

MINISTERO DELL'INTERNO

DECRETO 27 agosto 2025

Modalita' di accesso ai servizi di certificazione resi disponibili dall'Anagrafe nazionale della popolazione residente nella Piattaforma digitale nazionale dati, per consentire ai notai di richiedere certificati anagrafici per finalita' connesse all'esecuzione dell'incarico professionale, tramite il Consiglio nazionale del notariato. (25A05561)

(GU n.239 del 14-10-2025)

IL MINISTRO DELL'INTERNO

di concerto con

IL MINISTRO
PER LA PUBBLICA AMMINISTRAZIONE

e con

IL SOTTOSEGRETARIO DI STATO
ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI
con delega all'innovazione tecnologica

Vista la legge 24 dicembre 1954, n. 1228, recante «Ordinamento delle anagrafi della popolazione residente»;

Vista la legge 27 ottobre 1988, n. 470, recante «Anagrafe e censimento degli italiani all'estero»;

Vista la legge 7 agosto 1990, n. 241, recante «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi»;

Vista la legge 15 dicembre 1999, n. 482, recante «Norme in materia di tutela delle minoranze linguistiche storiche»;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale (di seguito CAD);

Visto il decreto del Presidente della Repubblica 30 maggio 1989, n. 223, recante «Approvazione del nuovo regolamento anagrafico della popolazione residente»;

Vista la legge 18 giugno 2009, n. 69, recante «Delega al Governo in materia di atto pubblico informatico redatto dal notaio»;

Vista il decreto legislativo 2 luglio 2010, n. 110, recante «Disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'art. 65 della legge 18 giugno 2009, n. 69»;

Vista la legge 16 febbraio 1913, n. 89, recante «Ordinamento del notariato e degli archivi notarili» e successive modificazioni;

Visto il regio decreto-legge 23 ottobre 1924, n. 1737, convertito dalla legge 18 marzo 1926, n. 562, recante «Norme complementari per

l'attuazione del nuovo ordinamento degli archivi notarili»;

Vista la legge 3 agosto 1949, n. 577, recante «Istituzione del Consiglio nazionale del notariato e modificazioni alle norme sull'amministrazione della Cassa nazionale del notariato» e successive modificazioni;

Visto il regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE;

Visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;

Visto il decreto del Presidente della Repubblica 30 maggio 2002, n. 115, recante «Testo unico delle disposizioni legislative e regolamentari in materia di spese di giustizia»;

Visto il decreto del Presidente del Consiglio dei ministri 23 agosto 2013, n. 109, «Regolamento recante disposizioni per la prima attuazione dell'art. 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'art. 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe nazionale della popolazione residente (di seguito ANPR)»;

Visto il decreto del Presidente del Consiglio dei ministri 10 novembre 2014, n. 194, «Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente»;

Visto il decreto del Ministro dell'interno del 3 novembre 2021, recante «Modalità di richiesta e rilascio dei certificati anagrafici in modalità telematica attraverso l'Anagrafe nazionale della popolazione residente»;

Visto il decreto del Ministro per l'innovazione tecnologica e la transizione digitale del 22 settembre 2022, recante «Obblighi e termini di accreditamento alla Piattaforma digitale nazionale dati (di seguito PDND)»;

Visto il decreto del Ministro dell'interno 6 ottobre 2023, recante l'aggiornamento dei servizi resi disponibili dall'Anagrafe nazionale della popolazione residente di cui all'art. 62, comma 3 del decreto legislativo 7 marzo 2005, n. 82, al fine di consentire agli avvocati iscritti nel relativo albo o elenco di cui all'art. 15, comma 1, lettere a) e b), della legge 31 dicembre 2012, n. 247 di richiedere, per finalità connesse all'esecuzione del mandato professionale, i certificati anagrafici in modalità telematica resi disponibili tramite l'ANPR;

Visto decreto del Ministro dell'interno 12 dicembre 2023, con il quale il Ministero ha reso disponibile su PDND il servizio di rilascio delle certificazioni anagrafiche per consentire a Poste Italiane S.p.A. l'emissione di certificati presso lo sportello degli uffici postali aderenti al progetto «POLIS» - Case dei servizi di cittadinanza digitale di cui all'art. 38 del decreto-legge 17 maggio 2022, n. 50 con modificazioni, dalla legge 15 luglio 2022, n. 91;

Viste le linee guida sulla formazione, gestione e conservazione dei documenti informatici adottate dall'Agenzia per l'Italia digitale (AgID) con determinazione n. 407 del 9 settembre 2020 e aggiornate con determinazione n. 371 del 17 maggio 2021;

