

## MINISTERO DELL'INTERNO

DECRETO 8 novembre 2016.

**Procedure per il trattamento dei dati, da parte della banca dati del DNA e del laboratorio centrale per la banca dati nazionale del DNA, e per la trasmissione del profilo del DNA da parte dei laboratori di istituzioni di elevata specializzazione, in attuazione degli articoli 3, 4 e 6 del decreto del Presidente della Repubblica 7 aprile 2016, n. 87.**

IL MINISTRO DELL'INTERNO

DI CONCERTO CON

IL MINISTRO DELLA GIUSTIZIA

Vista la legge 1° aprile 1981, n. 121, recante «Nuovo ordinamento dell'amministrazione della pubblica sicurezza»;

Vista la legge del 15 dicembre 1990, n. 395, recante «Ordinamento del Corpo di polizia penitenziaria»;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»;

Vista la legge 30 giugno 2009, n. 85, di adesione della Repubblica italiana al Trattato di Prüm, e in particolare l'art. 5, che istituisce presso il Ministero dell'interno, Dipartimento della pubblica sicurezza, la banca dati nazionale del DNA, e presso il Ministero della giustizia, Dipartimento dell'amministrazione penitenziaria, il laboratorio centrale per la banca dati nazionale del DNA;

Visto il decreto del Presidente della Repubblica 7 aprile 2016, n. 87, recante «Disposizioni di attuazione della legge 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, ai sensi dell'art. 16 della legge 30 giugno 2009, n. 85», e in particolare:

l'art. 3, comma 9, il quale dispone che con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia, sentito il Garante per la protezione dei dati personali, sono definiti i profili di autorizzazione, le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni relativi alla banca dati nazionale del DNA;

l'art. 4, comma 5, il quale dispone che con il decreto di cui all'art. 3, comma 9, sono specificati i profili di autorizzazione, le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni relativi al laboratorio centrale per la banca dati nazionale del DNA;

l'art. 4, comma 6, il quale dispone che con il decreto di cui all'art. 3, comma 9, sono definite le regole per la registrazione degli accessi ai locali e agli armadi del laboratorio centrale per la banca dati nazionale del DNA adibiti alla conservazione dei campioni biologici e degli elettroferogrammi, effettuati dagli operatori abilitati e in possesso di apposite chiavi di accesso;

l'art. 6, comma 7, il quale dispone che con il decreto di cui all'art. 3, comma 9, sono definite le regole per la trasmissione del profilo del DNA da parte delle istituzioni di elevata specializzazione, per via telematica, verso il laboratorio della Forza di polizia individuata dall'Autorità giudiziaria;

Visto il decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, 6 agosto 2015, con il quale è stata istituita, nell'ambito della Direzione centrale della polizia criminale, Servizio per il sistema informativo interforze, la Divisione quarta, cui sono attribuite le competenze relative alla banca dati nazionale del DNA;

Visto il decreto del Ministro della giustizia 2 marzo 2016, con il quale è stato istituito, nell'ambito della Direzione generale dei detenuti e del trattamento, l'Ufficio VI, cui sono attribuite le competenze relative al Laboratorio Centrale per la banca dati nazionale del DNA;

Ritenuto di dare attuazione al disposto di cui ai richiamati articoli: 3, comma 9, 4, commi 5 e 6 e 6, comma 7, del decreto del Presidente della Repubblica 7 aprile 2016, n. 87;

Udito il parere del Garante per la protezione dei dati personali in data 28 luglio 2016;

Decreta:

Art. 1.

*Oggetto e ambito di applicazione*

1. Il presente decreto definisce i profili di autorizzazione, le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni relativi alla banca dati nazionale del DNA collocata presso il Ministero dell'interno, Dipartimento della pubblica sicurezza, Servizio per il sistema informativo interforze della Direzione centrale della polizia criminale.

2. Il presente decreto definisce, altresì, i profili di autorizzazione e le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni relativi al sistema LIMS del laboratorio centrale per la banca dati nazionale del DNA, collocato presso il Ministero della giustizia, Dipartimento dell'amministrazione penitenziaria, Direzione generale dei detenuti e del trattamento, nonché le regole per la registrazione degli accessi ai locali e agli armadi del laboratorio centrale per la banca dati nazionale del DNA adibiti alla conservazione dei campioni biologici e degli elettroferogrammi effettuati dagli operatori abilitati e in possesso di apposite chiavi di accesso.

3. Il presente decreto delinea, inoltre, le regole per la trasmissione del profilo del DNA da parte delle istituzioni di elevata specializzazione, per via telematica, verso il laboratorio della Forza di polizia individuata dall'Autorità giudiziaria.

Art. 2.

*Definizioni*

1 Ai fini del presente decreto e degli allegati, si intende per:

a) «Regolamento», il decreto del Presidente della Repubblica 7 aprile 2016 n. 87, recante «Disposizioni di attuazione della legge 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, ai sensi dell'art. 16 della legge 30 giugno 2009, n. 85»;

b) «Codice», il Codice in materia di protezione dei dati personali, adottato con il decreto legislativo 30 giugno 2003, n. 196;

c) «Garante», il Garante per la protezione dei dati personali;

d) «BDN-DNA», la banca dati nazionale del DNA, istituita dall'art. 5, comma 1, della legge n. 85 del 2009;

e) «Laboratorio centrale», il laboratorio centrale per la banca dati nazionale del DNA, istituito dall'articolo 5, comma 2, della legge n. 85 del 2009;

f) «S.S.I.I.», il Servizio per il sistema informativo interforze della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza;



g) «SCIP», il Servizio per la cooperazione internazionale di polizia della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza;

h) «HTTPS» (*HyperText Transfer Protocol over Secure Socket Layer*), il protocollo di trasmissione dati sottoposto a procedure di crittografia;

i) «SSO» (*Single Sign-On*), la procedura di accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi informativi;

j) «IPSec» (*Internet Protocol Security*), la collezione di protocolli che permettono lo scambio sicuro di informazioni a livello IP;

k) «LIMS» (*Laboratory Information Management System*), il sistema informativo idoneo a gestire i dati ed il flusso di lavoro di un laboratorio;

l) «operatore», l'agente o l'ufficiale di polizia giudiziaria, in servizio presso la banca dati nazionale del DNA, il laboratorio centrale per la Banca dati nazionale del DNA, i laboratori delle Forze di polizia, il Servizio per la cooperazione internazionale di polizia, gli Uffici/Comandi delle Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico, gli Uffici delle Forze di polizia che eseguono richieste di ricerca internazionale designato quale incaricato del trattamento ai sensi dell'art. 30 del decreto legislativo 30 giugno 2003, n. 196 e specificamente abilitato ad accedere al sistema informativo della banca dati nazionale del DNA o al LIMS del laboratorio centrale per la banca dati nazionale del DNA;

m) «profilo di autorizzazione», l'insieme delle informazioni univocamente associate ad un operatore che consente di individuare a quali funzionalità della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA l'operatore può accedere, nonché i trattamenti che il medesimo può effettuare;

n) «autenticazione informatica», l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'operatore;

o) «credenziali di autenticazione», i dati e i dispositivi in possesso dell'operatore, da questi conosciuti e ad esso univocamente correlati, necessari per l'autenticazione;

p) «autenticazione forte», il metodo di autenticazione che si basa sull'utilizzo di più credenziali di autenticazione;

q) «istituzioni di elevata specializzazione», i laboratori pubblici o privati che hanno metodi di prova accreditati a norma EN ISO/IEC 17025 per la tipizzazione del DNA da reperti biologici acquisiti nel corso di procedimenti penali, di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati;

r) «portale S.S.I.I.», il portale che consente l'accesso ai servizi offerti dal Servizio per il sistema informativo interforze della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza ed è l'unico punto di accesso al portale per lo scambio IXP;

s) «portale per lo scambio dati - IXP» (*Information eXchange Platform*), il portale messo a disposizione dal Servizio per il sistema informativo interforze della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza per le attività necessarie alla formazione del personale e per accedere ai servizi offerti dalla banca dati nazionale del DNA, ivi compreso lo scambio di dati per finalità di collaborazione internazionale di polizia;

t) «punto di contatto nazionale - SPOC», (*Single Point Of Contact*), l'Autorità nazionale designata per lo scambio di dati e per le finalità di cooperazione internazionale di polizia, individuata dall'art. 11, comma 1, del decreto del Presidente della Repubblica 7 aprile 2016,

n. 87, nel Servizio per la cooperazione internazionale di polizia della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza;

u) «CODIS» (*CCombined DNA Index System*), il software utilizzato per la gestione dei profili del DNA fornito dal *Federal Bureau of Investigation* (FBI);

v) «elettroferogramma», il risultato dell'analisi elettroforetica della sequenza di frammenti del DNA utilizzata per estrapolare il profilo del DNA;

w) «sito secondario remoto della BDN-DNA» (*Disaster Recovery - DR*), l'infrastruttura tecnologica per il salvataggio ed il ripristino dei dati, di rete, di replica del sito primario della banca dati nazionale del DNA;

x) «focal point», la persona incaricata della certificazione delle postazioni di lavoro (PdL) e della gestione operativa degli utenti (abilitazione, convalida e reset delle utenze).

