



***Guida per l'emissione di un certificato di
Firma Digitale con riconoscimento in
presenza e acquisizione del consenso
con Firma Elettronica***

Sommario

SOMMARIO	2
1. ACCESSO AL PORTALE CMS ARUBA.....	3
2. ACCESSO CON FIRMA REMOTA.....	3
3. COMPILAZIONE DEI DATI DELLA SEZIONE “REGISTRAZIONE CERTIFICATO”	6
4. EMISSIONE CERTIFICATI DI FIRMA DIGITALE E ACQUISIZIONE DEL CONSENSO CON FIRMA ELETTRONICA.....	7
5. RECUPERO PIN E PUK.....	11


1. Accesso al portale CMS Aruba.

Per accedere al portale **Card Management System di Aruba**, in seguito **CMS**, ciascun **Operatore Di Registrazione**, in seguito **ODR**, deve preventivamente installare sulla propria postazione di lavoro **Java** dalla versione 7 in poi e un browser compatibile (Google Chrome) e deve inoltre disporre delle credenziali della propria **firma remota**.

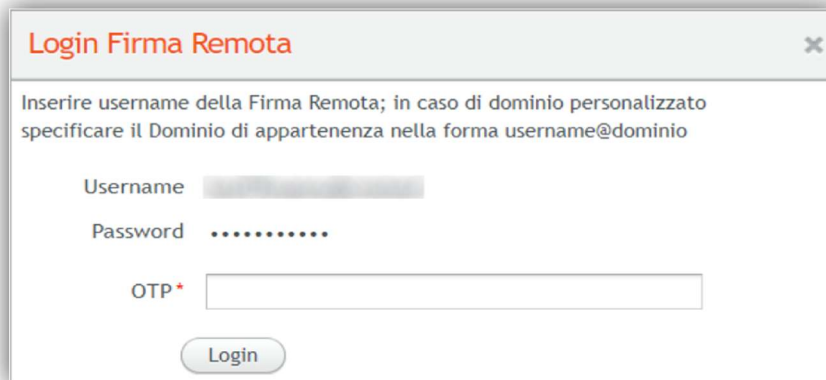
L'indirizzo del CMS Aruba è il seguente: <https://cms.gruppoaruba.it/CMSARUBA/cmsaruba/>.

2. Accesso con firma remota.

Una volta selezionato il pulsante **“Login con firma remota”**, l'**ODR** dovrà inserire il proprio username completo (nome.cognome@unina.it) e la password, ricevuta da Aruba all'atto della attivazione della firma remota.



Infine, dovrà inserire il codice **OTP**, ricevuto tramite l'app mobile **“Aruba OTP”** opportunamente configurata con le stesse credenziali utilizzate per l'accesso tramite firma remota.



Login Firma Remota

Inserire username della Firma Remota; in caso di dominio personalizzato specificare il Dominio di appartenenza nella forma username@dominio

Username

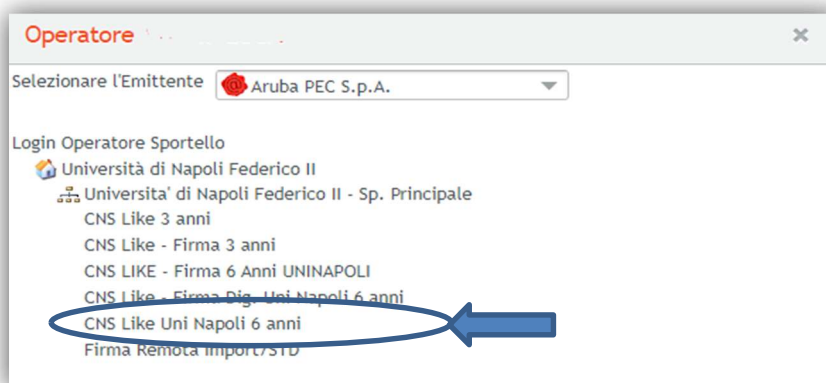
Password

OTP*


Login

Completato l'accesso al portale, viene mostrato in primo piano il menù a scelta multipla dove l'**ODR** deve selezionare il servizio che presenta la dicitura **"CNS LIKE – Firma 6 anni UNINAPOLI"**.

Poichè Aruba non lo ha ancora reso uniforme il menu per tutti gli operatori UNINA, l'ODR potrebbe visualizzare le seguenti opzioni:



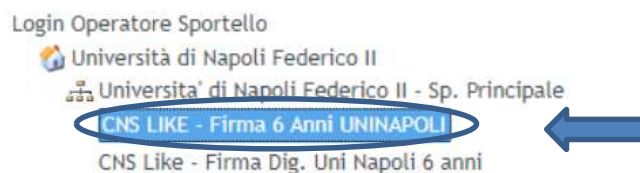
Operatore

Selezionare l'Emittente  Aruba PEC S.p.A.

