►**B**

DECISIONE 2008/616/GAI DEL CONSIGLIO

del 23 giugno 2008

relativa all'attuazione della decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera

(GU L 210 del 6.8.2008, pag. 12)

Modificata da:

		Gazzetta ufficiale		
		n.	pag.	data
►**M1**	Regolamento (UE) 2024/982 del Parlamento europeo e del Consiglio del 13 marzo 2024	L 982	1	5.4.2024

▼B

DECISIONE 2008/616/GAI DEL CONSIGLIO

del 23 giugno 2008

relativa all'attuazione della decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Obiettivo

L'obiettivo della presente decisione è di stabilire le disposizioni amministrative e tecniche necessarie all'attuazione della decisione 2008/615/GAI, in particolare per quanto riguarda lo scambio automatizzato di dati sul DNA, dati dattiloscopici e dati di immatricolazione dei veicoli di cui al capo 2 di tale decisione, nonché per le altre forme di cooperazione previste al capo 5 della stessa.

Articolo 2

Definizioni

Ai fini della presente decisione, si intende per:

a) «consultazione» e «raffronto», di cui agli articoli 3, 4 e 9 della decisione 2008/615/GAI, le procedure mediante cui si stabilisce se vi sia concordanza tra, rispettivamente, i dati sul DNA o i dati dattiloscopici comunicati da uno Stato membro e i dati sul DNA o i dati dattiloscopici memorizzati nella banche dati di uno, di alcuni o di tutti gli Stati membri;

b) «consultazione automatizzata», di cui all'articolo 12 della decisione 2008/615/GAI, la procedura di accesso on line per consultare le basi di dati di uno, di alcuni o di tutti gli Stati membri;

c) «profilo DNA» un codice alfanumerico che rappresenta una serie di caratteristiche identificative della parte non codificante di un campione di DNA umano analizzato, vale a dire la struttura molecolare particolare dei vari loci del DNA;

d) «parte non codificante del DNA» regioni cromosomiche che non contengono alcuna espressione genetica, vale a dire che notoriamente non forniscono alcuna proprietà funzionale di un organismo;

e) «dati indicizzati sul DNA» profilo DNA e numero di riferimento;

f) «profilo DNA indicizzato» il profilo DNA di una persona identificata;

g) «profilo DNA non identificato» profilo DNA ottenuto da tracce rilevate nel corso delle indagini sui reati e appartenente ad una persona non ancora identificata;

▼B

h) «annotazione» contrassegno apposto da uno Stato membro su un profilo DNA contenuto nella banca dati nazionale, indicante il fatto che è già stata evidenziata una concordanza su tale profilo DNA in seguito a una consultazione o a un raffronto realizzati da un altro Stato membro;

i) «dati dattiloscopici» immagini delle impronte digitali, immagini delle impronte digitali latenti, impronte palmari, impronte palmari latenti e modelli di tali immagini (minutiae codificate), quando sono memorizzati e trattati in una banca dati automatizzata;

j) «dati di immatricolazione dei veicoli» l'insieme dei dati di cui al capo 3 dell'allegato della presente decisione;

k) «caso per caso», espressione di cui all'articolo 3, paragrafo 1, seconda frase, all'articolo 9, paragrafo 1, seconda frase, e all'articolo 12, paragrafo 1, della decisione 2008/615/GAI, un singolo fascicolo d'indagine o fascicolo penale. Se tale fascicolo contiene più di un profilo DNA, dato dattiloscopico o dato di immatricolazione di un veicolo, questi possono essere trasmessi insieme come singola domanda.

▼M1

———————

▼B

CAPO 6

COOPERAZIONE DI POLIZIA

Articolo 17

Pattugliamenti congiunti e altre operazioni congiunte

1. Conformemente al capo 5 della decisione 2008/615/GAI, in particolare alle dichiarazioni presentate a norma dell'articolo 17, paragrafo 4, e dell'articolo 19, paragrafi 2 e 4, di tale decisione, ciascuno Stato membro designa uno o più punti di contatto al fine di consentire agli altri Stati membri di rivolgersi alle autorità competenti e ogni Stato membro può definire le procedure per porre in essere pattugliamenti congiunti e altre operazioni congiunte, le procedure per le iniziative degli altri Stati membri con riguardo a tali operazioni, nonché altri aspetti pratici e le modalità operative relative a tali operazioni.

2. Il segretariato generale del Consiglio compila e aggiorna un elenco dei punti di contatto e comunica alle autorità competenti qualsiasi variazione apportata a tale elenco.

3. Le autorità competenti di ciascuno Stato membro possono assumere l'iniziativa di porre in essere un'operazione congiunta. Prima dell'avvio di un'operazione specifica, le autorità competenti di cui al paragrafo 2 prendono accordi verbali o scritti che possono riguardare i seguenti aspetti:

a) le autorità competenti degli Stati membri per l'operazione;

b) lo scopo specifico dell'operazione;

▼B

c) lo Stato membro di destinazione in cui l'operazione deve avere luogo;

d) la zona geografica dello Stato membro di destinazione in cui l'operazione deve avere luogo;

e) il periodo coperto dall'operazione;

f) l'assistenza specifica che lo Stato membro o gli Stati membri di origine devono fornire allo Stato membro di destinazione, compresi funzionari o altri agenti, elementi materiali e finanziari;

g) i funzionari che partecipano all'operazione;

h) il funzionario responsabile dell'operazione;

i) i poteri che i funzionari e altri agenti dello Stato membro o degli Stati membri di origine possono esercitare nello Stato membro di destinazione durante l'operazione;

j) le armi, le munizioni e le attrezzature specifiche che i funzionari dello Stato membro di origine possono utilizzare durante l'operazione a norma della decisione 2008/615/GAI;

k) le modalità logistiche relative al trasporto, all'alloggio e alla sicurezza;

l) la ripartizione delle spese dell'operazione congiunta, se differisce da quanto disposto dall'articolo 34, prima frase, della decisione 2008/615/GAI

m) qualsiasi altro eventuale elemento richiesto.

4. Le dichiarazioni, le procedure e le designazioni di cui al presente articolo figurano nel manuale di cui all'articolo 18, paragrafo 2.

CAPO 7

DISPOSIZIONI FINALI

▼M1

———————

▼B

Articolo 19

Autorità indipendenti preposte alla protezione dei dati

A norma dell'articolo 18, paragrafo 2, della presente decisione, gli Stati membri comunicano al segretariato generale del Consiglio le autorità indipendenti preposte alla protezione dei dati o le autorità giudiziarie di cui all'articolo 30, paragrafo 5, della decisione 2008/615/GAI.

▼M1

———————

▼B

Articolo 22

Rapporto con l'accordo attuativo del trattato di Prüm

Per gli Stati membri vincolati dal trattato di Prüm le pertinenti disposizioni della presente decisione e del relativo allegato, una volta pienamente in vigore, prevalgono sulle disposizioni corrispondenti contemplate dall'accordo attuativo del trattato di Prüm. Eventuali altre disposizioni dell'accordo attuativo restano applicabili fra le parti contraenti del trattato di Prüm.

▼B

Articolo 23

Attuazione

Gli Stati membri adottano le misure necessarie per conformarsi alle disposizioni della presente decisione entro i termini previsti all'articolo 36, paragrafo 1, della decisione 2008/615/GAI.

Articolo 24

Applicazione

La presente decisione ha effetto venti giorni dopo la pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

▼B

ALLEGATO

INDICE

▼B

9.5. *Definizioni record tipo-1*

9.6. *Definizioni record tipo-2*

9.7. *Codici di compressione della scala dei grigi*

9.8. *Specifica dei messaggi*

CAPO 3: **Scambio di dati di immatricolazione dei veicoli**

1. ***Insieme comune di dati per la consultazione automatizzata dei dati di immatricolazione dei veicoli***

1.1. *Definizioni*

1.2. *Consultazione relativa al veicolo/proprietario/intestatario*

2. ***Sicurezza dei dati***

2.1. *Quadro generale*

2.2. *Caratteristiche di sicurezza connesse allo scambio di messaggi*

2.3. *Caratteristiche di sicurezza non connesse allo scambio di messaggi*

3. ***Condizioni tecniche dello scambio di dati***

3.1. *Descrizione generale dell'applicazione Eucaris*

3.2. *Requisiti funzionali e non funzionali*

CAPO 4: **Valutazione**

1. ***Procedura di valutazione a norma dell'articolo 20 (preparazione delle decisioni a norma dell'articolo 25, paragrafo 2, della decisione 2008/615/GAI)***

1.1. *Questionario*

1.2. *Esperienza pilota*

1.3. *Visita di valutazione*

1.4. *Relazione al Consiglio*

2. ***Procedura di valutazione a norma dell'articolo 21***

2.1. *Statistiche e relazione*

2.2. *Revisione*

3. ***Riunioni di esperti***

▼B

CAPO 1: **Scambio di dati sul DNA**

1. ***Questioni forensi relative al DNA, norme di concordanza e algoritmi***

1.1. *Proprietà dei profili DNA*

Il profilo DNA può contenere 24 coppie di numeri che rappresentano gli alleli di 24 loci utilizzati anche dall'Interpol nelle procedure relative al DNA. Nella tabella che segue sono riportati i nomi di tali loci:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenina
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

I sette loci evidenziati in grigio nella riga superiore rappresentano sia la serie europea standard (ESS) sia la serie di loci standard dell'Interpol (ISSOL) attuali.

Norme di inclusione:

I profili DNA messi a disposizione dagli Stati membri a fini di consultazione e raffronto ed i profili DNA trasmessi per consultazione e raffronto devono contenere almeno sei loci pienamente designati ([1]) e possono contenere loci supplementari o controlli negativi a seconda della loro disponibilità. I profili DNA indicizzati devono contenere almeno sei dei sette loci ESS. Per aumentare l'accuratezza delle concordanze, tutti gli alleli disponibili sono memorizzati nella banca dati del profilo DNA indicizzato e sono utilizzati a fini di ricerca e raffronto. Ciascuno Stato membro dovrebbe attuare non appena ciò sia materialmente possibile eventuali nuovi ESS di loci adottati dall'UE.

Non sono ammessi profili misti, quindi i valori degli alleli di ciascun locus saranno costituiti di due soli numeri, che in caso di omozigosi a un dato locus possono essere identici.

Per i caratteri jolly e le microvarianti si devono osservare le seguenti regole:

— qualsiasi valore non numerico eccetto l'amelogenina contenuto nel profilo (ad esempio «o», «f», «r», «na», «nr» o «un») deve essere automaticamente convertito in carattere jolly (*) per essere esportato e consultato in tutte le banche dati,

— i valori numerici «0», «1» o «99» contenuti nel profilo devono essere automaticamente convertiti in un carattere jolly (*) per essere esportati e consultati in tutte le banche dati,

— se per un locus sono forniti tre alleli, il primo allele sarà accettato e gli altri due devono essere automaticamente convertiti in un carattere jolly (*) per essere esportati e consultati in tutte le banche dati,

— se per l'allele 1 o 2 sono forniti valori con caratteri jolly, saranno consultate entrambe le permutazioni del valore numerico dato per il locus (ad esempio 12, * potrebbe concordare con 12,14 o 9,12),

([1]) «Pienamente designati» indica che l'elaborazione di valori degli alleli rari è inclusa.

▼B

— la concordanza delle microvarianti dei pentanucleotidi (Penta D, Penta E & CD4) sarà stabilita come segue:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x.4

x.4 = x.3, x.4, x + 1,

— la concordanza delle microvarianti dei tetranucleotidi (il resto dei loci è costituito da tetranucleotidi) sarà stabilita come segue:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x + 1.

1.2. *Norme di concordanza*

Il raffronto di due profili DNA sarà effettuato in base ai loci per i quali in entrambi i profili DNA è disponibile una coppia di valori dell'allele. Prima di dare una risposta positiva fra i due profili DNA deve esservi una concordanza di almeno sei loci pienamente designati (ad eccezione dell'amelogenina).

Per concordanza totale (qualità 1) si intende il caso in cui tutti i valori dell'allele dei loci raffrontati comunemente contenuti nel profilo DNA dello Stato richiedente e dello Stato richiesto sono identici. Per quasi concordanza si intende il caso in cui nei due profili DNA un solo allele fra tutti quelli raffrontati è di valore diverso (qualità 2, 3 e 4). Una quasi concordanza è ammessa solo in caso di concordanza totale di almeno sei loci pienamente designati dei due profili DNA raffrontati.

Una quasi concordanza può essere dovuta a:

— un errore umano di battitura al punto di ingresso di uno dei profili DNA nella richiesta di consultazione o nella banca dati sul DNA,

— un errore di determinazione o denominazione dell'allele nel corso della procedura di generazione del profilo DNA.

1.3. *Norme concernenti le relazioni*

Viene stilata una relazione per le concordanze totali, per le quasi concordanze e per le risposte negative («no hits»).

La relazione sulla concordanza sarà inviata al punto di contatto nazionale richiedente e messa altresì a disposizione del punto di contatto nazionale richiesto (per consentirgli di valutare la natura e l'entità del possibile seguito di richieste di altri dati personali disponibili e di altre informazioni connesse con il profilo DNA corrispondente alla risposta positiva, a norma degli articoli 5 e 10 della decisione 2008/615/GAI).

2. ***Tabella dei numeri di codice degli Stati membri***

In conformità della decisione 2008/615/GAI, per creare i nomi di dominio ed altri parametri di configurazione richiesti nelle applicazioni per lo scambio di dati sul DNA in una rete chiusa in ambito Prüm si utilizzano codici ISO 3166-1 alpha-2.

I codici ISO 3166-1 alpha-2 sono i codici di Stato membro di due lettere riportati qui di seguito.

▼B

Nome degli Stati membri	Codice	Nome degli Stati membri	Codice
Belgio	BE	Lussemburgo	LU
Bulgaria	BG	Ungheria	HU
Repubblica ceca	CZ	Malta	MT
Danimarca	DK	Paesi Bassi	NL
Germania	DE	Austria	AT
Estonia	EE	Polonia	PL
Grecia	EL	Portogallo	PT
Spagna	ES	Romania	RO
Francia	FR	Slovacchia	SK
Irlanda	IE	Slovenia	SI
Italia	IT	Finlandia	FI
Cipro	CY	Svezia	SE
Lettonia	LV	Regno Unito	UK
Lituania	LT		

3. ***Analisi funzionale***

3.1. *Accessibilità del sistema*

Le richieste a norma dell'articolo 3 della decisione 2008/615/GAI dovrebbero pervenire ad una determinata banca dati nell'ordine cronologico in cui ciascuna di esse è stata inviata, le risposte dovrebbero essere trasmesse in modo da pervenire allo Stato membro richiedente entro 15 minuti dall'arrivo delle richieste.

3.2. *Seconda fase*

Quando uno Stato membro riceve una relazione su una concordanza, spetta al suo punto di contatto nazionale raffrontare i valori del profilo oggetto della richiesta ed i valori del profilo (dei profili) ricevuto/i in risposta per convalidare e controllare il valore probatorio del profilo. I punti di contatto nazionali possono mettersi direttamente in contatto gli uni con gli altri per effettuare le convalide.

Le procedure di assistenza giudiziaria iniziano dopo la convalida della concordanza esistente tra due profili, in base alla «concordanza totale» o alla «quasi concordanza» riscontrata nel corso della fase di consultazione automatizzata.

4. ***Documento di controllo dell'interfaccia (ICD) per profili DNA***

4.1. *Introduzione*

4.1.1. Obiettivi

Il presente capo definisce i requisiti dello scambio di informazioni relative al profilo DNA tra i sistemi di banche dati sul DNA di tutti gli Stati membri. I campi dell'intestazione sono definiti specificamente per lo scambio di dati sul DNA in ambito Prüm, la parte di dati si basa sulla parte di dati del profilo DNA contenuto nello schema XML definito per il gateway di scambio di dati sul DNA dell'Interpol.

Lo scambio di dati avviene tramite SMTP (protocollo semplice per il trasferimento di posta) ed altre tecnologie di punta, usando un server centrale di relay dei messaggi fornito dal gestore di rete. Il file XML è trasportato come corpo del messaggio.

▼B

4.1.2. Campo di applicazione

Questo ICD definisce unicamente il contenuto del messaggio. Tutti gli elementi specifici della rete e dei messaggi sono definiti in modo uniforme per dare allo scambio di dati sul DNA una base tecnica comune.

Gli elementi definiti sono i seguenti:

— formato del campo «oggetto» del messaggio, in modo da rendere possibile/consentire il trattamento automatizzato dei messaggi,

— necessità o meno di cifrare il contenuto e, in caso affermativo, metodi da utilizzare,

— lunghezza massima dei messaggi.

4.1.3. Struttura e principi XML

La struttura del messaggio XML comprende:

— una parte di intestazione, contenente informazioni sulla trasmissione, e

— una parte di dati, contenente informazioni specifiche sul profilo ed il profilo stesso.

Per la richiesta e per la risposta si utilizza lo stesso schema XML.

Per un controllo completo dei profili DNA non identificati (articolo 4 della decisione 2008/615/GAI) è possibile inviare in un unico messaggio un gruppo di profili. Deve essere stabilito un numero massimo di profili per messaggio. Il numero dipende dalle dimensioni massime del messaggio elettronico consentite e viene stabilito dopo aver scelto il server di posta elettronica.

Esempio di XML:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> datas structure repeated, if multiple profiles sent by (….) a single SMTP message, only allowed for Articolo 4 cases

</datas>]

</PRUEMDNA>

4.2. *Definizione della struttura XML*

Le seguenti indicazioni sono fornite per fini documentari e una migliore leggibilità, le informazioni realmente vincolanti sono contenute in un file di schema XML (PRUEM DNA.xsd).