### Art. 3.

#### *Procedure per il trattamento dei dati della BDN-DNA*

1. I profili di autorizzazione, le procedure di autenticazione informatica, di registrazione e di analisi degli accessi e delle operazioni relativi alla BDN-DNA, in attuazione dell'art. 3, comma 9, del regolamento, sono definiti nell'allegato A del presente decreto.

### Art. 4.

#### *Procedure per il trattamento dei dati del LIMS del Laboratorio centrale*

1. I profili di autorizzazione, le procedure di autenticazione informatica, di registrazione e di analisi degli accessi e delle operazioni relativi al LIMS del Laboratorio centrale, e le regole per la registrazione degli accessi ai locali e agli armadi adibiti alla conservazione dei campioni biologici e degli elettroferogrammi effettuati dagli operatori abilitati e in possesso di apposite chiavi di accesso, in attuazione dell'art. 4, commi 5 e 6, del regolamento, sono definiti nell'allegato B del presente decreto.

### Art. 5.

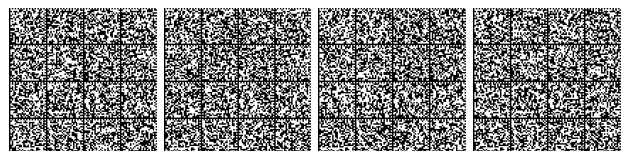
#### *Procedura per la trasmissione del profilo del DNA e dell'elettroferogramma da parte dei laboratori di istituzioni di elevata specializzazione*

1. Le regole per la trasmissione del profilo del DNA e dell'elettroferogramma da parte dell'istituzione di elevata specializzazione, per via telematica, verso il laboratorio della Forza di polizia individuata dall'Autorità giudiziaria, in attuazione dell'art. 6, commi 7 e 8, del regolamento, sono definite nell'allegato C del presente decreto.

### Art. 6.

#### *Clausola di invarianza finanziaria*

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti di cui al presente decreto con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.



Art. 7.

Entrata in vigore

1. Il presente decreto entra in vigore nel trentesimo giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.
2. La BDN-DNA entra in funzione dalla data di entrata in vigore del presente decreto.

Roma, 8 novembre 2016

Il Ministro dell'interno: ALFANO

Il Ministro della giustizia: ORLANDO

Registrato alla Corte dei conti il 22 novembre 2016  
Ufficio controllo atti Ministeri interno e difesa, reg.ne prev. n. 2144

ALLEGATO A

1. BANCA DATI NAZIONALE DEL DNA (BDN-DNA)

1.1 INFRASTRUTTURA GENERALE DEL SISTEMA INFORMATIVO

L'infrastruttura tecnologica (IT) della BDN-DNA prevede l'interconnessione con altri sistemi informativi attraverso una rete geografica.

Le reti informatiche delle Amministrazioni interessate utilizzano la Rete di Trasporto del Ministero dell'interno (VPN), il Sistema Pubblico di Connettività (SPC), collegamenti dedicati e la Rete Unificata Giustizia (RUG).

I canali di comunicazione sono soggetti a controllo di firewall alle due estremità.

La figura 1 illustra l'architettura IT del sistema informativo della BDN-DNA, i servizi offerti e i relativi utenti delle Forze di polizia.

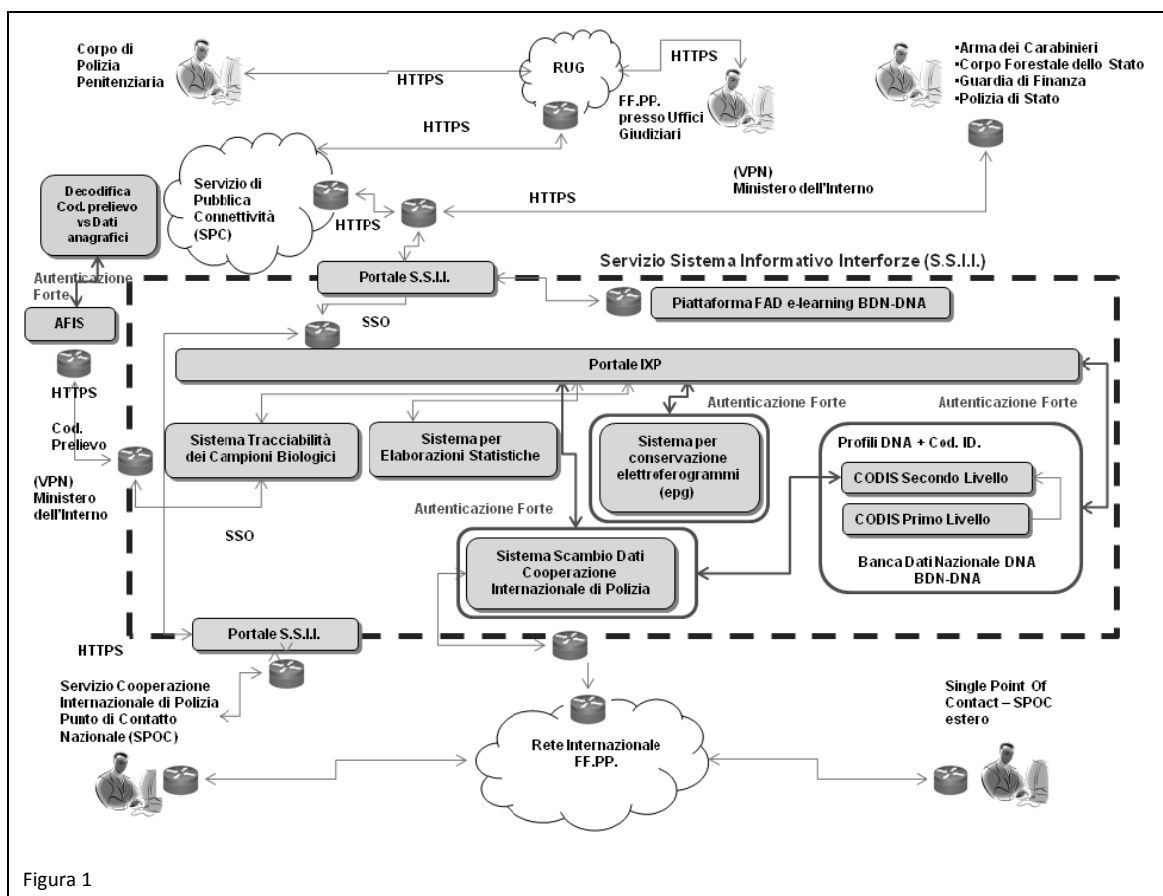


Figura 1





I servizi indicati nella figura 1 sono realizzati attraverso i sistemi di seguito elencati:

- portale S.S.I.I.;
- portale per lo scambio dati - IXP;
- piattaforma FAD *e-learning* BDN-DNA;
- sistema per la tracciabilità dei campioni biologici;
- sistema per le elaborazioni statistiche;
- sistema per la conservazione degli elettroferogrammi;
- sistema CODIS;
- sistema per lo scambio di dati di cooperazione internazionale di polizia.

Il portale S.S.I.I. consente l'accesso ai servizi offerti dal Servizio per il sistema informativo interforze ed è l'unico punto di accesso al portale per lo scambio dati - IXP.

Il portale per lo scambio dati - IXP consente l'accesso ai servizi offerti dalla BDN-DNA.

La piattaforma FAD *e-learning* BDN-DNA permette l'erogazione delle attività formative a distanza per l'acquisizione delle conoscenze necessarie agli operatori per l'espletamento dei compiti di incaricato del trattamento, le quali costituiscono condizione per il rilascio delle credenziali di accesso ai servizi.

Il sistema per la tracciabilità dei campioni biologici gestisce il flusso del campione biologico dal momento del prelievo fino all'arrivo al Laboratorio centrale ai fini della registrazione delle attività di cui all'articolo 12, comma 3 della legge n. 85 del 2009. Tale sistema acquisisce automaticamente dal sistema AFIS la data del prelievo e il codice del prelievo, unitamente ai dati dell'Ufficio AFIS che ha eseguito il prelievo, il protocollo SDI riguardante la motivazione del prelievo associata al reato di riferimento o alla denuncia di scomparsa, il sesso, la data, la provincia di nascita e la nazionalità del soggetto sottoposto a prelievo, anche ai fini delle elaborazioni statistiche. Gli operatori in servizio presso gli Uffici delle Forze di polizia abilitati alla procedura di prelievo del campione biologico o presso gli Uffici con funzione di punti di raccolta intermedi, possono associare solo il codice prelievo ai dati identificativi dell'Ufficio delle Forze di polizia che detiene il campione biologico fino al suo arrivo al Laboratorio centrale, incaricato della conservazione dei campioni biologici. Ai predetti operatori è vietato l'accesso alla funzionalità di AFIS che consente la decodifica del codice prelievo per acquisire i dati anagrafici della persona sottoposta a prelievo.

