Regione Basilicata

Guida Firma Remota per Windows

Categoria	**TSP-Firma Digitale**	Codice Documento	**NAM-Guida Remota Win-RegBas**	**Namirial S.p.A.**
Redatto da	**Umberto Ferrara**	Nota di riservatezza	**Documento Pubblico**	Registration Authority
Verificato da	**Antonio Taurisano**	Versione	**1.1**	**Antonio Taurisano**
Approvato da	**Antonio Taurisano**	Data di emissione	**24/06/2020**	_____

Namirial S.p.A.

Sede legale, direzione e amministrazione 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
C.F./ISCR. REG. IMPR. ANCONA N.02046570426 - P.I. IT02046570426 - CAP. SOC. € 6.500.000,00 i.v.
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

UNI EN ISO 9001:2015 - Certificato N. 223776 | **UNI EN ISO 27001:2013** - Certificato N. IT280490

– Questa pagina è lasciata intenzionalmente in bianco –

INDICE

STORIA DELLE MODIFICHE APPORTATE

VERSIONE	**1.0**
Data	15/01/2020
Motivazione	Prima emissione
Modifiche	

VERSIONE	**1.1**
Data	24/06/2020
Motivazione	Aggiornamento
Modifiche	Modificati i riferimenti al servizio di assistenza

INDICE DELLE FIGURE

1 INTRODUZIONE

Nell'Ordinamento Giuridico Italiano il termine FIRMA DIGITALE sta a indicare un tipo di firma elettronica qualificata, alla quale si attribuisce piena efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa. Così come la firma autografa sul documento cartaceo, la firma digitale può essere apposta su un documento informatico.

La tecnologia alla base della firma digitale garantisce, inoltre, che il documento firmato non possa essere in seguito modificato senza invalidare la firma stessa, e consente di associare al documento una data e un'ora certe, attraverso il meccanismo della marca temporale.

FirmaCerta è lo strumento ideale per firmare contemporaneamente grandi volumi di documenti digitali, come fatture, polizze, ricevute di pagamenti, bonifici e qualsiasi altro documento digitale;

- La firma dei documenti mantenendo il formato originale (il .PDF o .XML dopo essere stato firmato mantenendo lo stesso formato);
- La possibilità di poter scegliere il dispositivo hardware col quale si desidera apporre la firma (Smart Card - Token);
- La possibilità di apporre/associare una marca temporale ad un documento o a una firma (Grafometrica);
- Consente il drag & drop di uno o più file all'interno della stessa finestra di firma.
- Consente la firma di documenti .PDF protetti da password.

1.1 SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

Il presente documento è una "guida rapida" alla corretta configurazione del software Firmacerta per i possessori di una Firma Remota, una particolare firma digitale attraverso un certificato che non risiede su un dispositivo fisico in possesso del cliente ma che è installato su HSM (Hardware Security Module) della Certification Authority Namirial. Per poter utilizzare il certificato è necessario utilizzare:

- un PIN statico che viene inviato all'emissione del certificato stesso
- una codice OTP (One Time Password) che viene generato al momento dell'utilizzo e che viene usato una sola volta (usa e getta).

La Firma Remota garantisce altissimi livelli di sicurezza e disponibilità del servizio inoltre consente di utilizzare il servizio sia su sistemi Desktop che su sistemi Mobile.

2 INSTALLAZIONE E CONFIGURAZIONE INIZIALE

La configurazione ed installazione iniziale dipende dalla tipologia di dispositivo OTP (One Time Password) che viene utilizzato per la firma e che può essere:

- OTP fisico, cioè il classico OTP spesso usato nei servizi di home banking (vedi figura)
- OTP Virtuale, cioè OTP generato da una APP scaricabile su smartphone

Il dispositivo fisico utilizzato è il modello C-100.

Figura 1: OTP Fisico Modello C-100

2.1 INSTALLAZIONE E CONFIGURAZIONE SOFTWARE FIRMACERTA

Prima di poter utilizzare la firma remota è necessario effettuare le seguenti operazioni:

1) Download ed installazione del software **Firmacerta**. Il software può essere scaricato al seguente Link.
2) Abilitazione del servizio **SignEngine** sul software Firmacerta. Per farlo è necessario andare nella sezione *FirmaCerta -> Utilità -> Opzioni Generali -> Servizi Web*, selezionare la voce *SignEngine* e cliccare su Abilita.

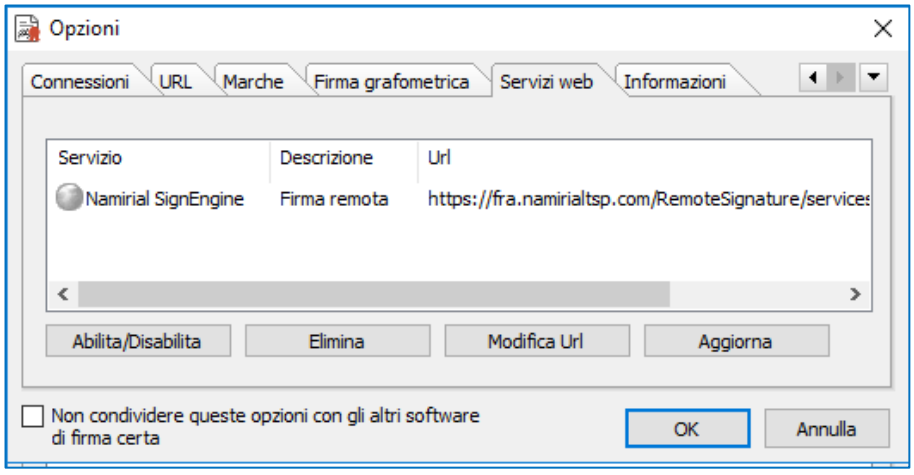


Figura 2: Abilitazione Servizio SignEngine

2.2 INSTALLAZIONE E CONFIGURAZIONE APP NAMIRIAL OTP (OTP VIRTUALE)

Namirial OTP è un'applicazione per dispositivi mobile per l'utilizzo delle così dette One Time Password (o password usa-e-getta). Questo tipo di password viene utilizzato ogni qual volta si richieda un'autenticazione con un alto livello di sicurezza (autenticazione forte). L'applicazione, oltre ad essere usata per la firma remota può essere usata anche:

- Per l'accesso SPID di livello 2 o superiore mediante servizio **Namirial ID**;
- Per l'accesso all'area privata dei servizi Namirial TS.

