

To besedilo je zgolj informativne narave in nima pravnega učinka. Institucije Unije za njegovo vsebino ne prevzemajo nobene odgovornosti. Verodostojne različice zadevnih aktov, vključno z uvodnimi izjavami, so objavljene v Uradnem listu Evropske unije. Na voljo so na portalu EUR-Lex. Uradna besedila so neposredno dostopna prek povezav v tem dokumentu

► **B**

SKLEP SVETA 2008/616/PNZ

z dne 23. junija 2008

o izvajanju Sklepa 2008/615/PNZ o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu

(UL L 210, 6.8.2008, str. 12)

spremenjen z:

		Uradni list		
		št.	stran	datum
► M1	Uredba (EU) 2024/982 Evropskega parlamenta in Sveta z dne 13. marca 2024	L 982	1	5.4.2024

▼B**SKLEP SVETA 2008/616/PNZ****z dne 23. junija 2008****o izvajanju Sklepa 2008/615/PNZ o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu****POGLAVJE I****SPLOŠNO***Člen 1***Namen**

Namen tega sklepa je, da se predvidijo potrebne upravne in tehnične določbe za izvajanje Sklepa 2008/615/PNZ, zlasti v zvezi z avtomatizirano izmenjavo podatkov o DNA, daktiloskopskih podatkov in podatkov iz registrov vozil iz poglavja 2 navedenega sklepa in druge oblike sodelovanja iz poglavja 5 navedenega sklepa.

*Člen 2***Opredelitve**

V tem sklepu:

- (a) „iskanje“ in „primerjava“ iz členov 3, 4, in 9 Sklepa 2008/615/PNZ pomenita postopka, s katerima se ugotavlja ujemanje med podatki o DNA oziroma daktiloskopskimi podatki, ki jih posreduje ena država članica, in podatki o DNA oziroma daktiloskopskimi podatki, shranjenimi v zbirkah podatkov kake druge države članice oziroma nekaterih drugih oziroma vseh držav članic;
- (b) „avtomatizirano iskanje“ iz člena 12 Sklepa 2008/615/PNZ pomeni postopek *on-line* dostopa, katerega namen je poizvedovanje po zbirkah podatkov druge države članice oziroma nekaterih drugih oziroma vseh držav članic;
- (c) „profil DNA“ pomeni črkovno ali številčno kodo, ki predstavlja niz razločevalnih značilnosti nekodirajočega dela analiziranega vzorca človeške DNA, tj. posebno molekularno strukturo različnih področij DNA (lokusov);
- (d) „nekodirajoči del DNA“ pomeni kromosomska področja, ki ne vsebujejo nobenih genetskih informacij, tj. ki jim ni mogoče pripisati nobenih funkcionalnih lastnosti nekega organizma;
- (e) „podatkovni zapis o DNA“ pomeni profil DNA in številko sklica;
- (f) „referenčni profil DNA“ pomeni profil DNA identificirane osebe;
- (g) „neznan profil DNA“ pomeni profil DNA še neidentificirane osebe, pridobljen iz sledi, zbranih pri preiskovanju kaznivih dejanj;

▼B

- (h) „opomba“ pomeni zabeležko pri profilu DNA, ki jo država članica vnese v svojo nacionalno zbirko podatkov, in navaja, da je bilo ob iskanju in primerjanju s strani druge države članice pri zadevnem profilu DNA že ugotovljeno ujemanje;
- (i) „daktiloskopski podatki“ pomenijo prstne odtise, sledi prstnih odtisov, odtise dlani, sledi odtisov dlani, pa tudi t. i. template (vzorci) takšnih podob (kodirane minucije), kadar so shranjeni in se obdelujejo v avtomatizirani zbirki podatkov;
- (j) „podatki iz registrov vozil“ pomeni niz podatkov, kakor je opredeljen v poglavju 3 Priloge k temu sklepu;
- (k) „posamezen primer“ iz drugega stavka člena 3(1), drugega stavka člena 9(1) in člena 12(1) Sklepa 2008/615/PNZ pomeni en sam preiskovalni ali kazenski spis. Če tak spis vsebuje več ko en profil DNA ali zapis daktiloskopskih podatkov ali podatkov iz registra vozil, jih je mogoče posredovati skupaj kot eno samo zaprosilo.

▼M1**▼B**

POGLAVJE 6

POLICIJSKO SODELOVANJE*Člen 17***Skupne patrulje in druge skupne operacije**

1. V skladu s poglavjem 5 Sklepa 2008/615/PNZ in še zlasti z izjavami, ki se predložijo v skladu s členi 17(4), 19(2) in 19(4) navedenega sklepa, vsaka država članica imenuje eno ali več kontaktnih točk, da se s tem drugim državam članicam omogoči, da se obrnejo na pristojne organe, in vsaka država članica lahko opredeli svoje postopke za vzpostavitev skupnih patrulj in drugih skupnih operacij, postopke za obdelavo pobud drugih držav članic za takšne operacije, pa tudi druge praktične vidike in operativne podrobnosti v zvezi s temi operacijami.

2. Generalni sekretariat Sveta sestavi in posodablja seznam kontaktnih točk ter pristojne organe obvešča o vseh spremembah na seznamu.

3. Pristojni organi vsake države članice lahko dajo pobudo za skupno operacijo. Pred začetkom konkretne operacije se pristojni organi iz odstavka 2 pisno ali ustno dogovorijo o podrobnostih, pri čemer gre med drugim lahko za naslednje:

- (a) organi v državah članicah, pristojni za operacijo;
- (b) točen namen operacije;

▼ B

- (c) država članica gostiteljica, v kateri poteka operacija;
- (d) zadevno geografsko območje države članice gostiteljice, na katerem poteka operacija;
- (e) obdobje, ki ga bo operacija obsegala;
- (f) konkretna pomoč, ki naj bi jo za državo članico gostiteljico prispevale druge države članice, vključno s tja napotenimi uradniki ali drugimi javnimi uslužbenci, materialnimi in finančnimi sredstvi;
- (g) uradniki, ki sodelujejo pri operaciji;
- (h) uradnik, odgovoren za operacijo;
- (i) pooblastila, ki jih smejo med operacijo v državi članici gostiteljici izvrševati uradniki in drugi javni uslužbenci, ki jih tja napoti druga država članica oziroma več takšnih držav;
- (j) konkretno katero orožje, strelivo in opremo smejo napoteni uradniki uporabljati med operacijo v skladu s Sklepom 2008/615/PNZ;
- (k) logistične rešitve za transport, namestitve in varnost;
- (l) dodelitev stroškov skupne operacije, če je drugačna od dodelitve, predvidene v prvem stavku člena 34 Sklepa 2008/615/PNZ;
- (m) morebitne druge pomembne zadeve.

4. Izjave, postopki in funkcije, predvidene v tem členu, so navedene v priložniku iz člena 18(2).

POGLAVJE 7

KONČNE DOLOČBE

▼ M1**▼ B***Člen 19***Neodvisni organi za varstvo podatkov**

Države članice v skladu s členom 18(2) tega sklepa generalni sekretariat Sveta obvestijo o neodvisnih organih za varstvo podatkov ali o sodnih organih iz člena 30(5) Sklepa 2008/615/PNZ.

▼ M1**▼ B***Člen 22***Razmerje med sporazumom o izvajanju in Prümško pogodbo**

Za države članice, ki jih zavezuje Prümška pogodba, se namesto ustreznih določb iz sporazuma o izvajanju Prümške pogodbe uporabljajo ustrezne določbe iz tega sklepa in pripadajoče priloge, takoj ko se bosta v celoti začela izvajati. Vse druge določbe sporazuma o izvajanju se še naprej uporabljajo med podpisnicami Prümške pogodbe.

▼B

Člen 23

Izvajanje

Države članice sprejmejo ukrepe, potrebne za uskladitev s tem sklepom, v rokih, ki so predvideni v členu 36(1) Sklepa 2008/615/PNZ.

Člen 24

Uporaba

Ta sklep začne učinkovati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

**B***PRILOGA***KAZALO****POGLAVJE 1: Izmenjava podatkov o DNK**

1. ***Z DNK povezana vprašanja sodne medicine, pravila ujemanja in algoritmi***
 - 1.1 *Lastnosti profilov DNK*
 - 1.2 *Pravila ujemanja*
 - 1.3 *Pravila poročanja*
2. ***Tabela s številčnimi kodami držav članic***
3. ***Funkcionalna analiza***
 - 3.1 *Razpoložljivost sistema*
 - 3.2 *Drugi korak*
4. ***Kontrolni dokument vmesnika DNK***
 - 4.1 *Uvod*
 - 4.2 *Opredelitev strukture XML*
5. ***Uporaba, varnost in komunikacijska struktura***
 - 5.1 *Pregled*
 - 5.2 *Struktura na višji ravni*
 - 5.3 *Varnostni standardi in varovanje podatkov*
 - 5.4 *Protokoli in standardi, ki se uporabijo za šifrirni mehanizem: sMIME in s tem povezani paketi*
 - 5.5 *Struktura aplikacije*
 - 5.6 *Protokoli in standardi, ki se uporabijo za strukturo aplikacije*
 - 5.7 *Komunikacijsko okolje*

POGLAVJE 2: Izmenjava daktiloskopskih podatkov (kontrolni dokument vmesnika)

1. ***Pregled vsebine datoteke***
2. ***Format zapisa***
3. ***Logični zapis tipa 1: glava datoteke***
4. ***Logični zapis tipa 2: opisno besedilo***
5. ***Logični zapis tipa 4: podoba visoke ločljivosti v lestvici sivine***
6. ***Logični zapis tipa 9: zapis minucij***
7. ***Zapis podobe sledi tipa 13 različne ločljivosti***
8. ***Zapis podobe odtisa dlani tipa 15 različne ločljivosti***
9. ***Dodatki k poglavju 2***
 - 9.1 *Ločilne kode ASCII*
 - 9.2 *Izračun alfanumeričnega kontrolnega znaka*
 - 9.3 *Znakovne kode*
 - 9.4 *Povzetek prenosa*

▼B

- 9.5 *Tip-1 opredelitve zapisa*
- 9.6 *Tip-2 opredelitve zapisa*
- 9.7 *Kompresijske kode v lestvici sivine*
- 9.8 *Specifikacija elektronske pošte*

POGLAVJE 3: Izmenjava podatkov o registraciji vozil

- 1. ***Skupni niz podatkov za avtomatizirano iskanje podatkov o registraciji vozil***
 - 1.1 *Opredelitve*
 - 1.2 *Poizvedba o vozilu/lastniku/imetniku*
- 2. ***Varnost podatkov***
 - 2.1 *Pregled*
 - 2.2 *Varnostne lastnosti, povezane z izmenjavo sporočil*
 - 2.3 *Varnostne lastnosti, ki niso povezane z izmenjavo sporočil*
- 3. ***Tehnični pogoji izmenjave podatkov***
 - 3.1 *Splošen opis aplikacije EUCARIS*
 - 3.2 *Funkcijske in nefunkcijske zahteve*

POGLAVJE 4: Ocenjevanje

- 1. ***Postopek ocenjevanja v skladu s členom 20 (Priprava sklepov v skladu s členom 25(2) Sklepa 2008/615/PNZ)***
 - 1.1 *Vprašalnik*
 - 1.2 *Preskus*
 - 1.3 *Ocenjevalni obisk*
 - 1.4 *Poročanje Svetu*
- 2. ***Ocenjevalni postopek v skladu s členom 21***
 - 2.1 *Statistični podatki in poročilo*
 - 2.2 *Revizija*
- 3. ***Sestanki strokovnjakov***

▼B**POGLAVJE 1: Izmenjava podatkov o DNK****1. Z DNK povezana vprašanja sodne medicine, pravila ujemanja in algoritmi****1.1 Lastnosti profilov DNK**

Profil DNK lahko vsebuje 24 parov števil, ki predstavljajo alele 24 lokusov, katere se uporablja tudi v postopkih DNK, ki jih izvaja Interpol. Nazivi teh lokusov so navedeni v spodnji tabeli:

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

Sedem s sivo barvo označenih lokusov v zgornji vrstici predstavlja tako trenutni evropski standardni niz (*European Standard Set – ESS*) kot Interpolov standardni niz lokusov (*Interpol Standard Set of Loci – ISSOL*).

Pravila vključevanja:

Profili DNK, ki so jih države članice dale na voljo za iskanje in primerjavo, ter profili DNK, poslani za iskanje in primerjavo, morajo vsebovati najmanj 6 polno opredeljenih⁽¹⁾ lokusov ter glede na njihovo razpoložljivost lahko vsebujejo dodatne lokuse ali prazna mesta (blanks). Referenčni profili DNK morajo vsebovati vsaj 6 od 7 ESS lokusov. Da bi povečali točnost ujemanj, so vsi razpoložljivi aleli razvrščeni v indeksirani zbirki podatkov profilov DNK in se uporabljajo za iskanje in primerjavo. Vsaka država članica bi morala takoj, ko je to praktično izvedljivo, izvajati vse nove sprejete ESS lokusov, ki jih sprejme EU.

Mešani profili niso dovoljeni, tako da vrednosti alelov vsakega lokusa sestavljata samo dve števili, ki sta v primeru homozigotnosti lahko enaki.

Za nadomestne znake in mikro variante je treba uporabljati naslednja pravila:

- Vse nenumerične vrednosti razen amelogenina, ki so zajete v profilu (npr. „O“, „f“, „r“, „na“, „nr“ ali „un“), morajo biti avtomatično pretvorjene za prenos v nadomestne znake (*) ter se jih lahko poišče v primerjavi z vsemi.
- Numerične vrednosti „0“, „1“ ali „99“, ki so zajete v profilu, morajo biti avtomatično pretvorjene za prenos v nadomestne znake (*) ter se jih lahko poišče v primerjavi z vsemi.
- Če so za 1 lokus zagotovljeni 3 aleli, bo sprejet prvi alel, preostala dva alela pa morata biti avtomatično pretvorjena za prenos v nadomestne znake (*) ter se jih lahko poišče v primerjavi z vsemi.
- Ko so zagotovljene vrednosti nadomestnih znakov za alel 1 ali 2, se iščeta obe premutaciji numerične vrednosti določenega lokusa (npr. 12, * se lahko ujema z 12,14 ali 9,12).

⁽¹⁾ „Polno opredeljeni“ pomeni, da zajemajo obravnavo vrednosti redkih alelov.

▼B

- Za mikro variante pentanukleotida (Penta D, Penta E & CD4) se bodo ujemanja izvajala v skladu z naslednjim:

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

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

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

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

- Za mikro variante tetranukleotida (preostali lokusi so tetranukleotidi) se bodo ujemanja izvajala v skladu z naslednjim:

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

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

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

1.2 *Pravila ujemanja*

Primerjava dveh profilov DNK se bo izvajala na podlagi lokusov, katerih vrednosti alelov so na voljo v obeh profilih DNK. Najmanj šest polno opredeljenih lokusov (razen amelogenina) se mora ujemanjati z obema profiloma DNK, še preden se zagotovi odgovor z zadetki.

Polno ujemanje (kakovost 1) je opredeljeno kot ujemanje, ko so vse vrednosti alelov primerjanega lokusa iz profila DNK prosilca in zaprosenega profila DNK enake. Delno ujemanje je opredeljeno kot ujemanje, ko je vrednost enega ali vseh primerjanih alelov drugačna v obeh profilih DNK (kakovost 2, 3 in 4). Delno ujemanje je sprejemljivo le, če v obeh primerjanih profilih DNK obstaja vsaj 6 polno opredeljenih lokusov, ki se ujemajo.

Razloga za delno ujemanje sta lahko:

- tipkarska človeška napaka pri vnašanju enega izmed profilov DNK v zaprosilo za iskanje ali v zbirko podatkov o DNK,
- napaka pri določanju alelov (allele-determination) ali pri obravnavi alelov (allele-calling) med postopkom generiranja profilov DNK.

1.3 *Pravila poročanja*

Poročati je treba o polnih ujemanjih, približnih ujemanjih ter o neujemanjih („no hits“).

Poročilo o ujemanju se pošlje na nacionalno kontaktno službo države članice prosilke, ki pa mora biti tudi na razpolago nacionalni kontaktni službi zaprosene države članice (da bi slednja lahko ocenila vrsto in število možnih nadaljnjih zaprosil za osebne podatke in druge informacije, povezane s profilom DNK, ki ustrezajo zadetku v skladu s členoma 5 in 10 Sklepa 2008/615/PNZ).