Viste le linee guida sull'infrastruttura tecnologica della piattaforma digitale nazionale dati per l'interoperabilità dei sistemi informativi e delle basi di dati adottate dall'AgID ai sensi dell'art. 50-ter, comma 2, ultimo periodo del CAD, con determinazione n. 627 del 15 dicembre 2021 e modificate con determinazione n. 26 del 3 febbraio 2022;

Considerata la necessità dei notai iscritti al ruolo di cui all'art. 24 della legge 16 febbraio 1913, n. 89, di richiedere i certificati anagrafici dei cittadini iscritti nell'ANPR per finalità

connesse all'esecuzione dell'incarico professionale;

Considerato che, il Consiglio nazionale del notariato, attraverso la rete unitaria del notariato, garantisce un sistema sicuro di autenticazione, consentendo, ai soli notai in esercizio, di fruire di servizi resi disponibili dalla medesima rete;

Sentito il Consiglio nazionale del notariato per gli ambiti di competenza;

Sentito il Garante per la protezione dei dati personali, che ha reso il parere di competenza con provvedimento n. 314 del 4 giugno 2025;

Sentita la Conferenza Stato-città ed autonomie locali, che ha reso il parere di competenza il 24 luglio 2025;

Acquisito il concerto del Ministro per la pubblica amministrazione e del Sottosegretario di Stato alla Presidenza del Consiglio dei ministri con delega all'innovazione tecnologica;

Decreta:

Art. 1

Oggetto

1. Il presente decreto disciplina le modalità di accesso ai servizi di certificazione resi disponibili dall'Anagrafe nazionale della popolazione residente nella piattaforma digitale nazionale dati (di seguito PDND), al fine di consentire ai notai iscritti al ruolo di cui all'art. 24 della legge 16 febbraio 1913, n. 89, di richiedere, tramite la Rete unitaria del notariato (di seguito RUN), gestita dal Consiglio nazionale del notariato (di seguito CNN), per finalità connesse all'esecuzione dell'incarico professionale, i certificati anagrafici individuati nell'allegato 1 «Accesso ai servizi, misure di sicurezza e tracciamento in ANPR ed elenco certificati anagrafici», che forma parte integrante del presente decreto, fatto salvo quanto previsto dalle disposizioni dalla legge 31 ottobre 1955, n. 1064.

2. Sono inibite al notaio le funzioni di consultazione diretta dei dati anagrafici nonché di estrazione di elenchi di iscritti.

Art. 2

Servizi dell'ANPR per i notai

1. Il Ministero dell'interno ed il CNN sono rispettivamente erogatore e fruitore dei servizi afferenti all'ANPR messi a disposizione tramite la PDND del Dipartimento per la trasformazione digitale di cui all'art. 50-ter del CAD.

2. La verifica dell'iscrizione del notaio al ruolo di cui all'art. 24 della legge n. 89 del 1913 è garantita dal CNN ed eventualmente interrogabile mediante appositi servizi resi fruibili per il tramite della piattaforma di cui all'art. 50-ter del CAD.

3. Il CNN mette a disposizione, attraverso la Rete unitaria del notariato (RUN), al notaio una interfaccia applicativa, in una specifica sezione, per la fruizione del servizio di rilascio dei certificati di cui all'allegato 1, previa identificazione informatica con credenziali di livello di sicurezza almeno significativo.

4. Il certificato è reso immediatamente disponibile al notaio che lo ha richiesto per il tramite di un colloquio applicativo le cui informazioni tecniche di implementazioni sono conformi a quanto espressamente indicato per i fruitori degli e-service esposti sulla PDND ed in conformità a quanto indicato nell'allegato 2 del presente decreto.

5. I certificati sono richiesti dal notaio per finalità connesse all'esecuzione dell'incarico professionale e sono esenti dall'imposta di bollo ai sensi dell'art. 18, comma 1, del decreto del Presidente della Repubblica 30 maggio 2002, n. 115.

6. Il CNN consente ai notai in esercizio di richiedere i certificati necessari a garantire lo svolgimento delle attività professionali, in un numero non superiore a trenta certificati al giorno per ogni notaio.

7. Ogni sei mesi, tramite procedura automatizzata, l'ANPR, estrae

un campione di notai individuati prevalentemente tra quelli che hanno richiesto oltre cento certificati nel semestre, nonché sulla base dei criteri ulteriori che sono individuati dal Ministero dell'interno, anche tenendo conto degli esiti delle verifiche precedenti, e resi pubblici sul sito internet www.anagrafenazionale.interno.it Il campione è corredato delle registrazioni relative agli accessi e alle operazioni compiute dal singolo notaio, comprensive di codice fiscale del notaio, data e ora degli accessi, numero dei certificati richiesti, esito delle operazioni e identificativo di sessione.