2.2.1 COME OTTENERLA

L'applicazione Namirial OTP è disponibile gratuitamente sia per **Android** (ver. 4.3 o superiore) scaricabile dal Google Play Store che per **iOS** (ver. 9 o superiore), scaricabile dal App Store.
Una volta istallata, per poter essere usata è necessario effettuare la procedura di prima attivazione.

2.2.2 ATTIVAZIONE INIZIALE NAMIRIAL OTP

Per eseguire la prima attivazione, l'utente deve avviare l'applicazione ed inserire il codice ricevuto via SMS al numero di cellullare registrato in fase di richiesta per l'attivazione del servizio (Firma Remota, SPID o altro servizio Namirial TSP).
Di seguito, al solo titolo d'esempio, è mostrato un messaggio SMS per l'attivazione del Virtual OTP.

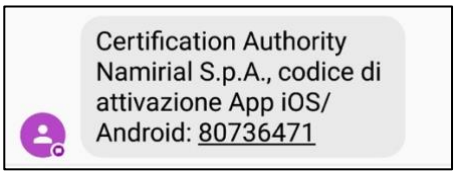


Figura 3: Esempio SMS con codice attivazione

2.2.2.1 ATTIVAZIONE APP SU ANDROID

Per l'attivazione di Namirial OTP è necessario fare tap su *Aggiungi OTP*
Di seguito, sono rappresentate la sequenza di azioni su Android che illustrano come procedere.

Figura 4: Schermata iniziale di Namirial OTP. Fare tap sul bottone rosso

Figura 5: Fare tap sul bottone verde (Aggiungi OTP)

Figura 6: Inserimento codice ed assegnazione etichetta

Nell'ultima schermata:

- ***Nome dell'OTP:*** è l'etichetta attribuibile al singolo token OTP per la quale può essere scelto un nome a piacimento (es. Firma). L'etichetta è di aiuto nell'individuare il token da utilizzare nel caso in cui sull'applicazione vengano attivati più token simultaneamente.
- ***Codice di attivazione App*:** qui va inserito il codice di attivazione ricevuto tramite SMS. nel campo *Token (numero di 8 cifre).*

2.2.2.2 ATTIVAZIONE APP SU IOS

Per l'attivazione del Virtual OTP è necessario fare tap su *Aggiungi OTP*
Di seguito, sono invece rappresentate la sequenza di azioni su iOS che illustrano come procedere.

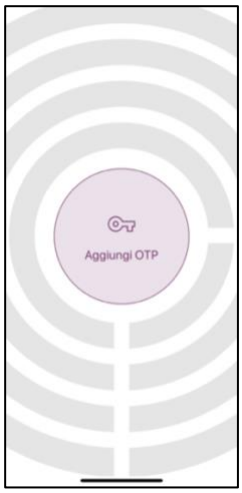


Figura 7: Schermata iniziale di Virtual OTP. Fare tap su Aggiungi OTP

Figura 8: Inserimento codice ed assegnazione etichetta

Nell'ultima schermata:

- ***Nome dell'OTP:*** è l'etichetta attribuibile al singolo token OTP per la quale può essere scelto un nome a piacimento (es. Firma). L'etichetta è di aiuto nell'individuare il token da utilizzare nel caso in cui sull'applicazione vengano attivati più token simultaneamente.
- ***Codice di attivazione App*:** qui va inserito il codice di attivazione ricevuto tramite SMS. nel campo *Token (numero di 8 cifre).*

N.B: *cliccando sull' icona* *vedrete in chiaro il codice che inserito.*
Una volta inserite le informazioni è sufficiente cliccare su *Aggiungi* per attivare l'OTP.
Al termine della procedura sarà mostrato a video un codice di 6 cifre che si aggiorna ogni 30 sec.

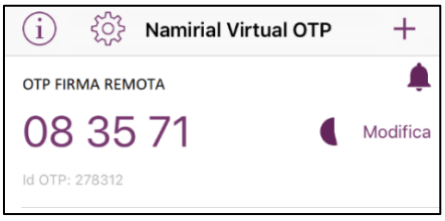


Figura 9: Schermata codice OTP generato dall'APP

2.2.3 COME USARE NAMIRIAL OTP

Per questioni di sicurezza, l'apertura dell'App è possibile solo previa operazione di sblocco che può avvenire con il meccanismo di sblocco del telefono oppure tramite PIN appositamente inserito.