2. *Tabela s številčnimi kodami držav članic*

V skladu s Sklepom 2008/615/PNZ se ISO 3166-1 alpha-2 kode uporabljajo za vzpostavitev domenskih imen in drugih konfiguracijskih parametrov, ki so potrebni v skladu s pürmskimi aplikacijami o izmenjavi podatkov o DNK v okviru zaprte mreže.

ISO 3166-1 alfa-2 kode so dvočrkovne kode držav članic, in sicer:



Imena držav članic	Koda	Imena držav članic	Koda
Belgija	BE	Luksemburg	LU
Bolgarija	BG	Madžarska	HU
Češka	CZ	Malta	MT
Danska	DK	Nizozemska	NL
Nemčija	DE	Avstrija	AT
Estonija	EE	Poljska	PL
Grčija	EL	Portugalska	PT
Španija	ES	Romunija	RO
Francija	FR	Slovaška	SK
Irska	IE	Slovenija	SI
Italija	IT	Finska	FI
Ciper	CY	Švedska	SE
Latvija	LV	Združeno kraljestvo	UK
Litva	LT		

3. **Funkcionalna analiza**

3.1 *Razpoložljivost sistema*

Zaprosila bi morala v skladu s členom 3 Sklepa 2008/615/PNZ prispeti v ciljno zbirko podatkov v kronološkem zaporedju pošiljanja posameznih zaprosil, odgovori pa bi morali biti poslani tako, da v državo članico prosilko prispejo v 15 minutah po prispetju zaprosila.

3.2 *Drugi korak*

Ko država prejme poročilo o ujemanju, je njena nacionalna kontaktna služba pristojna za primerjavo vrednosti profila, predloženega kot vprašanje, in vrednosti profila(-ov), prejetih kot odgovor, da bi lahko validirala in preverila dokazne vrednosti profila. Nacionalne kontaktne službe imajo za namene validacije lahko med seboj neposredne stike.

Postopki pravne pomoči se začnejo po validaciji obstoječega ujemanja med dvema profiloma, in sicer na podlagi „polnega ujemanja“ ali „približnega ujemanja“, pridobljenega med avtomatizirano posvetovalno fazo.

4. **Kontrolni dokument vmesnika DNK**

4.1 *Uvod*

4.1.1 *Cilji*

To poglavje določa zahteve za izmenjavo podatkov o profilih DNK med sistemi zbirk podatkov o DNK vseh držav članic. Polja glave so opredeljena posebej za prümisko izmenjavo DNK, podatkovni del pa temelji na podatkovnemu delu profila DNK v formatu XML, določenem za portal Interpola za izmenjavo DNK.

Izmenjava podatkov poteka preko SMPT (Simple Mail Transfer Protocol) in drugih najsodobnejših tehnologij z uporabo osrednjega rele poštne strežnika, ki ga zagotovi ponudnik dostopa do omrežja. Datoteka XML se prenaša kot telo elektronske pošte.

▼B**4.1.2 Področje uporabe**

Kontrolni dokument vmesnika (ICD) opredeljuje samo vsebino sporočila (elektronska pošta). Vsa vprašanja, ki se nanašajo posebej na omrežje ali na elektronsko pošto, so opredeljena enotno, da bi s tem zagotovili skupno tehnično osnovo za izmenjavo podatkov o DNK.

To vključuje:

- format polja, kamor se vpiše predmet sporočila, da bi s tem omogočili/upoštevali avtomatizirano obdelavo sporočil,
- ali je šifriranje vsebine potrebno in če je, katere metode je treba izbrati,
- najdaljšo možno dolžino sporočil.

4.1.3 Struktura XML in načela

Sporočilo XML je sestavljeno iz:

- glave, ki vsebuje informacije o prenosu, in
- podatkovnega dela, ki vsebuje specifične informacije o profilu, in še profil sam.

Za zaprosilo in za odgovor se uporablja isti format XML.

Zaradi celovitih preverjanj neznanih profilov DNK (člen 4 Sklepa 2008/615/PNZ) je v enem sporočilu mogoče poslati sveženj profilov. Določiti je treba največje možno število profilov v enem sporočilu. Število je odvisno od največje dovoljene velikosti elektronske pošte in se opredeli po izbiri poštne strežnika.

Primer 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> struktura podatkov se ponovi, če je v istem sporočilu SMTP (...) poslanih več profilov; to je dovoljeno samo v primerih iz člena 5

```
</datas>]
```

```
</PRUEMDNA>
```

4.2 Opredelitev strukture XML

Spodnje opredelitve so navedene za dokumentacijske namene in lažjo berljivost, zavezujoče informacije pa se nahajajo v shemski datoteki XML (PRUEMDNA.xsd).

▼B

4.2.1 Schema PRUEMDNax

Vsebuje naslednja polja:

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

4.2.2 Vsebina strukture glave

4.2.2.1 Glava PRUEM

Ta struktura opredeljuje glavo XML datoteke. Vsebuje naslednja polja:

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

Vrsta podatkov iz sporočila; vrednosti so lahko:

Value	Description
R	Request
A	Answer

4.2.2.3 Podatki glave PRUEM

Struktura z nazivom države članice in datum/uro sporočila. Vsebuje naslednja polja:

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 Vsebina podatkov profila PRUEM

4.2.3.1 PRUEM_datas

Ta struktura opredeljuje glavo podatkovnega dela XML profila. Vsebuje naslednja polja:

▼ 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

Vrsta podatkov iz sporočila; vrednosti so lahko:

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

Vrsta podatkov iz sporočila; vrednosti so lahko:

Value	Description
P	Person profile
S	Stain

4.2.2.5 PRUEM_data_result

Vrsta podatkov iz sporočila; vrednosti so lahko:

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

4.2.3.6 IPSTG_DNA_profile

Struktura, ki opisuje profil DNK. Vsebuje naslednja polja:

Fields	Type	Description
ess_issol	IPSTG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSTG_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 IPSTG_DNA_ISSOL

Struktura vsebuje ISSOL (Standard Group of Interpol loci). Vsebuje naslednja polja:

Fields	Type	Description
vwa	IPSTG_DNA_locus	Locus vwa
th01	IPSTG_DNA_locus	Locus th01
d21s11	IPSTG_DNA_locus	Locus d21s11
fga	IPSTG_DNA_locus	Locus fga
d8s1179	IPSTG_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

Struktura, ki vsebuje druge lokuse. Vsebuje naslednja polja:

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

Struktura, ki opisuje lokus. Vsebuje naslednja polja:

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

5. *Uporaba, varnost in komunikacijska struktura*5.1 *Pregled*

Pri izvajanju aplikacij za izmenjavo podatkov o DNK v okviru Sklepa 2008/615/PNZ se uporablja skupno komunikacijsko omrežje, ki bo med državami članicami zaprtega tipa. Za bolj učinkovito izrabo te skupne komunikacijske infrastrukture za pošiljanje

▼ B

zaposil in prejemanje odgovorov, se prevzame asinhroni mehanizem za pošiljanje zaprosil za podatke o DNK in daktiloskopske podatke v obliki zapakiranega elektronskega sporočila SMTP. Da bi zadostili varnostnim vprašanjem, se bo za vzpostavitev dejanskega in v celoti varnega tunela preko omrežja, uporabljal mehanizem sMIME, in sicer kot podaljšek delovanja SMTP.

Operativne storitve TESTA (Čezevropske telematske storitve med upravami – Trans European Services for Telematics between Administrations) se uporabljajo kot komunikacijsko omrežje za izmenjavo podatkov med državami članicami. TESTA je v pristojnosti Evropske komisije. Ob upoštevanju, da se nacionalne zbirke podatkov o DNK in trenutne nacionalne dostopne točke za omrežje TESTA, lahko nahajajo na različnih lokacijah v okviru držav članic, se lahko dostop do omrežja TESTA vzpostavi z:

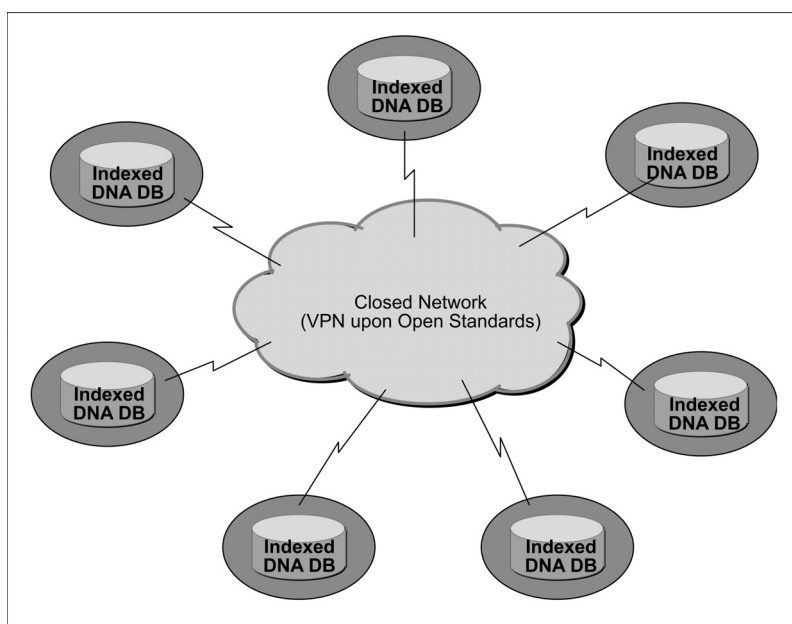
1. uporabo obstoječih nacionalnih dostopnih točk ali z oblikovanja novih dostopnih točk do omrežja TESTA ali
2. vzpostavitevijo zaščitene lokalne povezave od lokacije, kjer se nahaja zbirka podatkov o DNK, ki jo upravlja pristojna nacionalna agencija, do obstoječe nacionalne dostopne točke do omrežja TESTA.

Protokoli in standardi, ki se uporabljajo za izvajanje aplikacij iz Sklepa 2008/615/PNZ, so v skladu z odprtimi standardi in zahtevami oblikovalcev nacionalnih varnostnih politik držav članic.

5.2 *Struktura na višji ravni*

Področje uporabe Sklepa 2008/615/PNZ določa, da bo vsaka država članica v skladu s standardnim formatom podatkov omogočila izmenjavo svojih podatkov o DNK z drugo državo članico in/ali drugi državi članici omogočila iskanje po svojih podatkih o DNK. Struktura temelji na komunikacijskem modelu „vsak vsakemu“ (*any-to-any*). Za hranjenje profilov DNK ne obstaja osrednji računalniški strežnik niti centralizirana zbirka podatkov.

Slika 1: Tipologija izmenjave podatkov o DNK



▼ B

Poleg izpolnjevanja nacionalnih pravnih omejitev glede lokacij držav članic, se vsaka država članica lahko odloči kakšno vrsto strojne in programske opreme bo uporabljala za konfiguracijo na svoji lokaciji, da bo v skladu z zahtevami iz Sklepa 2008/615/PNZ.

5.3 *Varnostni standardi in varovanje podatkov*

Obstajajo tri ravni varnostnih vprašanj, o katerih se je razpravljalo in se jih tudi izvaja.

5.3.1 Podatkovna raven

Podatki o profilu DNK, ki jih zagotovi posamezna država članica, morajo biti oblikovani v skladu s skupnimi standardi o varovanju podatkov, in sicer tako, da država članica prosilka prejme odgovor, v katerem je navedeno, da obstaja zadetek (HIT) ali da zadetka ni (NO-HIT) ter v primeru zadetka (HIT) tudi identifikacijsko številko, ki pa ne vsebuje osebnih podatkov. Nadaljnje preiskovanje po prejetju obvestila o zadetku (HIT) se izvede na bilateralni ravni v skladu z veljavnimi nacionalnimi pravnimi in organizacijskimi predpisi lokacij zadevne države članice.

5.3.2 Komunikacijska raven

Sporočila, ki vsebujejo podatke o profilu DNK (zaposila in odgovori), bodo pred pošiljanjem na lokacije drugih držav članic šifrirana, in sicer s pomočjo najsodobnejšega a mehanizma v skladu z odprtimi standardi, kot je na primer sMIME.

5.3.3 Raven prenosa

Vsa šifrirana sporočila, ki vsebujejo podatke o profilu DNK, bodo poslana na lokacijo druge države članice s pomočjo zasebnega tunelskega sistema, ki ga na mednarodni ravni upravlja pooblaščen ponudnik dostopa do omrežja, in varnih povezav do tega tunelskega sistema, ki so v nacionalni pristojnosti. Navedeni virtualni zasebni tunelski sistem ni povezan z odprtim internetom.

5.4 *Protokoli in standardi, ki se uporabijo za šifrirni mehanizem: sMIME in s tem povezani paketi*

Za šifriranje sporočil, ki vsebujejo podatke o profilu DNK se bo uporabljal odprti standard sMIME, in sicer kot nadaljevanje dejanskega standarda za elektronsko pošto SMTP. Protokol sMIME (V3) omogoča podpisana potrdila o prejemu, varnostne oznake in zaščitene pošne seznime ter se opira na CMS (Cryptographic Message Syntax), ki je specifikacija IETF sporočila, ki so zaščitena s pomočjo šifriranja. Lahko se uporablja za digitalno podpisovanje, razporejanje, overjanje ali šifriranje vseh vrst digitalnih podatkov.

Osnovni certifikat, ki ga mehanizem sMIME uporablja, mora biti v skladu s standardom X.509. Da bi zagotovili skladnost skupnih standardov in postopkov z drugimi prümskimi aplikacijami, so procesna pravila za šifrirne operacije sMIME ali za uporabo v različnih komercialnih okoljih (COTS – Commercial Product of the Shelves) naslednja:

— Vrstni red operacij je: najprej šifriranje in potem podpis.

— Šifrirni algoritem AES (Advanced Encryption Standard) z 256-bitno dolžino ključa in RSA s 1 024-bitno dolžino ključa se uporablja za simetrično in asimetrično šifriranje.

— Uporablja se zagostitveni algoritem SHA-1.

▼ B

Funkcionalnost sMIME je vgrajena v veliko večino sodobnih programskih paketov za elektronsko pošto, med drugim tudi v Outlook, Mozilla Mail in Netscape Communicator 4.x, ter medsebojno deluje med vsemi večjimi programskimi paketi za elektronsko pošto.

Zaradi enostavne povezljivosti sMIME v nacionalno infrastrukturo IT na lokacijah vseh držav članic, je bil slednji izbran kot zanesljiv mehanizem za izvajanje varnostne komunikacijske ravni. Zaradi bolj učinkovitega doseganja cilja „Proof of Concept“ in znižanja stroškov je bil za prototipni razvoj izmenjave podatkov o DNK izbran odprti standard JavaMail API. JavaMail API zagotavlja enostavno šifriranje in dešifriranje elektronske pošte, in sicer z uporabo sMIME in/ali OpenPGP. Cilj je zagotoviti enoten in enostaven API za uporabnike elektronske pošte, ki želijo poslati in prejeti šifrirano elektronsko pošto v enem od obeh najbolj razširjenih formatov za šifriranje elektronske pošte. Zaradi tega bo izvajanje katerega koli najsodobnejšega JavaMail API, kot je na primer Bouncy Castle JCE (Java Cryptographic Extension), ki se bo uporabljal za izvajanje sMIME za prototipni razvoj izmenjave podatkov o DNK med državami članicami, izpolnilo zahteve iz Sklepa 2008/615/PNZ.

5.5 *Struktura aplikacije*

Vsaka država članica bo drugi državi članici zagotovila vrsto standardiziranih podatkov o profilu DNK, ki so v skladu s trenutnim skupnim kontrolnim dokumentom vmesnika (ICD). To se lahko izvede tako, da se zagotovi logični pregled posamezne nacionalne zbirke podatkov ali vzpostavi fizično izvoženo zbirko podatkov (indeksirana zbirka podatkov).

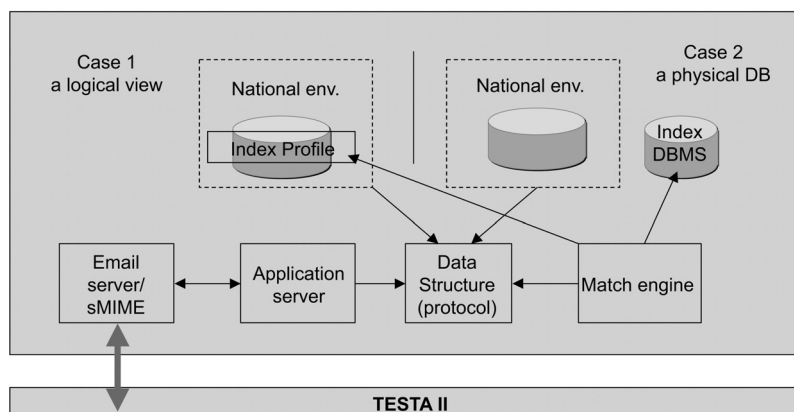
Štiri glavne komponente: poštni strežnik/sMIME, aplikacijski strežnik, območje za strukturo podatkov (Data Structure Area) za pobiranje/podajanje podatkov in registracijo prihajajočih/odhajajočih sporočil in motor ujemanja (Match Engine) izvajajo celotno aplikacijsko logiko, in sicer neodvisno od produkta.