Il sistema per le elaborazioni statistiche permette di analizzare in forma aggregata i dati riguardanti i servizi offerti dalla BDN-DNA, per consentire al Ministro dell'interno di svolgere l'attività di informazione al Parlamento di cui all'articolo 19 della legge n. 85 del 2009.

Il sistema per la conservazione degli elettroferogrammi permette di raccogliere gli elettroferogrammi prodotti dai laboratori delle istituzioni di elevata specializzazione, i quali non possono accedere alla BDN-DNA. Tali laboratori trasmettono il profilo del DNA, il relativo elettroferogramma e i dati relativi alla motivazione definiti nell'allegato C del presente decreto, attraverso una applicazione Web gestita dal portale per lo scambio dati - IXP. Gli operatori in servizio presso i laboratori delle Forze di polizia individuati dall'Autorità giudiziaria per l'inserimento del profilo del DNA provvedono all'inserimento nel sistema CODIS, dell'elettroferogramma e dei dati della motivazione nel sistema per la conservazione degli elettroferogrammi.

Il sistema CODIS è una piattaforma software, organizzata su più livelli, fornita dal Federal Bureau of Investigation degli Stati Uniti (FBI) alla Direzione centrale della polizia criminale, Dipartimento della pubblica sicurezza del Ministero dell'interno, che permette di raccogliere, raffrontare e consultare i profili del DNA acquisiti da determinate categorie di persone e sulla scena del crimine. Il sistema consente, inoltre, di raccogliere e raffrontare, esclusivamente tra loro e per fini identificativi, i profili del DNA di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati.

Il sistema per lo scambio dati di cooperazione internazionale di polizia è utilizzato dal punto di contatto nazionale - SPOC, che a partire dalle richieste di consultazione della polizia giudiziaria, mediante un sistema di autenticazione forte trasmette ai punti di contatto esteri e riceve da questi i profili del DNA ai fini di consultazione e raffronto in banca dati per finalità di cooperazione transfrontaliera.

I servizi sopra illustrati, ad eccezione dell'applicazione Web fornita dalla BDN-DNA alle istituzioni di elevata specializzazione e da questi utilizzata per la trasmissione del profilo del DNA, del relativo elettroferogramma e dei dati relativi alla motivazione della trasmissione

ne ai laboratori delle Forze di polizia, sono tutti accessibili dal portale per lo scambio dati - IXP della BDN-DNA e sono usufruibili da parte dell'incaricato del trattamento dei dati previo superamento di una procedura di autenticazione e autorizzazione.

Ogni Amministrazione interessata ha la responsabilità della sicurezza della rete geografica di riferimento e condivide con il S.S.I.I. le scelte tecniche e le configurazioni delle interconnessioni.

#### 1.2 FUNZIONALITÀ DELLA BDN-DNA E RUOLI DEL PERSONALE ABILITATO ALL'ALIMENTAZIONE, CONSULTAZIONE E RAFFRONTO

La BDN-DNA, ai sensi dell'articolo 7 della legge n. 85 del 2009, svolge le attività di seguito elencate:

- a) raccolta del profilo del DNA dei soggetti di cui all'articolo 9, commi 1 e 2, della legge n. 85 del 2009;
- b) raccolta dei profili del DNA relativi a reperti biologici acquisiti nel corso di procedimenti penali;
- c) raccolta dei profili del DNA di persone scomparse o dei loro consanguinei, di cadaveri e resti cadaverici non identificati;
- d) raffronto dei profili del DNA a fini d'identificazione.

I profili del DNA di cui alla lettera a) sono tipizzati unicamente dal Laboratorio centrale. I profili del DNA di cui alle lettere b) e c) sono tipizzati dai laboratori delle Forze di polizia e, in particolare, per la Polizia di Stato dai laboratori presso il Servizio polizia scientifica della Direzione centrale anticrimine della Polizia di Stato - Dipartimento della pubblica sicurezza o presso i Gabinetti Interregionali o Regionali di Polizia Scientifica (GIPS/GRPS), per l'Arma dei Carabinieri dai laboratori presso i Reparti Investigazioni Scientifiche (RIS). I profili del DNA di cui alle lettere b) e c) possono essere tipizzati anche dai laboratori delle istituzioni di elevata specializzazione.

La BDN-DNA, ai sensi dell'articolo 7 del Regolamento, è alimentata dagli operatori in servizio presso il Laboratorio centrale o presso i laboratori delle Forze di polizia mediante inserimento per via telematica del profilo del DNA che hanno provveduto a tipizzare. L'inserimento dei profili del DNA tipizzati dai laboratori delle istituzioni di elevata specializzazione è effettuato dagli operatori in servizio presso il laboratorio delle Forze di polizia indicato dall'Autorità giudiziaria. I medesimi operatori - fatti salvi i casi espressamente indicati dal Regolamento all'articolo 7, comma 1, nei quali è prevista la cancellazione dalla BDN-DNA del profilo del DNA - possono trattare ulteriormente i dati solo per la verifica della corrispondenza con la sequenza numerica dell'elettroferogramma fornita dal Laboratorio centrale.

Il raffronto ai fini di identificazione di cui alla lettera d) è effettuato, ai sensi dell'articolo 9 del Regolamento, mediante consultazione a livello nazionale della BDN-DNA (ricerca e raffronto dei profili del DNA), da parte degli operatori in servizio presso la BDN-DNA e presso i laboratori delle Forze di polizia.

Titolare del trattamento dei dati registrati nella BDN-DNA, ai sensi dell'articolo 26 del Regolamento, è il Ministero dell'Interno - Dipartimento della Pubblica Sicurezza.

Responsabile del trattamento dei dati registrati nella BDN-DNA, ai sensi dell'articolo 26 del Regolamento, è il Direttore del S.S.I.I., che esercita le proprie funzioni senza facoltà di delega.

Il Responsabile del trattamento impartisce per iscritto agli incaricati del trattamento dei dati registrati nella BDN-DNA le istruzioni necessarie al corretto funzionamento della banca dati. Effettua, inoltre, controlli sulla osservanza delle disposizioni in materia di trattamento di dati personali, incluse quelle relative alla sicurezza, e verifiche periodiche, anche a campione, sulle operazioni di trattamento effettuate dagli operatori.

Il Responsabile del trattamento, in particolare, adotta le misure tecniche e di sicurezza per garantire la trasmissione sicura, realizzata attraverso canali criptati, del profilo del DNA e dell'elettroferogramma, ai sensi dell'articolo 6, commi 7, 8 e 9, del Regolamento.

Incaricati del trattamento, a livello nazionale, dei dati registrati nella BDN-DNA sono gli operatori in servizio presso la BDN-DNA (Divisione 4<sup>a</sup> del S.S.I.I.), presso il Laboratorio centrale, e presso i laboratori delle Forze di polizia e presso gli Uffici/Comandi della Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico, inclusi il Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., il Direttore dell'Ufficio del Laboratorio centrale, nonché i dirigenti/comandanti dei laboratori delle Forze di polizia e degli Uffici/Comandi delle Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico. Tali incaricati sono designati, ai sensi dell'articolo 30 del Codice, in base alla documentata preposizione alla BDN-DNA (Divisione 4<sup>a</sup> del



S.S.I.I.), al Laboratorio centrale, ai laboratori delle Forze di polizia, agli Uffici/Comandi della Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico da parte delle Amministrazioni di appartenenza. L'ambito del trattamento dei dati registrati nella BDN-DNA consentito agli operatori in servizio presso i suddetti uffici è individuato per iscritto in relazione alle attività svolte dalle unità organizzative di appartenenza dal Responsabile del trattamento (il Direttore del S.S.I.I.).

Gli incaricati del trattamento dei dati registrati nella BDN-DNA, ai sensi dell'articolo 30 del Codice, operano sotto la diretta autorità del Titolare (Dipartimento della Pubblica Sicurezza) e del Responsabile del trattamento (il Direttore del S.S.I.I.), attenendosi alle direttive e alle istruzioni dagli stessi impartite. Il dovere di attenersi alle predette direttive e istruzioni è connesso alla preposizione dell'incaricato all'unità organizzativa e a tal fine l'Amministrazione di appartenenza, con atto scritto contestuale alla assegnazione, ne impone espressamente l'osservanza.

Il Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., il Direttore dell'Ufficio del Laboratorio centrale, i dirigenti/comandanti dei laboratori delle Forze di polizia e degli Uffici/Comandi della Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico controllano che gli operatori gerarchicamente dipendenti osservino le disposizioni in materia di trattamento e rispettino le direttive e le istruzioni impartite dal Titolare o dal Responsabile del trattamento, anche sotto il profilo relativo alla sicurezza. A tal fine, svolgono verifiche periodiche, anche a campione, sulle operazioni di trattamento effettuate dagli operatori gerarchicamente dipendenti.

