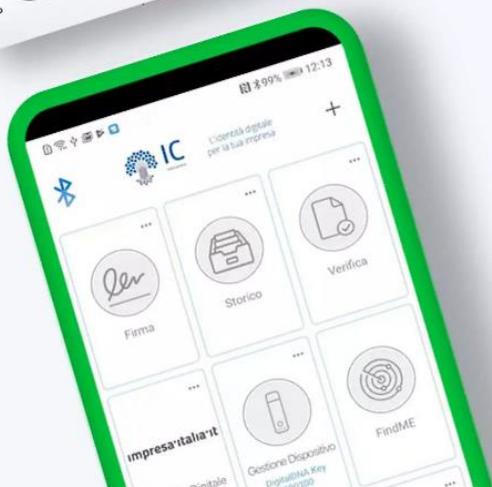


ID InfoCamere

DigitalDNA IC

Manuale Utente

Versione 9 del 02/04/2024



SOMMARIO

1	INTRODUZIONE	6
2	REQUISITI HARDWARE E SOFTWARE	6
2.1	Hardware - DigitalDNA Key	6
2.2	Software - Requisiti di sistema	7
3	AVVIO	8
3.1	Attivazione	8
3.1.1	Acquisto online: emissione certificati	9
3.1.2	Requisiti per l'attivazione del token Digital DNA	9
3.1.3	Procedura di attivazione del token Digital DNA da APP	10
4	ASSOCIAZIONE DI UNA DIGITALDNA KEY	15
4.1	Ricerca	15
4.2	Abbinamento	16
5	FUNZIONI DELL'APP DIGITALDNA IC	17
5.1	Firma Digitale	19
5.1.1	Preparazione della firma	19
5.1.2	Firma con DigitalDNA Key	23
5.1.3	Firma con certificato di firma remota	24
5.1.4	Firma di più documenti	25
5.1.5	Azioni successive	28
5.2	Verifica	29
5.3	Servizi web	31
5.4	Storico	34
5.5	Marca Temporale	35
5.6	FindME	37
5.7	Configura DigitalDNA Key	39
5.7.1	Certificati	40
5.7.2	Cambia PIN	41

5.7.3	Sblocca PIN	41
5.7.4	Configura.....	42
5.7.5	Rimuovi Associazione.....	46
5.8	Ultima Posizione Rilevata	46
5.9	Widget personalizzato.....	47
5.10	Impostazioni	47
5.10.1	Impostazioni di Firma digitale	48
5.10.2	Impostazioni di Marca temporale	54
5.10.3	Impostazioni della Home.....	60
5.10.4	Impostazioni account SPID INFOCAMERE	60
5.10.5	Impostazioni del FindME	65
5.10.6	Impostazioni dello Storico	66
5.10.7	Strumenti per il miglioramento dei servizi	66
5.10.8	Privacy Policy InfoCamere.....	66
5.11	Supporto.....	67
6	CONSIGLI D'UTILIZZO.....	68

Versioni del documento

Versione corrente

Versione:	9	Data Versione:	02/04/2024
Descr. modifiche:	Introduzione funzionalità SPID: associazione di Identità Digitale SPID InfoCamere all'app e attivazione della credenziale di secondo livello con generazione di codice OTP via app		
Motivazioni :			

Novità introdotte rispetto alla precedente emissione

Versione:	8	Data Versione:	22/06/2023
Descr. modifiche:	Aggiornamento versione minima Android richiesta; revisione documento		
Motivazioni :			

Versione:	7	Data Versione:	09/03/2023
Descr. modifiche:	Aggiunto § 5.1.4 Firma di più documenti		
Motivazioni :	Rilascio funzionalità di firma di più documenti contemporaneamente		

Versione:	6	Data Versione:	11 / 10 / 2022
Descr. modifiche:	Aggiunto § 3.1 Attivazione dispositivo		
Motivazioni :	Rilascio funzione di attivazione del dispositivo Token Digital DNA, acquistato online su id.infocamere.it		

Versione:	5	Data Versione:	14 / 04 / 2022
Descr. modifiche:	<p>Aggiunta § 5.1.3 Firma con certificati di Firma remota;</p> <p>Aggiunti § 5.10.6 Strumenti per il miglioramento dei servizi e §5.10.7 Privacy Policy InfoCamere</p> <p>Modifica §5.10.1 Configurazione Firma remota</p> <p>Rivisitazione completa del documento.</p> <p>Modifica §5.11 Supporto</p>		
Motivazioni :	Rilascio funzione di anteprima dei documenti verificati, Modifica al Self Care di Firma Remota, Inserimento nuove modalità di supporto.		



1 INTRODUZIONE

Gentile Utente, grazie per aver scelto DigitalDNA IC.

Il presente documento rappresenta una guida completa delle funzioni di uso e delle caratteristiche principali dell'app che ti permetterà di utilizzare il tuo ID Token Digital DNA (di seguito anche Digital DNA Key), la tua Firma Remota e la tua Identità Digitale SPID InfoCamere con dispositivi mobili, sia smartphone che tablet, siano essi Android o iOS o Huawei.

Tramite l'app descritta in questo manuale, potrai utilizzare il tuo dispositivo ID Token Digital DNA per accedere a servizi online e firmare documenti digitali a validità legale, nonché configurare ed utilizzare le tue credenziali di Firma Remota InfoCamere e dell'Identità Digitale SPID e infine apporre marche temporali.

2 REQUISITI HARDWARE E SOFTWARE

2.1 Hardware - DigitalDNA Key

La DigitalDNA Key (Figura 1), abbinata all'app DigitalDNA, permette di utilizzare la propria identità digitale sia su dispositivi mobili (smartphone e tablet) sia in ambienti desktop per firmare digitalmente a validità legale o accedere a servizi online.

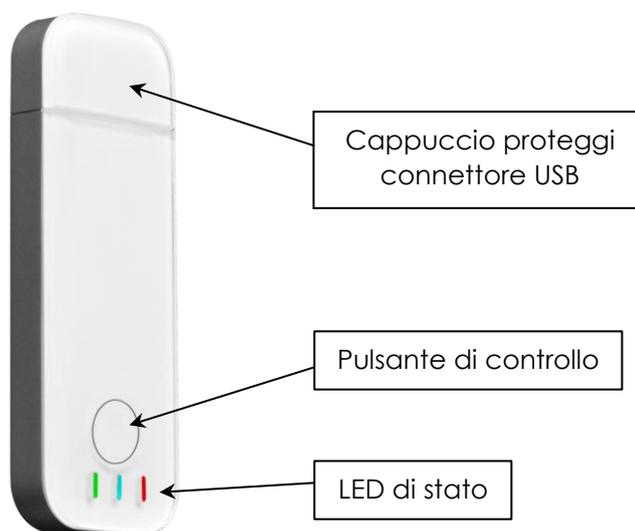


Figura 1

L'interfaccia machine-to-user della DigitalDNA Key presenta le seguenti caratteristiche:

- **Pulsante di controllo:** pulsante unico per il controllo di tutte le modalità di funzionamento;

- **Interruttore alimentazione:** al pari di altri accessori Bluetooth alimentati a batteria, il dispositivo presenta un interruttore per l'alimentazione dello stesso;
- **LED:** i piccoli LED nei tre colori primari principali segnalano all'utente importanti informazioni, che saranno dettagliate successivamente.

Il pulsante di controllo del dispositivo consente all'utente di accedere alle seguenti funzionalità:

- **ACCENSIONE:** a dispositivo spento, una pressione di circa mezzo secondo del pulsante di controllo provoca l'accensione del dispositivo, il quale entra in modalità di "pronto alla connessione" per accettare connessioni dai dispositivi precedentemente abbinati; tale modalità operativa è indicata da un doppio lampeggio rapido del LED blu, che si verifica ogni 3 secondi;
- **SPEGNIMENTO:** a dispositivo acceso, una pressione tra mezzo secondo e fino a 2 secondi del pulsante di controllo provoca lo spegnimento del dispositivo; tale modalità operativa è indicata dallo spegnimento del LED blu e il contestuale breve lampeggio del LED rosso;
- **BINDING o PAIRING:** a dispositivo acceso, una pressione superiore ai 3 secondi del pulsante di controllo provoca l'entrata in modalità di abbinamento del dispositivo; in questa modalità è possibile associare il Token ad un dispositivo mobile dotato di connessione Bluetooth Low-Energy. Tale modalità operativa è indicata da un lampeggio del LED blu con una frequenza di 120 millisecondi (ossia un lampeggio veloce e ininterrotto). La modalità di abbinamento è intuitiva, essendo comune a tutti gli accessori BLE, e faciliterà l'utente nel compiere questa operazione.

Requisiti HW: Bluetooth Low Energy 4.1 o superiori

2.2 Software - Requisiti di sistema

L'applicazione DigitalDNA IC è compatibile con i Sistemi mobile:

- Android 8.x e successivi
- iOS 10.x e successivi

3 AVVIO

All'avvio dell'app appare per alcuni secondi la schermata detta 'Launch Screen' con il logo InfoCamere. Subito dopo, l'utente visualizza la schermata principale dell'app detta 'Home' (Figura 3).

La prima volta che viene lanciata l'app, all'utente viene chiesta l'autorizzazione per utilizzare la sua posizione in modo da poter accedere alle funzionalità Bluetooth (Figura 2). Dopo aver espresso il consenso, così come previsto dal Regolamento GDPR sulla protezione dei dati personali, l'utente prosegue nella navigazione senza dover ripetere l'autorizzazione agli utilizzi successivi.



Figura 2

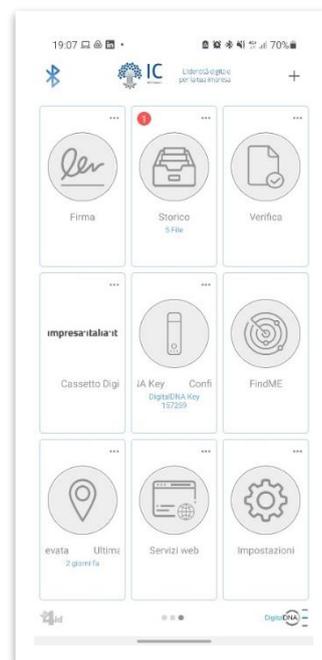


Figura 3

3.1 Attivazione

Il paragrafo è dedicato agli utenti che effettuano per la prima volta l'associazione dell'app al Token Digital DNA, richiesto tramite piattaforma id.infocamere.it e ricevuto a domicilio.

L'attivazione del dispositivo è una procedura obbligatoria e deve essere effettuata solo alla prima associazione, se il dispositivo non è stato mai attivato.

Tramite la procedura di invio del dispositivo inattivo e conseguente attivazione, il Titolare ha la certezza di essere l'utilizzatore esclusivo dei certificati, avendo accesso esclusivo ai relativi codici di attivazione, inviati telematicamente su contatto verificato.

L'attivazione del dispositivo di Firma Digitale e CNS, esclusivamente in formato ID Token Digital DNA, può essere eseguito da smartphone o tablet.

La procedura di attivazione è un'attività propedeutica all'utilizzo dei certificati sul dispositivo.

3.1.1 Acquisto online: emissione certificati

A seguito dell'emissione dei certificati CNS e Firma Digitale, vengono inviate due e-mail sull'indirizzo di posta elettronica del titolare: un'e-mail con le istruzioni per procedere all'attivazione del dispositivo ed una con i segreti, con oggetto **Nuova richiesta CNS: riferimenti per l'uso**.

All'interno del testo e-mail, cliccando su **Vai al PDF**, si accede alle credenziali per l'attivazione e l'utilizzo del dispositivo. L'accesso al contenuto è protetto dalla pass-phrase scelta in fase di richiesta.

Le informazioni contenute nel pdf cifrato sono le seguenti (Figura 4):

- **SERIALE DISPOSITIVO** nel formato numerico, che identifica il dispositivo fisico in cui sono contenuti i certificati;
- **ID SCRATCH-CARD** necessario per la gestione del ciclo di vita dei certificati, secondo le indicazioni riportate sul portale id.infocamere.it;
- **PUK** codice segreto necessario per l'attivazione del dispositivo;
- **CODICE DI EMERGENZA** necessario per la gestione del ciclo di vita del certificato, secondo le indicazioni riportate sul portale id.infocamere.it.



Figura 4

3.1.2 Requisiti per l'attivazione del Token Digital DNA

Per procedere all'attivazione del Token Digital DNA è necessario avere a disposizione:

- **Dispositivo da attivare** ricevuto a domicilio;
- PDF con i **segreti** (Figura 4);
- **Smartphone/Tablet** connesso ad internet;
- App **DigitalDNA IC** installata sul dispositivo mobile.

3.1.3 Procedura di attivazione del Token Digital DNA da APP

Accendere il Token Digital DNA utilizzando il tasto laterale ON/OFF: quando il dispositivo è acceso i led inizieranno a lampeggiare.

Avviare l'applicazione sullo smartphone/tablet e prendere visione dell'informativa privacy.

Attivare il Bluetooth e la geolocalizzazione (almeno "Solo una volta") per consentire la ricerca del dispositivo da associare (Figura 5).



Figura 5

Se è presente un dispositivo acceso nei paraggi, viene mostrato il numero del dispositivo, selezionarlo e procedere cliccando su **Avanti** (Figura 6).



Figura 6

A questo punto, viene richiesto di eseguire l'associazione (Figura 7), tenendo premuto il pulsante di controllo del dispositivo (Figura 8).



Figura 7



Figura 8

Conclusa l'associazione tra dispositivo e app, quest'ultima verifica lo stato di attivazione del dispositivo (Figura 9).

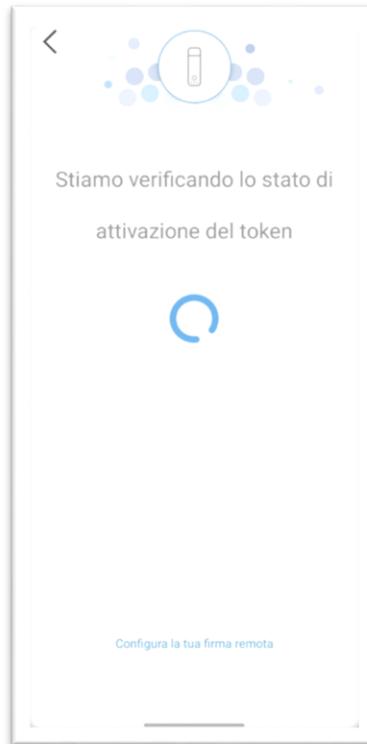


Figura 9

Se il dispositivo risulta ancora da attivare, è necessario procedere alla scelta del PIN.

L'attivazione, infatti, avviene inserendo il codice PUK ricevuto nel PDF cifrato via e-mail (Figura 4) e inserendo e confermando il PIN (Figura 10).