Login Operatore Sportello

- Università di Napoli Federico II
 - Università di Napoli Federico II - Sp. Principale
 - CNS Like 3 anni
 - CNS Like - Firma 3 anni
 - CNS LIKE - Firma 6 Anni UNINAPOLI
 - CNS Like - Firma Dig. Uni Napoli 6 anni
 - CNS Like Uni Napoli 6 anni**
 - Firma Remota Import/STU


Oppure, in alternativa, il seguente menu:



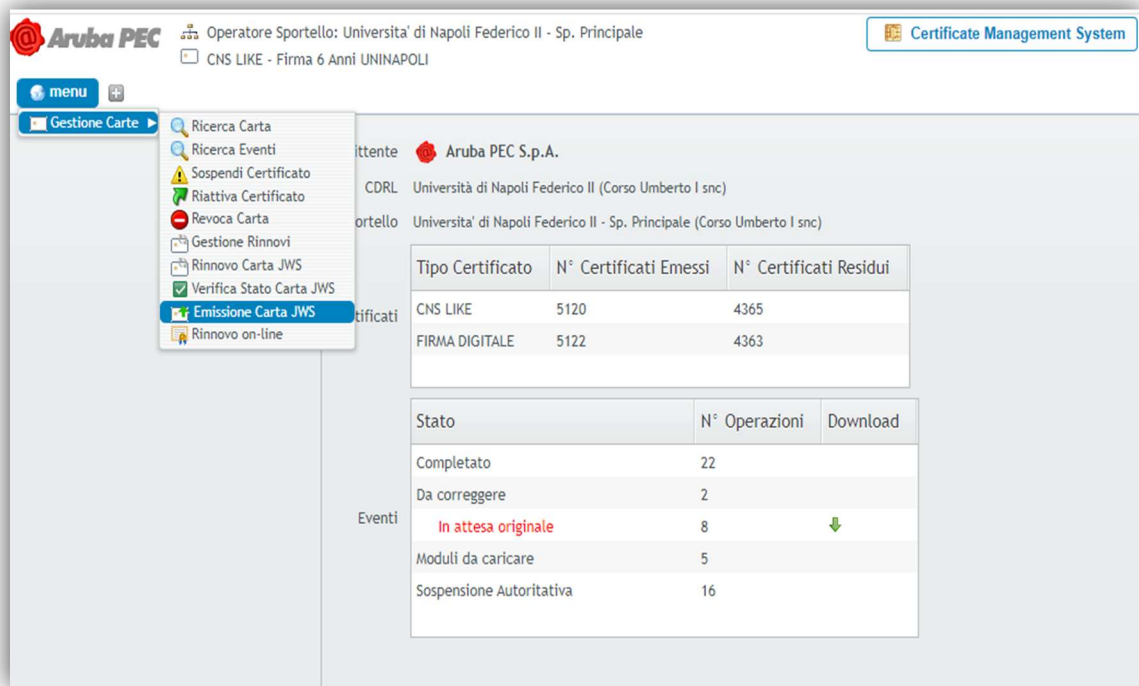
Login Operatore Sportello

- Università di Napoli Federico II
 - Università di Napoli Federico II - Sp. Principale
 - CNS LIKE - Firma 6 Anni UNINAPOLI**
 - CNS Like - Firma Dig. Uni Napoli 6 anni

Selezionato il servizio **"CNS LIKE – Firma 6 anni UNINAPOLI"**, si accede alla homepage del **CMS** che mostra il rendiconto dei certificati acquistati, emessi e residui per la tipologia di servizio attivo e, nella parte superiore sinistra della finestra, il menu **"Gestione Carte"**:

		OPERAZIONI
 <p>Gestione Carte</p> <ul style="list-style-type: none"> Ricerca Carta Ricerca Eventi Sospendi Certificato Riattiva Certificato Revoca Carta Verifica Stato Carta JWS Rinnovo Carta JWS Emissione Carta JWS Rinnovo on-line 	Emissione dei Certificati Digitali	Emissione Carta JWS (Java Web Start) Rinnovo Carta JWS (Java Web Start) Rinnovo Online
	Controllo Certificati Digitali	Ricerca Carta Ricerca Eventi Verifica Stato Carta
	Gestione del Ciclo Vita dei Certificati Digitali	Sospensione Riattivazione Revoca

Nel menu "Gestione carte" andrà selezionata la voce: "Emissione Carta JWS":



Operatori Sportello: Università di Napoli Federico II - Sp. Principale
CNS LIKE - Firma 6 Anni UNINAPOLI

Aruba PEC S.p.A.