Incaricati del trattamento, a livello internazionale, dei dati registrati nella BDN-DNA sono gli operatori in servizio presso:

- il punto di contatto nazionale, individuato dall'articolo 11, comma 1, del Regolamento nel SCIP;
- gli Uffici delle Forze di polizia che eseguono richieste di ricerca internazionale tramite il punto di contatto nazionale - SPOC, inclusi i rispettivi dirigenti/comandanti.

Tali incaricati sono designati, ai sensi dell'articolo 30 del Codice, in base alla documentata preposizione ai suddetti Uffici/Reparti da parte delle Amministrazioni di appartenenza. L'ambito del trattamento consentito riguardo ai dati registrati nella BDN-DNA è individuato per iscritto, in relazione alle attività svolte dalle unità organizzative di appartenenza, dal Responsabile del trattamento (il Direttore del S.S.I.I.) per finalità di collaborazione internazionale di polizia.

### 1.3 MISURE DI SICUREZZA DELLA BDN-DNA

#### 1.3.1 LIVELLI DI SICUREZZA O DI GARANZIA NELL'AUTENTICAZIONE INFORMATICA DELLA BANCA DATI

La BDN-DNA, coerentemente con la partizione in due livelli del software per la gestione dei profili del DNA (articolo 3, commi 3 e 4, del Regolamento), adotta due livelli di sicurezza o garanzia (*Level of Assurance - LoA*) compatibili con la norma ISO-IEC 29115.

In particolare, la BDN-DNA definisce i seguenti livelli di sicurezza:

- livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115): a tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema di autenticazione a singolo fattore (*user e password*).

I servizi della BDN-DNA accessibili attraverso il livello di sicurezza 1 sono: tracciabilità del campione biologico, elaborazioni di dati statistici, formazione a distanza (*FAD e-learning*). Agli operatori abilitati ai suddetti servizi è vietato l'accesso alla funzionalità di AFIS che consente la decodifica del codice prelievo per acquisire i dati anagrafici della persona sottoposta a prelievo;

- livello 2 (corrispondente al LoA4 dell'ISO-IEC 29115): a tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi digitali dedicati (*token*).

I servizi della BDN-DNA accessibili attraverso il livello di sicurezza 2 sono: ricerche sulla base di "riscontro positivo - riscontro negativo" ("*hit - no hit*") a livello nazionale o internazionale, alimentazione, consultazione e raffronto dei profili del DNA nella BDN-DNA, trasmissione dei profili del DNA e degli elettroferogrammi da parte dei laboratori di istituzioni di elevata specializzazione, consultazione degli elettroferogrammi di cui al punto 1.2.

#### 1.3.2 RILASCIO E GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE PER L'ACCESSO E PROFILI DI AUTORIZZAZIONE

Il rilascio delle credenziali di autenticazione agli incaricati del trattamento è preceduto da un periodo di formazione a distanza, la cui durata è definita dal Responsabile del trattamento, svolto attraverso la piattaforma di formazione a distanza (*FAD e-learning*) accessibile dal portale S.S.I.I.

Il Direttore del SCIP, il Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., il Direttore dell'Ufficio del Laboratorio centrale, i dirigenti/comandanti degli Uffici/Comandi da cui dipendono i laboratori delle Forze di polizia, i dirigenti/comandanti degli Uffici/Comandi delle Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico, i dirigenti/comandanti degli Uffici/Comandi delle Forze di polizia che eseguono richieste di ricerca internazionale verificato che l'operatore dipendente ha completato il periodo di formazione a distanza, dispone per iscritto al competente focal point il rilascio delle credenziali di autenticazione per l'accesso al portale per lo scambio dati - IXP, coerentemente con l'ambito di trattamento consentito (profilo di autorizzazione).

Ogni incaricato del trattamento che accede al portale per lo scambio dati - IXP è identificato tramite un codice univoco ed è abilitato allo svolgimento delle funzioni applicative di competenza dell'unità organizzativa cui è preposto, con un profilo di autorizzazione coerente con l'ambito del trattamento consentito.

In caso di variazione delle condizioni che hanno consentito il rilascio delle credenziali di autenticazione, in particolare quando l'incaricato cessa o è sospeso dal servizio, oppure è preposto, anche temporaneamente, ad altra unità organizzativa, il Direttore del SCIP, il Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., il Direttore dell'Ufficio del Laboratorio centrale, i dirigenti/comandanti degli Uffici/Reparti da cui dipendono i laboratori delle Forze di polizia, i dirigenti/comandanti degli Uffici/Reparti delle Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico, i dirigenti/comandanti degli Uffici/Comandi delle Forze di polizia che eseguono richieste di ricerca dispongono la disattivazione delle credenziali al focal point di competenza e comunicano tempestivamente al Responsabile del trattamento, l'avvenuta disattivazione. Si procede ad analogo disposizione e tempestiva comunicazione nel caso in cui all'incaricato sia modificato l'ambito di trattamento consentito, ai fini della variazione del profilo di autorizzazione del medesimo.

Il sistema procede automaticamente alla disattivazione delle credenziali di autenticazione nel caso in cui siano trascorsi 90 giorni dall'ultimo accesso al portale S.S.I.I. Per il ripristino è necessario che sia nuovamente disposto al focal point di competenza di procedere a una nuova autorizzazione.

L'utenza è cancellata automaticamente dopo 180 giorni dall'ultimo accesso al portale S.S.I.I.

Il Direttore del SCIP, il Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., il Direttore dell'Ufficio del Laboratorio centrale, i dirigenti/comandanti degli Uffici/Reparti da cui dipendono i laboratori delle Forze di polizia, i dirigenti/comandanti degli Uffici/Reparti delle Forze di polizia che effettuano il prelievo o la movimentazione del campione biologico, i dirigenti/comandanti degli Uffici/Comandi delle Forze di polizia che eseguono richieste di ricerca internazionale, almeno con frequenza trimestrale, svolgono verifiche riguardo alla sussistenza dei presupposti per il rilascio delle credenziali di autenticazione o di attribuzione di un determinato profilo. Tali verifiche sono svolte anche con l'ausilio di apposite applicazioni software. Il Responsabile del trattamento svolge di iniziativa analoghe attività di verifica.

#### 1.3.3 AUDIT LOG DELLE OPERAZIONI PER FINALITÀ DI VERIFICA DELLA LICITÀ DEI TRATTAMENTI

Gli accessi e le operazioni di trattamento dei profili del DNA in ambito nazionale, contenuti nella BDN-DNA, eseguiti dal personale in servizio presso i laboratori delle Forze di polizia e la BDN-DNA, sono memorizzati in appositi registri degli accessi e delle operazioni (*file di log*) della BDN-DNA.

La registrazione contiene, ai sensi dell'articolo 9, comma 4 del Regolamento, il riferimento normativo del reato per la motivazione, il codice identificativo dell'utente che ha effettuato l'accesso, l'identificazione dell'ufficio richiedente, la denominazione dell'ufficio e l'identificativo dell'Autorità giudiziaria, il numero del procedimento penale e l'anno di riferimento, le operazioni eseguite ed i loro riferimenti temporali. La registrazione è conservata per venti anni, ai sensi dell'articolo 3, commi 7 e 8, del Regolamento.



Gli accessi e le operazioni di trattamento dei profili del DNA contenuti nella BDN-DNA, effettuati dal personale in servizio presso il Laboratorio centrale, ai sensi dell'articolo 7, comma 1, lettera a) della legge 30 giugno 2009, n.85, sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*) della BDN-DNA.

La registrazione contiene, il codice identificativo dell'utente che ha eseguito l'accesso, l'identificazione dell'ufficio richiedente, le operazioni eseguite e i loro riferimenti temporali. La registrazione è conservata per venti anni, ai sensi dell'articolo 3, commi 7 e 8, del Regolamento.

Gli accessi e le operazioni di consultazione automatizzata dei profili del DNA contenuti nella BDN-DNA per finalità di cooperazione transfrontaliera, sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*) della BDN-DNA. La registrazione contiene l'esistenza o meno di una risposta positiva, i dati trasmessi, l'autorità che gestisce la banca dati, il riferimento normativo del reato per la motivazione, il codice identificativo dell'utente che ha eseguito l'accesso, l'identificazione dell'ufficio richiedente, la denominazione dell'ufficio e l'identificativo dell'Autorità giudiziaria, il numero del procedimento penale e l'anno di riferimento, le operazioni eseguite ed i loro riferimenti temporali. La registrazione è conservata per due anni, ai sensi dell'articolo 17 comma 6 del Regolamento.

Gli accessi effettuati dall'incaricato avente funzioni di amministratore di sistema, ad eccezione degli accessi concernenti l'infrastruttura hardware, sono registrati in appositi registri degli accessi e delle operazioni (file di *log*) della BDN-DNA. La registrazione, in particolare, riguarda il codice identificativo dell'utente che ha effettuato l'accesso ed il riferimento temporale di tali accessi, ed è conservata per venti anni.

La BDN-DNA adotta un sistema che acquisisce i dati degli accessi e delle operazioni registrati e prodotti dalle applicazioni della stessa, li arricchisce calcolando un codice di controllo, applicandolo su ciascun record. Le informazioni così ottenute sono memorizzate su una nuova base dati dedicata alla loro conservazione (confidenzialità, integrità e disponibilità dei dati).