<

DigitalDNA Key 000447
8C39-5C27-C083

Per attivare il dispositivo inserisci i dati e clicca Attiva

PUK

Nuovo PIN

Conferma nuovo PIN

Il PIN/PUK deve contenere almeno 8 caratteri

Attiva

Figura 10



<

DigitalDNA Key 000447
8C39-5C27-C083

Per attivare il dispositivo inserisci i dati e clicca Attiva

PUK

Nuovo PIN

Conferma nuovo PIN

Attiva

Figura 11

Una volta inseriti i dati richiesti, bisogna cliccare su **Attiva** per concludere l'operazione (Figura 11).

Per procedere all'utilizzo del ID Token Digital DNA tramite app, è necessario inserire il PIN scelto o impostare il riconoscimento biometrico (Figura 12 e 13).

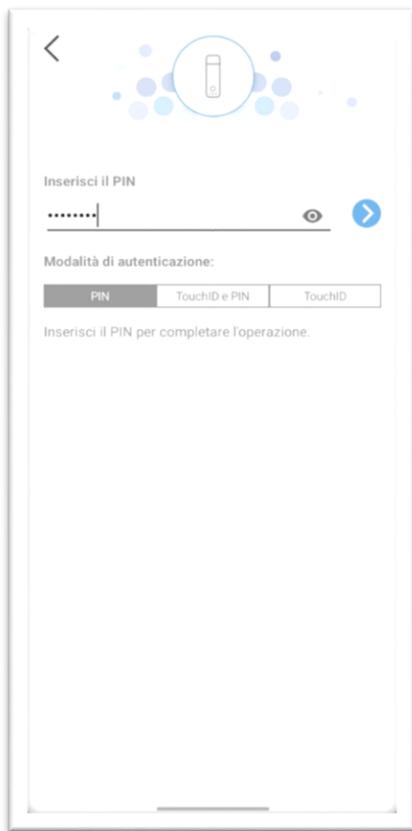


Figura 12



Figura 13

Il codice PIN e gli altri segreti devono essere conservati separatamente dal dispositivo di firma e non vanno comunicati a terzi.

4 ASSOCIAZIONE DI UNA DIGITALDNA KEY

Al primo avvio, se non risulta già associata una DigitalDNA Key o una firma remota, l'app mostra una procedura guidata per aiutare l'utente nell'associazione via Bluetooth. La stessa procedura è accessibile anche cliccando sul widget "Configura DigitalDNA Key" e, in caso di Android e Huawei, poi sulla voce "Associa dispositivo" o, in alternativa, cliccando sul simbolo del Bluetooth presente nella Home in alto a sinistra.

La procedura di associazione della DigitalDNA Key è costituita dai seguenti passaggi:

1. Ricerca
2. Abbinamento
3. Configurazione

Nel caso in cui venga rilevato un dispositivo da attivare in fase di Abbinamento, si rimanda al §3.1 per i successivi passaggi da effettuare.

4.1 Ricerca

Come primo step, la procedura richiede all'utente di accendere la propria DigitalDNA Key (Figura 14). Rilevata l'accensione della DigitalDNA Key, l'applicazione visualizza l'elenco di tutti i Token rilevati nel raggio di copertura del segnale Bluetooth (Figura 15); l'utente deve selezionare il proprio Token (il codice identificativo del dispositivo è visibile sul retro della chiavetta USB) per poter avanzare nella procedura di associazione e configurazione della DigitalDNA Key.

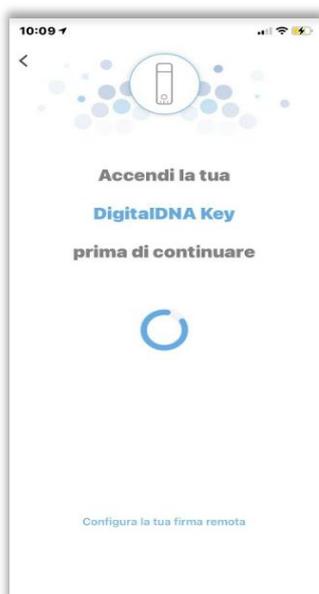


Figura 14

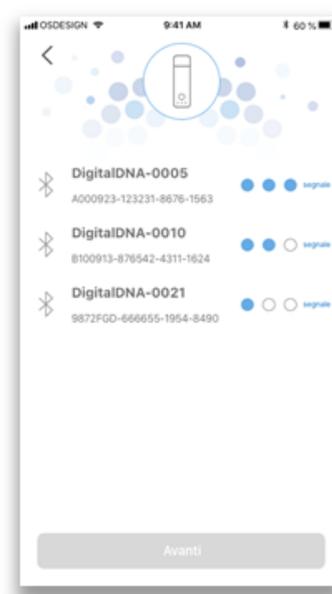


Figura 15

4.2 Abbinamento

Per effettuare l'abbinamento tra il dispositivo mobile (smartphone o tablet) e la DigitalDNA Key che si intende utilizzare è necessario selezionarla dall'elenco (Figura 16) tenere premuto il pulsante di "Controllo" per circa 3 secondi come suggerito dall'app (Figura 17) e poi inserire il PIN della DigitalDNA Key (Figura 18).

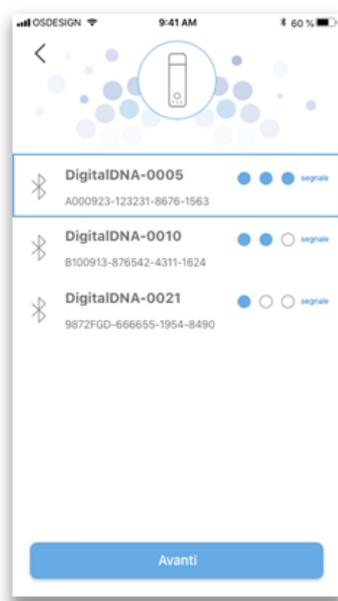


Figura 16



Figura 17

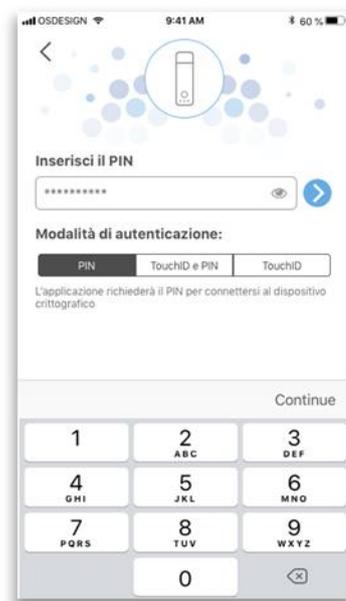


Figura 18

In questa fase è possibile impostare il metodo di autenticazione (PIN, TouchID/FaceID, PIN+TouchID/FaceID) alla DigitalDNA Key. L'accesso e l'utilizzo di alcuni elementi crittografici presenti sul dispositivo DigitalDNA Key, tipicamente le chiavi private correlate ai certificati, sono protetti e richiedono l'inserimento di un codice PIN, come del resto previsto dallo standard ISO 7816.

Al fine di rendere l'esperienza utente quanto più semplice e intuitiva, ma al contempo garantire elevati standard di sicurezza, è possibile, per i dispositivi mobili dotati di lettore biometrico di impronte digitali, utilizzare i dati biometrici dell'utente come elementi di autenticazione. Qualora lo smartphone/tablet in uso disponga della funzione di riconoscimento del volto (FaceID), questa può essere utilizzata in alternativa all'utilizzo dell'impronta digitale.

Nella schermata di autenticazione (Figura 18), infatti, è possibile scegliere quale un metodo utilizzare per accedere alle funzioni l'app DigitalDNA (in base alle tecnologie disponibili sul dispositivo in uso):

- **PIN:** prevede unicamente l'inserimento del PIN;
- **TouchID/FaceID e PIN:** prevede l'inserimento del PIN unitamente alla lettura dell'impronta digitale o al riconoscimento facciale;
- **TouchID/FaceID:** prevede unicamente la lettura dell'impronta digitale o il riconoscimento facciale, senza alcun inserimento del PIN.

5 FUNZIONI DELL'APP DIGITALDNA IC

Dalla schermata Home è possibile accedere a tutte le funzioni dell'app DigitalDNA IC, selezionandole attraverso i seguenti widget (Figura 19):

- Firma
- Storico
- Verifica
- Cassetto Digitale dell'Imprenditore
- Configura DigitalDNA Key
- FindME
- Ultima posizione rilevata
- Servizi web
- Impostazioni
- Supporto
- Applica Marca Temporale
- Telemaco
- Fattura Elettronica
- Impresainungiorno
- Diritto annuale
- Atti depositati
- Scuola lavoro
- INPS
- Agenzia delle Entrate
- Agenzia delle Entrate Riscossione
- Privacy Policy
- Genera OTP Firma Remota
- Gestione OTP (SPID)



Figura 19

Se l'utente non ha ancora associato una DigitalDNA Key o un account di firma remota, attraverso i widget viene automaticamente guidato nella procedura di associazione. Ad esempio, cliccando sul widget "Firma" l'utente può scegliere se associare un dispositivo DigitalDNA Key oppure un account di firma remota (Figura 20); cliccando su "Marca temporale" viene guidato alla configurazione di un servizio di marcatura temporale (Figura 21); cliccando sulle funzioni "Ultima posizione" e "FindME" viene riportato all'associazione di una DigitalDNA Key (Figura 14).

Una volta selezionata la modalità con la quale proseguire, l'utente procede con l'associazione di una DigitalDNA Key (capitolo 4) oppure con la configurazione di una firma remota (paragrafo 5.10.1) o di una marca temporale (paragrafo 5.10.2) all'interno delle "Impostazioni".



Figura 20



Figura 21



Figura 22

È possibile organizzare la schermata principale dell'app secondo le proprie preferenze "trascinando" i widget nella posizione desiderata (Figura 23). I widget configurati di default non sono eliminabili, ma è possibile aggiungerne altri (widget statistici – vedi §5.9). Se ci sono notifiche relative a una determinata funzione dell'app, potrebbe apparire un bollino rosso (badge) nell'angolo in alto a sinistra del widget. Il bollino rosso scompare dopo aver visualizzato la notifica.

Nei paragrafi che seguono verranno illustrate in maniera più approfondita le funzionalità associate ai singoli widget.

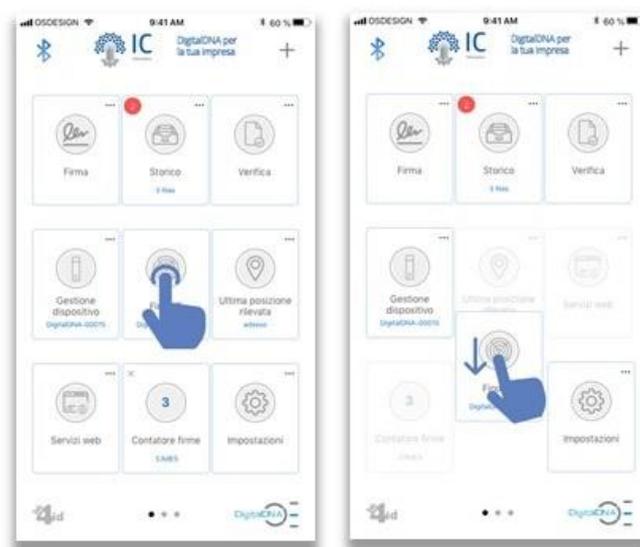


Figura 23

5.1 Firma Digitale

Cliccando sul widget "Firma" nella schermata Home, appare l'elenco delle cartelle e dei document provider disponibili (es. iCloud, Dropbox, Google Drive etc.) da cui selezionare il file o i file da firmare. Selezionata la sorgente desiderata e in seguito il file da firmare, viene avviato il processo di firma digitale del documento.

5.1.1 Preparazione della firma

Una prima schermata consente di selezionare il tipo di firma da apporre, prevedendo la scelta tra i formati CADES, XAdES e PAdES (Figura 24). Il formato CADES può essere applicato a tutte le tipologie di file (word, excel, immagine, ecc) e aggiunge al documento elettronico l'estensione p7m, che può essere visualizzato solo tramite software di verifica. Il formato XAdES è un formato di firma applicabile a file xml, che non ne altera l'estensione.

Il formato PAdES è disponibile solo per i file in formato PDF. Selezionando il formato di firma PAdES, è possibile abilitare anche la funzione di firma grafica PDF (checkbox "Abilita firma grafica"). Per annullare l'operazione e tornare alla Home cliccare sul pulsante "<" in alto a sinistra, altrimenti proseguire inserendo le altre impostazioni.

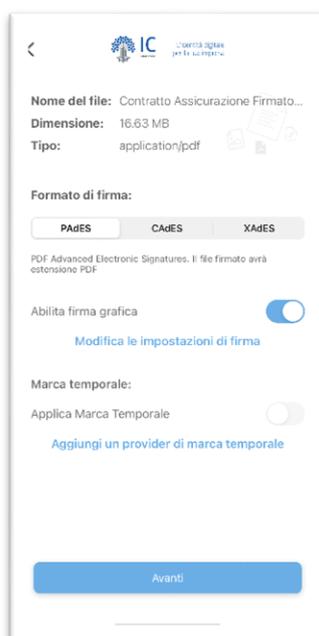


Figura 24

Dopo aver selezionato il formato di firma desiderato e aver eventualmente abilitato la funzione di firma grafica PDF disponibile nel formato PAdES, l'utente ha la possibilità di inserire altri parametri, cliccando su "Modifica le impostazioni di firma".

Le impostazioni di firma configurabili sono le seguenti:

- a) Servizio di storage
- b) Immagine
- c) Motivo
- d) Luogo
- e) Data

a) Servizio di storage

Alla voce “Servizio di storage” è possibile scegliere di salvare il file firmato, oltre che all’interno dell’app, anche su un servizio di storage remoto selezionabile tra iCloud (iOS), Dropbox e Google Drive. L’accesso al servizio di storage remoto necessita l’inserimento di credenziali di accesso che dovranno essere fornite all’app mediante un’apposita interfaccia grafica. L’app crea sul servizio di storage remoto una cartella denominata DigitalDNA in cui verranno salvati i file firmati.

b) Immagine

In questa sezione si gestisce la creazione/uso di un grafo di firma/iniziali e/o immagine utente per la firma grafica PDF. È possibile creare un grafo di firma o un grafo delle iniziali durante la procedura di firma o in un secondo momento andando nelle “Impostazioni” dalla schermata Home (Figura 18)

Il tasto “Immagine” permette di accedere alla schermata illustrata in Figura 25, dalla quale è possibile acquisire un grafo di firma/sigla da inserire all’interno dell’area di firma. Acquisito il grafo di firma/grafico delle iniziali da utilizzare, questo andrà a sostituire la dicitura “Aggiungi un grafo di firma”. Le prime due opzioni fornite dalla selezione in Figura 25 consentono di aprire un editor nel quale è possibile creare il grafo della propria firma (Figura 26) o il grafo delle proprie iniziali (Figura 27).



Figura 25



Figura 26



Figura 27

Qualora non si voglia utilizzare né il grafo di firma né il grafo di sigla, è possibile acquisire un'immagine dalla gallery di Sistema o attraverso la fotocamera del dispositivo (smartphone/tablet). Questa immagine viene utilizzata come immagine standard per la firma grafica dei file PDF quando non sono stati acquisiti né il grafo di firma né il grafo della sigla.