8. Il campione, di cui al precedente comma 7, è inviato dal Ministero dell'interno al CNN. Il CNN od il responsabile del trattamento di cui all'art. 3, comma 8, del presente decreto, lo trasmette, per le verifiche in ordine alla sussistenza dei presupposti fissati dal presente decreto ai fini della legittimità degli accessi, ai Consigli notarili distrettuali competenti per l'esercizio dei compiti di vigilanza di cui agli articoli 93 e 93-bis della legge n. 89 del 1913. L'esito della verifica è trasmesso dal Consiglio notarile distrettuale al CNN che ne dà comunicazione, a mezzo posta elettronica certificata, al Ministero dell'interno, nel termine di sei mesi dalla trasmissione del campione. In mancanza di esito positivo il servizio è sospeso nei confronti dei notai oggetto della verifica.

9. Le specifiche tecniche di accesso all'ANPR per il tramite della piattaforma PDND sono reperibili all'indirizzo <https://docs.pagopa.it> Nell'allegato 1 sono descritte le misure di sicurezza e le modalità di tracciamento effettuate da ANPR. La lista dei certificati che possono essere richiesti dal notaio è altresì definita nello stesso allegato 1, che forma parte integrante del presente decreto.

10. Le misure di sicurezza e le modalità di tracciamento effettuate dal CNN, sono contenute nell'allegato 2 (disciplinare tecnico) del presente decreto.

Art. 3

Trattamento dei dati personali

1. Il Ministero dell'interno è titolare del trattamento dei dati contenuti nell'ANPR per le finalità di conservazione, di comunicazione e di adozione delle relative misure di sicurezza nonché dei dati necessari alle verifiche di cui all'art. 2, comma 7 e 8, ed all'adozione delle conseguenti misure.

2. Il CNN è titolare del trattamento dei dati connessi alla gestione della infrastruttura RUN e del trattamento dei dati dei notai che utilizzano la RUN, sia ai fini della verifica dell'iscrizione al ruolo di cui all'art. 24 della legge n. 89/1913 che dell'identificazione informatica per l'accesso alla piattaforma.

3. Il CNN e i consigli notarili distrettuali trattano i dati necessari a svolgere le verifiche previste dal presente decreto in qualità di autonomi titolari del trattamento, ciascuno per le proprie competenze.

4. Fermo restando quanto previsto dai commi 2 e 3 del presente articolo, il CNN, attraverso la società Notartel S.p.a. - S.B., è altresì responsabile del trattamento dei dati relativi ai diversi servizi erogati dalla RUN ai singoli notai, incluso quello di accesso ai certificati di ANPR tramite la PDND, ai sensi dell'art. 28 del GDPR, per conto di ciascun notaio che aderisce al servizio. Il notaio procede, in tal senso, a nominare il CNN responsabile del trattamento, al momento della registrazione all'interno dell'infrastruttura RUN. La società Notartel S.p.a. - S.B., per le medesime finalità di cui sopra, svolge il ruolo di sub-responsabile del trattamento del CNN e viene autorizzata dal notaio, per il tramite della medesima nomina a responsabile.

5. I notai trattano i dati personali contenuti nei certificati ad essi rilasciati da ANPR, in qualità di autonomi titolari del trattamento, per svolgere le proprie funzioni, nel rispetto delle norme del regolamento UE 2016/679 e del decreto legislativo n. 101/2018.

6. Il CNN conserva fino ad un massimo di trentasei mesi le informazioni relative alle richieste effettuate dal notaio secondo le

modalita' definite dall'allegato 2 «Disciplinare tecnico», fatte salve esigenze di conservazione ulteriore in caso di eventuali contenziosi.

7. La societa' generale di informatica S.p.a. (Sogei S.p.a.), incaricata della gestione dell'infrastruttura ANPR, e' designata dal Ministero responsabile del trattamento dei dati ai sensi dell'art 3, comma 4, del decreto del Presidente del Consiglio dei ministri n. 194/2014.

8. La societa' di informatica del notariato (Notartel S.p.a. - S.B.), incaricata dal CNN della realizzazione del progetto e della gestione dell'infrastruttura RUN, e' designata dal CNN responsabile del trattamento dei dati ai sensi dell'art. 28 del regolamento (UE) 2016/679.

Art. 4

Disposizioni di attuazione e finali

1. Il presente decreto e il relativo allegato sono pubblicati nel sito internet www.anagrafenazionale.interno.it del Ministero dell'interno.

