Convenzione per la promozione e la realizzazione del servizio di estrazione e stampa di certificati anagrafici presso gli esercizi associati alla Federazione Italiana Tabaccai.

Tra

Comune di Rocca di Papa, in persona del suo legale rappresentante pt, _____, nata/o a _____ il _____, C.F. _____, ubicata per la carica presso il Palazzo comunale di _____;

Federazione Italiana Tabaccai, con sede legale in Roma, Via Leopoldo Serra 32, in persona del suo legale rappresentante pt. e Presidente Nazionale: Cav. Uff. Giovanni Risso, nato a Imperia (IM) il 24/11/1937, C.F. RSSGNN37S24E290D, domiciliato per la carica presso la sede legale, (di seguito anche FIT);

Premesso che

- L'art.62 del Codice dell'Amministrazione Digitale di cui al D.Lgs. 82/2005 ha istituito presso il Ministero dell'Interno l'Anagrafe Nazionale della Popolazione Residente (ANPR), quale base dati di interesse nazionale ai sensi dell'art.60 dello stesso Codice;

- Il Comune di Rocca di Papa ha positivamente completato il subentro nell'ANPR, mediante migrazione ed allineamento della banca dati locale;

- Alla luce dell'art. 62 comma 3 del citato D.Lgs. 82/2005, l'ANPR consente ai comuni la certificazione dei dati anagrafici nel rispetto di quanto previsto dagli articoli 33 e 35 del DPR 223/1989;

- In una logica di efficacia ed efficienza dell'azione amministrativa e di miglioramento dei servizi in favore degli utenti, il Comune di Rocca di Papa intende promuovere la possibilità del rilascio di certificati anagrafici attraverso punti distribuiti sul territorio in alternativa agli uffici istituzionali comunali;

- E' quindi interesse dell'Amministrazione realizzare forme di collaborazione che, attraverso l'ausilio di adeguati ed innovativi strumenti tecnologici, permettano di rendere più efficienti i servizi erogati alla collettività ed in particolare agli utenti con maggiore difficoltà di accesso ai sistemi informatici;

- La FIT, Federazione Tabaccai Italiani, rappresentativa a livello nazionale di un network di oltre 46.000 esercizi associati, vanta una consolidata esperienza nell'erogazione di servizi all'utenza ed ha già aderito in diverse realtà territoriali a progetti di decentramento delle attività di rilascio delle certificazioni anagrafiche attraverso il coinvolgimento degli operatori economici della rete;

- Per la realizzazione di tali progetti che hanno garantito capillarità e flessibilità dei servizi a vantaggio di tutte le fasce di utenza, generando peraltro minori oneri per le amministrazioni in termini di impiego di risorse interne sia di sportello che di back office, FIT si è avvalsa per tutti gli aspetti operativi, tecnici ed informatici della collaborazione

di Novares SpA, società del Gruppo che vanta una consolidata esperienza nel campo delle attività in favore della Pubblica Amministrazione;

- Il Comune di Rocca di Papa ha manifestato la propria disponibilità a sottoscrivere una Convenzione con FIT - senza alcun carattere di esclusività - finalizzata a garantire ai cittadini, attraverso modalità compatibili e coerenti con i vincoli e le disposizioni dettate dal quadro normativo di riferimento, punti alternativi presso i quali richiedere e stampare i certificati anagrafici, rispetto agli uffici dell'Amministrazione a ciò deputati;

- Con riferimento al progetto di decentramento di cui al punto che precede e nell'ambito della autonomia organizzativa riconosciuta per la sua realizzazione, FIT dichiara sin d'ora che si avvarrà della collaborazione di Novares SpA per i profili organizzativi, tecnici ed informatici previsti nella presente Convenzione, restando intesa l'estraneità del Comune a qualsiasi sottostante rapporto e/o accordo intercorrente tra FIT stessa e quest'ultima società;

- Le parti procedono pertanto alla stipula della presente Convenzione allo scopo di disciplinare i reciproci rapporti nonché gli obblighi che dovranno osservare gli esercizi aderenti, in relazione: a) alla fase preliminare di promozione del progetto; b) alla verifica di funzionalità e validazione dell'applicativo gestionale; c) ai tempi di avvio e le modalità di esecuzione delle attività previste dal successivo art.2; d) alle conseguenze derivanti dalla violazione degli impegni assunti dalle parti con la sottoscrizione della Convenzione; e) alle ipotesi di disabilitazione dell'accesso dei singoli esercizi aderenti per la violazione degli obblighi assunti; f) al trattamento dei dati personali.

Tutto ciò premesso
tra le parti si conviene e si stipula quanto segue.

Art.1
Premesse e considerato

1.1 Le premesse costituiscono parte integrante e sostanziale del presente accordo.

Art.2
Oggetto e finalità della Convenzione

2.1 Oggetto dell'accordo condiviso tra le parti è la promozione e l'attivazione presso gli esercizi associati a FIT presenti sul territorio comunale che manifesteranno la volontà di aderire alla presente Convenzione, del servizio di estrazione e rilascio all'utenza delle certificazioni anagrafiche di cui all'articolo 33 e 35 del DPR 223/1989, da realizzare attraverso il collegamento informatico con il Portale dell'Ente.

2.2 La presente Convenzione con la Federazione Italiana Tabaccai opera nel rispetto, tra le altre norme, del D.Lgs. 267/2000 atteso che non si configura un trasferimento delle funzioni delegate agli enti territoriali ai sensi degli artt.14 e 15 del T.U.E.L.