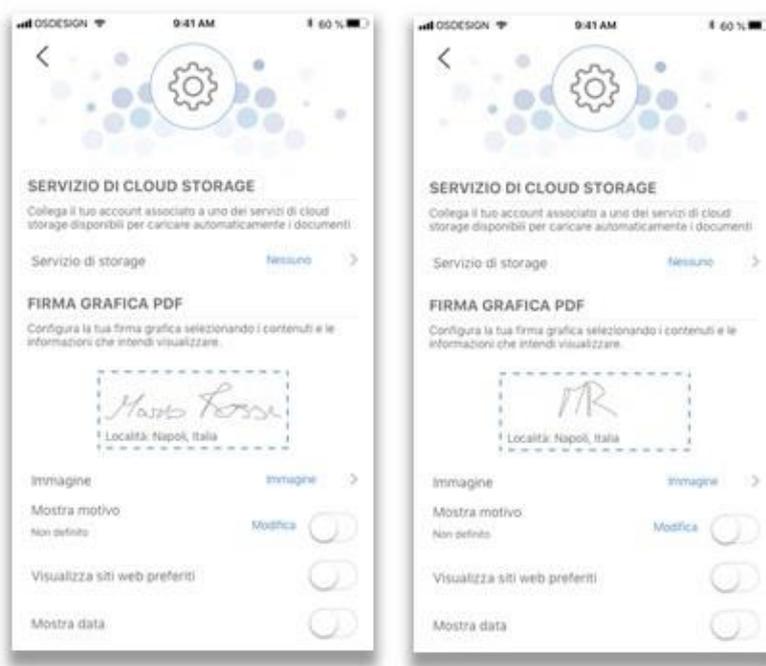


Figura 28

All'interno delle impostazioni della firma grafica è inoltre possibile aggiungere degli elementi alla firma (Figura 28), quali:

a) Motivo

Lo switch alla destra della dicitura "Mostra motivo" permette di attivare/disattivare l'inserimento nella firma grafica di un motivo per cui si realizza la firma, che l'utente può andare a digitare cliccando su "Modifica".

b) Luogo

Lo switch alla destra della dicitura "Mostra luogo" permette di attivare/disattivare l'inserimento nella firma grafica dei dettagli per la localizzazione geografica del dispositivo al momento della firma.

c) Data

Lo switch alla destra della dicitura "Mostra data" permette di attivare/disattivare l'inserimento nella firma grafica della data in cui si realizza la firma.

Oltre a modificare le impostazioni di firma, l'utente può anche scegliere se applicare al file una Marca Temporale contestualmente all'operazione di firma digitale. Attivando la voce corrispondente, viene richiesta la selezione del provider da utilizzare per la marca temporale (Figura 29).

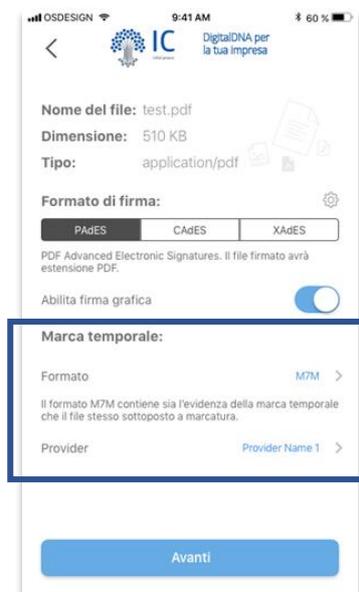


Figura 29

Anteprima del file

Il tasto "Avanti" porta all'anteprima del file da firmare (Figura 30). In questa fase è possibile visionare il documento e posizionare, eventualmente, la firma grafica selezionata. Di seguito viene riportata una possibile schermata con grafo di firma. Una volta impostate tutte le preferenze, è possibile procedere con la firma digitale premendo sul tasto "Firma" che si trova sotto l'anteprima del documento.

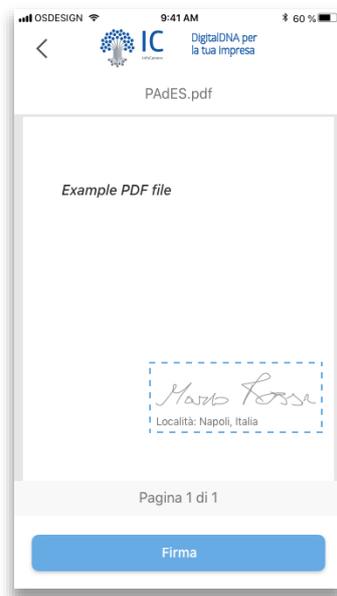


Figura 30

5.1.2 Firma con DigitalDNA Key

Una volta terminata la preparazione del documento da firmare, all'utente viene chiesto di inserire il PIN (o la modalità di autenticazione alternativa scelta) della propria DigitalDNA Key per applicare la firma digitale (Figura 31). Attendere il completamento dell'operazione, fino a quando sarà mostrata la schermata di conferma di firma avvenuta (Figura 32).



Figura 31

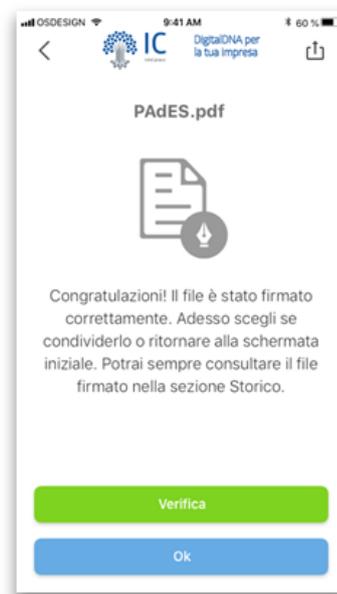


Figura 32

5.1.3 Firma con certificato di firma remota

In alternativa alla sottoscrizione tramite DigitalDNA Key mostrata nel paragrafo precedente e in Figura 31, è possibile firmare digitalmente il documento anche con un certificato di firma remota, precedentemente configurata (secondo la procedura disponibile al 5.10.1.2).

Una volta terminata la preparazione del documento e aver premuto "Firma" nella schermata di anteprima (Figura 30), nel caso in cui l'app non dovesse riconoscere alcun dispositivo DigitalDNA Key attivo nelle vicinanze, presenterà una schermata per chiedere all'utente con quale metodo intende procedere (Figura 33). Quindi, per firmare il documento con un certificato di firma remota, cliccare su "Utilizza la firma remota".

A seguire, in base a quanto previsto dal dispositivo smartphone/tablet in uso, l'app richiede l'inserimento del PIN di sblocco, l'impronta digitale o il riconoscimento facciale (Figura 34).



Figura 33



Figura 34

A questo punto, l'app ricava automaticamente il codice OTP (One Time Password) con cui completare la procedura di firma. Attendere il completamento dell'operazione, fino a quando sarà mostrata la schermata di conferma di firma avvenuta (Figura 32).

5.1.4 Firma di più documenti

Dopo aver associato la DigitalDNA Key o la Firma Remota, cliccare sul widget **Firma** (Figura 35) e selezionare la cartella di Sistema da cui verranno prelevati i file da firmare. Selezionare i file da firmare (Figura 36) e cliccare su **Apri**.



Figura 35

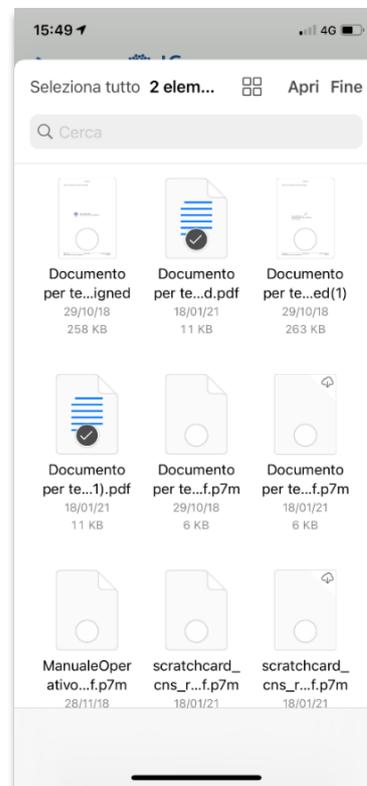


Figura 36

L'applicazione mostra l'elenco dei file da firmare e il formato di firma (PAdES, CAdES, XAdES).

Cliccando su **Firma** (Figura 37), verrà richiesto il PIN della Digital DNA Key (§5.1.2) – o in caso di Firma Remota (§5.1.3) l'autenticazione tramite codice di sblocco del dispositivo – (Figura 38).



Figura 37



Figura 38

Avviando il processo di firma dei documenti, l'applicazione mostra lo stato d'avanzamento dell'operazione (Figura 39), al termine della quale è possibile o condividere i file firmati – clic su **Condividi tutti** – o uscire dalla schermata – clic su **Fine** (Figura 40).

È possibile condividere anche un singolo documento accedendo al menu laterale (...) in corrispondenza del singolo file firmato.

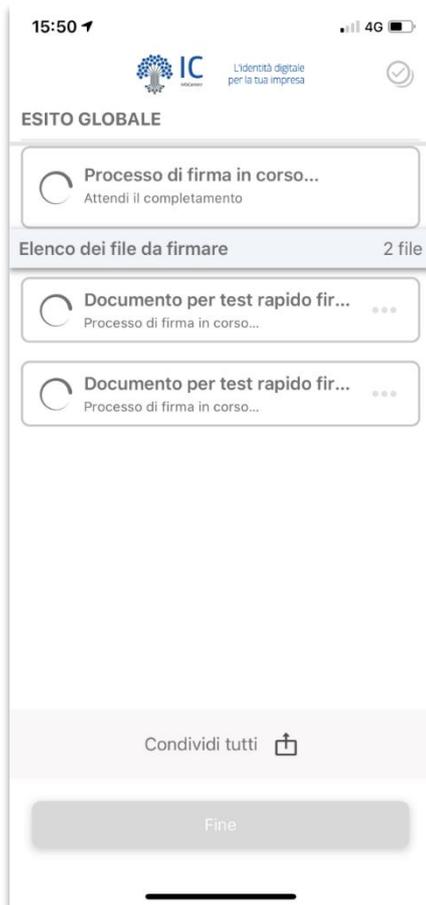


Figura 39

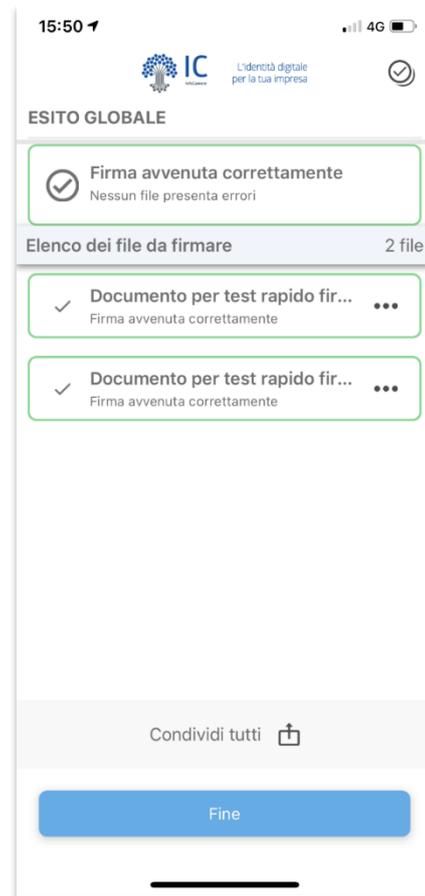


Figura 40

I documenti firmati saranno disponibili nella sezione **Storico** dell'app.

5.1.5 Azioni successive

Dopo aver firmato un documento, sia con la DigitalDNA Key sia con un certificato di firma remota, è possibile avviare la procedura di verifica cliccando sul tasto "Verifica" (Figura 32) e visualizzare così tutti i dettagli della firma digitale apposta al file. È inoltre possibile condividere il documento firmato in due modalità:

1. Cliccando sull'icona di condivisione in alto a destra subito dopo aver completato l'operazione di firma (Figura 32);
2. Selezionando il file firmato dallo "Storico" (Figura 19), accessibile dalla schermata Home.

Nel caso di firma di più documenti, la funzionalità di verifica del singolo documento è disponibile utilizzando i tre puntini in corrispondenza del singolo file firmato (Figura 40).

5.2 Verifica

La funzione di verifica permette di controllare la validità delle firme e delle marche temporali apposte ai file e di accedere al contenuto del file firmato (se il formato del file è supportato dal dispositivo).

Cliccando sul widget "Verifica" dalla schermata Home appare l'elenco delle cartelle e dei documenti provider (es. iCloud, Dropbox, Google Drive etc.) da cui selezionare il file da verificare. Selezionato il file, viene avviato il processo di verifica del documento.

Al termine del processo di verifica di un file l'app mostrerà una schermata con l'elenco delle buste crittografiche contenute nel file sottoposto a verifica (Figura 41). Per ciascuna busta crittografica sarà riportato il livello di annidamento, il nome del file e la sintesi dello stato delle firme e delle marche temporali in essa contenute. L'annidamento multiplo delle buste crittografiche sarà presente nel caso di marche temporali e quindi di file con estensione .m7m, .tsr, .tst e .tsd o nel caso di firme matrioska e quindi di file con estensione .p7m e .xml.

Cliccando sulla voce "Firme" l'utente visualizzerà una schermata riportante l'elenco delle marche temporali e delle firme singole e multiple contenute nella busta crittografica corrispondente (Figura 42).

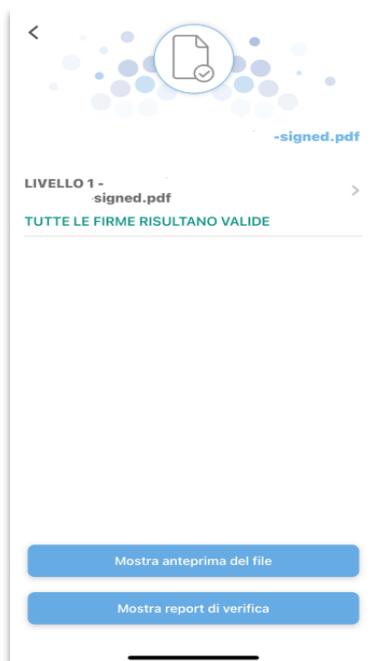


Figura 41

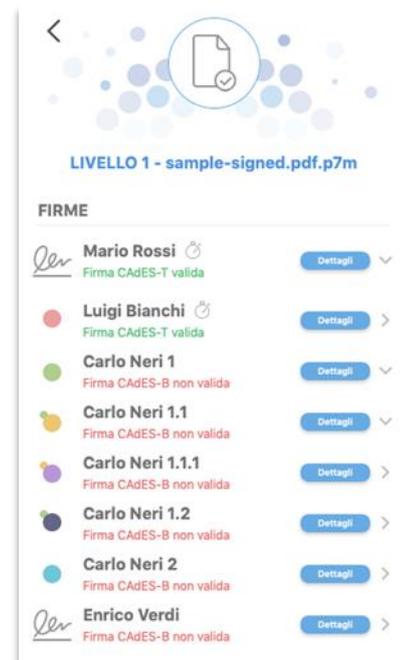


Figura 42

L'elenco delle firme e/o delle marche temporali è caratterizzato dai seguenti elementi distintivi:

- Le firme sono indicate dal simbolo di una firma;
- Le firme parallele sono indicate da un cerchio colorato;
- Le controfirme sono indicate da un cerchio colorato di misura inferiore;
- Le firme a cui è stata associata una marca temporale sono indicate dal simbolo a forma di orologio;
- In caso di esito positivo della verifica il testo è di colore verde, in caso di esito negativo è di colore rosso;
- Il pulsante "Dettagli" dà accesso alle informazioni di verifica;
- La freccetta verso destra o verso il basso indica lo stato di espansione/collisione dell'elemento a cui si riferisce.

