

Firma Digitale e Remota

GUIDA ALL'EMISSIONE DEI CERTIFICATI DA PANNELLO CMS

1

Sommario

1 Introduzione	3
2 Prerequisiti all'utilizzo del CMS.....	3
3 Dispositivi e certificati inclusi nel programma CMS.....	4
4 Autenticazione e accesso al pannello CMS.....	5
4.1 Conclusione operazioni di accesso.....	6
5 Homepage	6
6 Sessioni di lavoro.....	7
7 Procedura di emissione dei certificati.....	7
7.1 Registrazione dati Utente.....	7
7.2 Modalità di riconoscimento.....	13
7.2.1 Riconoscimento in presenza e acquisizione del consenso con Firma Autografa.....	13
Modifica dei dati relativi al rilascio del certificato di Firma Remota.....	16
7.2.2 Riconoscimento in presenza e acquisizione del consenso con Firma Elettronica.....	18
Procedura di correzione della documentazione.....	22
7.2.3 Riconoscimento DVO.....	23
Monitorare lo stato del DVO.....	25
7.2.4 Riconoscimento A Distanza.....	27
Monitorare lo stato del riconoscimento A Distanza.....	35
7.3 Emissione certificati di Firma Digitale con Aruba Enroll.....	36
8 Recupero PIN e PUK Smart Card.....	39
9 Funzionalità aggiuntive del CMS.....	40
9.1 Gestione ciclo di vita dei certificati.....	40
9.1.1 Sospensione del Certificato.....	40
9.1.2 Riattivazione del Certificato.....	41
9.1.3 Revoca del Certificato.....	41
9.2 Controllo delle attività.....	43
10 Rinnovo Certificati	43
10.1 Rinnovo Firma Remota da area Selfcare.....	43
10.2 Rinnovo carta con Aruba Enroll.....	48

1 Introduzione

Aruba PEC riserva un pannello denominato **Certificate Management System** ai clienti che rientrano nel programma CDRL (Centro Di Registrazione Locale) che consente la gestione dei servizi ad esso associati. Il CMS, infatti, è un sistema sviluppato in Java per l'emissione e la gestione di certificati digitali.

Ciascun CDRL dovrà preliminarmente sottoscrivere un apposito contratto di nomina degli **operatori di registrazione (ODR)**, i quali, superato con successo il corso di formazione organizzato da Aruba PEC e conseguentemente censiti sul sistema, potranno accedere al pannello per l'espletamento delle attività a loro delegate.

Attraverso il CMS è possibile compiere le seguenti principali operazioni:

- 1) registrazione e attivazione di Certificati di Firma Digitale;
- 2) registrazione e attivazione di Certificati di Firma Remota;
- 3) gestione del ciclo di vita dei certificati emessi (sospensione, riattivazione, revoca);
- 4) gestione delle operazioni di rinnovo dei certificati emessi.

Il CMS **registra gli eventi e le attività svolte dall'operatore**. Tutti i dati sensibili sono protetti da chiavi crittografiche.

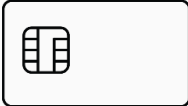
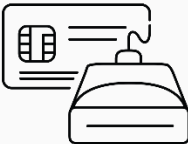
2 Prerequisiti per l'utilizzo del CMS

Per accedere al CMS e poterlo utilizzare correttamente si rendono necessari i seguenti requisiti:

3

- **PC** con sistema operativo Windows 7 o superiore;
- **browser** Internet Explorer, Mozilla Firefox o Google Chrome;
- installazione **Java** (versione 7 e successive);
- **connessione ad Internet** in grado di raggiungere l'indirizzo del CMS;
- **installazione dei driver** per i dispositivi da utilizzare (Smart Card operatore/vergini da produrre e lettori);
- **un lettore Smart Card** per la produzione di dispositivi;
- **stampante** per la produzione della modulistica necessaria al rilascio dei Certificati;
- **dispositivi vergini** (Smart Card) sui quali emettere i Certificati richiesti;
- **scanner** per la scansione dei documenti.

3 Dispositivi e Certificati inclusi nel Programma CDRL

IMMAGINE DISPOSITIVO	TIPOLOGIA DISPOSITIVO	CARATTERISTICHE
	Smart Card vergine	È il dispositivo vergine sul quale è possibile emettere Certificati.
	Smart Card/Sim Card vergine	È il dispositivo vergine sul quale è possibile emettere Certificati destinati all'utilizzo tramite Token/Aruba Key.
	Smart Card/Sim Card CNS vergine	È la Smart Card sulla quale è possibile emettere Certificati CNS.
	Aruba KEY	È il dispositivo completo che consente l'utilizzo di Certificati emessi su Smart Card/Sim Card. Contiene un software di firma preinstallato ed è utilizzabile tramite porta USB.
	Lettore Smart Card	È il dispositivo USB che consente l'utilizzo di Smart Card in lettura (es. login o apposizione di firme) e in scrittura (es. produzione Certificati).

	Token USB	È il dispositivo USB, in formato "pen-drive", che consente l'utilizzo di Smart Card/Sim Card in lettura (es. login o apposizione di firme) e in scrittura (es. produzione Certificati).
	OTP con display	È il dispositivo che genera One Time Password (OTP) necessarie all'apposizione di Firme Digitali Remote.
	OTP USB	È il dispositivo USB che genera One Time Password (OTP) necessarie all'apposizione di Firme Digitali Remote.
	OTP mobile	È il software, installabile sul proprio smartphone, che genera One Time Password (OTP).

5

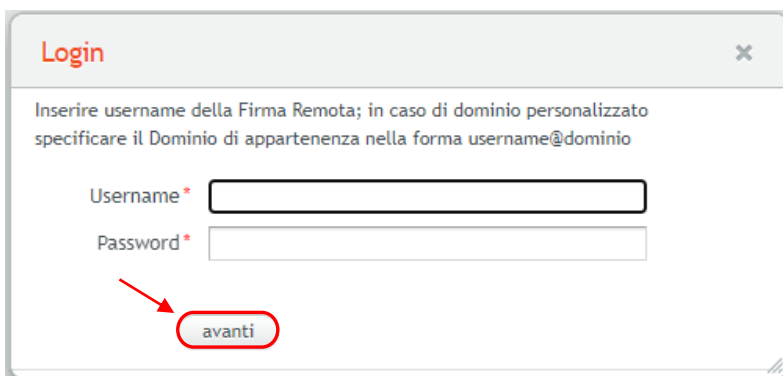
4 Autenticazione e accesso al pannello CMS

Il CMS è raggiungibile collegandosi al seguente link: <https://cms.gruppoaruba.it/CMSARUBA/cmsaruba/>

Gli operatori potranno autenticarsi al pannello con la Firma Remota Aruba rilasciatagli a tale scopo.

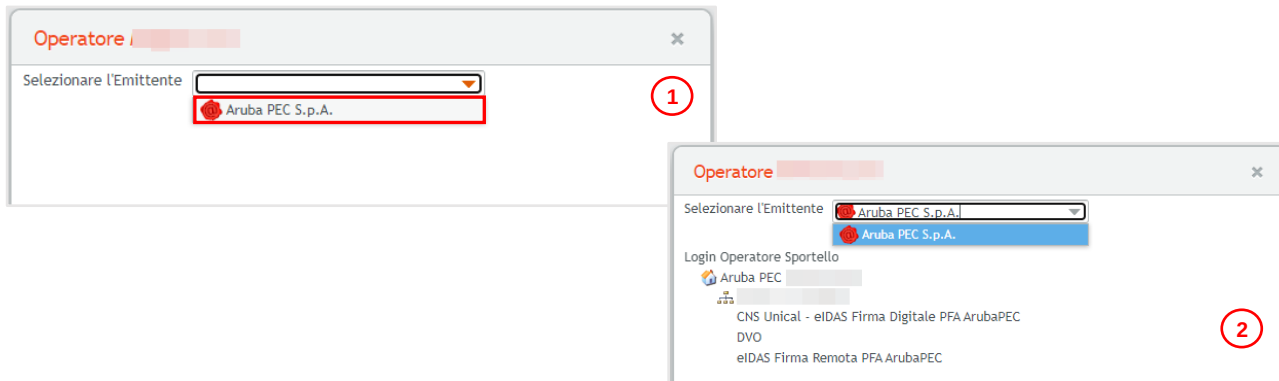
Una volta premuto il pulsante **Login**, apparirà la finestra dedicata all'inserimento delle relative credenziali. Provvedere in tal senso compilando i campi username e password (in caso di dominio personalizzato specificare *username@dominio*).

Dopodiché cliccare su **avanti** ed inserire il codice OTP nell'apposta casella. Premere quindi il tasto Login.



4.1 Conclusione operazioni di accesso

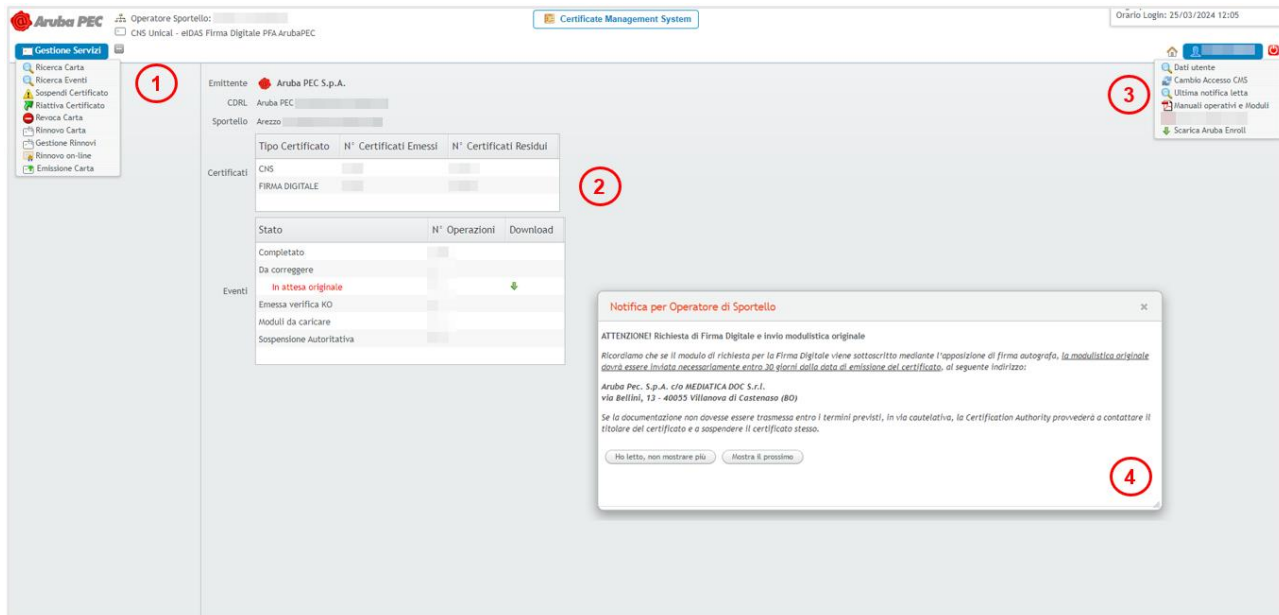
Una volta effettuata l'autenticazione al pannello, comparirà apposita finestra con l'indicazione del nome dell'operatore in quel momento collegato e menù a tendina nel quale selezionare il circuito di emissione (1) e il servizio di interesse (2) [**gli stessi varieranno a seconda delle proprie abilitazioni**].



5 Homepage

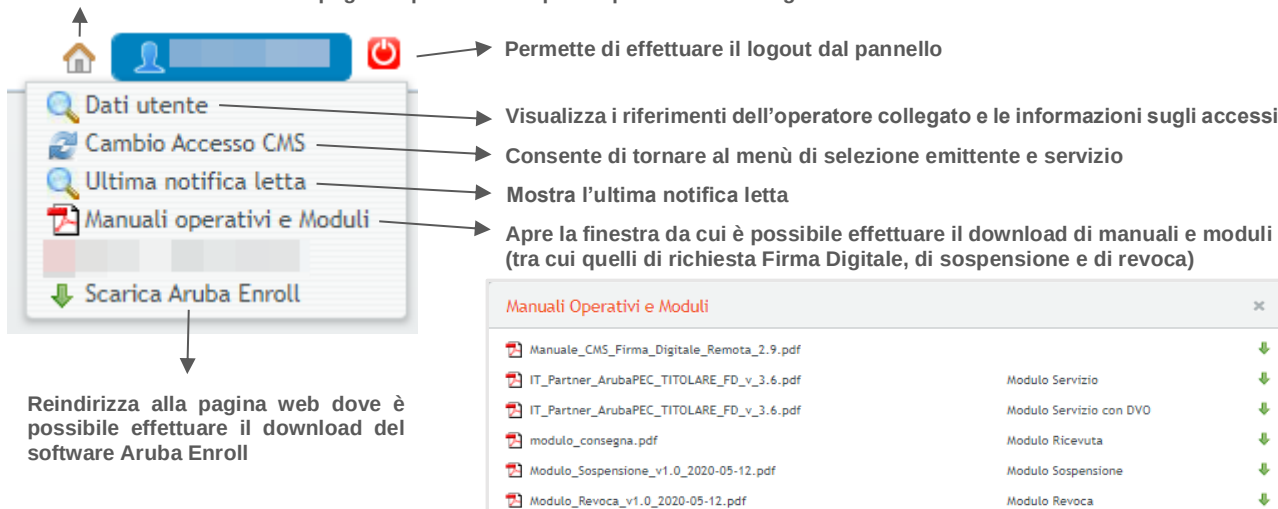
Effettuato l'accesso al pannello, apparirà la relativa homepage. La stessa presenta un menù sulla sinistra (1) dedicato alle funzioni per la gestione dei certificati di Firma Digitale, una dashboard riepilogativa su certificati ed eventi (2) a centro pagina [parametrata al servizio scelto in sede di accesso al pannello. Nell'esempio CNS Unical – eIDAS Firma Digitale], un menù sulla destra (3) funzionale, tra gli altri, alla gestione degli accessi e al download delle guide e della modulistica di riferimento. E', inoltre, prevista una finestra dedicata alle eventuali comunicazioni da parte della Certification Authority (4).

6



Considerato che le funzioni relative alla gestione dei certificati di Firma Digitale verranno illustrate nelle pagine seguenti, proponiamo di seguito schema riepilogativo del menù individuato sopra dal numero 3.

Consente di tornare alla homepage del pannello da qualunque livello di navigazione



Permette di effettuare il logout dal pannello

Visualizza i riferimenti dell'operatore collegato e le informazioni sugli accessi

Consente di tornare al menù di selezione emittente e servizio

Mostra l'ultima notifica letta

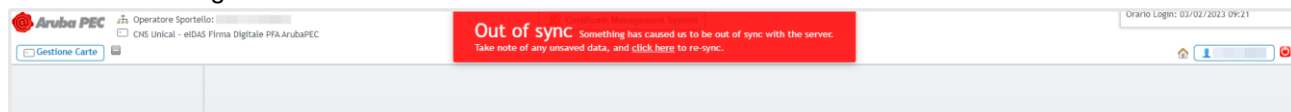
Apre la finestra da cui è possibile effettuare il download di manuali e moduli (tra cui quelli di richiesta Firma Digitale, di sospensione e di revoca)

Reindirizza alla pagina web dove è possibile effettuare il download del software Aruba Enroll

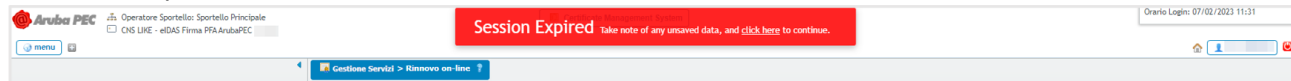
Manuali Operativi e Moduli		
Manuale_CMS_Firma_Digitale_Remota_2.9.pdf		↓
IT_Partner_ArubaPEC_TITOLARE_FD_v_3.6.pdf	Modulo Servizio	↓
IT_Partner_ArubaPEC_TITOLARE_FD_v_3.6.pdf	Modulo Servizio con DVO	↓
modulo_consegna.pdf	Modulo Ricevuta	↓
Modulo_Sospensione_v1.0_2020-05-12.pdf	Modulo Sospensione	↓
Modulo_Revoca_v1.0_2020-05-12.pdf	Modulo Revoca	↓

6 Sessioni di lavoro

Non è possibile aprire due applicazioni del CMS contemporaneamente nello stesso browser. In tal caso sullo schermo compare un messaggio di errore che invita a prendere nota dei dati non salvati e ad effettuare nuovamente il Login.



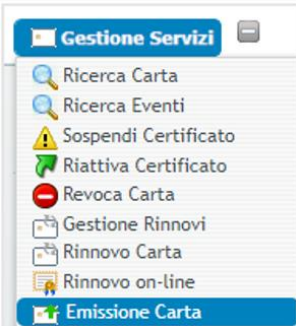
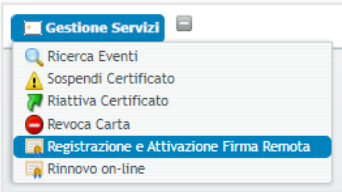
Una sessione di lavoro ha una durata limitata. In caso di inattività prolungata, il sistema disconnette l'operatore invitandolo a prendere nota dei dati non salvati e ad effettuare nuovamente l'accesso.



7 Procedura di emissione dei certificati

7.1 Registrazione dati Utente

Per emettere i certificati, è preliminarmente necessario registrare i dati anagrafici del Richiedente nel CMS.

Firma Digitale	Firma Remota
Per procedere, accedere al CMS e selezionare il servizio di interesse (nel nostro esempio CNS Unical - eIDAS Firma Digitale), quindi cliccare sul pulsante Gestione Servizi e selezionare la voce Emissione Carta. 	Una volta effettuato l'accesso con il servizio di interesse (ad esempio eIDAS Firma Remota), selezionare il pulsante Gestione Servizi e scegliere la voce Registrazione e attivazione Firma Remota. 

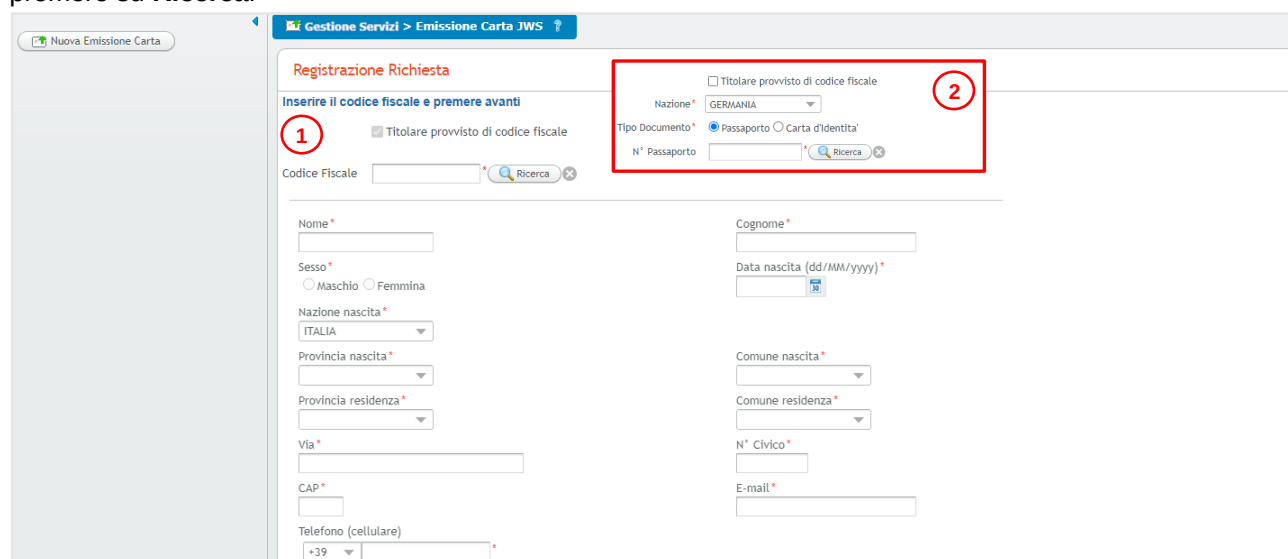
A seconda del servizio scelto, sarà possibile procedere con l'emissione di due tipi di certificato sul medesimo supporto ovvero del solo certificato di Firma Digitale. <u>A mero titolo esemplificativo, si segnala che la selezione del flusso CNS Unical - eIDAS Firma Digitale consentirà l'emissione, contemporaneamente, sulla medesima Smart Card (necessariamente di tipo CNS), di un certificato di autenticazione CNS e di un certificato di Firma Digitale. Mentre la selezione del servizio eIDAS Firma Digitale comporterà l'installazione del solo certificato di Firma Digitale (consigliato supporto CNS like).</u> Quest'ultima opzione si renderà obbligatoria nel caso di utenti che non sono in possesso di codice fiscale italiano.	
---	--

Come sopra anticipato, ai fini dell'emissione del certificato, dovranno essere rispettate le indicazioni riportate nella tabella sottostante.

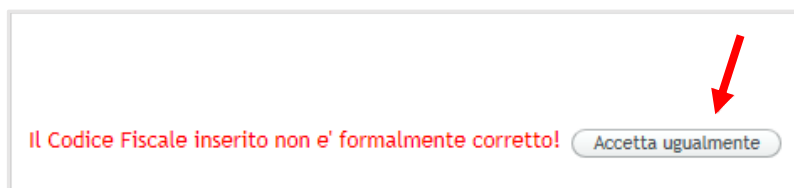
UTENTI DOTATI DI CODICE FISCALE	UTENTI NON DOTATI DI CODICE FISCALE
Per gli utenti in parola deve essere sempre indicato il codice fiscale: il sistema effettua un primo controllo sulla correttezza formale del codice fiscale, suggerendo eventuali correzioni sull'ultimo carattere, ma consentendo di ignorare il controllo stesso e forzare dunque l'inserimento, previo controllo da parte dell'operatore della correttezza del dato immesso.	Per gli utenti stranieri privi di codice fiscale italiano è necessario: 1) Non emettere Certificati di Autenticazione che prevedono obbligatoriamente l'inserimento di un codice fiscale italiano. Nel caso in cui si sia effettuato l'accesso al CMS con selezione del servizio <i>CNS Unical – eIDAS Firma Digitale</i>, l'ODR (Operatore di Registrazione) deve accedere nuovamente selezionando il solo servizio Firma Digitale. 2) Inserire numero seriale del passaporto (documento che l'Utente deve obbligatoriamente mostrare in fase di riconoscimento De Visu), deselegnando la voce Titolare provvisto di codice fiscale.

8

Inseriti i dati di cui sopra [codice fiscale (1) o numero di passaporto (2) a seconda dello scenario di riferimento], premere su **Ricerca**.



Qualora il codice fiscale inserito sia in formato non valido, ad esempio per gli utenti che hanno dati anagrafici tali da generare lo stesso codice fiscale, il sistema lo segnala, ma consente anche di proseguire con l'inserimento stesso cliccando su **Accetta ugualmente**.

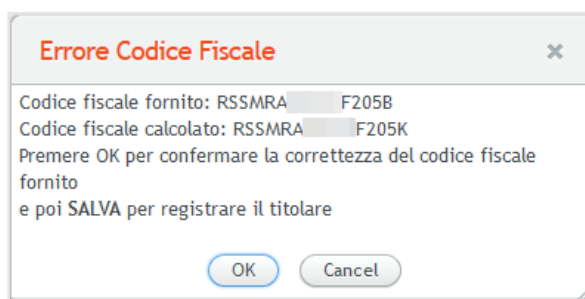


Se il Titolare è presente in archivio, la pagina *Registrazione Richiesta* sopra riportata, verrà automaticamente compilata con i dati dello stesso, in caso contrario procedere all'inserimento e cliccare su **Avanti**.