▼B

4.2.1. Schema PRUEMDNAx

Contiene i seguenti campi:

Fields	Type	Description
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. Contenuto della struttura dell'intestazione

4.2.2.1. Intestazione PRUEM

È una struttura che descrive l'intestazione del file XML. Contiene i seguenti campi:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting Member State info
requested	PRUEM_header_info	Requested Member State info

4.2.2.2. PRUEM_header dir

Tipo di dati contenuti nel messaggio, possono avere il seguente valore:

Value	Description
R	Request
A	Answer

4.2.2.3. Informazioni sull'intestazione PRUEM

La struttura fornisce indicazioni sullo Stato membro e sulla data/ora del messaggio Contiene i seguenti campi:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting Member State
destination_isocode	String	ISO 3166-2 code of the requested Member State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message
time	Time	Time of creation of message

4.2.3. Contenuto dei dati del profilo PRUEM

4.2.3.1. PRUEM_datas

È una struttura che descrive la parte di dati del profilo XML. Contiene i seguenti campi:

▼B

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique Member State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality ! = 0 (the original requested profile), then empty

4.2.3.2. PRUEM_request_type

Tipo di dati contenuti nel messaggio, possono avere il seguente valore:

Value	Description
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: Case «No Hit»: original requesting profile sent back only; Case «Hit»: original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)
4	Hit with mismatch

▼B

4.2.3.4. PRUEM_data_type

Tipo di dati contenuti nel messaggio, possono avere il seguente valore:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Tipo di dati contenuti nel messaggio, possono avere il seguente valore:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6. IPSG_DNA_profile

Struttura che descrive un profilo DNA. Contiene i seguenti campi:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7. IPSG_DNA_ISSOL

Struttura contenente i loci ISSOL (gruppo standard di loci dell'Interpol). Contiene i seguenti campi:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179

▼B

Fields	Type	Description
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogenin

4.2.3.8. IPSG_DNA_additional_loci

Struttura contenente gli altri loci. Contiene i seguenti campi:

Fields	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Struttura che descrive un locus. Contiene i seguenti campi:

Fields	Type	Description
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. ***Architettura delle applicazioni, della sicurezza e della comunicazione***

5.1. *Elementi generali*

Per utilizzare le applicazioni per lo scambio di dati sul DNA nel quadro della decisione 2008/615/GAI gli Stati membri si servono di una rete di comunicazione comune che sarà ovviamente riservata. Onde sfruttare più efficacemente questa infrastruttura di comunicazione comune per l'invio

▼B

delle richieste e la ricezione delle risposte, viene impiegato un meccanismo asincrono che trasmette le richieste di dati sul DNA e di dati dattiloscopici in un messaggio e-mail SMTP incapsulato (wrapped). Tenuto conto dei problemi connessi con la sicurezza, per stabilire un vero e proprio tunnel sicuro da punto a punto lungo la rete si utilizzerà il meccanismo S/MIME come estensione della funzionalità SMTP.

Come rete di comunicazione per lo scambio di dati tra Stati membri è utilizzata la rete operativa TESTA (Servizi transeuropei per la telematica tra amministrazioni), di cui è responsabile la Commissione europea. Poiché le banche dati nazionali sul DNA e gli attuali punti di accesso nazionali alla rete TESTA possono essere ubicati in siti diversi negli Stati membri, per accedere alla rete TESTA si può:

1) utilizzare il punto di accesso nazionale esistente o istituire un nuovo punto di accesso nazionale alla rete TESTA; oppure

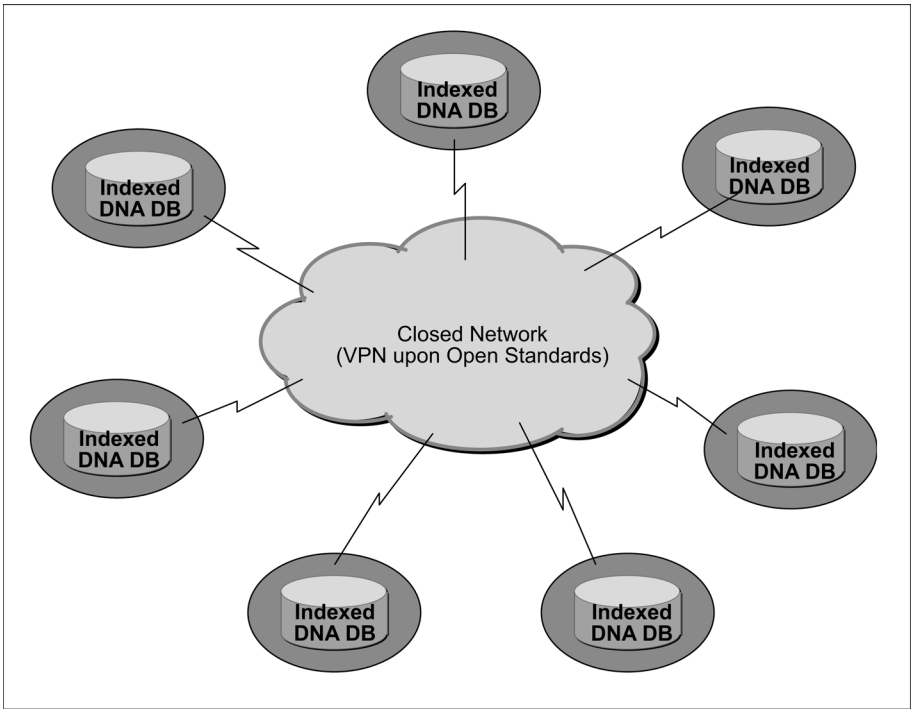
2) creare un collegamento locale sicuro tra il sito ove si trova la banca dati sul DNA e ove essa è gestita dall'agenzia nazionale competente ed il punto di accesso nazionale alla rete TESTA esistente.

I protocolli e le norme utilizzati per mettere in atto le applicazioni previste dalla decisione 2008/615/GAI sono conformi alle norme aperte ed ai requisiti imposti dai responsabili della sicurezza nazionale degli Stati membri.

5.2. *Architettura del livello superiore*

Il campo di applicazione della decisione 2008/615/GAI prevede che ciascuno Stato membro metta a disposizione i suoi dati sul DNA perché vengano scambiati con o consultati da altri Stati membri secondo il formato dati uniforme standardizzato. L'architettura si basa su un modello di comunicazione «any to any». Non esiste né un server centrale né una banca dati centralizzata in cui conservare i profili DNA.

Fig. 1: Topologia dello scambio di dati sul DNA



▼B

Fatto salvo il rispetto dei vincoli nazionali di natura giuridica presso i siti degli Stati membri, ciascuno Stato membro può decidere il tipo di hardware e di software da utilizzare nel proprio sito per la configurazione al fine di conformarsi ai requisiti della decisione 2008/615/GAI.

5.3. *Norme di sicurezza e protezione dei dati*

Sono stati presi in considerazione e messi in atto tre livelli di sicurezza:

5.3.1. Livello dei dati

I dati relativi al profilo DNA forniti da ciascuno Stato membro devono essere preparati conformemente a norme comuni di protezione dei dati, di conseguenza agli Stati membri richiedenti sarà essenzialmente comunicato che la risposta è positiva (hit) o negativa (no hit), e nel caso di risposta positiva sarà loro fornito un numero di identificazione che non contiene alcuna informazione di carattere personale. Le ulteriori indagini condotte in seguito alla notifica di una risposta positiva saranno effettuate a livello bilaterale conformemente alle disposizioni giuridiche e organizzative nazionali che vigono nei siti degli Stati membri in questione.

5.3.2. Livello della comunicazione

Prima di essere trasmessi ai siti di altri Stati membri, i messaggi (di richiesta e di risposta) contenenti informazioni relative a profili DNA saranno cifrati tramite un meccanismo di punta, quale l'S/MIME, conforme a norme aperte.

5.3.3. Livello della trasmissione

Tutti i messaggi cifrati contenenti informazioni relative a profili DNA saranno trasmessi ai siti degli altri Stati membri attraverso un sistema di tunnel virtuali privati amministrato a livello internazionale da un gestore di rete fidato, mentre le connessioni sicure a tale sistema di tunnel saranno di responsabilità nazionale. Questo sistema di tunnel virtuali privati non dispone di un punto di connessione con l'Internet accessibile al pubblico.

5.4. *Protocolli e norme da utilizzare per il meccanismo di cifratura: S/MIME e relativi pacchetti*

Per la cifratura di messaggi contenenti informazioni relative al profilo DNA si utilizzerà la norma aperta S/MIME come estensione della norma SMTP abitualmente usata per i messaggi elettronici. Il protocollo S/MIME (V3) consente di realizzare ricevute firmate, etichette di sicurezza ed elenchi di destinatari sicuri e si basa sulla Sintassi dei messaggi crittografati (CMS), una specifica IETF per i messaggi cifrati protetti. Può essere utilizzata per la firma digitale, il compendio, l'autenticazione o la cifratura di qualsiasi tipo di dati digitali.

Il certificato su cui si basa il meccanismo S/MIME deve essere conforme alla norma X.509. Per garantire l'uso di norme e procedure comuni con altre applicazioni in ambito Prüm, le norme di trattamento da applicare nelle operazioni di cifratura S/MIME o in vari ambienti COTS sono le seguenti:

— la sequenza delle operazioni è: prima la cifratura e poi la firma,

— per la cifratura simmetrica e asimmetrica si applicano, rispettivamente, gli algoritmi di cifratura AES (Advanced Encryption Standard — Norma di cifratura avanzata), con chiave di 256 bit, e RSA, con chiave di 1 024 bit,

— si applica l'algoritmo di hash SHA-1.

▼B

La funzionalità S/MIME è presente nella maggior parte dei moderni pacchetti di software per posta elettronica compresi Outlook, Mozilla Mail e Netscape Communicator 4.x ed assicura l'interoperabilità fra tutti i principali pacchetti di software per posta elettronica.

Essendo facilmente integrabile nell'infrastruttura informatica nazionale di tutti i siti degli Stati membri, S/MIME è stato scelto quale meccanismo in grado di garantire la sicurezza al livello della comunicazione. Tuttavia, per realizzare in modo più efficace l'obiettivo della dimostrazione di fattibilità (proof of concept) e ridurre i costi, per la prototipazione dello scambio di dati sul DNA si è scelta la norma aperta API JavaMail. JavaMail API effettua la semplice cifratura e decifratura dei messaggi elettronici utilizzando S/MIME e/o il PGP aperto. L'intento è quello di fornire un'API unica e di facile utilizzazione agli utenti che desiderano inviare e ricevere messaggi elettronici cifrati in uno dei due più comuni formati di cifratura della posta elettronica. Pertanto per soddisfare i requisiti della decisione 2008/615/GAI sarà sufficiente qualsiasi applicazione di punta di JavaMail API, ad esempio la JCE (Java Cryptographic Extension) della Bouncy Castle, che si utilizzerà per applicare l'S/MIME alla prototipazione dello scambio di dati sul DNA fra tutti gli Stati membri.

5.5. *Architettura dell'applicazione*

Ciascuno Stato membro fornirà agli altri Stati membri una serie di dati standardizzati relativi al profilo DNA conformi all'ICD comune in vigore. Ciò può avvenire o fornendo una rappresentazione delle banche dati nazionali, oppure istituendo materialmente una banca dati esportata (banca dati indicizzata).

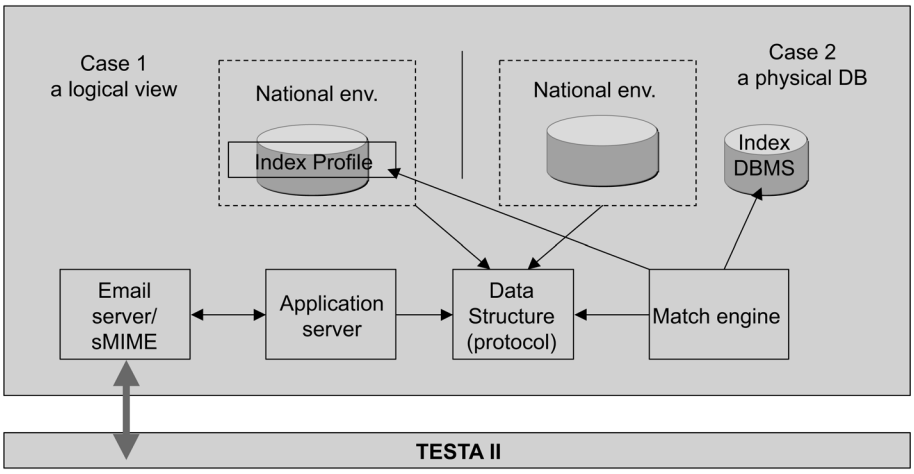
Le quattro componenti principali (server e-mail/S/MIME, server dell'applicazione, area della struttura dei dati per il recupero/inserimento dei dati e la registrazione di messaggi in entrata/in uscita e motore per la ricerca di corrispondenze) seguono la logica globale dell'applicazione in modo indipendente dal prodotto.

Per consentire a tutti gli Stati membri di integrare agevolmente le componenti nei rispettivi siti nazionali, la funzionalità comune specifica è stata applicata mediante componenti liberi (open source), che ciascuno Stato membro ha potuto scegliere in base alla politica ed ai regolamenti nazionali in materia di tecnologia dell'informazione. Considerate le caratteristiche indipendenti da implementare per accedere a banche dati indicizzate contenenti profili DNA contemplate dalla decisione 2008/615/GAI, ogni Stato membro può scegliere liberamente la propria piattaforma di hardware e software, inclusi la banca dati ed i sistemi operativi.

Un prototipo per lo scambio di dati relativi al DNA è stato messo a punto e sperimentato con successo sulla rete comune esistente. La versione 1.0 è stata applicata nell'ambiente produttivo ed è utilizzata per le operazioni correnti. Gli Stati membri possono utilizzare il prodotto messo a punto congiuntamente, ma anche svilupparne di propri. Le componenti del prodotto comune saranno sottoposte a manutenzione, personalizzate e ulteriormente sviluppate conformemente all'evoluzione della TI ed alle esigenze di polizia di ordine forense e/o funzionale.

▼B

Figura 2: Quadro della topologia dell'applicazione



5.6. *Protocolli e norme da utilizzare per l'architettura dell'applicazione*

5.6.1. XML

Lo scambio di dati sul DNA sfrutterà pienamente lo schema XML come allegato a messaggi elettronici SMTP. L'XML (linguaggio di marcatura estensibile) è un linguaggio di marcatura di uso generale per la creazione di linguaggi di marcatura specifici raccomandato dal W3C ed è in grado di descrivere molti tipi diversi di dati. La descrizione del profilo DNA appropriato per lo scambio fra gli Stati membri è stata effettuata tramite l'XML e lo schema XML nel documento ICD.

5.6.2. ODBC

La connettività aperta della banca dati (ODBC) è un metodo standard di software API per l'accesso ai sistemi di gestione della banca dati indipendentemente dai linguaggi di programmazione, dal tipo di banca dati e dai sistemi operativi. Tuttavia l'ODBC presenta alcuni inconvenienti. La gestione di un gran numero di macchine clienti può comportare una molteplicità di driver e DLL e tale complessità può rendere più difficile la gestione del sistema.

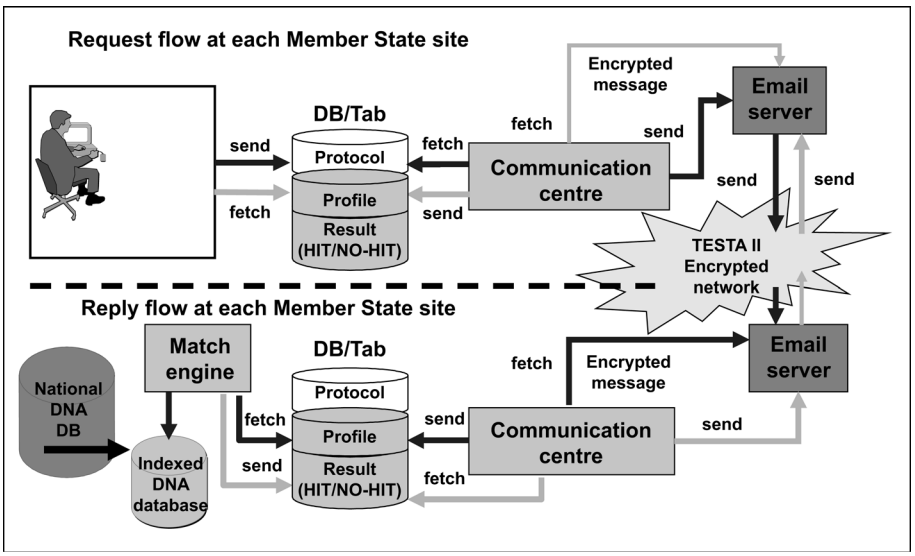
5.6.3. JDBC

La connettività Java a banche dati (JDBC) è un API per linguaggio di programmazione Java che definisce le modalità d'accesso del cliente a una banca dati. A differenza dell'ODBC, la JDBC non richiede l'uso di una specifica serie di DLL locali sul desktop.

Il seguente diagramma descrive la logica funzionale del trattamento delle richieste di profili DNA e delle relative risposte presso il sito di ogni Stato membro. Sia il flusso delle richieste che quello delle risposte interagiscono con un'area di dati neutra che comprende diversi insiemi di dati aventi una struttura di dati comune.

▼B

Figura 3: Quadro del flusso di dati presso il sito di ogni Stato membro



5.7 *Ambiente di comunicazione*

5.7.1. Rete di comunicazione comune: TESTA e la relativa infrastruttura di follow-up

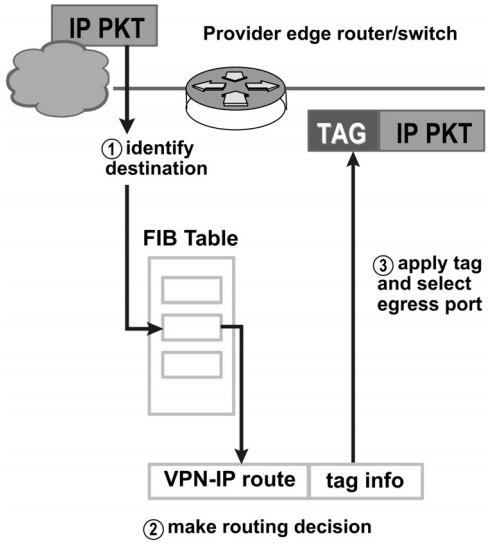
Lo scambio di dati sul DNA si servirà della posta elettronica, un meccanismo asincrono, per l'invio delle richieste e la ricezione delle risposte tra gli Stati membri. Poiché tutti gli Stati membri dispongono almeno di un punto di accesso nazionale alla rete TESTA, lo scambio di dati sul DNA avverrà attraverso questa rete. La rete TESTA offre una serie di servizi a valore aggiunto tramite il suo relay di posta elettronica. Oltre ad ospitare le specifiche caselle di posta elettronica di TESTA, l'infrastruttura può gestire elenchi di distribuzione e politiche di instradamento. Pertanto TESTA può essere usata come centro di raccolta e scambio dei messaggi indirizzati alle amministrazioni collegate con tutti i domini UE. Possono essere attivati anche meccanismi di controllo dei virus.

Il relay di posta elettronica TESTA si basa su una piattaforma hardware di elevata disponibilità situata presso la struttura centrale dell'applicazione TESTA e protetta da un firewall. I servizi del sistema dei nomi di dominio (DNS) di TESTA convertono gli URL in indirizzi IP ed occultano all'utente ed alle applicazioni le questioni relative all'indirizzamento.