In fase di consultazione dei file di *log*, la verifica del codice di controllo sui singoli record consentirà di evidenziare eventuali manipolazioni dei dati tracciati (integrità dei dati).

I file di *log* sono utilizzati ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali.

Il Responsabile del trattamento mette a disposizione del Garante e dell'Autorità Giudiziaria i file di *log* richiesti.

I dati aggregati provenienti dall'analisi degli accessi vengono messi a disposizione del *Security Manager* per le determinazioni di competenza. L'accesso ai suddetti dati può avvenire in forma non aggregata nel caso in cui sia indispensabile ai fini della verifica delle attività rilevanti per la sicurezza del trattamento dei dati.

#### 1.3.4 MISURE FISICHE

La BDN-DNA è collocata nell'edificio ove ha sede il S.S.I.I., situato all'interno di uno dei compendi ospitanti gli uffici del Dipartimento della pubblica sicurezza.

La vigilanza e la protezione del compendio è affidata all'Ispettorato di pubblica sicurezza "Viminale", il quale a tal fine si avvale di personale della Polizia di Stato.

L'ingresso ai locali della BDN-DNA (Divisione 4<sup>a</sup> del S.S.I.I.) è consentito al Direttore del S.S.I.I., al personale in servizio presso la BDN-DNA e ai visitatori specificamente autorizzati dal Direttore del S.S.I.I. o dal Dirigente della Divisione 4<sup>a</sup> del S.S.I.I.

L'ingresso ai locali ove è ubicata l'infrastruttura hardware e software della BDN-DNA (sala server) è consentito al Direttore del S.S.I.I., al Dirigente della Divisione 4<sup>a</sup> del S.S.I.I. e al solo personale in servizio presso il S.S.I.I., individuato per iscritto dal Dirigente della Divisione 4<sup>a</sup> del S.S.I.I., in relazione all'attività svolta presso la BDN-DNA.

Per poter accedere fisicamente al compendio e, successivamente, all'edificio ove ha sede il S.S.I.I. e, quindi, ai locali della BDN-DNA (Divisione 4<sup>a</sup> del S.S.I.I.), è necessario attraversare tre barriere elettroniche situate, rispettivamente, all'ingresso delle tre anzidette strutture. Il passaggio alle barriere elettroniche è consentito al personale in servizio previamente autorizzato e munito di badge individuale, nonché ai visitatori specificamente autorizzati, muniti di badge temporaneo rilasciato, previa identificazione, dal personale della Polizia di Stato che sorveglia l'ingresso principale del compendio.

Per poter accedere fisicamente ai locali che ospitano l'infrastruttura hardware e software della BDN-DNA (sala server) è ulteriormente

necessaria l'identificazione personale mediante l'utilizzo di caratteristiche biometriche.

I dati personali relativi all'identificazione per il rilascio dei badge temporanei e quelli concernenti i transiti alle barriere elettroniche mediante l'utilizzo dei badge, sia individuali sia temporanei, sono trattati per finalità di sicurezza dall'Ispettorato di pubblica sicurezza "Viminale" nel rispetto delle disposizioni previste dal decreto legislativo n. 196 del 2003. In particolare, le modalità di trattamento e gli strumenti utilizzati, ivi compresi il profilo della sicurezza e quello dei termini di conservazione dei dati, sono determinati con provvedimento scritto del responsabile del trattamento, individuato nell'Ispettorato di pubblica sicurezza "Viminale".

Ai fini della sicurezza, il patrimonio tecnologico (*asset IT*) riferito alle postazioni di lavoro (PdL) che consentono la trasmissione dei dati alla Banca Dati, viene controllato utilizzando anche strumenti di certificazione digitale.

#### 1.3.5 MISURE LOGICHE

I servizi della BDN-DNA sono forniti in una zona di sicurezza dedicata, protetta tramite una coppia di firewall in modalità *active stand-by*.

Sono, altresì, presenti oltre i firewall già citati, apparati IPS/IDS e bilanciatori di carico di rete.

#### 1.3.6 MISURE PER IL DISASTER RECOVERY

Al fine di assicurare la continuità di funzionamento del sito primario della BDN-DNA (avente sede a Roma) è stato predisposto un sito secondario remoto della BDN-DNA, presso il Centro Unico di *Backup* della Polizia di Stato ubicato a Bari (a circa 400 km di distanza dal sito primario), attivato in caso di disastro o di altro evento di eccezionale gravità dichiarato dal Responsabile del trattamento, che permette la replica dei dati in modalità asincrona per il salvataggio ed il ripristino dei dati.

Il Piano di *Disaster Recovery* della BDN-DNA, disponibile nel manuale della qualità dei servizi offerti dalla BDN-DNA a norma ISO 9001:2015, descrive il processo che garantisce la ripartenza dei servizi informatici della BDN-DNA in conformità a quanto previsto dall'articolo 50-bis del decreto legislativo 7 marzo 2005, n. 82.

Il funzionamento del sito secondario remoto della BDN-DNA è descritto in uno o più documenti del manuale della qualità dei servizi offerti dalla BDN-DNA contenenti ruoli, compiti, modalità, responsabilità, infrastruttura dell'hardware nonché la descrizione delle procedure tecniche di attivazione del sito secondario remoto e di riattivazione del sito primario.

L'infrastruttura hardware-software e tutti i servizi offerti dal sito primario della BDN-DNA sono replicati nel sito secondario remoto.

Le Forze di polizia attraverso la rete del Ministero dell'interno possono raggiungere sia il sito primario che il sito secondario remoto.

L'infrastruttura di *Disaster Recovery* limita il *Recovery Time Objective* (RTO) ad un periodo di tempo che sarà determinato con provvedimento del Responsabile del trattamento della BDN-DNA. Sia il sito primario che il sito secondario remoto sono in grado di fornire i servizi in alta affidabilità. Nel sito secondario remoto sono previste le stesse misure di sicurezza fisiche e logiche adottate per il sito primario.

#### 1.3.7 RUOLO DEL "SECURITY MANAGER" DELL'UFFICIO SICUREZZA DATI (USD).

L'Ufficio per la Sicurezza dei Dati, istituito nell'ambito della Direzione Centrale della Polizia Criminale, con compiti anche di *Security Manager* della BDN-DNA, fornisce pareri riguardanti i piani di sicurezza dei dati, l'analisi dei rischi relativi ai dati ed al loro trattamento, l'analisi di impatto dei rischi sulle attività e sulle risorse, il coordinamento ed indirizzo delle attività di registrazione, di esame e verifica delle attività rilevanti per la sicurezza del trattamento dei dati della BDN-DNA (*security auditing*).





## 2. LABORATORIO CENTRALE DELLA BANCA DATI NAZIONALE DEL DNA

## 2.1 INFRASTRUTTURA GENERALE DEL SISTEMA INFORMATIVO

Il Laboratorio centrale è dotato dei seguenti sistemi:

- sistema informativo denominato LIMS per la gestione dei dati e del flusso di lavoro a cui è sottoposto il campione biologico nel laboratorio centrale;
- sistema informativo per la gestione della conservazione dei campioni biologici e degli elettroferogrammi.

Il LIMS permette di gestire il flusso di lavoro a cui è sottoposto il campione biologico, a partire dall'accettazione e conservazione fino alla sua tipizzazione del DNA in laboratorio.

Il sistema informativo per la gestione della conservazione dei campioni biologici permette di conservare i campioni, a temperatura ambiente, in armadi accessibili mediante badge e dotati di sistema di archiviazione basato sull'identificazione degli oggetti anche mediante radio frequenza.

Entrambi i predetti sistemi non prevedono interconnessioni con i sistemi informativi della BDN-DNA. L'infrastruttura tecnologica del Laboratorio centrale è organizzata con sistemi ad alta affidabilità, sistemi di autenticazione forte e *firewall*.

Il Laboratorio centrale è collegato con il Dipartimento dell'Amministrazione Penitenziaria e con la BDN-DNA esclusivamente per le finalità di inserimento dei profili del DNA e per le operazioni di accettazione del campione biologico.

Il Laboratorio centrale utilizza il Sistema Pubblico di Connettività (SPC) per accedere alla BDN-DNA. I canali di comunicazione sono soggetti a controllo di firewall alle due estremità.

La Figura 2 illustra l'architettura IT del sistema informativo del Laboratorio centrale e la parte dell'architettura del sistema informativo della BDN-DNA relativa ai servizi offerti alle articolazioni del Dipartimento dell'Amministrazione Penitenziaria che effettuano il prelievo di campioni biologici.