***Nel campo E-mail è necessario inserire un indirizzo email valido (non inserire un indirizzo di Posta Elettronica Certificata) del Titolare del certificato di Firma Digitale.**

Il sistema effettua un controllo sulla correttezza del codice fiscale inserito, basandosi sui dati anagrafici dell'Utente, pertanto eventuali doppi nomi o doppi cognomi devono essere riportati nella scheda di compilazione.

In caso di errore, il sistema mostra una finestra di allerta che consente di apportare modifiche ai dati inseriti oppure di forzare il controllo cliccando su **OK**.

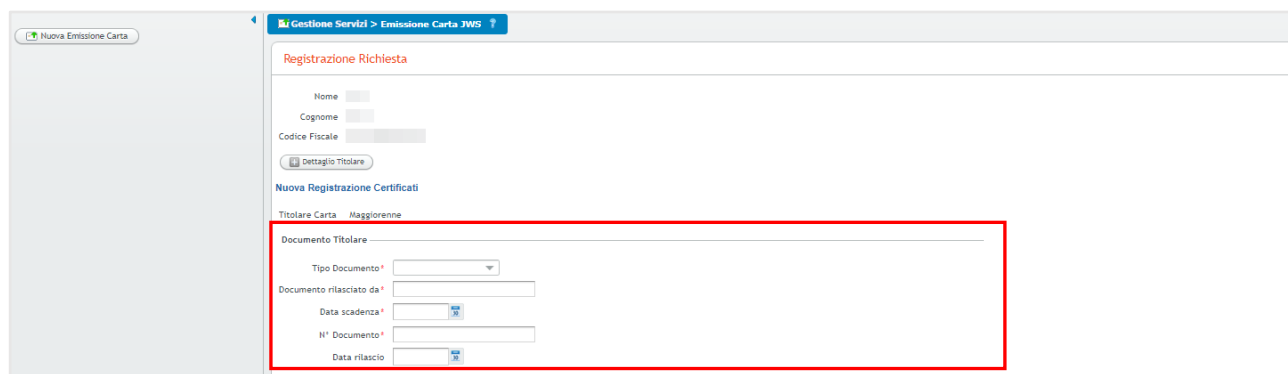


9

In alcuni casi l'indirizzo di residenza indicato nella carta d'identità potrebbe non essere più attuale, quindi riportare l'indirizzo comunicato dall'Utente.

Conclusa la compilazione di tutti i campi di registrazione, cliccare su **Salva** e poi su **Avanti**.

Nella schermata successiva inserire, nella scheda in alto, i dati del documento di identità mostrato dall'Utente in fase di riconoscimento.



Il **certificato di Firma Digitale (o di Firma Remota)** può contenere, oltre ai dati anagrafici dell'Utente, altri dati specifici, come ad esempio **un titolo professionale o una carica ricoperta all'interno di un'organizzazione**, oppure i dati di iscrizione ad un ordine/collegio professionale.

Di seguito uno schema riepilogativo dei casi e delle modalità di inserimento di dati accessori, oltre a quelli anagrafici.

TITOLO

Registrazione Certificati

Profilo ☒ Certificato CNS ArubaPEC Unical (Codice:)

Organizzazione (Cert. Auth.)

C.Fiscale/P.Iva Organizzazione (Cert. Auth.)

Country Organizzazione (Cert. Auth.)

Organization Unit

Smart Logon

E-mail

Profilo ☒ eIDAS Firma digitale ArubaPEC - 3 anni (Codice:)

Dimensione Chiavi

Organizzazione

Organizzazione (Cert. Firma)

C.Fiscale/P.Iva Organizzazione (Cert. Firma)

Country Organizzazione (Cert. Firma)

Organization Unit

OU2

OU3

OU4

OU5

Titolo/Carica ☒ Titolo ☐ Carica

Titolo

Dati Ruolo

E-mail

☒ Inserimento indirizzo email sui certificati

Qualora all'interno del certificato si desideri inserire soltanto la qualifica o abilitazione professionale del Richiedente, selezionare la voce **"Titolo"** e compilare la relativa casella sottostante, senza specificare l'organizzazione di appartenenza. Il titolo sarà considerato autocertificato con la sottoscrizione, da parte del Richiedente, del quadro C del modulo di richiesta Firma Digitale.

TITOLO E ORGANIZZAZIONE

Registrazione Certificati

Profilo ☒ Certificato CNS ArubaPEC Unical (Codice:)

Organizzazione (Cert. Auth.)

C.Fiscale/P.Iva Organizzazione (Cert. Auth.)

Country Organizzazione (Cert. Auth.)

Organization Unit

Smart Logon

E-mail

Profilo ☒ eIDAS Firma digitale ArubaPEC - 3 anni (Codice:)

Dimensione Chiavi

Organizzazione

Organizzazione (Cert. Firma)

C.Fiscale/P.Iva Organizzazione (Cert. Firma)

Country Organizzazione (Cert. Firma)

Organization Unit

OU2

OU3

OU4

OU5

Titolo/Carica ☒ Titolo ☐ Carica

Titolo

Dati Ruolo

E-mail

☒ Inserimento indirizzo email sui certificati

Selezionando la voce **"Titolo"** e compilando, oltre alla casella dedicata al titolo professionale, i campi **organizzazione** con relativa partita iva o codice fiscale (esempio: Ordine degli Architetti di XXX/12345678910) e **Dati ruolo** (***sezione non disponibile per Firma Remota**), si potrà attestare, all'interno del certificato di Firma Digitale, l'appartenenza del Titolare ad un ordine professionale. Nei casi in esame dovrà essere compilato il **quadro B1** del modulo di richiesta Firma Digitale con relativa sottoscrizione da parte dell'ordine professionale di appartenenza (Terzo Interessato).

N.B. Il campo **"Organizzazione,"** evidenziato a lato, dovrà permanere (salvo abilitazioni specifiche del CDRL) impostato su **"Inserisci manualmente..."**.

10

Registrazione Certificati

Profilo ☒ Certificato CNS ArubaPEC Unical (Codice:)

Organizzazione (Cert. Auth.)

C.Fiscale/P.Iva Organizzazione (Cert. Auth.)

Country Organizzazione (Cert. Auth.)

Organization Unit

Smart Logon

E-mail

Profilo ☒ eIDAS Firma digitale ArubaPEC - 3 anni (Codice:)

Dimensione Chiavi

Organizzazione 3

Organizzazione (Cert. Firma)

C.Fiscale/P.Iva Organizzazione (Cert. Firma)

Country Organizzazione (Cert. Firma)

Organization Unit

OU2

OU3

OU4

OU5

Titolo/Carica ☐ Titolo ☒ Carica 1

Carica 2

Dati Ruolo

E-mail

☒ Inserimento indirizzo email sui certificati

Selezionando la voce **“Carica” (1)**, si potrà attestare, all'interno del certificato di Firma Digitale, l'appartenenza ad una organizzazione di riferimento (ad esempio *“Azienda XXX”*) e si renderà necessario specificare anche partita iva/codice fiscale di quest'ultima. La compilazione della casella **“Carica” (2) (facoltativa)**, consentirà, inoltre, di specificare il ruolo ricoperto all'interno della predetta organizzazione. Nei casi in esame dovrà essere compilato il **quadro B2** del modulo di richiesta Firma Digitale con relativa sottoscrizione da parte del Terzo Interessato (che, tra l'altro, con l'apposizione della propria firma certificherà l'eventuale carica indicata dal Richiedente) e allegata la documentazione comprovante la rappresentanza dell'organizzazione indicata da parte di quest'ultimo.

N.B. Il campo *“Organizzazione,”* evidenziato a lato con il numero **(3)**, dovrà permanere (salvo abilitazioni specifiche del CDRL) impostato su *“Inserisci manualmente...”*.

Sulla base delle esigenze del cliente, si ha, poi, la facoltà, mediante l'applicazione o meno della relativa spunta nella casella dedicata (presente nelle immagini sopra proposte e contraddistinta da un asterisco rosso), di abilitare l'inserimento dell'indirizzo email del Titolare sul certificato di Firma Digitale da emettere (sia per Firma Digitale su Smart Card che per Firma Remota).

In caso di necessità, il CDRL potrà richiedere all'assistenza dedicata una modifica delle impostazioni di default, per far sì che la suddetta casella appaia sempre provvista della relativa spunta.

☒ Inserimento indirizzo email sui certificati

Si potrà, comunque, rimuovere il relativo flag nel corso delle operazioni di registrazione, se necessario.

A questo punto:

Firma Digitale

completato l'inserimento dei dati, seguire le indicazioni circa le modalità di riconoscimento di cui ai paragrafi successivi.

Firma Remota

dovrà essere indicato il Dominio (tipicamente “firma”, salvo domini personalizzati) e il tipo di OTP: **MOBILE (1)** o **DISPLAY (2)**.

Telefono (cellulare) +39

Tipo Riconoscimento In Presenza

Acquisizione Consenso Firma Autografa

Dominio*

OTP*

MOBILE

Dominio*

OTP*

DISPLAY

Invio mail all'utente per la configurazione

Concludi configurando utenza e dispositivo

Effettuerò io il riconoscimento (IR)

Avanti

I dispositivi di Firma Remota possono, infatti, essere **fisici** oppure di tipo **mobile**.

FISICI (token o dispositivo USB)		MOBILE (applicazione da scaricare sullo smartphone)
OTP con display		
OTP USB		

In caso di selezione dell'OTP display si renderà necessario specificare, nell'apposito menù, il tipo di configurazione preferita:

Invio mail all'utente per la configurazione: l'Utente inizia l'attivazione con l'operatore, ma conclude online l'operazione in autonomia. In tal caso l'Utente può prendere visione delle guide disponibili al seguente link <https://guide.pec.it/attivazione-firma-remota-senza-scratch-card.aspx>;

Concludi configurando utenza e dispositivo: l'Utente conclude l'attivazione con l'operatore. In tal caso l'operatore deve compilare i seguenti campi:

Username: da compilare in accordo con l'Utente;

Tipo OTP: selezionare dal menu a tendina il tipo di dispositivo OTP che verrà abbinato alla Firma Remota;

Seriale OTP: indicare il numero di serie visibile sul dispositivo utilizzato;

	OTP * DISPLAY Tipo Procedura Firma Remota * ☐ Invio mail all'utente per la configurazione ☒ Concludi configurando utenza e dispositivo Username * ? Tipo OTP * Seriale OTP * Completato l'inserimento dei dati, seguire le indicazioni circa le modalità di riconoscimento di cui ai paragrafi successivi.
--	---

Si ribadisce che l'operatore deve prestare attenzione all'inserimento dei dati anagrafici dell'Utente.

Prima dell'emissione del certificato è possibile modificare eventuali dati anagrafici non corretti. Qualora il certificato sia già stato emesso e si rilevino dati errati (dati presenti sul certificato) è necessario procedere alla revoca dello stesso ed effettuare una nuova emissione con i dati corretti.

7.2 Modalità di riconoscimento

Nei seguenti paragrafi verranno illustrate le modalità di riconoscimento previste.

Con riferimento al riconoscimento in presenza, si ricorda che per eseguire in modo corretto le relative operazioni, è necessario incontrare fisicamente l'utente e visionarne un documento di identità in corso di validità, tra quelli ammessi dalla Certification Authority. Per tutti i dettagli e le caratteristiche del servizio consultare il Manuale Operativo e relativi allegati (https://www.pec.it/documents/tc-files/it/21_firmadigitalemanualeoperativo.pdf e https://www.pec.it/documents/tc-files/it/94_cpdocumentidiriconoscimentoconsentiti.pdf). La verifica del documento di identità deve consentire il riconoscimento certo dell'Utente.

13

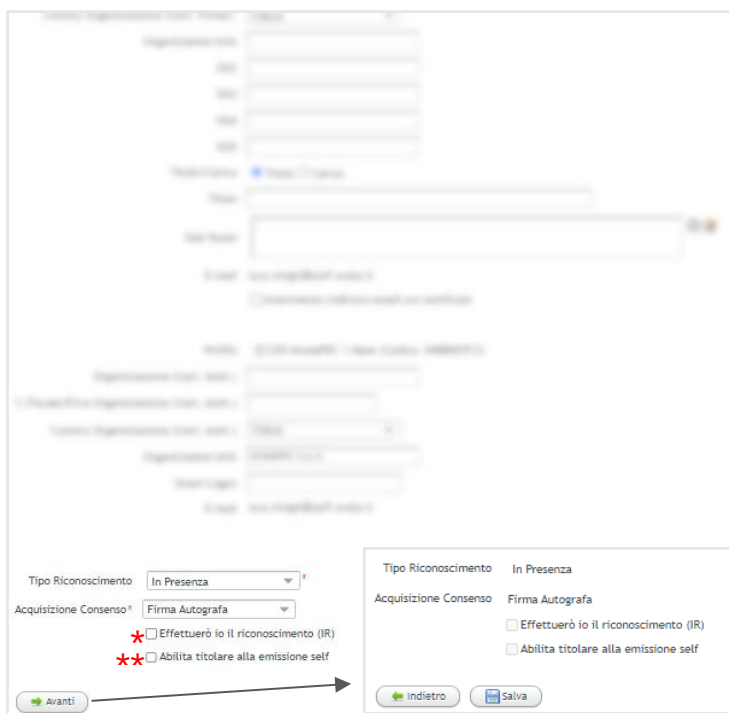
7.2.1 Riconoscimento in presenza e acquisizione del consenso con Firma Autografa

Una volta espletate le operazioni illustrate nei paragrafi precedenti, l'ODR dovrà procedere alla selezione del tipo di riconoscimento e alla relativa modalità di acquisizione del consenso tramite la scheda dedicata. Quest'ultima si trova nella parte terminale della pagina di *Registrazione Richiesta*.

Effettuata detta selezione, premere su **Avanti** e, successivamente su **Salva** per avanzare con gli step di emissione.

* se l'ODR effettuerà personalmente le operazioni di riconoscimento del Richiedente, potrà applicare la relativa spunta per ottenere la precompilazione del modulo con riferimento al quadro D, nella sezione dati IR.

** se disponibile in virtù delle proprie abilitazioni, l'applicazione della relativa spunta avvia il flusso che consente al Titolare di procedere all'installazione dei certificati (vedi paragrafo 7.3, Emissione certificati di Firma Digitale con Aruba Enroll).



Il sistema **genera** automaticamente il **modulo di richiesta certificato**, con estensione *.pdf*, contenente i dati dell'Utente.

A questo punto:

- scaricare e stampare il predetto modulo **precompilato (1)**;
- completarne la compilazione, ove necessario;
- apporre le **firme autografe** negli appositi spazi (**del Richiedente e dell'IR/ODR**) (2);
- caricare [pulsante **Upload**] (3), in un unico documento e per ogni singolo upload, una copia digitale del modulo firmato (scansione), del fronte e del retro del documento di identità del Richiedente e dell'eventuale documentazione comprovante la rappresentanza legale del Terzo Interessato, se valorizzato il quadro B2, in formato immagine (ad esempio .jpg, .png) oppure in formato .pdf.

1)

CondizioniArubaPecClientePartner_v2.0.pdf 

5021_20242_00083.pdf 



 Modulo firmato

 Scansione Documento

 Scansione Documento Retro

 Doc. comprovante Carica

2)

[illegible]


Aruba PEC

**Modulo di richiesta
FIRMA DIGITALE**

FORMULE DI ACCETTAZIONE

Il sottoscritto richiedente, consapevole delle sanzioni penali, nel caso di falsità non veritiera, di formazione e uso di atti falsi, richiamata dall'art. 76 del D.P.R. 445 del 28 dicembre 2000, al punto 9 per gli effetti dell'art. 46 del predetto D.P.R., dichiara che le informazioni fornite per la compilazione del presente Modulo, sono veritiere e perfettamente conformi. Dichiara, altresì, di aver preso visione del **Manuale CFS - Certificate Practice Statement**¹ e degli atti e documenti in esso richiamati che disciplinano l'operazione del certificato richiesto, disponibili per il download in <http://www.arubapec.it/ArubaCertification/centralita.asp>, che disciplina le tempistiche di rilascio del certificato richiesto nel Quadro 8 del presente Modulo, ed aver preso conoscenza altresì delle "Condizioni Generali di Contratto per il Certificato Digitale v.3.4", applicate al presente Modulo, e di accettare ed impegnare ad osservare quanto in esso contenuto.

Lungo _____ Data _____/_____/_____

Firma del Richiedente: _____

In sensi e per gli effetti degli artt. 1361 e 1362 c.c., il sottoscritto dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le clausole regolate dalle Condizioni Generali di Contratto per il Certificato Digitale v.3.4. Il sottoscritto si impegna, in qualità di richiedente, a sottoscrivere il certificato richiesto, a pagare la commissione di certificazione ed a versare le spese del certificato ed allineamenti. Il durata del contratto è valida del certificato. Il Obbligo del Cliente/Utente, il Obbligo e limitazioni di responsabilità del Certificatore. 14. Modifiche dei servizi e variazioni dei costi del certificato. 15. Limitazioni del contratto, chiavi tecniche espresse, 16. Rinnovo, 17. Rinnovo e sospensione del servizio, 18. Termini e condizioni.

Lungo _____ Data _____/_____/_____

Firma del Richiedente: _____

IDENTIFICAZIONE DEL RICHIEDENTE

Indicare in quale ruolo

Il sottoscritto dichiara, infine, di ritenere capo del presente Modulo conforme all'originale²

Lungo _____ Data _____/_____/_____

Firma del Richiedente: _____

Regione Sicula del Centro di Certificazione Locali (CRLs)

Il sottoscritto

☒ C.A.,
in qualità di incaricato al riconoscimento del Richiedente, sulle proprie personali responsabilità, dichiara di aver provveduto personalmente ad eseguire l'attività di identificazione del richiedente prendendo visione dell'originale del documento di identificazione del capo e validità e in buona stato di conservazione e che il documento del Richiedente è stato appeso alla presenza del sottoscritto.³

FIRMA DELL'INCARICATO AL RICONOSCIMENTO⁴

Il sottoscritto

☐ è necessario allegare alla presente richiesta:

☐ **CA FRONTI/NETID** del documento d'identità del richiedente in corso di validità⁵.

☐ Se completo il Quadro 92, la documentazione comprovante l'aperta di rappresentanza dell'organizzazione sopra indicata.

SPEDIZIONE DOCUMENTI

Tutte le documentazioni cartacea deve essere spedita in originale entro 32 giorni da essere messa a disposizione e con spedizione tracciabile all'indirizzo:

Aruba Pec S.p.A.

via. MEDIOBANCA 80-1-1

via Ruffini, 11 - 48055 Villanova di Certosa (BO)

¹ Applicabile solo in caso di firme autografe

² Applicabile in caso di riconoscimento attraverso la modalità 2 del Manuale "CFS - Certificate Practice Statement" (v.3.2.0)

³ Applicabile in caso di riconoscimento attraverso la modalità 1 del Manuale "CFS - Certificate Practice Statement" (v.3.2.0)

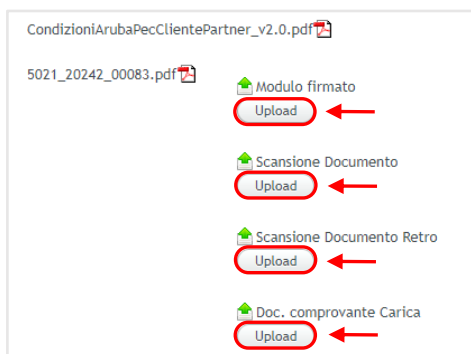
⁴ Applicabile solo in caso di firme autografe del Richiedente

⁵ Applicabile solo in caso di firme autografe del Richiedente

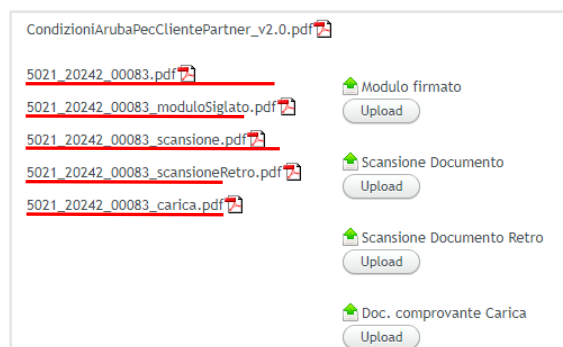
Aruba PEC S.p.A.
Via San Cristoforo 53 - 24036 Ponte San Pietro (BG) - P.IVA: 01790200517

MOD. 4.3
Documento Certificato

3)

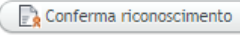


Effettuate le operazioni di cui sopra, i file caricati appariranno sulla sinistra dello schermo.



A questo punto l'operatore, oltre a poter modificare i dati con il tasto **Modifica**,

15

Firma Digitale su Smart Card	Firma Remota
potrà procedere con l'emissione dei certificati con Aruba Enroll , come illustrato nel paragrafo 7.3 .	potrà confermare il riconoscimento, per la successiva emissione del certificato, mediante il pulsante  .
La pratica passerà nello stato Da Verificare .	La pratica passerà nello stato Da Verificare .

Aruba PEC esaminerà, quindi, la documentazione allegata entro 2 (due) giorni lavorativi, notificando all'ODR eventuali mancanze e richiedendone l'integrazione.

Se la verifica avrà esito positivo (pratica nello stato *"In attesa originali"*):

Firma Digitale su Smart Card	Firma Remota
verranno inviate la seconda parte dei codici PIN e PUK e il Codice Utente all'email del Richiedente, che potrà pertanto iniziare a disporre del proprio dispositivo di Firma Digitale.	a seconda della procedura di attivazione scelta in fase di registrazione della richiesta, l'Utente riceve: con la procedura di attivazione online (Invio email all'utente per la configurazione) una email, all'indirizzo indicato in fase di registrazione, contenente il codice utente ed un link per collegarsi alle pagine di attivazione online; Nel caso in cui l'Utente non ricevesse l'email per l'attivazione, è possibile ripetere l'invio. Per procedere in tal senso, selezionare il

	percorso Gestione Servizi > Registrazione e attivazione Firma Remota, immettere il codice fiscale dell'Utente di interesse e premere Avanti, nella stringa relativa all'emissione effettuata per quel Titolare e con certificato nello stato “<i>Da Attivare</i>” premere il pulsante Reinvia Email. • con la procedura di attivazione contestuale (Concludi configurando utenza e dispositivo) un SMS, sul numero indicato in fase di registrazione, con una password (provvisoria) da cambiare al primo utilizzo. Il codice Utente viene inviato precedentemente all'indirizzo email fornito. Completate con successo le configurazioni di cui sopra, il Titolare potrà iniziare a disporre del proprio certificato di Firma Remota.
--	---

A questo punto, l'operatore dovrà inviare la documentazione raccolta, in originale, all'indirizzo indicato nel modulo entro e non oltre 30 (trenta) giorni. In caso contrario il certificato verrà sospeso. Prima di spedire gli originali, verificare che ogni fascicolo sia completo e che la spedizione sia tracciabile. La tracciabilità rappresenta una garanzia di sicurezza sia per chi spedisce che per chi riceve e per tenere sotto controllo eventuali slittamenti di consegna o inconvenienti.