CDRL Università di Napoli Federico II (Corso Umberto I snc)
Sportello Università di Napoli Federico II - Sp. Principale (Corso Umberto I snc)

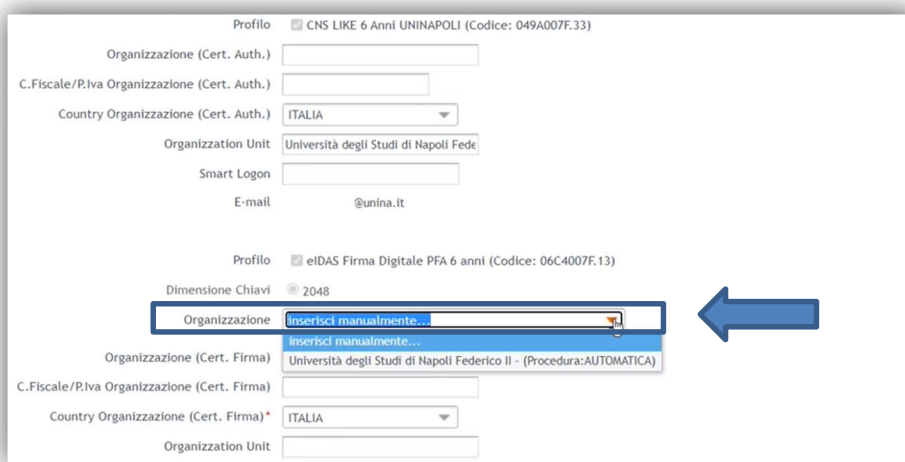
Tipo Certificato	N° Certificati Emessi	N° Certificati Residui
CNS LIKE	5120	4365
FIRMA DIGITALE	5122	4363

Stato	N° Operazioni	Download
Completato	22	
Da correggere	2	
In attesa originale	8	↓
Moduli da caricare	5	
Sospensione Autoritativa	16	

3. Compilazione dei dati della sezione “Registrazione certificato”

L’**ODR**, dopo aver inserito i dati anagrafici e gli estremi del documento di riconoscimento in corso di validità del Titolare richiesti per il rilascio del certificato, deve procedere con la compilazione sezione “**Registrazione del certificato**” necessari affinché il “**Quadro B2**” del modulo “Richiesta Certificato” sia debitamente redatto.

Pertanto, è necessario attivare il menu a tendina presente in corrispondenza del campo “**Organizzazione**” e selezionare l’opzione “**Università degli Studi di Napoli Federico II – (Procedura: AUTOMATICA)**”



Profilo CNS LIKE 6 Anni UNINAPOLI (Codice: 049A007F.33)

Organizzazione (Cert. Auth.)

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

Country Organizzazione (Cert. Auth.)


Organization Unit

Smart Logon

E-mail

Profilo eIDAS Firma Digitale PFA 6 anni (Codice: 06C4007F.13)

Dimensione Chiavi 2048

Organizzazione 

Organizzazione (Cert. Firma)

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

Country Organizzazione (Cert. Firma)*

Organization Unit

A seguito di questa operazione, i dati relativi alla denominazione e al codice fiscale dell’Ateneo vengono valorizzati secondo i valori preimpostati, lasciando all’**ODR** il compito di provvedere alla selezione da un ulteriore menu a tendina dell’identità designata a validare tali informazioni.



Profilo eIDAS Firma Digitale PFA 6 anni (Codice: 06C4007F.13)

