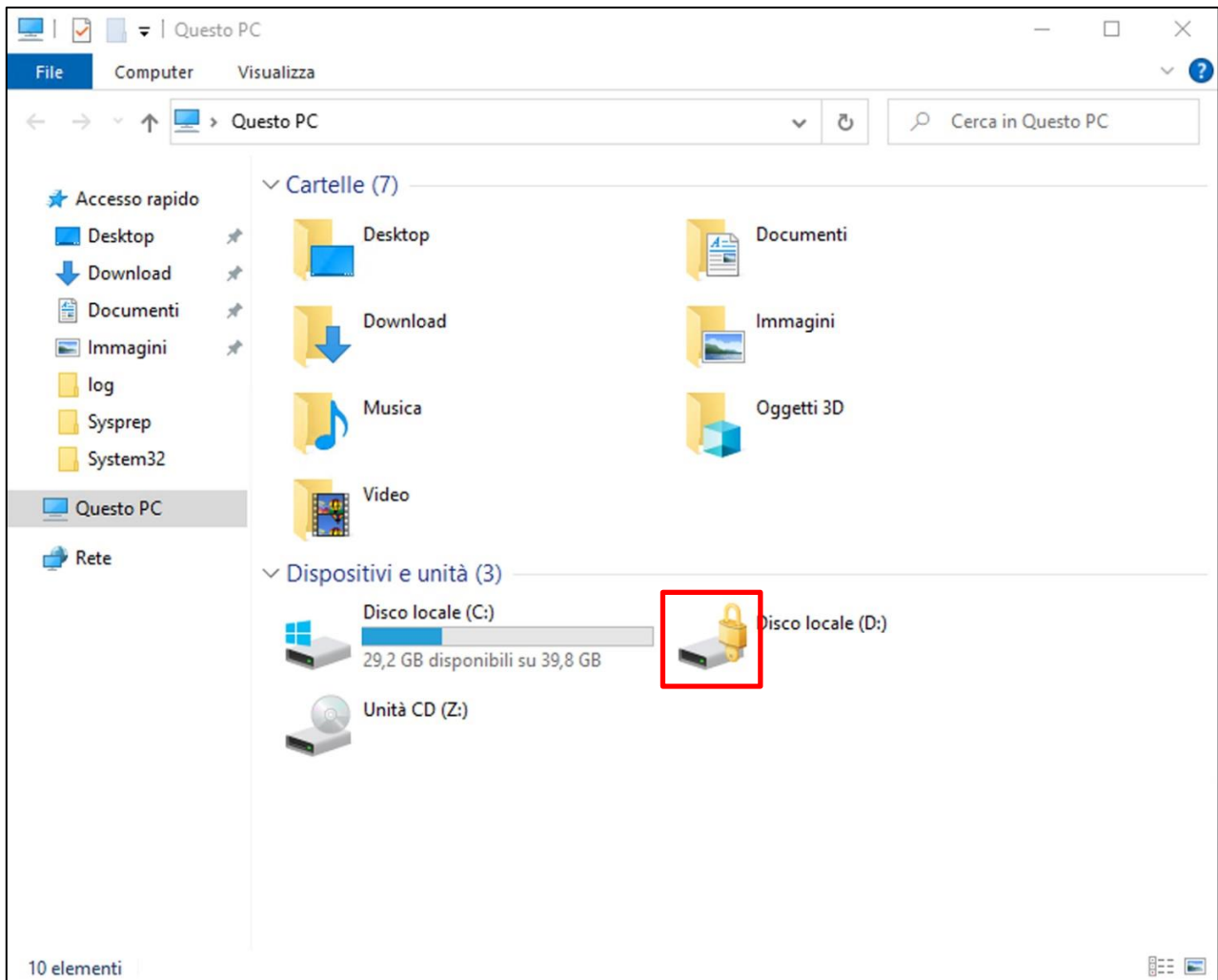
Per effettuare il blocco fare doppio click sull'icona **Strumenti VPS (1)** presente sul desktop del VPS. Si aprirà una nuova finestra con un elenco di strumenti, quindi fare doppio click sulla voce **Blocco accesso a partizione dati BitLocker (2)**:



Confermare la richiesta di apportare modifiche al dispositivo cliccando il tasto **Sì (3)**:



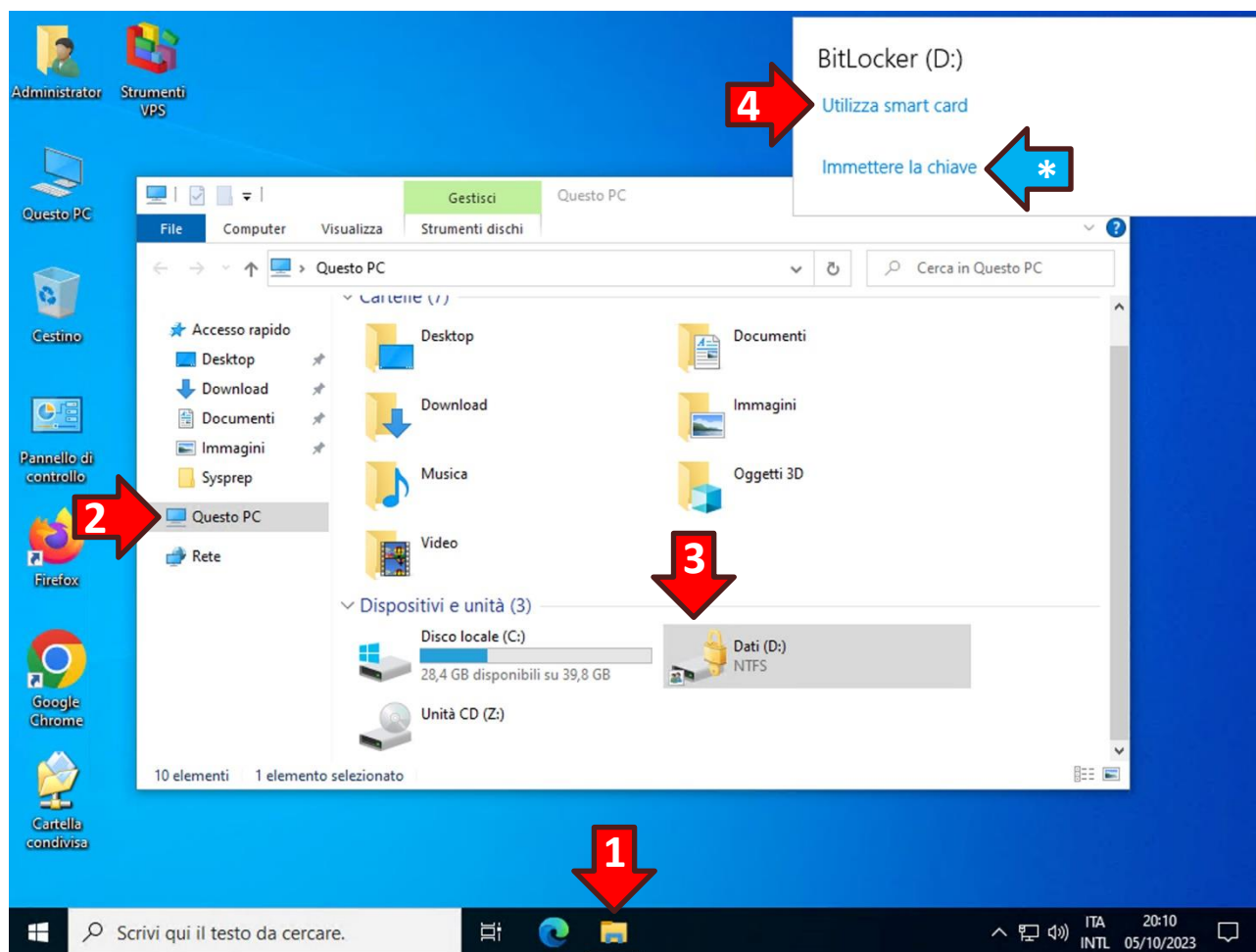
Ora nella finestra **Esplora Risorse** nell'icona dell'unità della partizione dati sarà presente un lucchetto dorato in posizione chiusa:



8.3 Nuovo accesso alla partizione cifrata con BitLocker

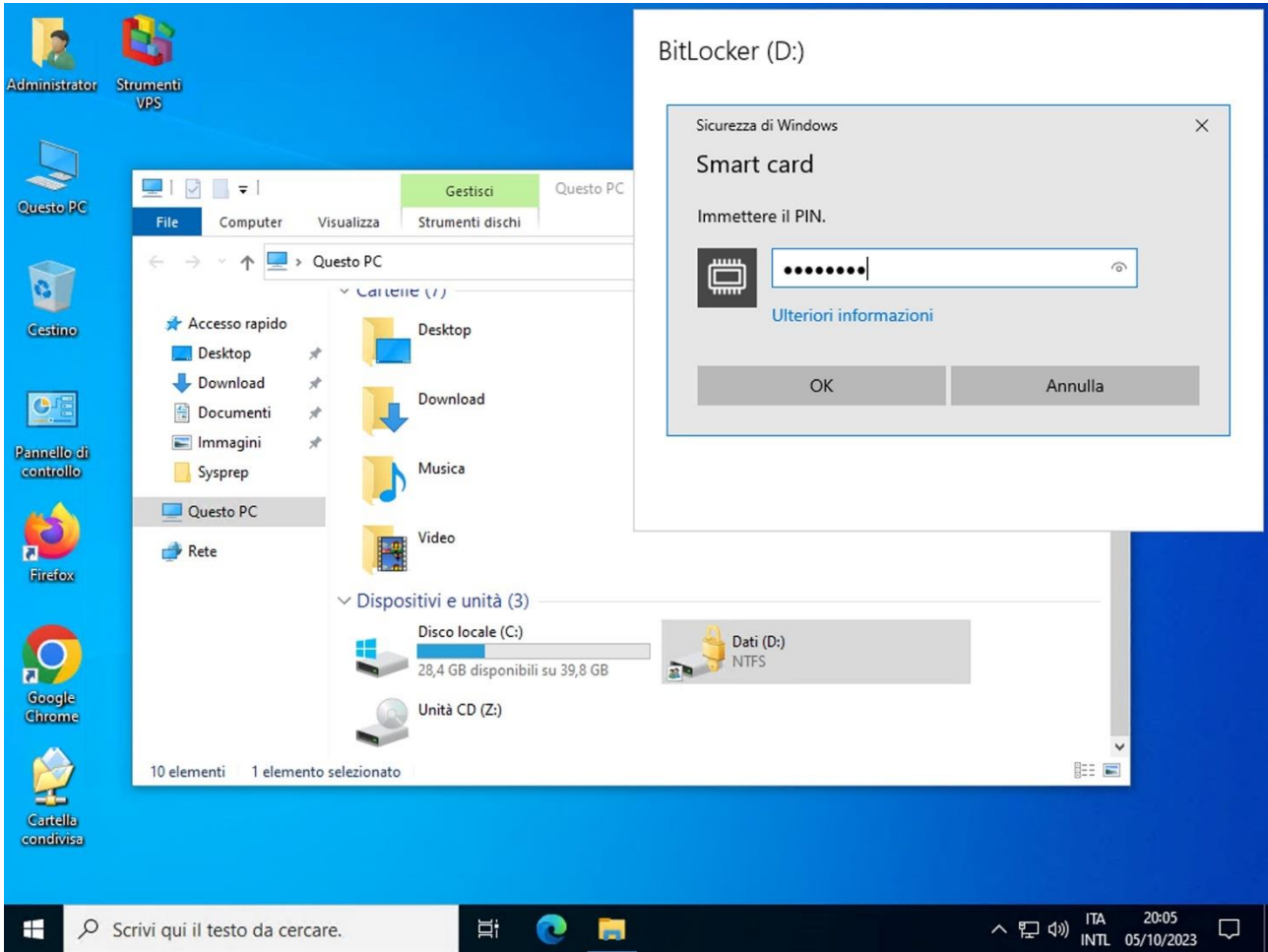
Per accedere nuovamente alla partizione cifrata BitLocker è necessario aprire **Esplora Risorse (1)** dalla barra delle applicazioni, poi cliccare sull'opzione **Questo PC (2)** nella sezione di destra e fare doppio click sull'icona della **partizione dati (3)**.

A questo punto, nel riquadro bianco in alto a destra, cliccare sulla dicitura **Utilizza smart card (4)**:



ATTENZIONE! In caso di smarrimento della password è possibile utilizzare la *Chiave di ripristino BitLocker* cliccando sulla dicitura blu **Immettere la chiave (*)**.

Inserire il PIN del dispositivo sicuro per accedere alla partizione dati:



8.4 Aggiunta di una seconda smart card per l'accesso alla partizione BitLocker

ATTENZIONE! L'accesso alla partizione BitLocker non è in alcun modo correlato all'identità digitale del certificato (UPN). Ciò significa che un certificato diverso da quello utilizzato per cifrare la partizione non riuscirà sbloccarla anche se contiene il medesimo UPN.

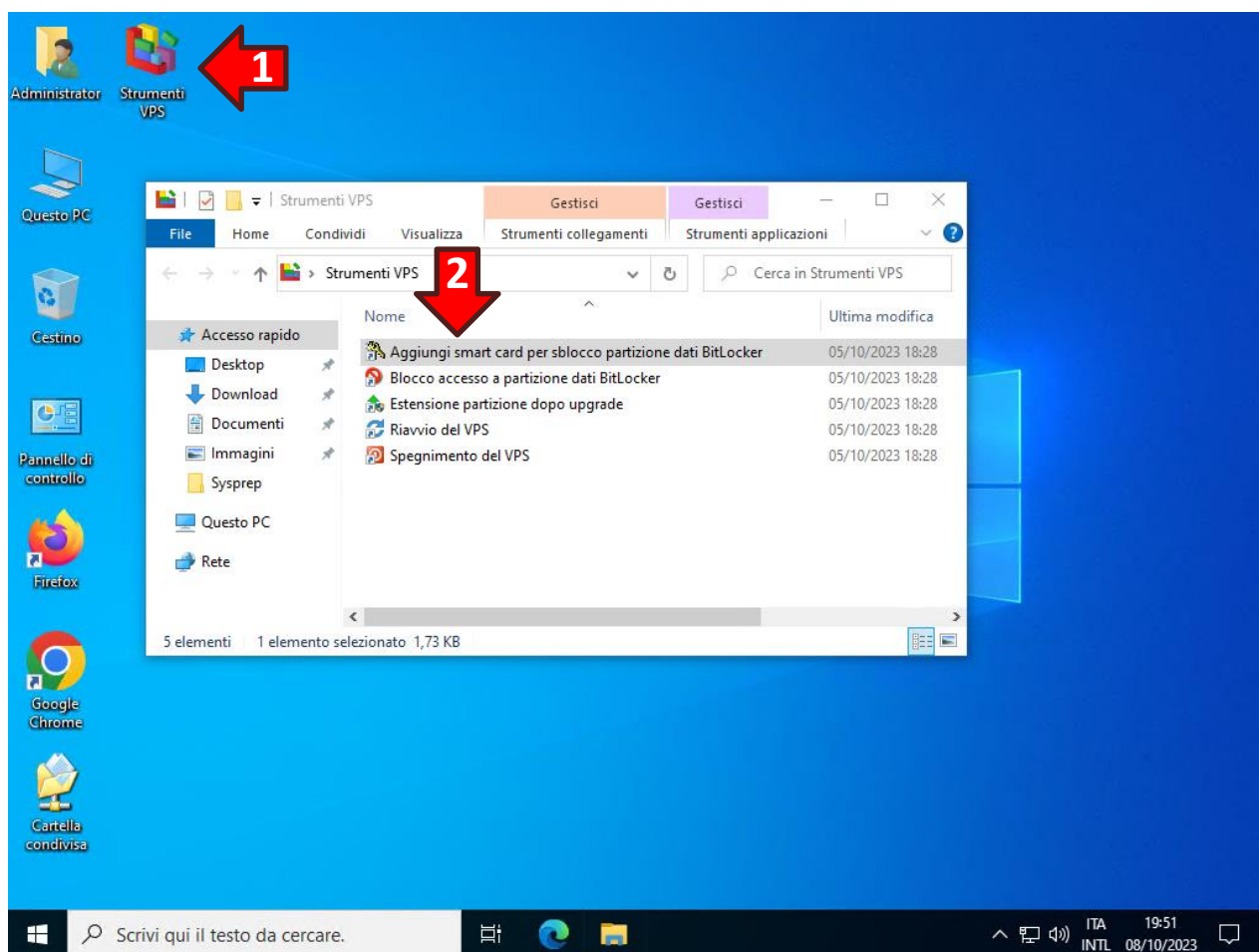
È comunque possibile aggiungere uno o più certificati a protezione della partizione cifrata con BitLocker seguendo la procedura seguente:

Accedere al desktop del VPS con il dispositivo sicuro con cui si è cifrata la partizione BitLocker e sbloccare la partizione.

ATTENZIONE! Per aggiungere un nuovo certificato a protezione della partizione è indispensabile che questa sia stata precedentemente sbloccata con un certificato valido.

Ora accedere al desktop del VPS con il nuovo dispositivo sicuro che dovrà essere abilitato per lo sblocco della partizione BitLocker.

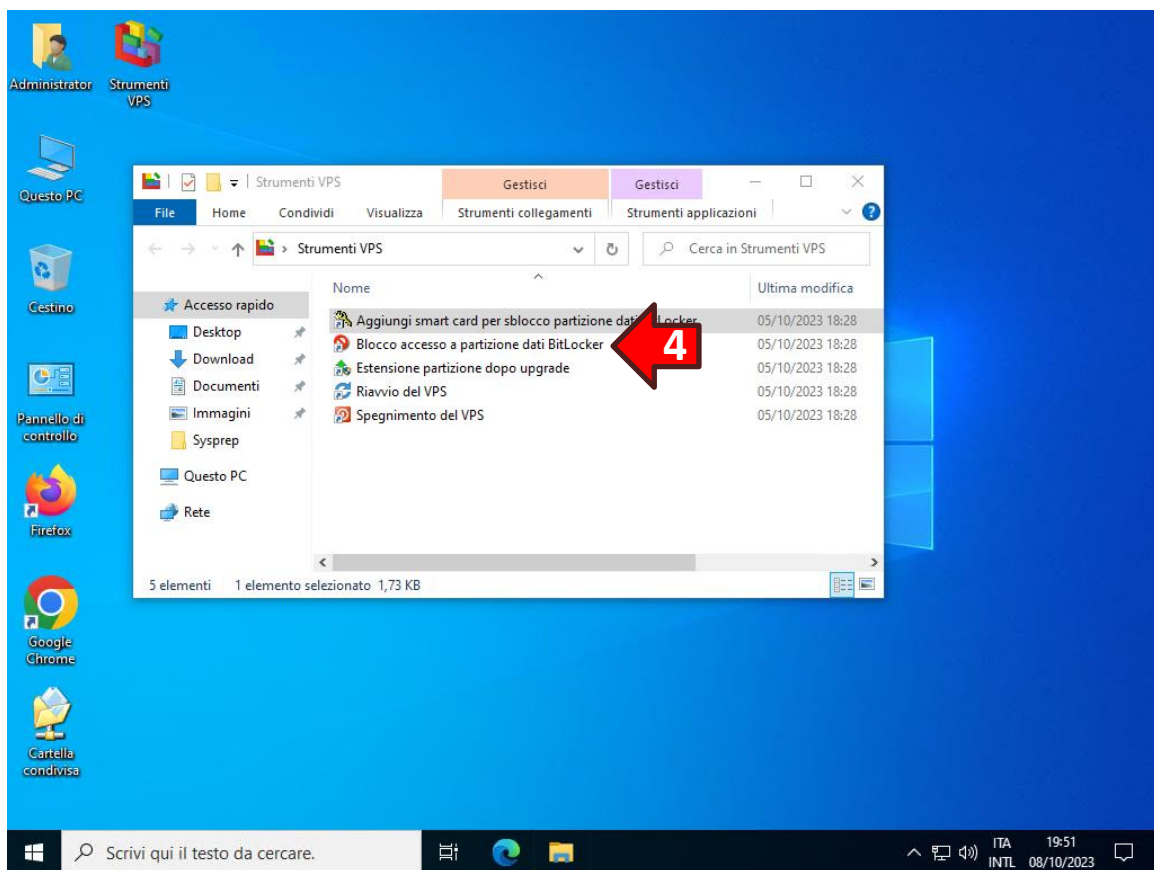
Aprire la cartella **Strumenti VPS (1)** ed eseguire il programma **Aggiungi smart card per sblocco partizione dati BitLocker (2)**:



Confermare la richiesta di apportare modifiche al dispositivo cliccando il tasto **Sì (3)**:



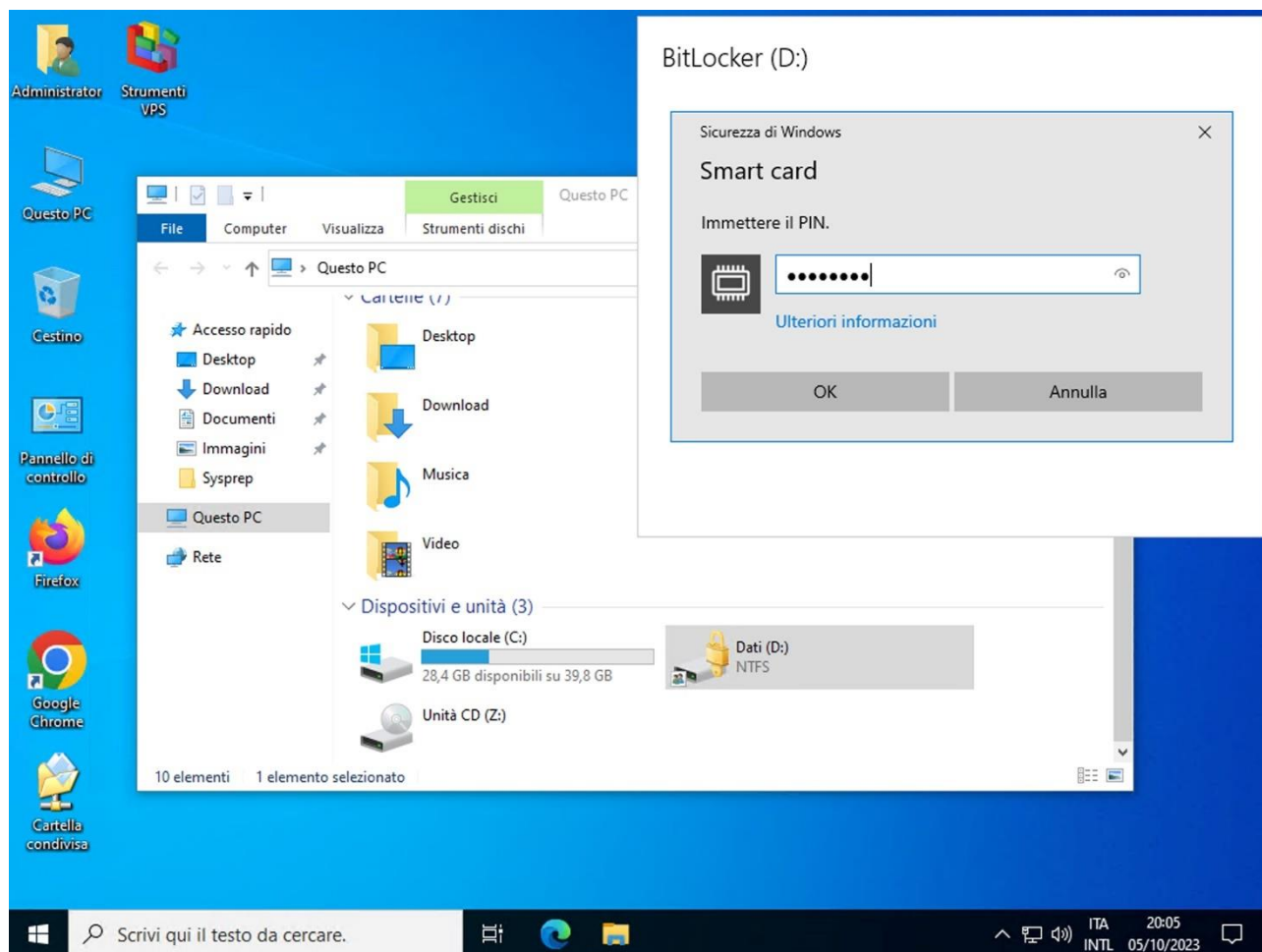
Bloccare la partizione BitLocker con il programma **Blocco accesso a partizione dati BitLocker (4)**:



Confermare la richiesta di apportare modifiche al dispositivo cliccando il tasto **Sì (5)**:



Ora provare a sbloccare la partizione BitLocker con il nuovo dispositivo sicuro:



Se le operazioni si sono svolte correttamente la partizione verrà sbloccata con il nuovo dispositivo sicuro.