5.7.2. Questioni relative alla sicurezza

Nell'ambito della rete TESTA è stato applicato il concetto di rete privata virtuale (VPN). La tecnica della commutazione di tag (Tag Switching) utilizzata per costruire questa VPN evolverà per supportare lo standard di commutazione di etichetta multiprotocollo (MPLS) messo a punto dall'Internet Engineering Task Force (IETF).

▼B



L'MPLS è una tecnologia standard dell'IETF che rende più rapido il flusso di traffico sulla rete evitando che i pacchetti siano analizzati dai router intermedi (salti). Ciò avviene tramite cosiddette etichette attaccate al pacchetto dai router perimetrali della dorsale, in base alle informazioni memorizzate nella tabella di inoltro (Forwarding Information Base — FIB). Le etichette sono utilizzate anche per implementare reti private virtuali (VPN).

L'MPLS unisce i vantaggi dell'instradamento di livello 3 a quelli della commutazione di livello 2. Poiché gli indirizzi IP non sono valutati mentre transitano lungo la dorsale, l'MPLS non impone alcuna limitazione all'assegnazione degli indirizzi IP.

Inoltre i messaggi di posta elettronica veicolati dalla rete TESTA saranno protetti da un meccanismo di cifratura controllato da S/MIME. Nessuno può decifrare i messaggi che passano lungo la rete senza conoscere la chiave ed essere in possesso del certificato appropriato.

5.7.3. Protocolli e norme da utilizzare nella rete di comunicazione

5.7.3.1. SMPT

Il protocollo semplice per il trasferimento di posta (SMTP) è di fatto il protocollo standard per la trasmissione di messaggi elettronici su Internet. L'SMPT è un protocollo relativamente semplice, su base testuale, in cui vengono specificati uno o più destinatari del messaggio, con la successiva trasmissione del contenuto testuale del messaggio. L'SMTP utilizza il protocollo TCP porta 25 su specifica dell'IETF. Per determinare il server SMTP per un certo nome di dominio si usa il record MX (Mail eXchange) del DNS (sistema dei nomi di dominio).

Poiché inizialmente questo protocollo era puramente basato su testo ASCII, non gestiva correttamente i file binari. Protocolli standard come la MIME sono stati messi a punto per codificare file binari da trasferire tramite SMTP. Oggi la maggior parte dei server SMTP supporta l'estensione 8BITMIME e S/MIME, rendendo il trasferimento di file binari quasi altrettanto agevole di quello di testo in chiaro. Le norme di trattamento applicabili alle operazioni S/MIME sono descritte nella sezione corrispondente (cfr. capo 5.4).

L'SMTP è un protocollo push che non consente di estrarre (pull) messaggi da un server remoto su richiesta. Per far ciò un programma di gestione della posta elettronica (mail client) deve usare POP3 o IMAP. Nel quadro dello scambio di dati sul DNA si è convenuto di utilizzare il protocollo POP3.

▼B

5.7.3.2. POP

I programmi locali di gestione della posta elettronica utilizzano il protocollo POP versione 3 (POP3), un protocollo standard Internet di livello applicativo, per estrarre messaggi di posta elettronica da un server remoto su una connessione TCP/IP. Servendosi della funzione «submit profile» del protocollo SMTP, i programmi di gestione della posta elettronica inviano messaggi attraverso Internet o reti aziendali. Nella posta elettronica, la MIME funge da standard per gli allegati e il testo non ASCII. Benché né il POP3 né l'SMTP richiedano messaggi elettronici formattati su base MIME, la posta elettronica su Internet ha essenzialmente un formato MIME, ed i POP client devono pertanto capire e utilizzare anche tale estensione. Tutto l'ambiente di comunicazione della decisione 2008/615/GAI comprenderà pertanto le componenti del protocollo POP.

5.7.4. Assegnazione degli indirizzi di rete

Ambiente operativo

Un blocco dedicato di sottorete di classe C è stato attualmente assegnato a TESTA dall'autorità europea di registrazione IP (RIPE). Se necessario, ulteriori blocchi di indirizzi possono essere assegnati a TESTA in futuro. L'assegnazione di indirizzi IP agli Stati membri si basa su uno schema geografico in Europa. Lo scambio di dati tra Stati membri nel quadro della decisione 2008/615/GAI è operato su una rete IP protetta logicamente riconducibile a livello europeo.

Ambiente di prova

Per assicurare il buon funzionamento delle operazioni quotidiane nei collegamenti tra tutti gli Stati membri, è necessario stabilire un ambiente di prova sulla rete chiusa per i nuovi Stati membri che si preparano ad accedere alle operazioni. È stato messo a punto un elenco di parametri che comprende indirizzi IP, parametri di rete, domini di posta elettronica e accrediti utente e che dovrebbe figurare nel sito dei rispettivi Stati membri. È stata inoltre costruita una serie di pseudo profili DNA a fini di prova.

5.7.5. Parametri di configurazione

È istituito un sistema sicuro di posta elettronica tramite il dominio eu-admin.NET che, insieme agli indirizzi associati, sarà accessibile soltanto da una posizione del dominio di livello TESTA EU, perché i nomi sono noti solo sul server centrale DNS TESTA, che è schermato dall'Internet.

La mappatura di questi indirizzi di sito TESTA (nomi di ospiti) ai rispettivi indirizzi IP è curata dal servizio TESTA DNS. Per ogni dominio locale, è aggiunta una voce di posta elettronica al server centrale DNS TESTA, che collega tutti i messaggi di posta elettronica inviati ai domini locali TESTA alla centrale di posta elettronica TESTA. Tale centrale li trasmette quindi al server di posta elettronica del dominio locale attraverso gli indirizzi elettronici del dominio locale. Collegando in questo modo la posta elettronica, le informazioni riservate contenute nei messaggi elettronici passano solo attraverso l'infrastruttura di rete chiusa a livello europeo e non attraverso la poco sicura Internet.

▼B

Occorre stabilire sottodomini (***in corsivo grassetto***) nei siti di tutti gli Stati membri secondo la sintassi seguente:

«***tipo di applicazione.*****pruem.*****Codice Stato membro.***eu-admin.NET», dove:

«Codice Stato membro» ha il valore del codice a due lettere dello Stato membro (ad esempio: AT, BE ecc.).

«***tipo di applicazione***» ha uno dei valori: DNA o FP.

Applicando la sintassi di cui sopra, i sottodomini degli Stati membri figurano nella tabella seguente:

MS	Sub Domains	Comments
BE	***dna*.pruem.be**.eu-admin.NET	Setting up a secure local link to the existing TESTA II access point
	***fp*.pruem.be**.eu-admin.NET	
BG	***dna*.pruem.bg**.eu-admin.NET	
	***fp*.pruem.bg**.eu-admin.NET	
CZ	***dna*.pruem.cz**.eu-admin.NET	
	***fp*.pruem.cz**.eu-admin.NET	
DK	***dna*.pruem.dk**.eu-admin.NET	
	***fp*.pruem.dk**.eu-admin.NET	
DE	***dna*.pruem.de**.eu-admin.NET	Using the existing TESTA II national access points
	***fp*.pruem.de**.eu-admin.NET	
EE	***dna*.pruem.ee**.eu-admin.NET	
	***fp*.pruem.ee**.eu-admin.NET	
IE	***dna*.pruem.ie**.eu-admin.NET	
	***fp*.pruem.ie**.eu-admin.NET	
EL	***dna*.pruem.el**.eu-admin.NET	
	***fp*.pruem.el**.eu-admin.NET	
ES	***dna*.pruem.es**.eu-admin.NET	Using the existing TESTA II national access point
	***fp*.pruem.es**.eu-admin.NET	
FR	***dna*.pruem.fr**.eu-admin.NET	Using the existing TESTA II national access point
	***fp*.pruem.fr**.eu-admin.NET	
IT	***dna*.pruem.it**.eu-admin.NET	
	***fp*.pruem.it**.eu-admin.NET	
CY	***dna*.pruem.cy**.eu-admin.NET	
	***fp*.pruem.cy**.eu-admin.NET	

▼B

MS	Sub Domains	Comments
LV	***dna*.pruem.lv**.eu-admin.NET	
	***fp*.pruem.lv**.eu-admin.NET	
LT	***dna*.pruem.lt**.eu-admin.NET	
	***fp*.pruem.lt**.eu-admin.NET	
LU	***dna*.pruem.lu**.eu-admin.NET	Using the existing TESTA II national access point
	***fp*.pruem.lu**.eu-admin.NET	
HU	***dna*.pruem.hu**.eu-admin.NET	
	***fp*.pruem.hu**.eu-admin.NET	
MT	***dna*.pruem.mt**.eu-admin.NET	
	***fp*.pruem.mt**.eu-admin.NET	
NL	***dna*.pruem.nl**.eu-admin.NET	Intending to establish a new TESTA II access point at the NFI
	***fp*.pruem.nl**.eu-admin.NET	
AT	***dna*.pruem.at**.eu-admin.NET	Using the existing TESTA II national access point
	***fp*.pruem.at**.eu-admin.NET	
PL	***dna*.pruem.pl**.eu-admin.NET	
	***fp*.pruem.pl**.eu-admin.NET	
PT	***dna*.pruem.pt**.eu-admin.NET	……
	***fp*.pruem.pt**.eu-admin.NET	……
RO	***dna*.pruem.ro**.eu-admin.NET	
	***fp*.pruem.ro**.eu-admin.NET	
SI	***dna*.pruem.si**.eu-admin.NET	.....
	***fp*.pruem.si**.eu-admin.NET	.....
SK	***dna*.pruem.sk**.eu-admin.NET	
	***fp*.pruem.sk**.eu-admin.NET	
FI	***dna*.pruem.fi**.eu-admin.NET	*[To be inserted]*
	***fp*.pruem.fi**.eu-admin.NET	
SE	***dna*.pruem.se**.eu-admin.NET	
	***fp*.pruem.se**.eu-admin.NET	
UK	***dna*.pruem.uk**.eu-admin.NET	
	***fp*.pruem.uk**.eu-admin.NET	

▼B

CAPO 2: **Scambio di dati dattiloscopici (documento di controllo dell'interfaccia)**

Scopo del seguente documento di controllo dell'interfaccia è definire i criteri dello scambio di informazioni dattiloscopiche tra i sistemi di identificazione automatizzati delle impronte digitali (AFIS) degli Stati membri. Si basa sull'attuazione Interpol dell'ANSI/NIST-ITL 1-2000 (INT-I, versione 4.22b).

Tale versione copre tutte le definizioni di base dei record logici tipo-1, tipo-2, tipo-4, tipo-9, tipo-13 e tipo-15 richiesti per l'elaborazione dattiloscopica basata sulle minuzie.

1. ***Descrizione del contenuto dei file***

Un file dattiloscopico è formato da vari record logici: ve ne sono sedici specificati nella norma originale ANSI/NIST-ITL 1-2000. Tra ciascun record e tra i campi e sottocampi all'interno dei record sono inseriti adeguati separatori ASCII.

Solo 6 tipi di record sono usati per lo scambio d'informazioni tra l'agenzia d'origine e quella di destinazione:

Tipo-1	→	informazioni sulla transazione
Tipo-2	→	dati alfanumerici persone/caso
Tipo-4	→	immagini dattiloscopiche a scala di grigi ad alta risoluzione
Tipo-9	→	record di minuzie
Tipo-13	→	record d'immagine latente a risoluzione variabile
Tipo-15	→	record d'immagine dell'impronta palmare a risoluzione variabile

1.1. *Tipo-1 — Intestazione*

Contiene informazioni sull'instradamento e la descrizione della struttura del resto del file. Questo tipo di record definisce inoltre i tipi di transazione che rientrano nelle grandi categorie seguenti.

1.2. *Tipo-2 — Descrizione*

Contiene informazioni testuali che interessano le agenzie mittenti e riceventi.

1.3. *Tipo-4 — Immagini a scala di grigi ad alta risoluzione*

Usato per lo scambio di immagini dattiloscopiche a scala di grigi (otto bit) raccolte a 500 pixel/pollice. Le immagini dattiloscopiche sono compresse con l'algoritmo WSQ e un rapporto non superiore a 15:1. Non si devono usare altri algoritmi di compressione o immagini non compresse.

1.4. *Tipo-9 — Record di minuzie*

Sono usati per lo scambio di dati sulle caratteristiche delle creste o sulle minuzie, allo scopo in parte di evitare doppioni inutili dei processi di codificazione AFIS e in parte di consentire la trasmissioni di codici AFIS che contengono meno dati delle immagini corrispondenti.

▼B

1.5. *Tipo-13 — Record d'immagine latente a risoluzione variabile*

È usato per scambiare immagini latenti d'impronte digitali e palmari a risoluzione variabile insieme a informazioni alfanumeriche sulla tessitura. La risoluzione della scansione delle immagini è di 500 pixel/pollice con 256 sfumature di grigio. Se la qualità dell'immagine latente è sufficiente, è compressa con l'algoritmo WSQ. Se necessario, la risoluzione delle immagini può essere espansa a più di 500 pixel/pollice e più di 256 sfumature di grigio, previo accordo bilaterale. In questo caso, si raccomanda vivamente l'uso del JPEG 2000 (cfr. appendice 7).

1.6. *Record d'immagine dell'impronta palmare a risoluzione variabile*

Il record d'immagine a etichetta tipo-15 è usato per scambiare immagini d'impronte palmari a risoluzione variabile insieme a informazioni alfanumeriche sulla tessitura. La risoluzione della scansione delle immagini è di 500 pixel/pollice con 256 sfumature di grigio. Per ridurre al minimo l'insieme dei dati, tutte le immagini d'impronte palmari sono compresse con l'algoritmo WSQ. Se necessario, la risoluzione delle immagini può essere espansa a più di 500 pixel/pollice e più di 256 sfumature di grigio, previo accordo bilaterale. In questo caso, si raccomanda vivamente l'uso del JPEG 2000 (cfr. appendice 7).

2. ***Formato del record***

Un file operativo è composto da uno o più record logici. Per ciascun record nel file sono presenti vari campi compatibili con quel tipo di record. Ciascun campo può contenere uno o più elementi d'informazione monovalore. L'insieme degli elementi d'informazione che compongono il campo definiscono il valore del campo stesso. Un campo d'informazione può anche essere composto da una o più elementi d'informazione raggruppati e ripetuti più volte all'interno del campo. Tale gruppo d'informazioni è noto come sottocampo. Un campo d'informazione può quindi essere composto da uno o più sottocampi.

2.1. *Separatori d'informazioni*

Nei record logici di campo a etichetta (tagged-field logical records) i meccanismi per delimitare l'informazione sono attuati tramite quattro separatori ASCII dell'informazione. Le informazioni delimitate possono essere voci all'interno di un campo o di un sottocampo, campi entro un record logico o ripetizioni multiple di sottocampi. I separatori di informazioni sono definiti nella norma ANSI X3.4. I caratteri sono usati per delimitare e qualificare logicamente l'informazione. In ordine d'importanza, il separatore di file «FS» è il più inclusivo, seguito dal separatore di gruppo «GS», dal separatore di record «RS» e infine dal separatore di unità «US». La tabella 1 contiene un elenco dei separatori ASCII con una descrizione del relativo uso nell'ambito della suddetta norma.

I separatori d'informazione dovrebbero dare un'indicazione del tipo di dati che segue. Il carattere «US» separa le informazioni individuali all'interno di un campo o sottocampo: indica che l'informazione seguente appartiene a quel campo o sottocampo. Il separatore «RS» di sottocampi multipli all'interno di un campo indica l'inizio del gruppo successivo di informazioni ripetute. Il separatore «GS» tra i campi d'informazione indica l'inizio di un nuovo campo prima del numero che identifica il campo stesso. Analogamente, il separatore «FS» segnala l'inizio di un nuovo record logico.

▼B

I quattro caratteri hanno significato solo se usati come separatori di testo ASCII. Non hanno alcun significato nei record o campi binari; fanno semplicemente parte dello scambio di dati.

Di solito, un campo o un elemento d'informazione non dovrebbe essere vuoto; pertanto tra due elementi d'informazione dovrebbe apparire un solo separatore. L'eccezione a questa regola si manifesta nei casi in cui i dati sono indisponibili, mancanti o facoltativi e l'elaborazione dell'operazione non dipende dalla presenza di quel particolare dato. In tali casi, si troveranno vari separatori uno accanto all'altro al posto di dati fittizi tra i separatori.

Per definire un campo composto da tre informazioni, si applicano i seguenti criteri. Se gli elementi della seconda informazione mancano, si introducono due caratteri «US» affiancati tra la prima e la terza informazione. Se mancano gli elementi della seconda e della terza informazione, occorre introdurre tre separatori: due caratteri «US» più il separatore che indica la fine del campo o sottocampo. In generale, se uno più elementi d'informazione obbligatori o facoltativi sono indisponibili per un campo o sottocampo, occorre introdurre il numero opportuno di separatori.

È possibile trovare affiancate diverse combinazioni di due o più dei quattro separatori disponibili. Quando mancano o sono indisponibili dati per un elemento d'informazione, un sottocampo o un campo, il numero dei separatori specificati deve essere pari al numero degli elementi d'informazione, dei sottocampi o dei campi richiesti, meno uno.

Tabella 1: Separatori

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2. *Tracciato dei record*

Nei record logici di campo a etichetta, ogni campo d'informazione è numerato secondo la presente norma. Il formato di ciascun campo è composto dal numero tipo di record logico seguito da un punto «.», un numero di campo seguito da due punti «:», seguito dall'informazione corrispondente a quel campo. Il numero del campo a etichetta può essere un numero qualsiasi da 1 a 9 cifre, situato tra il punto «.» e i due punti «:»; è interpretato come numero intero di campo non assegnato. Ciò implica che il numero di campo «2.123:» è equivalente al numero di campo «2.000000123:» ed è interpretato allo stesso modo.

A titolo d'esempio, in tutto il presente documento è usato un numero a tre cifre per designare i campi contenuti in ciascuno dei record logici di campo a etichetta. I numeri di campo si presentano in forma «TT.xxx:» dove «TT» rappresenta il tipo di record a uno o due caratteri seguito dal punto. I tre caratteri successivi corrispondono al numero di campo seguito da due punti («:»). Il descrittore ASCII o i dati relativi all'immagine vengono dopo i due punti.

▼B

I record logici di tipo-1 e tipo-2 contengono solo campi di testo ASCII. Il primo campo ASCII di ciascuno di questi tipi di record permette di registrare la lunghezza del record (compresi i numeri di campo, i due punti, i separatori). Il separatore di file ASCII o carattere di controllo «FS» (che indica la fine del record logico o dell'operazione) segue l'ultimo byte d'informazione ASCII ed è incluso nella lunghezza del record.