Dimensione Chiavi 2048

Organizzazione

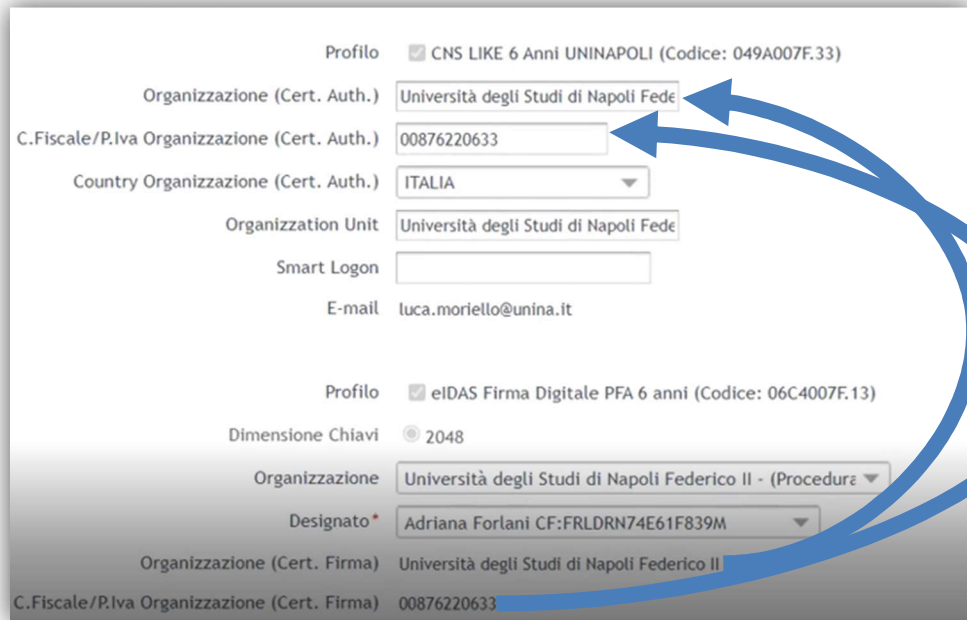
Designato* 

Organizzazione (Cert. Firma)

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

Country Organizzazione (Cert. Firma)

Infine, i dati relativi all'organizzazione e al suo codice fiscale vanno ricopiati, utilizzando due operazioni di copia/incolla, anche negli omologhi campi presenti nella parte superiore della videata e relativi al certificato **CNS**.



Profilo	<input checked="" type="checkbox"/> CNS LIKE 6 Anni UNINAPOLI (Codice: 049A007F.33)
Organizzazione (Cert. Auth.)	Università degli Studi di Napoli Fede
C.Fiscale/P.Iva Organizzazione (Cert. Auth.)	00876220633
Country Organizzazione (Cert. Auth.)	ITALIA
Organization Unit	Università degli Studi di Napoli Fede
Smart Logon	
E-mail	luca.moriello@unina.it
Profilo	<input checked="" type="checkbox"/> eIDAS Firma Digitale PFA 6 anni (Codice: 06C4007F.13)
Dimensione Chiavi	<input checked="" type="radio"/> 2048
Organizzazione	Università degli Studi di Napoli Federico II - (Procedur
Designato *	Adriana Forlani CF:FRLDRN74E61F839M
Organizzazione (Cert. Firma)	Università degli Studi di Napoli Federico II
C.Fiscale/P.Iva Organizzazione (Cert. Firma)	00876220633

4. Emissione certificati di Firma Digitale e acquisizione del consenso con Firma Elettronica.

L'**ODR**, dopo aver inserito i dati anagrafici, gli estremi del documento di riconoscimento in corso di validità del Titolare e tutte le ulteriori informazioni richieste per il rilascio del certificato, deve selezionare la modalità di riconoscimento in presenza con acquisizione consenso con Firma Elettronica dall'apposito menu a tendina.

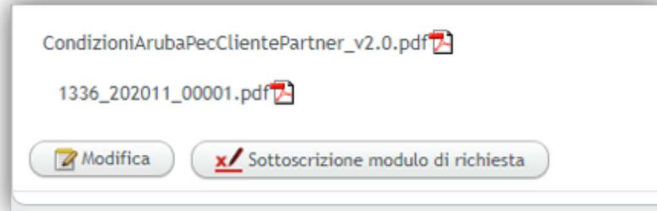


Tipo riconoscimento *	In Presenza
Acquisizione Consenso *	Firma Elettronica

Il processo prevede l'accettazione da parte del Titolare della firma 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 e trasmesso a mezzo SMS al numero di telefono del Titolare immesso in fase di registrazione.