Procedura manuale

Senza utilizzare l'apposita applicazione all'interno della cartella *Strumenti VPS* è possibile aggiungere una smart card per sbloccare la partizione BitLocker digitando il seguente comando da una finestra *Prompt dei comandi* con diritti di amministrazione:

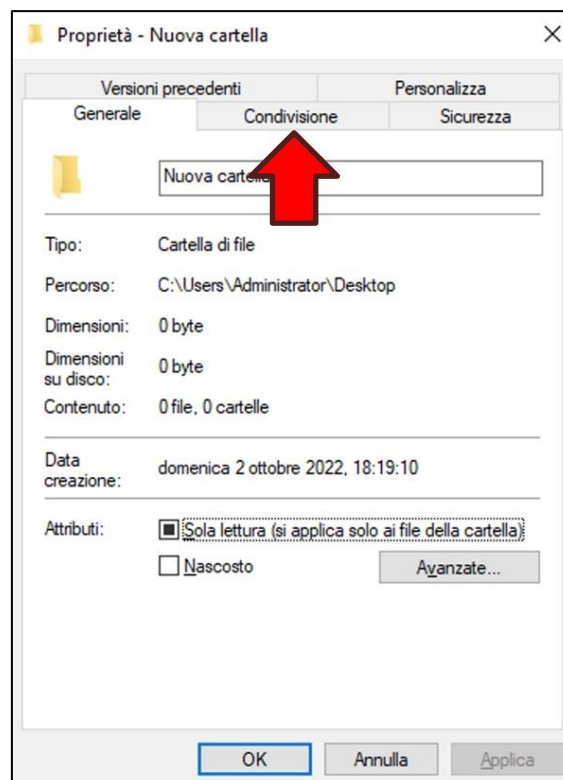
```
manage-bde -protectors -add d: -certificate
```

9. Creazione di una nuova condivisione di rete

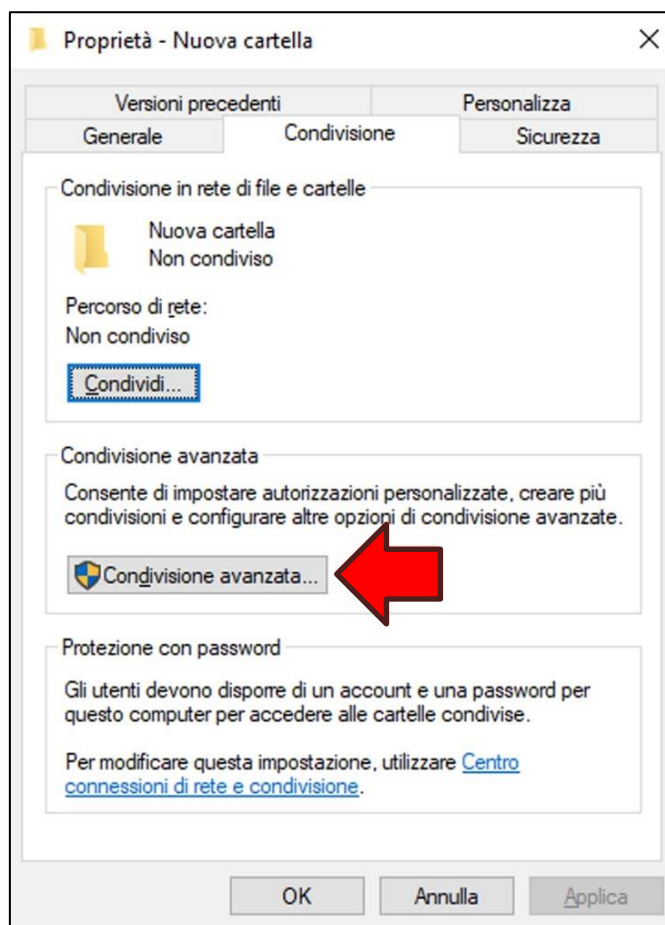
Per creare una nuova connettersi al Desktop Remoto del VPS e creare una nuova cartella sul desktop dell'utente *Administrator*. Poi con il tasto destro del mouse cliccare sopra la cartella appena creata e dal menu popup scegliere l'opzione **Proprietà**:



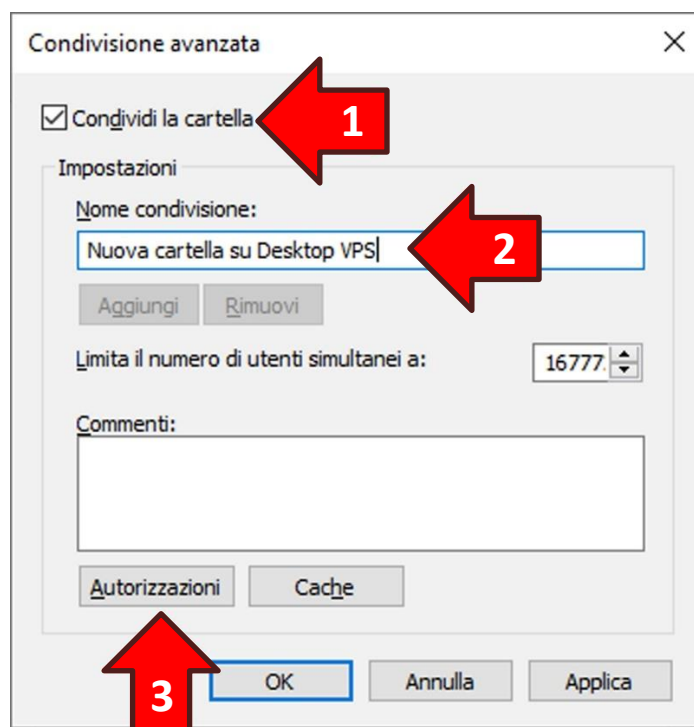
Dalla finestra *Proprietà* cliccare sulla sezione **Condivisione**:



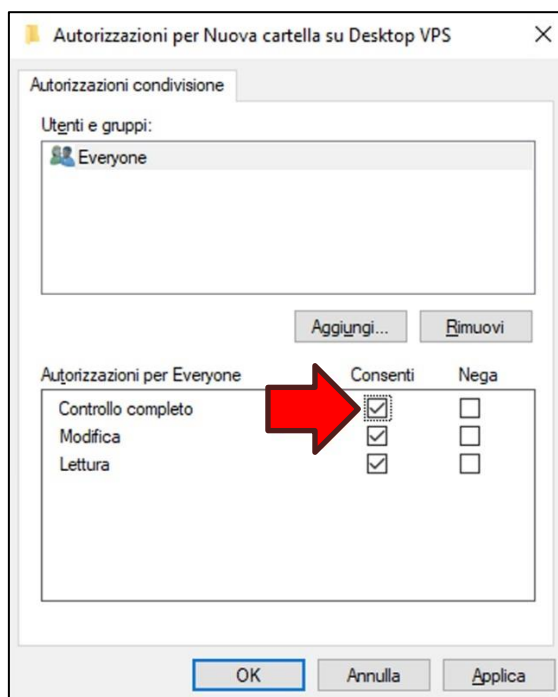
Cliccare quindi il tasto **Condivisione avanzata...**:



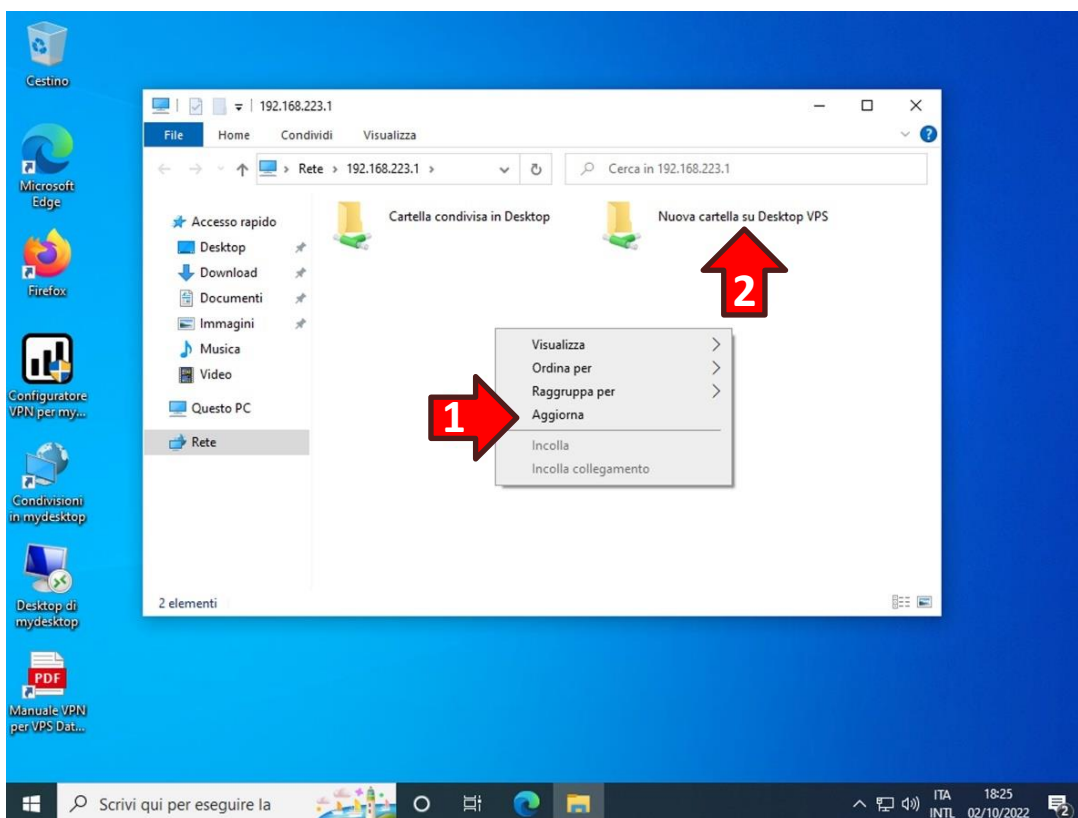
Spuntare l'opzione **Condividi la cartella (1)**, poi impostare il valore **Nome condivisione (2)** (Esempio: Nuova cartella su Desktop VPS) e successivamente cliccare il tasto **Autorizzazioni (3)**;



Nella finestra *Autorizzazioni* spuntare l'opzione **Controllo completo** nella colonna *Consenti*. Quindi cliccare il tasto **OK** sia della finestra corrente che delle finestre sottostanti:



Ora, facendo doppio click sull'icona **Condivisioni in <nome del vostro VPS>** (Esempio: **Condivisioni in mydesktop**) sul desktop del proprio PC, cliccando con il tasto destro del mouse all'interno del riquadro di destra della nuova finestra e scegliendo l'opzione **Aggiorna (1)** dal menu popup si noterà la nuova condivisione **(2)**:

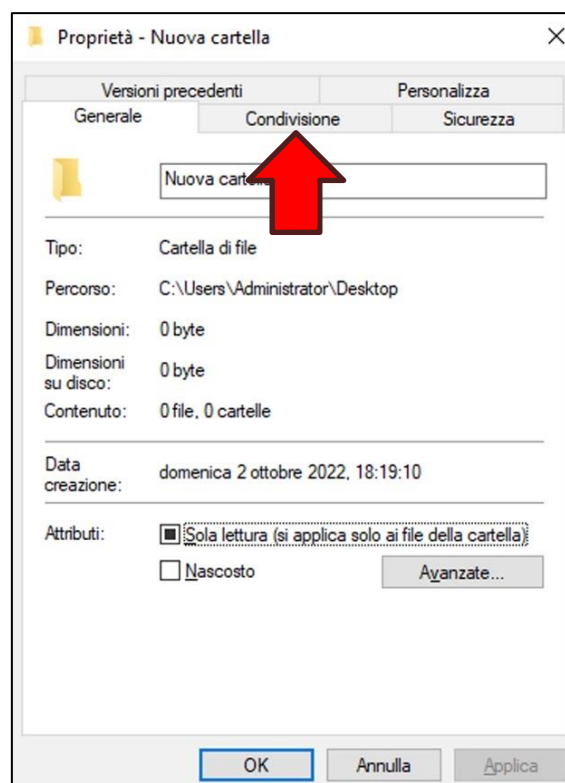


10. Rimozione di una condivisione di rete

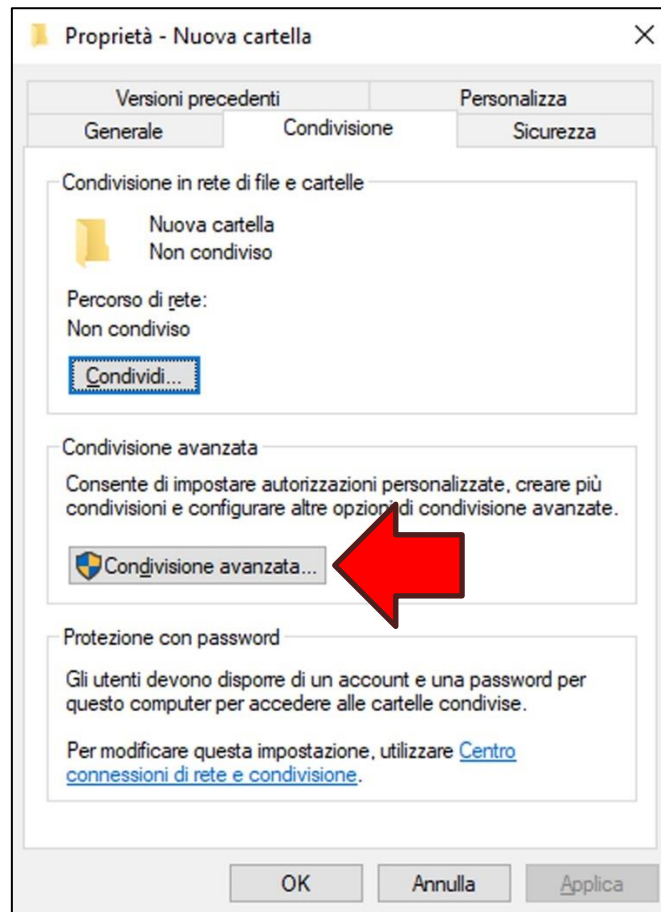
Per rimuovere una condivisione di rete attiva all'interno del VPS connettersi al Desktop Remoto del VPS. Poi con il tasto destro del mouse cliccare sopra la cartella per la quale si vuole rimuovere la condivisione e dal menu popup scegliere l'opzione **Proprietà**:



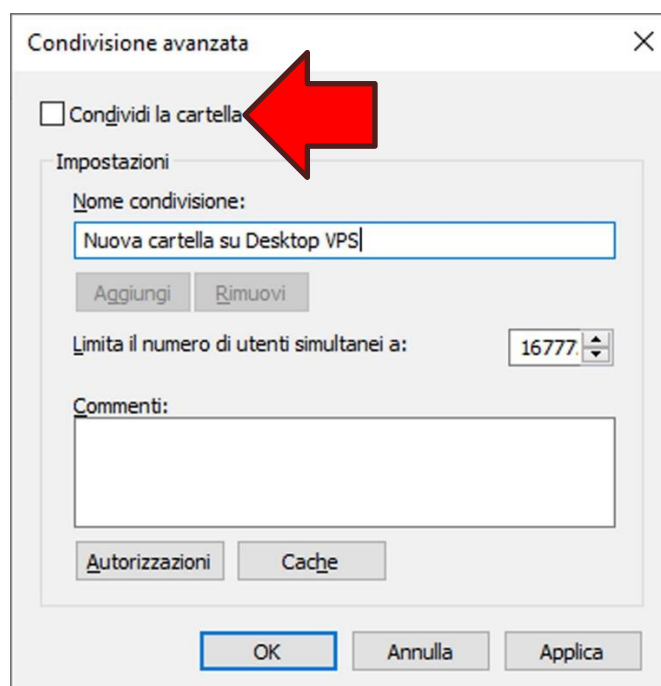
Dalla finestra *Proprietà* cliccare sulla sezione **Condivisione**:



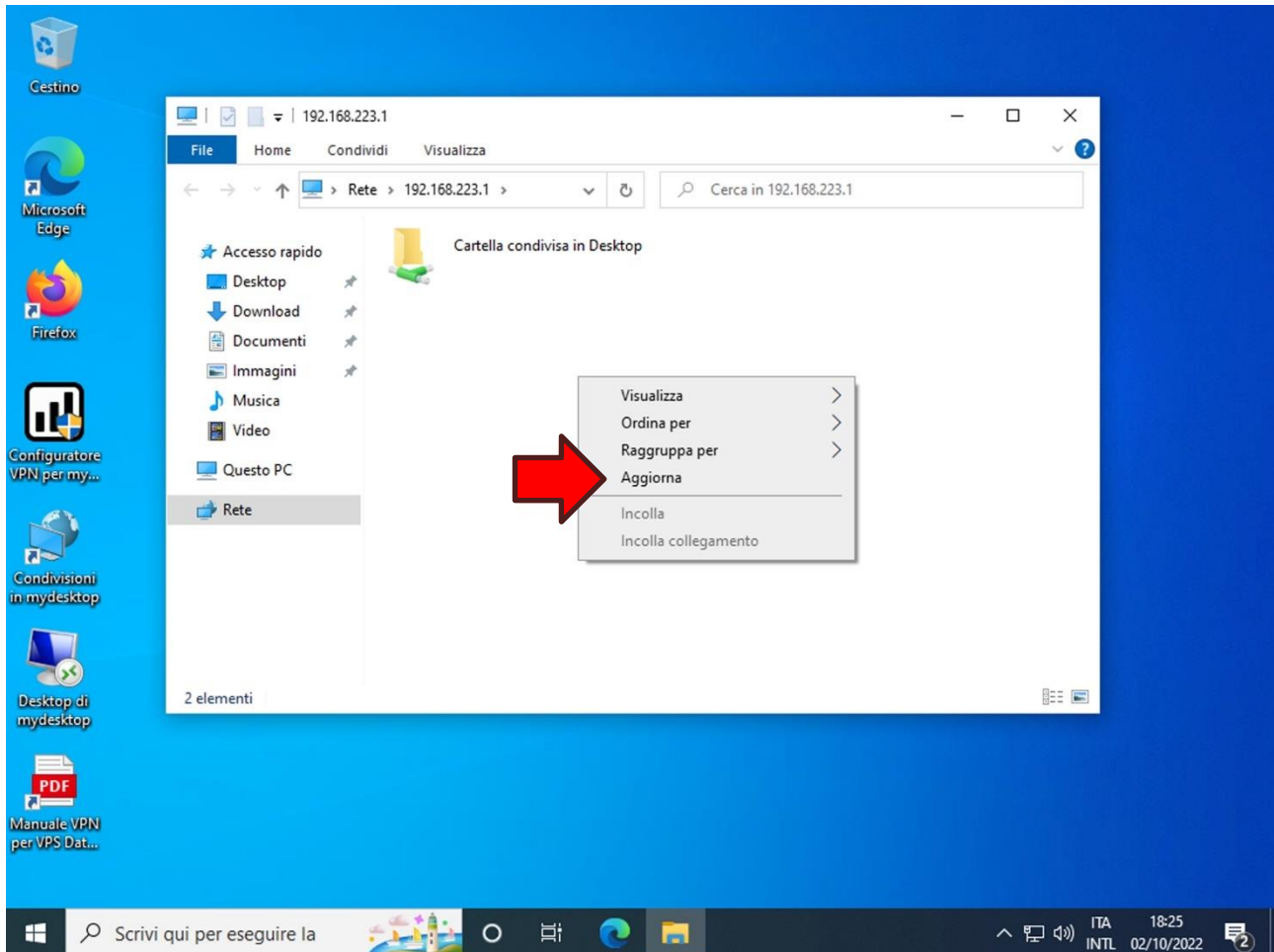
Cliccare quindi il tasto **Condivisione avanzata...**;



Togliere la spunta sull'opzione **Condividi la cartella** e cliccare il tasto **OK** sia della finestra corrente che della finestra *Proprietà*;



Ora, facendo doppio click sull'icona **Condivisioni in <nome del vostro VPS>** (Esempio: **Condivisioni in mydesktop**) nel desktop del proprio PC, cliccando con il tasto destro del mouse all'interno del riquadro di destra della nuova finestra e scegliendo l'opzione **Aggiorna** dal menu popup si noterà che la condivisione eliminata non è più in elenco:



11. Elenco dei certificati emessi e creazione di un nuovo certificato

ATTENZIONE! Il sito WPanel non memorizza le chiavi private dei certificati client, per cui per consentire l'accesso a più client verso i VPS della serie OpenVPN è necessario emettere un nuovo certificato client con il medesimo UPN del primo certificato.