Da bi vsem državam članicam zagotovili enostavno vključevanje komponent v njihove zadevne nacionalne lokacije, se je s pomočjo odprtokodnih komponent izvajala posebna skupna funkcionalnost, katero lahko izbere posamezna država članica glede na svoje politike in predpise IT. Zaradi izvajanja neodvisnih funkcij za dostop do indeksiranih zbirk podatkov profilov DNK iz Sklepa 2008/615/PNZ, lahko vsaka država članica izbere svojo strojno in programsko platformo, vključno z zbirko podatkov in operacijskimi sistemi.

Za izmenjavo podatkov o DNK je bil oblikovan prototip, ki je bil v obstoječem skupnem omrežju tudi uspešno testiran. Verzija 1.0 je bila oblikovana v produktivnem okolju in se uporablja za vsakodnevne operacije. Države članice lahko uporabljajo skupno razviti izdelek, ali pa razvijejo svoje lastne. Komponente skupnega izdelka bodo vzdrževane, prilagojene in nadalje razvite v skladu s spremembami v IT, sodni medicini in/ali praktičnimi zahtevami policije.

▼ B

Slika 2: Pregled topologije aplikacij

5.6 *Protokoli in standardi, ki se uporabijo za strukturo aplikacije*

5.6.1 XML

Izmenjava podatkov o DNK bo v celoti izkoristila shemo XML kot priložnost k elektronskim sporočilom SMTP. Razširljivi označevalni jezik (*eXtensible Markup Language – XML*) je označevalni jezik za splošne namene, ki ga priporoča W3C, za oblikovanje označevalnih jezikov s posebnim namenom, zmožnih opisovanja veliko različnih vrst podatkov. Opis profila DNK, primernega za izmenjavo med vsemi državami članicami, je bil izveden s XML in shemo XML v dokumentu ICD.

5.6.2 ODBC

Odperta povezljivost baz podatkov (*Open DataBase Connectivity – ODBC*) omogoča standardno metodo programske opreme API za dostop do sistemov za upravljanje baz podatkov in neodvisnost od programskih jezikov, sistemov baz podatkov in operacijskih sistemov. Kljub temu pa ima ODBC nekatere pomanjkljivosti. Upravljanje velikega števila naprav za odjemalce lahko pomeni več različnih gonilnikov in DLL. Ta kompleksnost lahko poveča skupne stroške za upravljanje sistema.

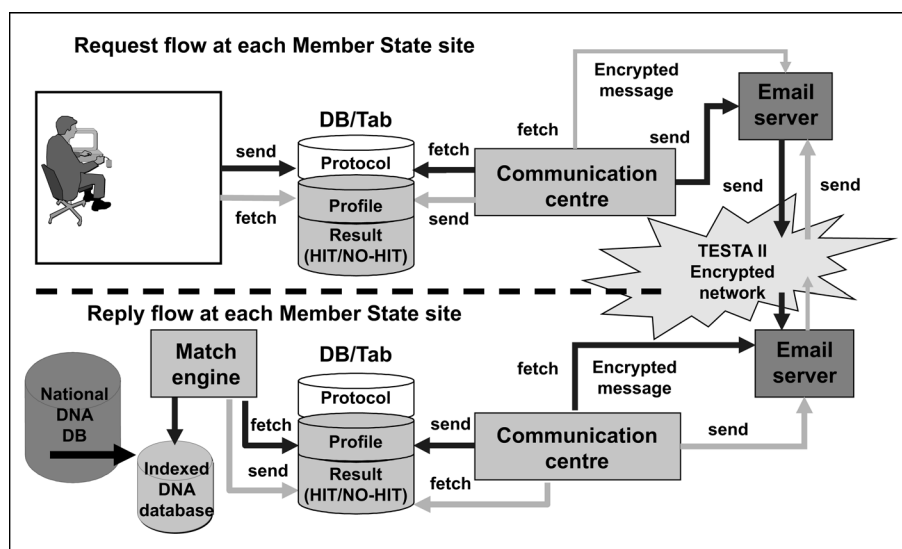
5.6.3 JDBC

Standard za baze podatkov pod java (Java DataBase Connectivity – JDBC) je API za programski jezik java, ki določa, kako lahko odjemalec vstopi v bazo podatkov. V nasprotju z ODBC pa JDBC ne zahteva uporabe določenega niza lokalnih DLL na namizju.

Poslovna logika za obdelavo zahtev za profil DNK in odgovorov na spletnih mestih držav članic je ponazorjena na spodnji sliki. Tokovi zahtev in odgovorov medsebojno vplivajo na nevtrarno področje podatkov, ki vsebujejo različne zaloge podatkov s skupno strukturo podatkov.

▼ B

Slika 3: Pregled aplikacije delovnega procesa na spletnih mestih vsake države članice



5.7 Komunikacijsko okolje

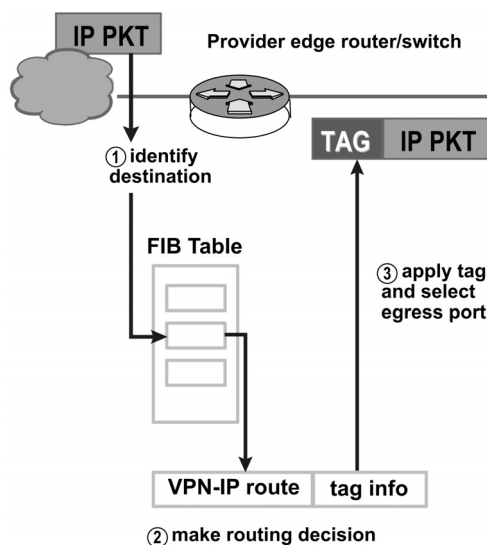
5.7.1 Skupno komunikacijsko omrežje: TESTA in njegova spremljevalna infrastruktura

Aplikacija izmenjave podatkov o DNK bo uporabljala e-pošto, asinhroni mehanizem, za pošiljanje zahtev in prejemanje odgovorov med državami članicami. Ker imajo vse države članice najmanj eno nacionalno dostopno točko do omrežja TESTA, bo izmenjava podatkov o DNK potekala prek omrežja TESTA. TESTA s svojim posredovanjem e-pošte omogoča več storitev z dodano vrednostjo. Poleg gostovanja e-poštnih nabiralnikov omrežja TESTA lahko ta infrastruktura uporablja tudi sezname distribucije pošte in politike usmerjanja. To omogoča uporabo omrežja TESTA kot klirinške hiše za sporočila, naslovljena na uprave, ki so povezane z domenami EU. Vzpostavijo se lahko tudi mehanizmi za preverjanje prisotnosti virusov.

Posredovanje pošte omrežja TESTA temelji na platformi strojne opreme visoke stopnje razpoložljivosti, ki se nahaja v prostorih centralne aplikacije omrežja TESTA in je zaščiteno s požarnim zidom. Storitve domenskih imen omrežja TESTA (*TESTA Domain Name Services – DNS*) bodo krajevne vire povezale z naslovi IP ter prikrile lastnosti naslova pred uporabniki in aplikacijami.

5.7.2 Pomisleki glede varnosti

Koncept VPN (virtualno zasebno omrežje (*Virtual Private Network*)) se izvaja v okviru omrežja TESTA. Tehnologija *tag switching*, ki se uporablja za izgradnjo omrežja VPN, bo postala podpora za standard *Multi-Protocol Label Switching (MPLS)*, ki ga je razvila organizacija IETF (*Internet Engineering Task Force*).

▼ B

MPLS je standardna tehnologija IETF, ki pospešuje pretok prometa omrežja z izogibanjem analize paketov vmesnih usmerjevalnikov (hopov). To poteka na podlagi t. i. oznak, ki jih paketu pripnejo robni usmerjevalniki hrbtenice, in sicer na podlagi podatkov, shranjenih v bazi za posredovanje podatkov (*forwarding information base – FIB*). Oznake se uporabljajo tudi za izvajanje virtualnih zasebnih omrežij (VPN).

MPLS združuje prednosti usmerjanja sloja 3 s prednostmi preklapljanja sloja 2. Ker se naslovi IP med prehodom skozi hrbtenico ne pregledajo, MPLS ne postavlja omejitev za naslavljanje IP.

Poleg tega bodo e-sporočila prek omrežja TESTA zaščitena s šifrirnim mehanizmom sMIME. Brez poznavanja ključa in pravega certifikata ne more nihče dešifrirati sporočil prek omrežja.

5.7.3 Protokoli in standardi, ki se uporabijo prek komunikacijskega omrežja

5.7.3.1 SMTP

Protokol enostavnega prenosa pošte (*Simple Mail Transfer Protocol – SMTP*) je *de facto* standard za prenos e-pošte prek interneta. SMTP je razmeroma enostaven, na besedilu temelječ protokol, pri katerem se določi eden ali več prejemnikov sporočila, preden se besedilo sporočila prenese. SMTP uporablja vrata TCP 25 na podlagi specifikacije IETF. Za določitev strežnika SMTP za določeno domensko ime se uporablja zapis MX (*Mail eXchange*) DNS (*Domain Name Systems*).

Ker je ta protokol sprva temeljil na besedilu v zapisu ASCII, ni bil najbolj primeren za binarne datoteke. Da bi se binarne datoteke lahko prenašale prek SMTP, so bili oblikovani standardi za kodiranje, kot je MIME. Danes večina strežnikov SMTP podpira 8BITMIME in končnico sMIME, kar omogoča, da se lahko binarne datoteke prenesejo skoraj tako enostavno kot navadno besedilo. Procesna pravila za operacije sMIME so opisana v odstavku sMIME (glej poglavje 5.4).

SMTP je „potisni“ protokol, ki ne dovoljuje „vlečenja“ sporočil iz oddaljenega strežnika na zahtevo. Za to mora poštni odjemalec uporabljati POP3 ali IMAP. V okviru izmenjave podatkov o DNK je sklenjeno, da se uporablja protokol POP3.



5.7.3.2 POP

Lokalni odjemalci e-pošte uporabljajo *Post Office Protocol version 3 (POP3)*, aplikacijsko-slojni standardni internetni protokol za pridobitev e-pošte iz oddaljenega strežnika prek povezave TCP/IP. Z uporabo profila SMTP Submit protokola SMTP e-poštni odjemalci pošiljajo sporočila po internetu ali prek korporacijskega omrežja. MIME služi kot standard za priponke in besedilo e-pošte, ki ni v zapisu ASCII. Čeprav POP3 in SMTP ne zahtevata e-pošte, formatirane v skladu s standardom MIME, je internetna e-pošta navadno v formatu MIME, zato morajo tudi odjemalci, ki uporabljajo POP, razumeti in uporabljati MIME. Celotno komunikacijsko okolje Sklepa 2008/615/PNZ bo zato vključevalo komponente POP.

5.7.4 Dodelitev omrežnega naslova

Operacijsko okolje

Evropski organ za dodeljevanje naslovov IP (*European IP Registration Authority – RIPE*) je omrežju TESTA trenutno dodelil namenski blok podomrežja razreda C 615 Omrežju TESTA se v prihodnje lahko po potrebi dodelijo nadaljnji naslovni bloki. Dodelitev naslovov IP državam članicam temelji na geografski shemi v Evropi. Izmenjava podatkov med državami članicami v okviru Sklepa 2008/615/PNZ se izvaja prek čezevropskega logično zaprtega omrežja IP.

Testno okolje

Za zagotovitev okolja, v katerem bi vsakodnevna izmenjava med vsemi povezanimi državami članicami potekala nemoteno, je treba vzpostaviti testno okolje v zaprtem omrežju za nove države članice, ki se pripravljajo na vključitev v operacijo. Določen je seznam parametrov, vključno z naslovi IP, nastavitvami omrežja, e-poštnimi domenami in računi uporabnikov aplikacije, ki mora biti vzpostavljen na ustreznem spletnem mestu zadevne države članice. Poleg tega je bil za namene testiranja izdelan niz izmišljenih profilov DNK.

5.7.5 Parametri konfiguracije

Vzpostavi se varni sistem e-pošte, ki uporablja domeno eu-admin.net. Ta domena in z njo povezani naslovi bodo dostopni samo z lokacij znotraj domene TESTA EU, kajti imena so poznana samo na centralnem strežniku DNS omrežja TESTA, ki je zaščiten pred internetom.

Preslikava teh naslovov mest omrežja TESTA (imen gostiteljev) na njihove naslove IP se izvaja s pomočjo storitve TESTA DNS. Za vsako lokalno domeno se bo temu centralnemu strežniku DNS omrežja TESTA dodal poštni vnos, ki bo centralnemu posredovalniku pošte omrežja TESTA posredoval vsa e-sporočila, poslana na lokalne domene omrežja TESTA. Ta centralni posredovalnik pošte omrežja TESTA jih bo nato posredoval specifičnemu strežniku e-pošte lokalne domene, in sicer ob uporabi e-poštnih naslovov lokalne domene. S takšnim posredovanjem e-pošte bodo kritični podatki, vsebovani v e-sporočilih, potekali le po zaprti čezevropski infrastrukturi omrežja in ne po nezaščitenem internetu.

▼ B

Poddomene je treba vzpostaviti (*v krepkem poševnem tisku*) na spletnih mestih vseh držav članic, in sicer z naslednjo sintakso:

„*application-type.pruem.Member State-code.eu-admin.net*“, pri čemer je:

„*Member State-code*“ ena od oznak države članice z dvema črkama (tj. AT, BE itd.);

„*application-type*“ ena izmed kratic: DNA ali FP.

Z uporabo zgornje sintakse so poddomene držav članic prikazane v naslednji tabeli:

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

▼ B

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

▼ B**POGLAVJE 2: Izmenjava daktiloskopskih podatkov (kontrolni dokument vmesnika)**

Namen naslednjega kontrolnega dokumenta vmesnika je opredeliti zahteve za izmenjavo daktiloskopskih podatkov med sistemi za avtomatsko identifikacijo prstnih odtisov (Automated Fingerprint Identification Systems – AFIS) držav članic. Dokument temelji na izvedbi ANSI/NIST-ITL 1-2000 (INT-I, različica 4.22b) s strani Interpol.

Ta različica zajema vse osnovne opredelitve za logične zapise tipa 1, tipa 2, tipa 4, tipa 9, tipa 13 in tipa 15, potrebne za daktiloskopsko obdelavo na podlagi podobe in minucij.

1. Pregled vsebine datoteke

Daktiloskopska datoteka je sestavljena iz več logičnih zapisov. Obstaja 16 tipov zapisa, opredeljenih v izvirnem standardu ANSI/NIST-ITL 1-2000. Ustrezni ločevalni znaki v zapisu ASCII so uporabljeni med vsakim zapisom ter polji in podpolji znotraj zapisov.

Za izmenjavo podatkov med agencijo izvora in ciljno agencijo se uporablja samo šest tipov zapisa:

- | | | |
|--------|---|--|
| Tip 1 | → | podatki o prenosu |
| Tip 2 | → | alfanumerične osebe/podatki o primerih |
| Tip 4 | → | daktiloskopske podobe visoke ločljivosti v lestvici sivine |
| Tip 9 | → | zapis minucij |
| Tip 13 | → | zapis podobe sledi različne ločljivosti |
| Tip 15 | → | zapis podobe odtisa dlani različne ločljivosti |

1.1 Tip 1 – naslovno polje datoteke

Ta zapis vsebuje usmerjevalne podatke in podatke o strukturi ostalih delov datoteke. Ta tip zapisa opredeljuje tudi tipe prenosa, ki se delijo na naslednje širše kategorije:

1.2 Tip 2 – besedilo opisa

Ta zapis vsebuje besedilne podatke, ki so v interesu agencij pošiljateljic in agencij prejemnic.

1.3 Tip 4 – podoba visoke ločljivosti v lestvici sivine

Ta zapis se uporablja za izmenjavo (8-bitnih) daktiloskopskih podob v lestvici sivine, skeniranih z ločljivostjo 500 slikovnih pik na palec. Daktiloskopske podobe se kompresirajo z uporabo algoritma WSQ z razmerjem največ 15:1. Drugi kompresijski algoritmi ali nekompresirane podobe se ne smejo uporabiti.