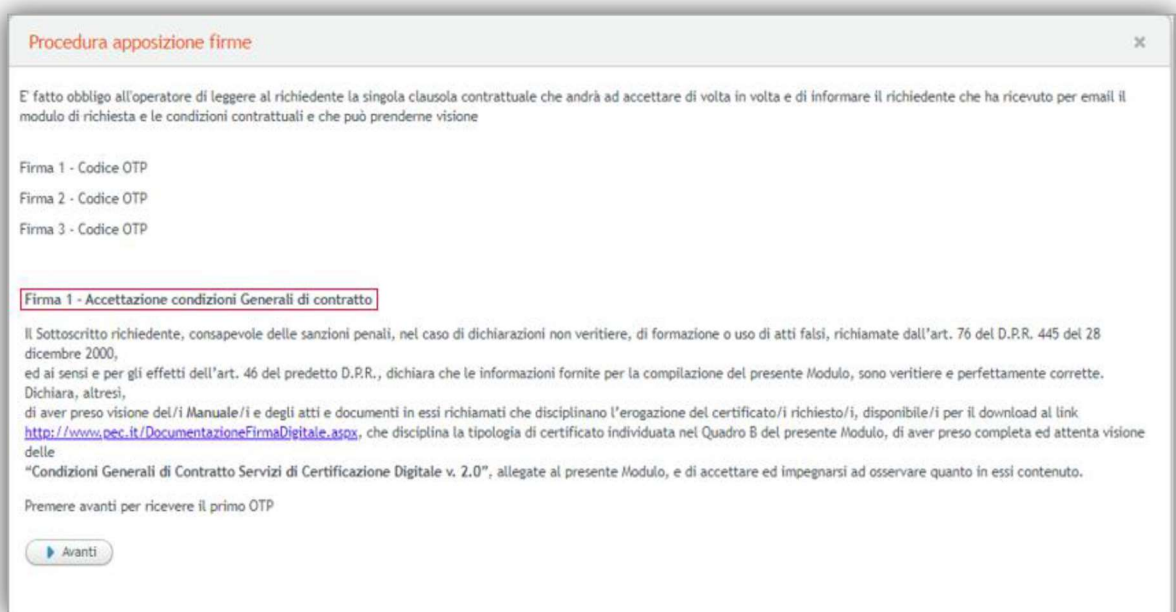
In dettaglio, selezionato il pulsante "**Sottoscrizione modulo di richiesta**", l'ODR avvia la procedura di apposizione firme da parte del Titolare, attraverso l'apposizione di tre firme elettroniche del

richiedente, obbligatorie e necessarie per l'accettazione delle *Condizioni Generali di Contratto*, delle *clausole vessatorie* e dell'*informativa privacy*, che devono essere lette e sottoposte al richiedente.



Il Titolare del certificato riceverà quindi, al proprio numero di cellulare inserito in fase di registrazione, 3 codici **OTP** di firma che comunicherà all'ODR, il quale dovrà digitarli all'interno degli appositi campi.

L'inserimento dei codici OTP avviene in sequenza, secondo i passi di seguito riportati, a seguito della selezione del pulsante "**Avanti**":



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 3 - Codice OTP

Firma 1 - Accettazione condizioni Generali di contratto

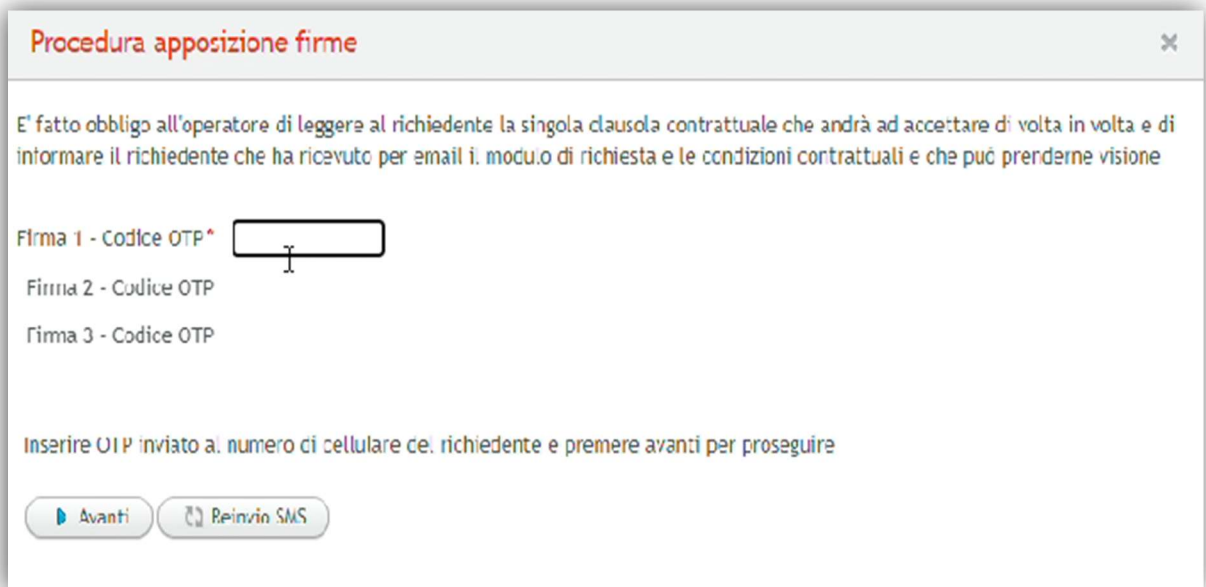
Il Sottoscritto richiedente, consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere, di formazione o uso di atti falsi, richiamate dall'art. 76 del D.P.R. 445 del 28 dicembre 2000, ed ai sensi e per gli effetti dell'art. 46 del predetto D.P.R., dichiara che le informazioni fornite 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

Il sistema invierà quindi al Titolare il primo SMS contenente il primo codice OTP.