Cliccare sull'icona dell'utente (1) nella barra in alto e dal pannello laterale che si aprirà cliccare l'opzione **Certificati** (2):

The image shows two screenshots of the WPanel web interface. The top screenshot shows the main navigation bar with a user profile icon in the top right corner, indicated by a red arrow labeled '1'. The bottom screenshot shows the user profile menu open on the right side of the page, with the 'Certificati' option highlighted and indicated by a red arrow labeled '2'. The main content area shows a list of VPS under the heading 'Elenco VPS' and a detailed view of a VPS named 'mydesktop.utent-kdzh.wpanel.io' with its status and resource usage.

Dalla sezione *Certificati* è possibile:

- creare un nuovo certificato per dispositivo sicuro attraverso una procedura guidata: cliccare il tasto rosso **Crea nuovo (1)** e selezionare l'opzione **Crea certificato per smart card (2)**;
- creare un nuovo certificato client per l'accesso ai VPS della serie OpenVPN: cliccare il tasto rosso **Crea nuovo (1)** e selezionare l'opzione **Crea nuovo certificato client (3)**;
- abilitare/disabilitare l'**accesso sicuro al sito WPanel (4)** con uno specifico certificato per dispositivo sicuro;
- verificare se un certificato per dispositivo sicuro è abilitato all'uso di **BitLocker (5)**;
- **riscaricare (6)** la procedura per l'installazione automatica di un certificato su un dispositivo sicuro. Il file zip dell'installazione contiene anche i file necessari alla procedura manuale;
- **riscaricare (7)** un certificato client emesso contenente solo la chiave pubblica;

The screenshot shows the 'Certificati' (Certificates) section of the WPanel interface. The page title is 'Certificati rilasciati'. There are three certificates listed in a table. The interface includes a navigation menu with 'Home', 'Gestione VPS', 'Account', 'Certificati', and 'Fatturazione'. A 'Crea nuovo' (Create new) button is highlighted with a red arrow and the number 1. A dropdown menu is open, showing 'Crea certificato per smart card' (highlighted with 2) and 'Crea nuovo certificato client' (highlighted with 3). The table has columns for 'Nome', 'Emissione', 'Seriale', 'User Principal Name', 'Login sito', 'BitLocker', 'Algoritmo', and 'Dim'. The 'Login sito' and 'BitLocker' columns have checkboxes. The first two certificates have their 'Login sito' checkboxes checked (highlighted with 4) and 'BitLocker' checkboxes checked (highlighted with 5). The third certificate has its 'Login sito' checkbox unchecked. The 'Download' buttons for the second and third certificates are highlighted with 6 and 7 respectively.

Nome	Emissione	Seriale	User Principal Name	Login sito	BitLocker	Algoritmo	Dim
Identita digitale WPanel	05/10/2023	01	utente.di.prova@utente-kdzgh.wpanel.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RSA	
Identita 2	08/10/2023	05	utente.di.prova@utente-kdzgh.wpanel.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RSA	2048
Certificato client WPanel	09/10/2023	06	utente.di.prova@utente-kdzgh.wpanel.local	<input type="checkbox"/>		RSA	2048

12. Creazione manuale della Virtual Smart Card per TPM

ATTENZIONE! Se sul vostro PC è stato preinstallato Windows 11 allora sarà sicuramente presente il dispositivo TPM 2.0.

ATTENZIONE! È possibile utilizzare la Virtual Smart Card anche con un TPM 1.1 (presente in alcuni PC desktop meno recenti).

ATTENZIONE! La Virtual Smart Card non supporta alcune funzionalità richieste dal protocollo TLS 1.3. Se le proprie politiche aziendali impongono l'utilizzo di questo protocollo è indispensabile acquistare un dispositivo sicuro come una smart card o un token USB con supporto PKCS#11.

ATTENZIONE! I comandi seguenti vanno eseguiti in una finestra *Prompt dei comandi* con diritti di amministrazione.

Per verificare se sul proprio PC è presente un TPM (Trusted Platform Module) digitare:

```
wmic.exe /namespace:\\root\CIMV2\Security\MicrosoftTpm path Win32_Tpm get /value
```

Se l'output è simile al seguente allora il vostro PC è presente un TPM:

```
C:\WINDOWS\system32> wmic /namespace:\\root\CIMV2\Security\MicrosoftTpm path Win32_Tpm get /value

IsActivated_InitialValue=TRUE
IsEnabled_InitialValue=TRUE
IsOwned_InitialValue=TRUE
ManufacturerId=1234567890
ManufacturerIdTxt=CST
ManufacturerVersion=2.0.0.1
ManufacturerVersionFull20=2.0.0.1
ManufacturerVersionInfo=Custom TPM2
PhysicalPresenceVersionInfo=1.3
SpecVersion=2.0, 0, 1.16
```

Se invece dovesse apparire questo output allora sul vostro PC non è installato alcun TPM:

```
C:\WINDOWS\system32> wmic /namespace:\\root\CIMV2\Security\MicrosoftTpm path Win32_Tpm get /value

Non vi sono istanze disponibili.
```

Se sul vostro PC è presente un TPM allora verificare se esiste già un'istanza Microsoft Virtual Smart Card digitando il seguente comando:

```
wmic path win32_PnPEntity where "ClassGuid like '{50DD5230-BA8A-11D1-BF5D-0000F805F530}'" get DeviceID,Name,Status
```

Se dovesse apparire questo output allora sul vostro PC è già presente la Virtual Smart Card quindi non sono necessarie ulteriori operazioni:

```
C:\WINDOWS\system32> wmic path win32_PnPEntity where "ClassGuid like '{50DD5230-BA8A-11D1-BF5D-0000F805F530}'" get DeviceID,Name,Status
```

DeviceID	Name	Status
ROOT\SMARTCARDREADER\0000	WPanel Virtual Smart Card	OK

Al contrario se dovesse apparire questo output allora è necessario creare la Virtual Smart Card:

```
C:\WINDOWS\system32> wmic path win32_PnPEntity where "ClassGuid like '{50DD5230-BA8A-11D1-BF5D-0000F805F530}'" get DeviceID,Name,Status
```

Non vi sono istanze disponibili.

Per la Virtual Smart Card sul proprio PC digitare il comando:

```
tpmvmgr.exe create /name "WPanel Virtual Smart Card" /AdminKey RANDOM /PIN PROMPT /PUK PROMPT /generate
```

e digitare e confermare un PIN e un PUK quando richiesto (PIN e PUK possono contenere numeri, lettere e simboli e devono avere una lunghezza minima di 8 caratteri):

```
C:\WINDOWS\system32> tpmvmgr.exe create /name "WPanel Virtual Smart Card" /AdminKey RANDOM /PIN PROMPT /PUK PROMPT /generate
PIN:
*****
Conferma PIN:
*****
Immettere il PUK:
*****
Conferma PUK:
*****
Creazione della smart card TPM in corso...
Inizializzazione del componente Smart card virtuale in corso...
Creazione del componente Smart card virtuale in corso...
Inizializzazione del simulatore di smart card virtuale in corso...
Creazione del simulatore di smart card virtuale in corso...
Inizializzazione del lettore di smart card virtuale in corso...
Creazione del lettore di smart card virtuale in corso...
In attesa del dispositivo smart card TPM...
Autenticazione per la smart card TPM in corso...
Generazione del file system nella smart card TPM in corso...
Smart card TPM creata.
ID istanza dispositivo lettore di smart card = ROOT\SMARTCARDREADER\0000
```

Eliminazione di una Virtual Smart Card

Esiste un comando per eliminare la Virtual Smart Card dal proprio PC cancellando così tutte le coppie di chiavi e tutti i certificati contenuti all'interno.

ATTENZIONE! L'eliminazione è un'operazione irreversibile! Dopo l'eliminazione non sarà più possibile recuperare le chiavi e/o i certificati.

Per eliminare la Virtual Smart Card dal proprio PC digitare il comando:

```
tpmvscmgr.exe destroy /instance ROOT\SMARTCARDREADER\0000
```

e attendere il seguente output di conferma:

```
C:\Windows\system32> tpmvscmgr.exe destroy /instance ROOT\SMARTCARDREADER\0000
Distruzione della smart card TPM in corso...
Inizializzazione del lettore di smart card virtuale in corso...
Eliminazione del lettore di smart card virtuale in corso...
Inizializzazione del simulatore di smart card virtuale in corso...
Eliminazione del simulatore di smart card virtuale in corso...
Inizializzazione del componente Smart card virtuale in corso...
Eliminazione del componente Smart card virtuale in corso...
Smart card TPM eliminata.
```


13. Cambio del PIN e riattivazione del dispositivo sicuro tramite PUK

ATTENZIONE! Non esiste in Windows un comando specifico per cambiare il PIN di un dispositivo sicuro. Solitamente i produttori di dispositivi sicuri rilasciano propri software per il cambio del PIN o lo sblocco del dispositivo tramite PUK.

È possibile utilizzare sul proprio PC uno strumento open source gratuito, chiamato *OpenSC*, per cambiare il PIN o sbloccare il dispositivo con il PUK.

ATTENZIONE! Se si sta utilizzando la Microsoft Virtual Smart Card è indispensabile utilizzare questo strumento.

È possibile scaricare il file di installazione di OpenSC dal seguente indirizzo:

<https://github.com/OpenSC/OpenSC/releases>

Scorrere la pagina verso il basso fino a trovare il link per scaricare il file:

- **per versioni di Windows a 64 bit** (più diffuso): OpenSC-<versione più recente>_win64.msi
(esempio: *OpenSC-0.23.0_win64.msi*);
- **per versioni di Windows a 32 bit**: OpenSC-< versione più recente >_win32.msi
(esempio: *OpenSC-0.23.0_win32.msi*).

Completata l'installazione digitare il seguente comando da una finestra del *Prompt dei comandi*:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs15-tool.exe" --change-pin
```

poi digitare:

- il vecchio PIN e premere **INVIO**;
- il nuovo PIN e premere **INVIO**;
- nuovamente il nuovo PIN per conferma e premere **INVIO**.

```
C:\Users\Utente\Desktop> "C:\Program Files\OpenSC Project\OpenSC\tools\pkcs15-  
tool.exe" --change-pin  
  
Using reader with a card: Microsoft Virtual Smart Card 0  
  
Enter old PIN [UserPIN]: Enter new PIN [UserPIN]: Enter new PIN again [UserPIN]:
```

Sblocco del dispositivo sicuro tramite PUK

L'inserimento ripetuto di un PIN errato potrebbe bloccare il dispositivo sicuro, sia esso una Virtual Smart Card o una smart card/token USB.



Per sbloccare il dispositivo sicuro con il software OpenSC digitare il seguente comando in una finestra *Prompt dei comandi*:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs15-tool.exe" -u
```

poi digitare:

- il PUK e premere **INVIO**;
- il nuovo PIN e premere **INVIO**;
- nuovamente il nuovo PIN per conferma e premere **INVIO**.

```
C:\Users\Utente\Desktop> "C:\Program Files\OpenSC Project\OpenSC\tools\pkcs15-tool.exe" -u
```

```
Using reader with a card: Microsoft Virtual Smart Card 0
```

```
Enter PUK [PUK]: Enter new PIN [UserPIN]: Enter new PIN again [UserPIN]:
```

Dispositivi sicuri Yubico

Per cambiare il PIN o sbloccare un dispositivo Yubico si consiglia di utilizzare il software YubiKey Manager scaricabile dal seguente indirizzo:

<https://www.yubico.com/support/download/yubikey-manager/>

14. Creazione manuale dei certificati

È possibile inviare al sito WPanel una *Richiesta di emissione certificato (CSR)* con un nome distintivo (*Distinguished Name*) completamente personalizzato.

Per creare una CSR personalizzata creare un file **request.inf** sul proprio desktop. È possibile utilizzare anche l'applicazione *Blocco Note*. Il file dovrà contenere i seguenti attributi facendo attenzione a sostituire le parti in rosso:

```
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "<Nome distintivo. Deve contenere almeno il nome comune (CN) (es. CN=Identita
Digitale WPanel)>"
KeyLength = 2048
KeyAlgorithm = RSA
KeySpec = AT_KEYEXCHANGE
Exportable = FALSE
MachineKeySet = FALSE
ProviderName = "Microsoft Base Smart Card Crypto Provider"
ProviderType = 1
RequestType = PKCS10
X500NameFlags = 0x20000000
FriendlyName = "<Nome identificativo del certificato (es. Identita Digitale WPanel)>"
```

Ora aprire una finestra *Prompt dei comandi* e, dopo essersi posizionati nella cartella desktop, digitare il comando:

```
certreq.exe -new request.inf request.csr
```

e inserire il PIN del dispositivo sicuro.

Attendere quindi il seguente output di conferma:

```
C:\Users\Utente\Desktop> certreq.exe -new request.inf request.csr
CertReq: Richiesta creata
```

Poi visualizzare il contenuto del file CSR con il comando:

```
notepad.exe request.csr
```

e copiare tutto il contenuto nella clipboard.

Ora seguire la procedura guidata per la creazione di un certificato per smart card indicata nel **Capitolo 11. Elenco dei certificati emessi e creazione di un nuovo certificato** fino alla scheda di caricamento della richiesta di emissione del certificato.

Quindi incollare il contenuto della clipboard all'interno dell'area **destinata all'inserimento della CSR (1)** e cliccare il tasto **Invia richiesta (2)**:

Rilascio nuovo certificato

Cliccare sul tasto seguente per scaricare il file batch contenente la procedura automatica di generazione della richiesta:

File batch creazione richiesta

Una volta generata la richiesta apparirà sullo schermo la finestra del Blocco Note contenente un file di testo. Copiare il file testo utilizzando le combinazioni di tasti **CTRL + A** e **CTRL + C** ed incollarlo nello spazio sottostante con la combinazione di tasti **CTRL + V**. Infine inviare la richiesta.

Se nella pagina precedente è stata utilizzata la procedura manuale trascinare il file **request-crt.csr** nello spazio sottostante oppure cliccare il tasto Seleziona richiesta dal PC per selezionare direttamente il file.

ATTENZIONE! La richiesta deve essere in formato PEM quindi deve contenere l'header **-----BEGIN NEW CERTIFICATE REQUEST-----** ed il footer **-----END NEW CERTIFICATE REQUEST-----**.

```
oV9MoZ8APMsdtWUHIITmLAZ1OQ6d+XN5eU76mBrbhqU4oiqIVmjN30VCizwfiUtNB
N5hjoCveXvILrEjwAQVouW/Z2GUww9tc0NIGZuCyvP...AVHBvfz0mdqmvAT3Hp
mYOe24cHtUuAa0Hpueow6pKIHBwmTCKXTOBakkEq...VGP2mz0FNtvHFgTc
7bbjpaOgbiRdpqxBVcz+H09kciQAxLPq06XPqDY6TY5g...hDP3TUaGFyhs4
xGvvg+eAlt1mkoDCnwbtdQ8=
-----END NEW CERTIFICATE REQUEST-----
```

1

2

Invia richiesta >

Dopo l'emissione del certificato verrà scaricato automaticamente un file ZIP. Scompattare il file nel desktop del proprio PC e con una finestra *Prompt dei comandi* con diritti di amministrazione posizionarsi nella cartella **Procedura manuale** del file scompattato.

Digitare poi il comando:

```
certutil.exe -addstore root "<Nome del vostro fornitore> Internal RSA CA.crt"
```

e attendere il seguente output di conferma:

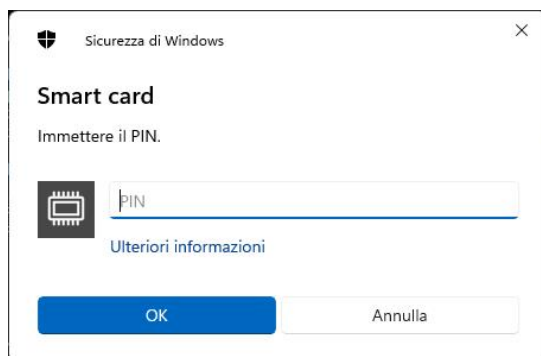
```
C:\Users\Utente\Desktop\Identita Digitale WPanel\Procedura Manuale> certutil.exe
-addstore root "WPanel Internal RSA CA.crt"

root "Autorità di certificazione radice attendibili"
La firma elettronica corrisponde alla chiave pubblica
Il certificato "WPanel Demo Services Root CA" è stato aggiunto all'archivio.
CertUtil: - Esecuzione comando addstore riuscita.
```

Ora digitare il comando:

```
certreq.exe -accept CertificatoEmesso.crt
```

ed inserire il PIN del dispositivo sicuro:



Attendere quindi il seguente output di conferma di inserimento del certificato nel dispositivo sicuro:

```
C:\Users\Utente\Desktop\Identita Digitale WPanel\Procedura manuale> certreq.exe
-accept CertificatoEmesso.crt

Certificato installato:
  Numero di serie: 02
  Soggetto: CN=Certificato personalizzato (Altro nome:Nome
principale=utente.di.prova@utente-kdzgh.wpanel.local)
  NotBefore: 10/10/2023 11:23
  NotAfter: 10/10/2038 11:23
  Identificazione personale: fb8bd01affd2403339beecc7792d5b2f99a36544
```

Configurazione autenticazione Kerberos

Se il PC verrà utilizzato per accedere ai VPS della linea Smart Card è indispensabile configurare il bypass dell'autenticazione Kerberos per la verifica della lista di revoca dei certificati.

ATTENZIONE! Onde precludere l'accesso al vostro VPS in caso di malfunzionamento del sito WPanel del vostro fornitore **non vengono gestite le liste di revoca dei certificati dalla PKI WPanel.**

ATTENZIONE! Senza questa configurazione non sarà possibile accedere al vostro VPS con il dispositivo sicuro.

È necessario quindi digitare il seguente comando da una finestra *Prompt dei comandi* con diritti di amministrazione:

```
reg.exe add HKLM\SYSTEM\CurrentControlSet\Control\LSA\Kerberos\Parameters /v
UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors /t REG_DWORD /d 1 /f
```

15. Mappatura degli UPN agli utenti del VPS

In fase di acquisto di un VPS della linea Smart Card l'utente sceglie un UPN, presente nei certificati emessi, da associare all'utente Administrator. In questo modo il cliente potrà accedere al VPS con tutti i certificati contenente quello specifico UPN.

Il cliente può poi creare nuovi utenti all'interno del dominio del VPS ed associarli ai nuovi certificati emessi mappando l'UPN del certificato all'attributo **userPrincipalName** dell'utente Active Directory. Ciò si rende utile se ad esempio un cliente vuole distribuire più smart card ai dipendenti della propria azienda. L'UPN del certificato viene impostato in una specifica scheda della procedura guidata per l'emissione di un certificato.

ATTENZIONE! Su ogni VPS della linea Smart Card viene preconfigurato il dominio Active Directory univoco per ogni cliente WPanel. Quindi un determinato cliente non può in alcun modo emettere certificati che permettano l'accesso sui VPS di un altro cliente.

È possibile recuperare il **dominio Active Directory univoco (2)** per i propri VPS della linea Smart Card accedendo al sito WPanel del vostro fornitore e cliccare sull'**icona dell'utente (1)** nella barra in alto:

The image consists of two screenshots of the WPanel web interface. The top screenshot shows the user profile icon in the top right corner, highlighted with a red arrow and the number '1'. The bottom screenshot shows the user profile page, with a red box around the 'Dominio per UPN' field and a red arrow pointing to it with the number '2'.