1.4 Tip 9 – zapis minucij

Zapisi tipa 9 se uporabljajo za izmenjavo podatkov o značilnosti grebenov ali minucijah. Deloma je njihov namen izogibanje nepotrebnim podvajanjem kodirnih postopkov sistema AFIS, deloma pa omogočenje prenosa kod tega sistema, ki vsebujejo manj podatkov kot ustrezne podobe.

▼ B1.5 *Tip 13 – zapis podobe sledi različne ločljivosti*

Ta zapis se uporablja za izmenjavo podob sledi prstnih odtisov in sledi odtisa dlani različne ločljivosti skupaj z alfanumeričnimi podatki tkiv. Ločljivost skeniranja podob je 500 slikovnih pik na palec pri 256 ravneh sivine. Če je kakovost podobe sledi zadostna, se kompresira z uporabo algoritma WSQ. Po potrebi se lahko na podlagi dvostranskega dogovora ločljivost podob razširi na več kot 500 slikovnih pik na palec in več kot 256 ravni sivine. V tem primeru je zelo priporočljivo, da se uporablja format JPEG 2000 (glej Dodatek 7).

1.6 *Tip 15 – zapis podobe odtisa dlani različne ločljivosti*

Zapisi podob tipa 15 v označenem polju se uporabijo za izmenjavo podob odtisa dlani različne ločljivosti z alfanumeričnimi podatki tkiv. Ločljivost skeniranja podob je 500 slikovnih pik na palec pri 256 ravneh sivine. Za zmanjšanje količine podatkov na najnižjo možno raven se vse podobe odtisa dlani kompresirajo z uporabo algoritma WSQ. Po potrebi se lahko na podlagi dvostranskega dogovora ločljivost podob razširi na več kot 500 slikovnih pik na palec in več kot 256 ravni sivine. V tem primeru je zelo priporočljivo, da se uporablja format JPEG 2000 (glej Dodatek 7).

2. *Format zapisa*

Datoteka prenosa je sestavljena iz enega ali več logičnih zapisov. Za vsak logični zapis, ki ga vsebuje datoteka, je prisotnih več podatkovnih polj, ustreznih temu tipu zapisa. Vsako podatkovno polje lahko vsebuje eno ali več osnovnih vrst podatkov z enojno vrednostjo. Ti podatki se kot celota uporabijo za prenos različnih vidikov podatkov, zajetih v tem polju. Podatkovno polje je lahko sestavljeno tudi iz ene ali več vrst podatkov, povezanih v skupino in večkrat ponovljenih v okviru polja. Taka skupina vrst podatkov se imenuje podpolje. Podatkovno polje je zato lahko sestavljeno iz enega ali več podpolj vrst podatkov.

2.1 *Ločevalni znaki med podatki*

V logičnih zapisih v označenem polju se mehanizmi za razmejitev podatkov izvajajo z uporabo štirih ločevalnih znakov med podatki v zapisu ASCII. Razmejeni podatki so lahko deli zapisa znotraj polja ali podpolja, polja znotraj logičnega zapisa ali več pojavov podpolj. Ti ločevalni znaki med podatki so opredeljeni v standardu ANSI X3.4. Ti znaki se uporabljajo za ločevanje in kvalificiranje podatkov v logičnem smislu. Z vidika hierarhičnega odnosa je znak za ločevalni znak za datoteko (*File Separator* „FS“) najbolj vključujoč, sledijo mu ločevalni znak za skupino (*Group Separator* „GS“), ločevalni znak za zapis (*Record Separator* „RS“) in končno ločevalni znak za enoto (*Unit Separator* „US“). V tabeli 1 so naštet ti ločevalni znaki v zapisu ASCII in opis njihove uporabe v okviru tega standarda.

Ločevalni znaki med podatki bi morali biti funkcionalno razumljeni kot označba tipa podatkov, ki sledi. Znak „US“ ločuje posamezne vrste podatkov znotraj polja ali podpolja. To je znak, da se naslednja vrsta podatkov nanaša na to polje ali podpolje. Več podpolj znotraj polja, ločenega z znakom „RS“, označuje začetek naslednje skupine ponovljene(-ih) vrst(-e) podatkov. Ločevalni znak „GS“, uporabljen med podatkovnimi polji, označuje začetek novega polja, ki mu sledi številka, ki označuje polje in se tudi pojavi. Podobno se začetek novega logičnega zapisa označi z znakom „FS“.

▼B

Ti štirje znaki imajo svoj pomen le, ko se uporabijo kot ločevalni znaki vrst podatkov v poljih besedil v zapisu ASCII. Ko se ti znaki pojavljajo v binarnih zapisih podob in binarnih poljih, nimajo posebnega pomena – so le del izmenjanih podatkov.

Praviloma ne bi smelo biti praznih polj ali vrst podatkov in zato bi se moral med katerima koli vrstama podatkov pojaviti po en ločevalni znak. Izjema tega pravila so primeri, ko podatki v poljih ali vrste podatkov pri prenosu niso na voljo, manjkajo ali je njihova navedba neobvezna in obdelava prenosa ni odvisna od prisotnosti teh podatkov. V teh primerih se več ločevalnih znakov in sosednji ločevalni znaki pojavijo skupaj in ne zahtevajo vnosa namišljenih podatkov med ločevalne znake.

Za opredelitev polja, sestavljenega iz treh vrst podatkov, velja naslednje. Če manjkajo podatki za drugo vrsto podatkov, se med prvo in tretjo vrsto podatkov pojavita dva sosednja ločevalna znaka med podatki „US“. Če manjkata druga in tretja vrsta podatkov, se morajo uporabiti trije ločevalni znaki – dva „US“ znaka poleg ločevalnega znaka končnega polja ali podpolja. Na splošno, če ena ali več obveznih ali neobveznih vrst podatkov za polje ali podpolje ni na voljo, je treba vstaviti ustrezno število ločevalnih znakov.

Možna je vzporedna uporaba kombinacij dveh ali več izmed štirih možnih ločevalnih znakov. Ko podatki manjkajo ali niso na voljo za vrste podatkov, podpolja ali polja, mora biti en ločevalni znak manj, kot je število zahtevanih vrst podatkov, podpolj ali polj.

Tabela 1: Uporabljeni ločevalni znaki

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

Razporeditev zapisa

Za logične zapise v označenem polju se vsako uporabljeno podatkovno polje oštevilči v skladu s tem standardom. Format za vsako polje je sestavljen iz logičnega zapisa številke tipa, ki mu sledi pika „.“, številke polja, ki mu sledi dvopičje „.“, temu pa sledi podatek, ustrezen za to polje. Številka označenega polja je lahko katera koli številka od 1 do 9 med piko „.“ in dvopičjem „.“. Razume se kot cela številka polja brez predznaka. To pomeni, da je številka polja „2.123.“ enako ali se razlaga enako kot številka polja „2.000000123.“.

Za ilustracijo se v celotnem pričujočem dokumentu uporabi trimesna številka za štetje polj v vsakem logičnem zapisu označenega polja, opisanem v dokumentu. Številke polj imajo obliko „TT.xxx.“, kadar „TT“ predstavlja tip zapisa z enim ali dvema znakoma, ki jima sledi pika. Naslednji trije znaki vsebujejo ustrezno številko polja, ki ji sledi dvopičje. Dvopičju sledijo deskriptivni podatki v zapisu ASCII ali podatki podobe.

▼B

Logični zapisi tipa 1 in tipa 2 vsebujejo samo tekstualna polja podatkov v zapisu ASCII. Celotna dolžina zapisa (vključno s števili polj, dvopičji in ločevalnimi znaki) se zapiše kot prvo polje v zapisu ASCII v vsakem izmed teh tipov zapisa. Ločevalni kontrolni znak „FS“ datotek v zapisu ASCII (ki označuje konec logičnega zapisa ali prenosa) sledi zadnjemu bajtu podatkov v zapisu ASCII in je vključen v dolžino zapisa.

Zapis tipa 4 v nasprotju s konceptom označenega polja vsebuje samo binarne podatke, zabeležene kot urejena binarna polja fiksne dolžine. Celotna dolžina zapisa se zabeleži v prvem štiribajtnem binarnem polju vsakega zapisa. Za ta binarni zapis se ne zabeleži niti številka zapisa s piko niti identifikacijska številka polja s piko, ki ji sledi. Ker so vse dolžine polj tega zapisa fiksne ali določene, se vsak ločevalni znak („US“, „RS“, „GS“ ali „FS“) razume zgolj kot binarni podatek. Znak „FS“ za binarni zapis se ne uporabi kot ločevalni znak zapisa ali končni znak prenosa.

3. *Logični zapis tipa 1: glava datoteke*

Ta zapis opisuje strukturo in tip datoteke ter druge pomembne podatke. Niz znakov, uporabljen za polja tipa 1, vsebuje samo 7-bitno kodo ANSI za izmenjavo podatkov.

3.1 *Polja logičnega zapisa tipa 1*

3.1.1 Polje 1.001: Dolžina logičnega zapisa (Logical Record Length – LEN)

To polje vsebuje skupno število bajtov v celotnem logičnem zapisu tipa 1. Polje se začne z „1.001:“, temu pa sledi skupna dolžina zapisa, vključno z vsemi znaki vseh polj in ločevalnih znakov med podatki.

3.1.2 Polje 1.002: Številka različice (Version Number – VER)

Da bi se zagotovilo, da uporabniki vedo, katera različica standarda ANSI/NIST se uporablja, to štiribajtno polje označuje številko različice standarda, ki ga uporablja programska oprema ali sistem, ki ustvari datoteko. Prva dva bajta navajata glavno referenčno številko različice, druga dva pa pomožno revizijsko številko. Na primer, izvirni standard 1986 naj bi bil prva različica z oznako „0100“, sedanjí standard ANSI/NIST-ITL 1-2000 pa „0300“.

3.1.3 Polje 1.003: Vsebina datoteke (File Content – CNT)

V tem polju so naštetí vsi zapisi v datoteki po tipih zapisa in v zaporedju, v katerem se zapisi pojavljajo v logični datoteki. Polje je sestavljeno iz enega ali več podpolj, od katerih vsako vsebuje dve vrsti podatkov, ki opisujeta enojni logični zapis iz trenutne datoteke. Podpolja so vnesena v istem vrstnem redu, v katerem se zapisi beležijo in posredujejo.

Prva vrsta podatkov v prvem podpolju je „1“ in se nanaša na ta zapis tipa 1. Sledi ji druga vrsta podatkov, ki vsebuje številko drugih zapisov iz te datoteke. Ta številka je tudi enaka številu preostalih podpolj polja 1.003.

▼ B

Vsako izmed preostalih podpolj se navezuje na en zapis v okviru datoteke, zaporedje podpolj pa ustreza zaporedju zapisov. Vsako podpolje vsebuje dve vrsti podatkov. Prva navaja tip zapisa. Druga je znak za označitev podobe (*image designation character* – IDC) zapisa. Znak „US“ se uporablja za ločevanje dveh vrst podatkov.

3.1.4 Polje 1.004: Tip prenosa (Type of Transaction – TOT)

To polje vsebuje mnemomik s tremi črkami, ki označuje tip prenosa. Te kode so lahko različne od tistih, ki jih uporabljajo druge izvedbe standarda ANSI/NIST.

CPS: Iskanje odtisov kaznivih dejanj v podatkovni bazi odtisov (*Criminal Print-to-Print Search*). Ta prenos je zahteva po iskanju zapisov v zvezi s kaznivimi dejanji v podatkovni bazi odtisov. Odtisi osebe se morajo v datoteko vključiti kot podobe, kompresirane z uporabo algoritma WSQ.

V primeru, da ni zadetka (*No-HIT*), se prikažeta naslednja logična zapisa:

- 1 Type-1 Record,
- 1 Type-2 Record.

V primeru zadetka (*HIT*) se prikažejo naslednji logični zapisi:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1-14 Type-4 Record.

Povzetek CPS TOT je v tabeli A.6.1 (Dodatek 6).

PMS: Iskanje od odtisa do sledi (*Print-to-Latent Search*). Ta prenos se uporablja, ko se išče niz odtisov v podatkovni bazi neprepoznanih sledi. Odgovor vsebuje odločitev (*Hit/No-Hit*) glede iskanja v ciljnem sistemu AFIS. Če obstaja več neprepznanih sledi, se prikaže več prenosov SRE z eno sledjo na prenos. Odtisi osebe se morajo v datoteko vključiti kot podobe, kompresirane z uporabo algoritma WSQ.

V primeru, da ni zadetka (*No-HIT*), se prikažeta naslednja logična zapisa:

- 1 Type-1 Record,
- 1 Type-2 Record.

V primeru zadetka (*HIT*) se prikažejo naslednji logični zapisi:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1 Type-13 Record.

Povzetek PMS TOT je v tabeli A.6.1 (Dodatek 6).

MPS: Iskanje od sledi do odtisa (*Latent-to-Print Search*). Ta prenos se uporablja, ko se sled išče v podatkovni bazi odtisov. Podatki o minucijah sledi in podoba (kompresirana z uporabo algoritma WSQ) morajo biti vključeni v datoteko.

V primeru, da ni zadetka (*No-HIT*), se prikažeta naslednja logična zapisa:

- 1 Type-1 Record,
- 1 Type-2 Record.

▼B

V primeru zadetka (*HIT*) se prikažejo naslednji logični zapisi:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1 Type-4 or Type-15 Record.

Povzetek MPS TOT je v tabeli A.6.4 (Dodatek 6).

MMS: Iskanje od sledi do sledi (*Latent-to-Latent Search*). Pri tem prenosu datoteka vsebuje sledi, ki se iščejo v bazi podatkov neprepoznanih sledi. Podatki o minucijah sledi in podoba (kompresirana z uporabo algoritma WSQ) morajo biti vključeni v datoteko.

V primeru, da ni zadetka (*No-HIT*), se prikažeta naslednja logična zapisa:

- 1 Type-1 Record,
- 1 Type-2 Record.

V primeru zadetka (*HIT*) se prikažejo naslednji logični zapisi:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1 Type-13 Record.

Povzetek MMS TOT je v tabeli A.6.4 (Dodatek 6).

SRE: Ta prenos uporabi ciljna agencija v odgovor na daktiloskopske vloge. Odgovor vsebuje odločitev (*Hit/No-Hit*) glede iskanja v ciljnim sistemu AFIS. Če obstaja več kandidatov, se prikaže več prenosov SRE z enim kandidatom na prenos.

Povzetek SRE TOT je v tabeli A.6.2 (Dodatek 6).

ERR: Ta prenos prikaže ciljni sistem AFIS, kadar pride do napake pri prenosu. Vključuje sporočilno polje (ERM), ki označuje odkrito napako. Prikažeta se naslednja logična zapisa:

- 1 Type-1 Record,
- 1 Type-2 Record.

Povzetek ERR TOT je v tabeli A.6.3 (dodatek 6).

Tabela 2: Dovoljene kode pri prenosu

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 = obvezno (*Mandatory*)

M* = vključi se lahko samo eden od obeh tipov zapisa

O = neobvezno (*Optional*)

C = pogojno, če so podatki na voljo (*Conditional on whether data is available*)

— = ni dovoljeno

1* = pogojno, odvisno od razpoložljivih sistemov

3.1.5 Polje 1.005: Datum prenosa (DAT)

To polje označuje datum, ko je bil prenos začet, in mora biti v skladu s standardnim zapisom ISO: YYYYMMDD,

pri čemer YYYY pomeni leto, MM mesec in DD dan v mesecu. Pri enomestnih številkah se na začetku uporabi ničla. Na primer, zapis „19931004“ označuje 4. oktober 1993.

3.1.6 Polje 1.006: Prioriteta (Priority – PRY)

To neobvezno polje označuje prioriteto zahteve od 1 do 9. „1“ je najvišja prioriteta in „9“ najnižja. Prenosi prioritete „1“ se obdelajo takoj.

3.1.7 Polje 1.007: Identifikator ciljne agencije (Destination Agency Identifier – DAI)

To polje označuje ciljno agencijo za prenos.

Zajema dve vrsti informacij v formatu: CC/agency.

Prva vrsta podatkov vsebuje kodo države, opredeljeno v ISO 3166, v dolžini dveh alfanumeričnih znakov. Druga vrsta podatkov, tj. agency, je identifikacija agencije v obliki prostega besedila, v dolžini največ 32 alfanumeričnih znakov.

3.1.8 Polje 1.008: Identifikator agencije izvora (Originating Agency Identifier – ORI)

To polje označuje vir datoteke in ima isti format kot DAI (polje 1.007).