In caso di intervenuta sospensione del certificato, lo stesso potrà essere riattivato dalla Certification Authority soltanto all'esito della ricezione e validazione della relativa documentazione in originale. Qualora lo stato di sospensione perdurasse oltre 120 giorni, il certificato dovrà essere sottoposto a revoca.

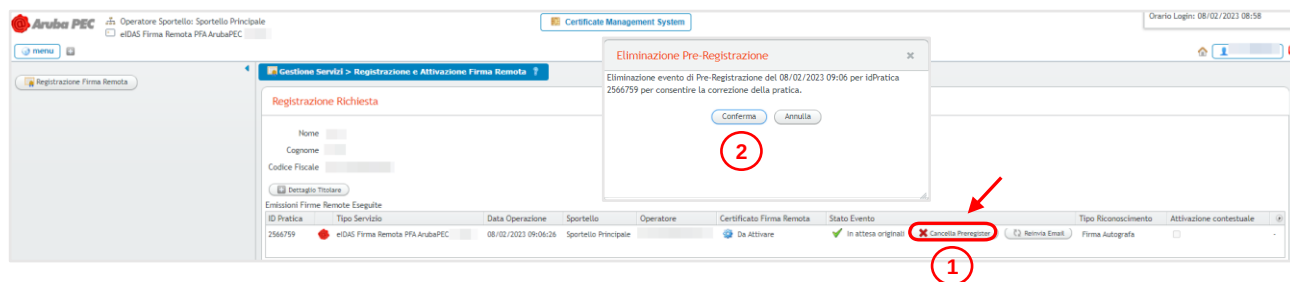
Se la verifica avesse esito negativo, la pratica passerà nello stato “*Da correggere*” e l'ODR riceverà una comunicazione con la richiesta di correzione/integrazione della documentazione. Le relative istruzioni sono contenute nel paragrafo **Procedura di correzione della documentazione** (pag. 22 e ss.).

Modifica dei dati relativi al rilascio del certificato di Firma Remota

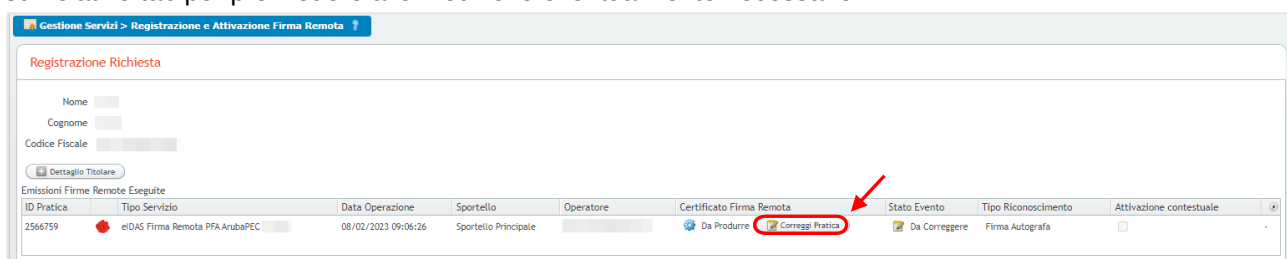
Per i certificati di Firma Remota in stato “*Da attivare*”, ovvero per i quali sia stata correttamente completata la fase di riconoscimento del Titolare, ma quest'ultimo non abbia ancora provveduto alla attivazione del certificato, è possibile, mediante la funzione **Cancella Preregister**, effettuare alcune modifiche, come, ad esempio, correggere eventuali dati riguardanti titolo professionale o carica rivestita, correggere il numero di cellulare, ecc.

Per procedere in tal senso, seguire il percorso **Gestione Servizi > Emissione e Attivazione Firma Remota** e, nella pagina dedicata, inserire il codice fiscale dell'Utente. Premere quindi il pulsante **Avanti**.

Apparirà così la schermata proposta nella pagina successiva.



Nella stringa di riferimento sarà presente il pulsante **Cancella Preregister**. Premendo lo stesso (1) e confermando l'operazione richiesta (2), la pratica passerà nello stato "Da correggere" e sarà possibile premere sul relativo tab per provvedere alle modifiche eventualmente necessarie.



Una volta cliccato sul predetto pulsante, si verrà reindirizzati alla pagina di Registrazione Richiesta, come da immagine a lato.

Tramite il tasto **Modifica**, sarà possibile apportare le eventuali variazioni necessarie tra quelle ammesse dal sistema.

Una volta completate le modifiche ed eventualmente integrata la relativa documentazione, premere su **Conferma riconoscimento** per completare l'iter in corso.

Così facendo, la pratica passerà al successivo step, parametrato a seconda della modalità di riconoscimento adottata (per esempio, in caso di riconoscimento in presenza con acquisizione del consenso con firma autografa, avanzerà nello stato "Da Verificare").

Registrazione Richiesta

Nome

Cognome

Codice Fiscale

Dettaglio Titolare

Titolare Carta

Maggiorenne

Documento Titolare

Tipo Documento

Carta d'identità

Documento rilasciato da

Comune di Prova

Data scadenza

28/02/2023

N° Documento

aaa000000

Data rilascio

16/01/2023

Registrazione Certificato Firma Remota

Profili

Firma Remota

E-mail

shotmail.it

Inserimento indirizzo email sui certificati

☐

Titolo/Carica

Titolo

Carica

Organizzazione

inserisci manualmente...

Organizzazione (Cert. Firma)

C.Fiscale/Riva Organizzazione (Cert. Firma)

Country

ITALIA

Organization Unit

Telefono (cellulare)

+39

Tipo Riconoscimento

In Presenza

Acquisizione Consenso

Firma Autografa

Dominio

OTP

MOBILE

Effettuerò io il riconoscimento (IR)

☐

CondizioniArubaPecClientePartner_v2.0.pdf

5335_20232_00005.pdf

5335_20232_00005_moduloSigilato.pdf

5335_20232_00005_scansione.pdf

Modulo firmato

Upload

Scansione Documento

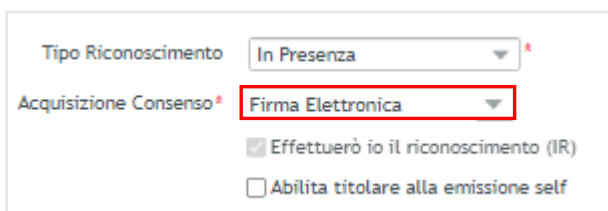
Upload

Modifica

Conferma riconoscimento

7.2.2 Riconoscimento in presenza e acquisizione del consenso con Firma Elettronica

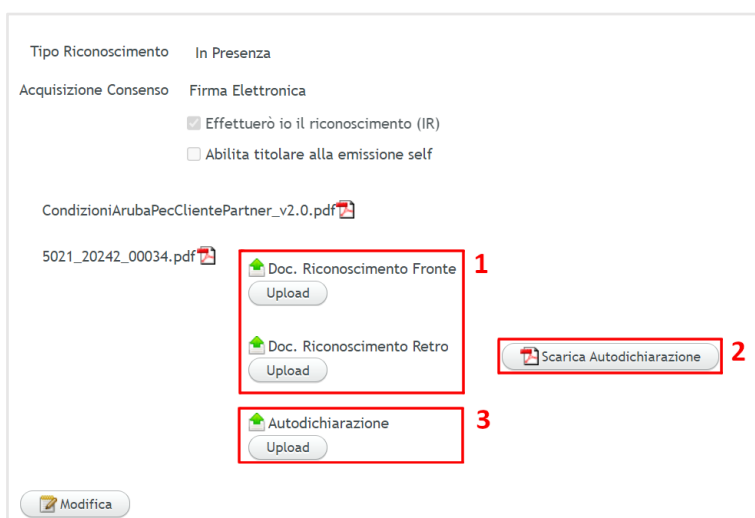
L'operatore, inseriti i dati relativi al rilascio del certificato come descritto nel **paragrafo 7.1**, può scegliere di effettuare il riconoscimento in presenza con acquisizione del consenso con Firma Elettronica, selezionando la relativa opzione dall'apposito menù a tendina.



The screenshot shows a form with two dropdown menus. The first, 'Tipo Riconoscimento', is set to 'In Presenza'. The second, 'Acquisizione Consenso', is set to 'Firma Elettronica' and is highlighted with a red box. Below these are two checkboxes: 'Effettuerò io il riconoscimento (IR)' (checked) and 'Abilita titolare alla emissione self' (unchecked).

Sono escluse dal flusso standard descritto nel presente capitolo le emissioni di certificati con Terzo Interessato, in quanto richiedono della documentazione aggiuntiva che deve essere verificata dalla Certification Authority.

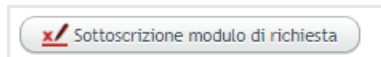
Una volta effettuato il salvataggio dei dati inseriti, sarà necessario procedere al caricamento di scansione del fronte e del retro del documento di riconoscimento (in cui estremi sono stati registrati in precedenza nella sezione dedicata) del Titolare (1) e dell'autodichiarazione attestante la conformità all'originale della scansione del documento di identità acquisita. Procedere quindi al download della predetta autodichiarazione (2), precompilata dal sistema con il numero del documento di identità registrato e il nome e cognome del Richiedente, sottoporla a quest'ultimo per la sottoscrizione con firma autografa (controllandone al contempo la leggibilità e corrispondenza a quella apposta sul documento di identità) ed effettuare l'upload (3) della relativa scansione mediante il pulsante dedicato.



The screenshot shows the 'Tipo Riconoscimento' set to 'In Presenza' and 'Acquisizione Consenso' set to 'Firma Elettronica'. Below, there are three upload sections: 'Doc. Riconoscimento Fronte' (1), 'Doc. Riconoscimento Retro' (2), and 'Autodichiarazione' (3). Each section has an 'Upload' button. A 'Scarica Autodichiarazione' button is also visible. A 'Modifica' button is at the bottom left.

18

Effettuate le operazioni richieste, il sistema proporrà il tab per l'avvio del processo di sottoscrizione del modulo.



The screenshot shows a button labeled 'Sottoscrizione modulo di richiesta' with a red checkmark icon.

Lo stesso prevede l'accettazione delle clausole contrattuali presenti nel modulo di richiesta tramite l'apposizione di **Firme Elettroniche** che si basano sull'uso di un codice OTP generato al momento di firmare.

Il flusso in esame prevede che copia del modulo di richiesta precompilato e copia delle condizioni generali di contratto vengano inviati al cliente per email (all'indirizzo indicato in fase di registrazione).

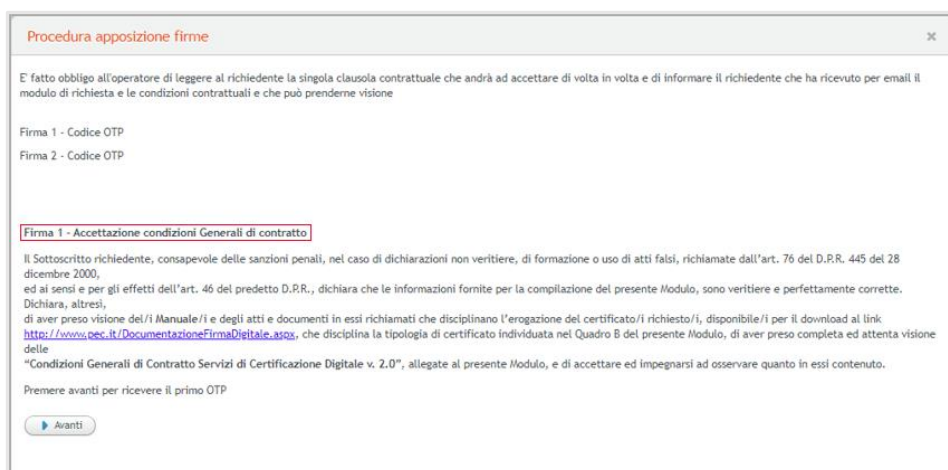
Per la comunicazione dell'OTP ci si avvale di un **SMS inviato al telefono cellulare del firmatario**. Il numero di telefono che viene utilizzato per la firma è quello dichiarato dal Richiedente in fase di registrazione dei dati anagrafici e di contatto. La password OTP è valida ed utilizzabile solo per una specifica transazione.

Si procede alle operazioni di sottoscrizione del modulo di richiesta attraverso **l'apposizione di due firme elettroniche del Richiedente**. Queste ultime sono obbligatorie e riguardano l'accettazione delle condizioni generali di contratto e delle clausole vessatorie.

È fatto **obbligo all'operatore di leggere al Richiedente la singola clausola contrattuale** che andrà ad accettare di volta in volta e di informarlo che ha ricevuto per email il modulo di richiesta e le condizioni contrattuali e che può prenderne visione.

Il Richiedente riceve, al **numero di cellulare indicato** in fase di registrazione, **due codici OTP** che comunica all'operatore, il quale li inserisce negli appositi campi sull'interfaccia (in caso di mancata ricezione, è possibile ripetere la procedura).

Firma 1- Accettazione delle condizioni generali di contratto:



Procedura apposizione firme

E' fatto obbligo all'operatore di leggere al richiedente la singola clausola contrattuale che andrà ad accettare di volta in volta e di informare il richiedente che ha ricevuto per email il modulo di richiesta e le condizioni contrattuali e che può prenderne visione

Firma 1 - Codice OTP
Firma 2 - Codice OTP

Firma 1 - Accettazione condizioni Generali di contratto

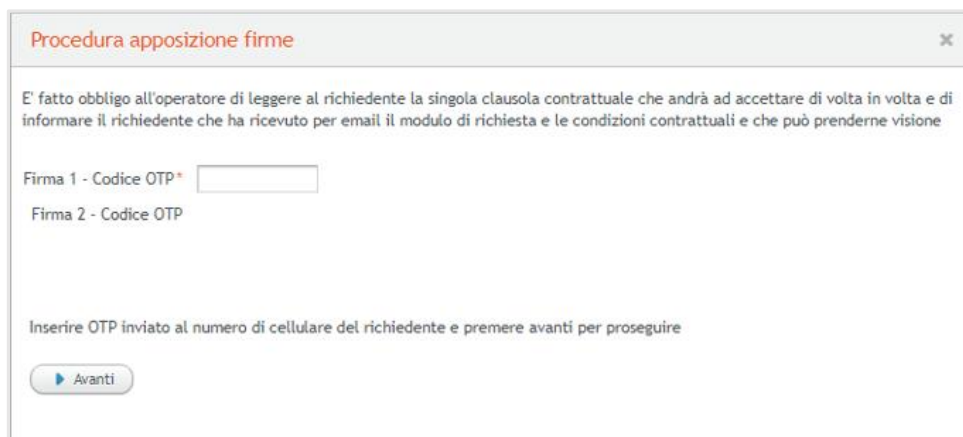
Il Sottoscritto richiedente, consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere, di formazione o uso di atti falsi, richiamate dall'art. 76 del D.P.R. 445 del 28 dicembre 2000, ed ai sensi e per gli effetti dell'art. 46 del predetto D.P.R., dichiara che le informazioni fornite per la compilazione del presente Modulo, sono veritiere e perfettamente corrette. Dichiara, altresì, di aver preso visione del/i Manuale/i e degli atti e documenti in essi richiamati che disciplinano l'erogazione del certificato/i richiesto/i, disponibile/i per il download al link <http://www.pec.it/DocumentazioneFirmaDigitale.aspx>, che disciplina la tipologia di certificato individuata nel Quadro B del presente Modulo, di aver preso completa ed attenta visione delle "Condizioni Generali di Contratto Servizi di Certificazione Digitale v. 2.0", allegate al presente Modulo, e di accettare ed impegnarsi ad osservare quanto in essi contenuto.

Premere avanti per ricevere il primo OTP

Avanti

19

Inserire il **primo codice OTP** inviato al numero di cellulare del Richiedente e premere su **Avanti** per proseguire:



Procedura apposizione firme

E' fatto obbligo all'operatore di leggere al richiedente la singola clausola contrattuale che andrà ad accettare di volta in volta e di informare il richiedente che ha ricevuto per email il modulo di richiesta e le condizioni contrattuali e che può prenderne visione

Firma 1 - Codice OTP*
Firma 2 - Codice OTP

Inserire OTP inviato al numero di cellulare del richiedente e premere avanti per proseguire

Avanti

Firma 2- Accettazione clausole vessatorie:

Procedura apposizione firme

E' fatto obbligo all'operatore di leggere al richiedente la singola clausola contrattuale che andrà ad accettare di volta in volta e di informare il richiedente che ha ricevuto per email il modulo di richiesta e le condizioni contrattuali e che può prenderne visione

Firma 1 - Codice OTP 580737
Firma 2 - Codice OTP

Firma 2 - Accettazione clausole vessatorie

Ai sensi e per gli effetti degli art. 1341 e 1342 c.c., il Sottoscritto dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le clausole seguenti delle "Condizioni Generali di Contratto Servizi di Certificazione Digitale v. 2.0": 3) Struttura del contratto; 5) Corrispettivi, modalità di pagamento e fatturazione; 6) Richiesta di registrazione e rilascio del certificato ed attivazione; 7) Durata del contratto e validità del certificato; 8) Obblighi del Cliente/Titolare; 9) Obblighi e limitazioni di responsabilità del Certificatore; 14) Modifiche dei servizi e variazioni alle condizioni dell'offerta; 15) Risoluzione del contratto, clausola risolutiva espressa; 16) Recesso; 17) Revoca e sospensione del certificato; 21) Foro competente.

Premere avanti per ricevere il secondo OTP

▶ Avanti

Inserire il **secondo codice OTP** inviato al numero di cellulare del Richiedente e premere su **Avanti** per proseguire:

Procedura apposizione firme

Firma 1 - Codice OTP 580737
Firma 2 - Codice OTP * 904563

Inserire OTP inviato al numero di cellulare del richiedente e premere avanti per proseguire

▶ Avanti

20

Completata l'apposizione delle firme elettroniche del Richiedente, l'operatore che ha effettuato il riconoscimento in presenza, **procede all'apposizione della propria firma** (tramite il dispositivo di Firma Remota con la quale ha effettuato l'accesso al CMS) sul modulo di richiesta cliccando su **Avanti**.

Con l'apposizione della propria firma, l'operatore, in qualità di incaricato al riconoscimento, certifica di aver **provveduto ad eseguire l'attività di identificazione** del Richiedente e di aver verificato le informazioni contenute all'interno del modulo.

Procedura apposizione firme

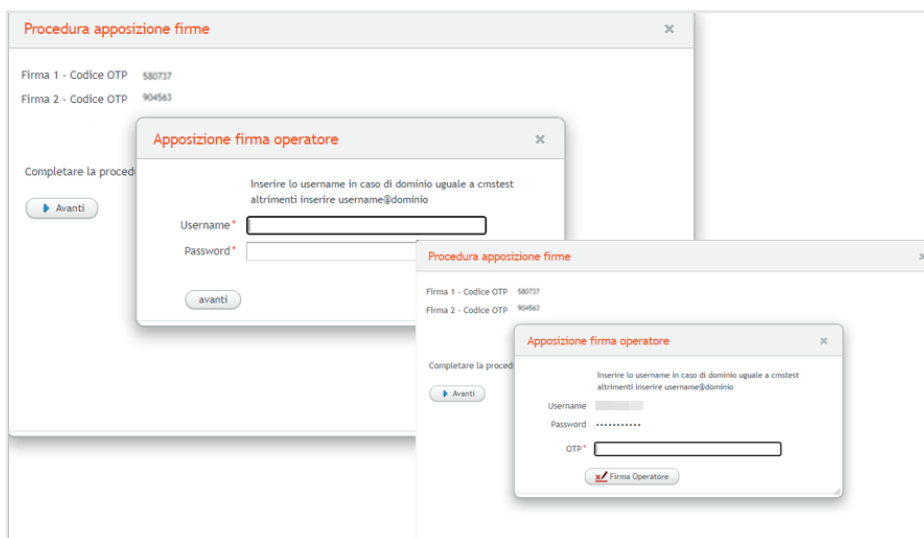
E' fatto obbligo all'operatore di leggere al richiedente la singola clausola contrattuale che andrà ad accettare di volta in volta e di informare il richiedente che ha ricevuto per email il modulo di richiesta e le condizioni contrattuali e che può prenderne visione

Firma 1 - Codice OTP 580737
Firma 2 - Codice OTP 904563

Con l'apposizione della presente sottoscrizione, l'operatore in qualità di incaricato al riconoscimento certifica di aver provveduto personalmente ad eseguire l'attività di identificazione del richiedente in presenza dello stesso e di aver verificato le informazioni contenute all'interno del modulo.

Completare la procedura con l'apposizione della firma dell'operatore sul modulo di richiesta

▶ Avanti



Il **modulo firmato dal Richiedente e controfirmato dall'operatore** viene versato in conservazione e inviato per email al Titolare.

È ora possibile:

Firma Digitale	Firma Remota
procedere con l'emissione dei certificati con Aruba Enroll come illustrato nel paragrafo 7.3 .	procedere con l'emissione del certificato. CondizioniArubaPecClientePartner_v2.0.pdf 5335_20232_00007.pdf 5335_20232_00007_firmato.pdf 5335_20232_00007_firmato_odr.pdf Riesegui Firma Emissione Firma Remota

** In caso di necessità, si possono ripetere le operazioni di apposizione delle firme elettroniche mediante il pulsante dedicato.*

Effettuate le operazioni di emissione:

Firma Digitale	Firma Remota
la prima parte del PIN e del PUK della Smart Card verranno inviati tramite SMS al numero di cellulare del Richiedente (o potranno essere stampati dall'ODR per la consegna all'Utente). <u>I certificati così emessi verranno, nell'immediato, sottoposti a sospensione autoritativa in attesa del buon esito delle operazioni di riconoscimento.</u> La pratica passerà nello stato Da Verificare .	la pratica passerà nello stato Da verificare .

Aruba PEC esaminerà la documentazione allegata entro due giorni lavorativi, notificando all'ODR eventuali mancanze e richiedendone l'integrazione.

Se la verifica avrà esito positivo (pratica nello stato **“Completato”**):

Firma Digitale	Firma Remota
verranno inviate la seconda parte dei codici PIN e PUK e il Codice Utente all'email del Richiedente, che potrà pertanto iniziare a disporre del proprio dispositivo di Firma Digitale.	a seconda della procedura di attivazione scelta in fase di registrazione della richiesta, l'Utente riceve: - con la procedura di attivazione online (Invio email all'utente per la configurazione una email, all'indirizzo indicato in fase di registrazione, contenente il codice utente ed un link per collegarsi alle pagine di attivazione online; Nel caso in cui l'Utente non ricevesse l'email per l'attivazione, è possibile ripetere l'invio. Per procedere in tal senso, selezionare il percorso Gestione Servizi > Registrazione e attivazione Firma Remota, immettere il codice fiscale dell'Utente di interesse e premere Avanti, nella stringa relativa all'emissione effettuata per quel Titolare e con certificato nello stato "Da Attivare" premere il pulsante Reinvia Email. - con la procedura di attivazione contestuale (Concludi configurando utenza e dispositivo) un SMS, sul numero indicato in fase di registrazione, con una password (provvisoria) da cambiare al primo utilizzo. Il codice Utente viene inviato precedentemente all'indirizzo email fornito. Completate con successo le configurazioni di cui sopra, il Titolare potrà iniziare a disporre del proprio certificato di Firma Remota.

Se la verifica avesse esito negativo, la pratica passerà nello stato "Da correggere" e l'ODR riceverà una comunicazione con la richiesta di correzione/integrazione della documentazione. Le relative istruzioni sono contenute nel capitolo successivo.