Contrariamente al concetto del campo a etichetta, il record di tipo-4 contiene solo dati binari registrati come campi binari ordinati a lunghezza fissa. La lunghezza totale del record è registrata nel primo campo binario a quattro byte di ciascun record. Per tale record binario non è registrato né il numero di record con il relativo punto, né il numero identificatore del campo con i suoi due punti successivi. Inoltre, poiché le rispettive lunghezze di campo di questo record sono fisse o specificate, nessuno dei quattro separatori («US», «RS», «GS», o «FS») è interpretato altrimenti che come dato binario. Per quanto riguarda il record binario, il carattere «FS» non è usato come separatore o carattere terminale di un'operazione.

3. ***Record logico tipo-1: Intestazione del file***

Questo record descrive la struttura e il tipo del file e fornisce altre importanti informazioni. La serie di caratteri usati per i campi del tipo-1 è solo il codice ANSI a 7 bit per lo scambio d'informazioni.

3.1. *Campi per il record logico tipo-1*

3.1.1. Campo 1.001: Lunghezza del record logico (LEN)

Contiene il numero totale di byte nell'intero record logico del tipo-1. Il campo inizia con «1.001:», seguito dalla lunghezza totale del record compresi tutti i caratteri di tutti i campi e i separatori d'informazione.

3.1.2. Campo 1.002: Numero di versione (VER)

Per far sì che gli utenti sappiano quale versione della norma ANSI/NIST stanno usando, questo campo di 4 byte specifica il numero della versione utilizzata dal software o dal sistema che crea il file. I primi due bytes specificano il numero della versione principale, gli altri due il numero di revisione: ad esempio, la norma originale del 1986 è considerata la prima versione e denominata «0100», mentre l'attuale norma ANSI/NIST-ITL 1-2000 è la «0300».

3.1.3. Campo 1.003: Contenuto del file (CNT)

Questo campo contiene l'elenco dei record del file secondo il tipo e nell'ordine in cui appaiono nel file logico. Comporta uno o più sottocampi ognuno dei quali a sua volta contiene due elementi d'informazione che descrivono un unico record logico del file. I sottocampi sono specificati seguendo lo stesso ordine in cui i record sono registrati e trasmessi.

Il primo elemento d'informazione nel primo sottocampo è «1», (ossia, «record tipo-1»). Il secondo elemento d'informazione contiene il numero degli altri record contenuti nel file. Questo numero equivale al totale dei sottocampi rimanenti del campo 1.003.

▼B

Ciascuno dei restanti sottocampi è associato ad un record del file, e la sequenza dei sottocampi corrisponde alla sequenza dei record. Ciascun sottocampo contiene due elementi d'informazione: il primo identifica il tipo del record; il secondo è l'IDC del record. Il carattere «US» separa i due elementi d'informazione.

3.1.4. Campo 1.004: Tipo di operazione (TOT)

Questo campo contiene un codice mnemonico di tre lettere che designa il tipo d'operazione. Questi codici possono essere diversi da quelli usati in altre versioni della norma ANSI/NIST.

CPS: (Criminal Print-to-Print Search — Confronto d'impronte nel quadro di un reato) corrisponde a una ricerca di concordanza tra le impronte rilevate nel quadro di un reato e quelle registrate in una base dati. Le impronte della persona devono essere inserite nel file come immagini compresse WSQ.

In caso di risposta negativa, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2.

In caso di risposta positiva, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2,

— 1-14 record tipo-4.

La CPS TOT è sintetizzata nella tabella A.6.1 (appendice 6).

PMS: (Print-to-Latent Search — Confronto impronte/latenti) corrisponde a una ricerca di concordanza tra un insieme d'impronte e le latenti non identificate registrate in una base dati. La risposta contiene la decisione positiva/negativa della ricerca di destinazione AFIS. Se esistono varie latenti non identificate, saranno trasmesse varie operazioni SRE, con una latente per operazione. Le impronte della persona devono essere inserite nel file come immagini compresse WSQ.

In caso di risposta negativa, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2.

In caso di risposta positiva, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2,

— 1 record tipo-13.

La PMS TOT è sintetizzata nella tabella A.6.1 (appendice 6).

MPS: (Latent-to-Print Search — Confronto latenti-impronte) corrisponde alla ricerca di concordanza tra una latente rilevata e le impronte registrate in una base dati. Le informazioni sulle minuzie latenti e l'immagine (compressa WSQ) devono essere inserite nel file.

In caso di risposta negativa, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2.

▼B

In caso di risposta positiva, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2,

— 1 record tipo-4 o tipo-15.

La MPS TOT è sintetizzata nella tabella A.6.4 (appendice 6).

MMS: (Latent-to-Latent Search — Confronto latente-latente): il file contiene una latente che va confrontata con le latenti non identificate registrate in una base dati per stabilire se vi siano legami tra diverse scene di reato. Le informazioni relative alle minuzie latenti e l'immagine (compressa WSQ) devono essere inserite nel file.

In caso di risposta negativa, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2.

In caso di risposta positiva, sono trasmessi i record logici seguenti:

— 1 record tipo-1,

— 1 record tipo-2,

— 1 record tipo-13.

L'MMS TOT è sintetizzata nella tabella A.6.4 (appendice 6).

SRE: Questa operazione è trasmessa dall'agenzia di destinazione in risposta a trasmissioni dattiloscopiche. La risposta contiene la decisione positiva/negativa della ricerca di destinazione AFIS. Se esistono vari candidati, sono trasmesse varie operazioni SRE, con un candidato per operazione.

L'SRE TOT è sintetizzata nella tabella A.6.2 (appendice 6).

ERR: Questa operazione è trasmessa alla destinazione AFIS per indicare un errore nell'operazione. Comprende un campo messaggio (ERM) con l'indicazione dell'errore. Sono trasmessi i seguenti record logici:

— 1 record tipo-1,

— 1 record tipo-2.

L'ERR TOT è sintetizzata nella tabella A.6.3 (appendice 6).

Tabella 2: Codici ammessi nelle operazioni

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

▼B

Legenda:

M = mandatory (obbligatorio)

M* = può essere incluso soltanto uno dei due tipi di record

O = facoltativo

C = condizionale secondo disponibilità dei dati

— = non consentito

1* = condizionale secondo i sistemi di legacy

3.1.5. Campo 1.005: Data dell'operazione (DAT — Date of transaction)

Questo campo indica la data di inizio dell'operazione e deve rispettare il formato della norma ISO: YYYYMMDD

dove YYYY sta per l'anno, MM per il mese e DD per il giorno del mese. Gli zero non significativi sono usati per i numeri a una cifra. Ad esempio, «19931004» sta per 4 Ottobre 1993.

3.1.6. Campo 1.006: Priorità (PRY — Priority)

Questo campo facoltativo definisce la priorità della richiesta, secondo una scala da 1 a 9. «1» è la priorità più alta e «9» la più bassa. Le operazioni con priorità «1» sono trattate immediatamente.

3.1.7. Campo 1.007: Identificativo dell'agenzia di destinazione (DAI-Destination Agency Identifier)

Questo campo specifica l'agenzia di destinazione dell'operazione.

Consiste in due informazioni nel formato seguente: *CC/agenzia*.

La prima è il codice paese secondo la norma ISO 3166: due caratteri alfanumerici. La seconda, *agenzia*, è un testo libero di 32 caratteri alfanumerici al massimo, che identifica l'agenzia.

3.1.8. Campo 1.008: Identificativo dell'agenzia d'origine (ORI — Originating Agency Identifier)

Questo campo specifica l'originatore del file nello stesso formato del DAI (Campo 1.007).

3.1.9. Campo 1.009: Numero di controllo dell'operazione (TCN — Transaction Control Number)

È un numero di controllo a fini di riferimento. Dovrebbe essere generato dal computer nel formato seguente: YYSSSSSSSSA

dove YY sta per l'anno dell'operazione, SSSSSSSS sta per un numero di serie a otto cifre e A è un carattere di controllo generato mediante la procedura riportata nell'appendice 2.

Se un TCN non è disponibile, il campo YYSSSSSSSS è riempito da zeri e il carattere di controllo è generato come detto.

3.1.10. Campo 1.010: Risposta del controllo dell'operazione (TCR — Transaction Control Response)

Nella risposta a una richiesta in questo campo facoltativo figura il numero di controllo dell'operazione del messaggio di richiesta. Il campo avrà quindi lo stesso formato del TCN (Campo 1.009).

▼B

3.1.11. Campo 1.011: Risoluzione nativa della scansione (NSR — Native Scanning Resolution)

Questo campo specifica la risoluzione normale della scansione del sistema dell'originatore dell'operazione. La risoluzione è specificata da un numero a due cifre seguito da due decimali.

Per tutte le operazioni ai sensi della decisione 2008/615/GAI il campionamento è 500 pixel/pollice o 19,68 pixel/mm.

3.1.12. Campo 1.012: Risoluzione di trasmissione nominale (NTR — Nominal Transmitting Resolution)

Questo campo a cinque byte specifica la risoluzione di trasmissione nominale delle immagini da trasmettere. La risoluzione è espressa in pixel/mm nello stesso formato dell'NSR (campo 1.011).

3.1.13. Campo 1.013: Nome di dominio (DOM — Domain name)

Questo campo obbligatorio identifica il nome di dominio per l'implementazione del record logico tipo-2 definito dall'utente. Consiste in due informazioni così scritte «INT-I{US}4.22{GS}».

3.1.14. Campo 1.014: Tempo medio di Greenwich (GMT — Greenwich mean time)

Questo campo obbligatorio fornisce un meccanismo per esprimere data e ora in unità universali GMT. Se usato, il campo contiene la data universale che si aggiunge alla data locale contenuta nel campo 1.005 (DAT). L'uso del campo GMT elimina le incoerenze riguardo all'ora locale che si verificano allorché un'operazione e la relativa risposta provengono da due luoghi separati da più fusi orari. Il GMT fornisce una data universale e un orologio di 24 ore indipendente dai fusi orari. Si presenta nel formato «CCYYMMDDHHMMSSZ», una stringa di 15 caratteri che è la concatenazione della data con il GMT e che termina con una «Z». «CCYY» sta per l'anno dell'operazione, «MM» per il mese, «DD» per il giorno, «HH» per l'ora, «MM» per i minuti e «SS» per i secondi. La data completa non può essere superiore alla data attuale.

4. ***Record logico tipo-2: Descrizione***

La struttura della maggior parte del record non è definita dalla norma originale ANSI/NIST. Il record contiene informazioni di interesse specifico per le agenzie che ricevono o trasmettono il file. Affinché le comunicazioni dei sistemi dattiloscopici siano compatibili il record deve contenere solo i campi elencati di seguito. Il presente documento specifica quali campi sono obbligatori e quali facoltativi e definisce altresì la struttura di ogni campo.

4.1. *Campi del record logico tipo-2*

4.1.1. Campo 2.001: Lunghezza del record logico (LEN — Logical Record Length)

Questo campo obbligatorio specifica la lunghezza del record tipo-2 e il numero totale di byte, compresi tutti i caratteri di tutti i campi nonché i separatori.

4.1.2. Campo 2.002: Carattere di designazione dell'immagine (IDC — Image Designation Character)

L'IDC contenuto in questo campo obbligatorio è una rappresentazione ASCII dell'IDC definito nel campo Contenuto del file (CNT) del record tipo-1 (campo 1.003).

▼B

4.1.3. Campo 2.003: Informazione di sistema (SYS — System Information)

Questo campo è obbligatorio e contiene quattro byte che indicano a quale versione di INT-I si conforma questo particolare record tipo-2.

I primi due byte si riferiscono al numero di versione principale, gli altri due al numero di revisione. Ad esempio questa applicazione si basa su INT-I versione 4, revisione 22, e sarà rappresentata da «0422».

4.1.4. Campo 2.007: Numero caso (CNO — Case Number)

È il numero attribuito dall'ufficio dattiloscopico locale a una serie di latenti raccolte sul luogo del reato. Il formato è: CC/numero

dove CC è il codice paese dell'Interpol, due caratteri alfanumerici, e il numero corrisponde alla direttiva locale e può essere composto da un massimo di 32 caratteri alfanumerici.

Il campo permette di identificare latenti collegate a uno specifico reato.

4.1.5. Campo 2.008: Numero di sequenza (SQN — Sequence Number)

Specifica ogni sequenza di latenti di un caso e può essere costituito da un massimo di quattro caratteri numerici. Una sequenza è una latente o serie di latenti raggruppate a fini di archiviazione e/o consultazione. Ciò implica che anche singole latenti riceveranno un numero di sequenza.

Questo campo, insieme con l'MID (campo 2.009) può essere incluso per identificare una determinata latente all'interno di una sequenza.

4.1.6. Campo 2.009: Identificativo di latente (MID — Latent Identifier)

Specifica la singola latente all'interno di una sequenza. È costituito da una o due lettere, dove «A» è attribuita alla prima latente, «B» alla seconda e così via fino al limite «ZZ». Questo campo è usato analogamente al numero di sequenza delle latenti di cui alla descrizione dell'SQN (campo 2.008).

4.1.7. Campo 2.010: Numero di riferimento penale (CRN — Criminal Reference Number)

È un numero di riferimento unico attribuito da un'agenzia nazionale a una persona accusata per la prima volta di un reato. All'interno dello stesso paese una persona non può avere più di un CRN, né può condividerlo con altri. Per contro più paesi possono assegnare altrettanti CRN a una stessa persona che si diversificheranno per il codice paese.

Il formato è: CC/numero

dove CC è il codice paese secondo l'ISO 3166, due caratteri alfanumerici, e il numero corrisponde alla direttiva locale dell'agenzia d'origine e può essere composto da un massimo di 32 caratteri alfanumerici.

Per le operazioni ai sensi della decisione 2008/615/GAI questo campo sarà usato per il numero di riferimento penale nazionale assegnato dall'agenzia d'origine che è collegato alle immagini nei record tipo-4 o tipo-15.

▼B

4.1.8. Campo 2.012: Numero di identificazione Varie (MN1 — Miscellaneous Identification Number)

Questo campo contiene il CRN (campo 2.010) trasmesso con un'operazione CPS o PMS senza codice paese.

4.1.9. Campo 2.013: Numero di identificazione Varie (MN2 — Miscellaneous Identification Number)

Questo campo contiene il CNO (campo 2.007) trasmesso con un'operazione MPS o MMS senza codice paese.

4.1.10. Campo 2.014: Numero di identificazione Varie (MN3 — Miscellaneous Identification Number)

Questo campo contiene l'SQN (campo 2.008) trasmesso con un'operazione MPS o MMS.

4.1.11. Campo 2.015: Numero di identificazione Varie (MN4 — Miscellaneous Identification Number)

Questo campo contiene l'MID (campo 2.009) trasmesso con un'operazione MPS o MMS.

4.1.12. Campo 2.063: Informazioni supplementari (INF — Additional Information)

Nel caso di un'operazione SRE a una richiesta PMS questo campo fornisce informazioni sul dito che ha dato origine a un'eventuale risposta positiva. Il formato è:

NN dove *NN* è il codice della posizione del dito di cui alla tabella 5, costituito da due cifre.

In tutti gli altri casi il campo è facoltativo, è costituito da un massimo di 32 caratteri alfanumerici e può fornire informazioni supplementari sulla richiesta.

4.1.13. Campo 2.064: Elenco rispondenti (RLS — Respondents List)

Questo campo contiene almeno due sottocampi. Il primo descrive il tipo di consultazione svolta usando la mnemonica a tre lettere che specifica il tipo di operazione in TOT (campo 1.004). Il secondo contiene un unico carattere: «I» per indicare che è stata trovata una risposta positiva (HIT) o «N» se non è stata trovata alcuna concordanza (NOHIT). Il terzo sottocampo contiene l'identificativo della sequenza per il possibile risultato e il numero totale dei possibili risultati separati da una barra. La molteplicità di possibili risultati darà luogo a messaggi multipli.

A fronte di un'eventuale risposta positiva il quarto sottocampo contiene un valore espresso con un massimo di sei cifre. Se la risposta positiva è stata verificata il valore di questo sottocampo è definito da «999999».

Esempio: «CPS{RS}I{RS}001/001{RS}999999{GS}»

Se l'AFIS remoto non attribuisce valore nel punto corrispondente il valore è pari a zero.

4.1.14. Campo 2.074: Campo/stato messaggio d'errore (ERM — Error Message Field)

Questo campo contiene messaggi d'errore derivanti da operazioni: sono rinviati al richiedente nel quadro di un'operazione di errore.

▼B

Tabella 3: Messaggi d'errore

Numeric Code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	Mandatory field missing
102	Invalid record type
103	Undefined field
104	Exceed the maximum occurrence
105	Invalid number of subfields
106	Field length too short
107	Field length too long
108	Field is not a number as expected
109	Field number value too small
110	Field number value too big
111	Invalid character
112	Invalid date
115	Invalid item value
116	Invalid type of transaction
117	Invalid record data
201	ERROR: INVALID TCN
501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY

Messaggi d'errore da 100 a 199:

Questi messaggi d'errore si riferiscono alla convalida dei record ANSI/NIST e sono definiti come:

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>…

dove:

— error _code è un codice che si riferisce esclusivamente a un motivo specifico (cfr. tabella 3)

— field_id è il numero di campo ANSI/NIST del campo errato (ad esempio 1.001, 2.001, ...) nel formato <record_type>.<field_id>.<sub_field_id>

▼B

— dynamic text è una descrizione dinamica più dettagliata dell'errore

— LF è un'interlinea che separa gli errori in caso di più errori

— per un record tipo-1 l'ICD è definito «-1»

Esempio:

201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION (201: IDC - 1 CAMPO 1.009 CARATTERE DI CONTROLLO ERRATO {LF} 115: IDC 0 CAMPO 2.003 INFORMAZIONE DI SISTEMA NON VALIDA)

Questo campo è obbligatorio per le operazioni di errore.

4.1.15. Campo 2.320: Numero previsto di possibili risultati (ENC — Expected Number of Candidates)

Questo campo contiene il numero massimo di possibili risultati da verificare previsto dall'agenzia richiedente. Il valore di ENC non deve superare i valori di cui alla tabella 11.

5. ***Record logico tipo-4: Immagine in scala di grigi ad alta risoluzione***

Si noti che i record tipo-4 sono per natura binari piuttosto che ASCII. Ad ogni campo è pertanto attribuita una posizione specifica nel record, il che comporta che tutti i campi sono obbligatori. La norma consente di specificare nel record sia la dimensione sia la risoluzione dell'immagine. Prescrive che i record logici tipo-4 contengano dati dell'immagine dattiloscopica da trasmettere ad una densità di pixel nominale compresa tra 500 e 520 pixel/pollice. Il valore preferito per i nuovi disegni è 500 pixel/pollice o 19,68 pixel/mm. 500 pixel/pollice è la densità specificata da INT-I, salvo che sistemi simili possono comunicare l'uno con l'altro servendosi di un valore diverso da quello preferito, nei limiti compresi tra 500 e 520 pixel/pollice.