2. In caso di evoluzione delle caratteristiche, della disponibilita' e/o necessita' di ulteriori certificati, nonche' delle modalita' tecniche dei servizi di cui agli allegati 1 «Accesso ai servizi, misure di sicurezza e tracciamento in ANPR ed elenco certificati anagrafici» e 2 «Disciplinare tecnico», sara' aggiornato con decreto del competente direttore centrale del Ministero dell'interno, sentiti il Garante per la protezione dei dati personali e il CNN.

3. All'attuazione delle disposizioni di cui al presente decreto, si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

4. Il presente decreto e' inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 27 agosto 2025

Il Ministro dell'interno
Piantedosi

Il Ministro
per la pubblica amministrazione
Zangrillo

Il Sottosegretario di Stato
alla Presidenza del Consiglio dei ministri
con delega all'innovazione tecnologica
Butti

Registrato alla Corte dei conti l'8 ottobre 2025

Ufficio di controllo sugli atti del Ministero dell'interno e del Ministero della difesa, reg. n. 3902

Parte di provvedimento in formato grafico

Allegato 1 Accesso ai servizi, misure di sicurezza e tracciamento in ANPR, elenco certificati anagrafici.

SOMMARIO

1. ACCESSO AI SERVIZI DI ANPR
 - 1.1 RICHIESTA DEI CERTIFICATI
 - 1.2 SCELTA DEL CERTIFICATO
 - 1.3 FORMAZIONE ED EMISSIONE DEL CERTIFICATO
 - 1.4 CONTRASSEGNO
 - 1.5 VERIFICA DEL CERTIFICATO TRAMITE CONTRASSEGNO SUL SITO ANPR
 - 1.6 ESENZIONE DALL'IMPOSTA DI BOLLO
2. MISURE DI SICUREZZA E TRACCIAMENTO IN ANPR

- 2.1 INTEGRITA' E RISERVATEZZA DEI DATI ANPR
- 2.2 SICUREZZA DEI SERVIZI E DELL'ACCESSO AD ANPR
- 2.3 TRACCIAMENTO IN ANPR DELLE OPERAZIONI EFFETTUATE
- 3. ELENCO CERTIFICATI

1. ACCESSO AI SERVIZI DI ANPR

1.1 RICHIESTA DEI CERTIFICATI

Il notaio che intende richiedere i certificati anagrafici lo fa tramite un portale reso disponibile dal CNN che richiama il servizio di certificazione di ANPR e che consente:

- di inserire gli elementi identificativi del soggetto del quale il notaio intenda richiedere il certificato (obbligatoriamente NOME, COGNOME, CODICE FISCALE, LINGUA, TIPOLOGIA DI CERTIFICATO, MOTIVO DELLA RICHIESTA);
- di ottenere il certificato digitale.

Il notaio e' informato del fatto che le dichiarazioni rese ai sensi del decreto del Presidente della Repubblica n. 445 del 2000, in ordine alla sussistenza del mandato professionale necessarie alla richiesta dei certificati, saranno oggetto delle previste verifiche da parte del Consiglio Nazionale del Notariato e dei Consigli notarili distrettuali territorialmente competenti nell'ambito dei compiti di vigilanza ad essi demandati e delle conseguenze di eventuali esiti negativi dei controlli effettuati.

1.2 SCELTA DEL CERTIFICATO

Il notaio puo' scegliere il tipo di certificato che intende richiedere. Il certificato puo' essere richiesto in una delle lingue disponibili ai sensi delle disposizioni in materia delle minoranze linguistiche e storiche.

I certificati possono essere richiesti anche in forma contestuale, come previsto dal DPR n. 445/2000.

Nel caso in cui il certificato non possa essere rilasciato ai sensi di legge, verra' restituito un apposito codice di errore.

1.3 FORMAZIONE ED EMISSIONE DEL CERTIFICATO

A seguito della conferma di emissione da parte del richiedente, il portale CNN fa una chiamata al servizio di certificazione ANPR che produce il certificato in formato pdf che riporta:

- il logo del Ministero dell'Interno e la dicitura: "Anagrafe Nazionale della Popolazione Residente";
- il contrassegno;
- il sigillo elettronico cosi' come previsto dall'articolo 62, comma 3, del CAD;
- la dicitura: "Il presente certificato e' rilasciato al notaio che ne ha fatto richiesta per finalita' connesse all'esecuzione del proprio mandato professionale".

In caso di mancata emissione del certificato, verra' restituito un apposito codice di errore.

1.4 CONTRASSEGNO

Ai sensi dell'art. 23, comma 2-bis, del CAD, al fine di verificare la conformita' della copia analogica del certificato all'originale informatico, ANPR appone sulla predetta copia analogica un contrassegno che consente di visualizzare l'originale informatico munito di sigillo elettronico.