Procedura di correzione della documentazione

In caso di ricezione di una richiesta di correzione/integrazione della documentazione, l'operatore dovrà:

- 1) accedere al CMS;
- 2) dal menu **Gestione Servizi**, in alto a sinistra, cliccare su:

Firma Digitale	Firma Remota
<i>Emissione Carta</i>	<i>Registrazione e Attivazione Firma Remota</i>

- 3) ricercare la pratica di interesse tramite uno dei filtri disponibili (ad esempio il codice fiscale) e cliccare su **Avanti**;
- 4) selezionare quindi il pulsante **Da correggere** (Firma Digitale) o **Correggi Pratica** (Firma Remota);
- 5) qualora la richiesta di integrazione riguardasse:

a. l'errata registrazione degli estremi del documento di identità del Richiedente:

Flusso firma autografa	Flusso firma elettronica
provvedere alla correzione del dato errato mediante il pulsante Modifica , salvare la correzione apportata con il pulsante Salva , scaricare il modulo aggiornato, completarne la compilazione, dove necessario, e apporre le firme richieste, scansionare il modulo e caricarlo tramite la funzione di Upload. Infine premere Correggi Pratica .	provvedere alla correzione del dato errato mediante il pulsante Modifica , salvare la correzione apportata con il pulsante Salva , scaricare l'autodichiarazione aggiornata, procedere con la sottoscrizione da parte del Richiedente e caricarla tramite la funzione di Upload. Ripetere la procedura di apposizione delle firme elettroniche cliccando sul tab Sottoscrizione modulo di richiesta . Infine cliccare su Correggi Pratica .

b. l'assenza della/e firma/e necessarie, una volta premuto il pulsante **Da correggere/Correggi Pratica:**

Flusso firma autografa	Flusso firma elettronica
completare la sottoscrizione del modulo di richiesta Firma Digitale, scansionarlo e caricarlo tramite il pulsante Upload . Dopodiché premere Correggi Pratica .	completare la sottoscrizione dell'autodichiarazione, scansionarla e caricarla tramite il pulsante Upload . Dopodiché premere Correggi pratica .

c. errato caricamento della documentazione necessaria ai fini del rilascio del certificato di firma (scansione del modulo, scansione del documento di identità del Richiedente, scansione dell'autodichiarazione o della documentazione comprovante la rappresentanza legale del Terzo Interessato), una volta premuto il pulsante **Da Correggere/Correggi Pratica**, provvedere al caricamento di quanto richiesto tramite la funzione di upload e premere:

Flusso firma autografa	Flusso firma elettronica
Il pulsante Correggi Pratica .	Il pulsante Correggi pratica .

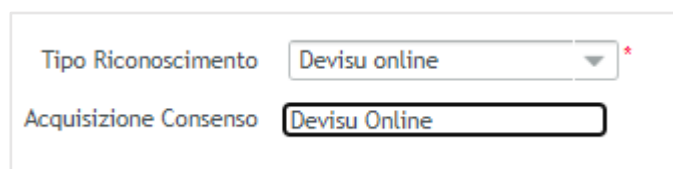
23

In caso di errata registrazione dei dati anagrafici del Richiedente e avvenuta emissione del relativo certificato, sarà necessario provvedere alla revoca di quest'ultimo e a successivo nuovo rilascio.

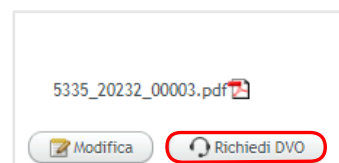
7.2.3 Riconoscimento DVO

L'operatore, inseriti i dati relativi al rilascio del certificato come descritto nel **paragrafo 7.1**, può scegliere di effettuare il **riconoscimento De Visu Online (DVO)** del Titolare come di seguito riportato:

- selezionare l'opzione **Devisu Online** dal menu *Tipo riconoscimento* e cliccare su **Avanti** e poi su **Salva**:



- generato il modulo di richiesta precompilato, cliccare sul pulsante **Richiedi DVO**



- compilare i campi obbligatori, evidenziati da un asterisco rosso, inserendo l'indirizzo email ed il numero di cellulare del Titolare e selezionando il **Tipo Operatore DVO** desiderato tra **CDRL** o **Aruba**. Scegliendo il tipo operatore **Aruba**, sarà necessario selezionare dal menù **Tipo DVO** la relativa opzione.

Tipo di operatore: CDRL	Tipo di operatore: Aruba
Aggiungi DVO Registrazione Richiesta DVO E-mail * Telefono (cellulare) +39 * Tipo Operatore DVO * CDRL * Tipo DVO Generico * Service Code * * Upload File 5021_20204_00072.pdf ✖ Condizioni Aruba Pec_servizi_certificazione_digitale_c ✖ ✖ Annulla Crea DVO	Aggiungi DVO Registrazione Richiesta DVO E-mail * Telefono (cellulare) +39 * Tipo Operatore DVO * ARUBA * Tipo DVO * Firma Digitale * Condizioni Aruba Pec_servizi_certificazione_digitale_c ✖ ✖ Annulla Crea DVO

- cliccare, infine, su **Crea DVO**:

✖ Annulla
Crea DVO

24

Sono escluse dal flusso standard descritto in questo capitolo le emissioni di certificati con Terzo Interessato, in quanto richiedono della documentazione aggiuntiva che deve essere verificata dalla Certification Authority.

Il Titolare riceve, all'indirizzo email indicato, il link per effettuare il riconoscimento. Per espletare le relative operazioni, si dovrà essere in possesso della seguente documentazione:

- **documento di identità** (i cui estremi sono stati inseriti al momento della registrazione dei dati Utente);
- **tessera sanitaria**, in sostituzione della tessera sanitaria non può essere accettato il certificato provvisorio del codice fiscale rilasciato dalla ASL, mentre possono essere accettati:
 - carta di identità elettronica (CIE);
 - certificato di attribuzione del codice fiscale rilasciato dall'Agenzia delle Entrate (anche per i cittadini italiani non residenti all'estero);
 - codice fiscale in tessera verde rilasciata dall'Agenzia delle Entrate (anche per i cittadini italiani non residenti all'estero);
 - codice fiscale in tessera bianca e verde con i caratteri in rilievo.

A questo punto:

Firma Digitale	Firma Remota
procedere con l'emissione dei certificati con Aruba Enroll , come illustrato nel paragrafo 7.3 .	restare in attesa dell'esito del riconoscimento.

Effettuate le operazioni di cui sopra:

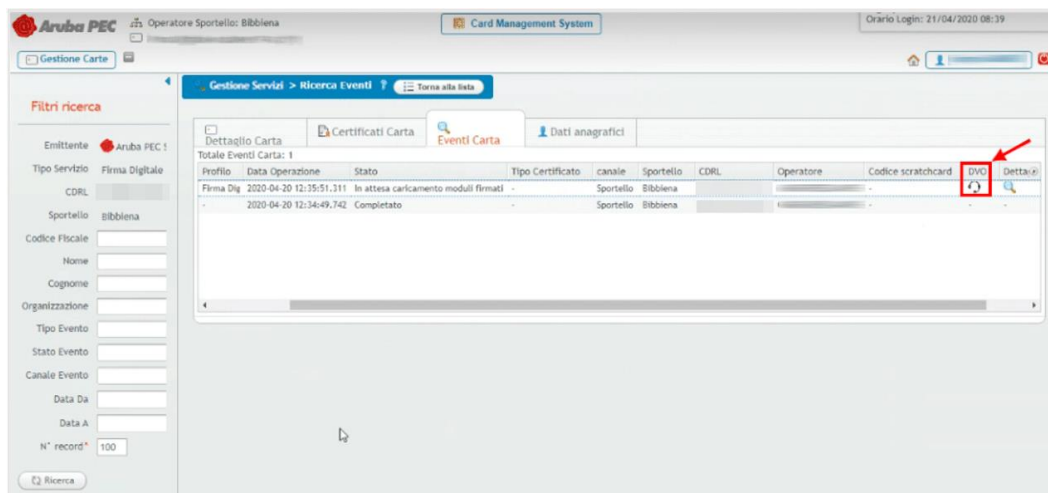
Firma Digitale	Firma Remota
l'operatore consegna all'Utente la Smart Card con il certificato di Firma Digitale. La prima parte dei codici PIN e PUK verrà trasmessa allo stesso tramite SMS al numero di cellulare censito in sede di registrazione (o potrà essere stampata dall'ODR per la consegna all'Utente). <u>I certificati così emessi verranno, nell'immediato, sottoposti a sospensione autoritativa in attesa del buon esito delle operazioni di riconoscimento.</u> Completato con successo quest'ultimo, i certificati verranno riattivati e il Titolare riceverà tramite email la seconda parte del PIN/PUK della Smart Card e il Codice Utente in modo da poter utilizzare il servizio di Firma Digitale.	completato con successo il riconoscimento: - se si è optato per l'attivazione contestuale, l'Utente riceverà tramite SMS la password provvisoria dell'account di Firma Remota e una email contenente il codice utente; - se si è optato per l'attivazione online, l'Utente riceverà una email contenente il link per effettuare l'attivazione online.

25

Monitorare lo stato del DVO

Per monitorare lo stato di avanzamento ed intervenire sulla richiesta DVO inviata, l'ODR può procedere come descritto di seguito:

- selezionare **Ricerca Eventi** dal menù **Gestione Servizi**;
- ricercare la pratica tramite uno dei filtri disponibili (ad esempio il codice fiscale) e cliccare su **Ricerca**;
- cliccare sulla pratica e poi sulla scheda **Eventi Carta**;
- cliccare sull'icona in corrispondenza di **DVO** per visualizzare il dettaglio della sessione DVO.



Dettaglio Sessione DVO

Nome _____

Cognome _____

Codice Fiscale _____

E-mail _____

Telefono +39 _____

Data Operazione 20/04/2020 12:37:51

Url DVO _____

Codice DVO _____

Tipologia DVO ARUBA

Tipo DVO Firma Digitale

Stato Configurato

Tipo Documento Carta d'Identita'

Documento rilasciato da ffffff

N° Documento dddddddd

Data rilascio _____

Data scadenza 26/04/20 12:34:52.371

Tramite il dettaglio della sessione DVO è possibile:

- verificare i dati inseriti nella richiesta del certificato (dati associati al Titolare come ad esempio indirizzo email, cellulare etc.);
- copiare il link del riconoscimento DVO dal campo **Url DVO** e, nel caso il Titolare non lo abbia ricevuto, rinviarlo nuovamente tramite email;
- verificare lo **Stato** del DVO che può essere:
 - **Configurato**: la richiesta DVO è stata inoltrata ed il link per il riconoscimento del DVO è stato inviato all'Utente;
 - **Completato**: il riconoscimento DVO è stato effettuato con successo;
 - **Terminato non identificato**: il riconoscimento DVO ha avuto esito negativo. Qualora quest'ultimo sia dovuto a problemi audio/video o di connessione, sarà possibile eseguire un nuovo riconoscimento mediante la funzione “Retry” presente all'intero della schermata di dettaglio della pratica DVO, come da immagine sottostante.

26

Filtri ricerca

Emittente Aruba PEC S.p.A.

Tipo Servizio DVO

CDRL _____

Sportello _____

Codice DVO _____

Codice Fiscale Titolare _____

Stato ▼

Tipo DVO ▼

Creato dal [icon]

Creato al [icon]

N° record 50

Ricerca

DVO CODE

Nome _____

Cognome _____

Codice Fiscale _____

E-mail _____

Telefono +393134262080

Data Operazione 28/11/2022 15:33:22

Url DVO _____

Codice DVO _____

Tipologia DVO ARUBA

Tipo DVO Generico

Service Code ECS_2020

Stato Terminato non identificato

Codice Errore GENERIC_ERROR

Tipo Documento Carta d'Identita'

Documento rilasciato da comune di putignano

N° Documento _____

Data rilascio 03/07/14 15:32:41.840

Data scadenza 20/10/24 15:32:41.840

5406_202211_00030.pdf

IT_ArubaPec_CondizioniServiziCertificazioneDigitaleTI

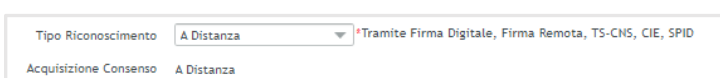
Retry
Invalida
Mostra Eventi
Rinvia Email

Il definitivo completamento della pratica DVO la cui sessione si sia conclusa in modo positivo avverrà soltanto all'esito della relativa validazione da parte della Certification Authority.

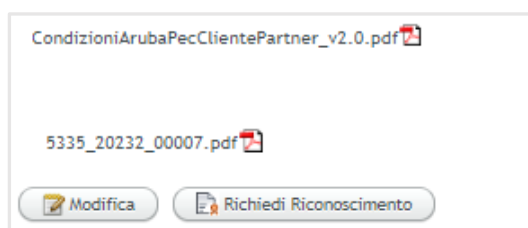
7.2.4 Riconoscimento “A Distanza” (tramite Firma Digitale, Firma Remota, TS-CNS, CIE o SPID)

L'operatore, inseriti i dati relativi al rilascio del certificato come descritto nel **paragrafo xx**, può scegliere di effettuare il **riconoscimento A Distanza** (tramite Firma Digitale, Firma Remota, TS-CNS, CIE o SPID) del Titolare, come di seguito riportato:

- selezionare l'opzione **A Distanza** dal menu Tipo riconoscimento e cliccare su **Avanti** e poi su **Salva**;



- generato il modulo di richiesta precompilato, cliccare su **Richiedi Riconoscimento**



27

A questo punto:

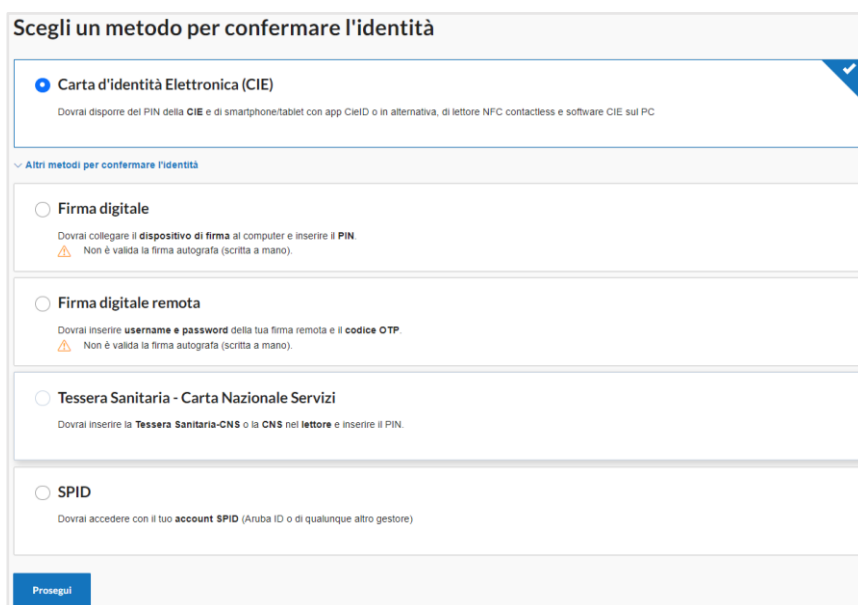
Firma Digitale	Firma Remota
L'operatore procedere con l'emissione dei certificati con Aruba Enroll, come illustrato nel paragrafo 7.3 e consegna all'Utente la Smart Card con il certificato di Firma Digitale. La prima parte dei codici PIN e PUK verrà trasmessa allo stesso tramite SMS al numero di cellulare censito in sede di registrazione (o potrà essere stampata dall'ODR per la consegna all'Utente). <u>I certificati così emessi verranno, nell'immediato, sottoposti a sospensione autoritativa in attesa del buon esito delle operazioni di riconoscimento.</u>	restare in attesa dell'esito del riconoscimento.

Il Titolare riceve, all'indirizzo email indicato, il link per effettuare il riconoscimento.

Operazioni di Riconoscimento

Una volta ricevuta l'email contenente il link per collegarsi al servizio di riconoscimento, il Titolare deve cliccare sullo stesso per essere reindirizzato alla pagina dedicata (procedere entro 90 giorni dalla ricezione della comunicazione).

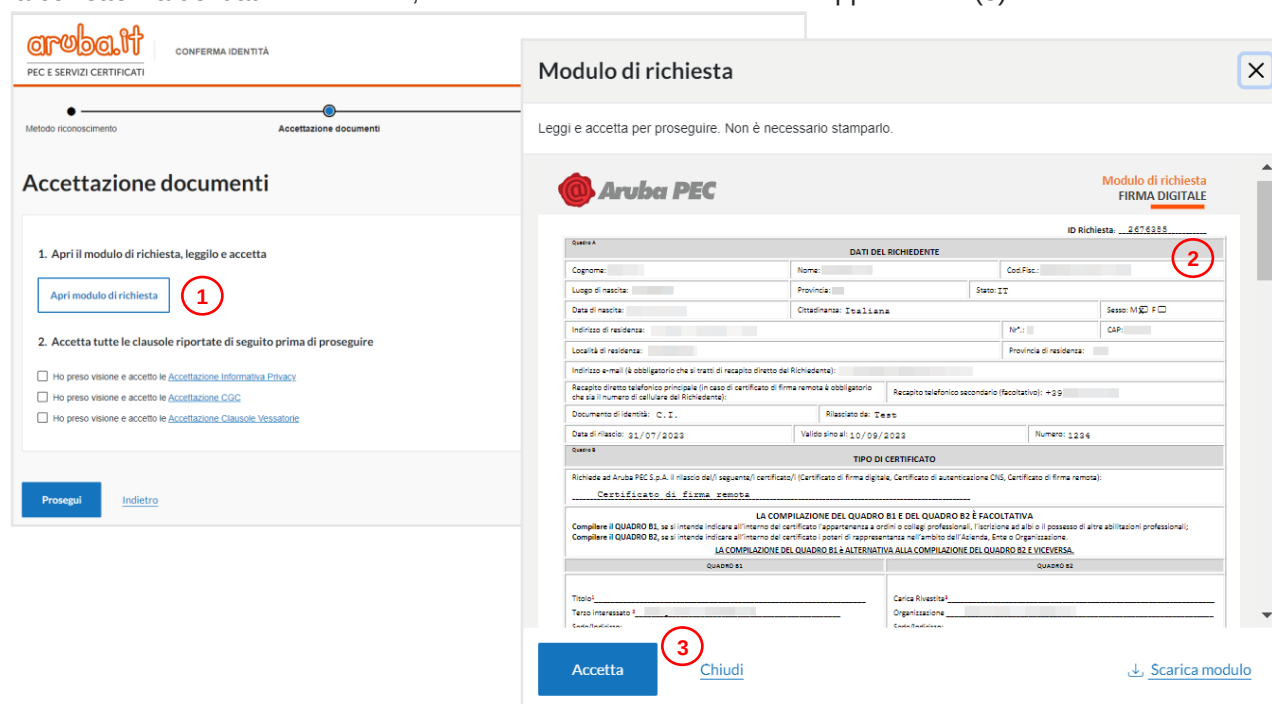
Nella scheda **Scegli un metodo per confermare l'identità**, sarà possibile selezionare la modalità di riconoscimento desiderata. Effettuata la selezione di interesse, cliccare su **Prosegui**.



28

A questo punto, indipendentemente dal metodo selezionato, il sistema proporrà la pagina di *Accettazione documenti*.

Sarà necessario aprire il modulo di richiesta tramite il pulsante dedicato (1), prenderne visione (2) e, verificata la correttezza dei dati ivi contenuti, accettare lo stesso cliccando sull'apposito tab (3).



*è possibile effettuare il download del modulo tramite il pulsante **Scarica modulo**

Procedere quindi con l'accettazione di tutte le clausole riportate al punto 2. della pagina applicando le relative spunte.

2. Accetta tutte le clausole riportate di seguito prima di proseguire

- ☐ Ho preso visione e accetto le [Accettazione Informativa Privacy](#)
- ☐ Ho preso visione e accetto le [Accettazione CGC](#)
- ☐ Ho preso visione e accetto le [Accettazione Clausole Vessatorie](#)

Cliccare quindi su **Prosegui**.

Si presenteranno ora diversi scenari a seconda del metodo di riconoscimento prescelto.

Riconoscimento con Tessera Sanitaria - Carta Nazionale Servizi

Tale metodo permette di effettuare le operazioni autenticandosi con un certificato CNS, che è contenuto anche sulla tessera sanitaria.

Il servizio di riconoscimento è compatibile con i seguenti sistemi operativi: Windows (versione 7 e successive) su sistemi 64 bit e Mac (dalla versione 10.10 alla versione 12.4).

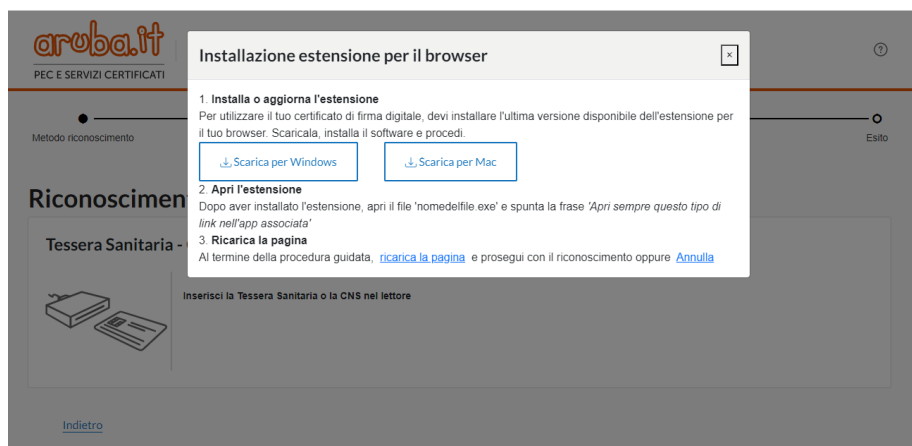
Il sistema proporrà allo step "Riconoscimento" un riepilogo di quanto necessario per procedere con tale metodo di identificazione, ovvero:

- **Letto smart card** collegato al computer;
- **CNS o Tessera Sanitaria** attiva;
- **PIN** della CNS o Tessera Sanitaria rilasciato in fase di attivazione.

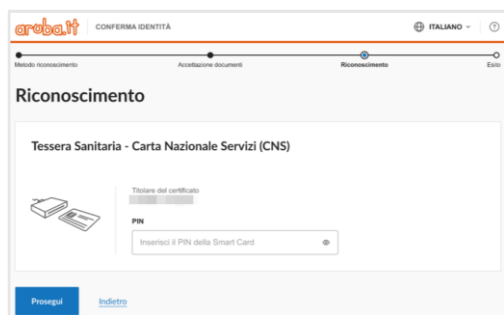
29

Cliccare su **Prosegui** per avanzare con le operazioni.

Effettuare l'installazione dell'estensione per il browser seguendo le indicazioni a schermo.



Effettuate le operazioni di cui sopra, verificare la presenza del dispositivo e successivamente inserire il **PIN** fornito in fase di attivazione dall'ente che ha erogato la carta. Poi cliccare su **Prosegui**.



Il riconoscimento è concluso.

Riconoscimento con Firma Digitale

Tale modalità permette di effettuare le operazioni di riconoscimento sottoscrivendo il modulo di richiesta Firma con un certificato di Firma Digitale installato su Smart/Sim Card.

Il servizio di riconoscimento è compatibile con i seguenti sistemi operativi: Windows (versione 7 e successive) su sistemi 64 bit e Mac (dalla versione 10.10 alla versione 12.4).