3.1.9 Polje 1.009: Kontrolna številka prenosa (Transaction Control Number – TCN)

To je kontrolna številka za namene sklicevanja. Prikaže jo računalnik in ima naslednji format: YYSSSSSSSA,

pri čemer je YY leto prenosa, SSSSSSSS osemestna serijska številka, A pa kontrolni znak, ki se prikaže ob izvedbi postopka, opisanega v Dodatku 2.

Kadar TCN ni na voljo, se v polju YYSSSSSSSS prikažejo ničle in kontrolni znak, kakor v zgornjem primeru.

3.1.10 Polje 1.010: Kontrolni odgovor prenosa (Transaction Control Response – TCR)

Kadar je bila poslana zahteva, na katero je to odgovor, to neobvezno polje vsebuje kontrolno številko prenosa sporočila zahteve. Zato je v enakem formatu kot TCN (polje 1.009).

▼B**3.1.11 Polje 1.011: Prvotna ločljivost skeniranja (Native Scanning Resolution – NSR)**

To polje označuje običajno ločljivost skeniranja sistema, ki jo podpira vir prenosa. Ločljivost je opredeljena z dvoštevničnim znakom, ki mu sledi decimalna pika in še dve številki.

Za vse prenose v skladu s Sklepom 2008/615/PNZ je velikost vzorca 500 slikovnih pik na palec ali 19,68 slikovnih pik/mm.

3.1.12 Polje 1.012: Nominalna ločljivost prenosa (Nominal Transmitting Resolution – NTR)

To petbajtno polje označuje nominalno ločljivost prenosa za podobe, ki se prenašajo. Ločljivost je izražena v slikovnih pikah na mm v istem formatu kot NSR (polje 1.011).

3.1.13 Polje 1.013: Domensko ime (DOM)

To obvezno polje označuje domensko ime za izvedbo logičnega zapisa tipa 2, ki ga opredelijo uporabniki. Sestavljeno je iz dveh vrst podatkov in je „INT-I{US}4.22{GS}“.

3.1.14 Polje 1.014: Greenwiški srednji čas (Greenwich mean time – GMT)

To obvezno polje omogoča mehanizem za zapis datuma in časa v enotah univerzalnega greenwiškega srednjega časa (GMT). Če se polje GMT uporabi, vsebuje univerzalni datum, ki bo poleg lokalnega datuma naveden v polju 1.005 (DAT). Uporaba polja GMT odpravlja nedoslednosti lokalnega časa, ki se pojavijo, ko prenos in odgovor potekata med dvema krajema v različnih časovnih območjih. GMT prikaže univerzalni čas in 24-urni čas ne glede na časovna območja. Predstavljen je kot „CCYYMMD-DUUMMSSZ“, 15-mestna številka, sestavljena iz datuma in GMT ter se konča z „Z“. Znaki „CCYY“ predstavljajo leto prenosa, „MM“ so desetice in enice vrednosti meseca, „DD“ desetice in enice vrednosti dneva v mesecu, „HH“ ure, „MM“ minute in „SS“ sekunde. Celotni datum ni poznejši od trenutnega datuma.

4. Logični zapis tipa 2: opisno besedilo

Struktura večine tega zapisa ni opredeljena z izvirnim standardom ANSI/NIST. Ta zapis vsebuje informacije posebnega pomena za agencije, ki pošiljajo ali sprejemajo datoteke. Za zagotovitev združljivosti daktiloskopskih sistemov se zahteva, da zapis vsebuje le spodaj naštetja polja. Ta dokument določa, katera polja so obvezna in katera neobvezna in opredeljuje strukturo posameznih polj.

4.1 Polja logičnega zapisa tipa 2**4.1.1 Polje 2.001: Dolžina logičnega zapisa (Logical Record Length – LEN)**

To obvezno polje vsebuje dolžino tega zapisa tipa 2 in določa skupno število bajtov, vključno z vsakim znakom vsakega polja, vsebovanega v zapisu, in ločevalnimi znaki med podatki.

4.1.2 Polje 2.002: Znak za označitev podobe (Image Designation Character – IDC)

IDC iz tega obveznega polja je IDC v zapisu ASCII, kakor je opredeljen v polju vsebina datoteke (*File Content – CNT*) zapisa tipa 1 (polje 1.003).

▼B**4.1.3 Polje 2.003: Podatki o sistemu (System Information – SYS)**

To polje je obvezno in vsebuje štiri bajte, ki označujejo, s katero različico INT-I je ta podatek tipa 2 skladen.

Prva dva bajta navajata glavno številko različice, druga dva pa pomožno revizijsko številko. Na primer, ta izvedba temelji na različici INT-I 4 revizija 22 in bi bila prikazana kot „0422“.

4.1.4 Polje 2.007: Številka zadeve (Case Number – CNO)

To je številka, ki jo določi lokalni daktiloskopski urad za zbirko sledi, najdenih na kraju kaznivega dejanja. Sprejme se naslednji format: CC/številka

pri čemer CC pomeni Interpolovo kodo države, dolgo dva alfanumerična znaka ter je številka skladna z ustreznimi lokalnimi smernicami in je lahko dolga do 32 alfanumeričnih znakov.

To polje omogoča sistemu, da prepozna sledi, povezane z določenim kaznivim dejanjem.

4.1.5 Polje 2.008: Številka sekvence (SQN)

Ta označuje vsako sekvenco sledi v okviru posameznega primera. Dolga je lahko največ dva numerična znaka. Sekvenca je sled ali niz sledi, povezane v skupino zaradi katalogizacije in/ali iskanja. Ta opredelitev pomeni, da je treba tudi enojnim sledem pripisati številko sekvence.

To polje je lahko skupaj z MID (polje 2.009) vključeno za prepoznavanje posamezne sledi znotraj posamezne sekvence.

4.1.6 Polje 2.009: Identifikator sledi (Latent Identifier – MID)

Ta označuje posamezno sled v okviru sekvence. Vrednost je ena ali dve črki, pri čemer je „A“ določena za prvo sled, „B“ za drugo in tako naprej do „ZZ“. To polje se uporablja analogno za številko sekvenco sledi, navedeno v opisu za SQN (polje 2.008).

4.1.7 Polje 2.010: Referenčna številka storilca kaznivih dejanj (Criminal Reference Number – CRN)

To je edinstvena referenčna številka, ki jo nacionalna agencija dodeli posamezniku, ki je prvič obtožen storitve kaznivega dejanja. Znotraj ene države noben posameznik nima več kot ene CRN ali jo deli z drugim posameznikom. Vendar pa ima lahko posameznik referenčne številke storilca kaznivih dejanj v več državah, ki se razlikujejo v kodi države.

Za polje CRN se sprejme naslednji format: CC/številka

pri čemer CC pomeni kodo države, opredeljeno v ISO 3166, dolgo dva alfanumerična znaka ter je številka skladna z ustreznimi nacionalnimi smernicami agencije izdajateljice in je lahko dolga do 32 alfanumeričnih znakov.

Za prenos v skladu s Sklepom 2008/615/PNZ se to polje uporablja za nacionalno referenčno številko storilca kaznivih dejanj agencije izvora, ki je povezana s podobami v zapisih tipa 4 in tipa 5.

▼B

4.1.8 Polje 2.012: Identifikacijska številka (Miscellaneous Identification Number – MN1)

To polje vsebuje CRN (polje 2.010), ki se prenaša prek CPS ali PMS brez kode vodilne države.

4.1.9 Polje 2.013: Identifikacijska številka (Miscellaneous Identification Number – MN2)

To polje vsebuje CNO (polje 2.007), ki se prenaša prek MPS ali MMS brez kode vodilne države.

4.1.10 Polje 2.014: Identifikacijska številka (Miscellaneous Identification Number – MN3)

To polje vsebuje SQN (polje 2.008), ki se prenaša prek MPS ali MMS.

4.1.11 Polje 2.015: Identifikacijska številka (Miscellaneous Identification Number – MN4)

To polje vsebuje MID (polje 2.009), ki se prenaša prek MPS ali MMS.

4.1.12 Polje 2.063: Dodatni podatki (Additional Information – INF)

V primeru prenosa SRE na zahtevo PMS to polje prikaže podatke o prstnem odtisu, ki bi bil lahko možni zadetek (*HIT*). Format polja je:

NN, pri čemer je *NN* koda položaja prsta, ki je opredeljena v tabeli 5 in ima dolžino dveh številčnih znakov.

V vseh drugih primerih je to polje neobvezno. Vsebuje do 32 alfanumeričnih znakov in lahko prikaže dodatne podatke o zahtevi.

4.1.13 Polje 2.064: Seznam zadetkov (Respondents List – RLS)

To polje vsebuje najmanj dve podpolji. Prvo podpolje opisuje tip izvedenega iskanja z uporabo mnemonikov s tremi črkami, ki označujejo tip prenosa v TOT (polje 1.004). Drugo podpolje vsebuje enojni znak. Za označitev zadetka (*HIT*) se uporabi „I“, če ni zadetka (*NO-HIT*) pa „N“. Tretje podpolje vsebuje identifikator sekvence za kandidata za rezultat in skupno število kandidatov, ločenih s poševnico. Več sporočil se vrne, če obstaja več kandidatov.

V primeru zadetka (*HIT*) četrto podpolje vsebuje rezultat, ki je največ šestmesten. Če je zadetek (*HIT*) potrjen, je vrednost podpolja opredeljena kot „999999“.

Primer: „CPS{RS}I{RS}001/001{RS}999999{GS}“

Če oddaljeni AFIS ne prikaže rezultata, se uporabi rezultat nič z ustrezno piko.

4.1.14 Polje 2.074: Polje sporočila o statusu/napaki (Status/Error Message Field – ERM)

To polje vsebuje sporočilo o napaki, ki nastane pri prenosu, ki se pošlje prosilcu kot del napake pri prenosu (*Error Transaction*).



Tabela 3: Sporočila o napaki

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.

Sporočila o napaki v razponu med 100 in 199:

Ta sporočila o napaki se nanašajo na validacijo zapisov ANSI/NIST in so opredeljena kot:

<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>...

pri čemer je

— *error_code* koda, ki se nanaša samo na specifični razlog (glej tabelo 3),

— *field_id* številka nepravilnega polja standarda ANSI/NIST (npr. 1.001, 2.001, ...) v formatu <record_type>.field_id>.sub_field_id>,

▼B

- dinamično besedilo podrobnejši dinamični opis napake,
- LF vrstični presledek (Line Feed), ki ločuje napake, če se odkrije več kot ena napaka,
- zapis tipa 1 ICD opredeljen kot „-1“.

Primer:

201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER
{LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION

To polje je obvezno za napake pri prenosu.

- 4.1.15 Polje 2.320: Predvideno število kandidatov
(Expected Number of Candidates – ENC)

To polje vsebuje največje možno število kandidatov za preverjanje, ki jih predvideva agencija prosilka. Vrednost ENC ne sme presegati vrednosti, določenih v tabeli 11.

5. **Logični zapis tipa 4: Podoba visoke ločljivosti v lestvici sivine**

Treba je opozoriti, da so zapisi tipa 4 v binarni obliki in ne v zapisu ASCII. Zato je za vsako polje določeno posebno mesto v zapisu, kar pomeni, da so vsa polja obvezna. Ta standard omogoča, da se v zapisu določita tako velikost podobe kot njena ločljivost. Logični zapisi tipa 4 morajo vsebovati daktiloskopske podatke o podobi, ki se prenašajo z nominalno gostoto 500 do 520 slikovnih pik na palec. Zaželena gostota za nove podobe je 500 slikovnih pik na palec ali 19,68 slikovnih pik na mm. Gostota 500 slikovnih pik na palec je določena v INT-I; podobni sistemi lahko sicer med seboj komunicirajo v drugačnem razmerju, vendar v okviru 500 do 520 slikovnih pik na palec.

5.1 *Polja logičnega zapisa tipa 4*

- 5.1.1 Polje 4.001: Dolžina logičnega zapisa (Logical Record Length – LEN)

To štiribajtno polje vsebuje dolžino tega zapisa tipa 4 in označuje skupno število bajtov, vključno z bajti iz vseh polj, ki so v zapisu.

- 5.1.2 Polje 4.002: Znak za označitev podobe (Image Designation Character – IDC)

To je enobajtna binarna predstavitev številke IDC iz datoteke „header file“.

- 5.1.3 Polje 4.003: Tip odčitavanja (Impression Type – IMP)

Tip odčitavanja je enobajtno polje, ki zavzema šesti bajt zapisa.

Tabela 4: Tip odčitavanja prsta (Finger Impression Type)

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 Polje 4.004: Položaj prstov (Finger Position – FGP)

To polje z določeno dolžino 6 bajtov zavzema bajtna mesta 7 do 12 v zapisu tipa 4. Vsebuje možne položaje prstov, začenši z bajtom na skrajni levi strani (7. bajt v zapisu). Znani ali najbolj verjetni položaj prstov je privzet iz tabele 5. Z vnosom nadomestnih položajev prstov v preostalih pet bajtov je ob uporabi enakega formata lahko razvrščeno do pet dodatnih prstov. Če je označeno manj kot pet položajev prstov se neuporabljeni bajti zapolnijo z binarno številko 255. Za označitev vseh položajev prstov se uporabi koda 0, tj. neznano.

Tabela 5: Kode za položaj prstov in največja velikost

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

Za sledi s kraja kaznivega dejanja bi se morale uporabiti le kode od 0 do 10.

▼B**5.1.5 Polje 4.005: Ločljivost skeniranja podobe (Image Scanning Resolution – ISR)**

To enobajtno polje zaseda 13. bajt zapisa tipa 4. Če vsebuje „0“, pomeni, da je bila podoba skenirana v zaželeni resoluciji 19,68 slikovnih pik na mm (500 slikovnih pik na palec). Če vsebuje „1“, pomeni, da je bila podoba skenirana v drugačni resoluciji, kakor je določeno v zapisu tipa 1.

5.1.6 Polje 4.006: Dolžina horizontalne vrstice (Horizontal Line Length – HLL)

To polje se nahaja pri 14. in 15. bajtu v zapisu tipa 4. Označuje število slikovnih pik iz vsake skenirane vrstice. Najbolj pomemben je prvi bajt.

5.1.7 Polje 4.007: Dolžina vertikalne vrstice (Vertical Line Length – VLL)

To polje v 16. in 17. bajtu beleži število skeniranih vrstic v podobi. Najbolj pomemben je prvi bajt.

5.1.8 Polje 4.008: Kompresijski algoritem lestvice sivine (Gray-scale Compression Algorithm – GCA)

To enobajtno polje označuje kompresijski algoritem lestvice sivine, ki se uporablja pri kodiranju podatkov o podobi. Pri tem binarna koda 1 označuje, da je bila uporabljena kompresija WSQ (Priloga 7).

5.1.9 Polje 4.009: Podoba (The image)

To polje vsebuje tok bajtov, ki predstavljajo podobo. Njegova struktura je seveda odvisna od uporabljenega kompresijskega algoritma.

6. Logični zapis tipa 9: Zapis minucij

Zapisi tipa 9 vsebujejo besedilo ASCII, ki opisuje minucije in z njimi povezane podatke, kodirane iz sledi. Pri prenosu iskanja sledi za te zapise tipa 9 v datoteki ni omejitev; vsaka izmed teh datotek je namenjena drugemu pogledu ali sledi.

6.1 Izločanje minucij**6.1.1 Določitev tipa minucije**

V tem standardu so opredeljene tri identifikacijske številke za opis tipa minucije. Te so navedene v tabeli 6. Tip 1 označuje zaključek grebena. Tip 2 označuje bifurkacijo (razdelitev). Tip 0, tj. „drugo“, označuje minucijo, ki je ni moč jasno opredeliti kot enega od prej navedenih dveh tipov.

Tabela 6: Tipi minucij

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2 Položaj in tip minucije

Da bi bile predloge v skladu z delom 5 standarda ANSI INCITS 378-2004, se za določanje položaja (lokacija in kotni položaj) posamezne minucije uporablja naslednja metoda, ki nadgrajuje sedanji standard INCITS 378-2004.

▼ **B**

Položaj ali lokacija minucije, tj. zaključka grebena, je točka razvejanja osrednje osi (*medial skeleton*) doline, neposredno pred zaključkom grebena. Če se tri veje doline stanjšajo na osrednjo os v širini ene slikovne pike, se položaj minucije nahaja v točki preseka. Podobno je položaj minucije v primeru bifurkacije določen s točko razvejanja osrednje osi grebena. Če se vsaka izmed treh vej grebena stanjša na osrednjo os v širini ene slikovne pike, se položaj minucije nahaja v točki preseka treh vej.