2.3 Resta ferma la facoltà del Comune di stipulare convenzioni, protocolli e/o accordi di contenuto analogo alla presente e per le medesime finalità, con altri soggetti anche di carattere associativo.

2.4 L'autorizzazione al collegamento informatico di cui al comma 1 del presente articolo deve intendersi riferito in favore di esercizi associati alla FIT operanti sul territorio del Comune di Rocca di Papa, ed abiliterà alla estrazione dei certificati anagrafici conformemente a quanto previsto dagli artt. 33 e 35 del DPR 223/1989.

Art. 3
Obblighi delle parti

3.1 Le parti si impegnano a cooperare per la realizzazione, nei tempi definiti dalla presente Convenzione, delle attività previste all'art.2.1.

3.2 Il Comune, in particolare, si impegna a svolgere una attività promozionale che garantisca la conoscenza del servizio presso l'utenza potenzialmente interessata.

3.3 L'Ente ha piena conoscenza ed ha condiviso la soluzione informatica proposta da FIT, così come descritta nel documento tecnico allegato (All.1), attraverso la quale le singole tabaccherie che sottoscriveranno il modulo di adesione predisposto dall'Amministrazione, garantiranno il servizio di cui all'art. 2.1. Tale documento deve intendersi passibile di revisioni nel corso della Convenzione in ragione di sopravvenute esigenze tecniche di sviluppo del progetto, che saranno in ogni caso oggetto di preventivo confronto e condivisione tra le Parti.

3.4 Con riferimento al punto che precede, l'integrazione con i webservices messi a disposizione da ANPR sarà realizzata attraverso un applicativo installato presso il datacenter dell'Ente. Fit assicurerà la legittima disponibilità in comodato d'uso gratuito del predetto applicativo per la durata della presente Convenzione, assumendosi ogni onere relativo al suo sviluppo e manutenzione da remoto, mentre la sua gestione - sia in termini di configurazione iniziale che di controllo e tracciatura dei log - farà capo esclusivamente all'Amministrazione.

3.5 Oltre che per le sopravvenute esigenze tecniche di sviluppo richiamate al punto 3.3, in conseguenza di rilevanti modifiche normative e/o tecnico procedurali che dovessero intervenire durante la vigenza del presente Accordo, le parti si impegnano a definire una diversa modalità di accesso ed esecuzione delle attività di estrazione e stampa delle certificazioni anagrafiche conforme alla eventuale sopravvenuta disciplina.

3.6 L'Ente garantirà l'accesso ai servizi anagrafici sette giorni su sette senza limitazioni di orario, fatta salva la sospensione o la disattivazione che dovessero derivare da ragioni di forza maggiore ovvero per esigenze tecniche. Nel caso di interruzioni programmate, anche per intervalli temporali dedicati all'aggiornamento della banca dati, l'Ente comunicherà via PEC i tempi di ripristino del servizio.

3.7 FIT si impegna a promuovere e sensibilizzare l'adesione al progetto di diffusione dei servizi anagrafici decentrati presso i propri esercizi associati, garantendo, ove possibile, una equa distribuzione nell'ambito del territorio comunale.

3.8 FIT garantirà all'esercizio autorizzato il software ed ogni altra infrastruttura, oltre alla relativa assistenza tecnica, che supporti i processi di collegamento informatico per il rilascio delle certificazioni anagrafiche.

3.9 FIT, attraverso Novares SpA, i cui incaricati si coordineranno con le competenti strutture del Comune, darà avvio alle attività di verifica della funzionalità della soluzione progettuale e di compatibilità ed integrazione con i sistemi informatici in uso all'Ente entro 15 giorni dalla sottoscrizione della Convenzione. Tale fase propedeutica per il successivo avvio del servizio all'utenza, dovrà concludersi entro i successivi 15 giorni.

3.10 L'Ente, che garantirà gratuitamente il collegamento telematico al proprio Portale, non sosterrà alcun onere per l'acquisizione e l'utilizzo della strumentazione hardware e software da parte dell'esercizio aderente funzionale all'erogazione dei servizi di cui all'art. 2.1. L'Ente è altresì estraneo a qualsiasi sottostante rapporto o accordo intercorrente tra FIT, Novares ovvero altre società del Gruppo, con il singolo esercizio aderente.

3.11 Nell'ambito del presente accordo è esclusa la possibilità da parte FIT e di Novares, avvalendosi dei propri sistemi tecnologici, di apportare modifiche e di alterare le informazioni presenti nella banca dati anagrafica, nonché di estrarre massivamente dati e/o informazioni, ovvero i dati di autenticazione dell'Ente per l'accesso ad ANPR.

3.12 Il Comune si riserva la facoltà di limitare o sospendere il collegamento informatico con il proprio Portale, qualora sopravvenute discipline normative e regolamentari introducano limiti e vincoli che rendono necessaria una revisione delle modalità tecniche ed operative di realizzazione del servizio così come previste della presente Convenzione.

3.13 Il presente accordo non genera costi per l'Amministrazione diversi da quelli riconducibili agli obblighi individuati ed assunti con la presente Convenzione, intendendosi a totale carico di FIT e degli esercizi aderenti, qualsiasi ulteriore onere diretto ed indiretto conseguente alle attività di cui all'art.2.1.