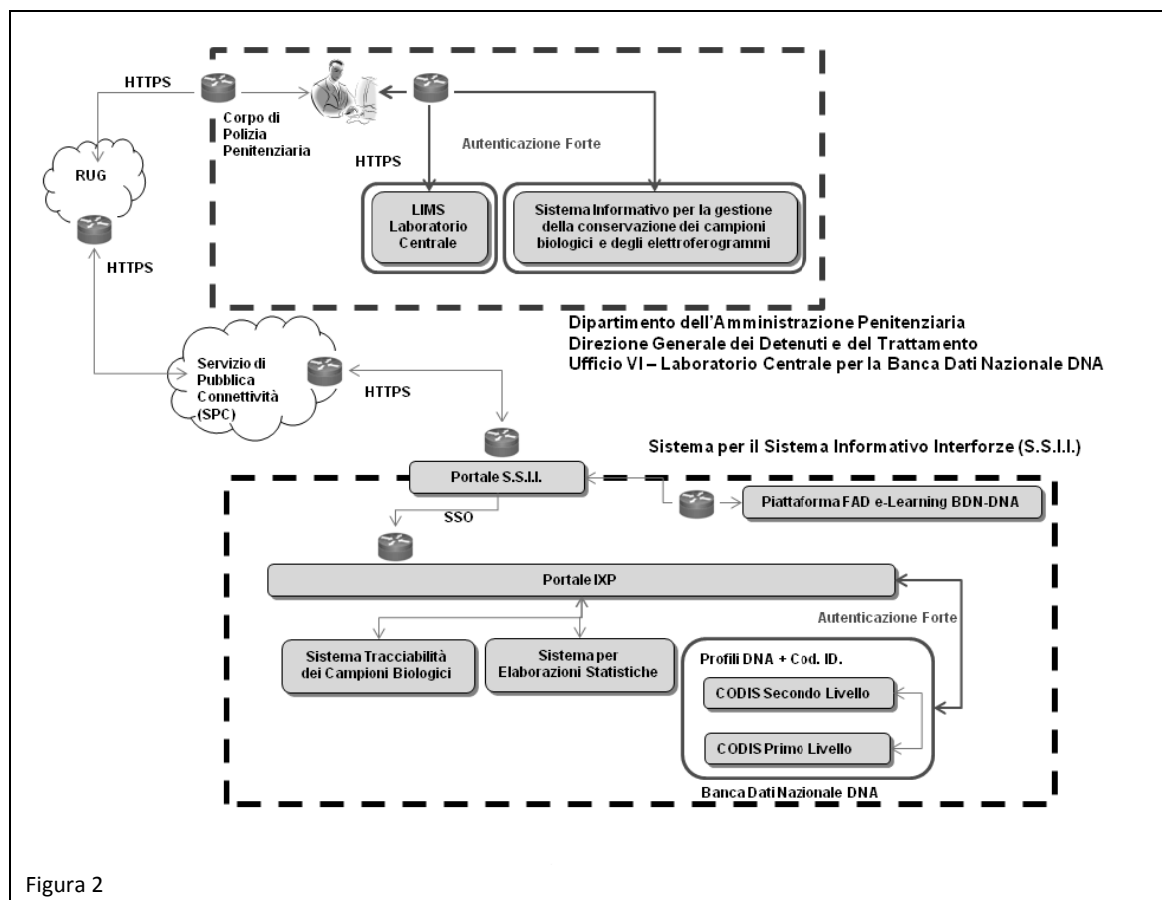
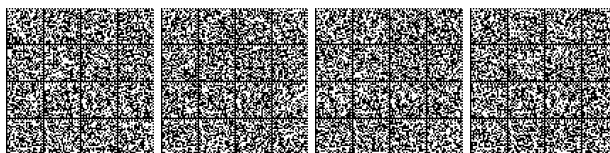


Figura 2



Il Dipartimento dell'Amministrazione Penitenziaria ha la responsabilità della sicurezza della rete geografica di riferimento e condivide con il S.S.I.I. le scelte tecniche e le configurazioni delle interconnessioni.

## 2.2 FUNZIONALITÀ DEL LABORATORIO CENTRALE E RESPONSABILITÀ DEL PERSONALE

Il Laboratorio centrale, ai sensi dell'articolo 8 della legge n. 85 del 2009, svolge le attività di seguito elencate:

a) tipizzazione del profilo del DNA dei soggetti di cui all'articolo 9, commi 1 e 2, della legge n. 85 del 2009 al fine dell'inserimento per via telematica nella BDN-DNA;

b) conservazione dell'elettroferogramma relativo al profilo del DNA ottenuto a seguito di tipizzazione del campione biologico;

c) distruzione dell'elettroferogramma a seguito della cancellazione del profilo del DNA dalla BDN-DNA;

d) conservazione del campione biologico dal quale è stato tipizzato il profilo del DNA;

e) distruzione del campione biologico secondo i tempi stabiliti dal dagli articoli 24, 29, 30, 31 e 32 del Regolamento.

Titolare del trattamento dei dati del Laboratorio centrale, ai sensi dell'articolo 27, comma 1, del Regolamento, è il Ministero della giustizia - Dipartimento dell'Amministrazione Penitenziaria.

Responsabile del trattamento dei dati del Laboratorio centrale, ai sensi dell'articolo 27, comma 2, del Regolamento, è il Direttore dell'Ufficio del Laboratorio centrale.

Il trattamento riguarda:

- i dati registrati nel LIMS del Laboratorio centrale;
- gli elettroferogrammi conservati presso il Laboratorio centrale;
- i campioni biologici conservati presso il Laboratorio centrale;
- i campioni biologici e i profili del DNA del personale che accede al laboratorio ai fini del controllo sulla correttezza del dato inserito nella BDN-DNA.

Il Direttore dell'Ufficio del Laboratorio centrale assicura l'organizzazione ed il funzionamento del Laboratorio centrale; identifica i metodi accreditati e le procedure tecniche idonee per la tipizzazione del DNA, nonché le procedure adottate per la conservazione e distruzione dei campioni biologici; individua l'amministratore/i di sistema; individua i corsi di formazione specifici per il personale del Laboratorio ai sensi del decreto legislativo 9 aprile 2008, n. 81; predispone il piano della sicurezza ed il manuale della qualità del Laboratorio. Il Direttore dell'Ufficio del Laboratorio centrale è responsabile della valutazione dei rischi sul lavoro, direttamente o tramite individuazione di una figura professionale idonea alla valutazione, nonché della gestione del personale assegnato.

Incaricati del trattamento dei dati registrati nel LIMS, degli elettroferogrammi e dei campioni biologici conservati presso il Laboratorio centrale sono gli operatori in servizio presso il Laboratorio centrale. Tali incaricati sono designati, ai sensi dell'articolo 30 del Codice, in base alla documentata preposizione al Laboratorio centrale. L'ambito del trattamento consentito è individuato per iscritto dal Direttore dell'Ufficio del Laboratorio centrale, in qualità di Responsabile del trattamento, in relazione alle attività svolte dalle unità organizzative di appartenenza.

Gli incaricati del trattamento, ai sensi dell'articolo 30 del Codice, operano sotto la diretta autorità del Titolare del trattamento (Dipartimento dell'Amministrazione Penitenziaria) e del Responsabile del trattamento (Direttore dell'Ufficio del Laboratorio centrale), attenendosi alle direttive e alle istruzioni dagli stessi impartite.

Il Direttore dell'Ufficio del Laboratorio centrale controlla che gli operatori gerarchicamente dipendenti osservino le disposizioni in materia di trattamento e rispettino le direttive e le istruzioni impartite, anche sotto il profilo relativo alla sicurezza. A tal fine, svolge verifiche periodiche, anche a campione, sulle operazioni di trattamento effettuate dagli operatori gerarchicamente dipendenti.

## 2.3 MISURE DI SICUREZZA DEL LABORATORIO CENTRALE PER LA BANCA DATI NAZIONALE DEL DNA

### 2.3.1 LIVELLI DI SICUREZZA O DI GARANZIA NELL'AUTENTICAZIONE INFORMATICA DEL LABORATORIO CENTRALE PER LA BANCA DATI NAZIONALE DEL DNA

Il Laboratorio centrale, per le attività di accettazione del campione biologico, si avvale dell'applicativo per la tracciabilità dei campioni biologici messo a disposizione dalla BDN-DNA attraverso il portale per lo scambio dati - IXP con livello di sicurezza 1, così come defini-

to nell'allegato A. L'accesso ai servizi offerti dalla BDN-DNA che ne permettono l'alimentazione dei profili del DNA avviene attraverso il portale per lo scambio dati - IXP e con livello di sicurezza 2. L'accesso al sistema LIMS e al sistema informativo per la gestione della conservazione dei campioni biologici e degli elettroferogrammi avviene con livello di sicurezza 2, definito nell'allegato A.

L'accesso agli armadi adibiti alla conservazione dei campioni biologici e degli elettroferogrammi è possibile solo attraverso le postazioni di lavoro presenti nei locali che custodiscono gli armadi. L'accesso alle postazioni avviene con livello di sicurezza 2.

Dalle suddette postazioni si accede al sistema informativo per la gestione della conservazione dei campioni biologici e degli elettroferogrammi che gestisce l'apertura degli armadi e l'ubicazione del campione biologico. L'apertura effettiva degli armadi è inoltre subordinata all'uso di badge specifici.