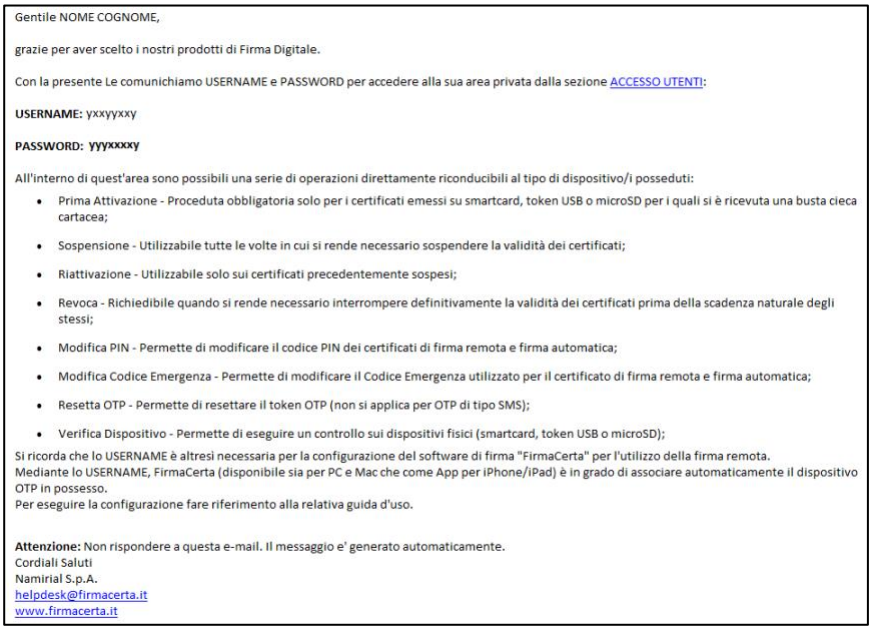
- Se l'utente ha abilitato sul proprio telefono un meccanismo di blocco/sblocco, è possibile usarlo anche per sbloccare Namirial OTP. I meccanismi di sblocco possono essere:
  - Digitazione PIN;
  - Esecuzione del Segno;

- Riconoscimento Biometrico: Impronta digitale (Touch ID), Riconoscimento del volto (Face ID)

- Se l'utente non ha impostato alcun meccanismo di blocco/sblocco, l'applicazione richiede di scegliere un apposito PIN da utilizzare.

2.2.4 ATTIVAZIONE INIZIALE OTP FISICO

Per attivare l'OTP fisico (token) è necessario accedere all'areaPrivata Namirial inserendo le credenziali Username e Password che sono state inviate all'indirizzo e-mail fornito in fase di registrazione. Di seguito un esempio di email



Gentile NOME COGNOME,

grazie per aver scelto i nostri prodotti di Firma Digitale.

Con la presente Le comunichiamo USERNAME e PASSWORD per accedere alla sua area privata dalla sezione ACCESSO UTENTI:

USERNAME: yxxyyxxy

PASSWORD: **yyyxxxxy**

All'interno di quest'area sono possibili una serie di operazioni direttamente riconducibili al tipo di dispositivo/i posseduti:

- Prima Attivazione - Proceduta obbligatoria solo per i certificati emessi su smartcard, token USB o microSD per i quali si è ricevuta una busta cieca cartacea;
- Sospensione - Utilizzabile tutte le volte in cui si rende necessario sospendere la validità dei certificati;
- Riattivazione - Utilizzabile solo sui certificati precedentemente sospesi;
- Revoca - Richiedibile quando si rende necessario interrompere definitivamente la validità dei certificati prima della scadenza naturale degli stessi;
- Modifica PIN - Permette di modificare il codice PIN dei certificati di firma remota e firma automatica;
- Modifica Codice Emergenza - Permette di modificare il Codice Emergenza utilizzato per il certificato di firma remota e firma automatica;
- Resetta OTP - Permette di resettare il token OTP (non si applica per OTP di tipo SMS);
- Verifica Dispositivo - Permette di eseguire un controllo sui dispositivi fisici (smartcard, token USB o microSD);

Si ricorda che lo USERNAME è altresì necessaria per la configurazione del software di firma "FirmaCerta" per l'utilizzo della firma remota.
Mediante lo USERNAME, FirmaCerta (disponibile sia per PC e Mac che come App per iPhone/iPad) è in grado di associare automaticamente il dispositivo OTP in possesso.
Per eseguire la configurazione fare riferimento alla relativa guida d'uso.

Attenzione: Non rispondere a questa e-mail. Il messaggio e' generato automaticamente.
Cordiali Saluti
Namirial S.p.A.
helpdesk@firmacerta.it
www.firmacerta.it

Figura 10: esempio email con le credenziali

***RECUPERO CREDENZIALI AREA PRIVATA**: In caso di smarrimento della username è possibile contattare Il servizio di assistenza via email all'indirizzo:* centroservizi@regione.basilicata.it*, indicando come OGGETTO: Recupero Username Firma Remota ed inserendo, nel corpo del messaggio, il nome cognome e codice fiscale del titolare del dispositivo di firma.*

All'interno dell'area privata, nel Menù laterale a destra, sotto la categoria FIRMA REMOTA è necessario cliccare su *Attivazione* e verificare che il numero di serie coincide con il numero di serie presente nel OTP FISICO.

Figura 11: Otp Fisico

A questo punto è necessario generare il codice con l'OTP, premendo il pulsante sul dispositivo, aggiungere il codice generato nel campo *Codice OTP e* premere il tasto **Attiva.**

Figura 12: Schermata Area Privata

3 COME FIRMARE UN DOCUMENTO

La firma dei documenti si differenzia in base al tipo di dispositivo OTP (One Time Password) che viene utilizzato. Di seguito vengono descritte le modalità di firm in caso di OTP virtuale su APP e di dispositivo OTP fisico.

Per firmare un documento, è necessario caricare il file all'interno del programma e cliccare sulla voce ***Firma***. Per selezionare il file è possibile cliccare sul tasto Firma e poi scegliere il file dalle cartelle del PC, oppure trascinare il file sull'icona Firma (drag & drop).