1.5 VERIFICA DEL CERTIFICATO TRAMITE CONTRASSEGNO SUL SITO ANPR

Per i soggetti in possesso di una copia analogica dotata di

contrassegno del certificato prodotto da ANPR, ANPR prevede una specifica funzione per verificare la corrispondenza con il certificato digitale tramite lettura del QR-code apposto sulla predetta copia, mediante:

a) smartphone

- l'accesso alla pagina WEB e' effettuato automaticamente;
- il richiedente deve inserire il captcha suggeritogli dall'applicazione web;
- con il pulsante Conferma si attiva la verifica e, in caso di esito positivo, l'applicazione web apre il certificato corrispondente alle informazioni reperite dal QR-code.

b) PC

- il richiedente deve scannerizzare il QR-code ed effettuare l'upload dell'immagine;
- il richiedente deve inserire il captcha suggeritogli dall'applicazione web;
- con il pulsante Conferma si attiva la verifica e, in caso di esito positivo, l'applicazione web apre il certificato corrispondente alle informazioni reperite dal QR-code.

L'applicazione di verifica legge il QR-code che contiene il link (URL) che permette di risalire, sul portale ANPR, all'esatta copia digitale del certificato, la quale potra' essere verificata con confronto visivo rispetto alla copia cartacea e garantita dalla presenza del sigillo elettronico del Ministero dell'Interno. L'accesso alla funzionalita' sopra descritta e' presente nell'area pubblica del sito web di ANPR.

1.6 ESENZIONE DALL'IMPOSTA DI BOLLO

I certificati richiesti dal notaio tramite il servizio sono rilasciati esenti dall'imposta di bollo ai sensi dell'articolo 18, comma 1, del decreto del Presidente della Repubblica 30 maggio 2002, n. 115.

2. MISURE DI SICUREZZA E TRACCIAMENTO IN ANPR

Le misure di sicurezza per l'erogazione dei servizi di cui al presente decreto sono quelle previste dall'allegato C "Misure di sicurezza" del decreto del Presidente del Consiglio dei ministri n. 194 del 2014 e successive integrazioni, secondo cui l'infrastruttura di sicurezza a supporto del sistema ANPR garantisce:

- l'integrita' e la riservatezza dei dati;
- la sicurezza dei servizi e dell'accesso ad essi;
- il tracciamento delle operazioni effettuate;
- il sistema dei controlli a presidio dei processi per la corretta erogazione dei certificati anagrafici.

2.1 INTEGRITA' E RISERVATEZZA DEI DATI ANPR

L'integrita' (la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali oppure effettuate volontariamente da una terza parte) e il non ripudio (condizione secondo la quale non si puo' negare la paternita' e la validita' del dato) sono garantiti dall'apposizione di firma ai messaggi scambiati nell'interazione tra il portale del CNN e il sistema ANPR, secondo le modalita' previste dalle vigenti "Linee Guida sull'interoperabilita' tecnica delle Pubbliche Amministrazioni" sopra richiamate. La riservatezza dell'accesso ai dati, invece, e' garantita dai meccanismi implementati dalla PDND relativi al controllo e alla tracciabilita' degli accessi applicativi eseguiti dal portale del CNN verso i servizi esposti dal sistema ANPR.

La cifratura del canale contribuisce ulteriormente a garantire la riservatezza dei dati in transito nell'interazione tra le due suddette piattaforme.

2.2 SICUREZZA DEI SERVIZI E DELL'ACCESSO AD ANPR

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilit , si utilizzano le seguenti tecnologie o procedure:

- a) Aggiornamenti periodici dei sistemi operativi e dei software di sistema, hardening delle macchine.
- b) Adozione di una infrastruttura di sistemi firewall e sistemi IPS (Intrusion Prevention System) che consentono la rilevazione dell'esecuzione di codice non previsto e l'esecuzione di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante.
- c) Esecuzione di WAPT (Web Application Penetration Test), per la verifica della presenza di eventuali vulnerabilit  sul codice sorgente.
- d) Adozione del captcha sull'applicazione web di controllo del QR-code e di sistemi di rate-limit sui web services che limitano il numero di transazioni nell'unit  di tempo, al fine di mitigare il rischio di accesso automatizzato alle applicazioni che genererebbe un traffico finalizzato alla saturazione dei sistemi e quindi al successivo blocco del servizio.
- e) Sono previsti sistemi di backup e disaster recovery per i log di accesso applicativo. Tali sistemi sono previsti anche per i dati, in quanto la perdita delle informazioni registrate pregiudica l'utilizzo e l'efficienza dei servizi, e non permette di raggiungere le finalit  stesse dei servizi.
- f) Nel rispetto del DPCM n. 194 del 2014 dove   prevista una federazione tra Enti, il fruitore (CNN) predispone un token di sicurezza firmato contenente i seguenti attributi:
 - codice identificativo del notaio richiedente;
 - identificativo univoco del client (IPADDRESS);
 - modalit  di autenticazione (LoA_3/SPID_L2).