3.14 FIT garantirà al Comune l'aggiornamento dinamico degli esercizi aderenti, avendo cura di trasmettere il modulo di adesione richiamato al punto 3.3 debitamente sottoscritto.

.

Art.4
Corrispettivo per gli esercizi aderenti

4.1 Gli esercizi aderenti potranno applicare un corrispettivo per l'erogazione del servizio di cui all'art.2.1 della presente Convenzione, pari ad **euro 2,00** (euro due/00) per ogni certificazione richiesta dall'utente.

4.2 Qualsiasi variazione del corrispettivo previsto dal comma che precede dovrà essere preventivamente e motivatamente richiesta da FIT ed autorizzata dall'Amministrazione.

4.3 Gli esercizi convenzionati sono tenuti ad applicare l'imposta di bollo sui certificati rilasciati, nei casi previsti dalla legge.

Art.5
Durata della Convenzione, cause di risoluzione e disabilitazione delle credenziali di accesso

5.1 La presente Convenzione avrà una durata di 24 mesi decorrenti dalla sua sottoscrizione. La stessa potrà essere rinnovata per un periodo di uguale durata, all'esito di una positiva valutazione del servizio erogato da parte dell'Amministrazione che terrà conto dell'indice di soddisfazione dell'utenza.

5.2 L'eventuale violazione da parte di FIT degli impegni previsti dal precedente art.3 nonchè dal successivo art.9, integra una condizione per esercitare il recesso immediato dalla presente Convenzione da parte dell'Amministrazione.

5.3 FIT potrà anticipatamente recedere dalla presente Convenzione con un preavviso di 30 giorni, nell'ipotesi in cui l'Amministrazione non autorizzi il richiesto adeguamento del corrispettivo previsto dall'art.4 del servizio.

5.4 Il Comune si riserva di monitorare l'esecuzione delle attività di cui all'art. 2.1 del presente accordo con possibilità di registrazione automatica di tutte le operazioni effettuate dall'esercizio aderente. L'Ente comunicherà a FIT la revoca della adesione del singolo esercizio nell'ipotesi in cui rilevi anomalie e/o violazioni delle prescrizioni previste dalla presente Convenzione.

Art.6
Manleva e limitazioni di responsabilità

6.1 Nel rispetto degli impegni assunti, FIT assicurerà l'adozione da parte degli esercizi aderenti, di misure tecniche e organizzative adeguate al tipo di attività, manlevando espressamente il Comune da anomalie, malfunzionamenti ed altre irregolarità riconducibili alle attività previste dall'art.2 della presente Convenzione, che possano dare luogo a risarcimenti in favore di terzi.

Art.7
Comunicazioni tra le parti

7.1 Le parti, ciascuna per la propria competenza, indicano quali referenti e responsabili della Convenzione nei confronti della controparte il sig. Giovanni Risso per FIT, al quale dovranno essere indirizzate le comunicazioni previste dalla presente Convenzione.

7.2 Le comunicazioni sono scambiate esclusivamente a mezzo pec ai seguenti indirizzi:
Per il Comune di Rocca di Papa: _____
Per FIT: **fit@pec.tabaccai.it.**

Art.8
Obbligo di riservatezza

8.1 Nel corso dell'esecuzione dell'incarico, l'Amministrazione potrà venire a conoscenza di informazioni, Know-how e metodologie di lavoro riservate che possono essere protette dalle leggi in materia di proprietà intellettuale e/o industriale in favore della Società. Il Comune si impegna, pertanto, a non divulgare e/o diffondere a terzi dette informazioni nonché qualsivoglia ulteriore notizia inerente all'attività della stessa della quale sia venuto a conoscenza in occasione dell'esecuzione dell'incarico, a tal fine adottando tutte le ragionevoli misure per impedire la divulgazione e/o l'accesso indebito alle informazioni.

Art.9
Protezione dei dati personali

9.1 Ai sensi della vigente normativa sul trattamento dei dati personali le Parti si autorizzano implicitamente e reciprocamente al trattamento dei dati personali riportati nella presente Convenzione esclusivamente per le finalità di esecuzione della medesima.

9.2 Le Parti si impegnano altresì a trattare i dati personali cui verranno a conoscenza nell'esecuzione della presente Convenzione nei limiti, nelle forme e con le modalità previste dal Regolamento UE 2016/679 (di seguito "GDPR") e dal Codice della Privacy di cui al D.lgs. n. 196 del 30/06/2003, come modificato dal D.lgs. n. 101 del 10/08/2018 ed eventuali successive modificazioni o integrazioni.

9.3 Le Parti dichiarano di essersi reciprocamente comunicate, oralmente e prima della sottoscrizione della Convenzione, le informazioni di cui all'art. 13 del GDPR circa il trattamento dei dati personali conferiti per la sottoscrizione e l'esecuzione della Convenzione stessa e di essere a conoscenza dei diritti che spettano loro in virtù della citata normativa.

Art. 10
Incarico a Responsabile esterno del trattamento

10.1 Ai sensi degli articoli 4 e 28 del GDPR, il Comune di Rocca di Papa titolare del trattamento di cui all'art. 2 (di seguito "Titolare"), individua FIT quale responsabile del trattamento dei dati personali (di seguito "Responsabile").

10.2 La formalizzazione e l'efficacia dell'incarico di Responsabile esterno del trattamento è subordinata alla sottoscrizione da parte di FIT e del Comune dell'Accordo per il trattamento dei dati personali di cui all'allegato 2.