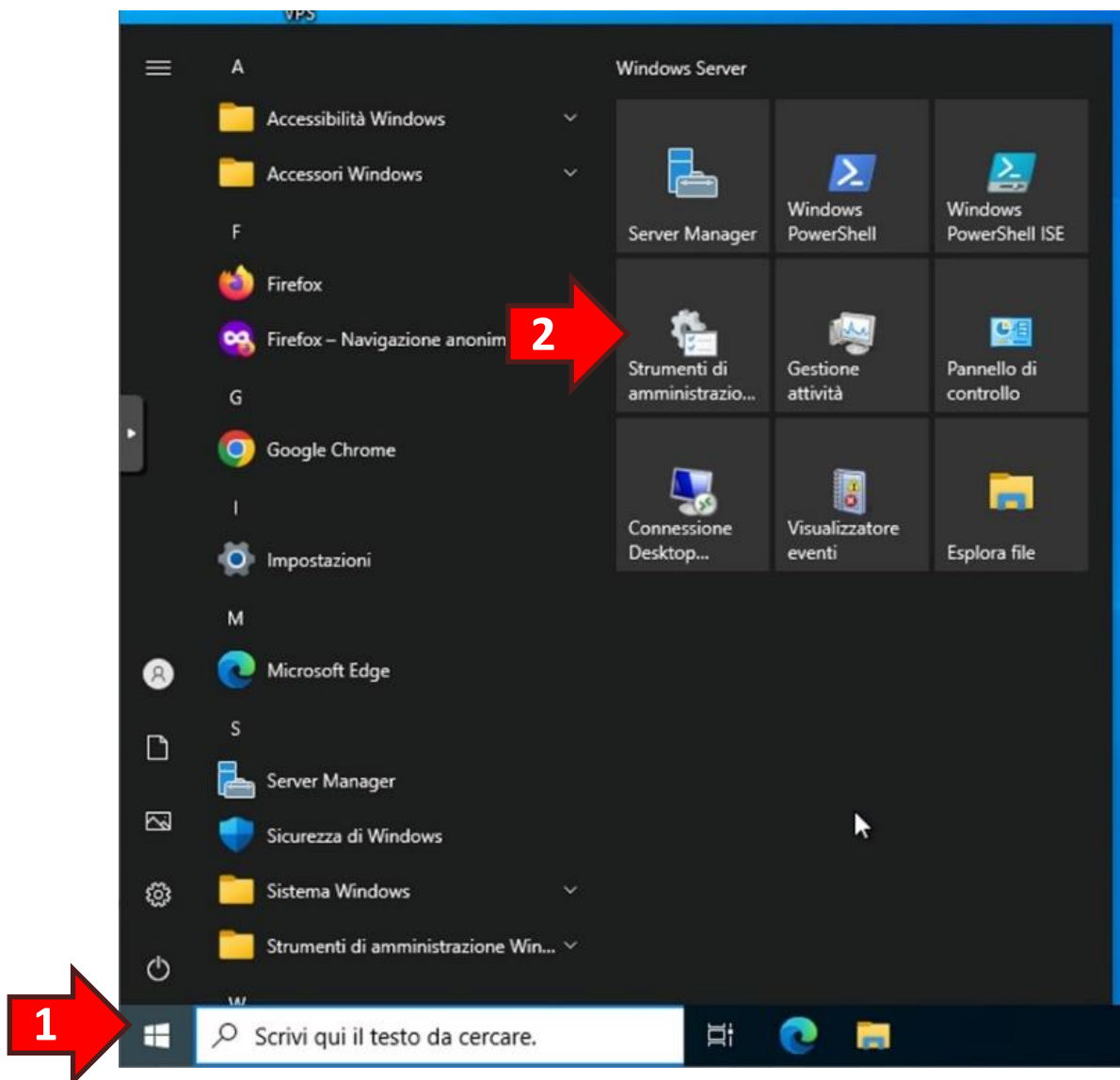
Screenshot 1: Shows the WPanel web interface. The top right corner features a user profile icon (a person silhouette) next to the Italian flag. A red arrow labeled '1' points to this icon.

Screenshot 2: Shows the WPanel web interface with the user profile page open. The 'Dominio per UPN' field is highlighted with a red box, and a red arrow labeled '2' points to it. The profile page includes the following information:

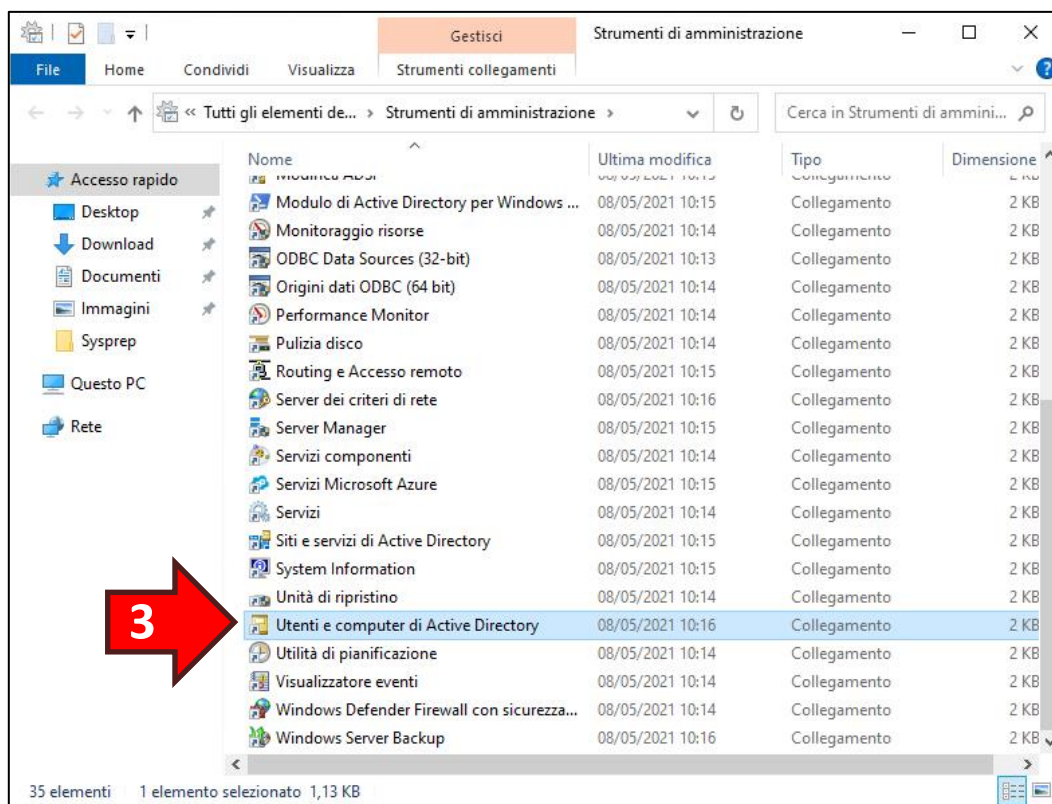
- Profilo** (Profile)
- Azienda di prova** (Test Company): utente.di.prova@wpanel.local
- Accesso con smart card** (Smart card access): Disabled
- Abilita l'accesso al sito tramite smart card** (Enable site access via smart card): Disabled
- Dominio per UPN:** utente-kdzh.wpanel.local
- Cambio password** (Change password): Cambia la password di accesso
- Modifica Account** (Modify account): Modifica le informazioni di registrazione
- Certificati** (Certificates): Crea e visualizza certificati di accesso
- Fatturazione** (Billing): Visualizza e scarica le fatture
- Logout** button
- Per ricevere assistenza scrivere a support@wpanel.local

ATTENZIONE! Prima di effettuare l'associazione dell'UPN creare l'utente desiderato nel dominio Active Directory del VPS.

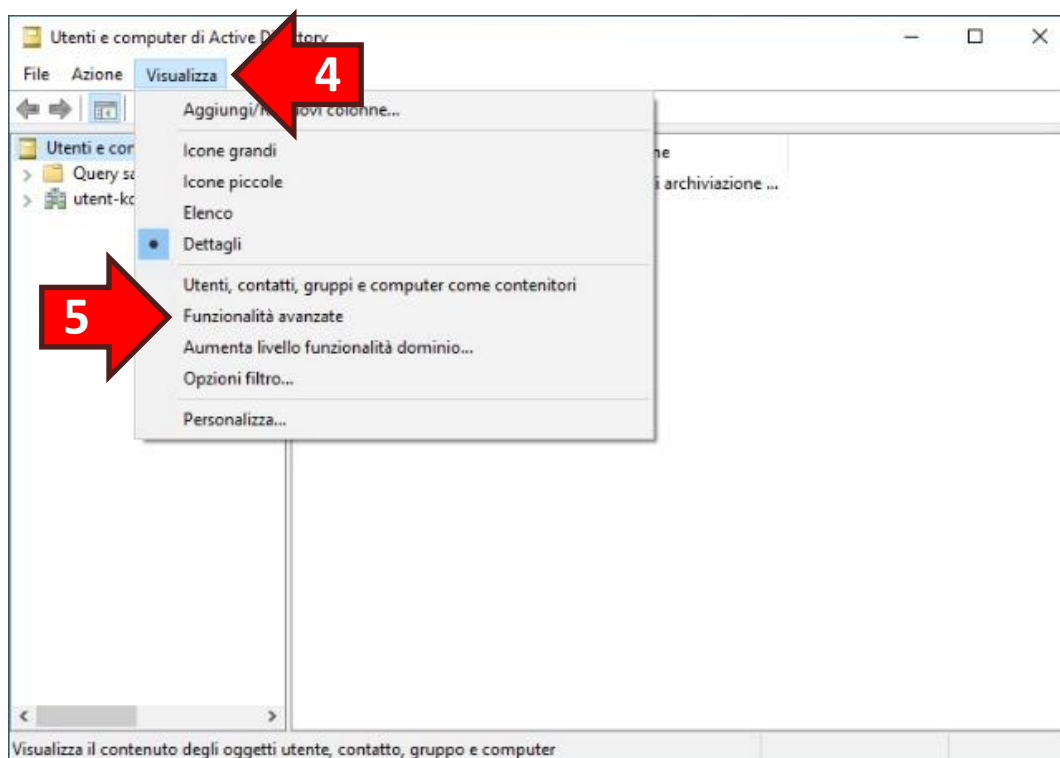
Per effettuare l'associazione dell'UPN ad un utente del VPS accedere al desktop del VPS con l'utente Administrator, cliccare sul **Menù start (1)** e successivamente sull'icona **Strumenti di amministrazione (2)**:



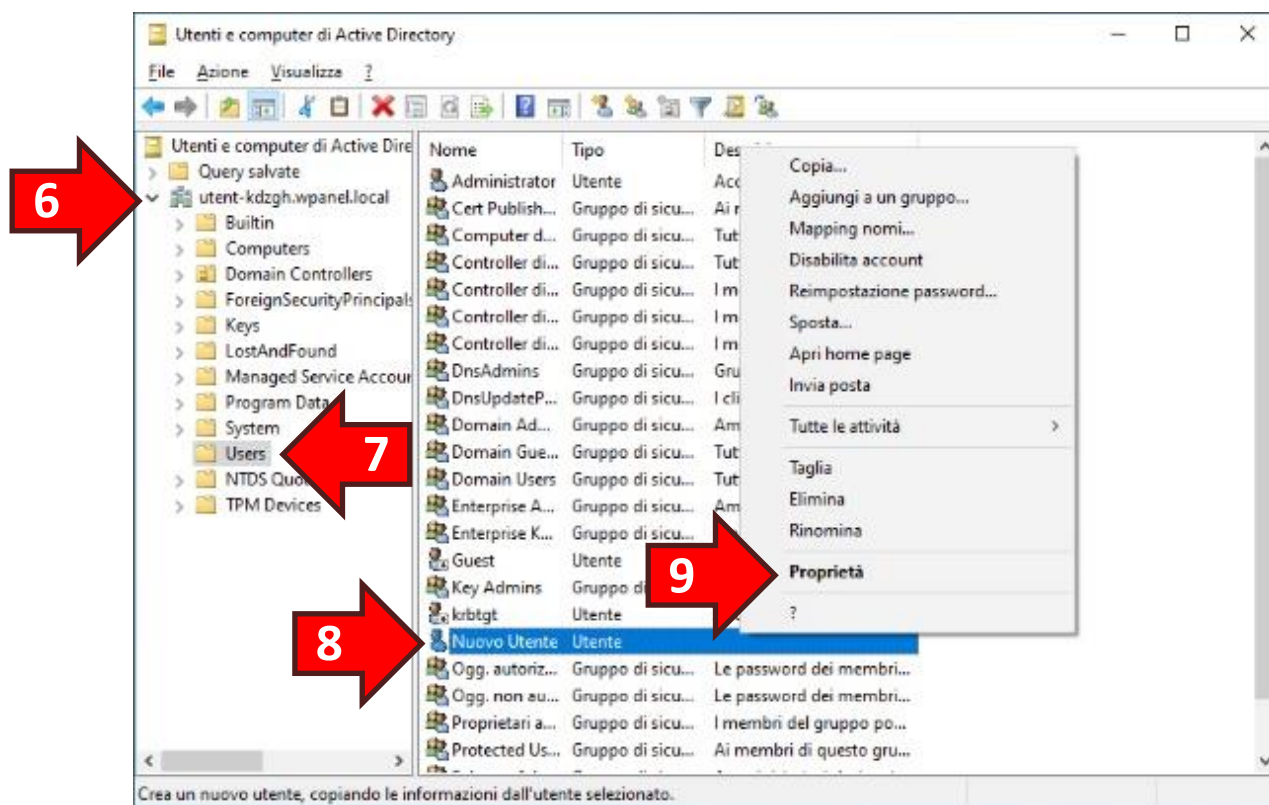
Dalla finestra *Strumenti di amministrazione* fare doppio click su **Utenti e computer di Active Directory (3)**:



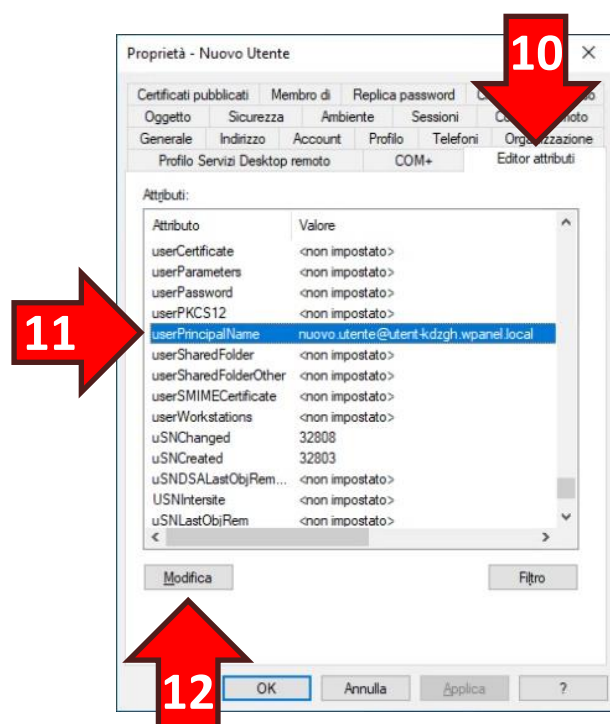
Nella finestra *Utenti e computer di Active Directory* cliccare sul menù **Visualizza (4)** e attivare l'opzione **Funzionalità avanzate (5)**:



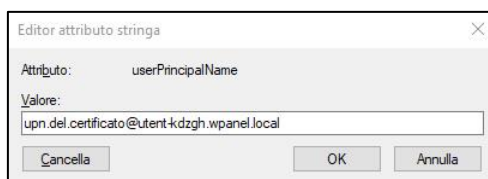
Quindi nel riquadro di sinistra espandere il **ramo del dominio (6)** (nell'esempio: *utente-kdzgh.wpanel.local*) e selezionare la foglia **Users (7)**. Poi nel riquadro di destra cliccare con il tasto destro del mouse sull'**utente che si desidera associare (8)**. Infine dal menù popup selezionare l'opzione **Proprietà (9)**:



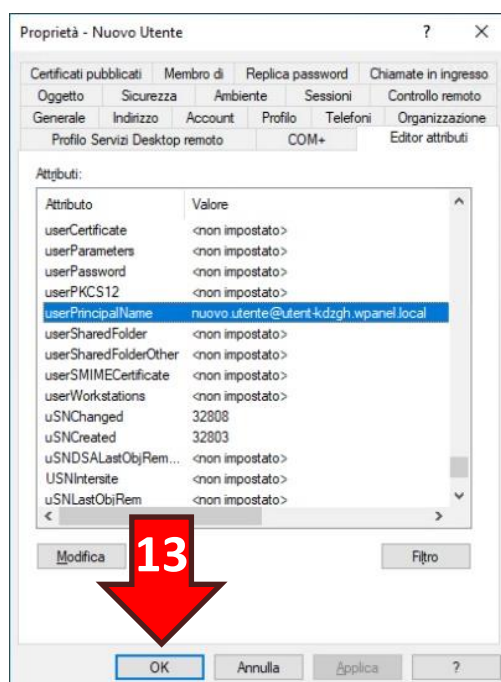
Nella finestra *Proprietà* selezionare la scheda **Editor attributi (10)** e, scorrendo verso il basso l'elenco *Attributi*, selezionare l'attributo **userPrincipalName (11)** e cliccare il tasto **Modifica (12)**:



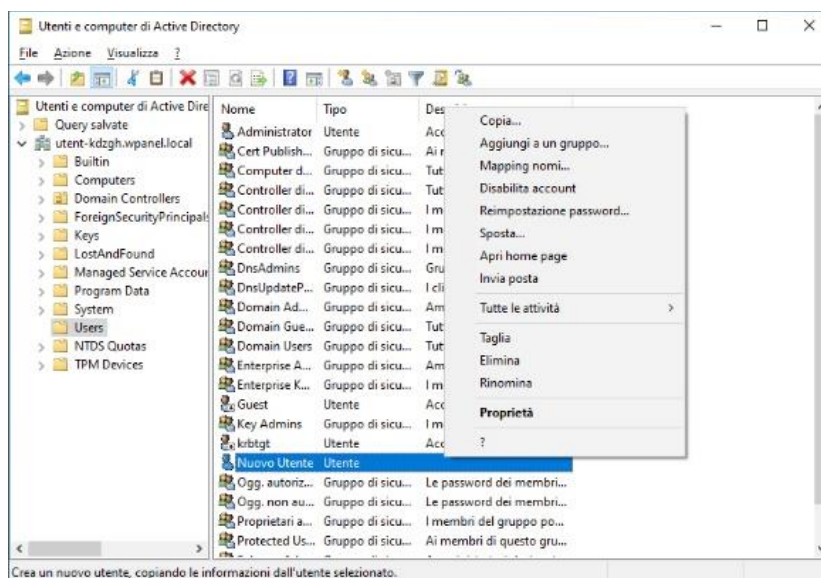
Nella finestra *Editor attributi stringa* inserire lo stesso UPN utilizzato nella generazione del certificato:



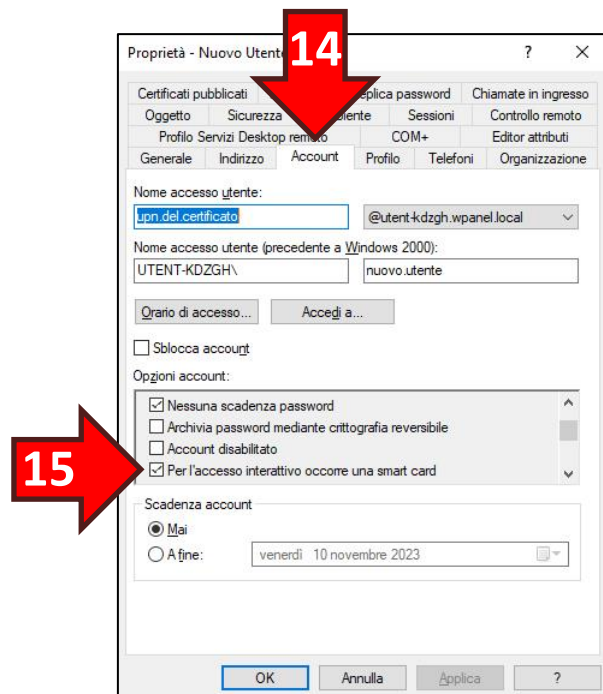
Una volta modificato il valore e ritornati nella finestra *Proprietà* confermare le modifiche cliccando il tasto **OK (13)**. **ATTENZIONE! Non saltare questo passaggio.**



Ritornare nelle proprietà del medesimo utente:



Nella finestra *Proprietà* selezionare la scheda **Account (14)** e impostare l'opzione **Per l'accesso interattivo occorre una smart card (15)**. **ATTENZIONE!** Quest'ultimo passaggio disabiliterà l'accesso dell'utente tramite la password rendendo l'account molto più sicuro.



Procedura manuale

Aprire una finestra *PowerShell* con diritti di amministrazione e digitare:

```
Set-ADUser <Nome Utente> -UserPrincipalName <UPN certificato>
$objUser = ([ADSI]'WinNT://localhost/<Nome Utente>,user')
$objUser.UserFlags.Value = $objUser.UserFlags.Value -bor 0x40000
$objUser.SetInfo()
```

Nell'esempio illustrato il testo da digitare risulterebbe il seguente:

```
Set-ADUser nuovo.utente -UserPrincipalName upn.del.certificato@utente-
kdzgh.wpanel.local
$objUser = ([ADSI]'WinNT://localhost/nuovo.utente,user')
$objUser.UserFlags.Value = $objUser.UserFlags.Value -bor 0x40000
$objUser.SetInfo()
```

16. Configurazione manuale per Windows 11

ATTENZIONE! Prima di iniziare la configurazione manuale recuperare l'email di configurazione del VPS inviata in fase di acquisto oppure prendere visione della configurazione del VPS dal *Pannello servizi* di cui al **Capitolo 4**.

16.1 Configurazione autenticazione Kerberos

ATTENZIONE! Onde precludere l'accesso al vostro VPS in caso di malfunzionamento del sito WPanel del vostro fornitore **non vengono gestite le liste di revoca dei certificati dalla PKI WPanel**.