2.3 TRACCIAMENTO IN ANPR DELLE OPERAZIONI EFFETTUATE

Il sistema ANPR registra gli accessi ai servizi da parte del CNN e l'esito delle operazioni.

Per ciascuna transazione effettuata sono registrati i seguenti dati relativi alla richiesta del servizio e all'esito dell'operazione:

- informazioni derivanti dal token di sicurezza di cui al paragrafo 3.2, lett. f);
- codice fiscale del cittadino e/o dei componenti della famiglia anagrafica;
- data-ora-minuti-secondi-millisecondi della richiesta;
- operazione richiesta;
- esito della richiesta;
- identificativo della richiesta;
- modalit  di autenticazione.

I log degli accessi cos  descritti sono storicizzati e sono conservati fino a un anno on line e storicizzati per 2 anni.

I file di log registrano le informazioni riguardanti le operazioni, per la verifica della correttezza e legittimit  del trattamento dei dati. I file di log presentano le caratteristiche di integrit  e inalterabilit , e sono protetti con idonee misure contro ogni uso improprio.

3. ELENCO CERTIFICATI

Elenco dei certificati di cui   consentita la richiesta e relative finalit :

- Anagrafico di nascita: per l'acquisizione dei dati anagrafici esatti delle parti dell'atto;
- Anagrafico di matrimonio: per l'accertamento dell'esistenza di matrimonio delle parti dell'atto;
- Di cittadinanza: per la scelta delle leggi applicabili e per la richiesta di agevolazioni fiscali;
- Di esistenza in vita: per la verifica dell'esistenza in vita di

- eventuali usufruttuari non intervenuti in atto;
- Di residenza: per la richiesta di agevolazioni fiscali;
 - Di residenza AIRE: per la richiesta di agevolazioni fiscali;
 - Di stato civile: per l'individuazione dello stato civile delle parti dell'atto;
 - Di stato di famiglia: per l'individuazione della composizione delle famiglie, necessaria per gli atti, le formalita' e le dichiarazioni di successione;
 - Di stato di famiglia AIRE: per l'individuazione della composizione delle famiglie, necessaria per gli atti, le formalita' e le dichiarazioni di successione;
 - Anagrafico di unione civile: per l'accertamento dell'esistenza dell'unione civile delle parti dell'atto;
 - Di contratto di convivenza: per l'accertamento dell'esistenza di un contratto di convivenza delle parti dell'atto;
 - Di morte: per la trascrizione dell'accettazione dell'eredita' (art.2660 cod. civ.).

Parte di provvedimento in formato grafico

Disciplinare Tecnico - Allegato 2

Data:18/06/2025

Sommario

1. Premessa
2. Modalita' di integrazione dei servizi ANPR con le applicazioni CNN
3. Modalita' di identificazione/autenticazione/profilazione degli utenti
4. Modalita' di tracciamento dell'utilizzo del servizio da parte dell'utenza
5. Misure per la sicurezza delle informazioni
 - 5.1. Struttura logica e infrastruttura di protezione logica e fisica
 - 5.1.1. Protezione fisica
 - 5.1.2. Protezione logica
 - 5.2. Componenti e architettura del sistema
 - 5.2.1. Componenti hardware
 - 5.2.2. Componenti di rete e connettivita'
 - 5.2.3. Monitoraggio del sistema
 - 5.3. Procedura di gestione delle copie di sicurezza dei dati
 - 5.4. Procedura di gestione dei disastri
 - 5.5. Analisi dei rischi e contromisure
 - 5.6. Modalita' di verifica dell'applicazione del piano di sicurezza

1. Premessa

Il presente disciplinare tecnico descrive:

- le modalita' di integrazione dei servizi ANPR con le applicazioni rese disponibili ai Notai dal CNN;
- le modalita' di identificazione/autenticazione/profilazione degli utenti che accedono al servizio;
- le modalita' di tracciamento dell'utilizzo del servizio da parte dell'utenza;
- le misure di sicurezza applicate dal CNN per la gestione del servizio ANPR;

per la consultazione del "Servizio Certificazioni Anagrafiche".

La gestione tecnico-informatica e' affidata alla societa' Notartel S.p.A - S.B. Societa' Informatica del Notariato del Consiglio Nazionale del Notariato.