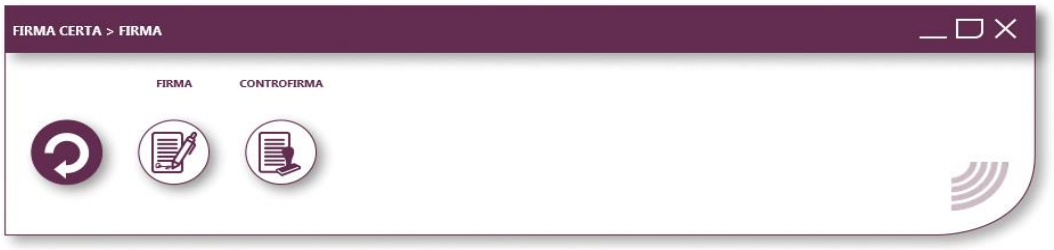


Figura 13: Pannello di Firma

Il software Firmacerta permette di firmare qualsiasi tipo di file in formato CAdES ovvero in .p7m.
Per i file PDF o XML il software chiederà all'utente se desidera firmare in formato .P7M (CAdES) o mantenere il formato originale (firma PaDES o XaDES). Di seguito il messaggio che viene rispettivamente visualizzato per i file XML e PDF:

Premere ***Si***, per effettuare una firma XAdES, mantenendo il formato .xml (valido solo per file XML) Premere ***No***, per effettuare una firma CAdES con il formato .p7m	Premere ***Si***, per effettuare una firma PAdES, mantenendo il formato .pdf (valido solo per file PDF) Premere ***No***, per effettuare una firma CAdES con il formato .p7m

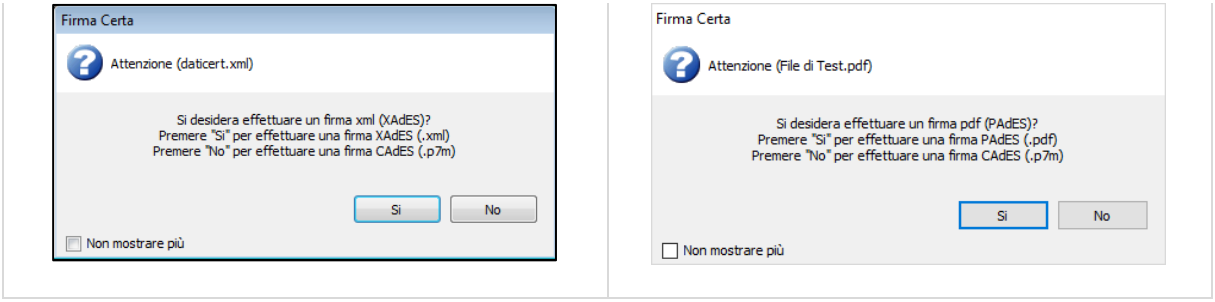


Figura 14: Scelta formato di firma

A questo punto è necessario selezionare la Cartella di destinazione del File Firmato e confermare cliccando su ***OK***

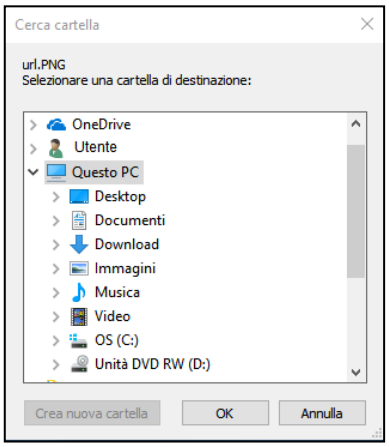


Figura 16: Selezione cartella di destinazione

Procedere con l'operazione di Firma premendo ***Si.***

N.B: *Consigliamo di creare una cartella dedicata per i File Firmati Digitalmente, così da evitare di sovrascrivere i file precedenti*

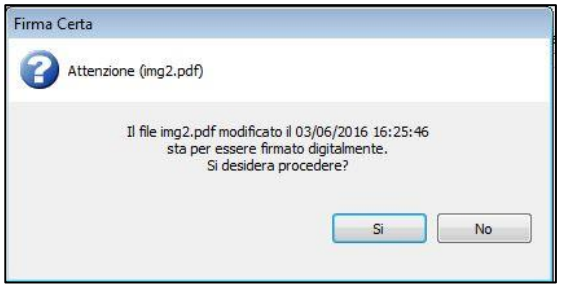


Figura 15: Conferma di firma

Una volta scelta la cartella di destinazione, viene visualizzata una finestra di selezione del dispositivo virtuale. La prima volta è necessario inserire la propria *username* cliccando sul tasto ***Impostazioni*** :

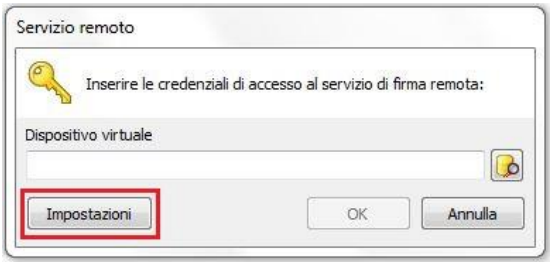
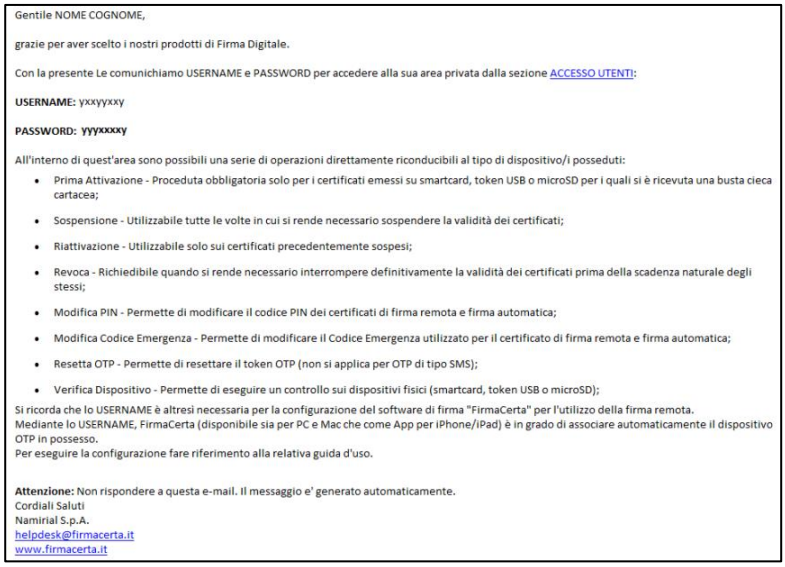