Potem ko se vsi zaključki grebenov pretvorijo v bifurkacije, so vse minucije daktiloskopske podobe predstavljene kot bifurkacije. Koordinate slikovnih pik X in Y v preseku treh vej v vsaki minuciji se lahko neposredno formatirajo. Določitev smeri minucije se lahko razbere iz vsake bifurkacije osi. Preučiti se morajo tri veje v vsaki bifurkaciji osi; določiti se mora zaključna točka vsake izmed treh vej. Slika 6.1.2 prikazuje tri metode za ugotavljanje zaključka veje na podlagi ločljivosti skeniranja 500 ppi.

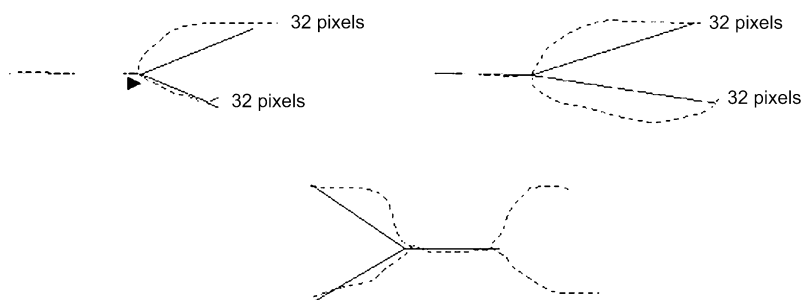
Zaključek se določi glede na to, kaj se zgodi najprej. Število slikovnih pik je določeno na podlagi ločljivosti skeniranja 500 ppi. Različne ločljivosti skeniranja bi pomenile različno število slikovnih pik.

— Razdalja .064“ (32. slikovna pika)

— Zaključek veje na razdalji .02“ in .064“ (10. do 32. slikovna pika); krajše veje se ne uporabljajo

— Do druge bifurkacije pride na razdalji .064“ (pred 32. slikovno piko)

Slika 6.1.2



Kotni položaj minucije se določi s pomočjo treh virtualnih žarkov, ki se raztezajo od točke bifurkacije do zaključka vsake veje. Smer minucij se določi z razpolovitvijo najmanjšega izmed treh kotov, ki jih ustvarijo žarki.

6.1.3 Koordinatni sistem

Za ponazarjanje minucij prstnih odtisov se uporablja kartezijski koordinatni sistem. Položaj minucij predstavljata njihovi koordinati x in y. Koordinatni sistem se začne v zgornjem levem kotu izvirne podobe; x se razteza proti desni strani, y pa navzdol. Koordinati minucij x in y sta prikazani v slikovnih pikah iz izvornika. Opozoriti je treba, da se položaj izvornika in merska enota ne skladata s konvencijo, ki se uporablja pri opredelitvi tipa 9 v ANSI/NIST-ITL 1-2000.

▼B

- 6.1.4 Smer minucij
- Koti so izraženi v standardni matematični obliki: kot 0 stopinj je na desni strani; koti naraščajo v nasprotni smeri urinega kazalca. Pri tipu zaključka grebena so zapisani koti usmerjeni nazaj vzdolž grebena, pri tipu bifurkacije pa kažejo proti središču doline. Ta konvencija je 180 stopinj nasprotna kotni konvenciji iz opredelitev tipa 9 v ANSI/NIST-ITL 1-2000.
- 6.2 Polja za format INCITS-378 logičnega zapisa tipa 9
- Vsa polja zapisa tipa 9 se zabeležijo kot besedilo ASCII. V tem zapisu označenega polja niso dopuščena binarna polja.
- 6.2.1 Polje 9.001: Dolžina logičnega zapisa (Logical record length – LEN)
- To obvezno polje v zapisu ASCII vsebuje dolžino logičnega zapisa, ki označuje skupno število bajtov, vključno z vsemi znaki vseh polj v zapisu.
- 6.2.2 Polje 9.002: Znak za označitev podobe (Image designation character – IDC)
- To obvezno dvobajtno polje se uporablja za prepoznavanje in lokacijo podatkov o minucijah. IDC iz tega polja se ujema z IDC iz polja vsebine datoteke zapisa tipa 1.
- 6.2.3 Polje 9.003: Tip odčitavanja (Impression type – IMP)
- V tem obveznem enobajtnem polju je opisan način pridobitve daktiloskopskih podatkov o podobi. Za označevanje tipa odčitavanja se v to polje vnese vrednost ASCII ustrezne kode, izbrane iz tabele 4.
- 6.2.4 Polje 9.004: Format minucij (Minutiæ format – FMT)
- „U“ v tem polju pomeni, da so minucije formatirane v obliki M1-378. Čeprav so podatki lahko zakodirani v skladu s standardom M1-378, morajo vsa podatkovna polja v zapisu tipa 9 ostati v besedilu ASCII.
- 6.2.5 Polje 9.126: Podatki CBEFF
- To polje vsebuje tri vrste podatkov. Prva vrsta podatkov vsebuje vrednost „27“ (0x1B). To je identifikacija lastnika formata CBEFF, ki ga je tehničnemu odboru INCITS M1 dodelilo mednarodno združenje biometrične industrije (*International Biometric Industry Association – IBIA*). Znak <US> loči to vrsto podatkov od formatnega tipa CBEFF, ki vsebuje vrednost „513“ (0x0201); s tem je označeno, da ta zapis vsebuje le podatke o lokaciji in kotnem položaju brez informacij o razširjenemu bloku podatkov (*Extended Data Block*). Znak <US> loči to vrsto podatkov od identifikatorja proizvoda CBEFF (*product identifier – PID*), ki identificira „lastnika“ opreme za kodiranje. To vrednost določi prodajalec. Če je objavljena, je navedena na spletnem mestu IBIA (www.ibia.org).
- 6.2.6 Polje 9.127: Identifikacija opreme za zajem podobe (Capture equipment identification)
- To polje vsebuje dve vrsti podatkov, ki sta ločeni z znakom <US>. Prva vrsta podatkov vsebuje vrednost „APPF“, če je oprema, ki je bila prvotno uporabljena pri pridobitvi podobe, prejela potrditev skladnosti z Dodatkom F (*IAFIS Image Quality Specification*, 29. januarja 1999) CJIS-RS-0010, tj. specifikacijami Zveznega preiskovalnega urada (FBI) za elektronski prenos prstnih odtisov. Če oprema ni skladna, vsebuje vrednost „NONE“. Druga vrsta podatkov vsebuje identifikacijo opreme za zajem podobe (*Capture Equipment ID*), ki je proizvodna številka opreme za zajem podobe, ki jo določi prodajalec. Vrednost „0“ označuje, da identifikacija opreme za zajem podobe ni prijavljena.

▼B**6.2.7 Polje 9.128: Dolžina horizontalne vrstice (Horizontal line length – HLL)**

To obvezno polje v zapisu ASCII vsebuje število slikovnih pik, ki so v eni horizontalni vrstici prenesene podobe. Največja horizontalna velikost je 65 534 slikovnih pik.

6.2.8 Polje 9.129: Dolžina vertikalne vrstice (Vertical line length – VLL)

To obvezno polje v zapisu ASCII vsebuje število horizontalnih vrstic iz prenesene podobe. Največja vertikalna velikost je 65 534 slikovnih pik.

6.2.9 Polje 9.130: Razmerje med enotami (Scale units – SLC)

To obvezno polje v zapisu ASCII označuje enote za opis frekvence odčitavanja podobe (gostota slikovnih pik). V tem polju „1“ označuje slikovne pike na palec, „2“ pa slikovne pike na centimeter. „0“ v tem polju pomeni, da ni podanega merila. V tem primeru se formalno razmerje slikovnih pik določi s kvocientom med HPS in VPS.

6.2.10 Polje 9.131: Razmerje horizontalnih slikovnih pik (Horizontal Pixel Scale – HPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v horizontalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja horizontalni del formalnega razmerja slikovnih pik.

6.2.11 Polje 9.132: Razmerje vertikalnih slikovnih pik (Vertical pixel scale – HPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v vertikalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja vertikalni del formalnega razmerja slikovnih pik.

6.2.12 Polje 9.133: Zorni kot prsta (Finger view)

To obvezno polje vsebuje številko zornega kota prsta, na katerega se nanašajo podatki iz tega zapisa. Številka zornega kota se začne z „0“ in postopoma narašča za 1 do „15“.

6.2.13 Polje 9.134: Položaj prsta (Finger position – FGP)

To polje vsebuje kodo, ki označuje položaj prsta, iz katerega izhajajo podatki v tem zapisu tipa 9. Za označevanje položaja prsta ali dlani se uporablja koda med 1 in 10 iz tabele 5 oziroma ustrezna koda dlani iz tabele 10.

6.2.14 Polje 9.135: Kakovost prstnega zapisa (Finger quality)

To polje vsebuje kakovost vseh podatkov o minucijah prsta; vrednost je med 0 in 100. Ta številka je splošen izraz kakovosti prstnega zapisa in predstavlja kakovost prvotne podobe in izvlečka minucije ter vse dodatne operacije, ki lahko vplivajo na zapis minucij.

6.2.15 Polje 9.136: Število minucij

To obvezno polje vsebuje število zabeleženih minucij v tem logičnem zapisu.

▼B**6.2.16 Polje 9.137: Podatki o minucijah prsta**

To obvezno polje vsebuje šest vrst podatkov, ki so ločeni z znakom <US>. Vsebuje več podpolj; v vsakem so navedene podrobnosti o eni minuciji. Skupno število podpolj, ki vsebujejo minucije, se mora skladati s številom iz polja 136. Prva vrsta podatkov je indeksna številka minucij, ki se označi z „1“ in se postopoma povečuje za „1“ za vsako dodatno minucijo v prstnem odtisu. Druga in tretja vrsta podatkov sta koordinati „x“ in „y“ minucij, izraženi v enotah slikovnih pik. Četrta vrsta podatkov je kot minucij, zapisan v enotah po dve stopinji. Ta vrednost ni negativna in je med 0 in 179. Peta vrsta podatkov je tip minucij. Vrednost „0“ se uporablja za minucijo tipa „OTHER“, vrednost „1“ za zaključek grebena in vrednost „2“ za bifurkacijo. Šesta vrsta podatkov je kakovost vsake minucije. Ta vrednost je v razponu od 1 – najmanjša do 100 – največja. Vrednost „0“ pomeni, da v zvezi s kakovostjo ni razpoložljive vrednosti. Podpolja so med sabo ločena z ločevalnim znakom <RS>.

6.2.17 Polje 9.138: Podatki o številu grebenov

To polje vsebuje niz podpolj; vsako izmed teh vsebuje tri vrste podatkov. Prva vrsta podatkov v prvem podpolju označuje metodo izločanja števila grebenov. Vrednost „0“ pomeni, da ni nobene predpostavke o metodi, uporabljeni za izločanje števila grebenov, niti o njihovem zaporedju v zapisu. Vrednost „1“ pomeni, da so za vse centralne minucije podatki o številu grebenov izločeni do najbližjih sosednjih minucij v štirih kvadrantih ter da so števila grebenov za vsako centralno minucijo navedena skupaj. Vrednost „2“ pomeni, da so za vse centralne minucije podatki o številu grebenov izločeni do najbližjih sosednjih minucij v osmih oktantih ter da so števila grebenov za vsako centralno minucijo navedena skupaj. Obe preostali vrsti podatkov v prvem podpolju vsebujeta „0“. Vrste podatkov so med seboj ločene z ločevalnim znakom <US>. Naslednja podpolja kot prvo vrsto podatkov vsebujejo indeksno številko centralnih minucij, indeksno številko sosednjih minucij kot drugo vrsto podatkov ter število prekrizanih grebenov kot tretjo vrsto podatkov. Podpolja so med seboj ločena z ločevalnim znakom <RS>.

6.2.18 Polje 9.139: Podatki o sredici

V tem polju je eno podpolje za vsako sredico („core“) iz prvotne podobe. V vsakem polju so tri vrste podatkov. Prvi dve vrsti podatkov vsebujeta koordinatna položaja „x“ in „y“ v enotah slikovnih pik. Tretja vrsta podatkov je kot sredice, zapisan v enotah po dve stopinji. Ta vrednost ni negativna in je med 0 in 179. Več sredič je med seboj ločeno z ločevalnim znakom <RS>.

6.2.19 Polje 9.140: Podatki o deltah

V tem polju je eno podpolje za vsako delto, ki se nahaja v prvotni podobi. V vsakem polju so tri vrste podatkov. Prvi dve vrsti podatkov vključujeta koordinatna položaja „x“ in „y“ v enotah slikovnih pik. Tretja vrsta podatkov je kot delte, zapisan v enotah po dve stopinji. Ta vrednost ni negativna in je med 0 in 179. Več sredič je med seboj ločeno z ločevalnim znakom <RS>.

▼B**7. Zapis podobe sledi tipa 13 različne ločljivosti**

Logični zapis označenega polja tipa 13 vsebuje podatke o podobi, pridobljene iz podob sledi. Te podobe so namenjene za prenos agencijam, ki iz njih avtomatično izločijo želene podatke o lastnostih, ali ki zagotovijo človeško posredovanje in obdelavo za pridobivanje teh podatkov.

Podatki o uporabljeni ločljivosti skeniranja, velikosti podobe in drugih parametrih, potrebnih za obdelavo podobe, so v zapisu zabeleženi kot označena polja.

Tabela 7: Razporeditev zapisa sledi tipa 13 različne ločljivosti

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 glede tipa znakov: N = numerični; A = abecedni; AN = alfanumerični; B = binarni

7.1 Polja logičnega zapisa tipa 13

V naslednjih odstavkih so opisani podatki, ki jih vsebujejo polja logičnega zapisa tipa 13.

V logičnem zapisu tipa 13 so vnosi zabeleženi v oštevilčenih poljih. Prvi dve polji zapisa morata biti urejeni, polje s podatki o podobi pa je zadnje fizično polje v zapisu. V tabeli 7 je za vsako polje zapisa tipa 13 navedena koda („condition code“), in sicer „M“ – obvezno ali „O“ – neobvezno; poleg tega so v tej tabeli navedeni še številka in ime polja, tip znakov, velikost polja in mejno število ponavljanj („occurrence limits“). Na podlagi trimestrne številke polja je v zadnjem stolpcu navedeno največje število bajtov. Največje število bajtov se veča skupaj z dodajanjem številčnih znakov številki polja. V vrednosti obeh vnosov, ki sta v stolpcu za „field size per occurrence“, so zajeti vsi ločevalni znaki v polju. Vrednost za „maximum byte count“ vključuje številko polja, podatke in vse ločevalne znake, vključno z znakom „GS“.

7.1.1 Polje 13.001: Dolžina logičnega zapisa (Logical record length – LEN)

To obvezno polje v zapisu ASCII vsebuje skupno število bajtov v logičnem zapisu tipa 13. Polje 13.001 označuje dolžino zapisa, vključno z vsakim znakom iz vsakega polja v zapisu ter ločevalnimi znaki med podatki.

7.1.2 Polje 13.002: Znak za označevanje podobe (Image designation character – IDC)

Obvezno polje v zapisu ASCII se uporablja za identifikacijo podatkov o podobi sledi iz zapisa. IDC iz tega polja se ujema z IDC iz polja vsebine datoteke (CNT) zapisa tipa 1.

7.1.3 Polje 13.003: Tip odčitavanja (Impression type – IMP)

To obvezno eno- ali dvobajtno polje v zapisu ASCII označuje način pridobitve podatkov o podobi sledi. V to polje se vnese ustrezna koda sledi iz tabele 4 (prst) ali tabele 9 (dlan).

7.1.4 Polje 13.004: Agencija izvora/ORI (SRC)

To obvezno polje v zapisu ASCII vsebuje identifikacijo uprave ali organizacije, ki je prva zajela podobo obraza iz zapisa. Običajno je v tem polju naveden identifikator agencije izvora (*Originating Agency Identifier – ORI*), ki je zajela podobo. Vsebuje dve vrsti podatkov v formatu: CC/agency.

▼B

Prva vrsta podatkov vsebuje Interpolovo kodo države v dolžini dveh alfanumeričnih znakov. Druga vrsta podatkov, tj. *agency*, je identifikacija agencije v obliki prostega besedila, v dolžini največ 32 alfanumeričnih znakov.

7.1.5 Polje 13.005: Datum zajema sledi (Latent capture date – LCD)

To obvezno polje v zapisu ASCII vsebuje datum zajema podobe sledi iz zapisa. Datum je naveden kot osem števk v obliki CCYYMMDD. Znaki CCYY predstavljajo leto zajema podobe. Znak MM sta vrednost v obliki desetih za enoto meseca; znak DD sta vrednost v obliki desetih za enoto dni v mesecu. Na primer, 20000229 pomeni 29. februar 2000. Popolni datum mora biti pravi datum.