Il Direttore dell'Ufficio del Laboratorio centrale (Responsabile del trattamento) dispone il prelievo dei campioni biologici e la tipizzazione del DNA del personale autorizzato ad accedere al Laboratorio.

Il prelievo dei campioni biologici e l'estrazione dei profili del DNA del personale autorizzato ad accedere al Laboratorio centrale sono finalizzati a ridurre il rischio di contaminazione da parte del predetto personale.

Il campione biologico, il profilo del DNA e l'elettroferogramma riferiti al predetto personale, sono associati a codici identificativi univoci generati dal sistema LIMS del Laboratorio centrale e non contengono informazioni che consentono l'identificazione diretta del soggetto cui sono riferiti e sono custoditi in apposito armadio sottoposto alle stesse misure di sicurezza indicate nel precedente capoverso. Una volta tipizzato il profilo del DNA, il campione biologico e l'elettroferogramma sono immediatamente distrutti e dell'operazione è redatto verbale.

Il profilo del DNA è memorizzato, per il tempo definito dal rapporto di lavoro che consente al predetto personale di accedere al Laboratorio, con uno specifico dispositivo dell'applicativo software utilizzato per l'interpretazione del profilo del DNA.

L'operatore del Laboratorio che effettua le analisi dei campioni biologici prima di inserire il profilo del DNA in banca dati confronta i profili analizzati con quelli del personale sopra indicato mediante tale dispositivo.

### 2.3.2 RILASCIO E GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE PER L'ACCESSO E PROFILI DI AUTORIZZAZIONE

Il rilascio delle credenziali di autenticazione agli incaricati del trattamento è preceduto da un periodo di formazione. Il Direttore dell'Ufficio del Laboratorio centrale, verificato che l'operatore dipendente ha completato il periodo di formazione, dispone per iscritto al competente focal point il rilascio delle credenziali di autenticazione per l'accesso al sistema LIMS o al sistema informativo per la gestione della conservazione dei campioni biologici e degli elettroferogrammi, coerentemente con l'ambito di trattamento consentito (profilo di autorizzazione).

Ogni incaricato del trattamento che accede ai suddetti sistemi è identificato tramite un codice univoco ed è abilitato allo svolgimento delle funzioni applicative di competenza dell'unità organizzativa cui è preposto, con un profilo di autorizzazione coerente con l'ambito del trattamento consentito.

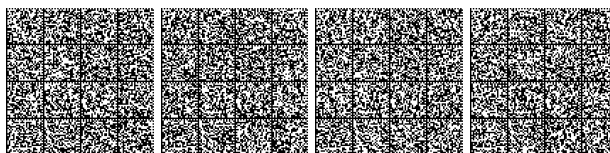
In caso di variazione delle condizioni che hanno consentito il rilascio delle credenziali di autenticazione, in particolare quando l'incaricato cessa o è sospeso dal servizio, oppure è preposto, anche temporaneamente, ad altra unità organizzativa, il Direttore dell'Ufficio del Laboratorio centrale (Responsabile del trattamento), dispone la disattivazione delle credenziali al focal point di competenza. Si procede ad analogha disposizione e tempestiva comunicazione nel caso in cui all'incaricato sia modificato l'ambito di trattamento consentito, ai fini della variazione del profilo di autorizzazione del medesimo.

Il sistema procede automaticamente alla disattivazione delle credenziali di autenticazione nel caso in cui siano trascorsi 90 giorni dall'ultimo accesso alla postazione di lavoro (PdL).

Per il ripristino sarà necessario che il Direttore dell'Ufficio del Laboratorio centrale disponga al focal point di competenza una nuova autorizzazione.

L'utenza è cancellata automaticamente dopo 180 giorni dall'ultimo accesso alla postazione di lavoro.

Il Direttore dell'Ufficio del Laboratorio centrale, almeno con frequenza trimestrale, svolge verifiche riguardo alla sussistenza dei presupposti per il rilascio delle credenziali di autenticazione o di attribui-





zione di un determinato profilo. Tali verifiche sono svolte anche con l'ausilio di apposite applicazioni software.

### 2.3.3 AUDIT LOG DELLE OPERAZIONI PER FINALITÀ DI VERIFICA DELLA LICITÀ DEI TRATTAMENTI

Gli accessi alla postazione di lavoro adibita all'uso del sistema LIMS sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso e il riferimento temporale ed è conservata per venti anni ai sensi dell'articolo 4, comma 5, del Regolamento.

Le operazioni di trattamento dei dati contenuti nel sistema LIMS in uso al Laboratorio centrale sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso, le operazioni eseguite e i loro riferimenti temporali ed è conservata per dieci anni ai sensi dell'articolo 4, comma 5, del Regolamento.

Gli accessi ai locali ove sono custoditi gli armadi adibiti alla conservazione dei campioni biologici e degli elettroferogrammi sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso, e il riferimento temporale ed è conservata per dieci anni.

Gli accessi alla postazione di lavoro presente all'interno dei locali adibita al controllo degli armadi sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso, e il riferimento temporale ed è conservata per dieci anni.

Gli accessi alla postazione di lavoro adibita all'interpretazione dei profili del DNA sono memorizzati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso, e il riferimento temporale ed è conservata per dieci anni.

Gli accessi effettuati dall'incaricato avente funzioni di amministratore di sistema, ad eccezione degli accessi relativi all'infrastruttura hardware, sono registrati in appositi registri degli accessi e delle operazioni (file di *log*). La registrazione, in particolare, contiene il codice identificativo dell'utente che ha effettuato l'accesso ed il riferimento temporale di tali accessi, ed è conservata per dieci anni.

Il Laboratorio centrale adotta un sistema che acquisisce i dati degli accessi e delle operazioni registrati e prodotti dall'applicazione LIMS, li arricchisce calcolando un codice di controllo, applicandolo su ciascun record. Le informazioni così ottenute sono memorizzate su una nuova base dati dedicata alla loro conservazione (confidenzialità, integrità e disponibilità dei dati).

In fase di consultazione dei file di log, la verifica del codice di controllo sui singoli record consentirà di evidenziare eventuali manipolazioni dei dati tracciati (integrità dei dati).

I file di log sono utilizzati ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali.

Il Responsabile del trattamento mette a disposizione del Garante e dell'Autorità Giudiziaria i file di log richiesti.

### 2.3.4 MISURE FISICHE

L'area ove è situata la struttura del Laboratorio centrale – comprensiva dei locali uffici e servizi e dei locali laboratori – nonché l'area esterna, di pertinenza del Laboratorio centrale, è ricavata all'interno del perimetro del cosiddetto "Polo logistico di Roma Rebibbia".

L'accesso alla struttura e all'area pertinenziale è vigilato da personale del Corpo di Polizia Penitenziaria, anche attraverso sistemi di videosorveglianza ed antintrusione.

L'ingresso al Laboratorio centrale è consentito al personale ivi in servizio, nonché ai visitatori e agli appartenenti alle Forze di polizia, solo previa autorizzazione del Direttore dell'Ufficio del Laboratorio centrale.

L'accesso all'edificio ove ha sede il Laboratorio centrale è consentito solo a seguito di identificazione personale e previo controllo del rilascio delle autorizzazioni a cura del personale del Corpo di Polizia Penitenziaria addetto al servizio di vigilanza.

Per l'accesso ai locali adibiti a laboratori e ai locali adibiti ad ospitare l'infrastruttura hardware e software è ulteriormente necessaria l'identificazione personale mediante l'utilizzo di caratteristiche biometriche.

I dati personali relativi all'identificazione di coloro che accedono sono trattati per finalità di sicurezza, nel rispetto delle disposizioni previste dal decreto legislativo n. 196 del 2003.

Le modalità di trattamento e gli strumenti utilizzati, ivi compreso il profilo della sicurezza e quello dei termini di conservazione dei dati, sono determinati con provvedimento, sulla base della normativa vigente in materia.

### 2.3.5 MISURE LOGICHE

I servizi forniti dal sistema LIMS e dal sistema informativo per la gestione della conservazione dei campioni biologici sono separati e risiedono in zone di sicurezza protette tramite firewall.

### 2.3.6 MISURE PER L'ALTA AFFIDABILITÀ E IL BACKUP

Al fine di assicurare la continuità di funzionamento dei servizi più critici e per cautelarsi dagli effetti derivanti da situazioni di crisi sono state previste risorse hardware e software ridondate ed è stato definito una procedura di backup del LIMS che prevede il salvataggio dei dati su appositi supporti custoditi in armadi che consentono di salvaguardare i dati da pericoli fisici, quali incendi, allagamenti, furti, onde magnetiche ed esplosioni.