Art. 11
Risoluzione delle controversie

11.1 Le parti si impegnano a risolvere amichevolmente qualsiasi controversia dovesse insorgere tra loro nel corso della vigenza dell'accordo o in dipendenza di esso. In caso di mancato componimento, il foro competente è quello di _____.

Letto, confermato e sottoscritto.

Per il Comune di Rocca di Papa_____

Per FIT il Presidente Nazionale Cav. Uff. Giovanni Risso

ALL. 1 alla Convenzione
PROGETTO TECNICO

Documento Tecnico Novabox

Nome file	Documento Tecnico Novabox
Preparato da	Giuseppe Sciascia
Data salvataggio	16/12/2021
Ultima revisione	16/12/2021

Indice

Sommario

1 DESCRIZIONE GENERALE DELLA SOLUZIONE

Il seguente documento descrive la realizzazione di un servizio di integrazione tra i WebServices messi a disposizione dall'Anagrafe Nazionale Popolazione Residente (ANPR) del Ministero dell'interno e la Piattaforma Novares.

Questa applicazione, sviluppata da Novares, sarà installata all'interno del Novabox che Novares spedirà presso la sede dell'ente Comunale il quale avrà accesso esclusivo. Il software sarà totalmente gestito dal Comune, sia come configurazione iniziale (quindi inserimento del certificato di postazione e relativa password) sia in termini di controllo e tracciatura dei log.

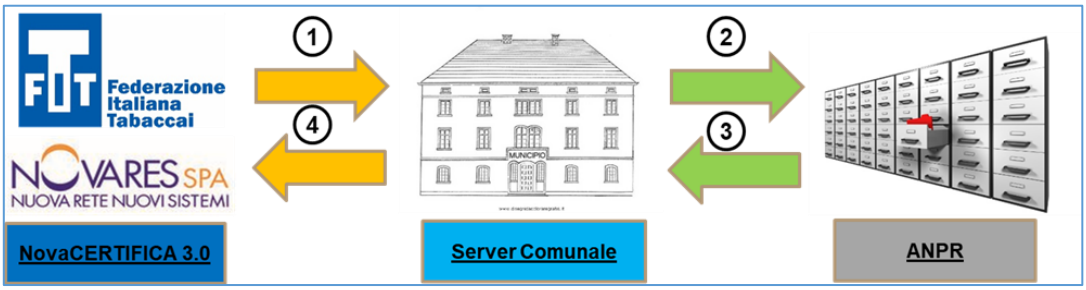
L'appliance sarà preconfigurata e all'interno ospita l'applicativo sviluppato seguendo le linee guida di Anpr, il quale interrogherà i servizi di ANPR ogni qualvolta un cittadino richiedere un certificato in una tabaccheria convenzionata del vostro Comune.

L'appliance interrogherà Anpr in base alle chiamate ricevute dalla nostra infrastruttura e inserite nel PortaleNovares (web application utilizzata dai tabaccai), la comunicazione tra Novares e l'appliance presente nella vostra infrastruttura comunale sarà gestita da una VPN tramite un client già preconfigurato.

Il Novabox farà da Gateway tra ANPR e Novares, questo ci permette di attivare il servizio senza necessità di cedere le credenziali privati di ANPR.
L'applicativo si interfaccia ad ANPR dalla rete del comune e si collega in VPN al Portale Novares (la piattaforma utilizzata dai tabaccai per emettere i certificati).
La vpn verso la nostra infrastruttura sarà gestita direttamente dal server.
La suddetta integrazione ha i seguenti obiettivi:

- permettere di creare un'istanza del servizio per ogni Comune aderente, in conformità ai termini di utilizzo delle API ANPR
- semplificare le API SOAP ANPR esponendo degli endpoint REST/JSON
- semplificare l'autenticazione al servizio implementando il SSO e fungendo da proxy verso l'implementazione WS-Security/SAML implementata nelle API ANPR
- normalizzare l'output delle API ANPR presentando i dati in un formato più attuale quale il JSON

2 SCHEMA ESEMPLIFICATIVO



1. Il cittadino richiede il certificato in tabaccheria
2. Il tabaccaio accede al portale Novares ed effettua la richiesta.
3. Il portale Novares invia una richiesta di emissione del certificato al software installato presso il comune.
4. Il software presente in comune recepisce la richiesta e si interfaccia al database di Anpr accedendo con le proprie credenziali.
5. Anpr risponde generando il certificato.
6. Il software presso il comune invia il certificato al portale Novares.
7. Il tabaccaio può scaricare e stampare il certificato da consegnare al cittadino.

3 DETTAGLI TECNICI HARDWARE

Il Novabox è una piccola appliance (dimensioni 8.8 x 5.8 x 2 cm), basata su sistema operativo Unix, che dovrà semplicemente essere collegata all'alimentazione e alla rete del comune.

4 DESCRIZIONE DEL SERVIZIO – LATO COMUNE

Nel microservizio deployato nel Novabox risiederanno anche i dati di autenticazione verso ANPR (credenziali) che non sarà possibile in nessun modo estrarre, neanche accedendo fisicamente al filesystem.
Il microservizio è stato realizzato utilizzando il linguaggio Java alla versione 1.8 e il framework spring-boot-starter-tomcat alla versione 2.3.4.
I servizi verranno eseguiti con l'utenza amministrativa root.