5.1. *Campi per record logico tipo-4*

5.1.1. Campo 4.001: Lunghezza del record logico (LEN — Logical Record Length)

Questo campo di quattro byte specifica la lunghezza del record tipo-4 e il numero totale di byte, compresi tutti i byte di tutti i campi presenti nel record.

5.1.2. Campo 4.002: Carattere di designazione dell'immagine (IDC — Image Designation Character)

È la rappresentazione binaria a un byte del numero IDC dato nel file di intestazione.

5.1.3. Campo 4.003: Metodo di ottenimento dell'immagine (IMP — Impression Type)

È un campo ad un unico byte che occupa il sesto byte del record.

Tabella 4: Metodo di ottenimento dell'impronta del dito

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper

▼B

Code	Description
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4. Campo 4.004: Posizione del dito (FGP — Finger Position)

Questo campo di lunghezza fissa a 6 byte occupa le posizioni settima-dodicesima di un record tipo-4. Contiene le possibili posizioni del dito a partire dal byte più a sinistra (byte 7 del record). La tabella 5 riporta le posizioni note o più probabili. Introducendo con lo stesso formato le posizioni alternative del dito nei cinque byte restanti è possibile registrare fino a cinque dita supplementari. Se sono registrate meno di cinque posizioni i byte inutilizzati sono riempiti con il numero binario 255. Il codice 0 è usato per registrare le posizioni non identificate.

Tabella 5: Codice della posizione del dito e dimensioni massime

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40,0	40,0
Right thumb	1	45,0	40,0
Right index finger	2	40,0	40,0
Right middle finger	3	40,0	40,0
Right ring finger	4	40,0	40,0
Right little finger	5	33,0	40,0
Left thumb	6	45,0	40,0
Left index finger	7	40,0	40,0
Left middle finger	8	40,0	40,0
Left ring finger	9	40,0	40,0
Left little finger	10	33,0	40,0
Plain right thumb	11	30,0	55,0
Plain left thumb	12	30,0	55,0
Plain right four fingers	13	70,0	65,0
Plain left four fingers	14	70,0	65,0

Per le impronte latenti del luogo del reato si usano soltanto i codici da 0 a 10.

▼B

5.1.5. Campo 4.005: Risoluzione della scansione dell'immagine (ISR — Image Scanning Resolution)

Questo campo a un byte occupa il tredicesimo byte di un record tipo-4. Se contiene «0» l'immagine è stata scandita alla risoluzione preferita di 19,68 pixel/mm (500 pixel/pollice). Se contiene «1» l'immagine è stata scandita a una risoluzione diversa da quella specificata nel record tipo-1.

5.1.6. Campo 4.006: Lunghezza di linea (HLL — Horizontal Line Length)

Questo campo occupa il quattordicesimo e il quindicesimo byte del record tipo-4 e specifica il numero di pixel contenuto in ogni linea di scansione. Il primo byte è il più significativo.

5.1.7. Campo 4.007: Lunghezza di colonna (VLL — Vertical Line Length)

Questo campo registra al sedicesimo e al diciassettesimo byte il numero di linee di scansione presenti nell'immagine. Il primo byte è il più significativo.

5.1.8. Campo 4.008: Algoritmo di compressione della scala di grigi (GCA — Gray-scale Compression Algorithm)

Questo campo a un byte specifica l'algoritmo di compressione della scala di grigi usato per codificare i dati immagine. Per la presente applicazione il codice binario 1 indica che è stata usata la compressione WSQ (appendice 7).

5.1.9. Campo 4.009: Immagine

Questo campo contiene un flusso di byte che rappresenta l'immagine. La struttura dipenderà naturalmente dall'algoritmo di compressione usato.

6. ***Record logico tipo-9: record delle minuzie (Minutiæ Record)***

I record tipo-9 contengono un testo ASCII che descrive le minuzie e relative informazioni codificate a partire da una latente. Ai fini della consultazione non vi è limite di record tipo-9 in un file poiché ad ognuno è attribuita una visione o una latente diversa.

6.1. *Estrazione delle minuzie*

6.1.1. Identificazione del tipo di minuzie

Questa norma definisce tre numeri identificativi, usati per descrivere il tipo di minuzie ed elencati nella tabella 6. Il termine di una cresta corrisponde al tipo 1; la biforcazione al tipo 2. Una minuzia che non può essere chiaramente classificata in uno di questi due tipi rientrerà nel tipo 0, ossia «altro».

Tabella 6: Tipi di minuzie

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Tipo e coordinate delle minuzie

Affinché i template siano conformi alla sezione 5 della norma ANSI INCITS 378-2004, per determinare le coordinate delle singole minuzie (posizione e direzione angolare) occorre usare il metodo seguente che rafforza l'attuale norma INCITS 378-2004.

▼B

La posizione di una minuzia che rappresenta il termine di una cresta è il punto di biforcazione della struttura mediale dell'area del solco immediatamente di fronte al termine della cresta. Se i tre rami del solco sono stati ridotti alla larghezza di un unico pixel, il punto di intersezione corrisponde alla posizione della minuzia. Analogamente la posizione di una minuzia in caso di biforcazione corrisponde al punto di biforcazione della struttura mediale della cresta. Se ognuno dei tre rami della cresta è stato ridotto alla larghezza di un unico pixel il punto in cui i tre rami si intersecano individua la posizione della minuzia.

Dopo aver convertito tutte i termini delle creste in biforcazioni tutte le minuzie dell'immagine dattiloscopica sono rappresentate come biforcazioni. Le coordinate pixel X e Y dell'intersezione dei tre rami di ogni minuzia possono essere direttamente formattate. La direzione della minuzia può essere estratta da ciascuna biforcazione della struttura. I tre rami di ogni biforcazione devono essere esaminati nel punto finale di ciascun ramo. La figura 6.1.2 illustra i tre metodi usati per determinare il termine di un ramo in base a una risoluzione di scansione di 500 pixel/pollice.

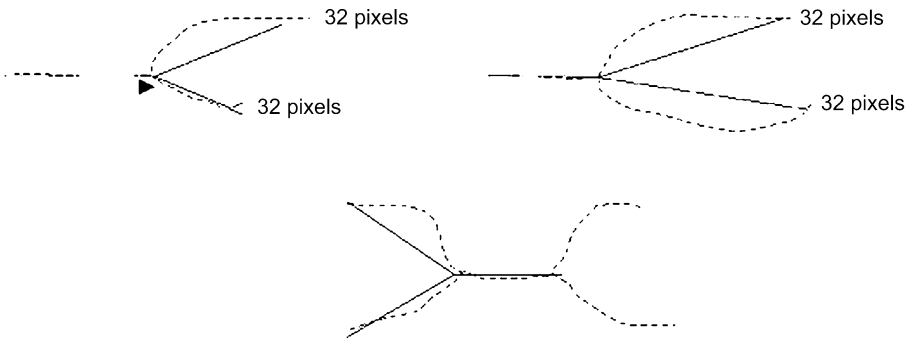
Il termine è stabilito secondo l'evento che si verifica per primo. Il conteggio dei pixel si basa su una risoluzione di 500 pixel/pollice. Risoluzioni diverse implicano conteggi di pixel diversi.

— Una distanza di 0,064 pollici (trentaduesimo pixel),

— il termine del ramo della struttura che si verifica a una distanza compresa fra 0,02 pollici e 0,064 pollici (dal decimo al trentaduesimo pixel); non si usano rami più corti,

— una seconda biforcazione si incontra a una distanza inferiore a 0,064 pollici (prima del trentaduesimo pixel).

Figura 6.1.2.



L'angolo della minuzia è determinato disegnando tre raggi virtuali che hanno origine nel punto della biforcazione e si estendono fino al termine di ciascun ramo. Il più piccolo dei tre angoli formati dai raggi è diviso in due per indicare la direzione della minuzia.

6.1.3. Sistema di coordinate

Il sistema usato per rappresentare le minuzie di un'impronta è un sistema di coordinate cartesiane. La posizione delle minuzie è rappresentata dalle coordinate x e y. Il punto d'origine del sistema di coordinate è l'angolo superiore sinistro dell'immagine originale, con il valore di x che aumenta verso destra e il valore di y che aumenta verso il basso. Entrambe le coordinate di una minuzia sono espresse in unità pixel dal punto d'origine. Si noti che la posizione del punto d'origine e le unità di misura non rispettano la convenzione usata nelle definizioni del tipo 9 di cui all'ANSI/NIST-ITL 1-2000.

▼B

6.1.4. Direzione delle minuzie

Gli angoli sono espressi nel formato matematico standard, con il valore 0 gradi a destra e i valori in aumento in senso antiorario. Nel caso del termine di una cresta gli angoli sono registrati nella direzione contraria lungo la cresta e, verso il centro del solco, nel caso di una biforcazione. Questa convenzione è ribaltata di 180° rispetto alla convenzione descritta nelle definizioni del tipo 9 di cui all'ANSI/NIST-ITL 1-2000.

6.2. *Campi per record logico tipo-9 Formato INCITS-378*

Tutti i campi dei record tipo-9 sono registrati come testo ASCII. In questo record di campo etichetta non sono ammessi campi binari.

6.2.1. Campo 9.001: Lunghezza del record logico (LEN — Logical Record Length)

Questo campo ASCII obbligatorio specifica la lunghezza del record logico e il numero totale di byte compresi tutti i caratteri di tutti i campi presenti nel record.

6.2.2. Campo 9.002: Carattere di designazione dell'immagine (IDC — Image Designation Character)

Questo campo obbligatorio a due byte è usato per identificare e localizzare i dati delle minuzie. L'IDC presente in questo campo corrisponde all'IDC nel campo Contenuto del file (CNT) del record tipo-1.

6.2.3. Campo 9.003: Metodo di ottenimento dell'immagine (IMP — Impression Type)

Questo campo obbligatorio a un byte descrive il modo in cui è stata ottenuta l'informazione dell'immagine dattiloscopica. In questo campo va inserito il valore ASCII del codice corrispondente dell'immagine della tabella 4 per indicare il metodo di ottenimento.

6.2.4. Campo 9.004: Formato delle minuzie (FMT — Minutiæ format)

Questo campo contiene un «U» per indicare che le minuzie sono formattate in termini M1-378. Benché le informazioni possano essere codificate secondo la norma M1-378, tutti i campi di dati del record tipo-9 devono figurare come campi testo ASCII.

6.2.5. Campo 9.126: Informazioni CBEFF

Questo campo contiene tre informazioni. Nella prima figura il valore «27» (0x1B), ossia l'identificazione del proprietario del formato CBEFF attribuito dall'International Biometric Industry Association (IBIA) al Comitato tecnico M1 dell'INCITS. Il carattere <US> distingue l'informazione dal tipo di formato CBEFF a cui è attribuito un valore di «513» (0x0201) per indicare che il record contiene soltanto dati relativi a posizione e direzione angolare e non blocchi di dati estesi. Il carattere <US> distingue l'informazione dall'identificativo prodotto CBEFF (PID — Product Identifier) che identifica il «proprietario» del dispositivo di codifica. Il venditore stabilisce questo valore che può essere ottenuto dal sito web IBIA (www.ibia.org) se presente.

6.2.6. Campo 9.127: Identificazione del dispositivo di acquisizione

Questo campo contiene due informazioni separate dal carattere <US>. La prima contiene «APPF» se il dispositivo usato inizialmente per acquisire l'immagine è certificato conforme all'appendice F (IAFIS Image Quality Specification, 29 gennaio 1999) della norma CJIS-RS-0010, specifica per la trasmissione elettronica delle impronte dell'FBI (Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification). Se il dispositivo non è conforme figurerà il valore «NONE». La seconda informazione contiene l'ID del dispositivo di acquisizione, ossia il numero prodotto attribuito dal venditore. Il valore «0» indica che l'ID del dispositivo non figura.

▼B

6.2.7. Campo 9.128: Lunghezza di linea (HLL — Horizontal line length)

In questo campo ASCII obbligatorio figura il numero di pixel di una linea dell'immagine trasmessa. La dimensione orizzontale massima è limitata a 65 534 pixel.

6.2.8. Campo 9.129: Lunghezza di colonna (VLL — Vertical line length)

In questo campo ASCII obbligatorio figura il numero di linee orizzontali dell'immagine trasmessa. La dimensione verticale massima è limitata a 65 534 pixel.

6.2.9. Campo 9.130: Unità di riduzioni (SLC — Scale units)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel dell'immagine): «1» sta per pixel/pollice, «2» per pixel/centimetro e «0» per nessuna unità. In quest'ultimo caso il quoziente HPS/VPS dà la risoluzione dell'immagine.

6.2.10. Campo 9.131: Unità utilizzata per le linee (HPS — Horizontal pixel scale)

Questo campo ASCII obbligatorio specifica in quale unità di lunghezza è espressa la densità in pixel delle linee dell'immagine, se nel campo SLC è specificato «1» o «2». Altrimenti, HPS indica la componente orizzontale della risoluzione.

6.2.11. Campo 9.132: Unità utilizzata per le colonne (VPS — Vertical pixel scale)

Questo campo ASCII obbligatorio specifica in quale unità di lunghezza è espressa la densità in pixel delle linee dell'immagine, se nel campo SLC è specificato «1» o «2». Altrimenti, HPS indica la componente verticale della risoluzione.

6.2.12. Campo 9.133: Vista del dito

Questo campo obbligatorio contiene il numero di vista del dito associato ai dati di questo record. Il numero inizia con «0» e aumenta fino a «15» di uno in uno.

6.2.13. Campo 9.134: Posizione del dito (FGP)

Questo campo contiene il codice che designa la posizione del dito da cui proviene l'informazione contenuta nel record tipo-9. Un codice da 1 a 10, di cui alla tabella 5, o il corrispondente codice del palmo, di cui alla tabella 10, indicano la posizione del dito o del palmo.

6.2.14. Campo 9.135: Qualità del dito

Questo campo indica la qualità dei dati complessivi inerenti alle minuzie, espressa con valori da 0 a 100. Il numero dà una valutazione della qualità del record del dito e rappresenta la qualità dell'immagine originale, dell'estrazione delle minuzie e di qualsiasi altra operazione che può influire sul record delle minuzie.

6.2.15. Campo 9.136: Numero di minuzie

In questo campo obbligatorio figura il conteggio delle minuzie registrate in questo record logico.

▼B

6.2.16. Campo 9.137: Dati delle minuzie del dito

Questo campo obbligatorio contiene sei informazioni separate dal carattere <US>. Comprende vari sottocampi, in ognuno dei quali figurano i particolari di singole minuzie. Il numero totale dei sottocampi di minuzie deve corrispondere al conteggio che figura nel campo 136. La prima informazione è il numero d'indice della minuzia, che inizia da «1» e aumenta di «1» per ogni ulteriore minuzia dell'impronta digitale. La seconda e la terza informazione sono le coordinate «x» e «y» delle minuzie in unità pixel. La quarta informazione è l'angolo della minuzia registrato in unità di due gradi. Questo valore deve essere non negativo e compreso tra 0 e 179. La quinta informazione è il tipo di minuzia: «0» corrisponde a minuzie di tipo «ALTRO» («OTHER»), «1» al termine di una cresta e «2» alla biforcazione di una cresta. La sesta informazione rappresenta la qualità di ciascuna minuzia ed è espressa con un valore compreso tra 1 e 100. Il valore «0» indica l'assenza di valutazione della qualità. Ciascun campo è separato dal successivo mediante il carattere <RS>.

6.2.17. Campo 9.138: Informazioni sul conteggio delle creste

Questo campo consiste in una serie di sottocampi contenenti ciascuno tre informazioni. La prima del primo sottocampo indica il metodo di estrazione del conteggio delle creste. Il valore «0» indica che non si fanno ipotesi sul metodo usato per estrarre il conteggio delle creste o il relativo ordine nel record. Il valore «1» indica che per ciascuna minuzia centrale il conteggio delle creste è stato estratto dalle minuzie contigue in quattro quadranti e i conteggi delle creste per ogni minuzia centrale sono elencati insieme. Il valore «2» indica che per ciascuna minuzia centrale il conteggio delle creste è stato estratto dalle minuzie contigue in otto ottanti e i conteggi delle creste per ogni minuzia centrale sono elencati insieme. Le due ultime informazioni del primo sottocampo contengono entrambe il valore «0». Le informazioni sono separate dal carattere <US>. I sottocampi successivi contengono, come prima informazione, il numero d'indice delle minuzie centrali, come seconda il numero d'indice delle minuzie contigue e, come terza, il numero di creste incrociate. I sottocampi sono separati dal carattere <RS>.

6.2.18. Campo 9.139: Informazioni sul centro dell'immagine

Questo campo consiste in un sottocampo per ogni centro presente nell'immagine originale Ogni sottocampo comprende tre informazioni. Le prime due contengono le coordinate «x» e «y» in unità pixel. La terza contiene l'angolo del centro registrato in unità di 2 gradi. Il valore è non negativo e compreso tra 0 e 179. Centri multipli sono separati dal carattere <RS>.

6.2.19. Campo 9.140: Informazioni sul delta

Questo campo consiste in un sottocampo per ogni delta presente nell'immagine originale Ogni sottocampo comprende tre informazioni. Le prime due contengono le coordinate «x» e «y» in unità pixel. La terza contiene l'angolo del delta registrato in unità di 2 gradi. Il valore è non negativo e compreso tra 0 e 179. Centri multipli sono separati dal carattere <RS>.

▼B

7. ***Record tipo-13: immagine latente a risoluzione variabile***

Il record logico del campo etichetta tipo-13 contiene i dati acquisiti da un'immagine latente. Queste immagini si intendono per l'invio alle agenzie che estrarranno automaticamente o interverranno manualmente per estrarre le caratteristiche desiderate.

Le informazioni sulla risoluzione di scansione usata, sulle dimensioni dell'immagine e su altri parametri necessari per elaborare l'immagine sono registrate, all'interno del record, come campi etichetta.

Tabella 7: Tracciato del record tipo-13 dell'immagine latente a risoluzione variabile

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE DATE	N	9	9	1	1	16
HLL	M	13.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13.013	FINGER POSITION	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—

▼B

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
COM	O	13.020	COMMENT	A	2	128	0	1	135
RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13.200 13.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13.999	IMAGE DATA	B	2	—	1	1	—

Legenda dei tipi di carattere: N = numerico; A = alfabetico; AN = alfanumerico; B = binario

7.1. *Campi riservati al record logico tipo-13*

I punti seguenti descrivono i dati contenuti in ciascun campo del record logico tipo-13.