Di seguito la schermata per l'immissione del codice OTP di firma ricevuto dal Titolare:



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

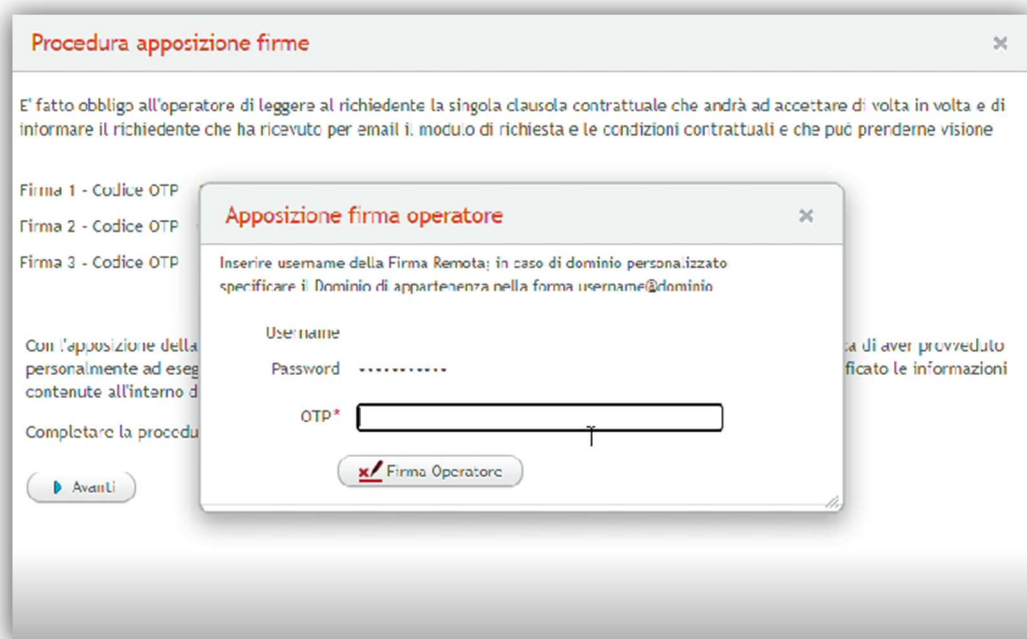
Firma 3 - Codice OTP

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

Qualora il titolare non abbia ricevuto il codice **OTP**, sarà compito dell'**ODR** richiedere un nuovo invio attraverso la funzionalità "**Reinvio SMS**".

Selezionando il tasto "**Avanti**", il processo sarà reiterato per la seconda e terza firma mediante OTP.

Una volta che completata l'apposizione delle tre firme elettroniche del richiedente, l'**ODR** procede all'apposizione della propria firma digitale sul modulo di richiesta, tramite il dispositivo di Firma Remota con la quale ha effettuato l'accesso al **CMS**, cliccando sul pulsante "**Avanti**".



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 3 - Codice OTP

Con l'apposizione della propria firma personale ad eseguire le operazioni contenute all'interno del modulo di richiesta. Completare la procedura premendo il pulsante Avanti.

Apposizione firma operatore

Inserire username della Firma Remota; in caso di dominio personalizzato specificare il Dominio di appartenenza nella forma username@dominio

Username

Password

OTP *

Con l'apposizione della propria firma, l'operatore certifica di aver provveduto ad eseguire l'attività di identificazione del richiedente e di aver verificato le informazioni contenute all'interno del modulo, che verrà inviato a richiedente a mezzo mail sul proprio indirizzo di posta istituzionale e che potrà essere scaricato dall'**ODR** mediante l'apposito collegamento:



Infine, si procede all'emissione del certificato utilizzando l'apposito pulsante "**Emissione live Carta**". Una volta emesso il certificato e dopo averlo caricato nella Smart Card, l'operatore consegna all'utente il kit completo di Firma Digitale e la prima parte dei codici **PIN** e **PUK** selezionando una delle due opzioni:

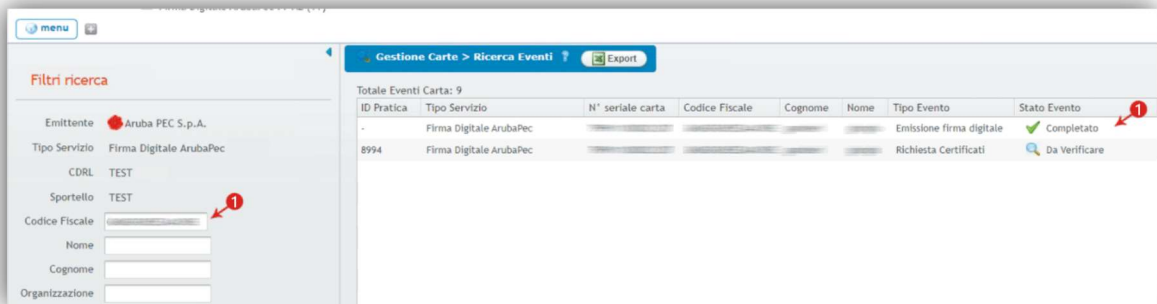
- **SMS**: inviato in tempo reale al cellulare del Titolare;
- oppure
- **Stampa**: è possibile stampare la metà dei codici cliccando su Stampa prima parte PIN e PUK e consegnarli all'utente.

Contemporaneamente, il Titolare riceverà la seconda parte del PIN e del PUK e il codice utente **all'indirizzo di posta elettronica** istituzionale indicato in fase di registrazione.

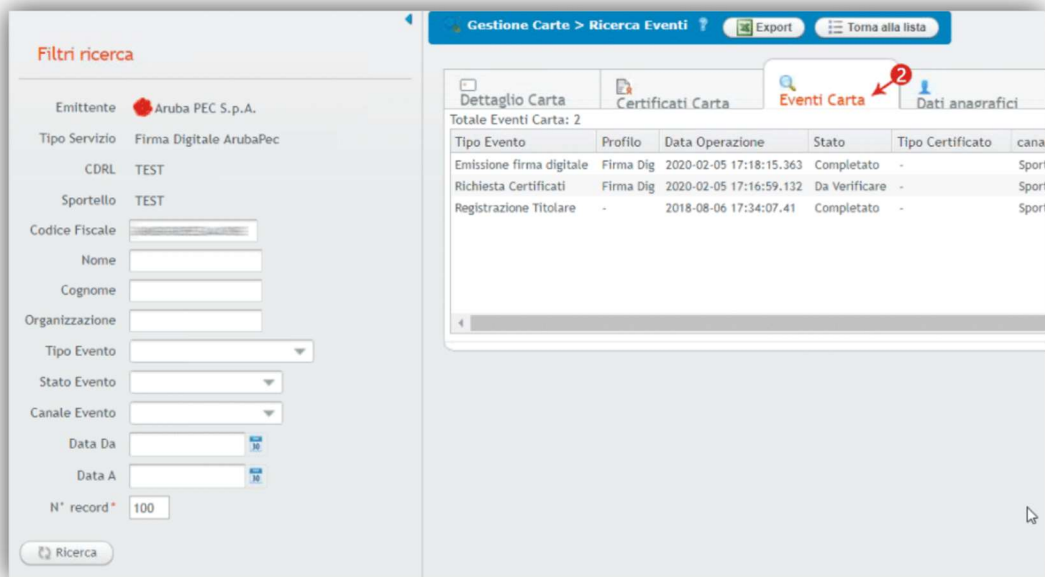
5. Recupero PIN e PUK

Nel caso in cui un utente dichiara di aver smarrito o di non aver mai ricevuto i codici **PIN** e **PUK**, ciascun **ODR** può richiedere che vengano rinviati al titolare del certificato di Firma Digitale seguendo la seguente procedura:

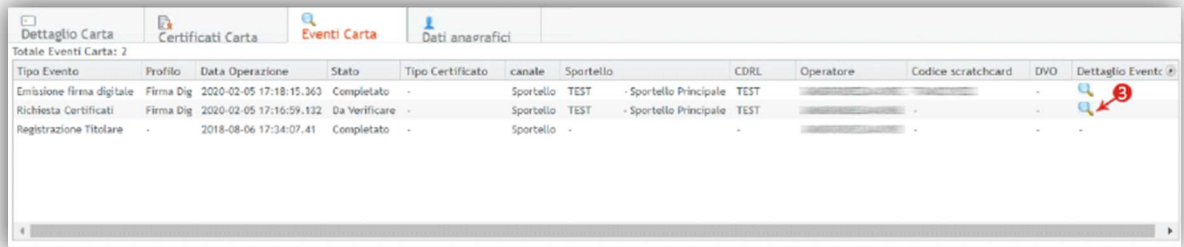
1. Selezionare la voce **“Ricerca carta”** dal menu **“Gestione carte”** e ricercare e selezionare il certificato emesso tramite uno dei filtri presenti (cognome, nome, codice fiscale).