4.0 VARIABILI D'AMBIENTE

Sarà possibile definire una variabile d'ambiente denominata

- ANPR_HOME

Questa variabile conterrà il path all'interno del quale saranno depositati i certificati e il file di database H2. Qualora la variabile non venga definita il sistema userà il path di default (/anpr_home).
N.B. Ovviamente, essendo il filesystem dei container volatile, se la variabile non fosse definita o il path non fosse montato su di un volume persistente, ad ogni riavvio del container le configurazioni andranno perse.

4.1 PANNELLO DI CONFIGURAZIONE

L'applicazione concessa in uso al comune consente la parametrizzazione tramite una interfaccia web, nello specifico un pannello realizzato tramite l'impiego del framework Angular e consentirà la configurazione di ciascuna istanza del microservizio.
Tale configurazione riguarderà i seguenti aspetti funzionali del servizio (il dettaglio di questa configurazione sarà presente nel Manuale Novabox che sarà inviato contestualmente alla spedizione dello stesso):

- **Credenziali di accesso al servizio ANPR:**
  - certificato CA
    - Del certificato verrà presentato solo il timestamp della versione presente nel filesystem in modo da poterla distinguere in caso di aggiornamento
    - Sarà possibile caricare un nuovo certificato sovrascrivendo il precedente
  - password certificato CA
  - ID operatore
  - ID sede
  - ID postazione
  - certificato postazione
    - Del certificato verrà presentato solo il timestamp della versione presente nel filesystem in modo da poterla distinguere in caso di aggiornamento
    - Sarà possibile caricare un nuovo certificato sovrascrivendo il precedente
  - PIN certificato postazione
- **Impostazioni sicurezza:**
  - cambio password di amministrazione

4.2 ENDPOINT ESPOSTI

4.2.1 Endpoint ANPR

Saranno esposti due endpoint di integrazione ai servizi ANPR

- **POST** /certificazione
- **GET** /consultazione/scheda_individuale/{codice_fiscale}

In conformità all'interfaccia definita per la versione precedente del servizio consultabile al seguente indirizzo:
https://generator.swagger.io/?url=https://lab.link.it/nardi/anpr.yaml
L'accesso a tali endpoint avverrà tramite l'utilizzo di token JWT rilasciato dal SSO.

4.2.2 Endpoint di servizio

Saranno esposti 6 endpoint di servizio a disposizione della web application di gestione del microservizio:

- **POST** /manager/api/login
- **POST** /manager/api/registrazione
- **PUT** /manager/api/credenziali (Autenticato)
- **GET** /manager/api/isConfig
- **GET** /manager/api/config (Autenticato)
- **PUT** /manager/api/config (Autenticato)

Tali servizi avranno lo scopo di permettere, tramite l'utilizzo dell'applicazione Angular, di configurare il microservice impostando tutti i parametri necessari all'interazione con le API ANPR e Novares.
L'accesso a tali endpoint sarà autorizzato tramite l'invio di token JWT rilasciato dal microservice stesso relativamente alle informazioni di login inserite dall'operatore al momento del setup iniziale.

4.3 SERVIZIO DI DISCOVERY

Dal momento che sarà istanziato uno o più microservices per ciascun comune aderente e non più una unica istanza centralizzata sarà necessario avere un elenco aggiornato in "tempo reale" di tutte le istanze attive e i relativi indirizzi a cui esse sono raggiungibili al fine di instradare correttamente le richieste di certificato provenienti dalla piattaforma Novares.
Per ottenere questo risultato il microservice, una volta completata la configurazione, interrogherà periodicamente un servizio esposto dalla piattaforma Novares fornendo una struttura dati contenente:

- Codice Comune
- Descrizione del Comune
- Codice Postazione
- Indirizzo Ip del servizio
- Porta del servizio

4.4 SICUREZZA DEI DATI E LOG

Tutti i dati di configurazione inseriti dall'operatore tramite la pagina di amministrazione saranno salvati in forma crittografata su di un database H2 locale al servizio tramite algoritmo di cifratura AES.
Non sarà possibile in nessun modo estrarre i dati di autenticazione verso ANPR, neanche accedendo fisicamente al filesystem del container.

Il database è H2 (database locale su file senza rdmbs stile sqlite). Il path sarà definito nella variabile d'ambiente ANPR_HOME (attualmente è /opt/anpr/ANPR_HOME però si può cambiare a piacimento) il database è cifrato in AES-128 a chiave simmetrica, e per non dover sbloccare manualmente il db ad ogni avvio la password è hardcoded nel codice dell'applicazione.

La durata della conservazione viene stabilità dal comune dall'interfaccia web nell'apposito tab (si rimanda al Manuale Novabox).

5 VPN

Come anticipato pocanzi, l'applicativo utilizza un tunnel VPN per interfacciarsi al Portale Novares (la piattaforma utilizzata dai tabaccai per emettere i certificati).
La vpn verso l'infrastruttura Novares sarà gestita direttamente dal server.

5.0 PREREQUISITI

Al fine di instaurare correttamente il tunnel VPN IPSec occorre abilitare in uscita le porte udp 500 e 4500 verso la destinazione vpn.novares.it .