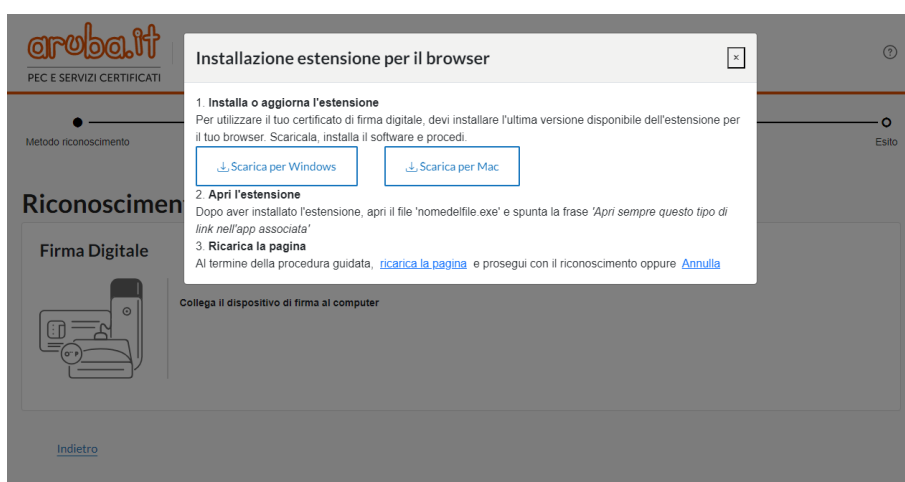
Il sistema proporrà allo step "Riconoscimento" un riepilogo di quanto necessario per procedere con tale metodo di identificazione, ovvero:

- **Dispositivo di firma** collegato al computer;
- **PIN** del dispositivo di firma.

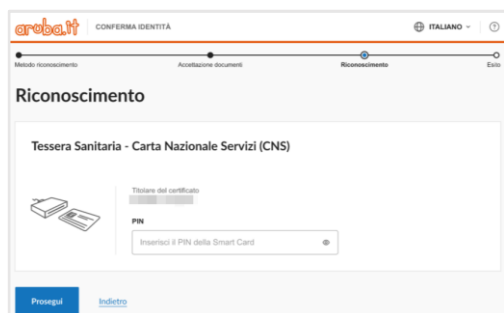
30

Cliccare su **Prosegui** per avanzare con le operazioni.

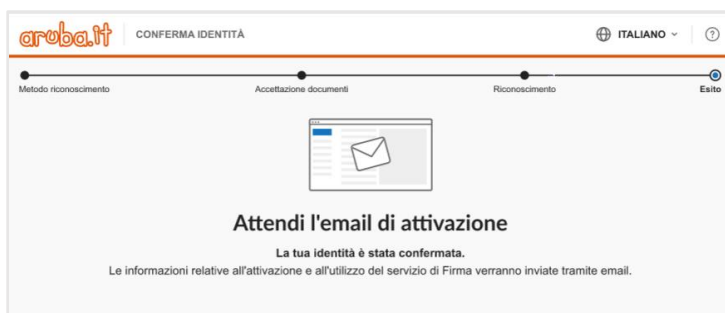
Procedere con l'installazione dell'estensione per il browser seguendo le indicazioni a schermo.



Effettuate le operazioni di cui sopra, verificare la presenza del dispositivo e successivamente inserire il **PIN** fornito in fase di attivazione dall'ente che ha erogato la carta. Poi cliccare su **Prosegui**.



Il riconoscimento è concluso.



Riconoscimento con Firma Remota

Tale flusso permette di effettuare il riconoscimento firmando il modulo di richiesta firma con un certificato di Firma Remota. Quest'ultima deve essere attiva, in corso di validità e rilasciata da Aruba.

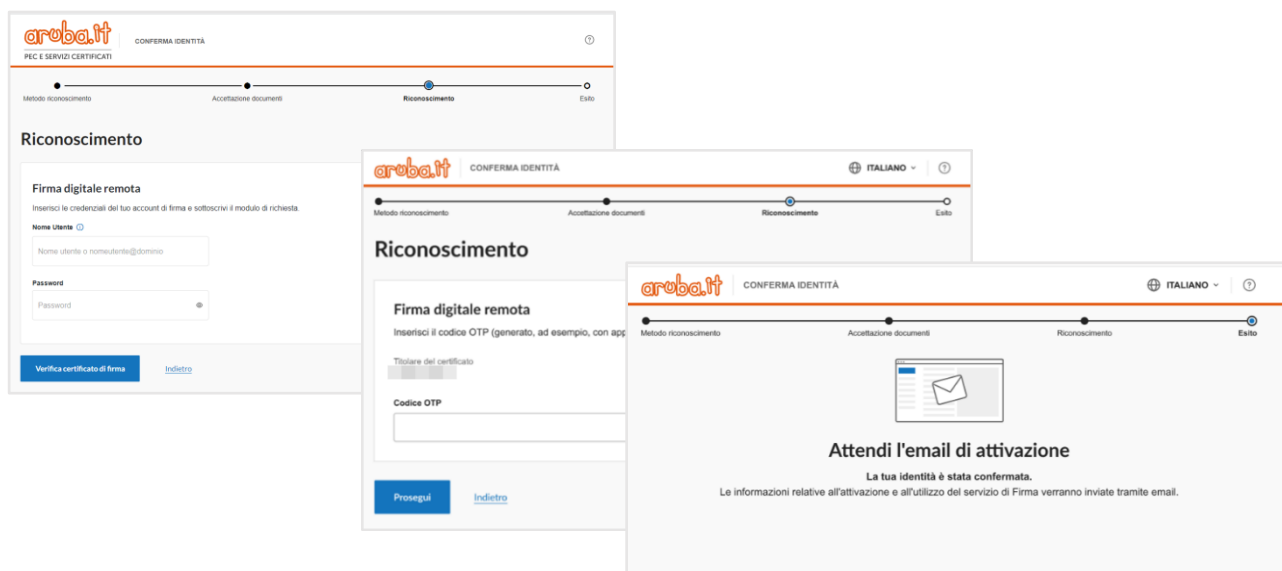
Il sistema proporrà allo step “*Riconoscimento*” un riepilogo di quanto necessario per procedere con tale metodo di identificazione, ovvero:

- **Firma Digitale Remota Aruba.** Se non se ne dispone usare la procedura alternativa (descritta nel paragrafo dedicato) per scaricare il modulo, firmarlo con apposito software e caricarlo;
- **Nome utente di firma;**
- **Password di firma;**
- **Codice OTP** (generato con app Aruba OTP, Aruba OTP Display, Aruba OTP USB, OTP SMS).

31

Cliccare su **Prosegui** per avanzare con le operazioni.

Inserire quindi le credenziali della Firma Remota e premere il pulsante **Verifica certificato di firma**. Dopodiché inserire il **codice OTP** e cliccare su **Prosegui**.

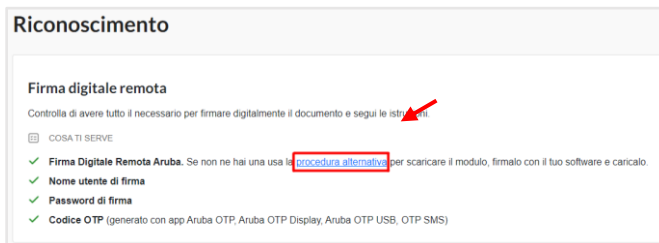


Il riconoscimento è concluso.

Riconoscimento con Firma Remota – Procedura alternativa

Se non si è in possesso di una Firma Remota rilasciata da Aruba, è possibile utilizzare la procedura alternativa per scaricare il modulo, firmarlo con l'apposito software e caricarlo.

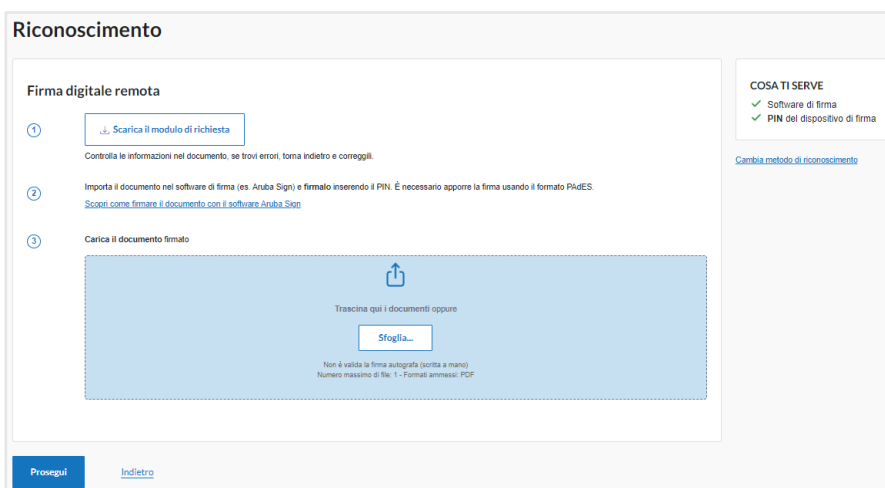
In tal caso, cliccare sull'apposito link proposto dal sistema.



Si visualizzerà così la pagina dedicata.

Procedere come segue:

1. effettuare il download del modulo di richiesta e prenderne visione, verificando inoltre la correttezza dei dati ivi riportati;
2. sottoscriverlo con la propria Firma Remota mediante apposito software usando il formato PAdES;
3. caricare il documento firmato nell'apposita sezione.



Il sistema effettuerà una verifica sulla correttezza e validità della firma apposta. In assenza di anomalie, la **procedura di riconoscimento risulterà conclusa**.

Riconoscimento con Carta d'Identità Elettronica (CIE)

Tale modalità permette di effettuare il riconoscimento autenticandosi con la Carta d'Identità Elettronica tramite l'applicazione ministeriale **CieID**.

Il sistema proporrà allo step "Riconoscimento" un riepilogo di quanto necessario per procedere con tale metodo di identificazione, ovvero:

- CIE versione 3.0 **valida e attiva**;
- **PIN** della CIE;
- smartphone/tablet con interfaccia NFC attiva + [app CieID installata e configurata](#) o in alternativa, lettore NFC RFID da tavolo + [software CIE](#) installato sul PC.

Cliccare su **Prosegui** per avanzare con le operazioni.

Si presenteranno due scenari:

- se la navigazione avviene da smartphone, verrà avviata automaticamente l'app CieID (purché già correttamente [installata e configurata](#)). Inserire, quindi, le **ultime 4 cifre del PIN** della Carta di Identità Elettronica. Se in precedenza è stata attivata la funzione di riconoscimento biometrico (ad esempio l'impronta digitale), l'app non richiederà l'inserimento del PIN, ma ci si potrà autenticare mediante il predetto sistema. Appoggiare quindi la carta sullo smartphone per avviare il processo di autenticazione, mantenendola in contatto fino al termine delle operazioni. Una volta letta con successo la carta, il riconoscimento sarà concluso.
- se la navigazione viene eseguita da PC, si verrà reindirizzati alla pagina del Ministero dell'Interno nella quale procedere con la selezione del metodo di autenticazione.




Seleziona la modalità di autenticazione



Scaricabile su
Google Play

Scaricabile su
App Store

Per autenticarti tramite uno smartphone con Android 6.0 o superiore, o iOS 13 o superiore, dotati di tecnologia NFC, munisci della nuova Carta d'identità elettronica e assicurati di avere l'applicazione CieID installata e configurata correttamente.

[Prosegui con smartphone](#)

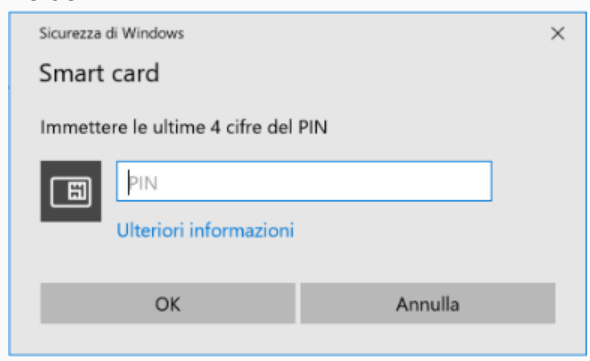


Windows, Mac, Linux

Per autenticarti con un lettore di smartcard contactless utilizzando un computer con Windows, Mac o Linux, dotati della nuova Carta d'identità elettronica. Assicurati inoltre di avere il software Cie installato e configurato correttamente e di appoggiare la carta sul lettore prima di cliccare sul pulsante prosegui.

[Prosegui con computer](#)

33

Prosegui con smartphone	Prosegui con computer
Questa modalità richiede l'utilizzo dell'app CieID installata e configurata sul proprio smartphone o tablet per la lettura della CIE. Verrà richiesto l'inserimento del numero di serie della Carta di Identità Elettronica. Una volta inserito, cliccare su Procedi. Inserisci il numero di serie della tua Carta d'Identità Elettronica  Seguire le indicazioni visualizzate a schermo e quindi inserire il codice OTP mostrato	In questo caso, dopo aver proceduto con l'installazione e configurazione del software Cie e collegato il lettore smartcard contactless (NFC), avvicinare la Carta di identità Elettronica a quest'ultimo e, una volta visualizzare la relativa finestra, procedere con l'inserimento delle ultime 4 cifre del PIN.  Se digitate correttamente, il sistema avvierà la procedura di verifica. Se conclusa con successo, il riconoscimento sarà completato.

dall'applicazione CielD e avanzare con le operazioni.

Completa l'autenticazione con CielD

FASE 1 - Apri la app CielD e scansiona il QR code



Apri l'applicazione CielD sul tuo smartphone e utilizza l'apposita funzione di scansione del codice QR. Completa poi l'autenticazione seguendo le indicazioni fornite dall'applicazione per generare il codice di sicurezza OTP.

Per tutelare la sicurezza della tua identità digitale il codice QR sarà valido ancora per **3:19*** minuti.

FASE 2 - Inserisci il codice OTP



Inserisci il codice OTP mostrato dall'applicazione CielD.

codice OTP

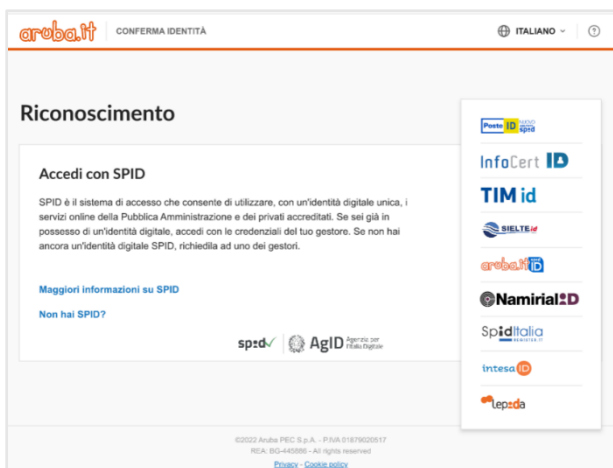
Il buon esito delle stesse sarà confermato da apposito messaggio. Il riconoscimento sarà concluso.

Riconoscimento con SPID

Si precisa che il certificato di Firma rilasciato tramite riconoscimento SPID contiene una limitazione d'uso:

- NON può essere utilizzato per richiedere un'altra identità SPID. La limitazione d'uso sarà recepita anche al rinnovo del certificato;
- il nuovo certificato di Firma potrà essere utilizzato per richiedere un ulteriore certificato di firma, ma anche quest'ultimo NON potrà essere utilizzato per richiedere un'identità SPID.

Una volta effettuati i primi due step della conferma identità, ovvero *Metodo di riconoscimento* e *Accettazione documenti*, il sistema proporrà la pagina relativa all'autenticazione con SPID. Per avanzare cliccare sul tab **Entra con SPID** e selezionare il proprio service provider dal menù a tendina.



Inserire le proprie credenziali SPID (eventualmente corredate dal codice OTP) e cliccare su **Entra con SPID**.

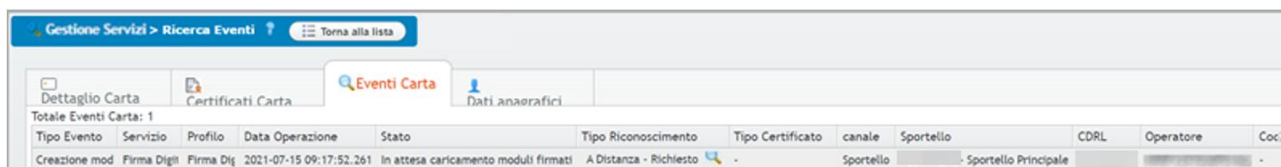
Qualora il sistema non rilevi anomalie, la **pratica di riconoscimento risulterà conclusa**.



Monitorare lo stato del riconoscimento A Distanza

Per monitorare lo stato di avanzamento della pratica, l'ODR può procedere come descritto di seguito:

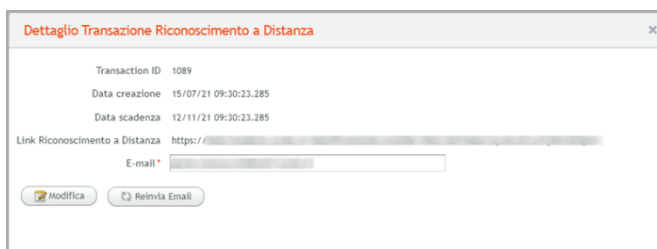
- selezionare **Ricerca Eventi** dal menu **Gestione Servizi**;
- ricercare la pratica tramite uno dei filtri disponibili (ad esempio il codice fiscale) e cliccare su **Ricerca**;
- cliccare sulla pratica e poi sulla scheda **Eventi Carta**;
- cliccare sull'icona in corrispondenza del riconoscimento a distanza per visualizzare il dettaglio.



Nella schermata sopra è possibile visionare lo stato del riconoscimento in corrispondenza della colonna “*Tipo riconoscimento*”:

- **Richiesto**: la richiesta è stata inoltrata ed il link per il riconoscimento è stato inviato all'Utente;
- **Completato**: il riconoscimento a distanza è stato effettuato con successo.

Entrando nel dettaglio della pratica, si aprirà la seguente scheda.



Tramite il pulsante **Reinvia Email** è possibile inoltrare nuovamente all'Utente il link per accedere al riconoscimento.

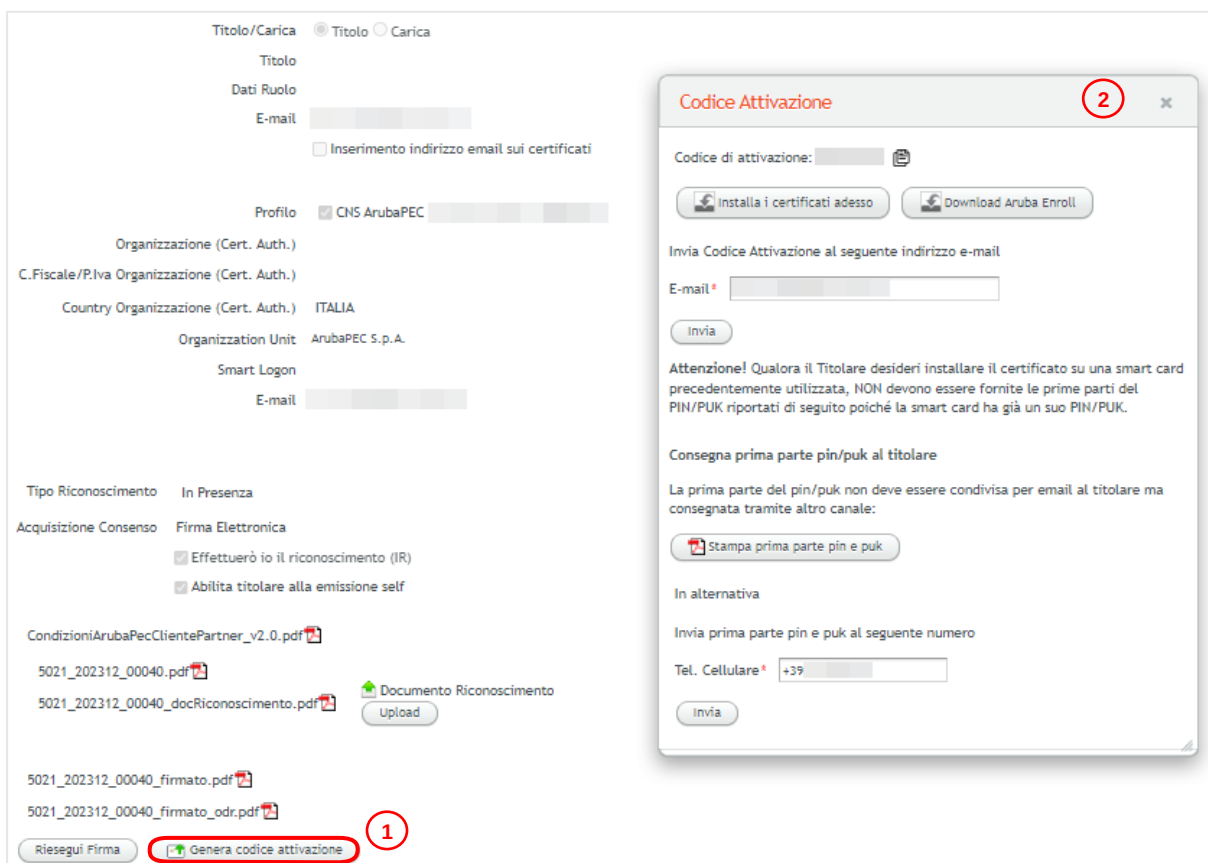
Espletate le operazioni di riconoscimento con uno dei metodi sopra illustrati:

Firma Digitale	Firma Remota
i certificati verranno riattivati e il Titolare riceverà tramite email la seconda parte del PIN/PUK della Smart Card e il Codice Utente in modo da poter utilizzare il servizio di Firma Digitale.	- se si è optato per l'attivazione contestuale, l'Utente riceverà tramite SMS la password provvisoria dell'account di Firma Remota e una email contenente il codice utente; - se si è optato per l'attivazione online, l'Utente riceverà una email contenente il link per effettuare l'attivazione online.

7.3 Emissione certificati di Firma Digitale con Aruba Enroll

In seguito alla registrazione dei dati del Titolare, alla selezione della relativa modalità di riconoscimento e all'avvenuto upload della documentazione richiesta, sarà possibile emettere i certificati di Firma Digitale su smart card con il software Aruba Enroll.

Terminate le procedure di cui sopra, cliccare sul pulsante **Genera codice attivazione** (1).



The screenshot shows the Aruba PEC CMS interface. On the left, there are various fields for user registration, including 'Titolo/Carica', 'Dati Ruolo', 'E-mail', 'Profilo', 'Organizzazione', 'C.Fiscale/P.Iva', 'Country', 'Organization Unit', 'Smart Logon', 'Tipo Riconoscimento', 'Acquisizione Consenso', and 'Condizioni'. At the bottom, there are several PDF files listed, including '5021_202312_00040_firmato.pdf' and '5021_202312_00040_firmato_odr.pdf'. A red circle (1) highlights the 'Genera codice attivazione' button. On the right, a dialog box titled 'Codice Attivazione' is shown, with a red circle (2) around its title bar. The dialog box contains fields for 'Codice di attivazione', 'E-mail', and 'Tel. Cellulare', along with buttons for 'Installa i certificati adesso', 'Download Aruba Enroll', 'Invia', and 'Stampa prima parte pin e puk'.