Selezionata una firma o una marca temporale, l'utente accede a una schermata riepilogativa che riporta le informazioni di verifica dell'elemento selezionato (Figura 43). Dalla schermata riepilogativa l'utente può accedere alle informazioni di dettaglio del certificato (Figura 44) e, nel caso di firma digitale di tipo XAdES-T, CADES-T o PAdES-T, alle informazioni relative all'esito della verifica della marca temporale correlata (Figura 45).



Figura 43



Figura 44

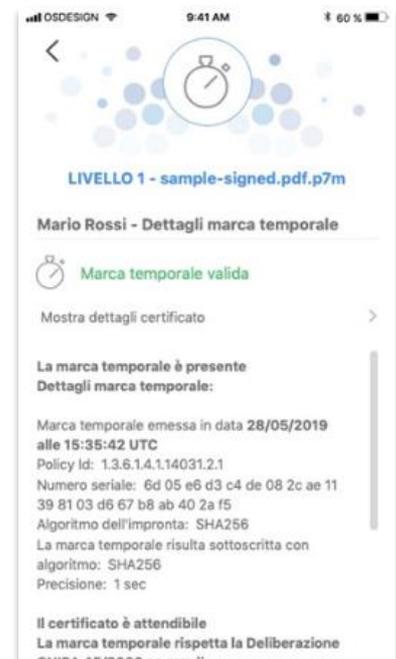
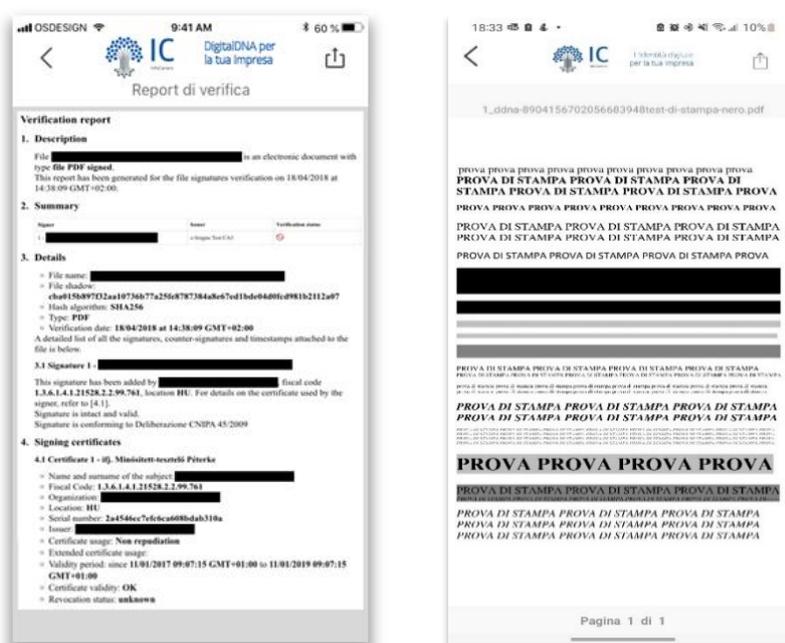


Figura 45

Nella schermata di verifica mostrata in Figura 41, cliccando sul pulsante “Mostra report di verifica”, l’utente può generare e visualizzare il report PDF contenente l’esito della verifica del file selezionato, mentre cliccando sul pulsante ‘Mostra anteprima del file’ l’utente può visualizzare il contenuto del file verificato (Figura 46). È possibile, in entrambi i casi, condividere i file cliccando sul pulsante “Condividi”. Cliccando sul pulsante “<” in alto a sinistra, l’utente torna alla schermata precedente.



(report di verifica)

(anteprima file firmato)

Figura 46

5.3 Servizi web

Dalla Home è possibile accedere ai servizi web di maggiore interesse per l’utente utilizzando il widget denominato “Servizi web”. Questa sezione dell’app è costituita da un browser. All’apertura il browser presenta una homepage in cui sono elencati i servizi web (Figura 47).

Nella barra degli indirizzi URL è possibile inserire manualmente una URL o l’oggetto di una ricerca che verrà effettuata attraverso il motore di ricerca Google. Nella parte inferiore della schermata “Servizi web” è presente una toolbar con diversi comandi:

- Freccia verso sinistra – Vai alla pagina web precedente
- Freccia verso destra – Vai alla pagina web successiva
- Rettangolo con freccia verso l’alto – Condividi link
- Cuore – Aggiungi ai preferiti

- Rettangoli sovrapposti – Attiva funzione multi-tab

Per aggiungere un sito tra i preferiti, è possibile cliccare sull'icona a forma di cuore. L'ultimo pulsante della toolbar (rettangoli sovrapposti in Figura 47) consente di accedere alla seconda schermata dell'app, ossia alla schermata di gestione delle sessioni di lavoro parallele *multi-tab* (Figura 48). In questa schermata l'utente può aggiungere nuove sessioni, cancellare una o più sessioni o accedere ad una sessione di lavoro.



Figura 47



Figura 48

Il Secure Browser dell'app DigitalDNA IC, inoltre, abilita web application di terze parti alla fruizione delle funzioni di firma digitale, verifica di file e apposizione di marche temporali in modalità online.

Il widget "Servizi web" permette, inoltre, la generazione del codice OTP per l'accesso con credenziali di secondo livello SPID dalla pagina di navigazione.

Per l'Identità Digitale SPID associata precedentemente all'app (vedi §5.10.4) è possibile accedere al servizio e generare l'OTP via app, previo inserimento delle credenziali username e password, cliccando sull'icona SPID in alto a destra (Figura 49). L'OTP viene generato a seguito di inserimento del PIN del dispositivo mobile o riconoscimento biometrico. Per concludere l'operazione di autenticazione è possibile copiare l'OTP negli appunti e incollarlo nel campo OTP (Figura 49).

L'OTP ha una durata di 60 secondi, dopo i quali sarà necessario generare un nuovo codice temporaneo.

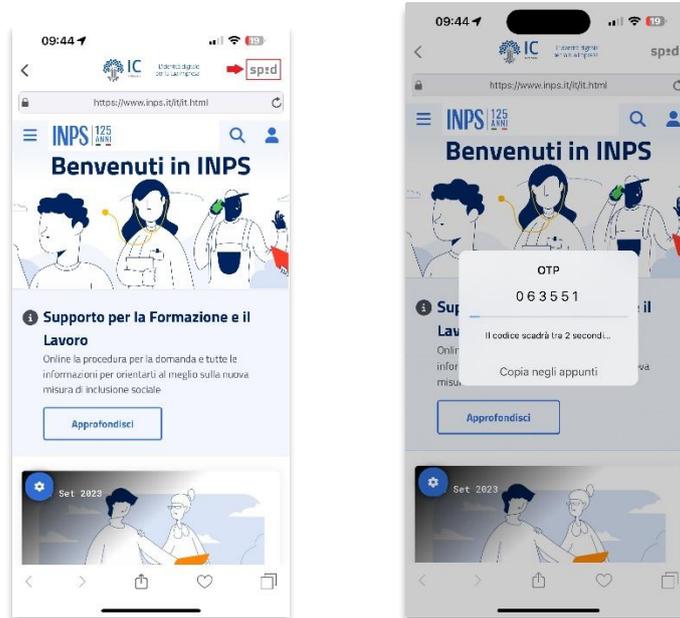


Figura 49

5.4 Storico

Cliccando sul widget “Storico” dalla schermata Home è possibile accedere alla cronologia delle attività svolte con l’app DigitalDNA IC. Nella sezione Storico sono elencati in ordine cronologico sia i file firmati digitalmente, sia le operazioni svolte con la DigitalDNA Key (es. Cambio PIN, accesso ad un servizio CNS ecc.).

Nella cartella **File** della sezione Storico si visualizza la lista dei file firmati digitalmente (Figura 50). L’utente può visualizzare l’anteprima, verificare, cancellare o condividere ciascun file attraverso i sistemi di condivisione offerti del sistema operativo in uso.

Nella cartella **Operazioni** della sezione Storico (Figura 51) si visualizza la lista delle operazioni di gestione e configurazione che hanno coinvolto la DigitalDNA Key, come le operazioni di cambio PIN, sblocco PIN o eventuali accessi richiesti da servizi online (es. accesso al portale INPS). L’utente può visualizzare le informazioni (es. la funzione di geo localizzazione dell’evento se i dati sono disponibili) o cancellare ciascuna operazione della lista. Cliccando su un elemento della lista l’app visualizza su mappa, quando possibile, la posizione dell’utente al momento dell’esecuzione dell’operazione o dell’inizio della transazione di autenticazione.



Figura 50



Figura 51

5.5 Marca Temporale

Cliccando sul widget “Applica Marca Temporale” dalla schermata Home (Figura 52) è possibile selezionare un file da marcare temporalmente scattando una nuova foto, scegliendolo dalla Galleria o ricercandolo tra i file resi disponibili dai file provider installati sul dispositivo mobile (Figura 53).



Figura 52



Figura 53

Selezionata la sorgente desiderata e in seguito il file da marcare, viene avviato il processo di marca temporale. Una prima schermata consente di selezionare il tipo di marca da apporre e il provider da utilizzare (Figura 54). Sono disponibili i seguenti formati di marca temporale: M7M standard mime multipart, TSD Time Stamped Data, CAdES-T, XAdES-T, PAdES-T, TSR. Al termine della selezione, cliccare su “Avanti” e attendere il completamento della procedura (Figura 55). Al termine dell’operazione di marcatura, appare la schermata di conferma di avvenuta apposizione della marca temporale (Figura 56).

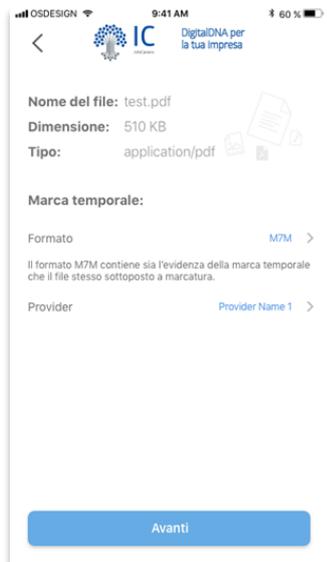


Figura 54

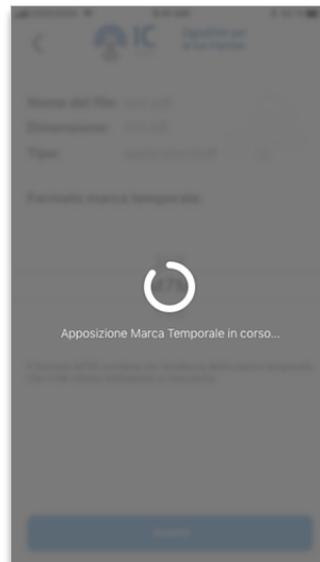


Figura 55

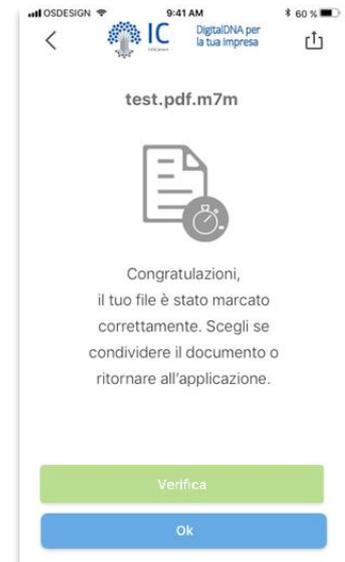


Figura 56

Cliccando su "Verifica" (Figura 56) è possibile avviare la procedura di verifica e visualizzare così tutti i dettagli delle firme/marche temporali apposte al file.

È possibile condividere il file marcato temporalmente in due modalità:

- Cliccando sull'icona di condivisione in alto a destra subito dopo aver completato l'operazione di marcatura (Figura 56);
- Selezionando il file marcato dallo "Storico" (Figura 50), accessibile dalla schermata Home.

I file marcati temporalmente vengono archiviati nello Storico e sono contrassegnati dal simbolo a forma di orologio. Selezionando il file dall'elenco è possibile visualizzare tutte le informazioni sulla marca temporale apposta.

L'app consente la condivisione di file direttamente da altre app (es. mail) per l'apposizione di marche temporali (Figura 57). Ricevuto il file da marcare temporalmente, si procede secondo le modalità di marcatura illustrata in Figura 54-55-56.



Figura 57

5.6 FindME

Dalla schermata Home è possibile attivare la funzione FindME con una pressione sull'omonimo widget (Figura 58). Tale interazione con l'app consente di inviare un segnale alla DigitalDNA Key che attiva il segnalatore acustico (buzzer) presente a bordo per consentire all'utente di localizzare il dispositivo in caso di smarrimento.

Per utilizzare la funzione FindME è necessario che la DigitalDNA Key smarrita sia accesa e nella portata del dispositivo mobile in uso. È possibile disattivare il segnalatore acustico sia dall'interfaccia dell'app sia dal tasto di controllo (tasto bianco) della DigitalDNA Key.

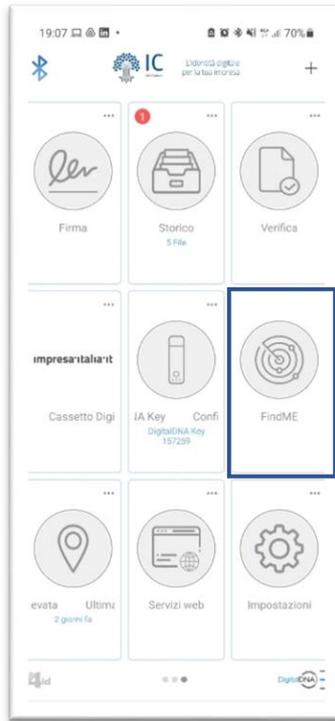


Figura 58

5.7 Configura DigitalDNA Key

Dopo aver associato una DigitalDNA Key, cliccando su “Configura DigitalDNA Key” nella schermata Home si accede al menu che permette di consultare, configurare e gestire le impostazioni della DigitalDNA Key in uso (Figura 59). Le voci presenti in questo menù sono:

- Visualizza certificati – Per la visualizzazione dei certificati
- Cambia PIN – Per cambiare il PIN
- Sblocca PIN – Per sbloccare il PIN
- Configura – Per accedere alle impostazioni del *Profilo Utente*
- Rimuovi associazione – Per rimuovere l'accoppiamento con la DigitalDNA Key

Quando all'app non si trova associata nessuna DigitalDNA Key, il menu presenta solo la voce “Associa dispositivo” (Android – Huawei) o, in caso di iOS, presenta la schermata di configurazione ID Token Digital DNA o Firma Remota.