Figura 17: Configurazione servizio remoto

Figura 18: Inserimento nome utente

ATTENZIONE: *la username da inserire è la stessa utilizzata per accedere all'Area Privata Namirial ed è stata inviata per email all'attivazione del certificato. Di seguito un esempio di email*



Gentile NOME COGNOME,

grazie per aver scelto i nostri prodotti di Firma Digitale.

Con la presente Le comunichiamo USERNAME e PASSWORD per accedere alla sua area privata dalla sezione ACCESSO UTENTI:

USERNAME: yxxyyxxy

PASSWORD: yyyxxxxy

All'interno di quest'area sono possibili una serie di operazioni direttamente riconducibili al tipo di dispositivo/i posseduti:

- Prima Attivazione - Proceduta obbligatoria solo per i certificati emessi su smartcard, token USB o microSD per i quali si è ricevuta una busta cieca cartacea;
- Sospensione - Utilizzabile tutte le volte in cui si rende necessario sospendere la validità dei certificati;
- Riattivazione - Utilizzabile solo sui certificati precedentemente sospesi;
- Revoca - Richiedibile quando si rende necessario interrompere definitivamente la validità dei certificati prima della scadenza naturale degli stessi;
- Modifica PIN - Permette di modificare il codice PIN dei certificati di firma remota e firma automatica;
- Modifica Codice Emergenza - Permette di modificare il Codice Emergenza utilizzato per il certificato di firma remota e firma automatica;
- Resetta OTP - Permette di resettare il token OTP (non si applica per OTP di tipo SMS);
- Verifica Dispositivo - Permette di eseguire un controllo sui dispositivi fisici (smartcard, token USB o microSD);

Si ricorda che lo USERNAME è altresì necessaria per la configurazione del software di firma "FirmaCerta" per l'utilizzo della firma remota.
Mediante lo USERNAME, FirmaCerta (disponibile sia per PC e Mac che come App per iPhone/iPad) è in grado di associare automaticamente il dispositivo OTP in possesso.
Per eseguire la configurazione fare riferimento alla relativa guida d'uso.

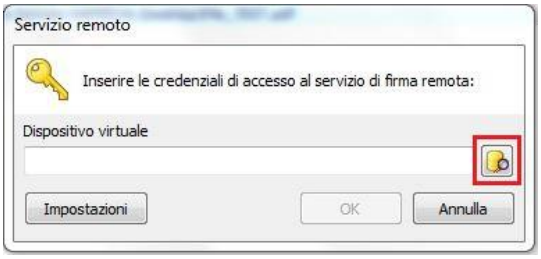
Attenzione: Non rispondere a questa e-mail. Il messaggio e' generato automaticamente.
Cordiali Saluti
Namirial S.p.A.
helpdesk@firmacerta.it
www.firmacerta.it

Figura 19: Esempio email con le credenziali

***RECUPERO CREDENZIALI AREA PRIVATA**: In caso di smarrimento della username è possibile contattare Il servizio di assistenza via email all'indirizzo:* centroservizi@regione.basilicata.it*, indicando come OGGETTO: Recupero Username Firma Remota ed inserendo, nel corpo del messaggio, il nome cognome e codice fiscale del titolare del dispositivo di firma.*

L'inserimento della Username deve essere fatto solamente la prima volta. Le volte successive è sufficiente selezionare solamente il dispositivo remoto come decritto di seguito.

Cliccare sulla figura nel riquadro rosso, per inserire il vostro *Dispositivo virtuale* di Firma.



Nella seguente finestra sono presenti tutti i vostri dispositivi virtuali di Firma, quindi selezionare quello desiderato e poi click *Ok*.

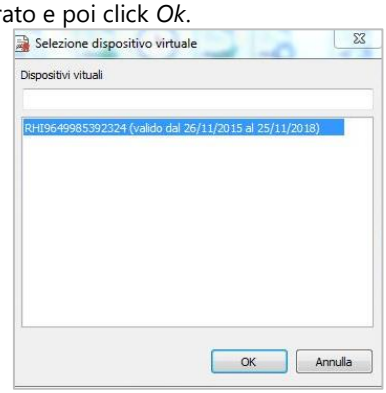


Figura 20: Selezione del dispositivo virtuale remoto

Inserito il dispositivo virtuale confermare cliccando su OK.

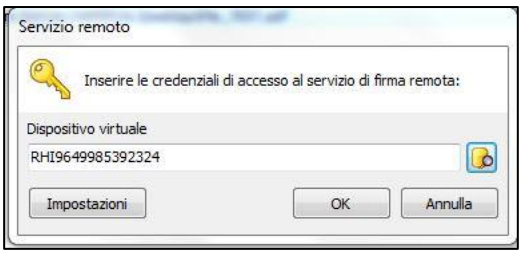


Figura 21: Conferma dispositivo remoto

Una volta effettuate queste operazioni comuni per tutti i tipi di OTP, l'operazione di firma è diversa nel caso in cui si utilizzi l'OTP virtuale o fisico. Di seguito la descrizione di entrambe le procedure.

3.1 FIRMA CON OTP VIRTUALE (NAMIRIAL OTP)

Di seguito la descrizione della finalizzazione del processo di firma nel caso di APP OTP su smartphone.