ALLEGATO C

## TRASMISSIONE DEL PROFILO DEL DNA DA PARTE DELL'ISTITUZIONE DI ELEVATA SPECIALIZZAZIONE AI LABORATORI DELLA FORZA DI POLIZIA INDIVIDUATA DALL'AUTORITÀ GIUDIZIARIA

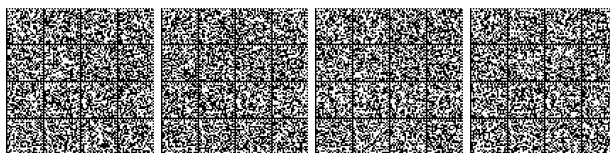
I laboratori delle istituzioni di elevata specializzazione, pubblici o privati – che hanno metodi di prova accreditati a norma EN ISO/IEC 17025 per la tipizzazione del DNA da reperti biologici acquisiti nel corso di procedimenti penali, da persone scomparse o dei loro consanguinei, da cadaveri e resti cadaverici non identificati – ai fini dell'inserimento e raffronto tra profili del DNA presenti nella BDN-DNA, trasmettono i profili del DNA, per via telematica, secondo lo schema riportato nella Figura 3 che segue.

Il patrimonio tecnologico (*asset IT*) riferito alle postazioni di lavoro (PdL), viene controllato utilizzando anche strumenti di certificazione digitale, ai fini della trasmissione, per via telematica, dei profili del DNA ai laboratori delle Forze di polizia, secondo lo schema di cui alla Figura 3.

La BDN-DNA mette a disposizione del laboratorio dell'istituzione di elevata specializzazione un'applicazione informatica per la trasmissione telematica del profilo del DNA e della documentazione riguardante i metodi di prova accreditati e i tempi di validità del certificato emesso dall'organismo nazionale di accreditamento, individuato ai sensi dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99.

Il laboratorio della istituzione di elevata specializzazione che ha proceduto alla tipizzazione del DNA a mezzo di accertamento tecnico, consulenza tecnica o perizia da parte dell'Autorità Giudiziaria, trasmette il profilo del DNA e l'elettroferogramma, ai sensi dell'articolo 6, commi 7, 8 e 9, del Regolamento, unitamente alle seguenti informazioni:

- codice dell'ente (art. 2, comma 1, lettera *l*), del Regolamento);
- codice del laboratorio (art. 2, comma 1, lettera *m*), del Regolamento);
- codice del reperto biologico / persone scomparse o dei loro consanguinei/ cadaveri e resti cadaverici non identificati (art. 2, comma 1, lettera *p*), del Regolamento);
- tipologia dell'Ufficio dell'Autorità Giudiziaria che ha conferito l'incarico di tipizzazione del DNA (ad esempio: "Procura della Repubblica", "Giudice per le indagini preliminari", "Corte di Assise", ecc.);
- provincia dell'Ufficio dell'Autorità Giudiziaria sopra indicata (ad esempio: "RM");
- numero di procedimento penale/anno di riferimento (ad esempio: "PP.1234/2016 RGNR");
- laboratorio delle Forze di polizia individuato all'Autorità giudiziaria per l'inserimento in Banca Dati (art. 2, comma 1, lettera *m*), del Regolamento);
- motivazione (fattispecie di reato oggetto del procedimento penale, ad esempio: "CP art. 628, Rapina");



- indicazione del numero complessivo dei profili del DNA oggetto della trasmissione (ad esempio: “3”);
- il numero di riferimento specifico del profilo del DNA trasmesso (ad esempio: “1 di 3”);
- standard internazionale di riferimento utilizzato per la tipizzazione del DNA (ad esempio: “ISO9001”, “ISO/IEC 17025”, ecc.).

L'applicazione informatica messa a disposizione dalla BDN-DNA, prima di consentire la trasmissione telematica, richiede all'operatore del laboratorio dell'istituzione di elevata specializzazione di autocertificare ai sensi dell'articolo 46 del D.P.R. 445 del 28 dicembre 2000, l'accreditamento a norma EN ISO/IEC 17025, cliccando su un apposito pulsante.

Il Titolare e il Responsabile (se designato) del trattamento dei dati presso il laboratorio delle istituzioni di elevata specializzazione controllano che le operazioni avvengano nel rispetto delle disposizioni in materia di trattamento dei dati personali e delle istruzioni da essi impartite, anche per quanto concerne il profilo della sicurezza.

Gli incaricati del trattamento dei profili del DNA presso il laboratorio della istituzione di elevata specializzazione sono designati per il compimento delle operazioni di trattamento dal Titolare o Responsabile (se designato) del trattamento dei dati del laboratorio, secondo le modalità stabilite dall'articolo 30 del Codice.

L'accesso all'applicazione informatica per la trasmissione dei dati e informazioni sopra indicati è consentito al Titolare, al Responsabile (se designato), agli incaricati del trattamento, attraverso l'impiego di un sistema di autenticazione con livello di sicurezza 2, definito nell'Allegato A del presente decreto.

Il portale per lo scambio dati - IXP acquisisce, dall'applicazione, il profilo del DNA, l'elettroferogramma ed i dati trasmessi dal laboratorio e li pone a disposizione del laboratorio delle Forze di polizia individuato dall'Autorità Giudiziaria.

Gli incaricati del trattamento dei dati, del laboratorio delle Forze di polizia individuato dall'Autorità Giudiziaria, inseriscono il profilo del DNA nel software CODIS in modalità “doppio cieco” e l'elettroferogramma nel sistema per la conservazione per gli elettroferogrammi.

I canali di comunicazione utilizzati sono soggetti a controllo di firewall alle due estremità, come di seguito riportato in Figura 3.

La Figura 3 mostra i componenti dell'architettura IT che permettono la trasmissione alla BDN - DNA dei profili del DNA da parte dei laboratori delle istituzioni di elevata specializzazione e l'inserimento dei profili del DNA da parte dei laboratori delle Forze di polizia e del Laboratorio centrale.

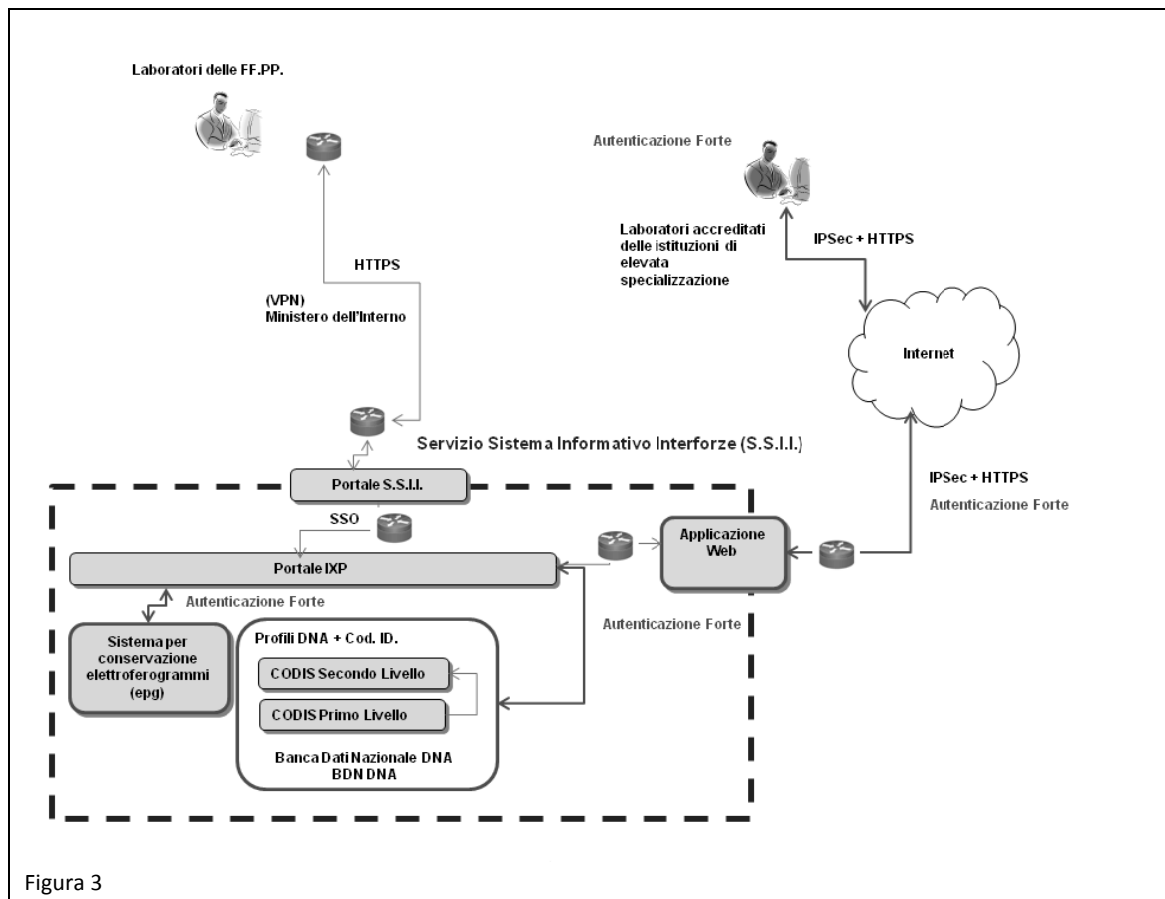


Figura 3