Figura 59

5.7.1 Certificati

Selezionando la voce "Visualizza certificati" dal menu di "Configura DigitalDNA Key", si visualizzano i certificati contenuti nella DigitalDNA Key. I dettagli della DigitalDNA Key in uso sono riportati al centro della schermata (Figura 60). Selezionando un certificato nella lista dei certificati installati sul dispositivo è possibile visualizzarne ulteriori informazioni (Figura 61).

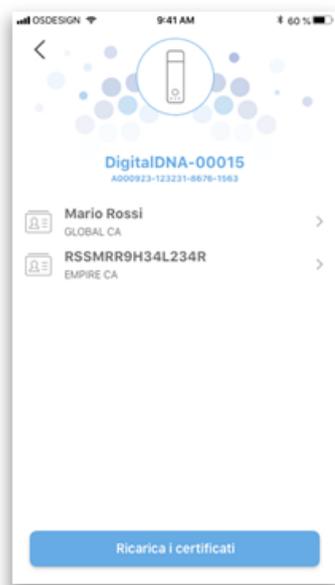


Figura 60



Figura 61

5.7.2 Cambia PIN

Selezionando la voce “Cambia PIN” dal menu di “Configura DigitalDNA Key”, è possibile sostituire il PIN in uso per la DigitalDNA Key con nuovo PIN.

Al centro della schermata sono riportati i dettagli della DigitalDNA Key associata. Per effettuare il cambio PIN è necessario inserire sia il vecchio PIN sia il nuovo PIN, confermandolo successivamente (Figura 62). È possibile controllare i dati inseriti cliccando sull'icona a destra dei campi di inserimento (pulsante a forma di occhio). Terminato l'inserimento di tutti i dati si compie l'operazione cliccando sul tasto “Cambia PIN”. Alla fine del processo di cambio PIN viene visualizzata una schermata di conferma di avvenuta sostituzione.

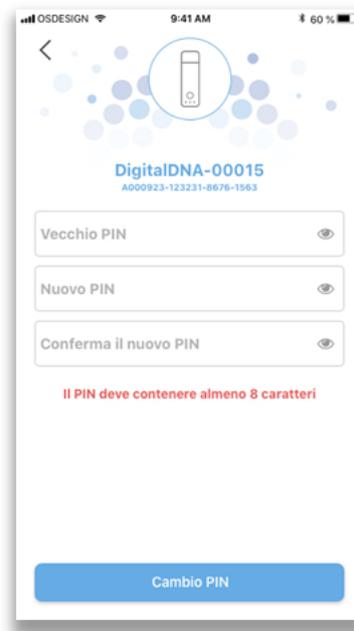


Figura 62

5.7.3 Sblocca PIN

Selezionando la voce “Sblocca PIN” dal menu di “Configura DigitalDNA Key”, è possibile sbloccare il PIN in uso per la DigitalDNA Key qualora si fosse bloccato (es. a causa dell'inserimento di un PIN errato per 3 volte consecutive).

Al centro della schermata sono riportati i dettagli della DigitalDNA Key associata. Lo sblocco del PIN prevede l'utilizzo del codice PUK (Personal Unlocking Key) fornito dal TSP emittitore dei certificati al momento dell'emissione del certificato congiuntamente al PIN.

Per effettuare lo sblocco del PIN è necessario inserire sia il PUK sia il nuovo PIN, confermandolo successivamente. In qualsiasi momento è possibile visualizzare i dati inseriti cliccando sull'icona a destra dei campi di inserimento (pulsante a forma di occhio). Terminato l'inserimento di tutti i dati si compie l'operazione cliccando sul tasto "Sblocca PIN" (Figura 63). Alla fine del processo di sblocco PIN viene visualizzata una schermata di conferma di avvenuto sblocco.



Figura 63

5.7.4 Configura

Selezionando la voce "Configura" dal menu di "Configura DigitalDNA Key", è possibile visualizzare il livello di carica del Token e impostare i seguenti parametri di configurazione (Figura 64):

- a) **Accensione:** intervalli di accensione e spegnimento automatici;
- b) **Profilo energetico:** intervallo di attesa prima dello standby quando il dispositivo è stato acceso al di fuori degli intervalli di accensione/spegnimento automatici;
- c) **Audio:** eventi per i quali il buzzer deve emettere dei segnali acustici;



Figura 64

a) Accensione

Tale funzione permette di impostare gli intervalli in cui si desidera accendere e spegnere automaticamente il dispositivo. In questo modo la DigitalDNA Key risulta immediatamente fruibile in determinate fasce orarie (impostate dall'utente) riducendo sensibilmente il consumo della batteria interna (Figura 65).

Aggiunta di una Fascia Oraria: Cliccando sul tasto “+” a destra della dicitura “Intervalli di accensione” (Figura 65) si accede alla schermata di definizione delle fasce orarie e dei giorni della settimana per cui programmare l'attività del dispositivo, premendo su “Aggiungi” (Figura 66).

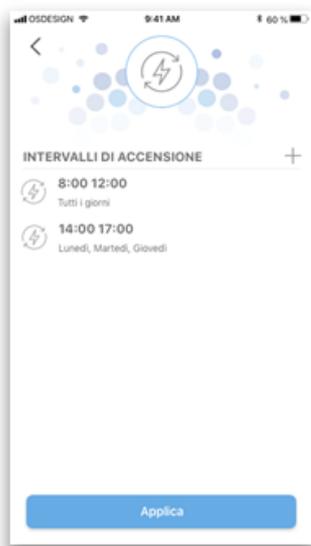


Figura 65



Figura 66

b) Profili

In questa sezione è possibile impostare il profilo utente del *Timeout* (spegnimento automatico dopo un dato periodo di inutilizzo) (Figura 67). Tale funzione permette di ridurre sensibilmente il consumo della batteria interna.

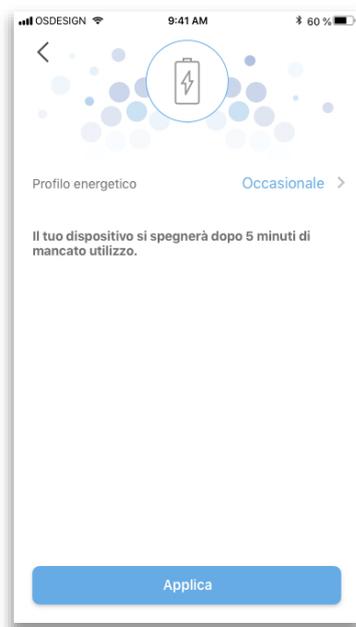


Figura 67



Figura 68

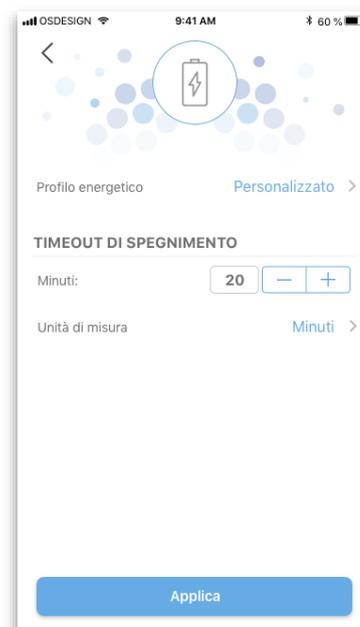


Figura 69

Cliccando su "Profilo energetico" appare il menu con i possibili profili da impostare (*Occasionale, Abituale, Frequente, Personalizzato*) e la possibilità di personalizzare il tempo di time-out (Figura 68).

1. Occasionale – Prevede lo spegnimento automatico dopo 5 minuti di inattività
2. Abituale – Prevede lo spegnimento automatico dopo 8 ore di inattività
3. Frequente – Prevede che il dispositivo rimanga sempre acceso
4. Personalizzato – Prevede che sia l'utente a impostare l'intervallo di inattività che preferisce prima dello spegnimento

Per quanto riguarda il profilo *Personalizzato* è possibile impostare l'unità di misura in *Ore* o *Minuti* (Figura 69).

c) Audio

Tale funzione permette di impostare il feedback acustico della DigitalDNA Key (Figura 70). A seconda delle voci attivate in questa schermata, la DigitalDNA Key emetterà un suono. Le funzioni per le quali sono previsti dei feedback acustici sono: Accensione, Spegnimento, Inizio associazione, Associazione completata.

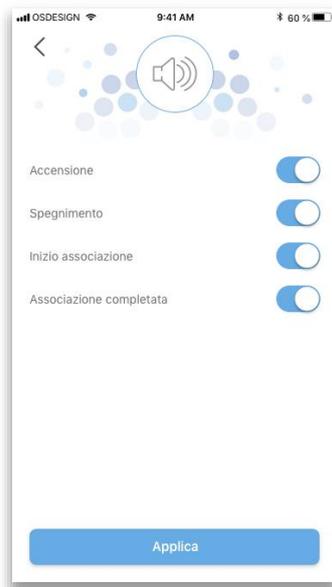


Figura 70

5.7.5 Rimuovi Associazione

Cliccando sulla voce “Rimuovi associazione” presente nel menu di “Configura DigitalDNA Key” (Figura 71) è possibile rimuovere l’associazione tra il dispositivo mobile e la DigitalDNA Key in uso, scegliendo se conservare i documenti sottoscritti e marcati o eliminarli definitivamente dal dispositivo mobile. Per procedere, cliccare su “Conferma” (Figura 72).

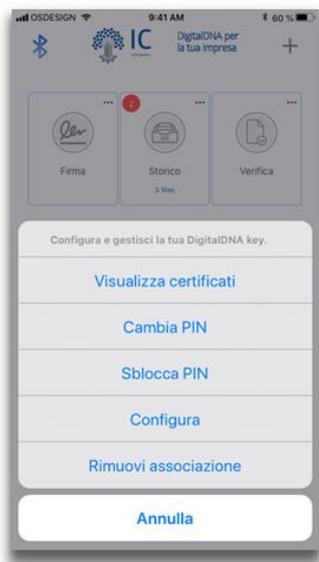


Figura 71

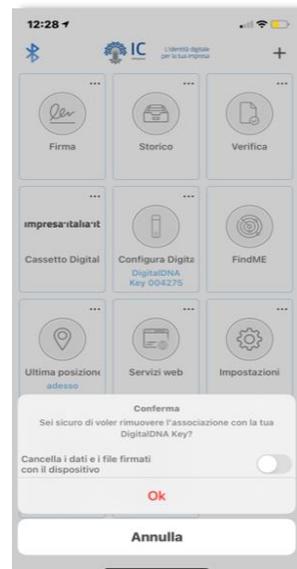


Figura 72

5.8 Ultima Posizione Rilevata

La funzione di “Ultima Posizione Rilevata”, accessibile cliccando sull’omonimo widget nella Home, permette di identificare l’ultima posizione nota della DigitalDNA Key, corrispondente alla posizione in cui questa ha interagito più recentemente con il dispositivo mobile.

A partire da questa schermata (Figura 73) è possibile avviare il navigatore di sistema cliccando sul tasto “Indicazioni” ed ottenere le indicazioni stradali per raggiungere il punto indicato sulla mappa.

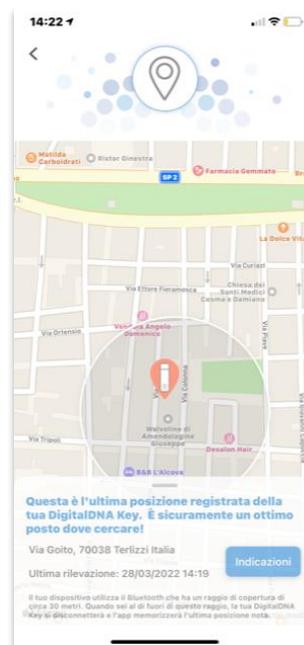


Figura 73

5.9 Widget personalizzato

Oltre ai widget predefiniti dell'app, è possibile creare nuovi widget personalizzati soprattutto a fini statistici. Questi widget consentono, infatti, di monitorare l'utilizzo dell'app DigitalDNA IC e della DigitalDNA Key; in questi widget si può scegliere di visualizzare il numero di firme digitali suddivise per tipologia, di autenticazioni client SSL e di file verificati. È possibile aggiungere widget statistici cliccando sul simbolo "+" che si trova in alto a destra nella schermata Home. Nella Figura 74 si mostra, a titolo esemplificativo, la creazione di un widget "Contatore firme" CADES.

In questa schermata è possibile selezionare la tipologia di dato da considerare (*Firme*, *Verifiche* e *Autenticazioni*) ed in alcuni casi (es. firma) anche il formato da controllare.