2. Modalita' di integrazione dei servizi ANPR con le applicazioni CNN

La modalita' di integrazione tra servizi ANPR e applicazione resa dal CNN, all'interno del portale Rete Unitaria del Notariato (RUN), prevede:

- L'implementazione di pattern di sicurezza prescritti dalle linee guida sull'interoperabilit  tecnica definiti da AGID detti: INTEGRITY_REST_02 e AUDIT_REST_02 e ricompresi sulla piattaforma PDND.
- La creazione di un token per fruire dei servizi indicati, utilizzando la chiave pubblica corrispondente a quella privata indicata nel client censito sulla piattaforma PDND.

In figura schema concettuale di funzionamento di interrogazione API e schema di principio della architettura generale:

Parte di provvedimento in formato grafico

3. Modalita' di identificazione/autenticazione/profilazione degli utenti

Gli utenti sono notai iscritti al ruolo di cui all'art.24 della legge n. 89 del 1913 il cui stato di servizio e' eventualmente interrogabile attraverso Albo Unico online, di cui e' disponibile l'interrogazione web sul sito www.notariato.it oppure attraverso API dedicate.

Il notaio e' accreditato alla RUN (Rete Unitaria del Notariato) attraverso un processo di registrazione standard. I servizi disponibili nella RUN sono accessibili ai notai come supporto nell'esercizio della professione notarile.

Le credenziali fornite ai notai vengono rilasciate e gestite attraverso un sistema di Identity and Access Management (IAM). Questo sistema e' stato implementato per la gestione degli accessi e delle identita' degli utenti, assicurando che l'accesso alle applicazioni e ai servizi sia controllato e monitorato.

Il sistema IAM garantisce che l'utente autenticato sia effettivamente la persona identificata durante il processo di onboarding iniziale, assicurando che solo utenti correttamente profilati e autorizzati possano accedere ai servizi e alle risorse richiesti.

All'interno della RUN e' resa disponibile una sezione dedicata all'accesso ai servizi ANPR, in cui e' richiesta un'autenticazione/identificazione con livello di garanzia almeno "sostanziale", in conformita' al Regolamento (UE) n. 910/2014 (eIDAS).

Tale identificazione puo' avvenire mediante SPID, CIE o altri strumenti di identificazione elettronica riconosciuti conformi e notificati ai sensi del regolamento eIDAS, garantendo un livello di sicurezza equivalente.

In sintesi, l'accesso ai servizi ANPR tramite la RUN avviene attraverso:

- una prima autenticazione alla RUN, con mantenimento della sessione mediante cookie;
- una seconda autenticazione, conforme al livello di garanzia "sostanziale" di cui al Regolamento eIDAS, per l'accesso al servizio specifico ANPR.

Il servizio di interrogazione dell'ANPR e' classificato nelle Access Control List del sistema IAM per tutti gli aspetti di controllo e monitoraggio

4. Modalita' di tracciamento dell'utilizzo del servizio da parte dell'utenza

La tracciabilita' delle operazioni effettuate sulla interfaccia applicativa della RUN e' gestita dal sistema di logging applicativo.

Su questo sistema vengono monitorate le seguenti attivita':

- Autenticazione e Accesso: ogni accesso dell'utente viene registrato con relativo esito (successo o fallimento).

Il tracciamento copre l'autenticazione e le operazioni eseguite dagli utenti, includendo:

- Data e ora dell'evento;
- Identificazione Utente (username, ID sessione);

I log applicativi sono conservati per 36 mesi nel sistema di Log Management centralizzato, che garantisce la sicurezza, il monitoraggio e la conformita' alle policy di sicurezza.

5. Misure per la sicurezza delle informazioni

Il sistema tecnologico della Notartel e' conforme alle regole e alle disposizioni in materia di sicurezza informatica: in particolare la societa' e' certificata ISO 27000.

Di seguito riportate, per macro punti, le caratteristiche salienti dei sistemi di sicurezza informatica e fisica.

5.1. Struttura logistica e infrastruttura di protezione logica e fisica

Le apparecchiature per l'esercizio dei servizi applicativi sono fisicamente ubicate presso i datacenter Notartel nelle sedi in Roma in Via Gravina 4 e in Via Flaminia 160 e in replica nel "SuperNap" (sito di Disaster Recovery) in Via Marche, 8/10, 27010 Siziano PV.

5.1.1. Protezione fisica

I perimetri fisici di sicurezza riguardano gli edifici di Via Flaminia e di via Gravina situati in Roma (sedi della Societa') e le parti del data center del provider di disaster recovery.

I perimetri sono sorvegliati per mezzo di apposite telecamere collegate a sistemi di video sorveglianza.