36

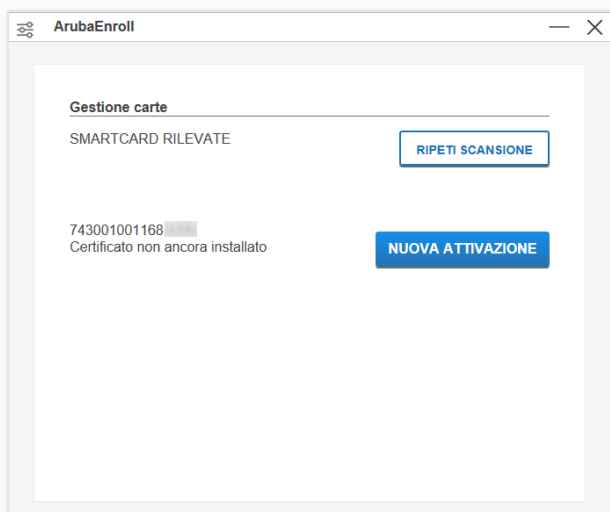
Si aprirà così la finestra dedicata sopra evidenziata (2). L'operatore consegnerà, quindi, all'Utente la Smart Card e **la prima parte dei codici PIN e PUK** tramite stampa dei medesimi ovvero invio via SMS.

A questo punto, a seconda che l'installazione dei certificati venga effettuata direttamente dall'operatore CDRL o dal cliente si avranno le due casistiche descritte di seguito.

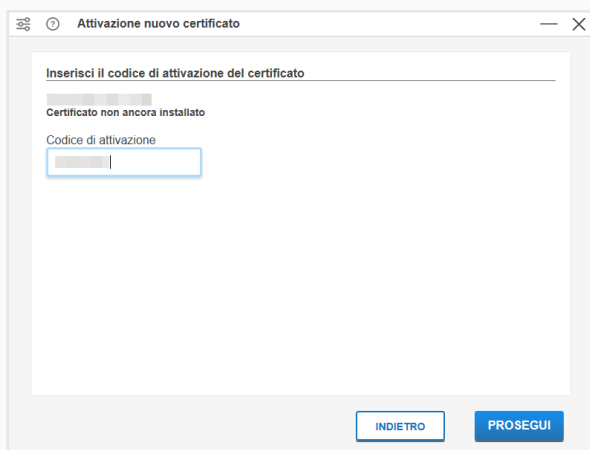
Installazione dei certificati a cura del CDRL	Installazione dei certificati a cura del Titolare
Scaricare il software Aruba Enroll e i driver della Card e/o del lettore (https://www.pec.it/gestione-supporto-firma-digitale.aspx) sulla postazione di emissione ed effettuare i seguenti step: - collegare il lettore al PC; - attendere il riconoscimento del sistema; - inserire la carta nel lettore.	Il codice di attivazione viene inoltrato tramite email. Dopo aver scaricato il software Aruba Enroll e i driver della Card e/o del lettore (https://www.pec.it/gestione-supporto-firma-digitale.aspx) sul proprio PC, procedere con i seguenti step: avviare l'esecuzione del software Aruba Enroll;

Premere il pulsante **Installa i certificati adesso**, posto in corrispondenza della finestra sopra illustrata.

Il software Aruba Enroll verrà avviato automaticamente. Cliccare su **NUOVA ATTIVAZIONE** per procedere con le relative operazioni.



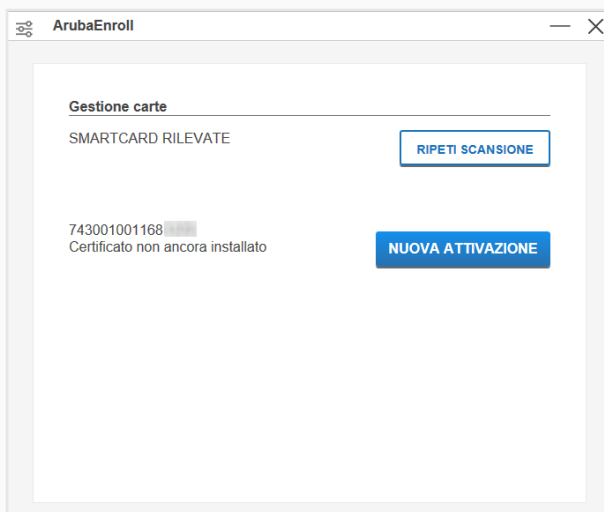
Inserire il **codice di attivazione** e cliccare su **PROSEGUI**.



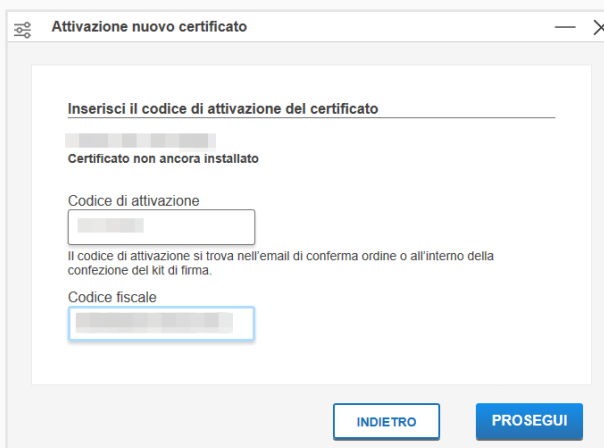
Attendere la conclusione dell'operazione di emissione del certificato.

- collegare il lettore al PC;
- attendere il riconoscimento del sistema;
- inserire la carta nel lettore.

Cliccare, quindi, sul pulsante **NUOVA ATTIVAZIONE**.

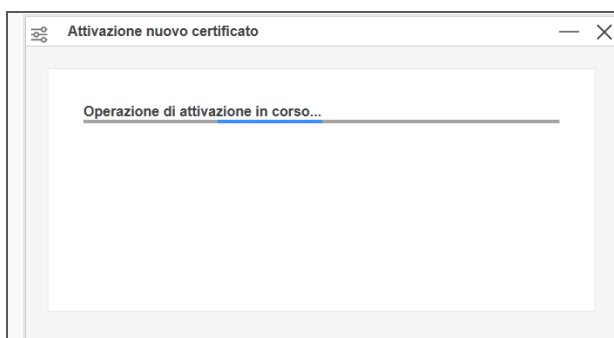


Inserire il **codice di attivazione** e il proprio **codice fiscale** e cliccare su **PROSEGUI**.

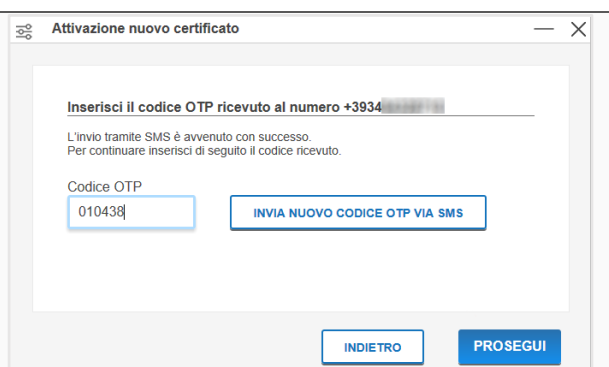
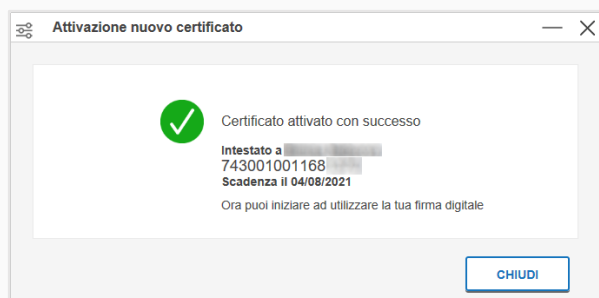


Inserire il codice OTP ricevuto per SMS al numero di telefono registrato nel sistema dal CDRL e cliccare su **PROSEGUI**.

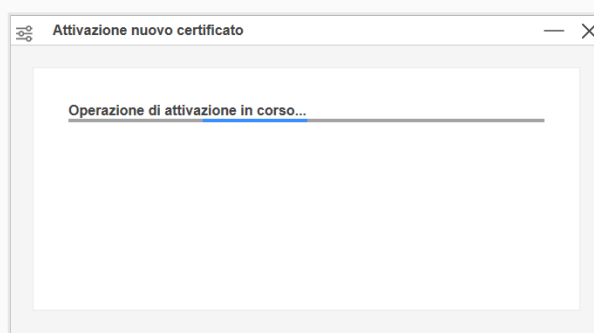
**Se l'SMS non è stato ricevuto dopo 30 secondi è possibile procedere con un nuovo invio del codice.*



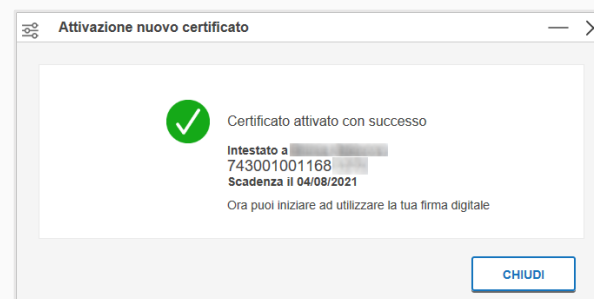
Se l'operazione è stata eseguita correttamente, l'attivazione del certificato si conclude con successo.



Attendere la conclusione dell'operazione di attivazione del certificato.



Se l'operazione è stata eseguita correttamente, l'attivazione del certificato si conclude con successo.



**Il software è utilizzabile con: Token, Aruba Key, Smart/Sim Card + lettore da tavolo.*

Completata la procedura (e ottenuta la validazione della scansione della modulistica in caso di riconoscimento con firma autografa ovvero espletate le operazioni di riconoscimento in caso di DVO e riconoscimento a distanza), il cliente riceverà email di conferma contenente la **seconda parte del PIN e PUK** necessari per la procedura di firma (la prima parte dei codici PIN e PUK è stata già inviata per SMS o fornita dal CDRL) e il codice utente.

Il certificato è dunque attivo ed è possibile firmare digitalmente i documenti.

In caso di **attivazione non riuscita**, è possibile **rieseguire** la procedura.

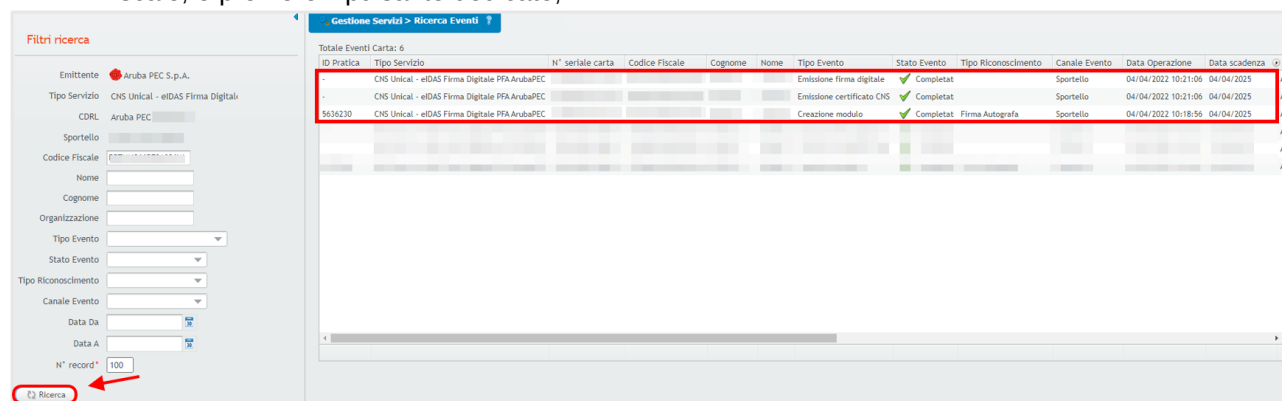
Qualora l'errore persistesse, è necessario aprire una richiesta di assistenza tramite i canali dedicati.

Per facilitare la risoluzione del problema è possibile scaricare il file di errore presente sul software e allegarlo alla richiesta.

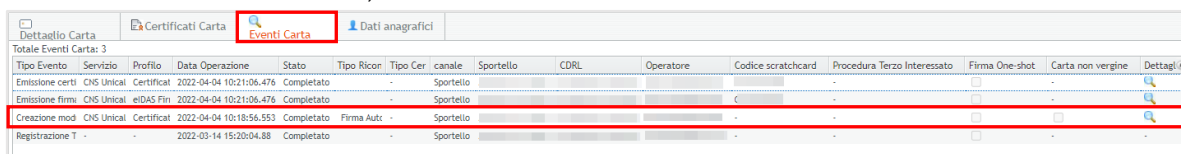
8 Recupero PIN e PUK Smart Card

In caso di smarrimento, oppure nel caso non fosse stata recapitata la comunicazione contenente la prima e la seconda parte dei codici PIN/PUK, è possibile rinviarli cliccando sul menu **Gestione Servizi > Ricerca Eventi** e procedendo come di seguito descritto:

- 1) tramite i filtri disponibili, impostare la ricerca del certificato di interesse, ad esempio inserendo il codice fiscale, e premere il pulsante dedicato;

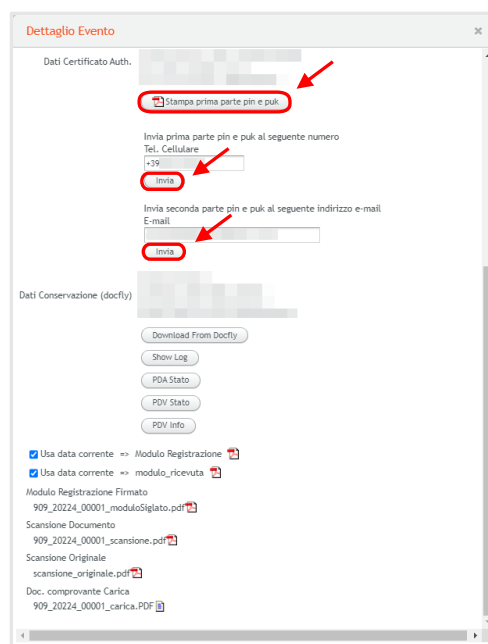


- 2) cliccare in corrispondenza di una delle stringhe riferibili agli eventi associati al certificato (ad esempio quella contraddistinta dalla voce "Creazione Modulo").
- 3) nella finestra che apparirà, spostarsi sul tab "Eventi Carta" e, eventualmente scorrendo con il cursore sulla destra dello schermo se necessario, cliccare sulla lente di ingrandimento posta in corrispondenza della voce "Creazione Modulo";



Tipo Evento	Servizio	Profilo	Data Operazione	Stato	Tipo Ricon	Tipo Cer	canale	Sportello	CDRL	Operatore	Codice scratchcard	Procedura Terzo Interessato	Firma One-shot	Carta non vergine	Dettagli
Emissione certi	CNS Unical	Certificat	2022-04-04 10:21:06.476	Completato	-	-	Sportello	-	-	-	-	-	-	-	
Emissione firmi	CNS Unical	eIDAS Pin	2022-04-04 10:21:06.476	Completato	-	-	Sportello	-	-	-	-	-	-	-	
Creazione mod	CNS Unical	Certificat	2022-04-04 10:18:56.553	Completato	Firma Aut	-	Sportello	-	-	-	-	-	-	-	
Registrazione T	-	-	2022-03-14 15:20:04.88	Completato	-	-	Sportello	-	-	-	-	-	-	-	

- 4) Si aprirà la scheda "Dettagli Evento" che consentirà, tra gli altri, di stampare o inviare tramite SMS la prima parte dei codici PIN e del PUK nonché di inoltrare, tramite email, la seconda parte dei predetti codici.



Sarà possibile inviare nuovamente la seconda parte dei codici PIN/PUK solo quando lo stato della pratica sarà "In attesa originali" o "Completata".

L'operatore non potrà rinviare e/o recuperare il codice PIN qualora il cliente lo abbia personalizzato a seguito della ricezione del codice completo.

9 Funzionalità aggiuntive del CMS

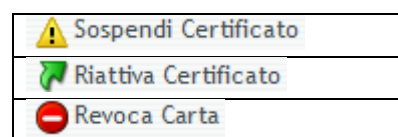
9.1 Gestione ciclo di vita dei certificati

Mediante il CMS è possibile effettuare il cambio di stato del certificato nonché ricercare le emissioni di certificati processate dal CDRL.

La procedura di cambio di stato del certificato consente all'ODR di **sospendere**, **riattivare** o di **revocare** i certificati intestati ad un Utente per il quale il CDRL ha emesso il dispositivo di Firma.

La relativa richiesta (di sospensione/riattivazione/revoca) dovrà pervenire dal **Titolare** del certificato di Firma Digitale o dal **Terzo Interessato**, se presente.

Per ogni servizio disponibile, è possibile selezionare la relativa voce nel menu **Gestione Servizi**, che compare in alto a sinistra nel CMS.



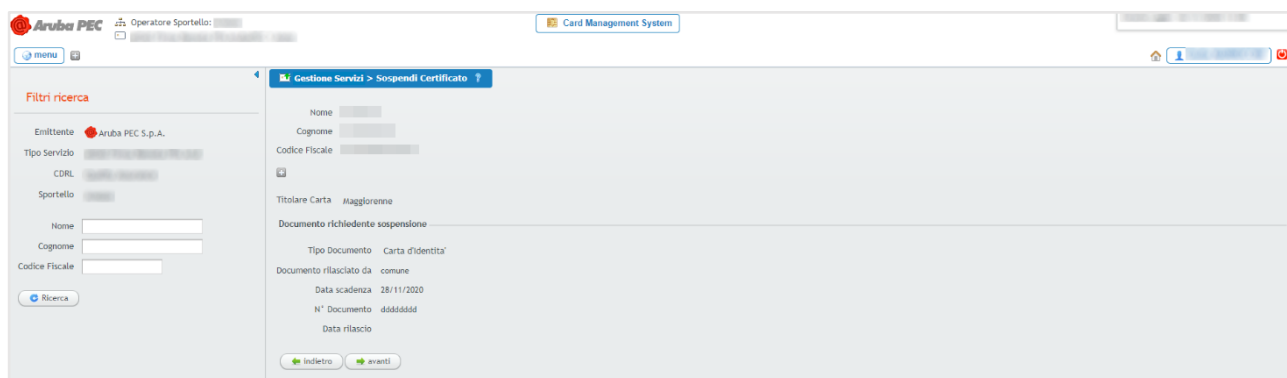
9.1.1 Sospensione del Certificato

Nel caso in cui sia necessario sospendere un certificato di Firma, ad esempio per momentaneo non utilizzo, è necessario accedere al CMS su **Gestione Servizi > Sospendi Certificato**, ricercare il certificato di interesse, per il quale si intende cambiare lo stato, tramite i filtri disponibili (Nome, Cognome, codice fiscale), selezionarlo e cliccare su **Sospendi Certificato**:

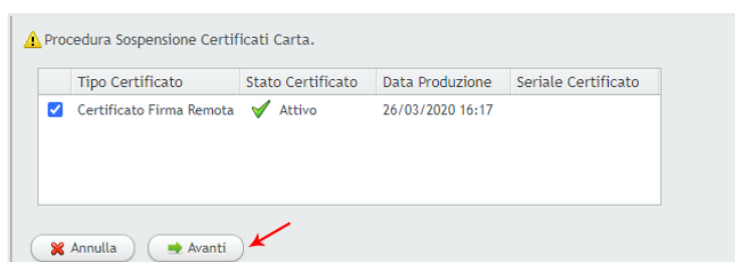
40

Servizio	N° seriale carta	European Code Carta	Nome	Cognome	Codice Fiscale	Stato Carta	operazione
CNS LIKE - eIDAS Firma PFA ArubaPEC						Operativa	⚠ Sospendi Certificato

L'operatore dovrà compilare i campi dedicati riportando gli estremi del documento di identità dell'Utente che ha richiesto il cambio di stato e cliccare su **Avanti**.

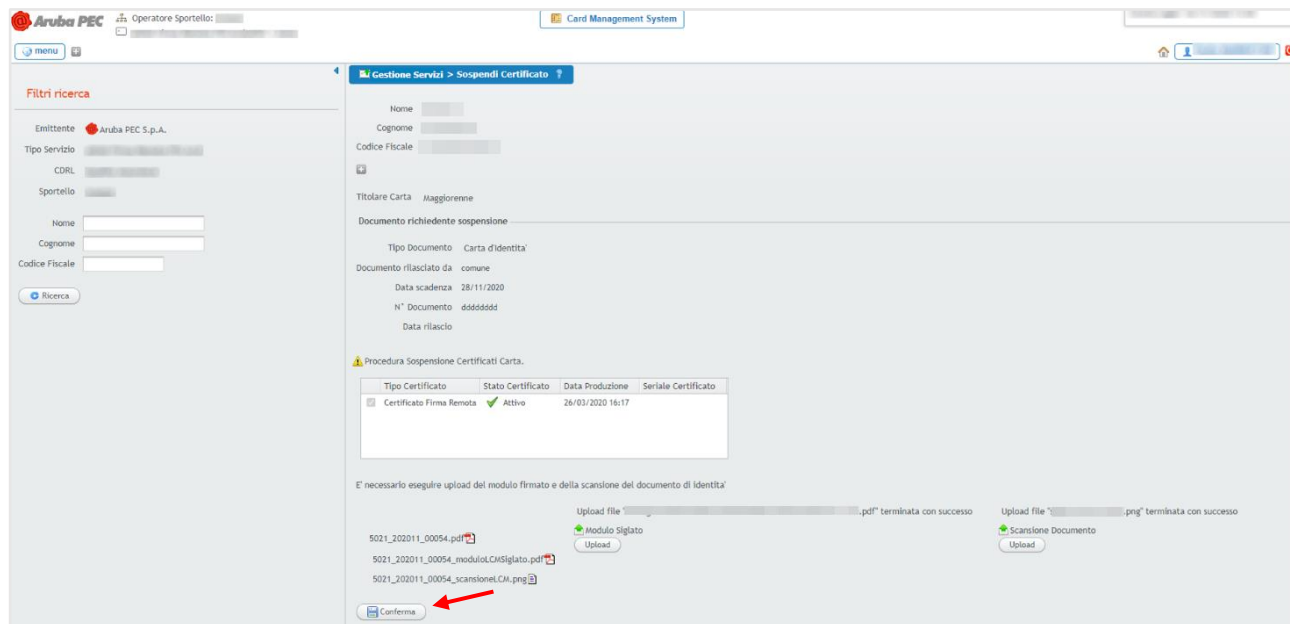


Proseguire con la procedura di sospensione del certificato e cliccare su **Avanti**.



È necessario scaricare il modulo dedicato alla sospensione e farlo firmare da chi ha richiesto la sospensione.

Successivamente eseguire l'upload del modulo firmato unitamente alla copia del documento di identità del Richiedente la revoca e infine cliccare su **Conferma** per concludere la procedura.



Il certificato è sospeso.

41

9.1.2 Riattivazione del Certificato

Per riattivare un certificato di Firma, l'ODR procede preliminarmente alla ricerca dello stesso accedendo al menù **Gestione Servizi > Riattiva Certificato**. Il CMS mostrerà i certificati intestati all'Utente, dando la possibilità di procedere con il cambio di stato. Selezionare quello di interesse e cliccare su **Riattiva Certificato**.

L'ODR dovrà far compilare e sottoscrivere il modulo di riattivazione all'Utente che ha richiesto il cambio di stato nonché acquisire copia del documento di identità dello stesso. Effettuato poi l'upload della predetta documentazione, completerà la procedura confermando le relative operazioni. Nel caso in cui sia necessario riattivare urgentemente un certificato di Firma, il Titolare potrà farlo in completa autonomia seguendo le indicazioni della guida dedicata <https://guide.pec.it/firma-digitale/sospensione-e-revoca/firma-digitale-riattivare-certificato.aspx>.