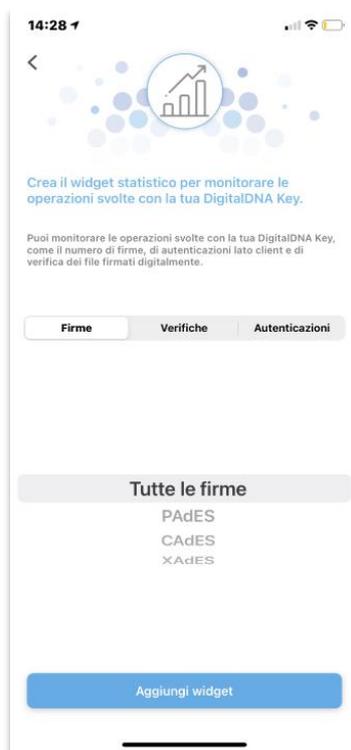


Figura 74

5.10 Impostazioni

È possibile accedere alle "Impostazioni" dalla schermata principale Home. In questa sezione (Figura 75) è possibile configurare le impostazioni che riguardano Firma digitale, Marca Temporale, visualizzazione della schermata Home, funzione FindME e Strumenti per il miglioramento dei servizi, Privacy policy InfoCamere e azioni di gestione dell'account SPID (associazione o dissociazione)

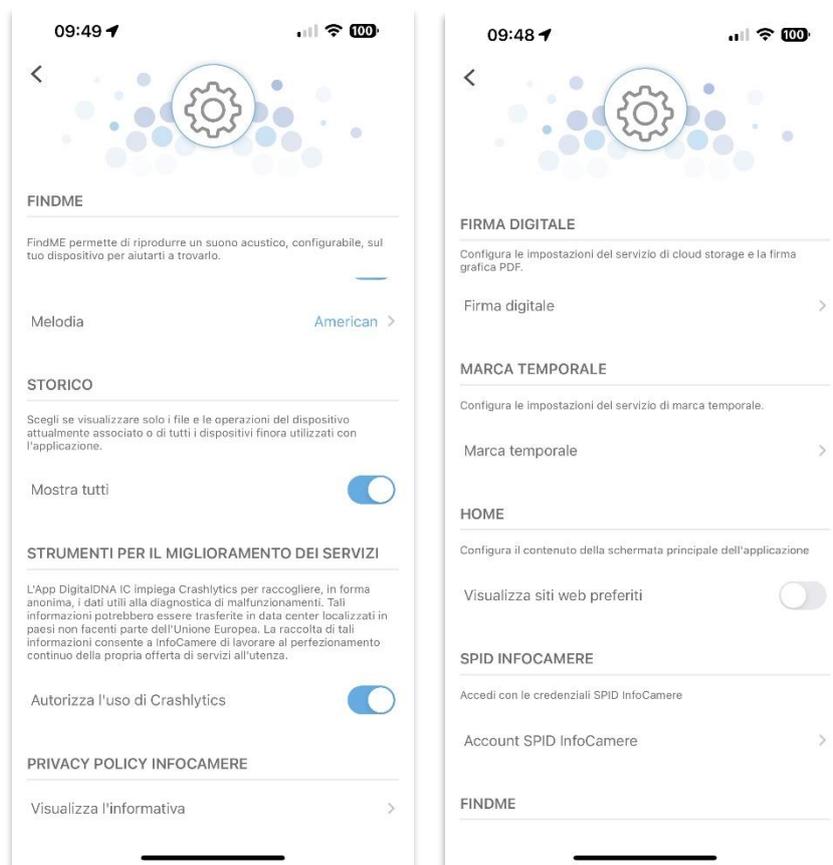


Figura 75

5.10.1 Impostazioni di Firma digitale

Cliccando sulla voce “Firma digitale” all’interno delle “Impostazioni” (Figura 75) si accede alla configurazione del servizio di firma digitale. In questa sezione (Figura 76) è possibile impostare le preferenze di firma disponibili anche durante il processo di firma (paragrafo 5.1.1).

In più, nella sezione “Impostazioni”, è possibile anche:

1. Configurare un servizio di storage (iCloud, Drive, ecc) in cui verrà creata una cartella “DigitalDNA Key”, in cui automaticamente verrà salvata tutta la documentazione firmata.
2. Acquisire l’immagine dell’utente dalla gallery di Sistema o attraverso la camera del dispositivo mobile (smartphone/tablet). Questa immagine viene utilizzata come immagine standard per la firma grafica dei file PDF quando non sono stati acquisiti né il grafo di firma né il grafo delle iniziali. La dicitura “Grafo firma” riporta al processo di acquisizione della firma/iniziali illustrata nel paragrafo 5.1.1.

3. Configurare il servizio di firma remota e la funzione di generazione di codici OTP per la fruizione del servizio di firma remota da client di firma desktop Firma4ng InfoCamere.

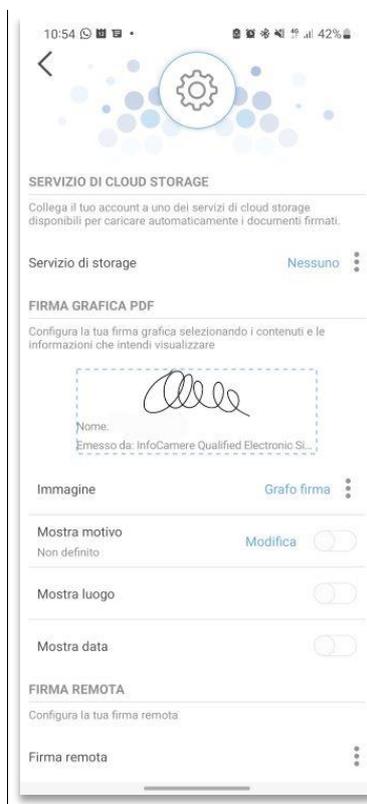


Figura 76

5.10.1.1 Acquisizione dell'immagine utente

Cliccando su "Immagine" si apre il menù mostrato in Figura 77. Cliccando sul tasto "Galleria" si sfoglia la galleria di immagini disponibili sul dispositivo, mentre cliccando sul tasto "Camera" si attiva la fotocamera. Una volta selezionata o scattata un'immagine, questa verrà utilizzata nella firma grafica dei file in formato PDF andando a sostituire il logo InfoCamere di default (Figura 78).



Figura 77

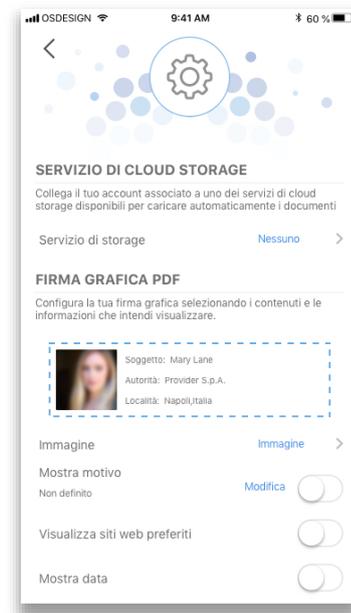


Figura 78

5.10.1.2 Configurazione Firma Remota

Cliccando su “Firma Remota” all’interno della sezione “Impostazioni di firma digitale” (Figura 76), è possibile configurare il servizio di generazione di codici OTP (One Time Password) per la firma remota InfoCamere, direttamente all’interno dell’app DigitalDNA.

Attenzione: per la seguente configurazione è necessario impiegare contestualmente il dispositivo smartphone/tablet su cui è installata l’app DigitalDNA e un PC (o qualsiasi altro dispositivo adibito alla navigazione web).

Dopo aver cliccato su “Firma Remota” all’utente viene chiesto di inserire le credenziali Username (ID Login) e Password (Figura 79) relative al proprio certificato di firma remota, precedentemente attivato. Inserirle nei rispettivi campi e non chiudere l’app. Contestualmente, collegarsi dal PC alle funzioni di gestione della firma remota dal sito InfoCamere all’indirizzo <https://id.infocamere.it/selfcare/>. Accedere al Self Care e dopo aver cliccato sulla voce “Firma Remota” sarà possibile inserire le credenziali di firma remota (Nome utente (ID Login) e Password e cliccare su Accedi (Figura 80).

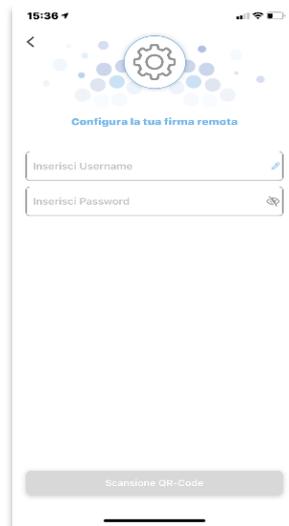


Figura 79

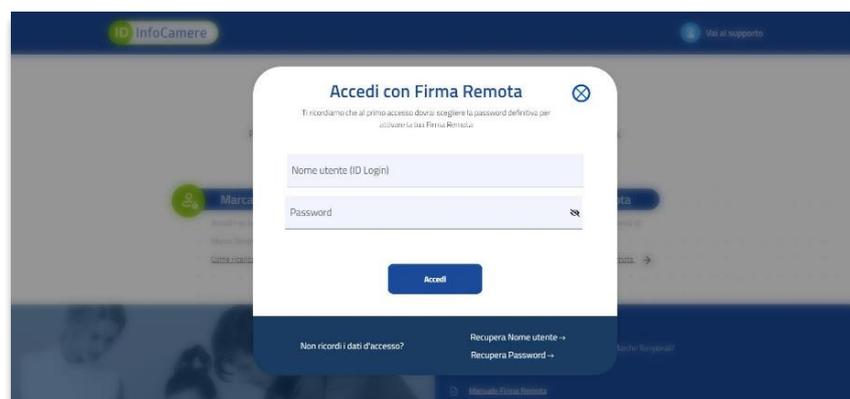
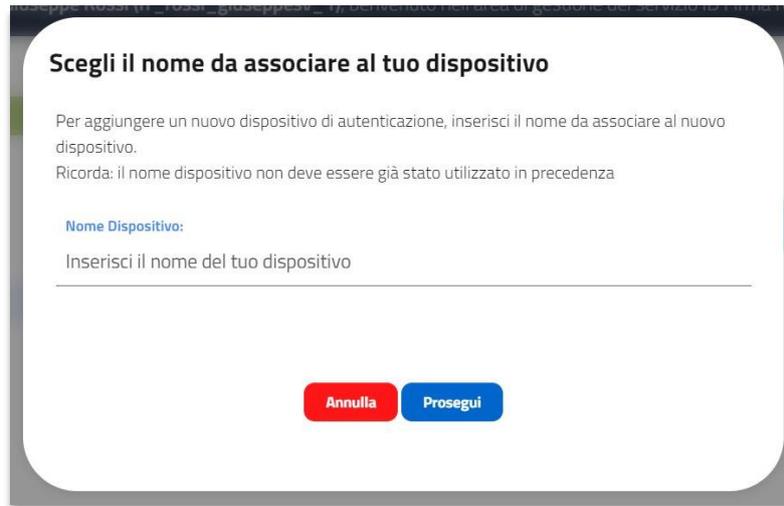


Figura 80

Una volta effettuato l'accesso, cliccare su "Configura l'APP DigitalDNA IC" e nella finestra "Aggiungi dispositivo" (Figura 81) inserire il nome del dispositivo da associare (è possibile utilizzare il nome dispositivo solo una volta). Inserito il nome, cliccare su "Prosegui".



Scegli il nome da associare al tuo dispositivo

Per aggiungere un nuovo dispositivo di autenticazione, inserisci il nome da associare al nuovo dispositivo.
Ricorda: il nome dispositivo non deve essere già stato utilizzato in precedenza

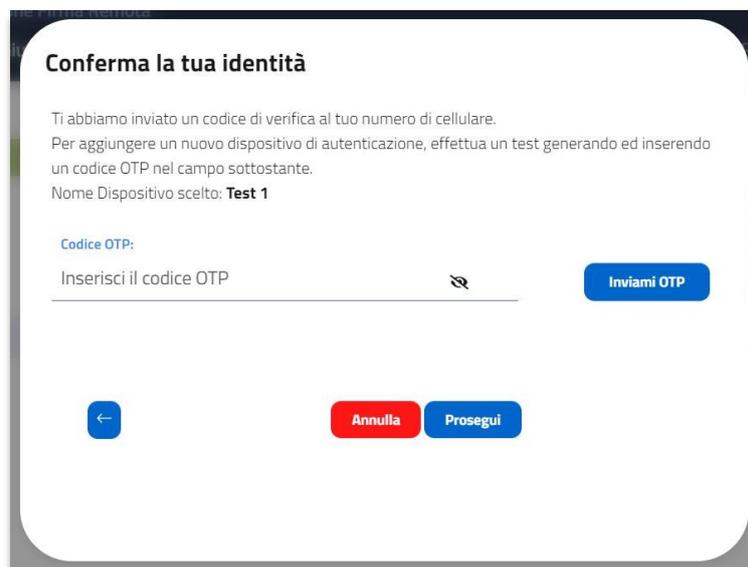
Nome Dispositivo:

Inserisci il nome del tuo dispositivo

Annulla Prosegui

Figura 81

Cliccando su Prosegui, verrà richiesta la conferma dell'operazione tramite inserimento di OTP (Figura 82). L'OTP può essere generato da un dispositivo associato via app o tramite SMS, cliccando su "Inviami OTP".



Conferma la tua identità

Ti abbiamo inviato un codice di verifica al tuo numero di cellulare.
Per aggiungere un nuovo dispositivo di autenticazione, effettua un test generando ed inserendo un codice OTP nel campo sottostante.
Nome Dispositivo scelto: **Test 1**

Codice OTP:

Inserisci il codice OTP 

Inviami OTP

← Annulla Prosegui

Figura 82

A questo punto riprendere l'app DigitalDNA IC sul dispositivo sul quale si erano inserite le credenziali della firma remota e cliccare su "Scannerizza QR code", quindi inquadrare il QR Code con lo smartphone (Figura 83).

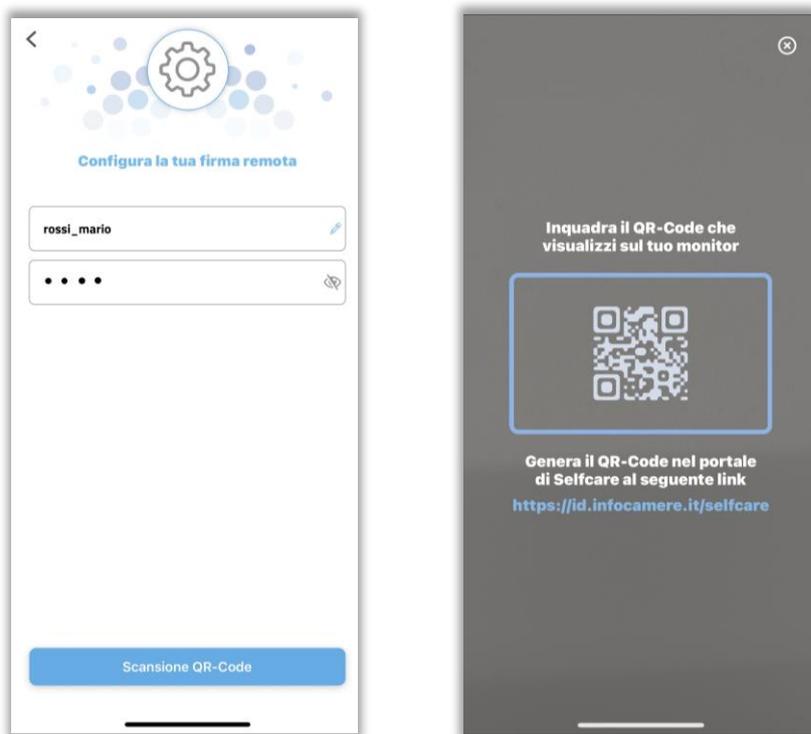


Figura 83

Dopo aver inquadrato il QR code, l'App richiede l'inserimento di PIN, impronta digitale o riconoscimento facciale, secondo quanto previsto come verifica di sicurezza dal dispositivo smartphone/tablet in uso.

La configurazione è terminata e nella Home dell'app compare un nuovo widget con la voce "Genera OTP" (Figura 84).

Tramite il nuovo widget "Genera OTP" è possibile generare rapidamente codici OTP (Figura 85) da utilizzare nella procedura di firma remota tramite l'app desktop Firma4ng InfoCamere, evitando così di richiedere codici via sms.