ATTENZIONE! Senza questa configurazione non sarà possibile accedere al vostro VPS con il dispositivo sicuro.

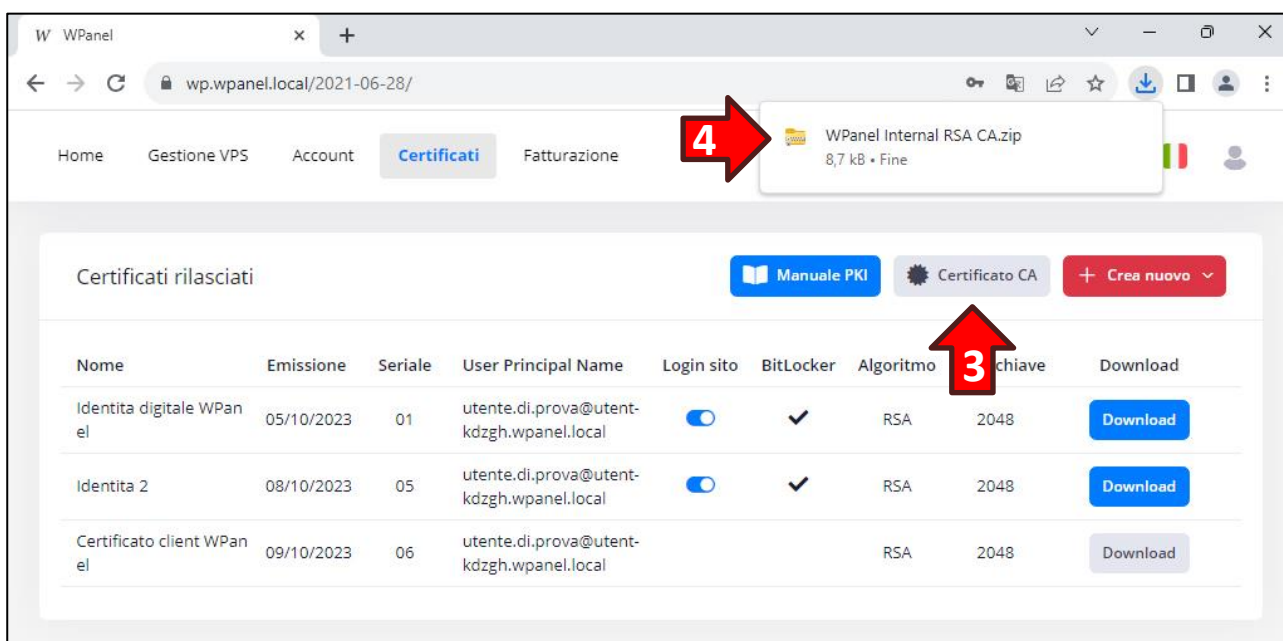
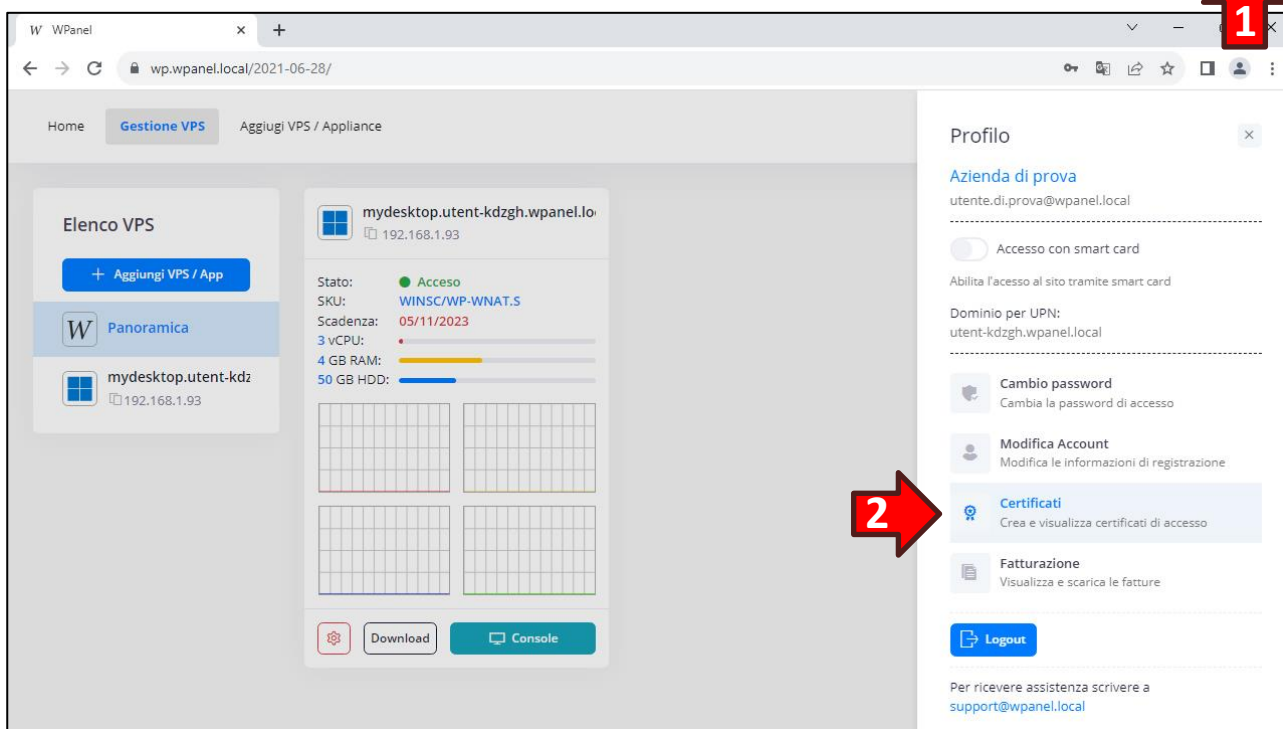
Il primo passaggio per la configurazione manuale del PC client è impostare il bypass dell'autenticazione Kerberos per la verifica della lista di revoca dei certificati. **L'impostazione diventa subito effettiva quindi non è necessario riavviare il PC.**

Da una finestra *Prompt dei comandi* con diritti di amministrazione digitare:

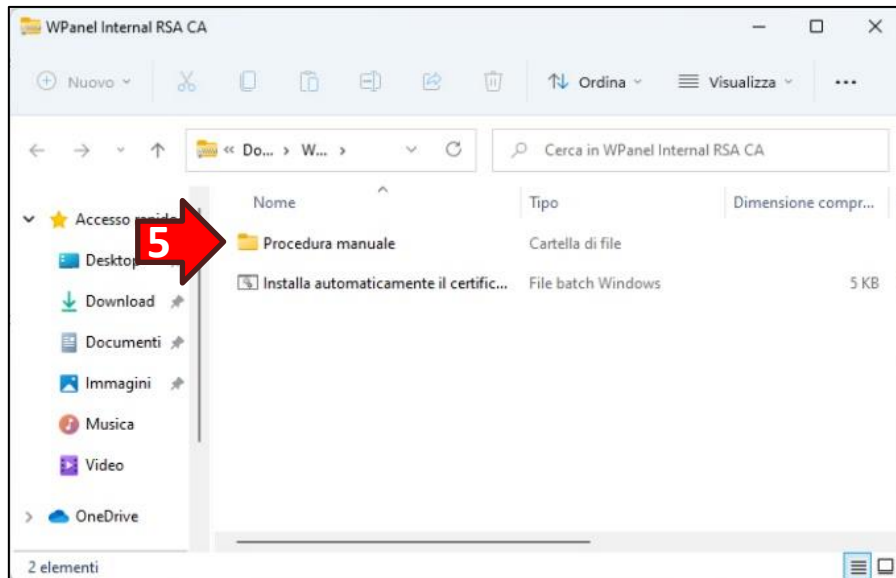
```
reg.exe add HKLM\SYSTEM\CurrentControlSet\Control\LSA\Kerberos\Parameters /v  
UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors /t REG_DWORD /d 1 /f
```

16.2 Installazione del certificato CA

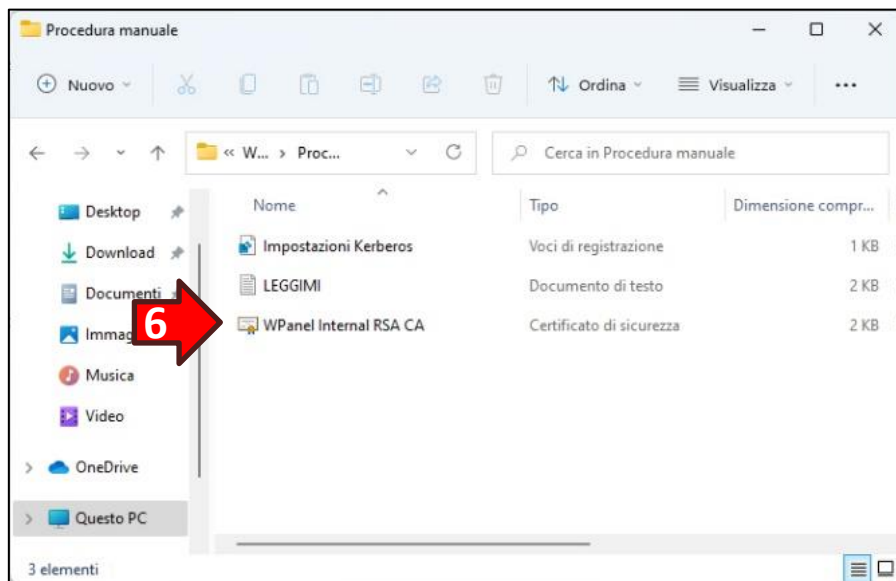
Accedendo al sito WPanel del vostro fornitore e cliccare sull'**icona dell'utente (1)** nella barra in alto. Dalla barra laterale del *Profilo* cliccare l'opzione **Certificati (2)**. Nella scheda *Certificati* cliccare il tasto grigio **Certificato CA (3)** e aprire file compresso **<Nome fornitore> Internal RSA CA (4)**:



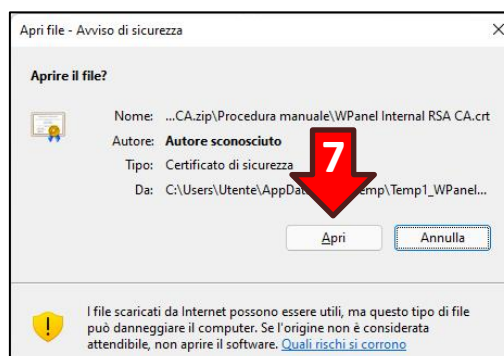
All'interno della cartella compressa aprire la sottocartella **Procedura Manuale (5)**:



Fare doppio click sul file <Nome fornitore> Internal RSA CA (6):



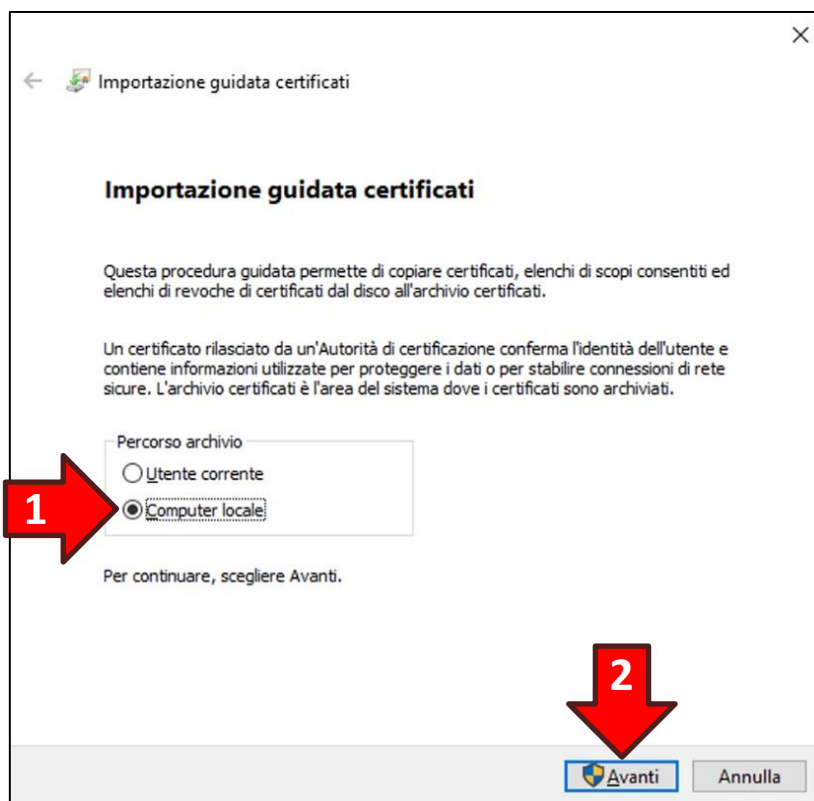
Cliccare il tasto **Apri (7)** nella finestra dell'Avviso di sicurezza:



Dalla finestra *Certificato* cliccare il tasto **Installa certificato**:



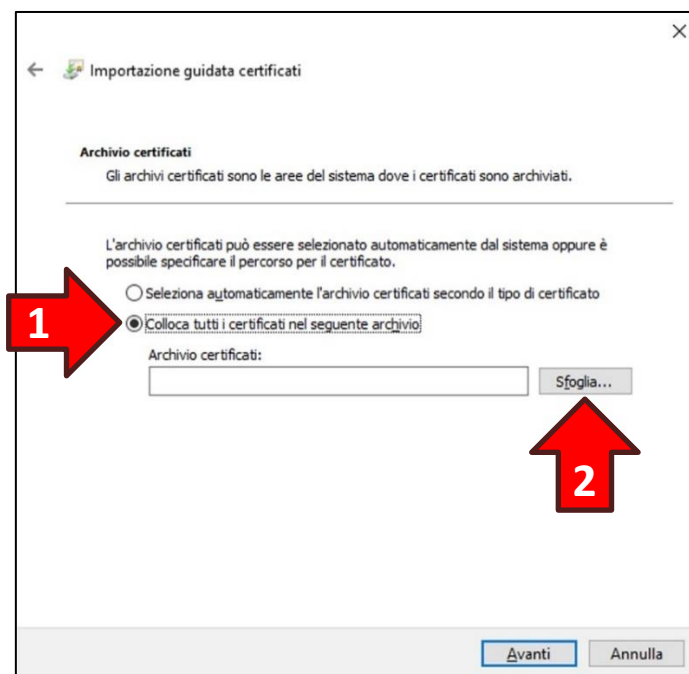
Nella finestra *Installazione guidata certificati* selezionare **Computer locale (1)** dalla sezione *Percorso archivio* e poi cliccare il tasto **Avanti (2)**:



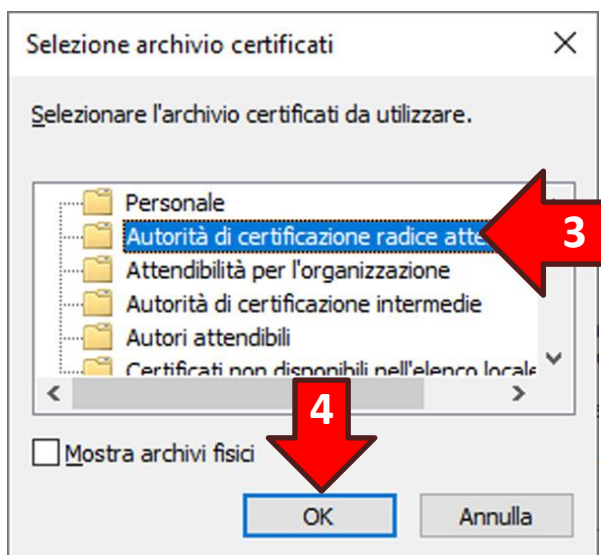
Verrà visualizzata la finestra di conferma operazione del *Controllo dell'Account Utente*. Cliccare il tasto **Si** per continuare. Se l'utente non possiede i diritti di amministrazione verranno richieste le credenziali dell'utente di amministrazione:



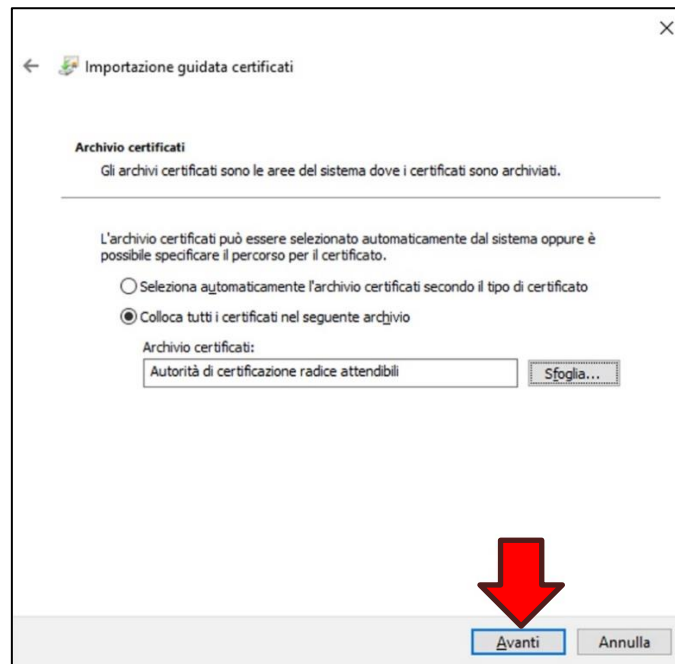
Nella finestra successiva selezionare l'opzione **Colloca tutti i certificati nel seguente archivio (1)** e poi cliccare il tasto **Sfoglia... (2)**:



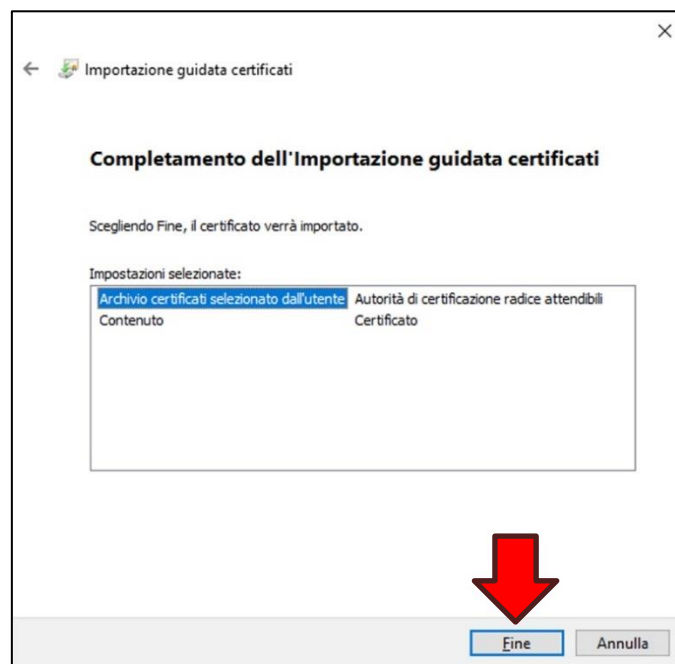
Nella finestra di selezione cliccare su **Autorità di certificazione radice attendibili (3)** e poi **OK (4)**:



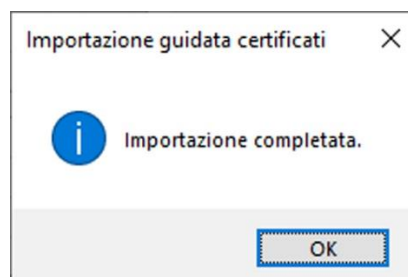
Si ritornerà nella finestra precedente, quindi cliccare il tasto **Avanti**:



Nella finestra di completamento dell'operazione cliccare il tasto **Fine**:

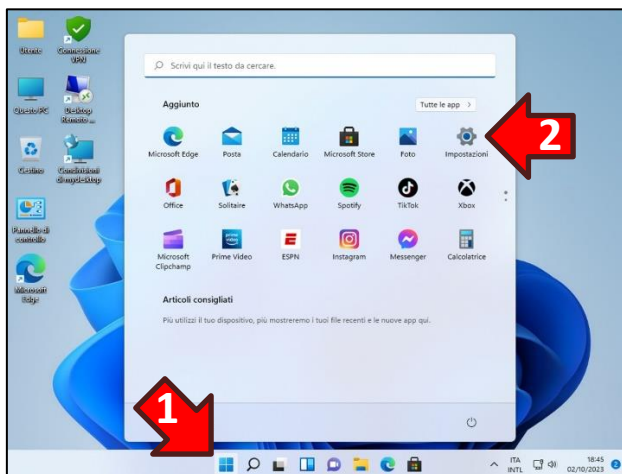


Se l'installazione del certificato è andata buon fine verrà visualizzata la relativa conferma:



16.3 Creazione della connessione VPN

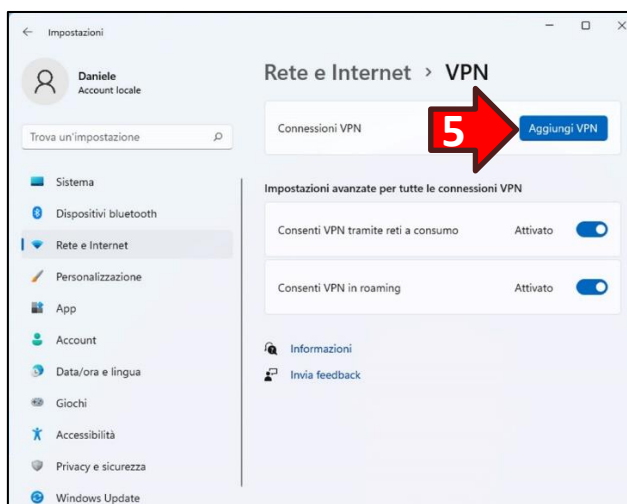
Dal **menu Start (1)** cliccare sull'icona **Impostazioni (2)**:



Nella finestra *Impostazioni* cliccare prima sull'opzione **Rete e Internet (3)** nel riquadro di sinistra e successivamente il tasto **VPN (4)** nel riquadro che apparirà a destra:



Dal riquadro di destra denominato *Rete e Internet > VPN* cliccare il tasto **Aggiungi VPN (5)**:



Nella finestra *Aggiungi connessione VPN* impostare le seguenti informazioni:

- Provider VPN: **Windows (predefinito)**
- Nome connessione: **VPN per nome del vostro VPS**
- Nome o indirizzo server: **Indirizzo server VPN indicato nell’email di attivazione**
- Tipo di VPN: **SSTP (Secure Socket Tunneling Protocol)**
- Tipo di info di accesso.....: **Smart card**
- Nome utente (facoltativo).....: **Non è impostabile e deve restare vuoto**
- Password (facoltativa): **Non è impostabile e deve restare vuoto**

Verificare che l’opzione **Memorizza le mie info di accesso** sia spuntata.