5.1 SPECIFICHE VPN

Il tunnel VPN instaurato è di tipologia dialup IPSec con PSK e Xauth.
In tabella sono elencate le specifiche del tunnel VPN:

Phase 1	
Encryption	AES128
Authentication	SHA256
DH Group	5
Key Lifetime	86400
Phase 2	
Encryption	AES128
Authentication	SHA256
PFS	enabled
DH Group	5
Key Lifetime	86400
Key Lifetime	43200

Il tunnel vpn è instaurato automaticamente non appena il server è abilitato a raggiungere la destinazione vpn.novares.it .
E' necessario preventivamente verificare che il box dalla vostra rete possa raggiungere:

1. L'indirizzo pubblico dei sevizi di ANPR https://ws.anpr.interno.it da un ip pubblico abilitato allo stesso
2. L'indirizzo 185.8.36.68 porte udp 500 e 4500 necessario per instaurare il tunnel vpn verso Novares

Il Novabox collegato alla rete del comune dovrà essere posizionato in un luogo sicuro con accesso ristretto al solo personale autorizzato e attestato in una DMZ in modo tale da consentire la sola raggiungibilità ai servizi di Anpr e alla vpn di Novares.

ALL. 2

Accordo per il trattamento dei dati personali

Tra

Comune di_____**,** in persona del suo legale rappresentante pt, _____, nato a _____ il _____, C.F. _____, ubicata per la carica presso il Palazzo comunale di _____;

e

FEDERAZIONE ITALIANA TABACCAI, con sede legale in Roma, Via Leopoldo Serra n. 32, C.F. e P. IVA 00992981001, nella persona del suo legale rappresentante pt. e Presidente Nazionale: Cav. Uff. Giovanni Risso

Comune di _____ e Federazione Italiana Tabaccai sono di seguito indicate anche, rispettivamente, come "Comune" e "FIT", ovvero "Titolare" e "Responsabile", e singolarmente, come "Parte" e, nell'insieme, come "Parti".

premesso che:

a) Il presente accordo regola l'affidamento del trattamento di dati personali previsto all'art. 10 della "*Convenzione per la promozione e la realizzazione del servizio di estrazione e stampa di certificati anagrafici presso gli esercizi associati alla Federazione Italiana Tabaccai*" stipulata in data _____ in ragione della quale FIT cura per conto del Comune di _____ i profili tecnici, informatici ed organizzativi relativi ai servizi previsti dall'art. 2 comma 1 della convezione richiamata (di seguito Convenzione);
b) Il Comune di _____, nell'ambito dei servizi sopra richiamati per i quali si avvale dei servizi di FIT di cui alla Convenzione, tratta i dati personali dei propri residenti e pertanto è identificata nella Convenzione quale Titolare del trattamento (di seguito "Titolare"),
c) Ai fini dell'esecuzione della Convenzione, ai sensi e per gli effetti di cui all'articolo 10, comma 1 della medesima Convenzione, il Comune di _____, in qualità di Titolare, ha individuato FIT, che ha accettato, quale Responsabile del trattamento (di seguito "Responsabile");
d) Le Parti, ai sensi del comma 2 dell'art. 10 della Convenzione, intendono disciplinare in dettaglio le modalità del trattamento dei dati personali affidato dal Titolare al Responsabile, attraverso la redazione del presente accordo denominato "*Accordo per il trattamento di dati personali*" (di seguito "Accordo") che, una volta sottoscritto dalle Parti, è parte integrante della Convenzione;
e) FIT, in qualità di Responsabile, dichiara di possedere esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate atte a garantire la conformità del trattamento alla normativa in materia di tutela dei dati personali e degli interessati.

Tutto quanto sopra premesso, le Parti come in epigrafe rappresentate

CONVENGONO E STIPULANO

quanto segue:

Art. 1 – Valore delle premesse e degli allegati

Le premesse e gli allegati ivi richiamati sono da considerarsi parte integrante e sostanziale del presente Accordo.

Art. 2 - Oggetto

2.1 Le presenti clausole stabiliscono istruzioni e modalità del trattamento dei dati personali affidato dal Titolare del trattamento al Responsabile del trattamento ai sensi dell'art. 28 del Regolamento Generale per la Protezione dei Dati personali dell'Unione Europea n. 2016/679 (di seguito anche RGPD o GDPR).

2.2 Le specifiche e i dettagli del trattamento sono riportati nell'Allegato 2.a - Specifiche del trattamento di dati personali affidato al responsabile (di seguito "Allegato 2.a") che costituisce parte integrante e sostanziale del presente Accordo.

Si evidenzia comunque che qualsiasi uso dei dati personali oggetto del trattamento non è consentito per scopi che non siano previsti nel presente Accordo o comunque non funzionali al trattamento in oggetto e alle istruzioni del Titolare. È altresì vietata qualsiasi forma di profilazione sui dati personali trattati.

Art. 3 – Durata

Il presente Accordo e la connessa nomina di FIT quale Responsabile rimangono in vigore fino alla cessazione della Convenzione, indipendentemente dalla causa di detta cessazione.