Tutte le porte perimetrali sono controllate da appositi sensori antintrusione e possono essere aperte per mezzo di appositi badge in dotazione al personale autorizzato. Relativamente alle aree dei data center eventuali ospiti, fornitori o comunque persone estranee possono accedere solo se accompagnate, per tutta la durata della loro presenza, da personale Notartel autorizzato e comunque dotate di badge.

Le sale server sono dotate di:

- sistemi di rilevazione incendi e fumo;
- sistemi di estinzione automatica degli incendi;
- sistemi antintrusione costituiti da porte e finestre di sicurezza;
- sistemi di allarme, antieffrazione e antintrusione.

La gestione degli apparati e' assicurata dal sistema di monitoraggio Notartel.

N.B.: La sicurezza perimetrale degli ambienti di disaster recovery e' affidata a SUPERNAP ITALIA azienda a cui e' stato affidato il contratto di housing per il sito di Disaster Recovery.

5.1.2. Protezione logica

L'infrastruttura dei sistemi per le interfacce applicative per i servizi di consultazione dell'ANPR e' collocata all'interno della rete di Front-End della RUN protetta da Firewall e da bilanciatore di carico. Attraverso regole FW ad hoc il servizio puo' raggiungere le parti in Back-End.

La disponibilita' logica delle funzioni e dei dati e' garantita da un sistema di accesso ridondato in tutte le sue componenti.

I sistemi operativi e i DBMS mantengono file di log con gli accessi per le verifiche periodiche ed eventuali ispezioni.

5.2. Componenti e architettura del sistema

5.2.1. Componenti hardware

Le componenti computazionali hardware sono implementate con sistemi server blade di produttori primari e virtualizzate tramite soluzioni di maggior diffusione e affidabilita'.

5.2.2. Componenti di rete e connettivita'

I componenti di rete sono elencati in maniera sintetica appena di seguito:

- connettivita' ridondata per ogni sistema in rete;
- infrastruttura di networking ridondata;
- connettivita' esterna Internet su Autonomous System (AS)

attraverso tre Provider con ridondanza su percorsi fisici differenti con banda a 1Gbps;

- cablaggio strutturato in cat.6E ridondato (fino a 10Gbps);
- apparati di connettività LAN Switch in Load Balancing e High Availability;
- LAN Front-End protetta da Firewall (IPS) e Bilanciatori (DMZ).

5.2.3. Monitoraggio del sistema

Calendari di verifica settimanale provvedono ai principali controlli:

- il backup dei log;
- l'analisi delle performance e dell'utilizzo del sistema;
- il monitoraggio della disponibilità del sistema;
- il monitoraggio degli aggiornamenti di sicurezza del sistema.

5.3. Procedura di gestione delle copie di sicurezza dei dati

E' previsto il backup per tutti i dati presenti sul server, secondo la seguente modalità:

1. quotidianamente viene effettuato un backup completo di tutti i dati del sistema;
2. il database archivia i log delle transazioni in tre siti su supporti fisici differenti;
3. tramite i backup effettuati giornalmente ed i log transazionali e' sempre possibile ripristinare l'intero sistema all'ultima transazione;
4. il database e' costantemente replicato su un sistema in standby rapidamente ripristinabile;
5. tutti i componenti dell'infrastruttura sono ridondati e ne viene effettuato un backup giornalmente, tramite due sistemi di backup indipendenti;
6. i sistemi di backup sono replicati su dispositivi posti in ambienti separati.

5.4. Procedura di gestione dei disastri

Le procedure di gestione dei disastri sono parte integrante delle misure adottate da Notartel per la certificazione ISO 27001 (copia dei certificati e' disponibile sul sito internet di Notartel).

5.5. Analisi dei rischi e contromisure

Notartel dispone di un gruppo interno di specialisti sulla sicurezza delle informazioni che si occupano del monitoraggio dei sistemi e della gestione degli incidenti di sicurezza oltre la valutazione dei rischi e la revisione dell'efficacia dei controlli e delle contromisure adottati.

Notartel applica una valutazione ragionata del livello di sicurezza della propria infrastruttura relativamente ai suoi aspetti tecnologici e fisici; ha operato la scelta dei propri Datacenter in conformita' con le prescrizioni e le best practices ISO27001, ISO27017 e ISO27018 in materia di sicurezza delle informazioni.

La struttura tecnologica viene analizzata rispetto ai fattori di rischio e sottoposta a tutti gli interventi correttivi necessari per garantirne il livello di sicurezza.

5.6. Modalita' di verifica dell'applicazione del piano di sicurezza

Le modalità di verifica dell'applicazione del Piano della Sicurezza sono parte integrante delle misure adottate da Notartel per le certificazioni ISO 27001, ISO 27017 e ISO 27018 (copia dei certificati e' disponibile sul sito internet di Notartel).