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Cliccare sulla figura nel riquadro rosso, Selezionare il Dispositivo OTP poi cliccare OK
Da questa schermata si legge la tipologia di OTP in questo caso **GENERATOR**

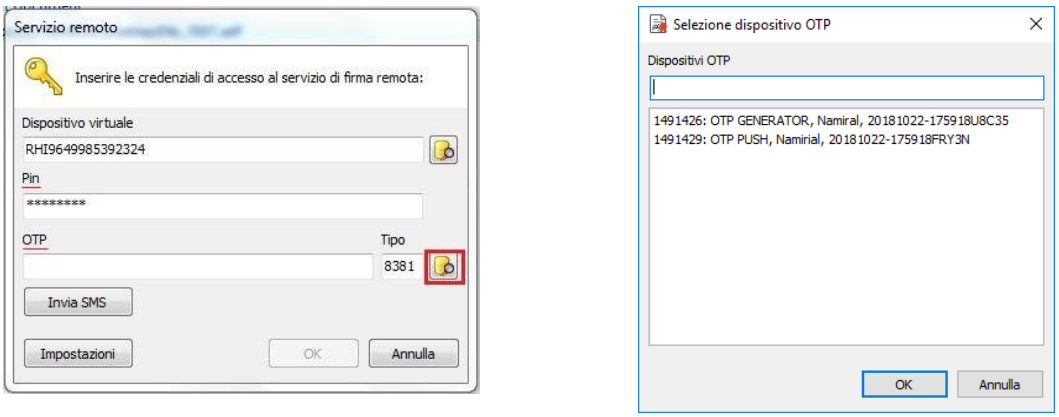


Figura 22: Selezionare dispositivo OTP

Aprire l'applicazione Namirial OTP, e inserire il codice nel riquadro. OTP.

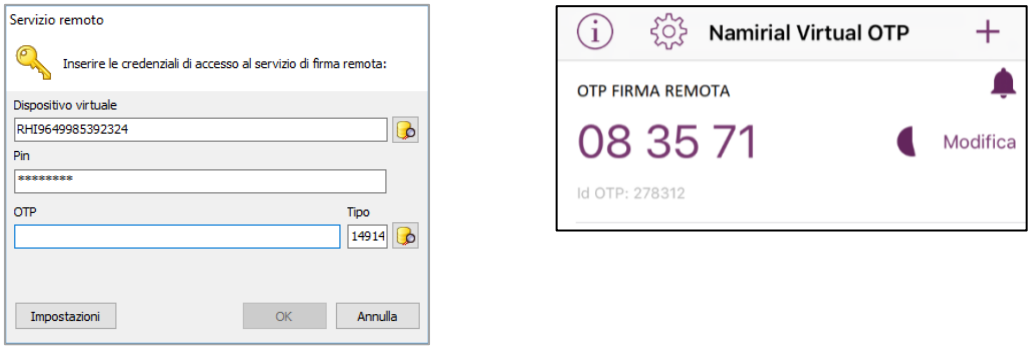


Figura 23: OTP Generator

Alla fine della procedura comparirà il seguente messaggio di Conferma.

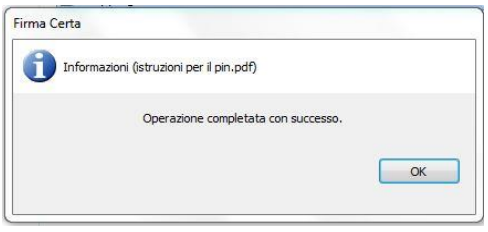


Figura 24: Messaggio di conferma

3.2 FIRMA CON OTP FISICO

Di seguito la descrizione della finalizzazione del processo di firma nel caso OTP fisico.

Inserire il PIN ricevuto tramite Busta Cieca Digitale.

Cliccare sulla figura nel riquadro rosso, Selezionare il Dispositivo OTP poi cliccare OK
Da questa schermata si legge la tipologia di OTP in questo caso **FISIC**

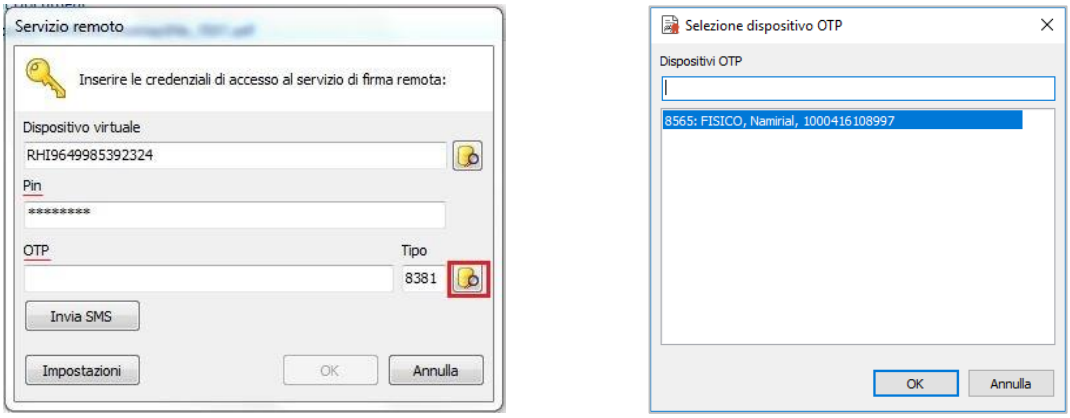


Figura 25: Selezionare dispositivo OTP

Generare il codice OTP, utilizzando il dispositivo assegnato e inserirlo nel campo OTP