7.1.6 Polje 13.006: Dolžina horizontalne vrstice (Horizontal line length – HLL)

To obvezno polje v zapisu ASCII vsebuje število slikovnih pik, ki so v eni horizontalni vrstici prenesene podobe.

7.1.7 Polje 13.007: Dolžina vertikalne vrstice (Vertical line length – VLL)

To obvezno polje v zapisu ASCII vsebuje število horizontalnih vrstic iz prenesene podobe.

7.1.8 Polje 13.008: Razmerje med enotami (Scale units – SLC)

To obvezno polje v zapisu ASCII označuje enote za opis frekvence odčitavanja podobe (gostota slikovnih pik). V tem polju „1“ označuje slikovne pike na palec, „2“ pa slikovne pike na centimeter. „0“ v tem polju pomeni, da ni podanega merila. V tem primeru se formalno razmerje slikovnih pik določi s kvocientom med HPS in VPS.

7.1.9 Polje 13.009: Razmerje horizontalnih slikovnih pik (Horizontal pixel scale – HPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v horizontalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja horizontalni del formalnega razmerja slikovnih pik.

7.1.10 Polje 13.010: Razmerje vertikalnih slikovnih pik (Vertical pixel scale – VPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v vertikalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja vertikalni del formalnega razmerja slikovnih pik.

7.1.11 Polje 13.011: Kompresijski algoritem (Compression algorithm – CGA)

To obvezno polje v zapisu ASCII označuje algoritem za stiskanje podob lestvice sivine. Za kompresijske kode glej Dodatek 7.

7.1.12 Polje 13.012: Biti na slikovno piko (Bits per pixel – BPX)

To obvezno polje v zapisu ASCII vsebuje število bitov, ki predstavljajo slikovno piko. Vsebuje vnos „8“ za običajne vrednosti na lestvici sivine od „0“ do „255“. Vnos, višji od „8“, predstavlja slikovno piko z lestvice sivine večje natančnosti.

▼B**7.1.13 Polje 13.013: Položaj prsta/dlani (Finger/palm position – FGP)**

To obvezno označeno polje vsebuje eno ali več možnih položajev prsta ali dlani, ki se lahko ujema s podobo sledi. Desetiška kodna številka, ki ustreza znanemu ali najbolj verjetnemu položaju prsta, se prevzame iz tabele 5, oziroma, če gre za ujemanje z najbolj verjetnim položajem dlani, iz tabele 10; vnese se kot eno- ali podpolje z dvema znakoma v zapisu ASCII. Nadomestni položaji prstov in/ali dlani se lahko označijo z vnosom drugih kod za položaje, in sicer kot podpolja, ločena z znakom „RS“. Za označitev vseh položajev prstov od ena do deset se uporabi koda „0“, tj. „neznani prst“. Za označitev vseh naštetih položajev odtisa dlani se uporabi koda „20“, tj. „neznana dlan“.

7.1.14 Polja 13.014–019: Rezervirano za prihodnje opredelitve (Reserved for future definition – RSV)

Ta polja so rezervirana za vključitev v prihodnje revizije tega standarda. Nobeno od teh polj se ne sme uporabiti v tej fazi revizije. Če se katero od teh polj pojavi, se ne sme upoštevati.

7.1.15 Polje 13.020: Opomba (Comment – COM)

To prostovoljno polje se lahko uporabi za vnos opomb ali drugih informacij v besedilu ASCII s podatki o podobi sledi.

7.1.16 Polja 13.021–199: Rezervirano za prihodnje opredelitve (Reserved for future definition – RSV).

Ta polja so rezervirana za vključitev v prihodnje revizije tega standarda. Nobeno od teh polj se ne sme uporabiti v tej fazi revizije. Če se katero od teh polj pojavi, se ne sme upoštevati.

7.1.17 Polja 13.200–998: Polja, ki jih opredelijo uporabniki (User-defined fields – UDF)

Ta polja lahko definirajo uporabniki; uporabljala se bodo za prihodnje potrebe. Njihova velikost in vsebina je v skladu z agencijo sprejema. Če se polje uporablja, vsebuje podatke v obliki besedila ASCII.

7.1.18 Polje 13.999: Podatki o podobi (Image data – DAT)

To polje vsebuje vse podatke iz zajete podobe sledi. To polje je vedno oštevilčeno z 999; mora biti zadnje fizično polje v zapisu. Na primer, številki „13.999“ sledijo podatki o podobi v binarni predstavitvi.

Vsaka slikovna pika nezgoščenih podatkov na lestvici sivine je ponavadi kvantizirana na osem bitov (256 ravni sivine), ki so zajeti v enem samem bajtu. Če je vnos v polju BPX 13.012 večji ali manjši od „8“, bo število bajtov, potrebnih za slikovno piko, drugačno. Pri kompresiji se podatki iz slikovnih pik stisnejo v skladu s tehniko stiskanja, ki je določeno v polju GCA.

7.2 Konec zapisa podobe sledi tipa 13 različne ločljivosti

Takoj za zadnjim bajtom podatkov iz polja 13.999 se zaradi doslednosti in ločevanja od naslednjega logičnega zapisa uporabi ločevalni znak „FS“. Ta ločevalni znak mora biti vključen v polje dolžine („length field“) zapisa tipa 13.

▼ B8. *Zapis podobe odtisa dlani tipa 15 različne ločljivosti*

Logični zapis označenega polja tipa 15 vsebuje podatke o podobi odtisa dlani in se uporablja za izmenjavo teh podatkov, skupaj z določenimi polji tekstovnih podatkov oziroma polji tekstovnih podatkov, ki jih opredelijo uporabniki, in ki se nanašajo na digitalizirano podobo. Podatki o uporabljeni ločljivosti skeniranja, velikosti podobe in drugih parametrih ali opombah, potrebnih za obdelavo podobe, so v zapisu zabeleženi kot označena polja. Agencije sprejema obdelajo podobe odtisa dlani, ki so prenesene drugim agencijam, zaradi pridobivanja želenih podatkov o lastnostih, potrebnih za primerjavo ujemanja.

Podatki o podobi se od subjekta pridobijo neposredno z uporabo čitalca „live-scan“ ali plošče za odtis dlani (*palmpoint card*) oziroma drugih medijev, ki vsebujejo odtise dlani subjekta.

Vsaka metoda za pridobivanje podob odtisa dlani mora biti zmožna zajeti niz podob za vsako roko. Ta niz vključuje del dlani, imenovan „*writer's palm*“ kot eno samo skenirano podobo ter celotno površino dlani od zapestja to konice prstov kot eno ali dve skenirani podobi. Če se za polno dlan uporabita dve podobi, spodnja pokriva površino od zapestja do vrha področja med prsti (tretji prstni sklep) ter vključuje področje tenarja in hipotenarja. Zgornja podoba pa sega od spodnjega dela področja med prsti do konic prstov. S tem je zagotovljena ustrezna mera prekrivanja dveh podob, saj obe pokrivata področje dlani med prsti. S primerjanjem ujemanja strukture grebenov in podrobnosti s tega skupnega področja lahko preučevalec z gotovostjo pritrди, da sta obe podobi povezani z isto dlanjo.

Ker se prenos odtisa dlani lahko uporabi za različne namene, lahko vsebuje eno ali več edinstvenih področij podobe dlani ali roke. Popolni zapis odtisa dlani posameznika običajno vsebuje del dlani, imenovan „*writer's palm*“, in podob(-e) celotne dlani obeh rok. Ker označeno polje logičnega zapisa podobe lahko vsebuje le eno binarno polje, je za vsak del dlani, imenovan „*writer's palm*“, potreben en sam zapis tipa 15, za vsako polno dlan pa sta potrebna eden ali dva zapisa tipa 15. Zato je za predstavitev odtisov dlani subjekta v običajnem prenosu odtisa dlani potrebnih štiri do šest zapisov tipa 15.

8.1 *Polja logičnega zapisa tipa 15*

V naslednjih odstavkih so opisani podatki, ki jih vsebujejo polja logičnega zapisa tipa 15.

V logičnem zapisu tipa 15 so vnosi zabeleženi v oštevilčenih poljih. Prvi dve polji zapisa morata biti urejeni, polje s podatki o podobi pa je zadnje fizično polje v zapisu. V tabeli 8 je za vsako polje zapisa tipa 15 navedena koda („*condition code*“), in sicer „M“ – obvezno ali „O“ – neobvezno; poleg tega so v tej tabeli navedeni še številka in ime polja, tip znakov, velikost polja in mejno število ponavljanj („*occurrence limits*“). Na podlagi trimestne številke polja je v zadnjem stolpcu navedeno največje število bajtov. Največje število bajtov se veča skupaj z dodajanjem številke k številki polja. V vrednosti obeh vnosov, ki sta v stolpcu za „*field size per occurrence*“, so zajeti vsi ločevalni znaki v polju. Vrednost za „*maximum byte count*“ vključuje številko polja, podatke in vse ločevalne znake, vključno z znakom „GS“.

▼B**8.1.1 Polje 15.001: Dolžina logičnega zapisa (Logical record length – LEN)**

To obvezno polje v zapisu ASCII vsebuje skupno število bajtov v logičnem zapisu tipa 15. Polje 15.001 označuje dolžino zapisa, vključno z vsakim znakom iz vsakega polja v zapisu ter ločevalnimi znaki med podatki.

8.1.2 Polje 15.002: Znak za označitev podobe (Image designation character – IDC)

To obvezno polje v zapisu ASCII se uporablja za identifikacijo podobe odtisa dlani iz zapisa. IDC iz tega polja se ujema z IDC iz polja vsebine datoteke (CNT) zapisa tipa 1.

8.1.3 Polje 15.003: Tip odčitavanja odtisa (Impression type – IMP)

V tem obveznem enobajtnem polju v zapisu ASCII je opisan način pridobitve podatkov o podobi odtisa dlani. V to polje se vnese ustrezna koda iz tabele 9.

8.1.4 Polje 15.004: Agencija izvora/ORI (SRC)

To obvezno polje v zapisu ASCII vsebuje identifikacijo uprave ali organizacije, ki je prva zajela podobo obraza iz zapisa. Običajno je v tem polju naveden identifikator agencije izvora (*Originating Agency Identifier* – ORI), ki je zajela podobo. Zajema dve vrsti podatkov v formatu: *CC/agency*.

Prva vrsta podatkov vsebuje Interpolovo kodo države v dolžini dveh alfanumeričnih znakov. Druga vrsta podatkov, tj. *agency*, je identifikacija agencije v obliki prostega besedila, v dolžini največ 32 alfanumeričnih znakov.

8.1.5 Polje 15.005: Datum zajema odtisa dlani (Palm-print capture date – PCD)

To obvezno polje v zapisu ASCII vsebuje datum zajema podobe odtisa dlani. Datum je naveden kot osem števk v obliki CCYYMMDD. Znaki CCYY predstavljajo leto zajema podobe. Znaka MM sta vrednost v obliki desetice na enoto meseca; znaka DD sta vrednost v obliki desetice na enoto dni v mesecu. Na primer, vnos 20000229 pomeni 29. februar 2000. Popolni datum mora biti pravi datum.

8.1.6 Polje 15.006: Dolžina horizontalne vrstice (Horizontal line length – HLL)

To obvezno polje v zapisu ASCII vsebuje število slikovnih pik, ki so v eni horizontalni vrstici prenesene podobe.

8.1.7 Polje 15.007: Dolžina vertikalne vrstice (Vertical line length – VLL)

To obvezno polje v zapisu ASCII vsebuje število horizontalnih vrstic iz prenesene podobe.

8.1.8 Polje 15.008: Razmerje med enotami (Scale units – SLC)

To obvezno polje v zapisu ASCII označuje enote za opis frekvenca odčitavanja podobe (gostota slikovnih pik). V tem polju „1“ označuje slikovne pike na palec, „2“ pa slikovne pike na centimeter. „0“ v tem polju pomeni, da ni podanega merila. V tem primeru se formalno razmerje slikovnih pik določi s kvocientom med HPS in VPS.

▼B

8.1.9 Polje 15.009: Razmerje horizontalnih slikovnih pik (Horizontal pixel scale – HPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v horizontalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja horizontalni del formalnega razmerja slikovnih pik.

8.1.10 Polje 15.010: Razmerje vertikalnih slikovnih pik (Vertical pixel scale – VPS)

To obvezno polje v zapisu ASCII označuje celo število gostote slikovnih pik v vertikalni smeri, če polje SLC vsebuje „1“ ali „2“. Drugače pa ponazarja vertikalni del formalnega razmerja slikovnih pik.

Tabela 8: Razporeditev zapisa odtisov dlani tipa 15 različne ločljivosti

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	—

Tabela 9: Tip odčitavanja dlani

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 Polje 15.011: Kompresijski algoritem (Compression algorithm – CGA)

To obvezno polje v zapisu ASCII označuje algoritem za stiskanje (kompresijo) podob lestvice sivine. Vnos „NONE“ v tem polju označuje, da podatki iz tega zapisa niso stisnjeni. Za podobe, ki bodo stisnjene, to polje vsebuje priporočeno metodo stiskanja podob odtisov desetih prstov. Veljavne kompresijske kode so opredeljene v Dodatku 7.

8.1.12 Polje 15.012: Biti na slikovno piko (Bits per pixel – BPX)

To obvezno polje v zapisu ASCII vsebuje število bitov, ki predstavljajo slikovno piko. To polje vsebuje vnos „8“ za običajne vrednosti lestvice sivine od „0“ do „255“. Vnos v tem polju, ki je večji ali manjši od „8“, predstavlja slikovno piko z lestvice sivine večje oziroma manjše natančnosti.

Tabela 10: Kode dlani, površina in velikosti

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 Polje 15.013: Položaj odtisa dlani (Palmprint position – PLP)

To obvezno označeno polje vsebuje položaj dlani, ki se ujema s podobo odtisa dlani. Desetiška kodna številka, ki ustreza znanemu ali najbolj verjetnemu položaju odtisa dlani, se prevzame iz tabele 10 in vnese kot podpolje z dvema znakoma v zapisu ASCII. V tabeli 10 so naštetje tudi največja površina podobe in dimenzije vseh možnih položajev odtisa dlani.

8.1.14 Polje 15.014–019: Rezervirano za prihodnje opredelitve (Reserved for future definition – RSV).

Ta polja so rezervirana za vključitev v prihodnje revizije tega standarda. Nobeno od teh polj se ne sme uporabiti v tej fazi revizije. Če se katero od teh polj pojavi, se ne sme upoštevati.

8.1.15 Polje 15.020: Opomba (Comment – COM)

To prostovoljno polje se lahko uporabi za vnos opomb ali drugih informacij v besedilu ASCII s podatki o podobi odtisa dlani.

8.1.16 Polje 15.021–199: Rezervirano za prihodnje opredelitve (Reserved for future definition – RSV).

Ta polja so rezervirana za vključitev v prihodnje revizije tega standarda. Nobeno od teh polj se ne sme uporabiti v tej fazi revizije. Če se katero od teh polj pojavi, se ne sme upoštevati.

8.1.17 Polja 15.200–998: Polja, ki jih opredelijo uporabniki (User-defined fields – UDF)

Ta polja lahko definirajo uporabniki; uporabljala se bodo za prihodnje potrebe. Njihova velikost in vsebina je v skladu z agencijo sprejema. Če je polje prisotno, vsebuje podatke v obliki besedila ASCII.

8.1.18 Polje 15.999: Podatki o podobi (Image data – DAT)

To polje vsebuje vse podatke iz zajete podobe odtisa dlani. Vedno je oštevilčeno z 999; mora biti zadnje fizično polje v zapisu. Na primer, številki „15.999“ sledijo podatki o podobi v binarni predstavitvi. Vsaka slikovna pika nezgoščenih podatkov na lestvici sivine je ponavadi kvantizirana na osem bitov (256 ravni sivine), ki so zajeti v enem samem bajtu. Če je vnos v polju BPX 15.012 večji ali manjši od „8“, bo število bajtov, ki so potrebni za slikovno piko, drugačno. Pri kompresiji se podatki iz slikovnih pik stisnejo v skladu s tehniko stiskanja, določeno v polju CGA.

▼ B**8.2** *Konec zapisa podobe odtisa dlani tipa 15 različne ločljivosti*

Takoj za zadnjim bajtom podatkov iz polja 15.999 se zaradi doslednosti in ločevanja od naslednjega logičnega zapisa uporabi ločevalni znak „FS“. Ta ločevalni znak mora biti vključen v polju dolžine zapisa tipa 15.