Infine cliccare il tasto **Salva**.

Aggiungi connessione VPN

Provider VPN

Windows (predefinito) ▼

Nome connessione

mydesktop

Nome o indirizzo server

wrx-192-168-1-92.wpanel.local:22001

Tipo di VPN

SSTP (Secure Socket Tunneling Protocol) ▼

Tipo di info di accesso

Smart card ▼

Nome utente (facoltativo)

Password (facoltativa)

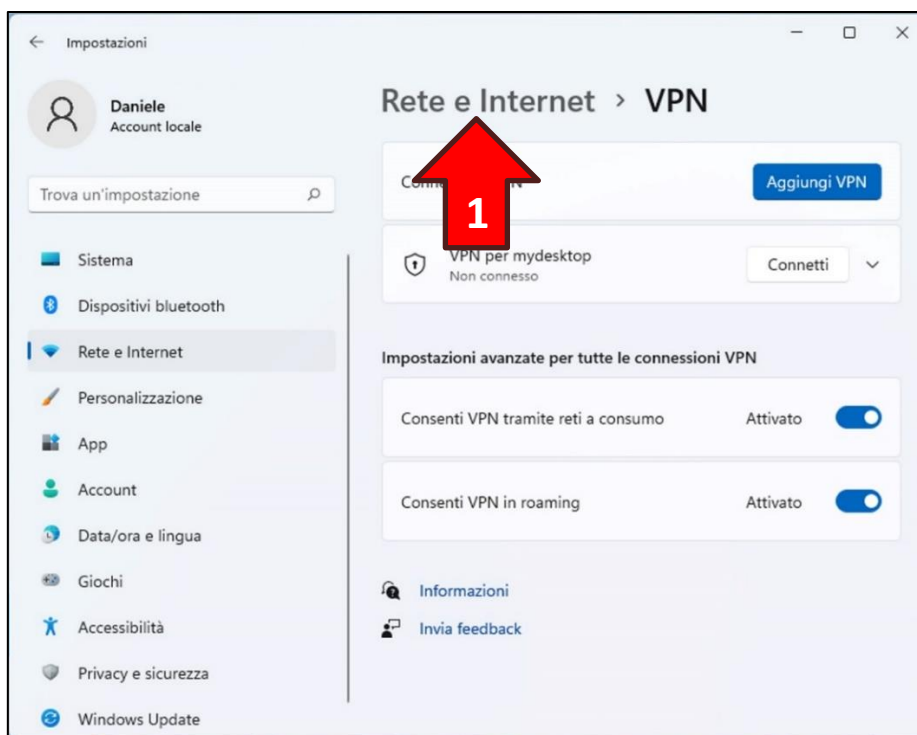
Memorizza le mie info di accesso

Salva

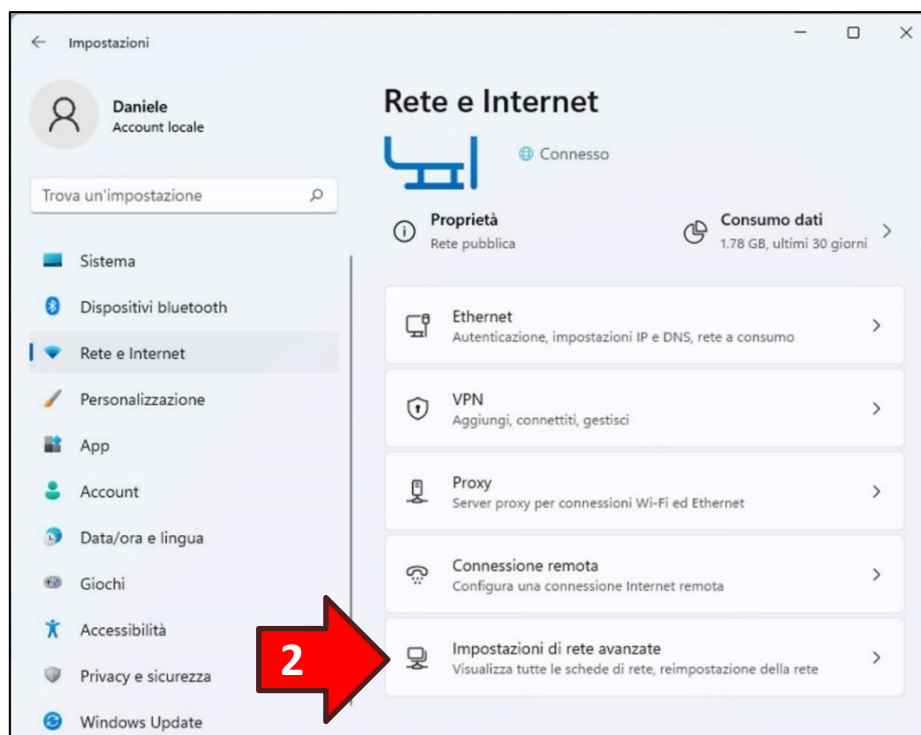
Annulla

Una volta aggiunta la VPN è indispensabile impostare un server DNS statico per il tunnel VPN ed è consigliabile rimuovere l'impostazione di **Usa gateway predefinito sulla rete remota** per evitare che l'intera navigazione Internet del PC attraversi il tunnel VPN e quindi risulti rallentata.

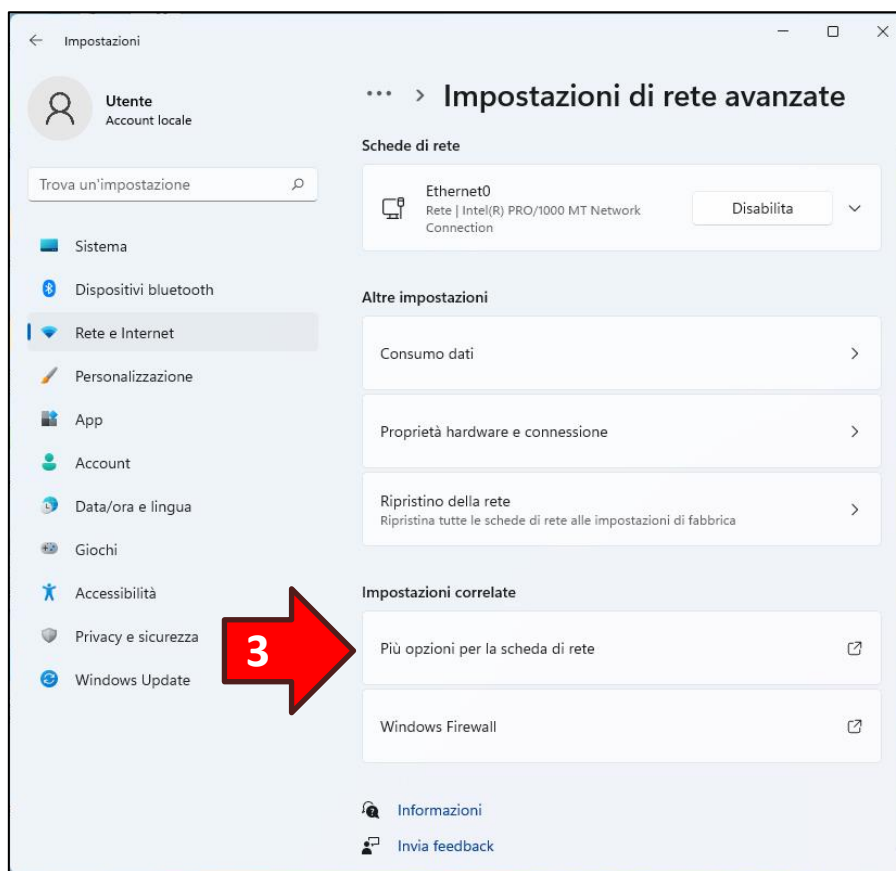
Quindi ritornati nella finestra precedente cliccare sulla dicitura **Rete e Internet (1)** nel titolo del riquadro di destra:



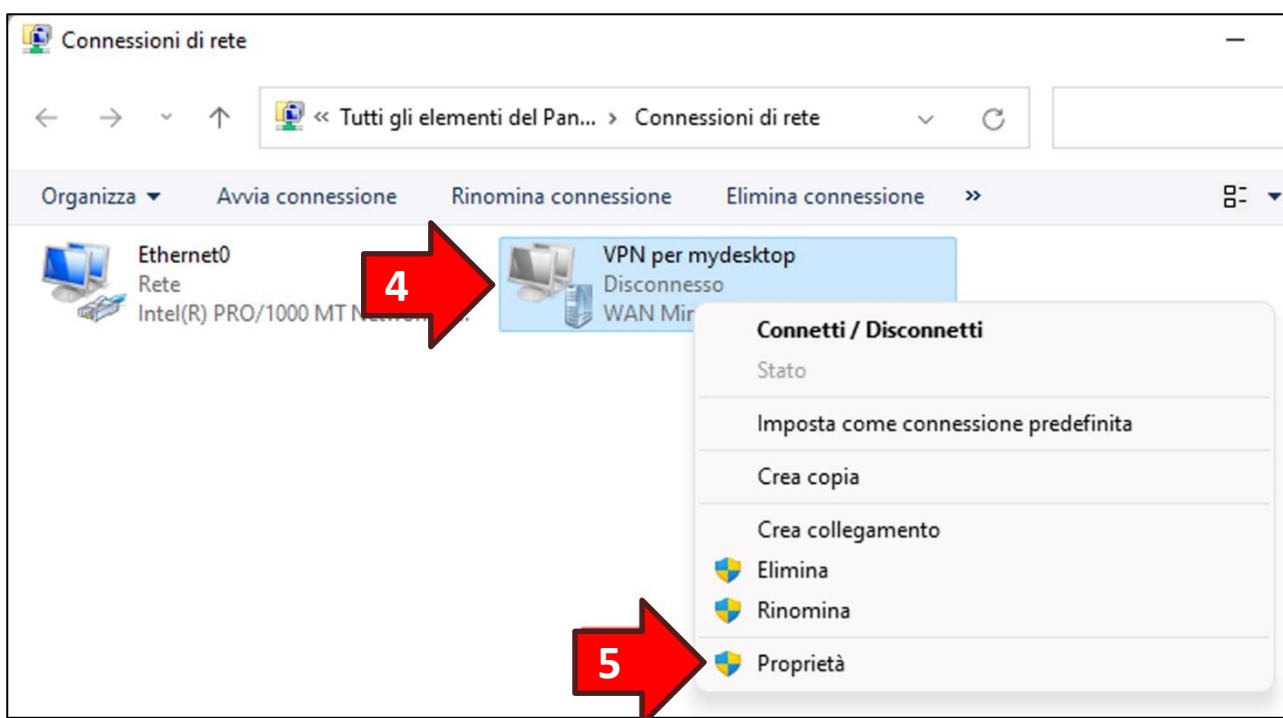
Dal nuovo riquadro di destra cliccare il tasto **Impostazioni di rete avanzate (2)**:



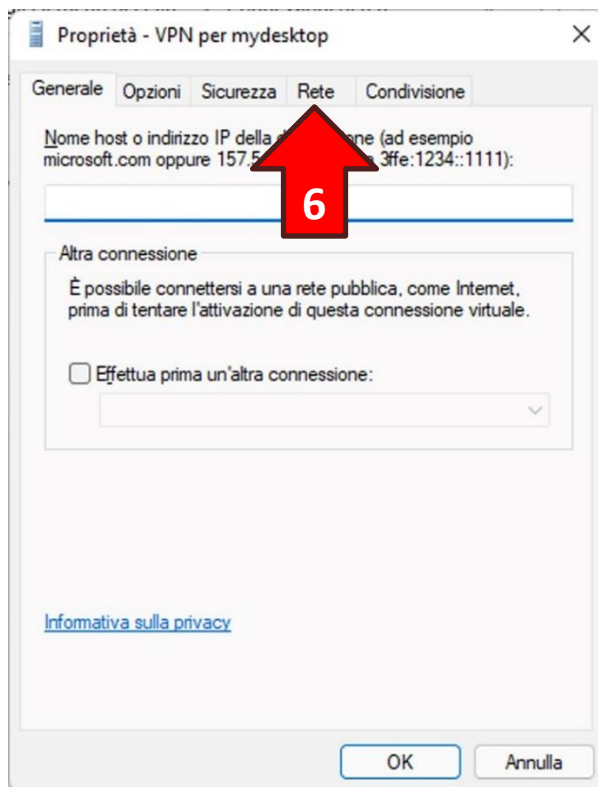
Dal successivo riquadro di destra cliccare il tasto **Più opzioni per la scheda di rete (3)**:



Apparirà la finestra *Connessioni di rete*. Cliccare con il tasto destro del mouse sull'icona **VPN per <nome del vostro VPS> (4)** (Esempio: **VPN per mydesktop**) quindi cliccare sull'opzione **Proprietà (5)** dal menu popup che apparirà:

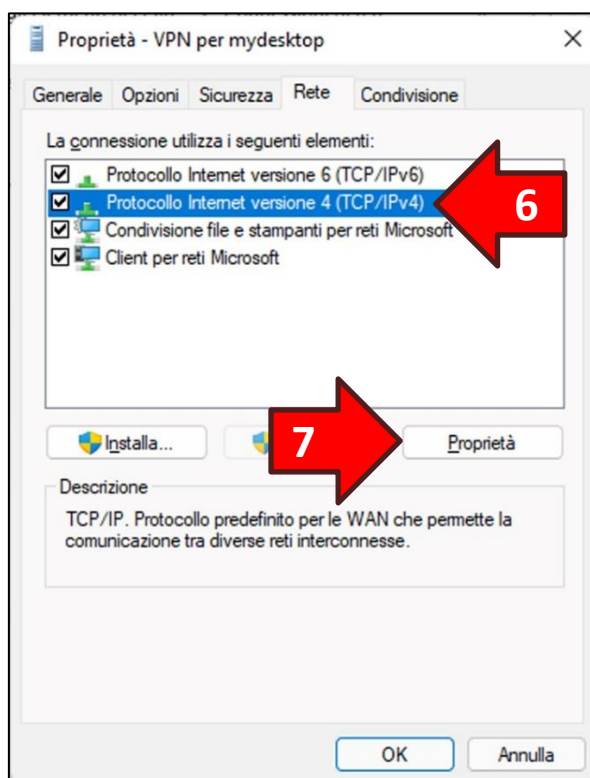


Una volta apparsa la finestra *Proprietà* cliccare sulla sezione **Rete (6)**:

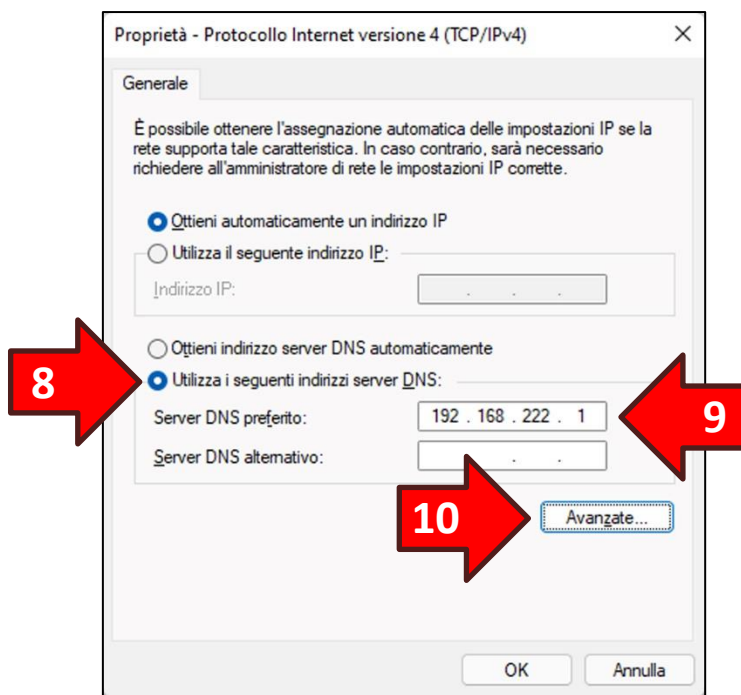


Dalla lista selezionare la voce **Protocollo Internet versione 4 (TCP/IPv4) (6)** e successivamente cliccare il tasto **Proprietà (7)**:

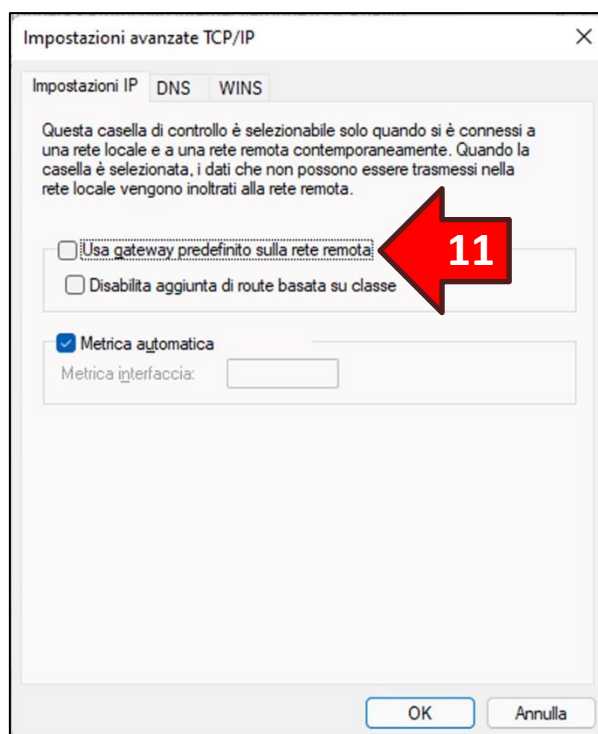
ATTENZIONE! Non togliere la spunta posta a sinistra della voce.





Si aprirà una nuova finestra. Cliccare l'opzione **Utilizza i seguenti indirizzi server DNS (8)** e in **Server DNS preferito (9)** impostare il valore *DNS da impostare per la VPN nel Pannello servizi del VPS* di cui al **Capitolo 4** oppure nell'email inviata in fase di acquisto del VPS. Cliccare poi il tasto **Avanzate... (10)**:



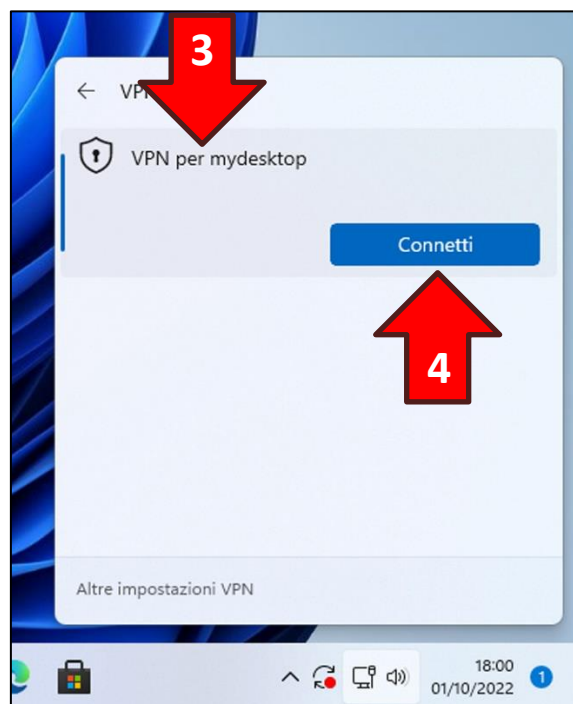
Rimuovere la spunta dell'opzione **Usa gateway predefinito sulla rete remota (11)**. Ora premere il tasto **OK** sia nella finestra corrente che in quelle precedenti:



Per verificare il corretto completamento della procedura cliccare sul **simbolo di rete (1)**, che potrebbe essere un monitor  oppure una sequenza di onde , nella barra delle applicazioni a sinistra dell'orologio (system tray). Nel riquadro che apparirà cliccare il tasto con l'icona di un lucchetto denominato **VPN (2)**:



Apparirà un nuovo riquadro contenente un elenco di connessioni, quindi cliccare sulla voce **VPN per <nome del vostro VPS> (3)** (Esempio: **VPN per mydesktop**) per mostrare il tasto **Connetti (4)**. Infine per aprire il tunnel VPN cliccare il tasto **Connetti (4)**:



17. Configurazione manuale per Windows 10



ATTENZIONE! Prima di iniziare la configurazione manuale recuperare l'email di configurazione del VPS inviata in fase di acquisto oppure prendere visione della configurazione del VPS dal *Pannello servizi* di cui al **Capitolo 4**.