In questo tipo di record i dati sono inseriti in campi numerati. I primi due campi del record si presentano sempre nello stesso ordine se il campo contenente i dati dell'immagine è l'ultimo campo del record. Per ciascun campo del record tipo-13 la tabella 7 indica il carattere obbligatorio «M» o facoltativo «O» del campo, il numero, il nome, il tipo di caratteri, le dimensioni, e i limiti di ricorrenza. Sulla base di un numero di campo a tre cifre le dimensioni massime di ciascun campo in numero di byte figurano nell'ultima colonna. Se per il numero di campo sono usate più di tre cifre anche le dimensioni massime aumentano. I numeri nelle colonne «dimensioni per ricorrenza del campo» comprendono tutti i separatori usati nel campo. Il numero massimo di byte comprende il numero del campo, l'informazione e tutti i separatori, compreso il carattere «GS».

7.1.1. Campo 13.001: Lunghezza del record logico (LEN — Logical record length)

Questo campo ASCII obbligatorio contiene il numero totale di byte nel record logico tipo-13. Il campo 13.001 specifica la lunghezza del record compresi tutti i caratteri di tutti i campi e i separatori.

7.1.2. Campo 13.002: Carattere di designazione dell'immagine (IDC — Image Designation Character)

Questo campo ASCII obbligatorio è usato per identificare i dati dell'immagine latente contenuti nel record. L'IDC presente corrisponde all'IDC nel campo Contenuto del file (CNT) del record tipo-1.

7.1.3. Campo 13.003: Metodo di ottenimento dell'immagine (IMP — Impression Type)

Questo campo ASCII obbligatorio a un byte descrive il modo in cui è stata ottenuta l'informazione dell'immagine latente. In questo campo va inserito il corrispondente codice della tabella 4 (dito) o della tabella 9 (palmo).

7.1.4. Campo 13.004: Agenzia d'origine/ORI (SRC)

Questo campo ASCII obbligatorio identifica l'amministrazione o l'organizzazione che ha in origine acquisito l'immagine facciale contenuta nel record. Di norma il codice ORI dell'agenzia che ha acquisito l'immagine è contenuto in detto campo che consiste di due informazioni nel formato seguente: CC/agenzia.

▼B

La prima si riferisce al codice paese dell'Interpol, due caratteri alfanumerici; la seconda è un testo libero di 32 caratteri alfanumerici al massimo, che identificano l'agenzia.

7.1.5. Campo 13.005: LCD (Latent capture date — Data di acquisizione dell'immagine latente)

Questo campo ASCII obbligatorio contiene la data di acquisizione dell'immagine latente nel record. La data è espressa in otto cifre, nel formato CCYYMMDD. CCYY corrisponde all'anno di acquisizione dell'immagine, MM corrisponde al mese, DD corrisponde al giorno. Ad esempio, 20000229 corrisponde al 29 febbraio 2000. La data completa deve essere una data plausibile.

7.1.6. Campo 13.006: HLL (Horizontal line length — Lunghezza di linea)

Questo campo ASCII obbligatorio indica il numero di pixel di una linea dell'immagine trasmessa.

7.1.7. Campo 13.007: VLL (Vertical line length — Lunghezza di colonna)

Questo campo ASCII obbligatorio indica il numero di linee orizzontali dell'immagine tramessa.

7.1.8. Campo 13.008: SLC (Scale units — Unità di risoluzioni)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel dell'immagine. 1 sta per «pixel/pollice», 2 sta per «pixel/centimetro», 0 per «nessuna unità». In questo ultimo caso, il quoziente HPS/VPS dà la risoluzione dell'immagine.

7.1.9. Campo 13.009: HPS (Horizontal pixel scale — Unità utilizzata per le linee)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel delle linee dell'immagine, se nel campo SLC è specificato 1 o 2. Altrimenti, HPS indica la componente orizzontale della risoluzione.

7.1.10. Campo 13.010: VPS (Vertical pixel scale — Unità utilizzata per le colonne)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel delle colonne dell'immagine, se nel campo SLC è specificato 1 o 2. Altrimenti, HPS indica la componente verticale della risoluzione.

7.1.11. Campo 13.011: CGA (Compression algorithm — algoritmo di compressione)

Questo campo ASCII obbligatorio indica l'algoritmo utilizzato per comprimere le immagini a scala di grigi. Per i codici di compressione, cfr. appendice 7.

7.1.12. Campo 13.012: BPX (Bit per pixel)

Questo campo ASCII obbligatorio specifica il numero di bit utilizzati per rappresentare un pixel. Occorre precisare «8» per i valori di scala di grigi normali tra 0 e 255. Qualsiasi valore superiore a 8 rappresenta un pixel in scala di grigi di più alta precisione.

▼B

7.1.13. Campo 13.013: FGP (Finger position — Posizione del dito/del palmo)

Questo campo etichetta obbligatorio specifica la posizione del dito ovvero la parte del palmo che potrebbe corrispondere all'immagine latente. Contiene un codice decimale della tabella 5 corrispondente in modo certo o assai probabile al dito in questione, oppure un codice della tabella 10 corrispondente alla parte del palmo probabilmente interessata e si presenta in forma di sottocampo ASCII a uno o due caratteri. È possibile introdurre altri codici di dita/parti palmari sotto forma di sottocampi separati da «RS». Il codice «0», corrispondente a «dito non identificato» può essere usato per qualsiasi dito; il codice «20» corrispondente a «immagine palmare non identificata» può essere usato per qualsiasi parte del palmo della mano.

7.1.14. Campo 13.014-019: RSV (Reserved for future definition — Riservati in vista di ulteriore definizione)

Questi campi saranno definiti nelle future revisioni della presente norma. Nessuno di essi può essere utilizzato nel quadro della presente revisione. Qualora uno di essi fosse specificato, non se ne deve tener conto.

7.1.15. Campo 13.020: COM (Comment — Osservazioni)

Questo campo facoltativo può essere usato per aggiungere osservazioni o del testo ASCII ai dati concernenti l'immagine latente.

7.1.16. Campo 13.021-199: RSV (Reserved for future definition — Riservati in vista di ulteriore definizione)

Questi campi saranno definiti nelle future revisioni della presente norma. Nessuno di essi può essere utilizzato nel quadro della presente revisione. Qualora uno di essi fosse specificato, non se ne deve tener conto.

7.1.17. Campo 13.200-998: UDF (User-defined fields — Campi definiti dall'utente)

Questi campi possono essere definiti dall'utente e saranno utilizzati per ulteriori requisiti. Dimensioni e contenuto sono fissati dall'utente d'accordo con l'agenzia di destinazione. Se sono presenti, contengono testo ASCII.

7.1.18. Campo 13.999: DAT (Image data — Dati riguardanti l'immagine)

Questo campo contiene tutti i dati relativi ad un'immagine latente acquisita. Occorre sempre attribuirle il numero 999 e deve sempre essere l'ultimo campo del record. Per esempio, «13.999:» è seguito dai dati binari relativi all'immagine.

Ciascun pixel dei dati di un'immagine a scala di grigi non compressa è di solito descritto sugli otto bit (256 sfumature di grigio) di un unico byte. Se il campo 13.012 (BPX) contiene un valore inferiore o superiore a 8, il numero di byte richiesto per descrivere un pixel sarà diverso. Se l'immagine è compressa, i dati relativi ai pixel saranno compressi secondo la tecnica indicata nel campo CGA.

7.2. *Fine del record logico tipo-13: Immagine latente a risoluzione variabile*

A fini di coerenza, l'ultimo byte del campo 13.999 deve essere separato dal record logico successivo mediante il separatore «FS». Il separatore deve essere incluso nel campo LEN del record tipo-13.

▼B

8. ***Record tipo-15: Immagini d'impronta del palmo a risoluzione variabile***

Il record logico etichetta tipo-15 contiene dati relativi alle immagini d'impronte palmari, campi di testo predefinito o definito dall'utente relativi all'immagine digitalizzata e permette lo scambio di tali dati. Le informazioni relative alla risoluzione di scansione utilizzata, alle dimensioni dell'immagine e agli altri parametri o osservazioni necessari al trattamento dell'immagine sono registrate sotto forma di campi etichetta all'interno del record. Le immagini d'impronte palmari trasmesse alle altre agenzie sono trattate dai destinatari che estraggono le informazioni volute ai fini della ricerca di corrispondenze.

Le immagini sono acquisite per scansione diretta o da una scheda o altro supporto contenente le impronte palmari del soggetto.

I metodi di acquisizione devono poter acquisire una serie d'immagini per ciascuna mano. Tale serie deve comprendere il palmo propriamente detto (una sola immagine) e l'intera mano, dal polso alla punta delle dita (una o due immagini). Se l'intera mano figura su due immagini, l'immagine corrispondente alla parte inferiore deve coprire la parte della mano dal polso fino alla zona infradigitale superiore (articolazione del medio) e comprende l'eminenza tenar e l'ipotenar. L'immagine della parte superiore si estende dal basso della zona infradigitale fino alla punta delle dita. Grazie a questo metodo, si ottiene un accavallamento sufficiente tra le due immagini situato a livello dell'area infradigitale/palmare. Avvicinando le linee contenute in quest'area comune uno specialista può accertare che le due immagini corrispondono al medesimo palmo.

Poiché un'operazione riguardante un'impronta palmare può servire a fini diversi, può contenere una o più immagini del palmo o della mano. Per un dato individuo, un record completo comprende l'impronta palmare vera e propria e l'impronta della mano completa (una o due immagini), il tutto per ciascuna delle due mani. Poiché un record logico etichetta può contenere un solo campo binario, occorrerà un record tipo-15 per ciascuna impronta palmare, più uno o due record per ciascuna impronta palmare completa. In altri termini, sono necessari da quattro a sei record tipo-15 per rappresentare le impronte palmari di un soggetto nel quadro di un'operazione normale.

8.1. *Campi del record logico tipo-15*

I punti seguenti descrivono i dati contenuti in ciascun campo del record logico tipo-15.

In questo tipo di record, i dati sono specificati in campi numerati. I primi due campi del record si presentano sempre nello stesso ordine, e il campo contenente i dati relativi all'immagine è l'ultimo del record. La tabella 8 indica, per ciascun campo tipo-15, il carattere obbligatorio «M» o facoltativo «O» del campo, il numero, il nome, il tipo di caratteri che contiene, le dimensioni e i limiti di ricorrenza. Sulla base di un numero di campo a tre cifre, le dimensioni massime di ciascun campo, in numero di byte, figurano nell'ultima colonna della tabella. Se si utilizzano più di tre cifre per il numero di campo, le dimensioni massime aumentano. I numeri figuranti nelle due colonne «Dimensioni per ricorrenza del campo» tengono conto di tutti i separatori usati nel campo. Il numero massimo di byte indicato comprende il numero di campo, le informazioni e tutti i separatori, compreso il carattere «GS».

▼B

8.1.1. Campo 15.001: LEN (Logical Record Length — Lunghezza del record logico)

Questo campo ASCII obbligatorio definisce il numero totale di byte nel record logico tipo-15. Il campo 15.001 specifica la lunghezza del record compresi tutti i caratteri di tutti i campi e i separatori d'informazione.

8.1.2. Campo 15.002: IDC (Image designation character — Caratteri di designazione dell'immagine)

Questo campo ASCII obbligatorio serve a identificare l'immagine d'impronta palmare contenuta nel record. L'IDC presente corrisponde all'IDC nel campo CNT del record tipo-1.

8.1.3. Campo 15.003: IMP (Impression type — Metodo di ottenimento dell'immagine)

Questo campo ASCII obbligatorio di un byte descrive in che modo è stata ottenuta l'immagine dell'impronta palmare. In questo campo va inserito il corrispondente codice della tabella 9.

8.1.4. Campo 15.004: ORI (SRC) (Source agency — agenzia d'origine)

Questo campo ASCII obbligatorio identifica l'amministrazione o l'organizzazione che ha acquisito l'immagine facciale contenuta nel record. Di regola il codice ORI dell'agenzia che ha acquisito l'immagine è contenuto in questo campo. Comporta due elementi d'informazione che si presentano nel formato seguente: CC/agenzia.

CC corrisponde al codice paese dell'Interpol, composto da due caratteri alfanumerici. Agenzia designa l'agenzia destinataria, in 32 caratteri alfanumerici di testo libero.

8.1.5. Campo 15.005: PCD (Palmprint capture date — Data di acquisizione dell'immagine dell'impronta palmare)

Questo campo ASCII obbligatorio contiene la data di acquisizione dell'immagine dell'impronta palmare nel record. La data è espressa in otto cifre, nel formato CCCMMDD. CCC corrisponde all'anno di acquisizione dell'immagine; MM corrisponde al mese, DD corrisponde al giorno. Ad esempio, 20000229 corrisponde al 29 febbraio 2000. La data completa deve essere una data plausibile.

8.1.6. Campo 15.006: HLL (Horizontal line length — Lunghezza di linea)

Questo campo ASCII obbligatorio indica il numero di pixel di una linea dell'immagine trasmessa.

8.1.7. Campo 15.007: VLL (Vertical line length — Lunghezza di colonna)

Questo campo ASCII obbligatorio indica il numero di linee orizzontali dell'immagine trasmessa.

8.1.8. Campo 15.008: SLC (Scale units — Unità di risoluzioni)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel dell'immagine. 1 sta per «pixel/pollice», 2 sta per «pixel/centimetro», 0 per «nessuna unità». In questo ultimo caso, il quoziente HPS/VPS dà la risoluzione dell'immagine.

▼B

8.1.9. Campo 15.009: HPS (Horizontal pixel scale — Unità utilizzata per le linee)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel delle linee dell'immagine, se nel campo SLC è specificato 1 o 2. Altrimenti, HPS indica la componente orizzontale della risoluzione.

8.1.10. Campo 15.010: VPS (Vertical pixel scale — Unità utilizzata per le colonne)

Questo campo ASCII obbligatorio indica in quale unità di lunghezza è espressa la densità in pixel delle colonne dell'immagine, se nel campo SLC è specificato 1 o 2. Altrimenti, HPS indica la componente verticale della risoluzione.

Tabella 8: Tracciato del record tipo-15 dell'impronta palmare a risoluzione variabile

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15.020	COMMENT	AN	2	128	0	1	128

▼B

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15.200 15.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15.999	IMAGE DATA	B	2	—	1	1	—

Tabella 9: Metodo di ottenimento delle immagini d'impronte palmari

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11. Campo 15.011: CGA (Compression algorithm — Algoritmo di compressione)

Questo campo ASCII obbligatorio indica l'algoritmo utilizzato per comprimere le immagini a scala di grigi. «NONE» significa che i dati contenuti in questo campo non sono compressi. Quando si vuole comprimere le immagini, questo campo specifica il metodo migliore di compressione delle immagini d'impronte delle dieci dita. I modi di compressione che si possono utilizzare figurano nell'appendice 7.

8.1.12. Campo 15.012: BPX (Bit per pixel)

Questo campo ASCII obbligatorio specifica il numero di bit utilizzati per rappresentare un pixel. Occorre precisare «8» per i valori di scala di grigi normali compresi tra 0 e 255. Qualsiasi valore superiore o inferiore a 8 rappresenta un pixel in scala di grigi di precisione rispettivamente più alta o meno alta.

Tabella 10: Codici delle varie parti del palmo e dimensioni dell'immagine

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28 387	139,7	203,2
Right Full Palm	21	28 387	139,7	203,2
Right Writer s Palm	22	5 645	44,5	127,0
Left Full Palm	23	28 387	139,7	203,2
Left Writer s Palm	24	5 645	44,5	127,0
Right Lower Palm	25	19 516	139,7	139,7

▼B

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Right Upper Palm	26	19 516	139,7	139,7
Left Lower Palm	27	19 516	139,7	139,7
Left Upper Palm	28	19 516	139,7	139,7
Right Other	29	28 387	139,7	203,2
Left Other	30	28 387	139,7	203,2

8.1.13. Campo 15.013: PLP (Palmprint position — Posizione dell'impronta palmare)

Questo campo etichetta obbligatorio specifica la parte del palmo rappresentata dall'immagine. Contiene uno dei codici decimali della tabella 10 corrispondenti in modo certo o assai probabile alla parte di palmo in questione, sotto forma di campo o sottocampo ASCII a due caratteri. La tabelle 10 precisa anche la superficie massima che può essere trasmessa per ciascuna parte del palmo.

8.1.14. Campo 15.014-019: RSV (Reserved for future definition — Riservati in vista di ulteriore definizione)

Questi campi saranno definiti nelle future revisioni della presente norma. Nessuno di essi può essere utilizzato nel quadro della presente revisione. Qualora uno di essi fosse specificato, non se ne deve tener conto.

8.1.15. Campo 15.020: COM (Comment — Osservazioni)

Questo campo facoltativo può essere usato per aggiungere osservazioni o testo ASCII ai dati concernenti l'immagine dell'impronta palmare.

8.1.16. Campo 15.021-199: RSV (Reserved for future definition — Riservati in vista di ulteriore definizione)

Questi campi saranno definiti nelle future revisioni della presente norma. Nessuno di essi può essere utilizzato nel quadro della presente revisione. Qualora uno di essi fosse specificato, non se ne deve tener conto.

8.1.17. Campo 15.200-998: UDF (User-defined fields — Campi definiti dall'utente)

Questi campi possono essere definiti dall'utente e saranno utilizzati per ulteriori requisiti. Dimensioni e contenuto sono fissati dall'utente d'accordo con l'agenzia di destinazione. Se sono presenti, contengono testo ASCII.

8.1.18. Campo 15.999: DAT (Image data — Dati riguardanti l'immagine)

Questo campo contiene tutti i dati relativi ad un'immagine latente acquisita. Occorre sempre attribuirle il numero 999 e deve sempre essere l'ultimo campo del record. Per esempio, «15.999:» è seguito dai dati binari relativi all'immagine. Ciascun pixel dei dati di un'immagine a scala di grigi non compressa è di solito descritto sugli otto bit (256 sfumature di grigio) di un unico byte. Se il campo 15.012 (BPX) contiene un valore inferiore o superiore a 8, il numero di byte richiesto per descrivere un pixel sarà diverso. Se l'immagine è compressa, i dati relativi ai pixel saranno compressi secondo la tecnica indicata nel campo CGA.

▼B

8.2. *Fine del record logico tipo-15: Immagine dell'impronta del palmo a risoluzione variabile*

A fini di coerenza, l'ultimo byte del campo 15.999 deve essere separato dal record logico successivo mediante il separatore «FS». Il separatore deve essere incluso nel campo LEN del record tipo 15.