Art. 4 - Garanzie

4.1. Il Responsabile, tenendo conto della natura, dell'ambito di applicazione, delle finalità del trattamento, della tipologia di dati personali trattati, delle categorie di interessati nonché dei rischi per i diritti e le libertà delle persone fisiche, si impegna nei confronti del Titolare a:

I. trattare i dati personali nel rispetto dei principi e delle disposizioni previsti dal GDPR, dagli indirizzi e dai provvedimenti a carattere generale emanati dall'Autorità Garante per la protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali.
II. trattare dati personali attenendosi alle istruzioni documentate fornite dal Titolare. Sono considerate istruzioni documentate le prescrizioni previste dalla Convenzione, dai suoi allegati e dal presente Accordo comprensivo dei relativi

allegati, ed ogni altra comunicazione scritta del Titolare sulle modalità di trattamento dei dati da parte del Responsabile. Il Responsabile garantisce che nel caso rilevasse un profilo di illegittimità nelle istruzioni conferite dal Titolare segnalerà prontamente e per iscritto gli elementi ritenuti illegittimi al Titolare non dando luogo alle istruzioni medesime fino a nuova e legittima definizione delle istruzioni. A tale scopo Titolare e Responsabile comunicano reciprocamente che il rispettivo Responsabile della protezione dei dati - DPO:

- Per il comune di _____ è il responsabile incaricato dal Comune con Delibera di Giunta;
- Per FIT è Veris Servizi S.r.l., contattabile all'indirizzo dpo@tabaccai.it e via PEC all'indirizzo dpo@pec.tabaccai.it;

III. Garantire che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza dei dati personali trattati e siano state adeguatamente formate in materia di protezione dei dati personali e sullo specifico trattamento oggetto dell'incarico;

IV. Adottare le misure tecniche ed organizzative previste all'art.3 della Convenzione, oltre a quelle di cui all'art. 32 del GDPR e quelle specificate nell'apposita sezione dell'allegato 2a, nonché assistere il Titolare nell'implementazione delle ulteriori misure di sicurezza che si rendessero necessarie;

V. Provvedere formalmente alla nomina dei propri amministratori di sistema, ove previsto, secondo il provvedimento del Garante italiano per la protezione dei dati personali del 27 novembre 2008 e s.m.i., e che l'elenco aggiornato degli amministratori di sistema è a disposizione del Titolare;

VI. Non trasferire, né in tutto né in parte, in un Paese Terzo i dati personali trattati.

Art. 5 - Ricorso a sub-responsabili

5.1 Ai fini di cui all'art. 2 comma 1 della Convenzione, il Titolare conferisce sin d'ora al Responsabile autorizzazione generale a ricorrere ad altri responsabili del trattamento (di seguito, "sub-responsabili").A tal fine il Responsabile terrà a disposizione del titolare un elenco aggiornato dei sub-responsabili incaricati.

5.2 Il Responsabile si impegna a ricorrere esclusivamente a soggetti che presentino le necessarie garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dal GDPR.

5.3 Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

5.4 Nell'affidare il trattamento o parte di esso a sub-responsabili il Responsabile utilizzerà un atto giuridico che impone i medesimi obblighi di sicurezza e protezione dei dati personali contenuti nel presente Accordo.

5.5 Il Responsabile si impegna a supportare tempestivamente il Titolare per qualunque richiesta da parte degli interessati che richieda il coinvolgimento del Responsabile e dei

sub-Responsabili per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR.

Art. 6 - Sicurezza

6.1 Il Responsabile supporterà il Titolare nel garantire il rispetto degli obblighi di cui agli artt. dal 32 al 36 del Regolamento UE 2016/679.

6.2 In caso di violazione dei dati (Data Breach) o supposta tale, il Responsabile informa il Titolare, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, anche qualora la violazione avvenga nella sfera di controllo di un suo eventuale sub-responsabile, mediante la comunicazione a _____, contenente almeno una descrizione della natura della violazione di dati personali, delle probabili conseguenze della violazione e delle misure proposte o adottate dal Responsabile per porvi rimedio e, se del caso, per attenuarne i possibili effetti negativi. Il Responsabile inoltre collabora attivamente con il Titolare per l'individuazione di rimedi, oltre che per gli obblighi di comunicazione verso l'Autorità di Controllo e/o gli Interessati, ai sensi dell'art. 34 del GDPR.

6.3 Al termine del Trattamento il Responsabile restituirà i dati personali eventualmente detenuti al Titolare concordando per iscritto le modalità di restituzione o in alternativa, su istruzione del Titolare, distruggerà tali dati.

Qualora il Responsabile ritenga di dover conservare copia dei dati affidatigli per eventuali obblighi di legge o tutela giuridica, dovrà adottare le misure di sicurezza necessarie indicate dal Titolare (che possono comprendere cifratura e pseudonimizzazione, se necessario) e cancellare e/o distruggere i dati all'esaurimento della finalità. La distruzione o cancellazione avverranno dando al Titolare opportuna evidenza formale.

6.4 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di conformità al Regolamento UE 2016/679 e consente le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato, singolarmente o congiuntamente ad altri Titolari, e comunque alla presenza di un incaricato del Responsabile. Tali ispezioni devono compiersi con modalità tali da:

A. Non pregiudicare la sicurezza e la riservatezza dei dati (e dei relativi trattamenti) dei quali sono "titolari" il Responsabile ovvero altri Titolari;
B. Non interferire con il normale e corretto svolgimento dell'attività del Responsabile;
C. Non pregiudicare la riservatezza dell'organizzazione aziendale e commerciale del Responsabile.

6.5 Il Responsabile si impegna a tenere presso di sé il registro dei trattamenti effettuati per conto del Titolare e a mantenerlo aggiornato.

Art. 7 - Varie

7.1 Il presente Accordo sostituisce tutti i precedenti accordi o intese, anche verbali, in vigore fra le Parti in relazione al medesimo oggetto.