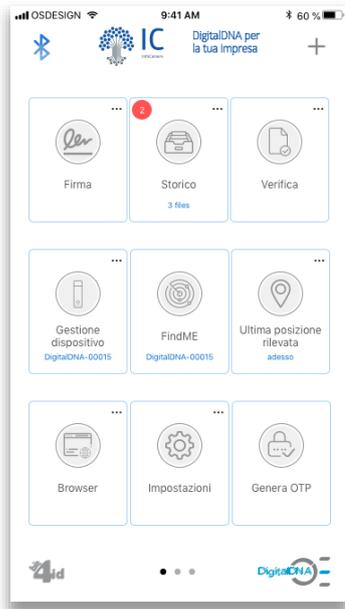


Figura 84

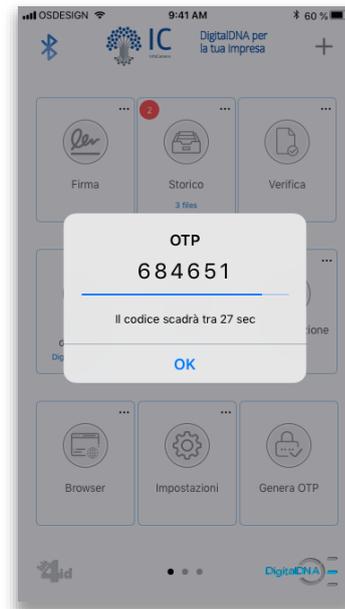


Figura 85

Configurando la firma remota, sarà inoltre possibile procedere alla sottoscrizione dei documenti dall' app secondo le indicazioni riportate al paragrafo 5.1.3..

5.10.2 Impostazioni di Marca temporale

Cliccando su "Marca Temporale" all'interno della sezione "Impostazioni" (Figura 86) è possibile configurare il servizio di Marca Temporale direttamente all'interno dell'App DigitalDNA IC.

Per la configurazione è necessario impiegare contestualmente il dispositivo smartphone/tablet su cui è installata l'App DigitalDNA IC e un PC (o qualsiasi altro dispositivo adibito alla navigazione web).

Dopo aver cliccato su "Marca Temporale" (Figura 87) viene chiesto di aggiungere un nuovo provider. Cliccando su "Aggiungi Nuovo Provider" (Figura 88) si può scegliere la modalità di configurazione che si preferisce, scegliendo tra le seguenti opzioni (Figura 89):

- Scansione QR-Code;
- Manuale.

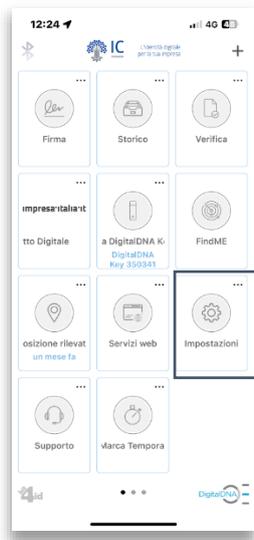


Figura 86



Figura 87

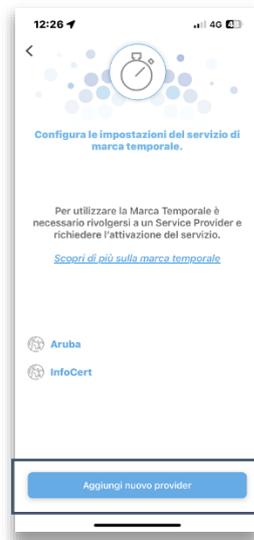


Figura 88



Figura 89

In caso si volesse procedere con la configurazione tramite "Scansione QR-Code" contestualmente è necessario collegarsi dal PC al pannello di gestione della Marche Temporal dal sito InfoCamere all'indirizzo <https://id.infocamere.it/selfcare/> (Figura 90).



Figura 90

Una volta effettuato l'accesso con le proprie credenziali, è necessario cliccare sul pulsante "Configura l'APP DigitalDNA IC" (Figura 91).



Figura 91

Dal pop up 'Scegli il nome del tuo dispositivo' inserire il nome del dispositivo da associare: il nome scelto non deve essere stato utilizzato in precedenza (Figura 92).

Successivamente cliccare su "Proseguì".

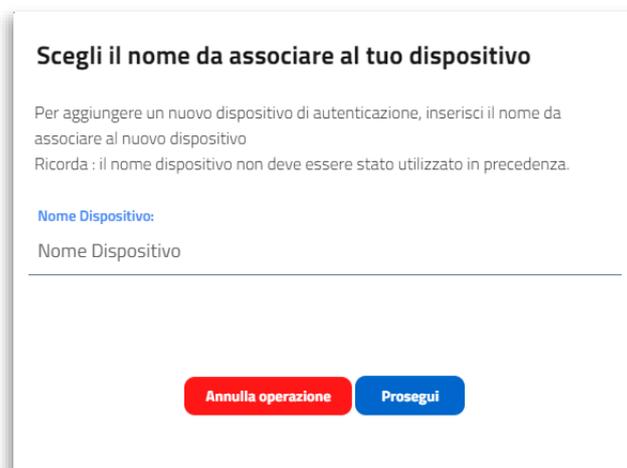


Figura 92

Viene richiesta la conferma dell'operazione tramite inserimento del Codice di verifica (Figura 93), inviato tramite SMS sul proprio numero di cellulare. Dopo aver inserito il Codice di verifica, cliccare sul tasto "Proseguì".

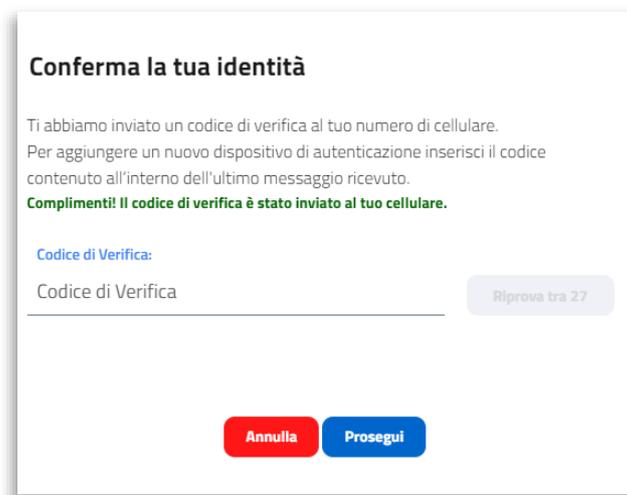


Figura 93

Si genera in automatico un QR-Code da scansionare con il proprio smartphone (Figura 94).

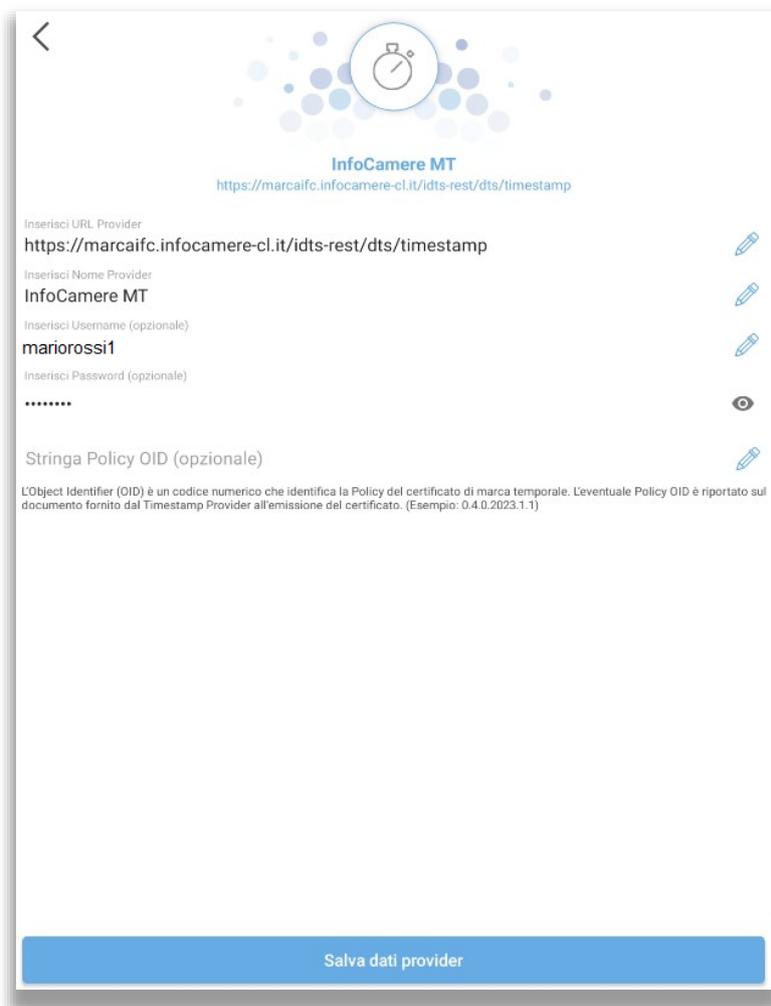


Figura 94

A questo punto, riprendere l'App DigitalDNA IC sul dispositivo e cliccare su "Scansione QR-Code"; quindi inquadrare il QR-Code con lo smartphone/tablet.

Dopo aver effettuato la scansione, le voci elencate di seguito vengono compilate di default (Figura 95):

- Inserisci URL Provider
- Inserisci Nome Provider
- Inserisci Username (opzionale)
- Inserisci Password (opzionale)



<



InfoCamere MT
<https://marcaifc.infocamere-cl.it/ids-rest/dts/timestamp>

Inserisci URL Provider
https://marcaifc.infocamere-cl.it/ids-rest/dts/timestamp 

Inserisci Nome Provider
InfoCamere MT 

Inserisci Username (opzionale)
marirossi1 

Inserisci Password (opzionale)
..... 

Stringa Policy OID (opzionale) 

L'Object Identifier (OID) è un codice numerico che identifica la Policy del certificato di marca temporale. L'eventuale Policy OID è riportato sul documento fornito dal Timestamp Provider all'emissione del certificato. (Esempio: 0.4.0.2023.1.1)

Salva dati provider

Figura 95

Dopo aver cliccato sul pulsante "Salva dati provider", si visualizza nell'elenco il nuovo provider appena configurato (Figura 96).

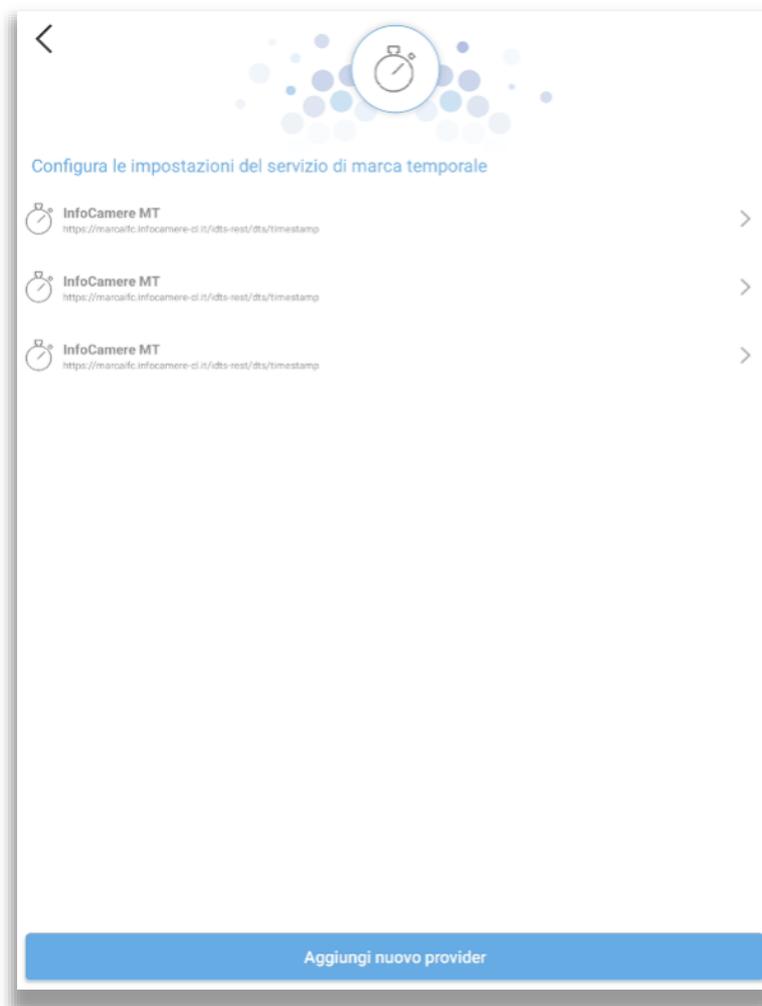
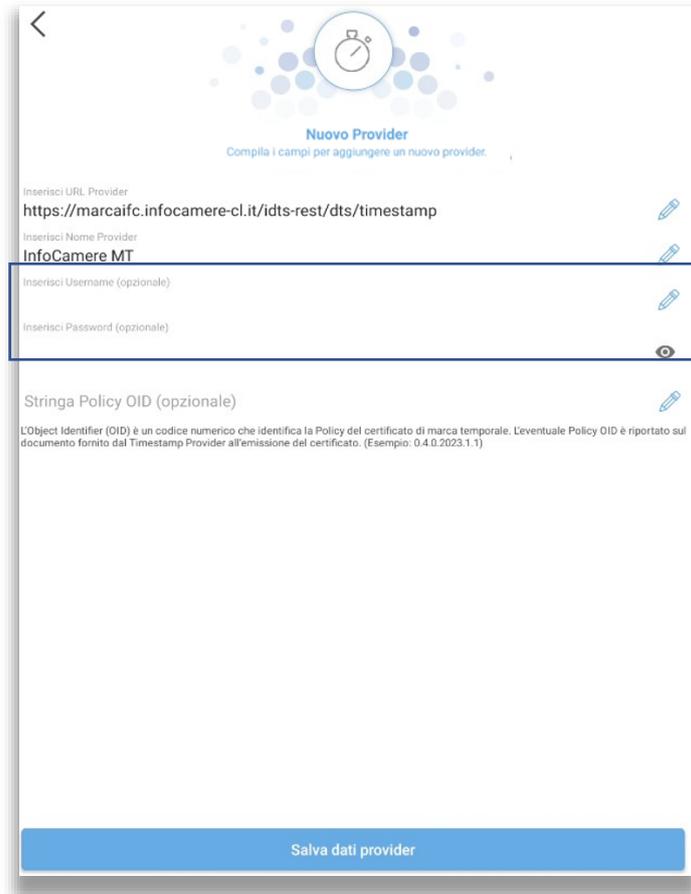


Figura 96

Nel caso si volesse procedere invece con la configurazione "Manuale" (Figura 89), le voci da compilare manualmente sono le seguenti (Figura 97):

- Inserisci Username (opzionale)
- Inserisci Password (opzionale)



<

Nuovo Provider
Compila i campi per aggiungere un nuovo provider.

Inserisci URL Provider
https://marcaifc.infocamere-cl.it/ids-rest/dts/timestamp

Inserisci Nome Provider
InfoCamere MT

Inserisci Username (opzionale)

Inserisci Password (opzionale)

Stringa Policy OID (opzionale)

L'Object Identifier (OID) è un codice numerico che identifica la Policy del certificato di marca temporale. L'eventuale Policy OID è riportato sul documento fornito dal Timestamp Provider all'emissione del certificato. (Esempio: 0.4.0.2023.1.1)

Salva dati provider

Figura 97

Dopo aver effettuato la compilazione dei campi e cliccato sul pulsante "Salva dati provider", la configurazione delle credenziali sul nuovo dispositivo è terminata (Figura 96).