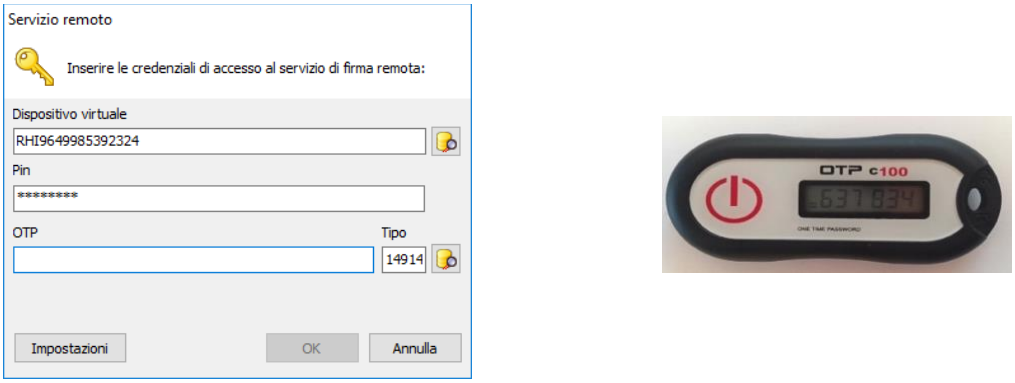


Figura 26: Codice generato con OTP Fisico

Alla fine della procedura comparirà il seguente messaggio di Conferma.

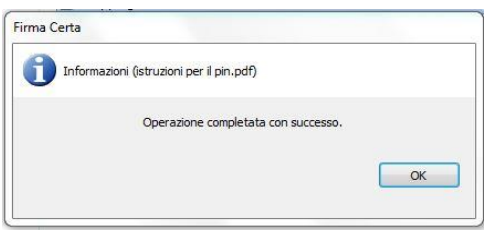


Figura 27: Messaggio di conferma

3.3 FIRMA PDF

In caso di file PDF è possibile effettuare una firma mantenendo il formato originale (vedi 3).
In questo caso, dopo aver selezionato la cartella di destinazione del file, viene visualizzata una finestra nella quale è possibile inserire il motivo della firma, la località ed eventuali informazioni di contatto. Tali informazioni verranno riportate all'interno del file di destinazione e saranno visibili con Adobe.

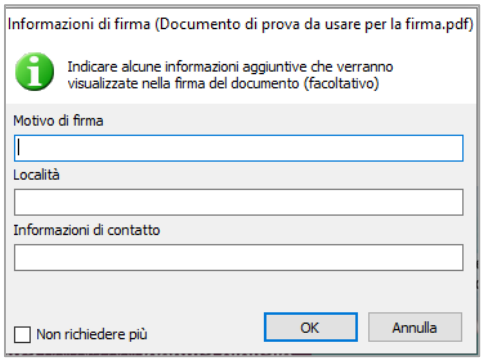


Figura 28: Informazioni aggiuntive sulla firma

Dopo aver confermato l'operazione viene visualizzato il file in modo che l'utente possa scegliere dove inserire l'etichetta di firma.

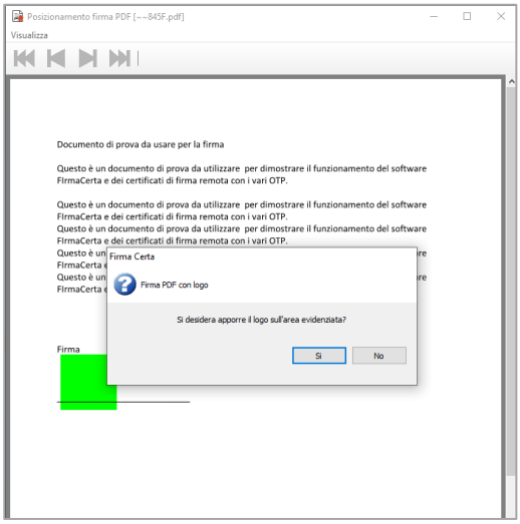


Figura 29: Posizionamento etichetta di firma

A questo punto viene visualizzata la pagina di inserimento PIN e OTP come già descritto ai precedenti paragrafi e l'operazione viene completata.
Aprendo il file con Adobe è possibile vedere l'etichetta di firma, le informazioni inserite al punto precedente (Motivo e Località).

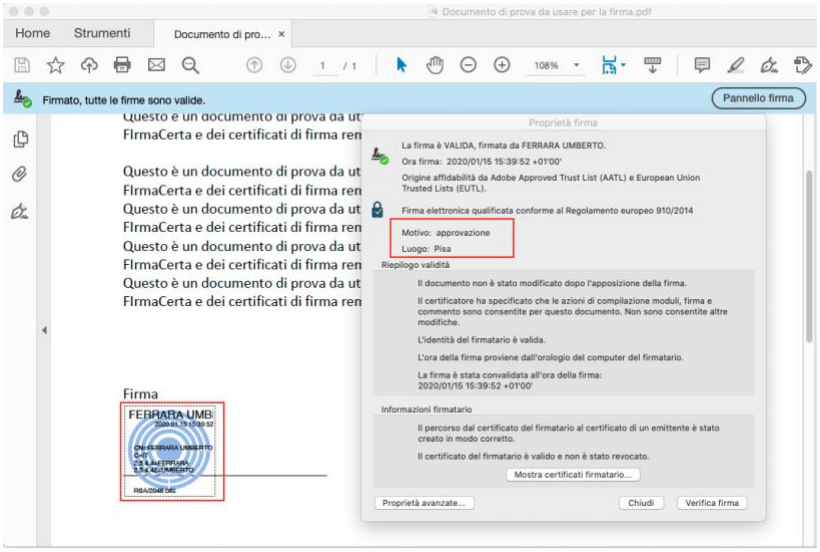


Figura 30: Visualizzazione informazioni aggiuntive firma con Adobe

Cliccando sul tasto Mostra certificati del firmatario è possibile visualizzare i dettagli del certificato usato per la firma.