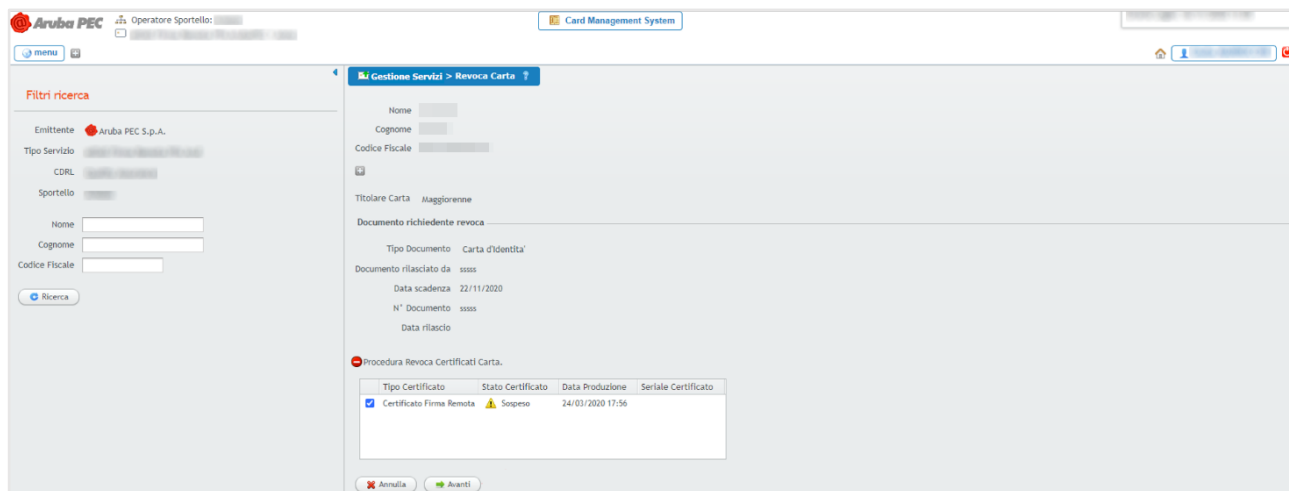
9.1.3 Revoca del Certificato

Accedere al menù **Gestione Servizi > Revoca Certificato** e procedere, tramite i filtri disponibili (Nome, Cognome, codice fiscale) alla ricerca del certificato per il quale si intende cambiare lo stato.

Il CMS mostrerà i certificati intestati all'Utente, dando la possibilità di provvedere al cambio di stato. Selezionare, quindi, il certificato da revocare e cliccare su **Revoca Certificato**.

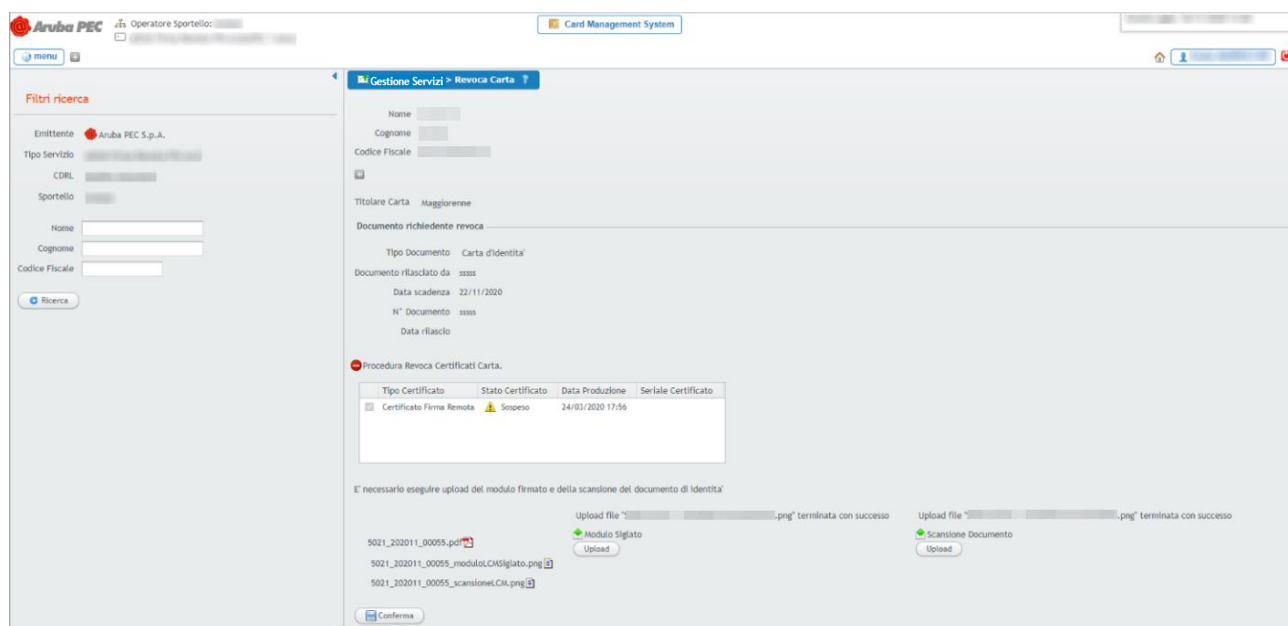
Servizio	N° seriale carta	European Code Carta	Nome	Cognome	Codice Fiscale	Stato Carta	operazione
CNS LIKE - eIDAS Firma PFA ArubaPEC						Operativa	 Revoca Certificato

L'operatore dovrà compilare i campi dedicati riportando gli estremi del documento di identità dell'Utente che ha richiesto il cambio di stato e proseguire con la procedura di revoca del certificato cliccando su **Avanti**.



È necessario scaricare l'apposito modulo e farlo firmare a chi ha richiesto la revoca.

Successivamente eseguirne l'upload unitamente a copia del documento di identità del Richiedente la revoca. Infine cliccare su **Conferma** per concludere la procedura.



42

Il certificato è revocato.

È importante ricordare le seguenti regole circa i cambi di stato dei certificati:

- per un certificato attivo può essere richiesta la sospensione o la revoca;
- un certificato sospeso, può essere riattivato o revocato;
- un certificato revocato cessa la propria funzionalità. La revoca è, pertanto, un processo irreversibile.

Nel caso in cui sia necessario revocare urgentemente un certificato di Firma Digitale, ad esempio per smarrimento, furto o guasto del dispositivo di Firma, è possibile farlo in completa autonomia tramite

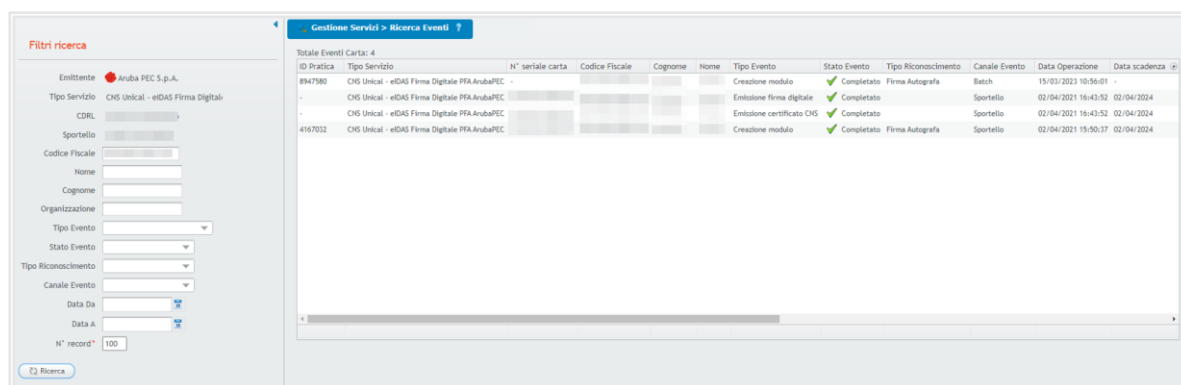
procedura online, come indicato nella guida dedicata raggiungibile al seguente link https://guide.pec.it/firma-digitale/sospensione-e-revoca-certificato/revocare-certificato-firma-digitale.aspx#a_1532941508407

Maggiori dettagli in merito alla revoca sono contenuti nel manuale operativo consultabile al seguente link https://www.pec.it/documents/tc-files/it/21_firmadigitalemanualeoperativo.pdf

9.2 Controllo delle attività

Il CMS consente di effettuare ricerche sui Certificati (Ricerca Eventi) e sui dispositivi Smart Card (Ricerca Carta) emessi.

La ricerca può essere effettuata tramite alcuni criteri come il codice fiscale, il nome, il cognome, ecc. Nell'esempio riportato di seguito la ricerca è stata effettuata tramite il codice fiscale.



The screenshot shows the 'Gestione Servizi > Ricerca Eventi' interface. On the left, there are various filters for searching events, including 'Emittente' (Aruba PEC S.p.A.), 'Tipo Servizio' (CNS Unical - eIDAS Firma Digitale), 'CDRL', 'Sportello', 'Codice Fiscale', 'Nome', 'Cognome', 'Organizzazione', 'Tipo Evento', 'Stato Evento', 'Tipo Riconoscimento', 'Canale Evento', 'Data Da', 'Data A', and 'N° record' (set to 100). On the right, a table displays the search results for 4 events.

ID Pratica	Tipo Servizio	N° seriale carta	Codice Fiscale	Cognome	Nome	Tipo Evento	Stato Evento	Tipo Riconoscimento	Canale Evento	Data Operazione	Data scadenza
8947580	CNS Unical - eIDAS Firma Digitale PFA.ArubaPEC					Creazione modulo	✓ Completato	Firma Autografa	Batch	15/03/2023 10:56:01	-
-	CNS Unical - eIDAS Firma Digitale PFA.ArubaPEC					Emissione firma digitale	✓ Completato		Sportello	02/04/2021 16:43:52	02/04/2024
-	CNS Unical - eIDAS Firma Digitale PFA.ArubaPEC					Emissione certificato CNS	✓ Completato		Sportello	02/04/2021 16:43:52	02/04/2024
4167032	CNS Unical - eIDAS Firma Digitale PFA.ArubaPEC					Creazione modulo	✓ Completato	Firma Autografa	Sportello	02/04/2021 15:50:37	02/04/2024

Per ricercare gli eventi su CMS, come la registrazione di un Utente e/o l'emissione dei certificati, è possibile selezionare la rispettiva voce dal menu **Gestione Servizi** ed impostare uno dei parametri di ricerca messi a disposizione.

10 Rinnovo Certificati

10.1 Rinnovo Firma Remota da area Selfcare

La procedura di rinnovo della Firma Remota deve essere effettuata dall'Utente **(per coloro che risultano già abilitati in tal senso)** direttamente dall'area Selfcare <https://selfcare.firma-remota.it/asmonitor/login.xhtml>.

Chi non ancora abilitato a tale flusso di rinnovo, effettuerà le relative operazioni collegandosi al link <https://manage.pec.it/KitFirmaDigitale/PrerequisitiFirmaDigitale.aspx> e seguendo i relativi step. Il CDRL potrà autorizzare il rinnovo dal menu **Gestione Servizi**, accedendo all'area **Rinnovo online**.

A partire, infatti, dal sessantesimo giorno antecedente la data di scadenza del certificato, verranno inoltrati, all'indirizzo email ad esso associato, i relativi avvisi contenenti le istruzioni per procedere al rinnovo ed il link dedicato di cui sopra.

Una volta effettuata l'autenticazione nell'area Selfcare con le proprie credenziali di Firma Remota, il Titolare verrà reindirizzato alla sezione dedicata al rinnovo del certificato dove visualizzerà il riepilogo dei dati intestatario. Potrà, se necessario, procedere alla modifica di alcuni di essi tra i quali indirizzo email, numero di cellulare e residenza.

Italiano ▼




Firma Remota

PANNELLO DI GESTIONE

Login

Nome utente ¹

Password

Login

[Recupero nome utente](#)
[Recupero password](#)

Se necessiti di aiuto, consulta le guide cliccando qui.

Rinnovo

Repliego Dati
Modulo Rinnovo
Firma Modulo
Conclusione

Dati Titolare

Nome

Cognome

Codice Fiscale

Sesso

Nazione di nascita

Provincia di nascita

Comune di nascita

Data di nascita

Dati modificabili

Nazione

Provincia

Comune Residenza

Telefono [Modifica](#)

Email [Modifica](#)

Via

Numero Civico

CAP

Organizzazione di appartenenza [i](#)

P.IVA Organizzazione appartenenza [i](#)

Titolo o carica [i](#)

Torna alla Home

Prosegui

Nel caso in cui si procedesse con la modifica dei dati, sarà necessario reinserire la password di Firma Remota (nell'apposita finestra dedicata che apparirà a centro pagina), aggiornare il dato di interesse (immagine 1 -

esempio modifica numero di cellulare) e, infine, confermare le operazioni mediante inserimento del codice OTP ricevuto via SMS (immagine 2).

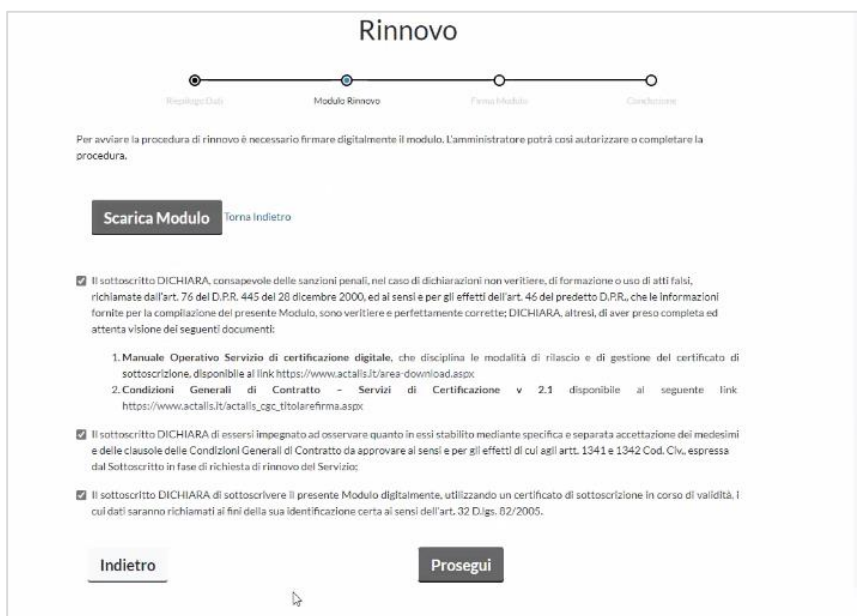


In caso di modifica dell'email o del numero di cellulare verrà effettuato un controllo su questi ultimi: se risultano già associati ad un diverso codice fiscale (ovvero non si è Titolare del recapito in maniera univoca), il rinnovo viene bloccato e per procedere è necessario modificare i dati inseriti. Ricordiamo che l'indirizzo email e numero di cellulare rappresentano **un canale di contatto riservato e importanti fattori di autenticazione** che devono essere riconducibili ad un'unica persona.

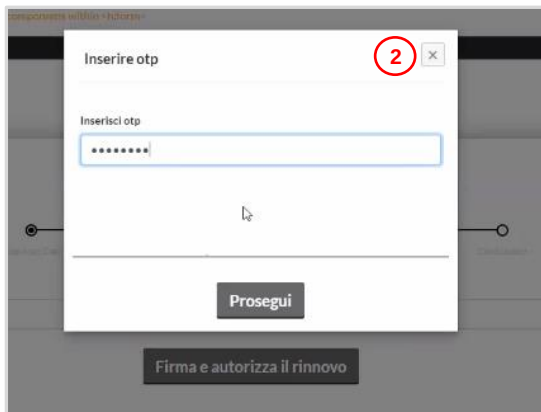
Nella medesima schermata saranno mostrati anche eventuali dati di ruolo già presenti nel certificato. Gli stessi non saranno modificabili. Qualora l'Utente necessitasse di un loro aggiornamento, dovrà richiedere un nuovo certificato di Firma Remota.

Una volta confermati o aggiornati i dati relativi alla propria utenza, verrà generato il modulo di rinnovo e le condizioni generali di contratto.

Il Titolare dovrà prendere visione degli stessi (con possibilità di effettuarne il download) e darne relativa conferma tramite la checkbox dedicata.



Procederà quindi alla sottoscrizione del modulo di rinnovo mediante inserimento delle credenziali di Firma Remota [Password (1) e OTP (2)].

Un apposito messaggio confermerà il buon esito delle operazioni e informerà che, per completare l'iter di rinnovo, sarà necessaria la relativa autorizzazione da parte del CDRL di riferimento (**immagine sottostante**)

salvo che quest'ultimo abbia optato per il rinnovo automatico dei certificati. In tal caso la procedura risulterà già completata.

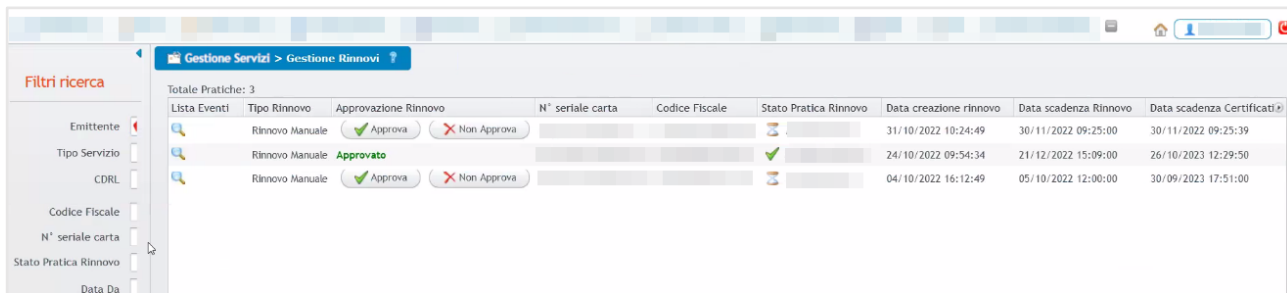


46

Procedura di autorizzazione da parte del CDRL

Dal menu **Gestione Servizi**, l'ODR, autenticatosi nel pannello CMS con il servizio riferibile al certificato da rinnovare (ad esempio **Firma Remota** o **elDAS Firma Remota, ecc.**), accede all'area **Gestione Rinnovi**. Da questa sezione è possibile ricercare le pratiche di rinnovo di interesse ed effettuare le conseguenti azioni.

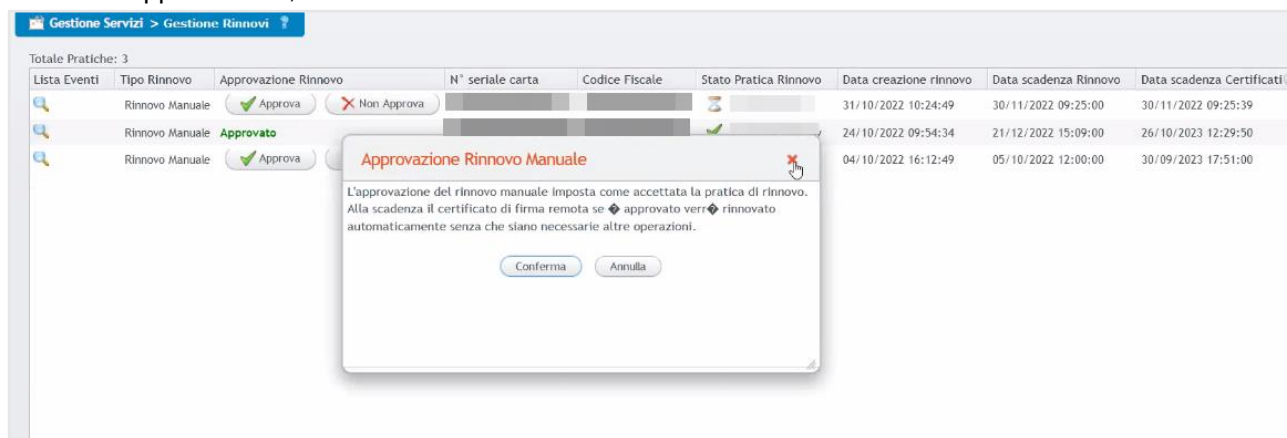
N.B. A mero titolo esemplificativo, il rinnovo di un certificato già emesso (o rinnovato) con il servizio **Firma Remota** potrà essere gestito dal menù dedicato selezionando detto servizio in sede di autenticazione al CMS.



Lista Eventi	Tipo Rinnovo	Approvazione Rinnovo	N° seriale carta	Codice Fiscale	Stato Pratica Rinnovo	Data creazione rinnovo	Data scadenza Rinnovo	Data scadenza Certificati
	Rinnovo Manuale	Approva / Non Approva				31/10/2022 10:24:49	30/11/2022 09:25:00	30/11/2022 09:25:39
	Rinnovo Manuale	Approvato				24/10/2022 09:54:34	21/12/2022 15:09:00	26/10/2023 12:29:50
	Rinnovo Manuale	Approva / Non Approva				04/10/2022 16:12:49	05/10/2022 12:00:00	30/09/2023 17:51:00

L'operatore può rinnovare solo i certificati in scadenza degli utenti che ne hanno richiesto il rinnovo. In tal caso, infatti, il sistema proporrà le due opzioni (pulsanti) “Approva” e “Non Approva”.

In caso di approvazione, verrà visualizzata la schermata sottostante.



Cliccando sul pulsante “Conferma”, il certificato si rinnoverà automaticamente alla scadenza senza necessità di ulteriori azioni da parte dell’ODR.

Qualora l’operatore di registrazione volesse, invece, chiudere la pratica senza autorizzare il rinnovo, dovrà premere sul pulsante “Non Approva”.

La procedura di autorizzazione da parte del CDRL potrà essere eseguita entro 90 giorni dalla sottoscrizione del modulo di rinnovo nell’area Selfcare. Superati 90 giorni, il rinnovo non potrà essere concluso.

47

Gli stati della pratica visibili dall'operatore sono:

- 1) **Comunicato**: in attesa della firma del modulo;
- 2) **Inoltrato**: in attesa rinnovo;
- 4) **Completato**: rinnovo completato;
- 5) **Scaduto**: pratica di rinnovo scaduta;
- 6) **Cancellato**: pratica di rinnovo cancellata;

Nella procedura di rinnovo, così come accade in sede di prima emissione, vengono scalati dal contatore dei certificati disponibili del pannello CMS quelli funzionali alle relative operazioni.

In caso di giacenza insufficiente, provvedere all’acquisto dei certificati in base alla tipologia richiesta.

10.2 Rinnovo carta con Aruba Enroll

Il rinnovo del certificato può essere eseguito a partire da 2 mesi prima della data di scadenza dello stesso.

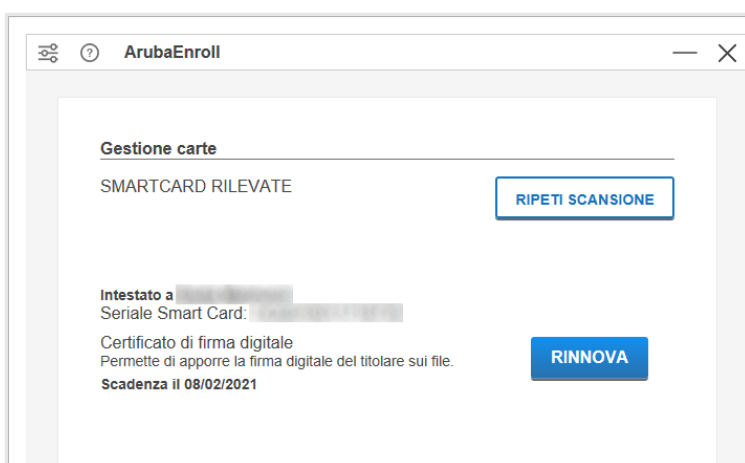
Dato che dopo la scadenza il servizio non potrà più essere rinnovato, consigliamo di effettuare il rinnovo con qualche giorno di anticipo: questo non comporterà la perdita di alcun giorno di validità o l'anticipo della data di scadenza successiva.