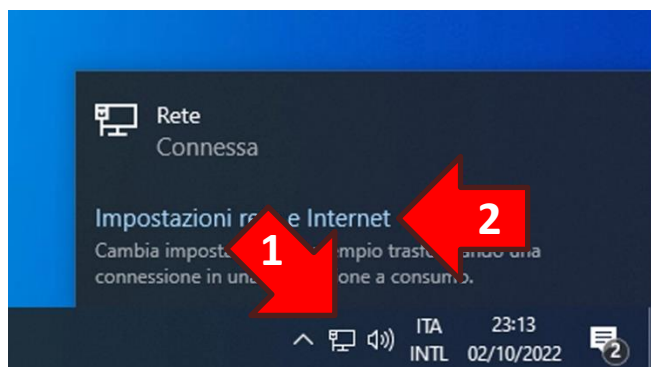
17.1 Note preliminari

Le procedure di installazione del Certificato CA e di impostazione della connessione al Desktop Remoto nonché l'accesso alle condivisioni di rete sono equivalenti a quelle utilizzabili per Windows 11 per cui si consiglia di procedere nel modo seguente:

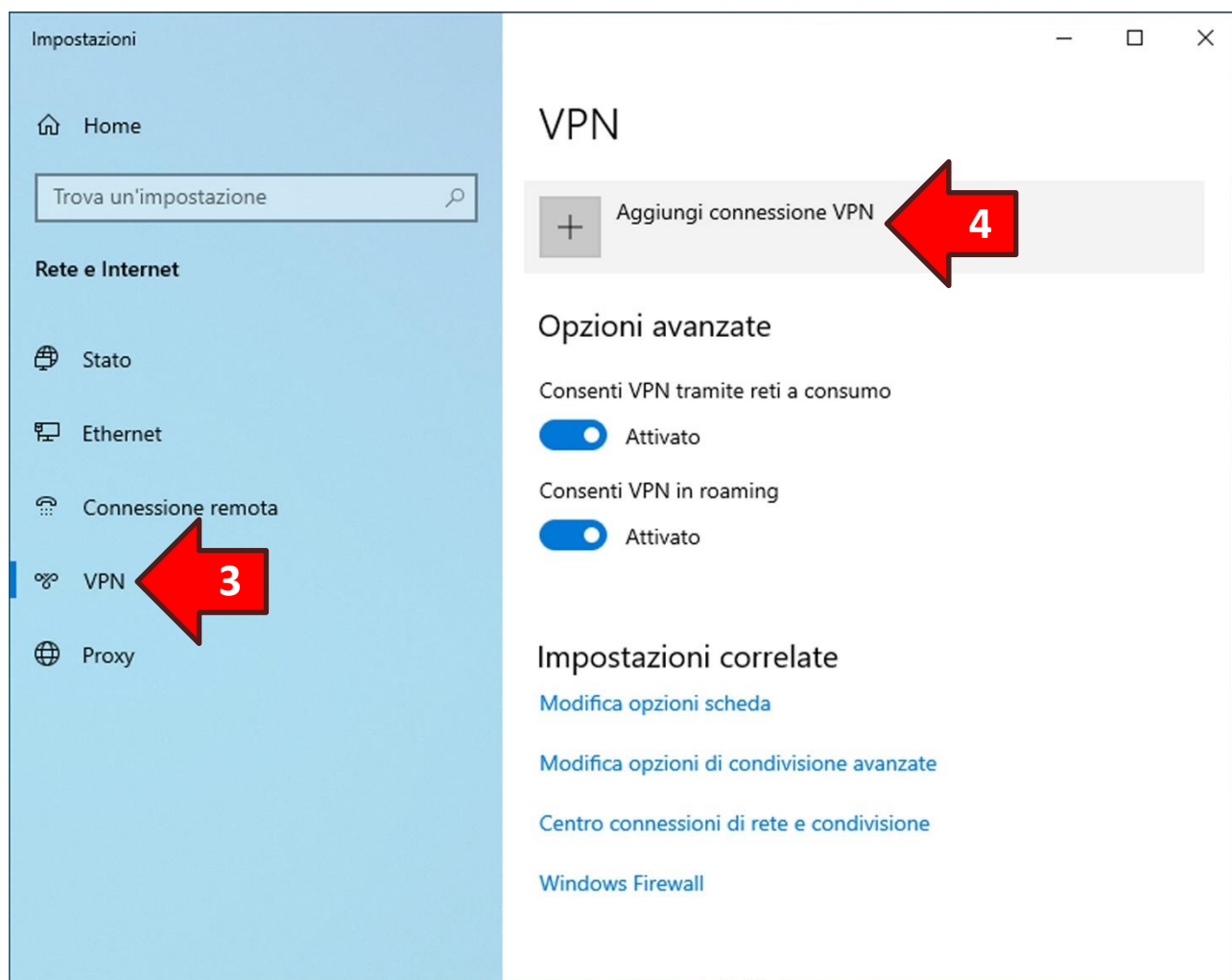
1. Seguire le procedure di installazione del Certificato CA indicata ai **paragrafi 16.1** e **16.2** del capitolo precedente;
2. Seguire la procedura di creazione della connessione VPN indicata al paragrafo successivo (**paragrafo 17.2**) di questo capitolo;
3. Seguire le procedure di impostazione della connessione al Desktop Remoto nonché l'accesso alle condivisioni di rete indicate al **paragrafo 16.4** del capitolo precedente.

17.2 Creazione della connessione VPN

Cliccare sul **simbolo di rete (1)**, che potrebbe essere un monitor  oppure una sequenza di onde , nella barra delle applicazioni a sinistra dell'orologio (system tray). Nella parte bassa del riquadro cliccare sulla dicitura azzurra **Impostazioni rete e Internet (2)**:



Nella finestra *Impostazioni* cliccare sull'opzione **VPN (3)** nel riquadro di sinistra. Cliccare poi sulla funzione **Aggiungi connessione VPN (4)** che apparirà nel riquadro di destra:



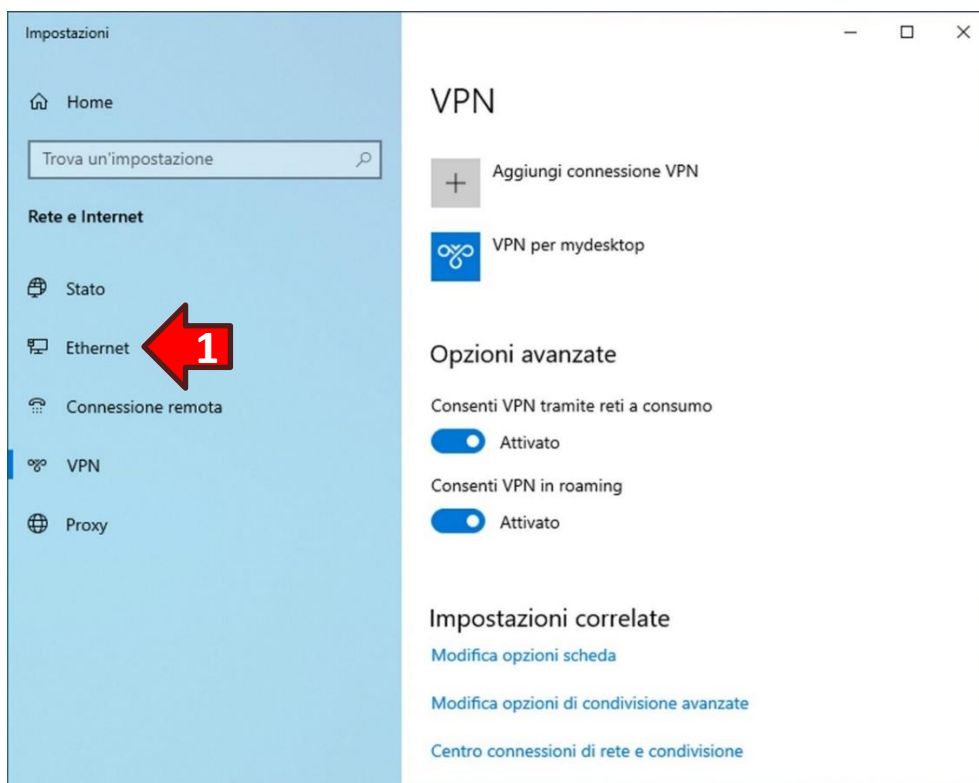
Nella finestra *Aggiungi connessione VPN* impostare le seguenti informazioni:

- Provider VPN: **Windows (predefinito)**
- Nome connessione: **VPN per nome del vostro VPS**
- Nome o indirizzo server: **Indirizzo server indicato nell'email di attivazione**
- Tipo di VPN: **SSTP (Secure Socket Tunneling Protocol)**
- Tipo di info di accesso.....: **Smart card**
- Nome utente (facoltativo).....: **Non è impostabile e deve restare vuoto**
- Password (facoltativa): **Non è impostabile e deve restare vuoto**

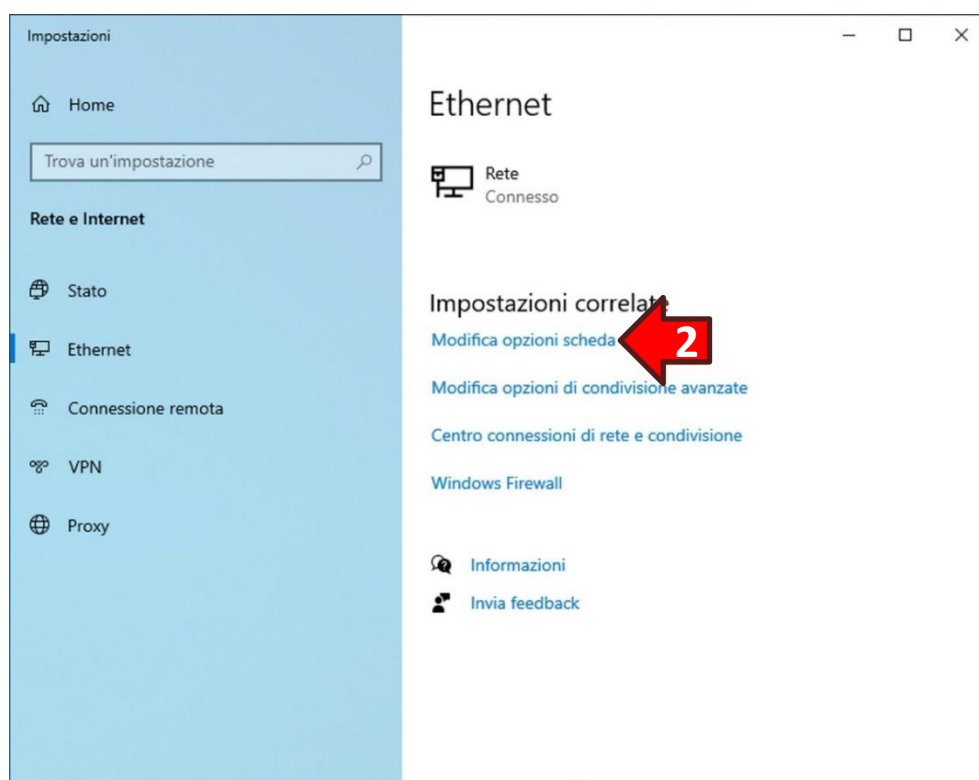
Verificare che l'opzione **Memorizza le mie info di accesso** sia spuntata.

Infine cliccare il tasto **Salva**.

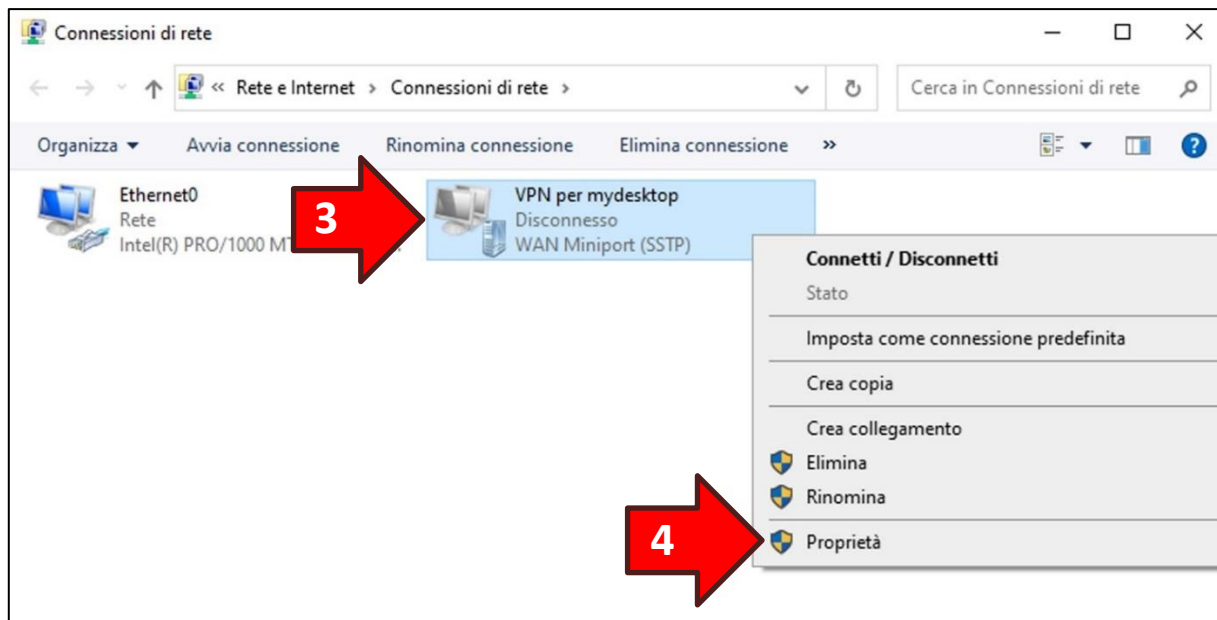
Una volta aggiunta la VPN è indispensabile impostare un server DNS statico per il tunnel VPN ed è consigliabile rimuovere l'impostazione di **Usa gateway predefinito sulla rete remota** per evitare che l'intera navigazione Internet del PC attraversi il tunnel VPN e quindi risulti rallentata. Quindi dal riquadro di sinistra dalla finestra *Impostazioni* selezione l'opzione **Ethernet (1)**:



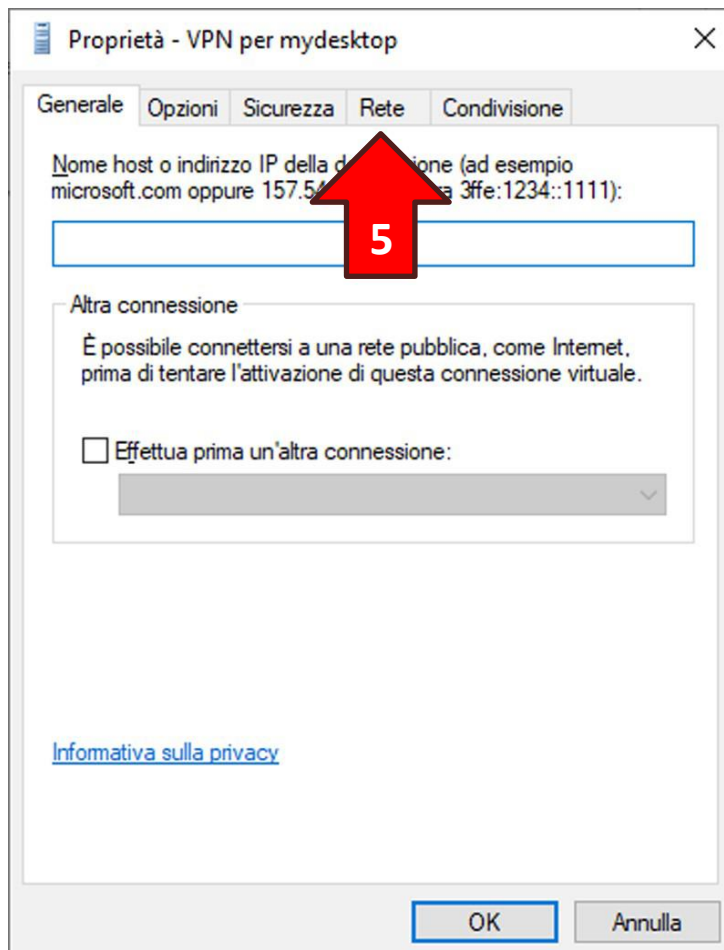
Poi dal riquadro di destra cliccare su **Modifica opzioni scheda (2)**:



Apparirà la finestra **Connessioni di rete**. Cliccare con il tasto destro del mouse sull'icona **VPN per <nome del vostro VPS> (3)** (Esempio: **VPN per mydesktop**) quindi cliccare sull'opzione **Proprietà (4)** dal menu popup che apparirà:

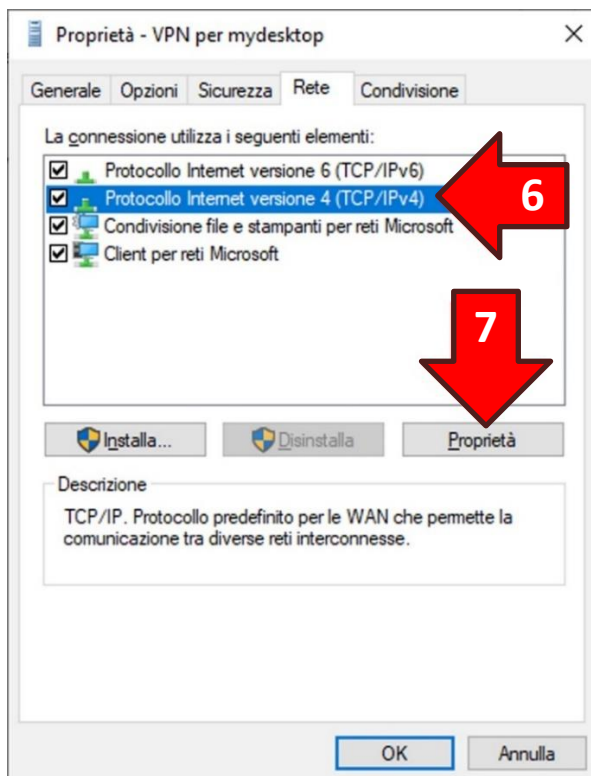


Una volta apparsa la finestra *Proprietà* cliccare sulla sezione **Rete (5)**:

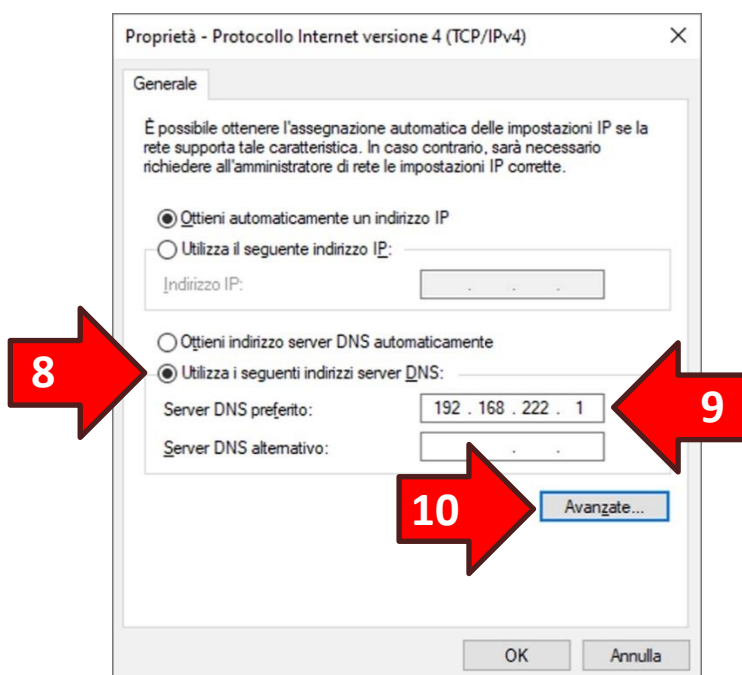


Dalla lista selezionare la voce **Protocollo Internet versione 4 (TCP/IPv4) (6)** e successivamente cliccare il tasto **Proprietà (7)**:

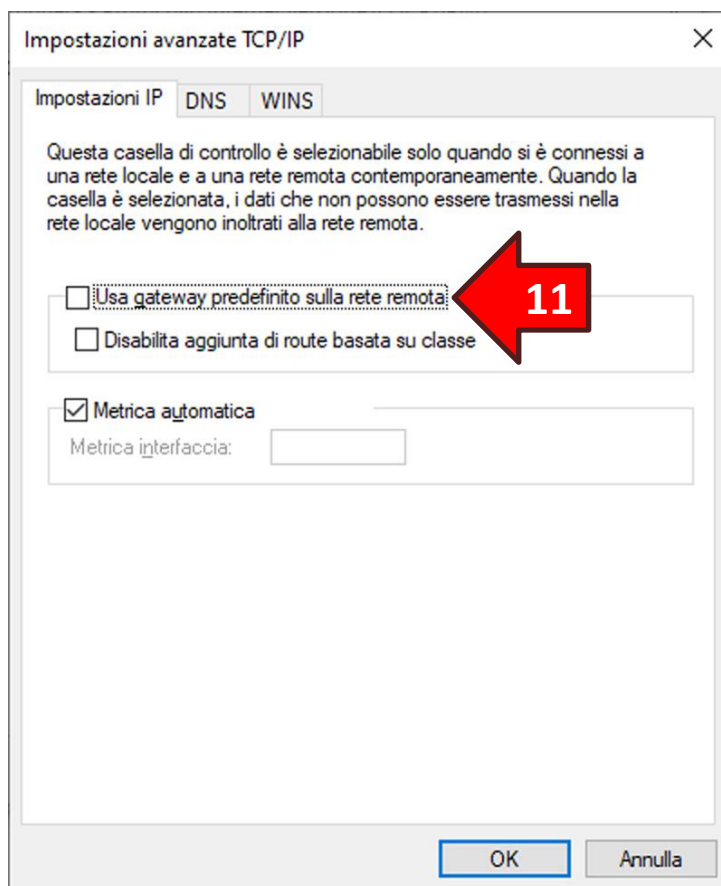
ATTENZIONE! Non togliere la spunta posta a sinistra della voce.