8.3. *Record supplementari tipo-15: Immagine dell'impronta del palmo a risoluzione variabile*

Nel file si possono inserire record tipo-15 supplementari. Per ciascuna immagine supplementare dell'impronta del palmo, occorre un record logico tipo-15 completo e un separatore «FS».

Tabella 11: Numero massimo di risultati possibili accettati alla verifica per ogni trasmissione

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Tipo di consultazione:

TP/TP: impronta delle dieci dita-impronta delle dieci dita

LT/TP: impronta latente del dito-impronta delle dieci dita

LP/PP: impronta palmare latente-impronta palmare

TP/UL: impronta delle dieci dita-latente irrisolta dell'impronta del dito

LT/UL: impronta latente del dito-latente irrisolta dell'impronta del dito

PP/ULP: impronta palmare-latente irrisolta dell'impronta palmare

LP/ULP: impronta palmare latente-latente irrisolta dell'impronta palmare

9. ***Appendici del capo 2 (scambio di dati dattiloscopici)***

9.1. *Appendice 1 Codici separatori ASCII*

ASCII	Position ([1])	Description
LF	1/10	Separates error codes in field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

([1]) Posizione definita nella norma ASCII.

▼B

9.2. *Appendice 2 Calcolo dei caratteri di controllo alfanumerici*

Per TCN e TCR (campi 1.09 e 1.10):

Il numero corrispondente al carattere di controllo è generato mediante la formula seguente:

(YY * 10^8 + SSSSSSSS) Modulo 23

dove YY e SSSSSSSS stanno rispettivamente per le due ultime cifre dell'anno e per il numero di serie.

Il carattere di controllo è generato mediante la tabella riportata di seguito.

Per CRO (campo 2.010)

Il numero corrispondente al carattere di controllo è generato mediante la formula seguente:

(YY * 10^6 + NNNNNN) Modulo 23

dove YY e SSSSSSSS stanno rispettivamente per le due ultime cifre dell'anno e per il numero di serie.

Il carattere di controllo è generato mediante la tabella riportata di seguito.

Tabella dei caratteri di controllo

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3. *Appendice 3 Codici dei caratteri*

Codice ANSI a 7 bit per lo scambio di informazioni.

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	»	#	$	%	&	’
40	(	)	*	+	,	—	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	'	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

▼B

9.4. *Appendice 4 Sommario delle operazioni*

Record tipo-1 (obbligatorio)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Sotto la colonna Condizioni:

O = facoltativo; M = obbligatorio; C = condizionale se l'operazione è una risposta all'agenzia d'origine

Record tipo-2 (obbligatorio)

Identifier	Field Number	Field Name	CPS/PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C

▼B

Identifier	Field Number	Field Name	CPS/PMS	MPS/ MMS	SRE	ERR
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Sotto la colonna Condizioni:

O = facoltativo; M = obbligatorio; C = condizionale se i dati sono disponibili

* = se la trasmissione dei dati è conforme alla legislazione nazionale (non disciplinato dalla decisione 2008/615/GAI)

9.5. *Appendice 5 Definizioni record tipo-1*

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS} 2{US}00{RS} 4{US}01{RS} 4{US}02{RS} 4{US}03{RS} 4{US}04{RS} 4{US}05{RS} 4{US}06{RS} 4{US}07{RS} 4{US}08{RS} 4{US}09{RS} 4{US}10{RS} 4{US}11{RS} 4{US}12{RS} 4{US}13{RS} 4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}

▼B

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Sotto la colonna Condizioni (Condition): O = facoltativo; M = obbligatorio; C = condizionale

Sotto la colonna Tipo di carattere (Character Type): A = alfa, N = numerico, B = binario

1* caratteri ammessi per il nome dell'agenzia: [«0..9», «A..Z», «a..z», «_», «.», «», «-»]

9.6. *Appendice 6 Definizioni record tipo-2*

Tabella A.6.1: Operazioni CPS e PMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Tabella A.6.2: Operazioni SRE

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}

▼B

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Tabella A.6.3: Operazioni ERR

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

▼B

Tabella A.6.4: Operazioni MPS e MMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CNO	M	2.007	Case Number	AN	2.007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2.008:0001{GS}
MID	C	2.009	Latent Identifier	A	2.009:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Sotto la colonna Condizioni (Condition): O = facoltativo; M = obbligatorio; C = condizionale

Sotto la colonna Tipo di carattere (Character Type): A = alfa, N = numerico, B = binario

1* caratteri ammessi per il nome dell'agenzia: [«0..9», «A..Z», «a..z», «_», «.», «», «-»]

9.7. *Appendice 7 Codici di compressione della scala dei grigi*

Codici di compressione

Compression	Value	Remarks
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated 19 December 1997	WSQ	Algorithm to be used for the compression of grayscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500 dpi
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of grayscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi

9.8. *Appendice 8 Specifica dei messaggi*

Per migliorare il flusso interno l'oggetto del messaggio di un'operazione PRUEM deve essere completato con il codice paese (CC) dello Stato membro che invia il messaggio e con il tipo di operazione (campo 1.004 TOT).

Formato: CC/tipo di operazione

Esempio: «DE/CPS»

Il corpo del messaggio può essere vuoto.

▼B

CAPO 3: **Scambio di dati di immatricolazione dei veicoli**

1. ***Insieme comune di dati per la consultazione automatizzata dei dati di immatricolazione dei veicoli***

1.1. *Definizioni*

Seguono le definizioni di elementi obbligatori di dati e di elementi facoltativi di dati di cui all'articolo 16, paragrafo 4:

Obbligatorio (mandatory — M):

L'elemento in questione deve essere comunicato quando le informazioni sono disponibili nel registro nazionale di uno Stato membro. V'è pertanto l'obbligo di scambiare le informazioni quando sono disponibili.

Facoltativo (optional — O):

L'elemento in questione può essere comunicato quando le informazioni sono disponibili nel registro nazionale di uno Stato membro. Non v'è pertanto l'obbligo di scambiare le informazioni, anche se disponibili.

Un'indicazione (Y) è inserita in corrispondenza di ciascun elemento dell'insieme di dati di cui si ravvisi specificatamente l'importanza con riguardo alla decisione 2008/615/GAI.

1.2. *Consultazione relativa al veicolo/proprietario/intestatario*

1.2.1. Attivazione della consultazione

La consultazione di dati può essere attivata in due modi diversi, come definito al punto successivo:

— mediante numero di telaio (VIN), data e ora di riferimento (facoltativo),

— mediante numero di patente, numero di targa (VIN) (facoltativo), data e ora di riferimento (facoltativo).

Attraverso questi criteri di ricerca saranno fornite informazioni riguardanti un veicolo e talvolta più veicoli. Se le informazioni da fornire riguardano un solo veicolo, tutte le voci sono inviate in un'unica risposta. Se riguardano più veicoli, lo stesso Stato membro richiesto può determinare quali voci saranno fornite: tutte le voci o solo quelle volte ad affinare la consultazione (ad esempio per motivi di riservatezza o di efficacia).

Le voci necessarie per affinare la consultazione sono illustrate al punto 1.2.2.1. L'insieme completo di dati è descritto al punto 1.2.2.2.

La consultazione, se eseguita mediante numero di telaio, data e ora di riferimento, può svolgersi in uno o in tutti gli Stati membri partecipanti.

Quando è svolta con numero di patente, data e ora di riferimento, la consultazione deve essere eseguita in un determinato Stato membro.

Si procede alla consultazione inserendo, di norma, la data e l'ora reali, ma è possibile svolgere una consultazione servendosi di una data e di un'ora di riferimento nel passato. Quando per una consultazione si usano una data e un'ora di riferimento nel passato e nel registro di un determinato Stato membro non sono disponibili dati storici in quanto non ne è prevista la registrazione, è possibile trasmettere i dati reali corredandoli dell'indicazione che si tratta di dati reali.

▼B

1.2.2. Insieme di dati

1.2.2.1. Voci da trasmettere necessarie per affinare la consultazione

Item	M/O (1)	Remarks	Prüm Y/N (2)
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	[D.1 (3)] e.g. Ford, Opel, Renault ecc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
EU Category Code	M	(J) mopeds, motorbikes, cars ecc.	Y

(1) M (mandatory) = obbligatorio quando disponibile nel registro nazionale, O (optional) = facoltativo.
(2) Tutti gli attributi specificatamente assegnati dagli Stati membri sono indicati con Y.
(3) Abbreviazione armonizzata, cfr. direttiva 1999/37/CE del Consiglio.

1.2.2.2. Insieme completo di dati

Item	M/O (1)	Remarks	Prüm Y/N
Data relating to holders of the vehicle		[C.1 (2)] The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for surname, infixes, titles ecc., and the name in printable format will be communicated	Y
First name	M	(C.1.2) separate fields for first name(s) and initials will be used, and the name in printable format will be communicated	Y
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence ecc., and the Address in printable format will be communicated	Y
Gender	M	Male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm ecc.	Y
Place of Birth	O		Y

▼B

Item	M/O (1)	Remarks	Prüm Y/N
ID Number	O	An identifier that uniquely identifies the person or the company	N
Type of ID Number	O	The type of ID Number (e.g. passport number)	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner — is not the vehicle owner — is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y
Address	M	(C.2.3)	Y
Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm ecc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company	N
Type of ID Number	O	The type of ID Number (e.g. passport number)	N
Start date ownership	O	Start date of the ownership of the car	N
End date ownership	O	End data of the ownership of the car	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault ecc.	Y

▼B

Item	M/O (1)	Remarks	Prüm Y/N
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle/EU Category Code	M	(J) mopeds, motorbikes, cars ecc.	Y
Date of first registration	M	B) date of first registration of the vehicle somewhere in the world	Y
Start date (actual) registration	M	I) Date of the registration to which the specific certificate of the vehicle refers	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H)	Y
Status	M	scrapped, stolen, exported ecc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	regular, transito ecc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document	Y
Vehicle document id 2 (3)	O	A second document ID as printed on the vehicle document	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y
ID Number	O	An identifier that uniquely identifies the company.	N
Type of ID Number	O	The type of ID Number (e.g. number of the Chamber of Commerce)	N

(1) M (mandatory) = obbligatorio quando disponibile nel registro nazionale, O (optional) = facoltativo.
(2) Abbreviazione armonizzata, cfr. direttiva 1999/37/CE del Consiglio.
(3) In Lussemburgo sono usati due distinti identificativi del documento di immatricolazione del veicolo.

▼B

2. ***Sicurezza dei dati***

2.1. *Quadro generale*

L'applicazione software Eucaris gestisce la comunicazione sicura con gli altri Stati membri e comunica con i sistemi legacy di back-end degli Stati membri che utilizzano l'XML. Gli Stati membri scambiano messaggi inviandoli direttamente al destinatario. Il centro dati di uno Stato membro è collegato alla rete TESTA dell'UE.

I messaggi XML trasmessi attraverso la rete sono cifrati. Per cifrare questi messaggi la tecnica usata è l'SSL. I messaggi inviati al back-end sono messaggi XML contenenti testo in chiaro in quanto il collegamento tra l'applicazione e il back-end avviene in ambiente protetto.

È prevista un'applicazione client che può essere utilizzata all'interno di uno Stato membro per interrogare il proprio registro o quello di altri Stati membri. I client saranno identificati mediante un ID utente/una password o un certificato client. Il collegamento con un utente può essere cifrato ma questo è lasciato alla responsabilità dei singoli Stati membri.

2.2. *Caratteristiche di sicurezza connesse allo scambio di messaggi*

Il concetto di sicurezza si fonda sul protocollo HTTPS associato alla firma XML. Questa alternativa si avvale della firma XML per firmare tutti i messaggi inviati al server ed è in grado di autenticare il mittente del messaggio verificandone la firma. L'SSL unilaterale (solo un certificato di server) viene usato per proteggere la riservatezza e l'integrità dei messaggi in transito e garantisce protezione da attacchi di tipo eliminazione (deletion)/riproduzione (replay) e inserimento (insertion). Al posto dello sviluppo di software su misura per implementare l'SSL bilaterale, si applica la firma XML. L'uso della firma XML è più affine alla roadmap dei servizi web rispetto all'SSL bilaterale e come tale è più strategico.

La firma XML può essere applicata in vari modi ma l'approccio scelto consiste nell'usare la firma XML quale parte del protocollo Web Services Security (WSS). Il WSS definisce le modalità di utilizzo della firma XML. Poiché il WSS si fonda sullo standard SOAP, pare logico conformarsi quanto più possibile a detto standard.

2.3. *Caratteristiche di sicurezza non connesse allo scambio di messaggi*

2.3.1 Autenticazione degli utenti

Gli utenti dell'applicazione web Eucaris si autenticano utilizzando un nome utente e una password. Poiché viene usata l'autenticazione standard Windows, gli Stati membri possono rafforzare, se necessario, il livello di autenticazione degli utenti utilizzando certificati client.

2.3.2. Ruoli utente

L'applicazione software Eucaris supporta vari ruoli utente. Ciascun cluster di servizi ha la propria autorizzazione. Ad esempio utenti (esclusivi) della funzionalità «Treaty of Eucaris» non sono autorizzati ad usare la funzionalità «Prüm». I servizi dell'amministratore sono separati dai normali ruoli utente finale.

▼B

2.3.3. Registrazione (logging) e tracciamento (tracing) dello scambio di messaggi

La registrazione di tutte le tipologie di messaggi è agevolata dall'applicazione software Eucaris. Una funzione di amministrazione consente all'amministratore nazionale di determinare quali messaggi sono registrati: richieste di utenti finali, richieste in entrata di altri Stati membri, informazioni tratte dai registri nazionali, ecc.

L'applicazione può essere configurata in modo tale da usare, per questa registrazione, una base dati interna o una base dati esterna (Oracle). La decisione riguardo a quali messaggi devono essere registrati dipende chiaramente dai dispositivi di registrazione in altre parti dei sistemi legacy e delle applicazioni client collegate.

L'intestazione di ciascun messaggio contiene informazioni sullo Stato membro richiedente, l'organizzazione richiedente all'interno di tale Stato membro e l'utente interessato. È indicato anche il motivo della richiesta.

La registrazione combinata nello Stato membro richiedente e rispondente consente il completo tracciamento di qualsiasi scambio di messaggi (ad esempio su richiesta di un cittadino interessato).

La registrazione è configurata attraverso l'Eucaris web client (menu Administration, Logging configuration). La funzionalità di registrazione è eseguita dal sistema centrale. Quando la registrazione è attivata, il messaggio completo (intestazione e corpo) è memorizzato in un apposito record. Il livello di registrazione può essere fissato per servizio specifico e per tipologia di messaggi che transitano attraverso il sistema centrale.

Livelli di registrazione

Sono possibili i seguenti livelli di registrazione:

Private (privato) — il messaggio è registrato: la registrazione NON è accessibile al servizio di estrazione delle registrazioni ma è disponibile soltanto a livello nazionale, per gli audit e la risoluzione di problemi.

None (nessuno) — il messaggio non è registrato.

Tipologie di messaggi

Gli scambi di informazioni fra Stati membri consistono in una serie di messaggi illustrati schematicamente nella figura riportata di seguito.

Seguono le possibili tipologie di messaggi (nella figura, per il sistema centrale Eucaris di uno Stato membro X):

1. Request to Core System_Request message by Client

2. Request to Other Member State_Request message by Core System of this Member State

3. Request to Core System of this Member State_Request message by Core System of other Member State

4. Request to Legacy Register_Request message by Core System

5. Request to Core System_Request message by Legacy Register

6. Response from Core System_Request message by Client

7. Response from Other Member State_Request message by Core System of this Member State

▼B

8. Response from Core System of this Member State_Request message by other Member State

9. Response from Legacy Register_Request message by Core System

10. Response from Core System_Request message by Legacy Register

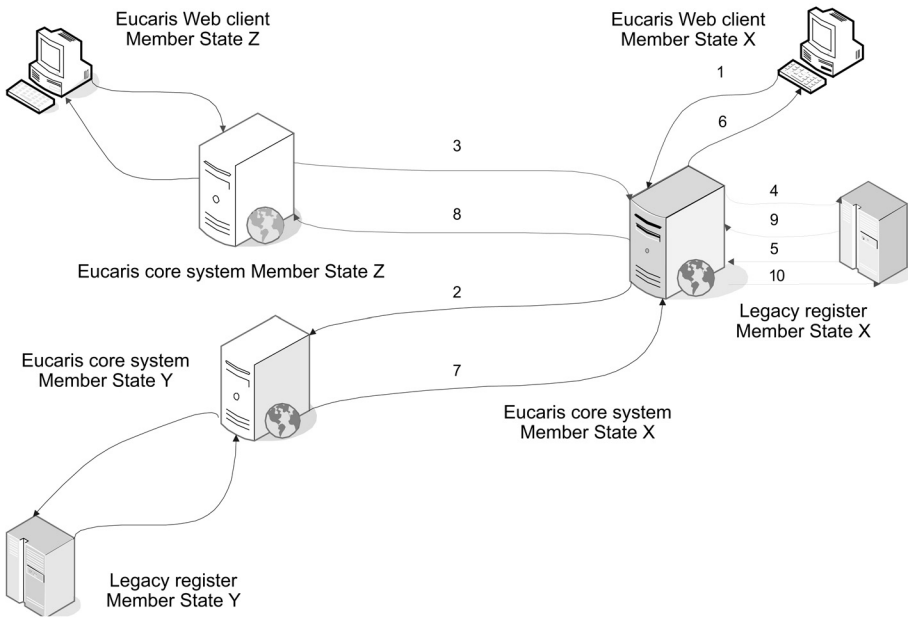
Nella figura sono illustrati i seguenti scambi di informazioni.

— Richiesta di informazioni dello Stato membro X allo Stato membro Y — frecce blu. In questo caso, richiesta e risposta consistono in messaggi, rispettivamente, di tipo 1, 2, 7 e 6.

— Richiesta di informazioni dello Stato membro Z allo Stato membro X — frecce rosse. In questo caso, richiesta e risposta consistono in messaggi, rispettivamente, di tipo 3, 4, 9 e 8.

— Richiesta di informazioni del registro legacy al relativo sistema centrale (questo tragitto comprende anche la richiesta di un client personalizzato oltre il registro legacy) — frecce verdi. In questo caso, la richiesta corrisponde a messaggi di tipo 5 e 10.

Figura: Tipologie di messaggi per la registrazione



2.3.4. Modulo hardware di sicurezza

Non è usato un modulo hardware di sicurezza.