7.2 Qualsiasi modifica del presente Accordo, nonché eventuali integrazioni o eliminazioni, devono essere concordate per iscritto da entrambe le Parti.

7.3 Per quanto non espressamente previsto dalla presente Accordo, si fa espresso riferimento alla normativa, sia europea sia nazionale, in materia di protezione dei dati personali nonché alla Convenzione.

Roma, lì _____

Comune di _____ **FEDERAZIONE ITALIANA TABACCAI**

All. 2.a

SPECIFICHE DEL TRATTAMENTO DI DATI PERSONALI AFFIDATO AL RESPONSABILE

Trattamento

Di seguito vengono esposte le finalità di trattamento per le attività oggetto della Convenzione "Convenzione per la promozione e la realizzazione del servizio di estrazione e stampa di certificati anagrafici presso gli esercizi associati alla Federazione Italiana Tabaccai" tra il Comune di _____ (per brevità Comune) e la Federazione Italiana Tabaccai (per brevità FIT), per le quali FIT agisce in qualità di responsabile del trattamento:

Natura e finalità del trattamento

1. *Registrazione del richiedente e della richiesta di certificato presso l'esercizio convenzionato;*
2. *Erogazione di certificati anagrafici ai cittadini richiedenti per conto del Comune.*

Categorie di interessati

1. Persone che richiedono certificati anagrafici relativi alle medesime o a terzi;
2. Persone i cui dati compaiono nei certificati anagrafici emessi.

Dati personali trattati

I dati personali trattati sono di varia natura e comprendono le categorie identificate per tipologia di interessato, di seguito esposte.

Dati del richiedente il certificato:

1. Dati anagrafici (nome, cognome, luogo e data di nascita, sesso, codice fiscale);
2. Estremi del documento di identità
3. Tipologia di certificato richiesto.

Dati presenti nei certificati emessi relativi al/ai soggetto/i presente/i nei certificati richiesti:

1. Dati anagrafici;
2. Dati di residenza;
3. Dati relativi allo stato civile;
4. Altri dati eventualmente contenuti nelle varie tipologie di certificati anagrafici gestiti.

Operazioni di trattamento consentite

Sono consentite al Responsabile, nell'ambito delle finalità del trattamento, tutte le operazioni necessarie ai fini della corretta gestione delle finalità specificate e della relativa sicurezza dei dati trattati in termini di riservatezza, integrità, disponibilità e resilienza. In particolare,

- per quanto riguarda la finalità 1:
  a) Raccolta dei dati del richiedente in un apposito formulario presente nel Portale dedicato che viene compilato e stampato (a cura della tabaccheria) e

conservazione del medesimo per un periodo di mesi sei dalla data di compilazione, presso la tabaccheria; il Portale consente la conservazione informatica, con accesso limitato, dei dati inseriti ai fini della stampa del formulario, per finalità di controllo e per un tempo di mesi sei dalla data della richiesta;

b) Conservazione dei formulari cartacei di cui al punto precedente in maniera sicura e riservata;
c) Distruzione dei formulari scaduti (la scadenza è riferita ai sei mesi dalla data di compilazione).

- per quanto riguarda la finalità 2:
  d) Richiesta del certificato anagrafico della persona fisica e degli eventuali famigliari mediante accesso a banca dati messo a disposizione dal Comune;
  e) Messa a disposizione del certificato presso la tabaccheria ove è ne stata effettuata la richiesta;
  f) Stampa del certificato presso la tabaccheria richiedente;
  g) Cancellazione entro e non oltre le ore 24 di ogni giorno da tutti i sistemi informatici coinvolti nella gestione della richiesta, compreso il terminale della tabaccheria, dei certificati anagrafici in formato PDF generati a seguito di richiesta.

1. Misure di sicurezza

Di seguito vengono elencate le misure di sicurezza generali richieste alla Federazione Italiana Tabaccai.

➢ Misure di sicurezza organizzative

Policy e Regolamenti utenti – Il Responsabile applica dettagliate policy e regolamenti ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.

Autorizzazione accessi logici – Il Responsabile definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

Gestione interventi di assistenza – Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali.

Valutazione d'impatto sulla protezione dei dati (DPIA) – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione

d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Responsabile ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento.

Incident Management – Il Responsabile ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.

Data Breach – Il Responsabile ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Titolare.

Formazione: Il Responsabile eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento, corsi di formazione sulla corretta gestione dei dati personali.

Data Center – L'accesso fisico al Data Center è limitato ai soli soggetti aderenti.

Vigilanza – Durante gli orari di chiusura degli uffici è attivo un servizio di vigilanza.

Armadi – la documentazione cartacea riservata viene conservata in appositi armadi chiusi a chiave e le cui chiavi sono in possesso del solo personale autorizzato.

- **Misure di sicurezza tecniche**

Firewall, IDPS - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention mantenuti aggiornati in relazione alle migliori tecnologie disponibili.

Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Responsabile protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.

Protezione nei confronti del malware – I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica.

Credenziali di autenticazione – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi: codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di

autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave; caratteristica biometrica dell'utente, eventualmente associata a un codice identificativo o a una parola chiave.

Parola chiave – Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle *best practices*. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.

Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi da parte delle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.

Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Eliminazione dei dati - Il Responsabile si obbliga alla cancellazione e alla distruzione immediata dei backup obsoleti eventualmente in suo possesso non più utili per le attività di supporto.

Videosorveglianza - Il Data Center dispone di un impianto di videosorveglianza.