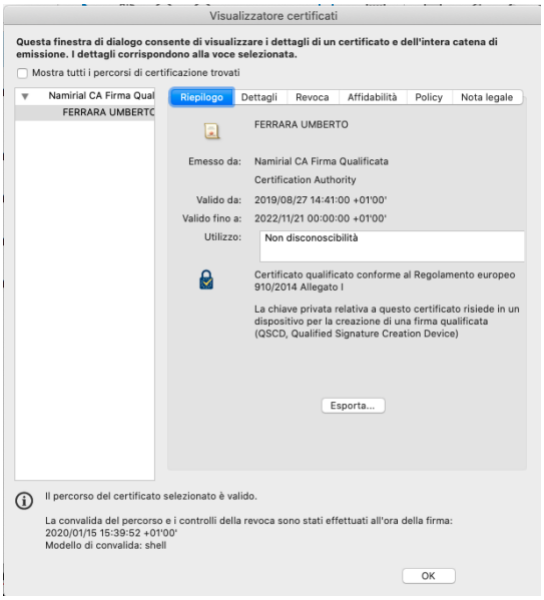


Figura 31: Visualizzazione dettagli certificato con Adobe

4 COME VERIFICARE UN FILE FIRMATO

Il software Firmacerta consente di controllare i file firmati per verificare che la firma sia valida e che sia stato utilizzato un certificato emesso da una Certification Authority riconosciuta ed in corso di validità.
Con FirmaCerta è possibile verificare file firmati anche con altri software e con certificati di Certification Authority diverse da Namirial.

Per verificare un file firmato con FirmaCerta è necessario caricare il file all'interno del programma e cliccare sulla voce ***Firma***. Per caricare il documento è possibile cliccare sul tasto Firma e poi scegliere il file dalle cartelle del PC, oppure trascinare il file sull'icona Verifica (drag & drop).

Figura 32: Interfaccia FirmaCerta – Verifica di un file firmato

Una volta attivata la funzionalità l'applicazione restituisce un risultato come il seguente:

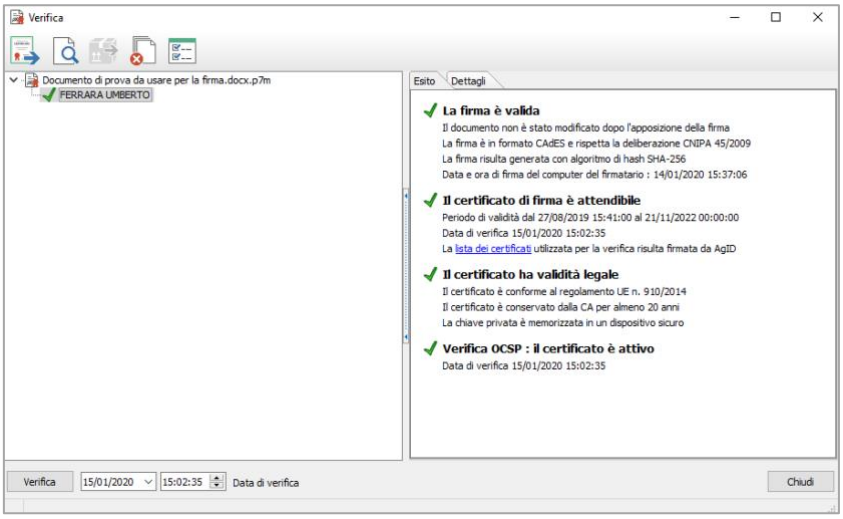


Figura 33: Risultato della verfica

In caso di firma non valida, certificato non valido o scaduto il software restituirà il messaggio opportuno.
Facciamo notare che in basso a sinistra è possibile impostare una data specifica per verificare se, a tale data, il certificato e quindi la firma fosse valida. Questa funzionalità è utile nel caso in cui si vada a verificare la firma apposta molto tempo addietro e, nel frattempo, il certificato usato è scaduto.

Cliccando sul "tab" dettagli è possibile visualizzare ulteriori informazioni relative al certificato utilizzato per la firma (la CA che lo ha emesso, i dati anagrafici del titolare, ecc).

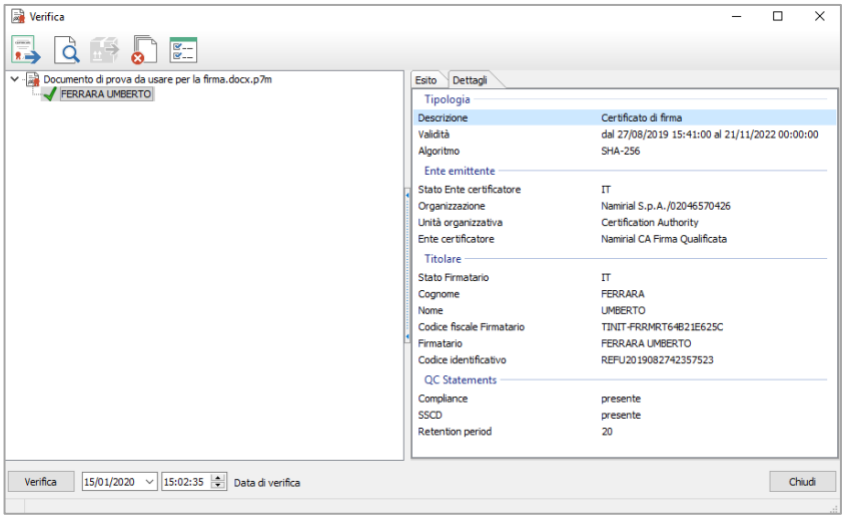


Figura 34: Dettagli certificato usato per la firma