È possibile eliminare un provider dall'elenco con uno *swipe*, ovvero trascinando il dito da destra verso sinistra sulla voce corrispondente.

5.10.3 Impostazioni della Home

La sezione Impostazioni (Figura 75) permette di configurare anche la schermata principale dell'applicazione. Cliccare sulla voce "Visualizza siti web preferiti" per attivare/disattivare la funzione corrispondente.

5.10.4 Impostazioni account SPID INFOCAMERE

Cliccando su "Account SPID InfoCamere" all'interno del widget "Impostazioni" (Figura 75), è possibile configurare il servizio di generazione di codici OTP (One Time Password) per la credenziale di secondo livello SPID InfoCamere, direttamente all'interno dell'app DigitalDNA IC.

Attenzione: per la seguente configurazione è necessario impiegare contestualmente il dispositivo smartphone/tablet su cui è installata l'app DigitalDNA e un PC (o qualsiasi altro dispositivo adibito alla navigazione web).

Dopo aver cliccato su "Account SPID InfoCamere" viene chiesto di inserire le credenziali Username e Password (Figura 98) relative alla propria Identità Digitale SPID, precedentemente attivata. Inserirle nei rispettivi campi e non chiudere l'app. Contestualmente, collegarsi dal PC (o da un secondo device) all'area riservata per la gestione dell'Identità SPID <https://selfcarespid.infocamere.it/spid-selfCare/#/login>. Inserirle le credenziali dell'Identità SPID nella finestra di accesso (Figura 99) e cliccare su "Accedi" (nel caso in cui all'Identità SPID sia già associata una credenziale di secondo livello con OTP via SMS verrà richiesta anche la generazione e l'inserimento del codice nell'apposita schermata).

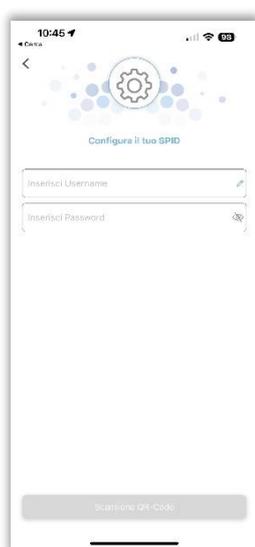


Figura 98

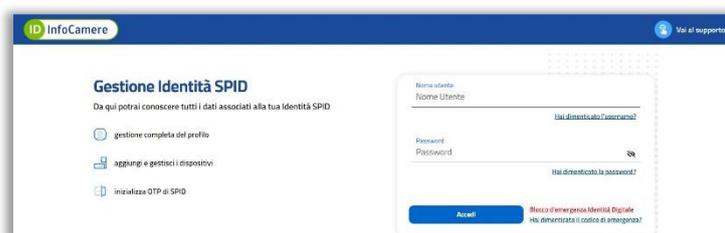


Figura 99

Una volta effettuato l'accesso, cliccando sul pulsante "Configura DigitalDNA IC OTP" (Figura 100), viene mostrata una schermata in cui è possibile, tramite la scansione del QR Code essere reindirizzati allo store del proprio dispositivo per effettuare il download dell'app (Figura 101). Qualora si disponesse già dell'applicazione sul proprio dispositivo cliccare su "Prosegui" e, nella schermata successiva inserire il nome da associare come generatore di OTP (es. Smartphone di Andrea), poi cliccare su "Prosegui" (Figura 102).

Per confermare l'operazione di associazione è richiesto l'inserimento di un codice OTP inviato in automatico dal sistema al numero di cellulare associato all'Identità SPID (Figura 103).



Figura 100



Figura 101



Figura 102



Figura 103

Inserire il codice di 6 cifre ricevuto e confermare l'operazione attraverso il pulsante "Verifica": la pagina mostrerà un QR Code della validità di 2 minuti (Figura 104).

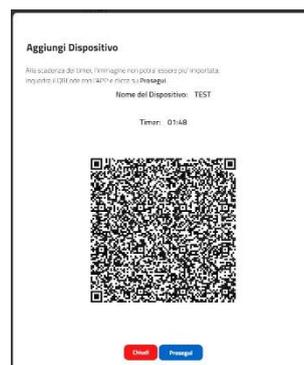


Figura 104

A questo punto riprendere l'app DigitalDNA IC dal dispositivo alla quale si vuole associare l'Identità Digitale SPID e cliccare su "Scansione QR-Code" (Figura 98). Quindi inquadrare il QR Code con lo smartphone/tablet.

Dopo aver inquadrato il QR Code l'app richiede l'inserimento del codice di sblocco, impronta digitale o riconoscimento facciale secondo quanto previsto dal dispositivo (Figura 105). Successivamente l'app

mostrerà una schermata che conferma la corretta configurazione dell'account SPID e mostra un codice OTP della durata di 60 secondi (al termine dei quali viene generato un nuovo codice) (Figura 106). L'Utente, nel Self Care, clicca su "Prosegui" (Figura 104).



Figura 105

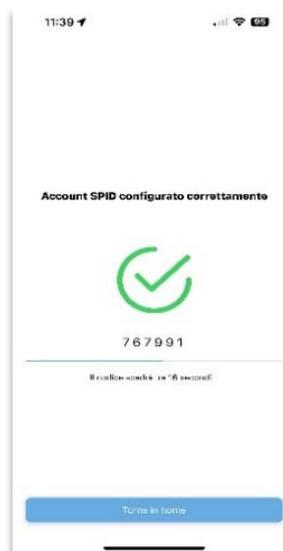


Figura 106

Il Self Care mostrerà una schermata in cui inserire il codice OTP generato dall'app DigitalDNA IC, necessario alla sincronizzazione del dispositivo con l'account SPID InfoCamere. Inserire il codice OTP e cliccare su "Conferma" (Figura 107).



Figura 107

Successivamente, per terminare la configurazione, nell'app cliccare su "Torna in home" (Figura 108).



Figura 108

La configurazione è terminata e nella Home dell'app compare un nuovo widget con la voce "Genera OTP SPID" (Figura 109).

Tramite il nuovo widget "Genera OTP SPID" è possibile generare rapidamente codici OTP da utilizzare per l'autenticazione ai portali online dei fornitori di servizi o per l'autenticazione al Self Care, evitando così di richiedere codici via sms.

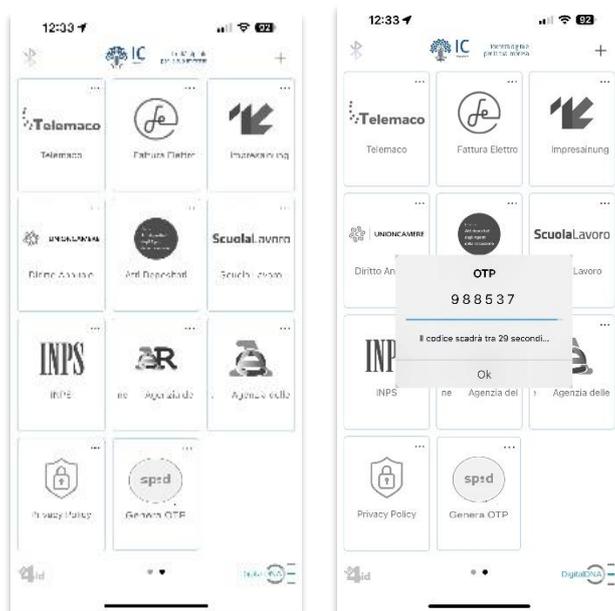


Figura 109

Dopo aver terminato correttamente la configurazione, il Self Care mostrerà un messaggio di conferma dell'attivazione della credenziale di secondo livello. Nella sezione "Gestione credenziali" la credenziale risulterà nello stato "ATTIVA" (Figure 110 e 111)



Figura 110

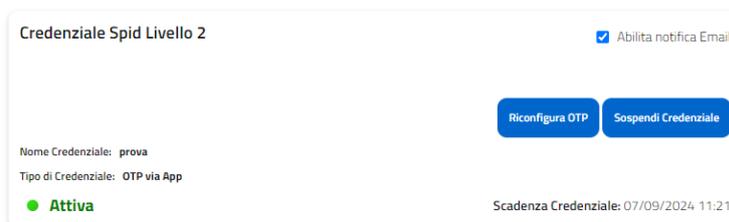


Figura 111

5.10.5 Impostazioni del FindME

Nella sezione delle Impostazioni che riguarda la funzione FindME (Figura 74), l'utente può abilitare le funzionalità che consentono sia di ritrovare lo smartphone/tablet dalla DigitalDNA Key sia la DigitalDNA Key stessa dall'app.

Abilitando tali funzionalità, l'app chiede all'utente l'autorizzazione per utilizzare la sua posizione. Dopo aver espresso il consenso alla geolocalizzazione, così come previsto dal Regolamento GDPR sulla protezione dei dati personali, l'utente può usufruire delle funzioni dettagliate di seguito:

- **Ricerca dello Smartphone/Tablet**

Se la funzione FindME è abilitata per trovare il proprio smartphone/tablet, basta cliccare sul bottone di controllo della DigitalDNA Key due volte in rapida successione. In base allo stato dell'app DigitalDNA IC, questa si comporta in maniera differente a seconda se sia in esecuzione in background o in foreground. Se in background, il dispositivo mobile abbinato presenta una notifica e simultaneamente è avviato un feedback sonoro per richiamare l'attenzione. Se invece l'app è foreground, viene visualizzato un alert e contemporaneamente sarà emesso un feedback sonoro. Il feedback sonoro termina quando l'utente clicca sulla push notification nel primo caso o sull>alert nel secondo caso.

- **Ricerca della DigitalDNA Key**

La ricerca della DigitalDNA Key avviene attraverso la schermata Home così come illustrato nel paragrafo 5.6.

- **Melodia**

Cliccando sulla voce "Melodia" è possibile impostare il suono riprodotto dalla funzione findME.

5.10.6 Impostazioni dello Storico

Nella sezione Impostazioni è possibile configurare la visualizzazione dello Storico e quindi scegliere se visualizzare solo i file e le operazioni della DigitalDNA Key attualmente associata o di tutte quelle che sono state utilizzate con l'applicazione. Cliccare sulla voce "Mostra tutti" per attivare/disattivare la funzione corrispondente.

5.10.7 Strumenti per il miglioramento dei servizi

Nella sezione *Strumenti per il miglioramento dei servizi* è possibile autorizzare l'uso di Crashlytics e, in caso di Android e Huawei, di Google Analytics, per consentire ad InfoCamere di raccogliere, in forma anonima, i dati utili alla diagnostica di malfunzionamenti. Queste funzioni ci permettono di lavorare al perfezionamento dei servizi offerti. Cliccare sulla voce "Autorizza l'uso di Crashlytics" e "Autorizza l'uso di Google Analytics" per attivare/disattivare le funzioni corrispondenti.

5.10.8 Privacy Policy InfoCamere

Cliccando su 'Visualizza l'Informativa' è possibile visualizzare la Policy Privacy dell'App DigitalDNA.

5.11 Supporto

Cliccando sul widget "Supporto" presente nella schermata principale Home, l'utente accede alla sezione in cui si trovano le informazioni sul prodotto e sulle modalità di assistenza (Figura 112).

In caso di necessità, è infatti possibile richiedere supporto al Servizio Clienti tramite telefono o posta elettronica. Nella sezione Assistenza, l'utente può scegliere come mettersi in contatto con l'assistenza dedicata (tramite appuntamento telefonico, ricontatto o form di richiesta compilabile). Inoltre è possibile accedere direttamente dal sito di ID InfoCamere id.infocamere.it e alle FAQ sulla DigitalDNA Key.



Figura 112

6 CONSIGLI D'UTILIZZO

Per velocizzare l'apertura e la firma dei documenti su iOS 13 e tutte le versioni successive, si consiglia di impostare l'app DigitalDNA IC tra i Preferiti attraverso i seguenti passaggi:

- Selezionare un file e cliccare sull'icona "Condividi" in basso a sinistra (Figura 113 e 114)
- Scorrere tutto il menu a tendina e cliccare su "Modifica azioni" (Figura 115)
- Tenere premuto su "DigitalDNA" e trascinare la voce verso l'alto fino a raggiungere la sezione "Preferiti". Rilasciare una volta scelta la posizione desiderata e cliccare su "Fine" (Figura 116 e Figura 117)

L'app DigitalDNA IC è impostata tra le app preferite per l'apertura e la condivisione dei file (Figura 118).

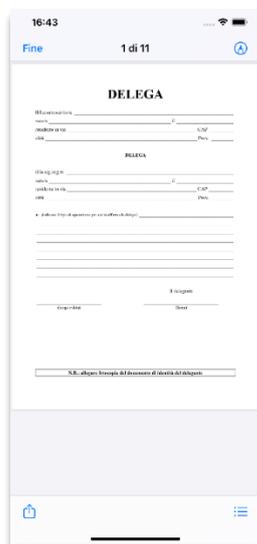


Figura 113



Figura 114

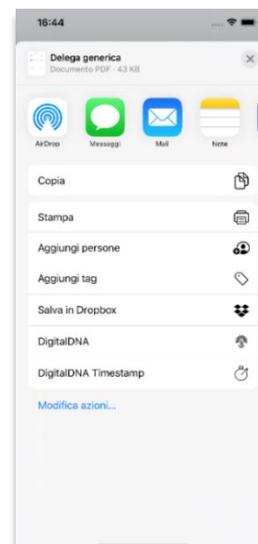


Figura 115

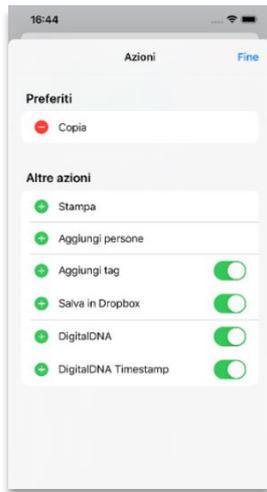


Figura 116

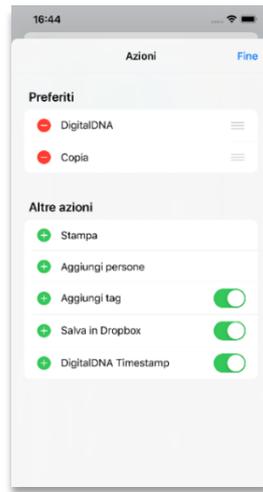


Figura 117

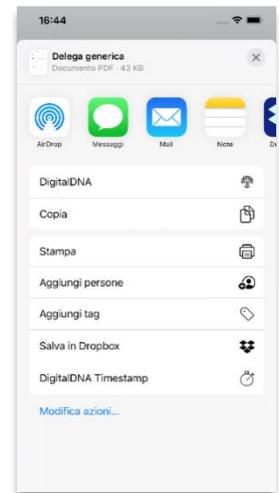


Figura 118