Un modulo hardware di sicurezza (Hardware Security Module — HSM) offre una buona protezione della chiave usata per firmare i messaggi e identificare i server. Contribuisce al livello generale di sicurezza, ma è costoso da acquistare/mantenere e non vi sono requisiti per decidere se optare per un HSM certificato FIPS 140-2 di livello 2 o di livello 3. Poiché viene usata una rete chiusa che attenua efficacemente i rischi, si è deciso di non usare inizialmente un HSM. Se necessario, ad esempio per ottenere un accreditamento, l'HSM può essere aggiunto all'architettura.

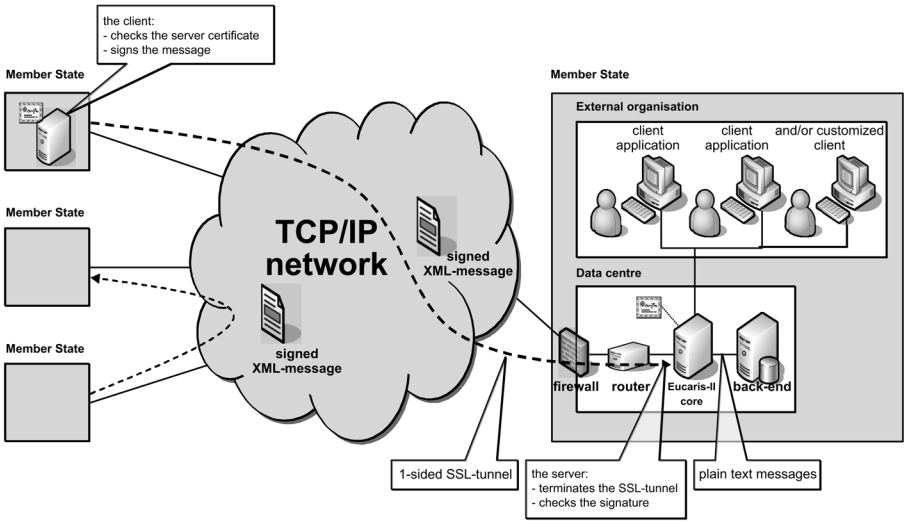
▼B

3. ***Condizioni tecniche dello scambio di dati***

3.1. *Descrizione generale dell'applicazione Eucaris*

3.1.1. Quadro generale

L'applicazione Eucaris collega tutti gli Stati membri partecipanti in una rete a maglie in cui ciascuno Stato membro comunica direttamente con un altro Stato membro. Non occorre una componente centrale per stabilire la comunicazione. L'applicazione Eucaris gestisce la comunicazione sicura con gli altri Stati membri e comunica con i sistemi legacy di back-end degli Stati membri che utilizzano l'XML. La figura seguente illustra tale architettura.



Gli Stati membri scambiano messaggi inviandoli direttamente al destinatario. Il centro dati di uno Stato membro è collegato alla rete utilizzata per lo scambio di messaggi (TESTA). Per accedere alla rete TESTA, gli Stati membri vi si collegano tramite il rispettivo gate nazionale. Per il collegamento alla rete viene utilizzato un firewall e un router collega l'applicazione Eucaris al firewall. A seconda dell'opzione scelta per proteggere i messaggi, viene utilizzato un certificato dal router o dall'applicazione Eucaris.

È prevista un'applicazione client che può essere utilizzata all'interno di uno Stato membro per interrogare il proprio registro o quello degli altri Stati membri. L'applicazione client consente il collegamento ad Eucaris. I client saranno identificati attraverso un ID utente/una password o un certificato client. Il collegamento con un utente di un'organizzazione esterna (ad esempio polizia) può essere cifrato, ma questo è lasciato alla responsabilità di ogni singolo Stato membro.

3.1.2. Ambito del sistema

L'ambito del sistema Eucaris è limitato ai processi afferenti allo scambio di informazioni tra le autorità di immatricolazione degli Stati membri e ad una presentazione di base di tali informazioni. Le procedure e i processi automatizzati nei quali le informazioni sono destinate ad essere utilizzate esulano dall'ambito del sistema.

Gli Stati membri hanno la scelta tra la funzionalità client Eucaris o la creazione di una propria applicazione client personalizzata. La tabella seguente mostra gli aspetti del sistema Eucaris da utilizzare obbligatoriamente e/o prescritti e quelli da utilizzare facoltativamente e/o lasciati alla determinazione degli Stati membri.

▼B

Eucaris aspects	M/O (1)	Remark
Network concept	M	The concept is an «any-to-any» communication.
Physical network	M	TESTA
Core application	M	The core application of Eucaris has to be used to connect to the other Member States. The following functionality is offered by the core: — Encrypting and signing of the messages; — Checking of the identity of the sender; — Authorization of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the Eucaris II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the Eucaris organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the Eucaris organisation and this Council Decision. The specifications can only be changed by the Eucaris organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the Eucaris organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

(1) M = (mandatory) utilizzazione o conformità obbligatoria O = (optional) utilizzazione o conformità facoltativa.

3.2. *Requisiti funzionali e non funzionali*

3.2.1. Funzionalità generica

La presente sezione offre una descrizione in termini generali delle principali funzioni generiche.

N.	Descrizione
1.	Il sistema consente alle autorità di immatricolazione degli Stati membri di scambiare messaggi di richiesta e di risposta in modo interattivo.
2.	Il sistema comprende un'applicazione client che consente agli utenti finali di inviare le loro richieste e presenta le informazioni di risposta per il trattamento manuale.
3.	Il sistema agevola la «diffusione», consentendo ad uno Stato membro di inviare una richiesta a tutti gli altri Stati membri. Le risposte in entrata sono consolidate dall'applicazione centrale in un unico messaggio di risposta all'applicazione client (questa funzionalità è detta «interrogazione multipaese»).

▼B

N.	Descrizione
4.	Il sistema è in grado di trattare diversi tipi di messaggi. I ruoli utente, l'autorizzazione, l'instradamento, la firma e la registrazione sono tutti definiti per servizio specifico.
5.	Il sistema permette agli Stati membri di scambiare gruppi di messaggi o messaggi contenenti un alto numero di richieste o risposte. Tali messaggi sono trattati in modo asincrono.
6.	Il sistema effettua l'accodamento dei messaggi asincroni qualora lo Stato membro destinatario sia temporaneamente indisponibile e garantisce la consegna non appena il destinatario è nuovamente raggiungibile.
7.	Il sistema memorizza i messaggi asincroni in entrata fino a quando è possibile trattarli.
8.	Il sistema offre solo accesso alle applicazioni Eucaris degli altri Stati membri e non a singole organizzazioni all'interno di tali altri Stati membri, vale a dire che ogni autorità d'immatricolazione funge da unico gateway tra i relativi utenti finali nazionali e le corrispondenti autorità degli altri Stati membri.
9.	È possibile definire utenti di diversi Stati membri su un unico server Eucaris e autorizzarli in base ai diritti dello Stato membro interessato.
10.	Le informazioni sullo Stato membro richiedente, l'organizzazione e l'utente finale sono incluse nei messaggi.
11.	Il sistema facilita la registrazione dello scambio di messaggi tra i diversi Stati membri e tra l'applicazione centrale e i sistemi di immatricolazione nazionali.
12.	Il sistema permette ad un segretario specifico, ossia un'organizzazione o uno Stato membro appositamente designati per questo compito, di raccogliere le informazioni registrate sui messaggi inviati/ricevuti da tutti gli Stati membri partecipanti al fine di elaborare rapporti statistici.
13.	Ogni Stato membro stabilisce quali informazioni registrate sono a disposizione del segretario e quali informazioni sono «private».
14.	Il sistema permette agli amministratori nazionali di ciascuno Stato membro di estrarre statistiche utili.
15.	Il sistema permette l'aggiunta di nuovi Stati membri attraverso semplici operazioni amministrative.

3.2.2. Usabilità

N.	Descrizione
16.	Il sistema offre un'interfaccia per il trattamento automatizzato dei messaggi attraverso sistemi/legacy di back-end e permette l'integrazione dell'interfaccia utente in tali sistemi (interfaccia utente personalizzata).
17.	Il sistema è facile da imparare, è intuitivo e contiene un testo di aiuto.
18.	Il sistema è corredato della documentazione necessaria per aiutare gli Stati membri nell'integrazione, nelle attività operative e nella futura manutenzione (per esempio guide di riferimento, documentazione funzionale/tecnica, guida operativa ecc.).
19.	L'interfaccia utente è multilingue e offre dispositivi all'utente finale per la selezione della lingue preferita.
20.	L'interfaccia utente comprende dispositivi che consentono ad un amministratore locale di tradurre le voci della schermata nonché le informazioni codificate nella lingua nazionale.

▼B

3.2.3. Affidabilità

N.	Descrizione
21.	Il sistema è progettato come un sistema operativo robusto e affidabile che tollera gli errori dell'operatore e si ripristina correttamente in seguito a cadute di corrente o altri incidenti. Dev'essere possibile riavviare il sistema con nessuna o una minima perdita di dati.
22.	Il sistema deve offrire risultati stabili e riproducibili.
23.	Il sistema è stato progettato per funzionare in modo affidabile. È possibile implementarlo in una configurazione che garantisce una disponibilità del 98 % (attraverso la ridondanza, l'uso di server di backup, ecc.) in ogni comunicazione bilaterale.
24.	È possibile utilizzare una parte del sistema anche durante il guasto di alcune componenti (in caso di guasto nello Stato membro C, gli Stati membri A e B sono ancora in grado di comunicare). Il numero dei singoli punti di guasto nella catena informativa dovrebbe essere ridotto al minimo.
25.	Il tempo di ripristino dopo un grave guasto dovrebbe essere inferiore ad un giorno. Dovrebbe essere possibile ridurre al minimo il tempo di guasto utilizzando il supporto remoto, per esempio a cura di un service desk centrale.

3.2.4. Prestazioni

N.	Descrizione
26.	Il sistema può essere utilizzato 24x7. Questa finestra temporale (24x7) è quindi richiesta anche ai sistemi legacy degli Stati membri.
27.	Il sistema risponde rapidamente alle richieste dell'utente, indipendentemente da eventuali operazioni in background. Questo requisito vale anche per i sistemi legacy delle parti per garantire tempi di risposta accettabili. Un tempo di risposta complessivo di massimo 10 secondi per una singola richiesta è accettabile.
28.	Il sistema è stato progettato come sistema multiutente e in modo tale che le operazioni in background possano proseguire mentre l'utente procede ad operazioni in foreground.
29.	Il sistema è stato progettato per essere modulabile al fine di supportare un eventuale aumento del numero di messaggi in caso di aggiunta di nuove funzionalità o di nuove organizzazioni o Stati membri.

3.2.5. Sicurezza

N.	Descrizione
30.	Il sistema è adatto (per esempio per quanto riguarda le relative misure di sicurezza) allo scambio di messaggi contenenti dati personali sensibili per la privacy (per esempio proprietari/intestatari di veicoli) classificati come «EU restricted» («riservato UE»).
31.	Il sistema è mantenuto in modo tale da prevenire l'accesso non autorizzato ai dati.
32.	Il sistema comprende un servizio per la gestione dei diritti e permessi degli utenti finali nazionali.
33.	Gli Stati membri sono in grado di controllare l'identità del mittente (a livello di Stato membro) attraverso la firma XML.

▼B

N.	Descrizione
34.	Gli Stati membri devono esplicitamente autorizzare gli altri Stati membri a richiedere informazioni specifiche.
35.	Il sistema offre a livello applicativo un meccanismo completo di sicurezza e cifratura compatibile con il livello di sicurezza richiesto in tali contesti. L'esclusività e l'integrità delle informazioni sono garantite dall'uso della firma XML e la cifratura avviene con il tunnelling SSL.
36.	Tutti gli scambi di messaggi possono essere tracciati attraverso la registrazione.
37.	È assicurata la protezione contro gli attacchi di tipo eliminazione (un terzo elimina un messaggio) e contro gli attacchi di tipo riproduzione o inserimento (un terzo riproduce o inserisce un messaggio).
38.	Il sistema si avvale di certificati di una terza parte fidata (Trusted Third Party — TTP).
39.	Il sistema è in grado di trattare diversi certificati per Stato membro, a seconda del tipo di messaggio o servizio.
40.	Le misure di sicurezza a livello applicativo sono sufficienti per consentire il ricorso a reti non accreditate.
41.	Il sistema è in grado di utilizzare le nuove tecnologie di sicurezza come il firewall XML.

3.2.6. Adattabilità

N.	Descrizione
42.	Il sistema può essere esteso con nuovi messaggi e nuove funzionalità. Il costo degli adattamenti è minimo grazie allo sviluppo centralizzato delle componenti applicative.
43.	Gli Stati membri possono definire nuove tipologie di messaggi per uso bilaterale. Non tutti gli Stati membri sono tenuti a supportare tutte le tipologie di messaggi.

3.2.7. Supporto e manutenzione

N.	Descrizione
44.	Il sistema offre dispositivi di monitoraggio per un service desk centrale e/o operatori, riguardanti la rete e i server nei diversi Stati membri.
45.	Il sistema offre dispositivi di supporto remoto da parte di un service desk centrale.
46.	Il sistema offre dispositivi per l'analisi dei problemi.
47.	Il sistema può essere esteso a nuovi Stati membri.
48.	L'applicazione può essere installata facilmente da personale con un minimo di competenza ed esperienza in materia di TI. La procedura d'installazione è il più possibile automatizzata.
49.	Il sistema offre un ambiente di prova e di collaudo permanente.
50.	Le spese annuali di manutenzione e supporto sono state ridotte al minimo aderendo agli standard di mercato e creando un'applicazione che richiede quanto meno supporto possibile da parte di un service desk centrale.

▼B

3.2.8. Requisiti di progettazione

N.	Descrizione
51.	Il sistema è progettato e documentato per una vita operativa di molti anni.
52.	Il sistema è stato progettato in modo tale da essere indipendente dal gestore di rete.
53.	Il sistema è compatibile con l'HW/SW esistente negli Stati membri grazie all'interazione con i sistemi di immatricolazione che si avvalgono della tecnologia standard aperta di servizi web [XML, XSD, SOAP, WSDL, HTTP(s), servizi Web, WSS, X.509 ecc.].

3.2.9. Norme applicabili

N.	Descrizione
54.	Il sistema è conforme alle prescrizioni di protezione dei dati di cui al regolamento (CE) n. 45/2001 (articoli 21, 22 e 23) e alla direttiva 95/46/CE.
55.	Il sistema è conforme alle norme IDA.
56.	Il sistema supporta l'UTF8.

CAPO 4: **Valutazione**

1. ***Procedura di valutazione a norma dell'articolo 20 (decisione di cui all'articolo 25, paragrafo 2, della decisione 2008/615/GAI)***

1.1. *Questionario*

Il gruppo di lavoro competente del Consiglio elabora un questionario riguardo a ciascuno degli scambi automatizzati di dati di cui al capo 2 della decisione 2008/615/GAI.

Non appena uno Stato membro ritiene di soddisfare le condizioni preliminari per lo scambio di dati nella pertinente categoria di dati, esso risponde al corrispondente questionario.

1.2. *Esperienza pilota*

Al fine di valutare i risultati del questionario, lo Stato membro che desidera avviare lo scambio di dati effettua un'esperienza pilota unitamente ad uno o più altri Stati membri che già scambiano dati in virtù della decisione del Consiglio. L'esperienza pilota viene effettuata poco prima o poco dopo la visita di valutazione.

Le condizioni e le modalità dell'esperienza pilota sono definite dal gruppo di lavoro competente del Consiglio e sono basate su un preliminare accordo individuale con lo Stato membro interessato. Gli Stati membri partecipanti all'esperienza pilota definiscono le modalità pratiche.

1.3. *Visita di valutazione*

Al fine di valutare i risultati del questionario, viene effettuata una visita di valutazione nello Stato membro che desidera avviare lo scambio di dati.

Le condizioni e le modalità della visita sono definite dal gruppo di lavoro competente e sono basate su un preliminare accordo individuale tra lo Stato membro interessato e il gruppo di valutazione. Lo Stato membro interessato consente al gruppo di valutazione di controllare lo scambio automatizzato di dati nella o nelle categorie di dati da valutare, in particolare organizzando un programma per la visita che tenga conto delle richieste del gruppo di valutazione.

▼B

Entro un mese, il gruppo di valutazione elabora una relazione sulla visita di valutazione e la trasmette allo Stato membro interessato per raccoglierne le osservazioni. Se opportuno, la relazione è riveduta dal gruppo di valutazione sulla base delle osservazioni dello Stato membro.

Il gruppo di valutazione è composto da non più di tre esperti, designati dagli Stati membri partecipanti allo scambio automatizzato di dati nelle categorie di dati da valutare, che abbiano esperienza in ordine alla categoria di dati interessata, siano in possesso dell'appropriato nulla osta di sicurezza nazionale per trattare le materie in questione e siano disposti a partecipare ad almeno una visita di valutazione in un altro Stato membro. La Commissione è invitata a partecipare al gruppo di valutazione in qualità di osservatore.

I membri del gruppo di valutazione rispettano il carattere riservato delle informazioni acquisite nell'espletamento della loro funzione.

1.4. *Relazione al Consiglio*

Conformemente all'articolo 25, paragrafo 2, della decisione 2008/615/GAI, viene presentata al Consiglio una relazione globale di valutazione che sintetizza i risultati dei questionari, della visita di valutazione e dell'esperienza pilota.

2. ***Procedura di valutazione a norma dell'articolo 21***

2.1. *Statistiche e relazione*

Ogni Stato membro elabora statistiche sui risultati dello scambio automatizzato di dati. Al fine di assicurare la comparabilità, il modello statistico è elaborato dal gruppo di lavoro competente del Consiglio.

Tali statistiche sono trasmesse annualmente al segretariato generale, che elabora un quadro sinottico per l'anno trascorso, e alla Commissione.

Gli Stati membri sono inoltre invitati periodicamente, e non più di una volta l'anno, a fornire le informazioni sull'attuazione amministrativa, tecnica e finanziaria dello scambio automatizzato di dati necessarie per analizzare e migliorare la procedura. Sulla base di tali informazioni viene elaborata una relazione per il Consiglio.

2.2. *Revisione*

Entro un termine ragionevole, il Consiglio esamina il meccanismo di valutazione descritto in questa sede e procede, se necessario, alla sua revisione.

3. Riunioni di esperti

Nel gruppo di lavoro competente del Consiglio, si tengono periodicamente riunioni di esperti per organizzare e attuare le summenzionate procedure di valutazione, scambiare esperienze e discutere eventuali miglioramenti. Se del caso, i risultati di queste discussioni tra esperti sono integrati nella relazione di cui al punto 2.1.