Di seguito gli step previsti per effettuare rinnovo:

- Ricezione email di avviso rinnovo e con le istruzioni per procedere;
- Collegarsi alla pagina indicata [qui](#), ed effettuare il download del software Aruba Enroll;

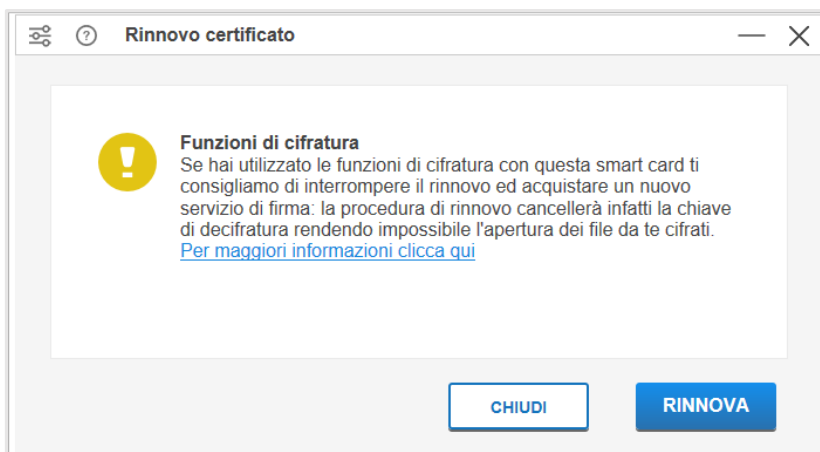
Aruba Enroll è compatibile con il sistema operativo Windows 7 SP3 o superiore, OSX 10.10 o superiore.

- Completare la procedura guidata di installazione;
- Installato e aperto il software e collegata la carta al computer, in automatico viene scansionata la carta e mostrato a video il seriale;
Qualora si rilevassero più Smart Card e certificati, è necessario scegliere il certificato in scadenza.
- A questo punto cliccare su **Rinnova**.

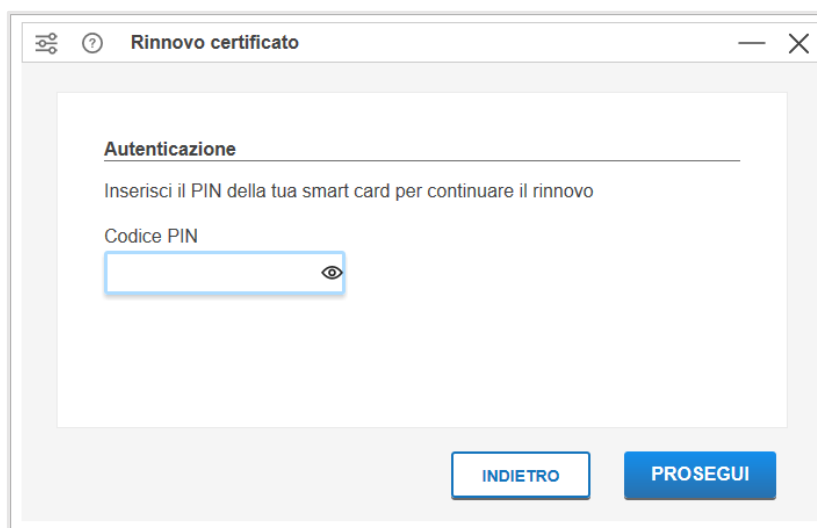


48

Se sono state utilizzate le **funzioni di cifratura con questa Smart Card**, consigliamo di **interrompere il rinnovo ed acquistare un nuovo servizio di Firma**: la procedura di rinnovo cancellerà la chiave di decifratura rendendo impossibile l'apertura del file cifrato. Per maggiori informazioni cliccare [qui](#).

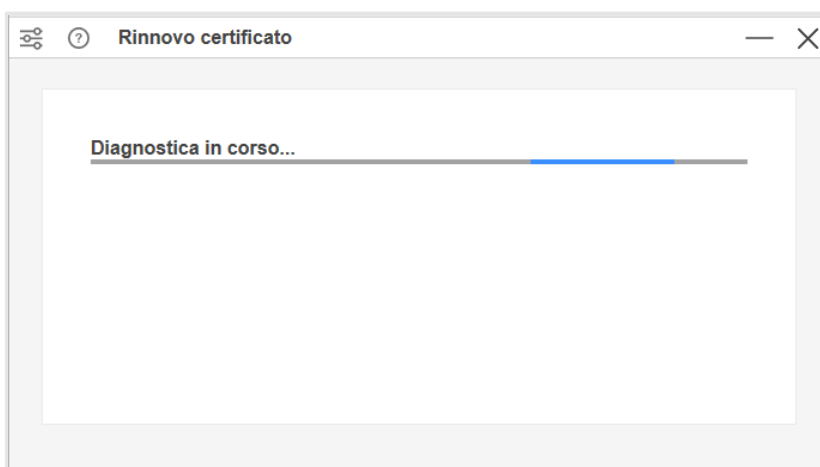


- Inserire il **PIN** della Smart Card per l'autenticazione;



49

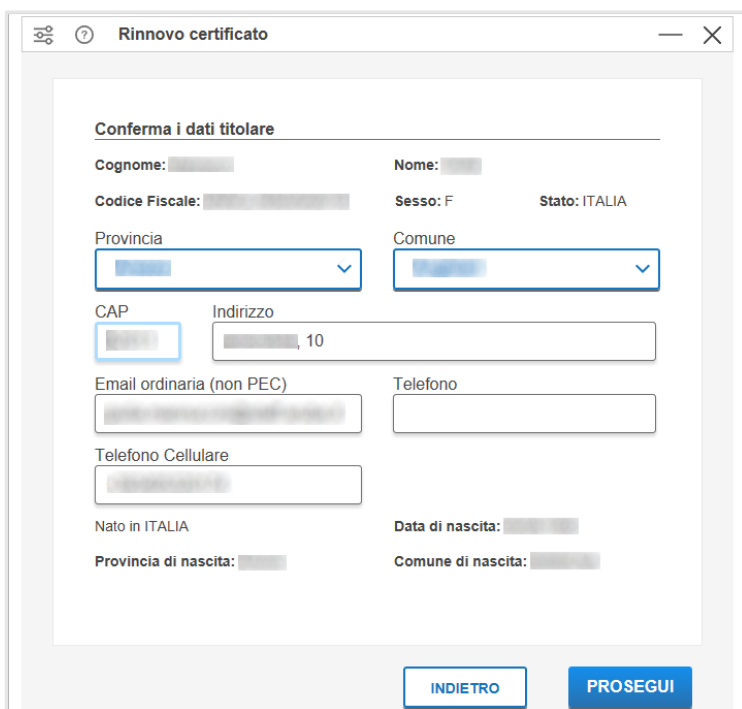
Successivamente viene svolta una **diagnostica sulla Smart Card** per capire se è possibile proseguire con il rinnovo.



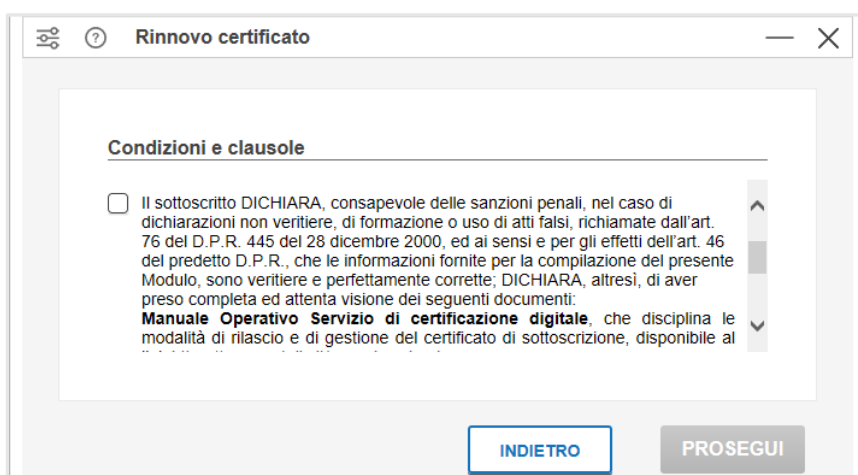
Qualora la carta risulti non adatta al rinnovo (ad esempio carta obsoleta) è necessario procedere con un nuovo acquisto.

- Vengono poi mostrati i dati relativi all'utenza di Firma con possibilità di modificare i dati non contenuti sul certificato (cellulare, email, indirizzo).

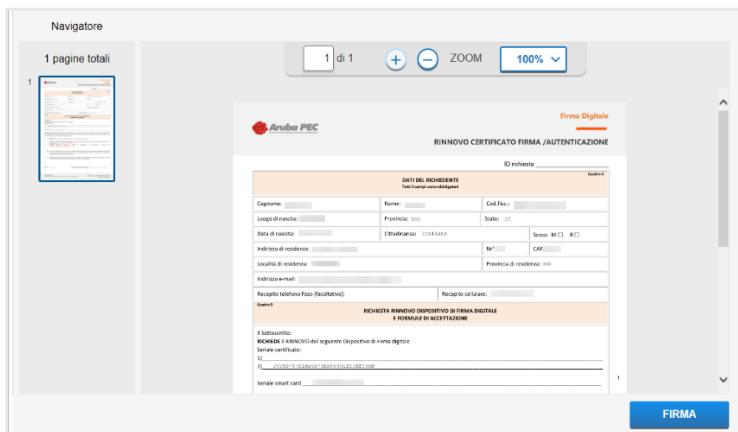
In fase di rinnovo viene effettuato un controllo su indirizzo email e numero di cellulare: se risultano già associati ad un diverso codice fiscale (ovvero non si è Titolare del recapito in maniera univoca, il rinnovo viene bloccato e per procedere è necessario modificare i dati inseriti. Ricordiamo che l'indirizzo email e numero di cellulare **rappresentano un canale di contatto riservato e importanti fattori di autenticazione** che devono essere riconducibili ad un'unica persona.



- Verificati i dati, è necessario procedere con l'accettazione contratti e clausole su Aruba Enroll.

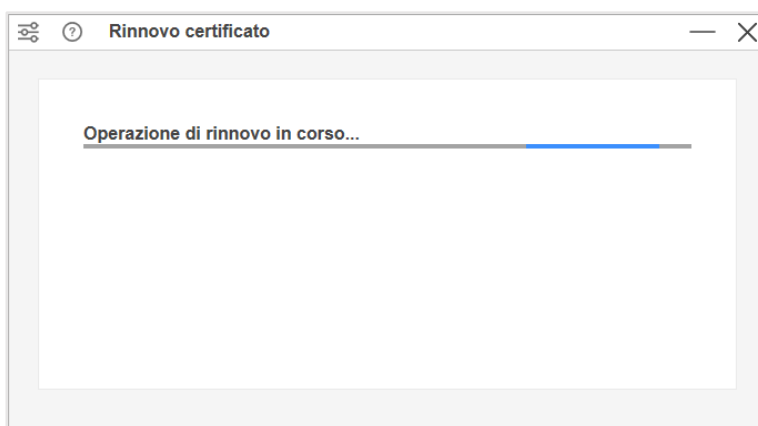


- Dopo questo passaggio viene visualizzato il modulo rinnovo e viene richiesta la firma dello stesso con il certificato in scadenza. Cliccare dunque su **FIRMA**:



Il modulo di richiesta firmato digitalmente, viene inviato tramite email, all'indirizzo associato al Titolare.

Successivamente avviene l'aggiornamento dei certificati tramite Aruba Enroll e relativo rinnovo.

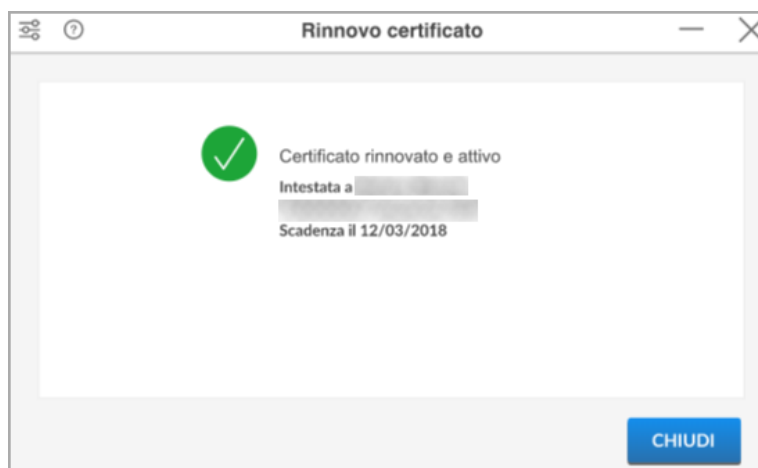


51

Sulla base degli accordi con il proprio CDRL Il rinnovo può avvenire in **modo automatico** o può essere **soggetto ad autorizzazione del CDRL**.

RINNOVO AUTOMATICO

Qualora il rinnovo sia stato concordato con il CDRL in modo automatico la procedura di rinnovo si conclude.

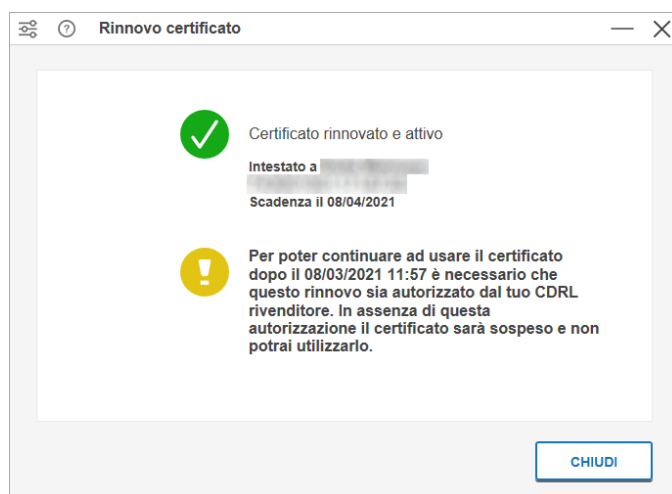


In caso di rinnovo certificato non riuscito, è necessario aprire una richiesta di assistenza tramite i canali dedicati.

Viene, inoltre, inviata un'email di avvenuto rinnovo contenente anche il **codice utente**, il quale deve essere conservato con la massima riservatezza, in quanto necessario per eseguire alcune operazioni sulla propria Firma Digitale, come la **sospensione**, **revoca** o **riattivazione** dei certificati.

RINNOVO SOGGETTO AD AUTORIZZAZIONE

In caso di rinnovo **soggetto ad autorizzazione del CDRL**, la procedura di rinnovo del servizio di Firma Digitale risulta conclusa solo in parte, in quanto è necessaria un'autorizzazione da parte del proprio CDRL rivenditore:



52

Una volta concluso il rinnovo sul software Aruba Enroll, il certificato è attivo e funzionante e si riceve un'email di avvenuto rinnovo contenente anche il **codice utente**.

Tuttavia, se il proprio **CDRL rivenditore non autorizza il rinnovo entro la data di scadenza del vecchio certificato**, lo stesso verrà sottoposto ad una sospensione autoritativa ed il **servizio di Firma Digitale non sarà più utilizzabile**.

Pertanto si consiglia di contattare il proprio CDRL, per sollecitare l'autorizzazione del rinnovo.

Una volta autorizzato, la procedura di rinnovo si conclude.

Potrebbe accadere che il rinnovo non venga autorizzato entro la scadenza del vecchio certificato, questo comporta la sospensione del certificato che potrà comunque essere **riattivato entro 120 giorni dalla sospensione**, con l'intervento del CDRL che autorizza il rinnovo.

Superati i 120 giorni dalla sospensione il certificato sarà revocato in modo irreversibile ed il rinnovo del servizio non potrà essere concluso.

Per usufruire del servizio di Firma Digitale, sarà quindi necessario effettuare un nuovo acquisto.

Verranno, comunque, inviati tramite email, degli **avvisi di prossima sospensione** e **avvisi di prossima revoca**, al Titolare della Firma.

Procedura di autorizzazione da parte del CDRL

L'operatore può controllare lo stato dei rinnovi e gestirne l'approvazione autenticandosi al CMS e accedendo alla sezione **Gestione Servizi > Gestione rinnovi**. A seconda del servizio scelto in sede di accesso al pannello, ad esempio **CNS - Firma 3 anni**, **CNS Unical – eIDAS Firma Digitale** o **CNS Like - Firma 3 anni** ecc., si visualizzeranno le relative pratiche di rinnovo disponibili.

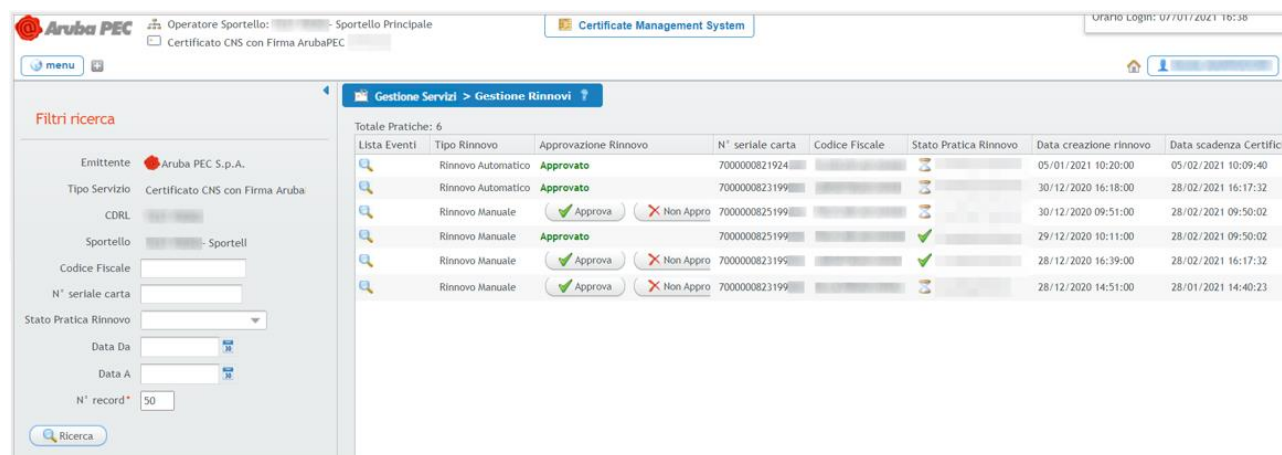
N.B. A mero titolo esemplificativo, il rinnovo di un certificato già emesso (o rinnovato) con il servizio **CNS - Firma 3 anni** potrà essere gestito dal menù dedicato selezionando detto servizio in sede di autenticazione al CMS.

Nel caso di CDRL provenienti dalla **WebRA Actalis** è necessario selezionare il vecchio servizio di emissione che presenta la dicitura WebRA.

N.B. Aruba Enroll non può essere utilizzato per i rinnovi dei certificati di Firma Remota, la cui procedura è visibile nei paragrafi dedicati.

L'operatore può autorizzare le singole richieste di rinnovo cliccando su **Approva**. Qualora si volesse rifiutare la richiesta di rinnovo è necessario cliccare su **Non approva**.

Si ricorda che in mancanza di approvazione il certificato viene sospeso alla data scadenza del vecchio certificato. **Superati i 120 giorni dalla sospensione il certificato sarà revocato** in modo irreversibile ed il rinnovo del servizio non potrà essere concluso.



Aruba PEC Operatore Sportello: Sportello Principale | Certificato Management System | Utente Login: 07/01/2021 16:38

Filtri ricerca

Emittente: **Aruba PEC S.p.A.**

Tipo Servizio: **Certificato CNS con Firma Aruba**

CDRL: **CDRL**

Sportello: **Sportello**

Codice Fiscale:

N° seriale carta:

Stato Pratica Rinnovo:

Data Da:

Data A:

N° record:

Ricerca

Gestione Servizi > Gestione Rinnovi

Totale Pratiche: 6

Lista Eventi	Tipo Rinnovo	Approvazione Rinnovo	N° seriale carta	Codice Fiscale	Stato Pratica Rinnovo	Data creazione rinnovo	Data scadenza Certificato
	Rinnovo Automatico	Approvato	7000000821924			05/01/2021 10:20:00	05/02/2021 10:09:40
	Rinnovo Automatico	Approvato	7000000823199			30/12/2020 16:18:00	28/02/2021 16:17:32
	Rinnovo Manuale	Approva Non Appro	7000000825199			30/12/2020 09:51:00	28/02/2021 09:50:02
	Rinnovo Manuale	Approvato	7000000825199			29/12/2020 10:11:00	28/02/2021 09:50:02
	Rinnovo Manuale	Approva Non Appro	7000000823199			28/12/2020 16:39:00	28/02/2021 16:17:32
	Rinnovo Manuale	Approva Non Appro	7000000823199			28/12/2020 14:51:00	28/01/2021 14:40:23

53

Gli stati della pratica visibili dall'operatore sono:

1. **Comunicato:** in attesa della firma del modulo
2. **In attesa emissione:** in attesa della installazione dei nuovi certificati
3. **Completato:** rinnovo completato
4. **Scaduto:** pratica di rinnovo scaduta
5. **Cancellato:** pratica di rinnovo cancellata

Eseguita la procedura di rinnovo sarà poi possibile ricercare le pratiche rinnovate, accedendo al servizio di emissione che presenta la dicitura **eIDAS**. Per procedere in tal senso, dal menù **"Gestione Servizi"**, selezionare la funzione **"Ricerca Eventi"**, e, inseriti i dati del certificato di interesse, avviare la ricerca. Sarà così possibile

visionare la modalità di rinnovo adottata (canale evento), l'esito della stessa e la nuova data di scadenza dei certificati.

ID Pratica	Tipo Servizio	N° seriale carta	Codice Fiscale	Cognome	Nome	Tipo Evento	Stato Evento	Tipo Riconoscimento	Canale Evento	Data Operazione	Data scadenza	CDRL
-	CNS Unical - eIDAS Firma Digitale PFA ArubaPEC					Emissione firma digitale	✓ Completat		Aruba Enroll	07/02/2023 14:38:32	10/02/2026	
-	CNS Unical - eIDAS Firma Digitale PFA ArubaPEC					Emissione certificato CNS	✓ Completat		Aruba Enroll	07/02/2023 14:38:32	10/02/2026	
	CNS Unical - eIDAS Firma Digitale PFA ArubaPEC					Rinnovo	✓ Completat		Aruba Enroll	07/02/2023 14:37:40	10/02/2026	

Nella procedura di rinnovo, così come accade in sede di prima emissione, verranno scalati dal contatore dei certificati disponibili del pannello CMS quelli funzionali alle relative operazioni (ad esempio per il rinnovo di una Smart Card Carta Nazionale dei Servizi contenente certificato di autenticazione CNS e certificato di Firma Digitale verrà scalata la suddetta coppia di certificati).

In caso di giacenza insufficiente, provvedere all'acquisto dei certificati in base alla tipologia richiesta.