Si aprirà una nuova finestra. Cliccare l'opzione **Utilizza i seguenti indirizzi server DNS (8)** e in **Server DNS preferito (9)** impostare il valore *DNS da impostare per la VPN nel Pannello servizi del VPS* di cui al **Capitolo 4** oppure nell'email inviata in fase di acquisto del VPS. Cliccare poi il tasto **Avanzate... (10)**:



Rimuovere la spunta dell'opzione **Usa gateway predefinito sulla rete remota (11)**. Ora premere il tasto **OK** sia nella finestra corrente che in quelle precedenti:



Per verificare il corretto completamento della procedura cliccare sul **simbolo di rete (1)**, che potrebbe essere un monitor  oppure una sequenza di onde , nella barra delle applicazioni a sinistra dell'orologio (system tray). Apparirà un elenco di connessioni, quindi cliccare sulla voce **VPN per <nome del vostro VPS> (2)** (Esempio: **VPN per mydesktop**) per mostrare il tasto **Connetti (3)**. Infine per aprire il tunnel VPN cliccare il tasto **Connetti (3)**:

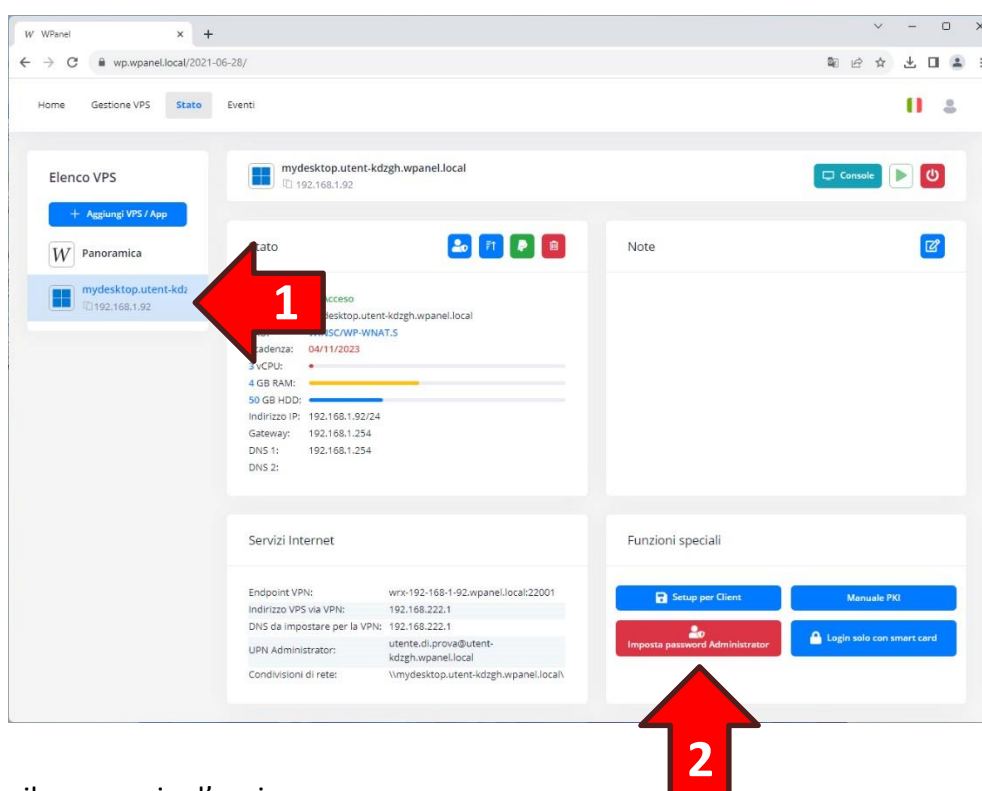


18. Accesso al VPS con una password

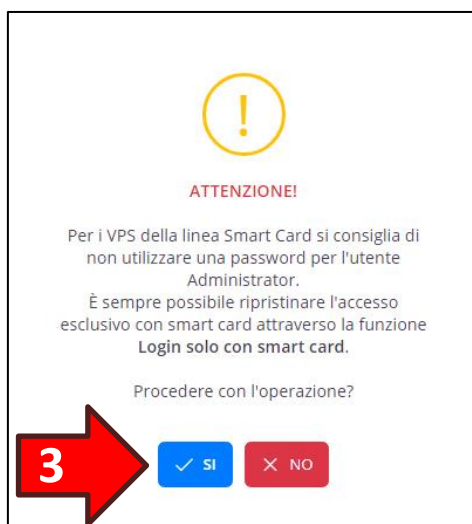
ATTENZIONE! La creazione di una password di accesso per l'utente Administrator abbassa il livello di sicurezza di accesso al VPS per cui se ne consiglia l'uso solo nei casi strettamente necessari.

Potrebbero verificarsi casi in cui il cliente debba accedere al VPS senza il dispositivo sicuro, ad esempio se tale dispositivo è stato smarrito o non è più funzionante.

Per creare una password per l'utente Administrator accedere al sito WPanel del vostro fornitore, poi entrare nello **stato del VPS (1)** e dal *Pannello funzioni speciali* cliccare il tasto rosso **Imposta password utente Administrator (2)**:



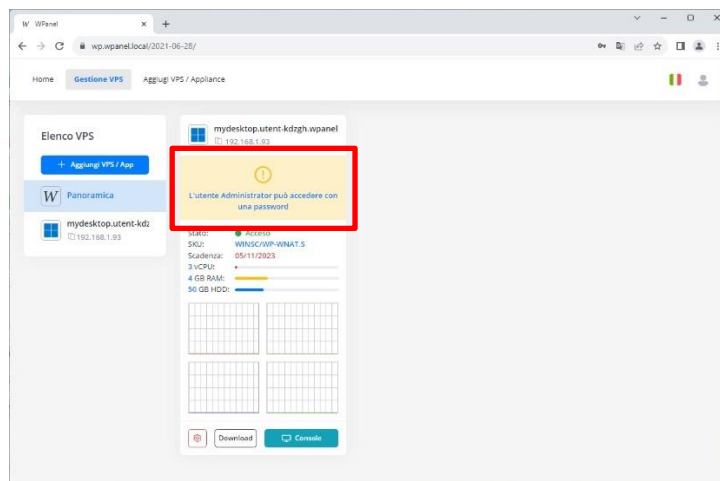
Confermare il messaggio d'avviso:



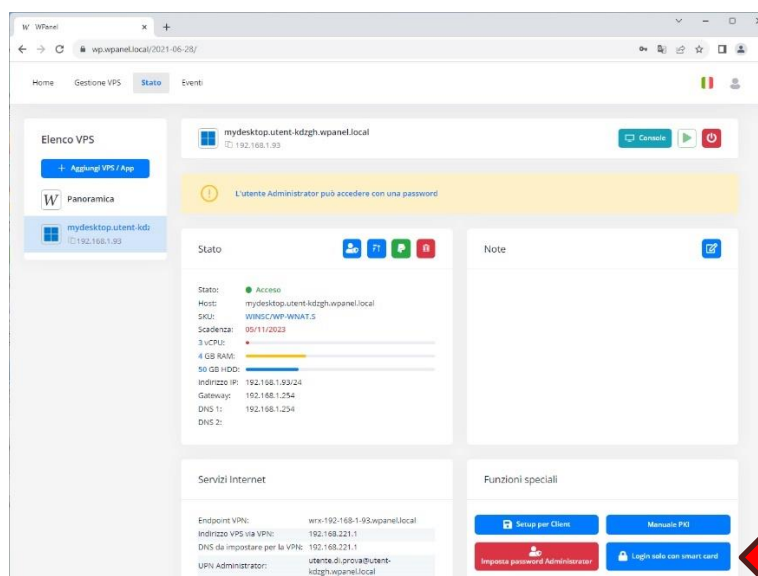
Impostare la password nel pannello *Password VPS*:

A dialog box titled "Password VPS mydesktop.utent-kdzh.wpanel.local" with a close button (X) in the top right corner. It contains two input fields: "Nuova password:" and "Conferma pass:.". Both fields have a masked password (seven dots) and a toggle icon (eye) to the right. At the bottom, there are two buttons: "Annulla" (light blue) and "Conferma" (dark blue).

Quando nei VPS della linea Smart Card è presente una password per l'utente Administrator viene visualizzato un particolare avviso:



ATTENZIONE! terminate le operazioni di manutenzione si consiglia di rimuovere la password dell'utente Administrator attraverso il tasto **Login solo con smart card**:

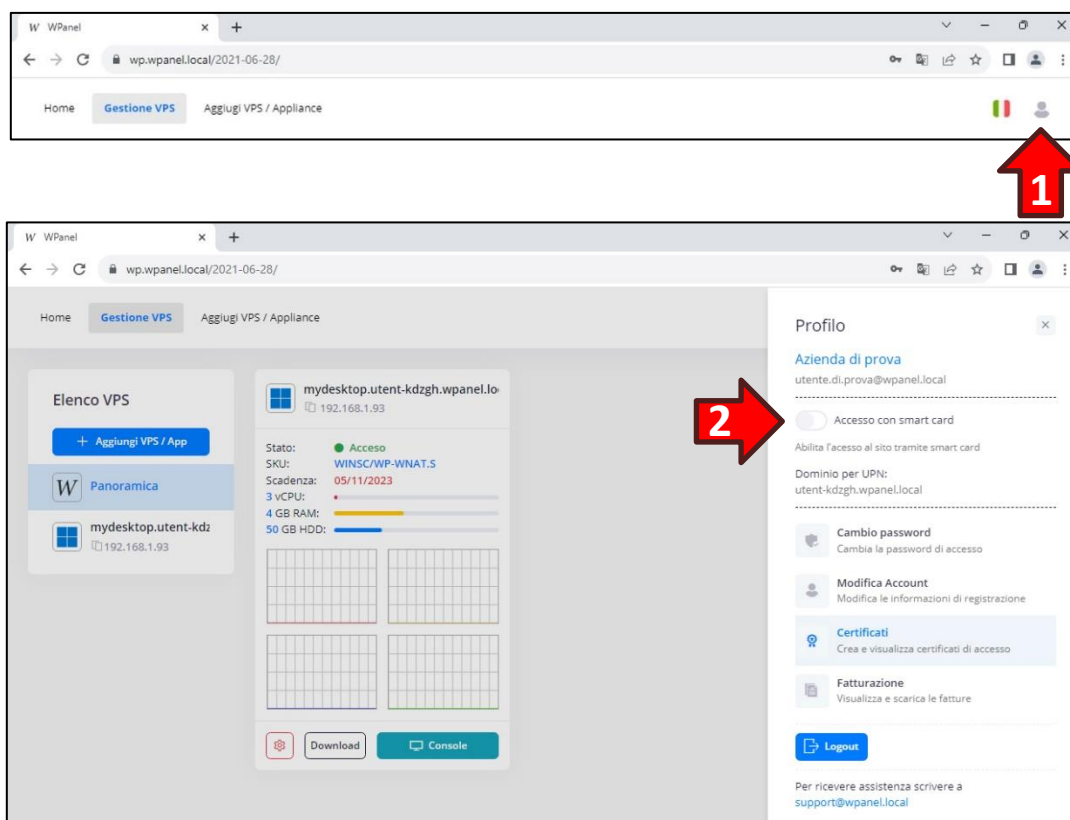


19. Disabilitazione accesso sicuro al sito WPanel

Nel momento in cui si dispone di un dispositivo sicuro è consigliabile accedere al sito WPanel attraverso questo dispositivo come proposto in fase di emissione del primo certificato.

Nel caso si preveda di non utilizzare più il dispositivo o comunque si avesse la necessità di accedere al sito WPanel senza dispositivo è possibile disattivare l'accesso sicuro.

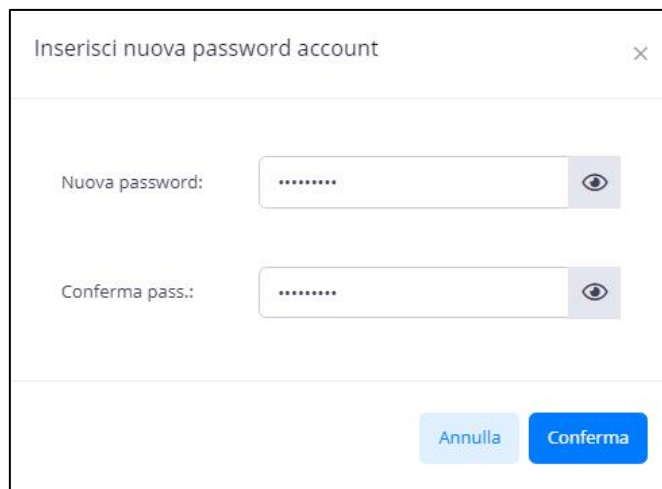
Cliccare quindi sull'icona dell'utente (1) nella barra in alto e disattivare l'opzione **Accesso con smart card (2)** nella barra laterale del *Profilo*:




Confermare il messaggio di avviso:




Quindi creare una password di accesso al sito WPanel:



Inserisci nuova password account

Nuova password: 

Conferma pass.: 

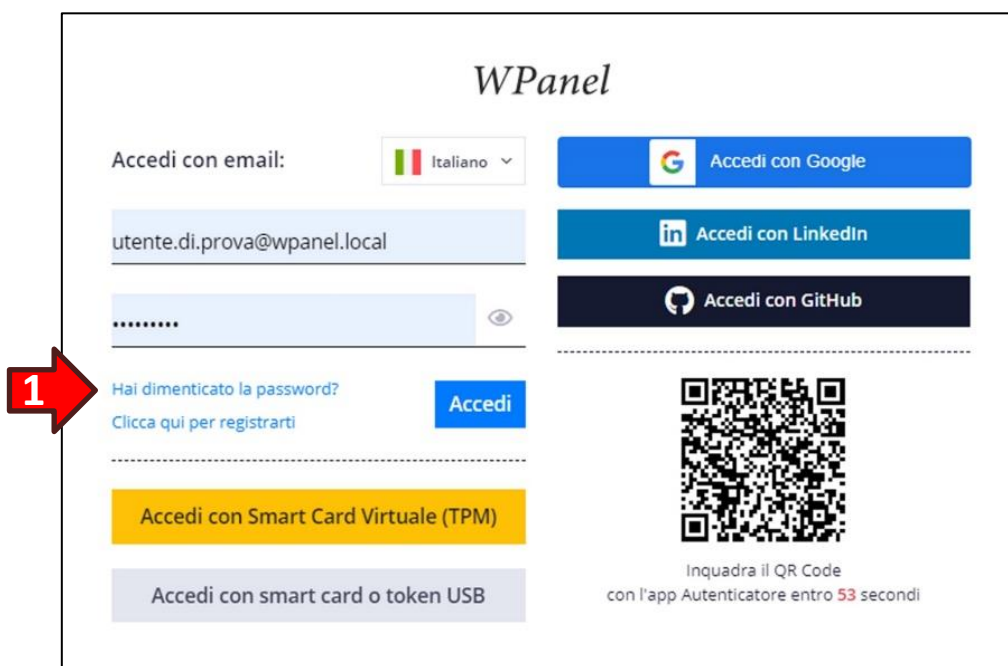
Annulla Conferma

ATTENZIONE! Se la registrazione al sito WPanel è avvenuta tramite un provider di identità digitali OpenID Connect non verrà richiesta la password ma verrà semplicemente ripristinato l'accesso tramite il provider utilizzato.

20. Accesso al sito WPanel in caso di smarrimento del dispositivo sicuro

ATTENZIONE! Prima di iniziare questa procedura munirsi del **Foglio recupero account** allegato all’email di registrazione del sito WPanel del vostro fornitore.

Avviare la tipica procedura di recupero password cliccando sulla dicitura **Hai dimenticato la password? (1)** nella form di login al sito WPanel:

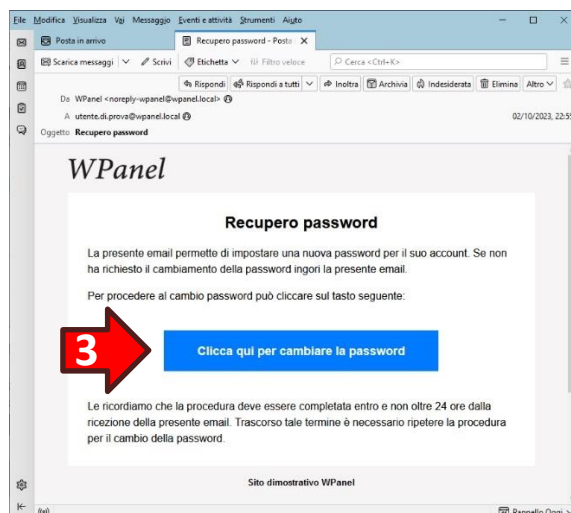


Inserire l’**indirizzo email (2)** utilizzato per registrarsi sul sito WPanel.

ATTENZIONE! Se si è utilizzato un provider di identità digitali OpenID Connect utilizzare l’indirizzo email con cui ci si è registrati presso il provider.



Se l'indirizzo email è corretto si riceverà la tipica email per il recupero della password. Cliccare quindi sul link associato al tasto **Clicca qui per cambiare la password (3)**:



Si aprirà la form di creazione della password di accesso al sito WPanel contestualmente alla disabilitazione dell'accesso con il dispositivo sicuro.

L'utente ha **5 minuti (4)** di tempo per inserire e confermare una **nuova password (5)** di accesso e inserire i tre codici di 8 cifre indicati nel **Foglio recupero account (6)**.

ATTENZIONE! I codici sono codificati come immagine quindi per ragioni di sicurezza non possono essere selezionati e copiati dal file PDF ma devono essere trascritti manualmente.

ATTENZIONE! Se la registrazione al sito WPanel è avvenuta tramite un provider di identità digitali OpenID Connect non verrà richiesta la password ma verrà semplicemente ripristinato l'accesso tramite il provider utilizzato.

21. Revoca dei certificati

Onde precludere l'accesso al vostro VPS in caso di malfunzionamento del sito WPanel del vostro fornitore **non vengono gestite le liste di revoca dei certificati dalla PKI WPanel** né sono disponibili risponditori OCSP.

Questo significa che i certificati emessi nella PKI WPanel del vostro fornitore non possono essere revocati.

Qualora un dispositivo sicuro o un certificato dovessero essere compromessi è necessario:

- Disattivare l'accesso al sito WPanel per quel certificato dalla scheda *Certificati*, come indicato al **Capitolo 11. Elenco dei certificati emessi e creazione di un nuovo certificato**;
- Generare nuovi certificati con UPN mai utilizzati prima e associare questi nuovi UPN negli utenti dei VPS, come descritto nel **Capitolo 15. Mappatura degli UPN agli utenti del VPS**.

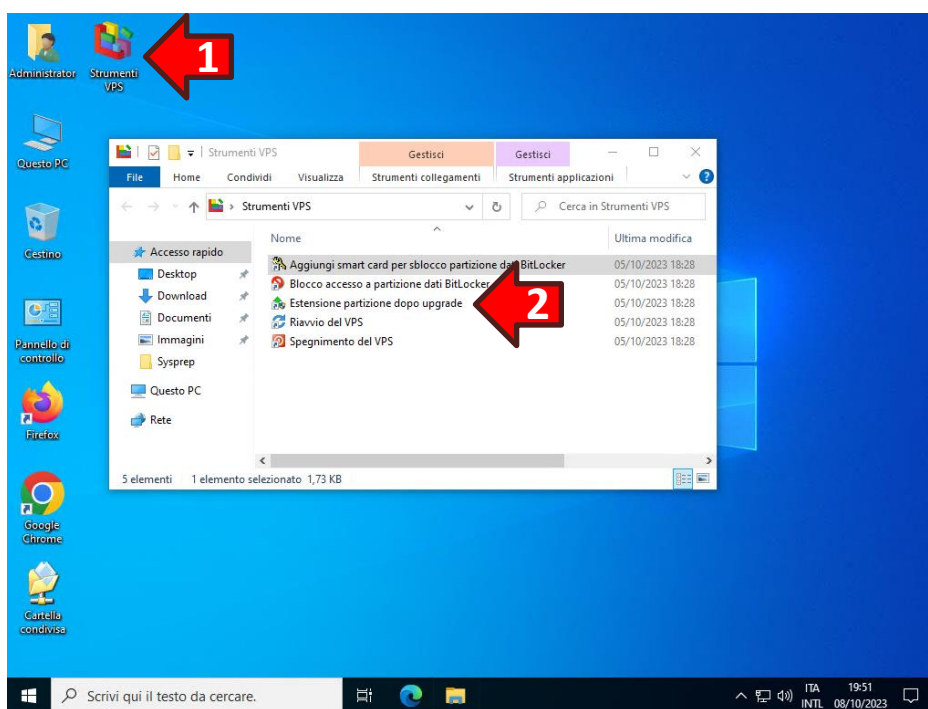
22. Estensione della partizione BitLocker dopo un upgrade

L'upgrade di un VPS comporta il suo spegnimento ed il conseguente blocco della partizione BitLocker. Al successivo riavvio il software WPanel non è in grado di sbloccare tale partizione e di conseguenza non può aumentarne la dimensione.

ATTENZIONE! L'operazione di allargamento della partizione BitLocker deve essere effettuata manualmente dall'utente dopo aver effettuato lo sblocco.

Per effettuare l'allargamento della partizione in seguito ad un upgrade:

1. Accedere al desktop del VPS;
2. Sbloccare la partizione BitLocker con la smart card;
3. Dal desktop del VPS aprire la cartella **Strumenti VPS (1)**;
4. Fare doppio click sull'icona **Estensione partizione dopo upgrade (2)**;



5. Confermare la richiesta di **modifiche al dispositivo (3)**.