2. Selezionare la scheda **“Eventi Carta”**

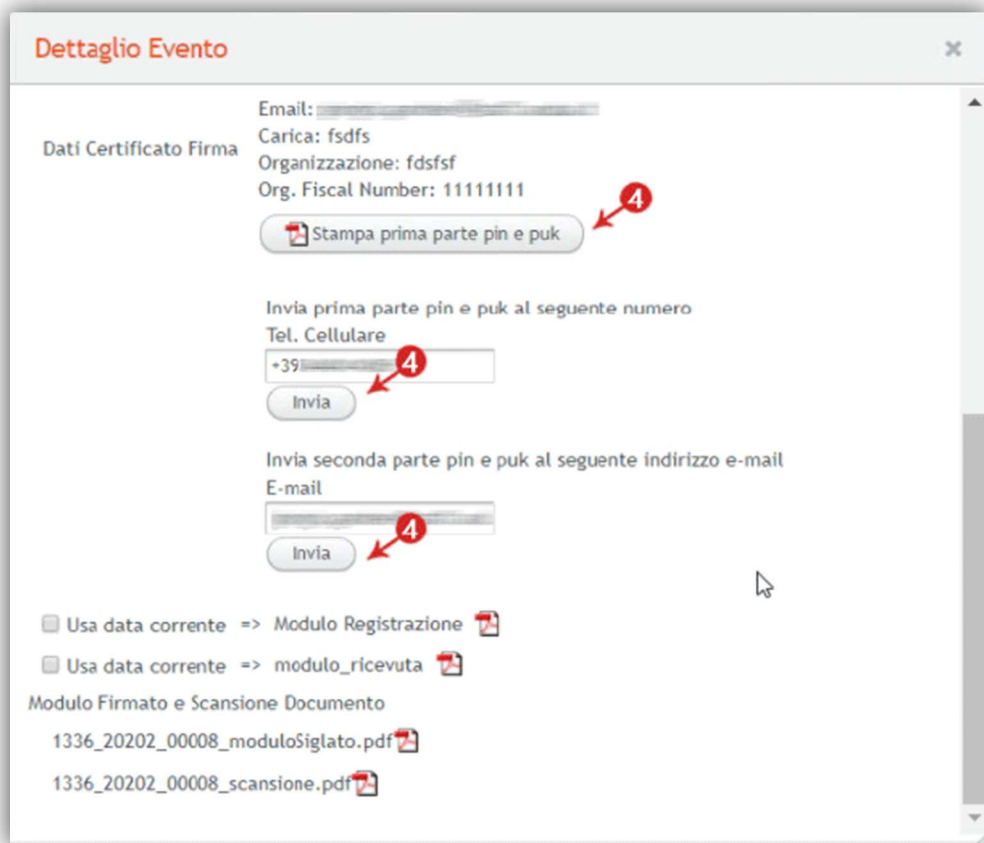


3. Cliccare sull'icona lente di ingrandimento in corrispondenza della riga denominata **"Richiesta certificato"**.



Tipo Evento	Profilo	Data Operazione	Stato	Tipo Certificato	canale	Sportello	CDRL	Operatore	Codice scratchcard	DVO	Dettaglio Event: 9
Emissione firma digitale	Firma Dig	2020-02-05 17:18:15.363	Completato	-	Sportello	TEST	- Sportello Principale	TEST	-	-	
Richiesta Certificati	Firma Dig	2020-02-05 17:16:59.132	Da Verificare	-	Sportello	TEST	- Sportello Principale	TEST	-	-	
Registrazione Titolare	-	2018-08-06 17:34:07.41	Completato	-	Sportello	-	-	-	-	-	

4. Selezionare nella finestra le operazioni di rinvio codici PIN e PUK.




Dettaglio Evento

Email: _____

Carica: fsdfs

Organizzazione: fsdfs

Org. Fiscal Number: 11111111

 Stampa prima parte pin e puk

Invia prima parte pin e puk al seguente numero

Tel. Cellulare


+39: _____


Invia

Invia seconda parte pin e puk al seguente indirizzo e-mail


E-mail


Invia

Usa data corrente => Modulo Registrazione 

Usa data corrente => modulo_ricevuta 

Modulo Firmato e Scansione Documento

1336_20202_00008_moduloSiglato.pdf 

1336_20202_00008_scansione.pdf 

Tale procedura è disponibile se e solo se la pratica di rilascio del certificato di firma è in stato emesso.

Qualora il titolare abbia modificato il PIN originario, dovrà allora utilizzare il PUK per resettarlo e nuovamente impostarlo utilizzando l'apposita funzionalità presente sulla toolbar della ArubaKey:



e quindi "Sblocco PIN":



Tale procedura non potrà invece essere eseguita nel caso in cui il Titolare abbia modificato (e successivamente smarrito) anche il codice PUK. In tal caso, dovrà essere emesso un nuovo certificato di firma e il precedente certificato dovrà essere revocato.