8.3 *Dodatni zapisi podobe odtisa dlani tipa 15 različne ločljivosti*

V datoteko se lahko vključijo dodatni zapisi tipa 15. Za vsako dodatno podobo odtisa dlani je potreben popolni logični zapis tipa 15 ter ločevalni znak „FS“.

Tabela 11: Največje število kandidatov, ki se lahko v okviru enega prenosa sprejme v preverjanje

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

Tipi iskanja:

TP/TP: primerjava odtisa desetih prstov z odtisom desetih prstov

TP/TP: primerjava sledi prstnega odtisa z odtisom desetih prstov

LP/PP: primerjava odtisa dlani z odtisom dlani

TP/UL: primerjava odtisa desetih prstov z nerazrešeno sledjo prstnega odtisa

LT/UL: primerjava sledi prstnega odtisa z nerazrešeno sledjo prstnega odtisa

PP/ULP: primerjava odtisa dlani z nerazrešeno sledjo odtisa dlani

LP/ULP: primerjava sledi odtisa dlani z nerazrešeno sledjo odtisa dlani

9. *Dodatki k poglavju 2 (Izmenjava daktiloskopskih podatkov)***9.1** *Dodatek 1: Ločilne kode 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⁾ To je položaj, kakor je opredeljen v standardu ASCII.

▼B9.2 *Dodatek 2: Izračun alfanumeričnega kontrolnega znaka*

Za TCN in TCR (poljai 1.09 in 1.10):

Številko, ki ustreza kontrolnemu znaku, dobimo z uporabo naslednje formule:

$$(YY * 10^8 + SSSSSSSS) \text{ Modul } 23$$

Pri čemer sta YY in SSSSSSSS numerični vrednosti zadnjih dveh števk leta in serijska številka.

Kontrolni znak dobimo iz spodnje konverzijske tabele.

Za CRO (polje 2.010)

Številko, ki ustreza kontrolnemu znaku, dobimo z uporabo naslednje formule:

$$(YY * 10^6 + NNNNNN) \text{ Modul } 23$$

Pri čemer sta YY in NNNNNN numerični vrednosti zadnjih dveh števk leta in serijska številka.

Kontrolni znak dobimo iz spodnje konverzijske tabele.

Konverzijska tabela za kontrolni znak

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 *Dodatek 3: Znakovne kode***7-bitna koda ANSI za izmenjavo informacij**

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

*Dodatek 4: Povzetek prenosa***Tip 1 Zapis (obvezen)**

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

V stolpcu Stanje:

O = neobvezno; M = obvezno; C = pogojno, če je prenos odgovor izvorni agenciji

Tip 2 Zapis (obvezen)

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	—	—

V stolpcu Stanje:

O = neobvezno; M = obvezno; C = pogojno, če so podatki na voljo

* = če je prenos podatkov v skladu z nacionalno zakonodajo (ni zajet v Sklepu 2008/615/PNZ)

9.5

Dodatek 5: Tip-1 Opredelitve zapisa

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

V stolpcu Stanje: O = neobvezno, M = obvezno, C = pogojno

V stolpcu Tip znaka: A = alfa, N = numerični, B = dvojiški

1* dovoljeni znaki za ime agencije so [„0..9“, „A..Z“, „a..z“, „_“, „“, „“, „-“]

9.6

Dodatek 6 Tip-2 Opredelitve zapisa

Tabela A.6.1: Prenos CPS in 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}

Tabela A.6.2: Prenos 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}

Tabela A.6.3: Prenos 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

Tabela A.6.4: Prenos MPS in 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}

V stolpcu Stanje: O = neobvezno, M = obvezno, C = pogojno

V stolpcu Tip znaka: A = alfa, N = numerični, B = dvojiški

1* dovoljeni znaki so [„0..9“, „A..Z“, „a..z“, „_“, „-“, „“ , „-“, „“]

9.7 *Dodatek 7: Kompresijske kode v lestvici sivine*

Kompresijske kode

Compression	Value	Remarks
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated December 19, 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 > 500dpi.
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 *Dodatek 8: Specifikacija elektronske pošte*

Zaradi izboljšave notranjega pretoka dela je treba v polje „zadeva“ v elektronski pošti za prenos PRUEM vnesti kodo države (CC) države članice, ki pošilja sporočilo in tip prenosa (polje TOT 1.004).

Oblika: CC/tip prenosa

Primer: „DE/CPS“

Vsebina elektronske pošte je lahko prazna.

▼B**POGLAVJE 3: Izmenjava podatkov o registraciji vozil****1. *Skupni niz podatkov za avtomatizirano iskanje podatkov o registraciji vozil*****1.1 *Opredelitve***

Opredelitve obveznih elementov podatkov in neobveznih elementov podatkov iz člena 16(4) so naslednje:

Obvezno (M):

Element podatka je treba sporočiti, ko so informacije na voljo v nacionalnem registru države članice. Zato je izmenjava informacij obvezna, ko so te na voljo.

Neobvezno (O):

Element podatka se lahko sporoči, ko so informacije na voljo v nacionalnem registru države članice. Zato izmenjava informacij ni obvezna, tudi ko so informacije na voljo.

Za vsak element v nizu podatkov, ki je posebej opredeljen kot pomemben glede na Sklep 2008/615/PNZ se navede oznaka (Y).

1.2 *Poizvedba o vozilu/lastniku/imetniku***1.2.1 *Sprožilci poizvedbe***

Obstajata dva različna načina iskanja informacij, ki sta opredeljena v naslednjem odstavku:

— po številki šasije (VIN), referenčnem datumu in času (neobvezno),

— po številki registrske tablice, številki šasije (VIN) (neobvezno), referenčnem datumu in času (neobvezno).

S pomočjo teh meril iskanja bodo posredovane informacije v zvezi z enim ali več vozili. Če je treba posredovati informacije o le enem vozilu, se vse informacije posredujejo v enem odgovoru. Če je najdeno več kot eno vozilo, lahko zaprosena država članica sama določi, katere informacije bo posredovala; vse elemente ali le elemente za izpopolnitev poizvedbe (npr. zaradi zasebnosti ali delovanja).

Elementi, ki so potrebni za izpopolnitev poizvedbe so navedeni v odstavku 1.2.2.1. V odstavku 1.2.2.2 je opisan celoten niz informacij.

Kadar se poizvedba opravlja po številki šasije, referenčnem datumu in času, se lahko opravi v eni ali vseh sodelujočih državah članicah.

Kadar se poizvedba opravlja po številki dovoljenja, referenčnem datumu in času, jo je treba opraviti v eni določeni državi članici.

Navadno se za poizvedbo uporabi dejanski datum in čas, poizvedbo pa je mogoče opraviti tudi s preteklim referenčnim datumom in časom. Kadar se opravi poizvedba s preteklim referenčnim datumom in časom in preteklih informacij ni na voljo v registru določene države članice, ker se take informacije sploh ne evidentirajo, se dejanske informacije lahko posredujejo z navedbo, da je informacija dejanska informacija.

▼B

1.2.2 Niz podatkov

1.2.2.1 Posredovane informacije, potrebne za izpolnitev poizvedbe

Item	M/O ⁽¹⁾	Opombe	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 etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

⁽¹⁾ M = obvezno, ko je na voljo v nacionalnem registru, O = neobvezno.

⁽²⁾ Vsi atributi, ki jih posebej dodelijo države članice, so označeni z Y.

⁽³⁾ Usklajena okrajšava dokumentov, glej Direktivo Sveta 1999/37/ES z dne 29. aprila 1999.

1.2.2.2 Celoten niz podatkov

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 etc., 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 etc., 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 etc.	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 etc.	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 etc.	Y



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 etc.	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 etc.	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 etc.	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 = obvezno, ko je na voljo v nacionalnem registru, O = neobvezno

⁽²⁾ Usklajena okrajšava dokumentov, glej Direktivo Sveta 1999/37/ES z dne 29. aprila 1999.

⁽³⁾ V Luksemburgu se uporabljata dva ločena identifikacijska dokumenta o registraciji vozil.

▼ B**2. Varnost podatkov****2.1 Pregled**

Programska aplikacija Eucaris omogoča varno sporočanje drugim državam članicam in z uporabo formata XML komunicira z obstoječimi sistemi v državah članicah. Države članice izmenjujejo sporočila, tako da jih neposredno pošljejo prejemniku. Podatkovni center države članice je povezan z omrežjem EU TESTA.

XML sporočila, ki se pošiljajo v omrežju, so šifrirana. Tehnika za šifriranje teh sporočil je SSL. Sporočila, poslana podpori, so sporočila XML v navadnem besedilu, saj povezava med aplikacijo in podporo poteka v zavarovanem okolju.

Zagotovljena je aplikacija odjemalca, ki se lahko uporabi v državi članici za poizvedbo v lastnem registru ali v registrih drugih držav članic. Odjemalci bodo identificirani s pomočjo uporabniškega imena/gesla ali certifikata odjemalca. Povezava do uporabnika je lahko šifrirana, vendar je to v pristojnosti vsake posamezne države članice.

2.2 Varnostne lastnosti, povezane z izmenjavo sporočil

Varnostni načrt temelji na kombinaciji HTTPS in XML podpisa. Pri tej možnosti se uporablja podpis XML za podpis vseh sporočil, poslanih na strežnik, tako da se pošiljatelja sporočila lahko potrdi s preverjanjem podpisa. 1-stranski SSL (le certifikat strežnika) se uporablja za zaščito zaupnosti in integritete sporočil, ki se prenašajo, in zagotavlja zaščito pred izbrisom/ponovnim predvajanjem in vstavljanjem. Namesto dogovorjenega razvoja programske opreme za izvedbo 2-stranskega SSL, se izvaja podpis XML. Uporaba podpisa XML je bližje načrtu spletnih storitev kot 2-stranski SSL in je zato bolj strateška.

Podpis XML se lahko izvede na več načinov, vendar je izbrani pristop uporaba podpisa XML, in sicer kot dela varnosti spletnih storitev (WSS). WSS določa, kako je treba uporabljati podpis XML. Ker WSS izhaja iz standarda SOAP, je logično, da se kolikor je mogoče držimo standarda SOAP.

2.3 Varnostne lastnosti, ki niso povezane z izmenjavo sporočil**2.3.1 Avtentifikacija uporabnikov**

Uporabniki spletne aplikacije Eucaris se potrdijo z uporabniškim imenom in geslom. Ker se uporablja standardna avtentifikacija za Windows, lahko države članice okrepijo raven avtentifikacije uporabnikov, če je to potrebno, in sicer z uporabo certifikatov strank.

2.3.2 Vloge uporabnikov

Programska aplikacija Eucaris podpira različne vloge uporabnikov. Vsak skupek storitev ima lastno pooblastilo. Npr. (izključni) uporabniki funkcionalnosti „Pogodbe Eucaris“ ne smejo uporabljati funkcionalnosti „Prüm“. Administratorske storitve so ločene od rednih vlog končnih uporabnikov.

▼B**2.3.3 Kontrolno beleženje in sledenje izmenjavi sporočil**

Kontrolno beleženje vseh tipov sporočil omogoča programska aplikacija Eucaris. Funkcija administratorja omogoča, da nacionalni administrator določi, katera sporočila se zabeležijo: zaprosila končnih uporabnikov, zaprosila, ki prihajajo iz drugih držav članic, informacije iz nacionalnih registrov, itd.

Aplikacija se lahko konfigurira tako, da se za to kontrolno beleženje uporabi notranja ali zunanja baza podatkov (Oracle). Odločitev o tem, katera sporočila je treba zabeležiti, je jasno odvisna od naprav za kontrolno beleženje drugje v podedovanih sistemih in povezanih aplikacijah ojemalcev.

Glava vsakega sporočila vsebuje informacije o državi članici prosilki, organizaciji prosilke v tej državi članici in zadevnem uporabniku. Naveden je tudi razlog zaprosila.

S pomočjo kombiniranega kontrolnega beleženja v državi članici prosilke in državi članici, ki odgovarja, je možno popolno sledenje vsem izmenjavam sporočil (npr. na zahtevo zadevnega državljana).

Kontrolno beleženje se konfigurira prek spletnega odjemalca v sistemu Eucaris (meni Administracija, Konfiguracija kontrolnega beleženja). Funkcionalnost kontrolnega beleženja opravlja centralni sistem. Ko je kontrolno beleženje omogočeno, se celotno sporočilo (glava in vsebina) shrani v en zapis. Stopnja kontrolnega beleženja se lahko določi glede na opredeljeno storitev in na tip sporočila, ki prihaja prek centralnega sistema.

Stopnje kontrolnega beleženja

Možne so naslednje stopnje kontrolnega beleženja:

zasebno – sporočilo je zabeleženo: kontrolno beleženje NI na voljo službi za pridobivanje kontrolnih beleženj, ampak je na voljo le na nacionalni ravni za revizije in reševanje problemov;

Nni – sporočilo sploh ni zabeleženo.

Tipi sporočil

Izmenjava informacij med državami članicami je sestavljena iz več sporočil, ki so shematsko prikazana na spodnji sliki.

Možni tipi sporočil (na sliki, prikazani za centralni sistem Eucaris države članice X) so:

1. zaprosilo centralnemu sistemu_sporočilo o zaprosilu odjemalca
2. zaprosilo drugi državi članici_sporočilo o zaprosilu centralnega sistema te države članice
3. zaprosilo centralnega sistema te države članice_sporočilo o zaprosilu centralnega sistema druge države članice
4. zaprosilo podedovanemu registru_sporočilo o zaprosilu centralnega sistema
5. zaprosilo centralnemu sistemu_sporočilo o zaprosilu podedovanega registra
6. odgovor centralnega sistema_sporočilo o zaprosilu odjemalca
7. odgovor druge države članice_sporočilo o zaprosilu centralnega sistema te države članice

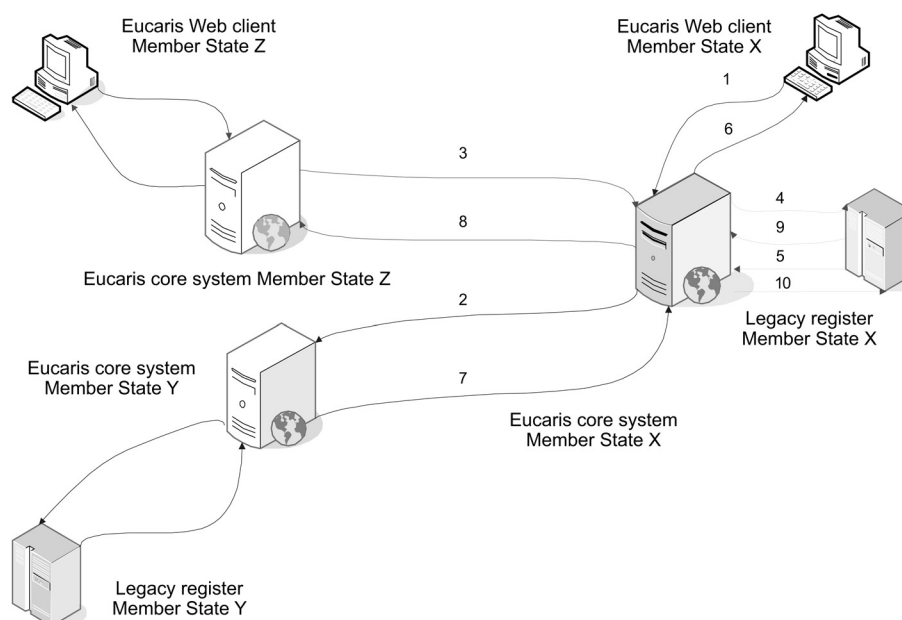
▼ B

8. odgovor centralnega sistema te države članice_sporočilo o zaprosilu druge države članice
9. odgovor podedovanega registra_sporočilo o zaprosilu centralnega sistema
10. odgovor centralnega sistema_sporočilo o zaprosilu podedovanega registra

Na sliki so prikazane naslednje izmenjave informacij:

- Zaposilo za informacijo s strani države članice X državi članici Y – modre puščice. To zaposilo in odgovor je sestavljeno iz tipov sporočil 1, 2, 7 in 6.
- Zaposilo za informacijo s strani države članice Z državi članici X – rdeče puščice. To zaposilo in odgovor je sestavljeno iz tipov sporočil 3, 4, 9 in 8.
- Zaposilo za informacijo s strani podedovanega registra njegovemu centralnemu sistemu (ta pot vključuje tudi zaposilo posameznega odjemalca za razpoložljivim registrom) – zelene puščice. Ta vrsta zaposila je sestavljena iz sporočil tipa 5 in 10.

Slika: Tipi sporočil za kontrolno beleženje



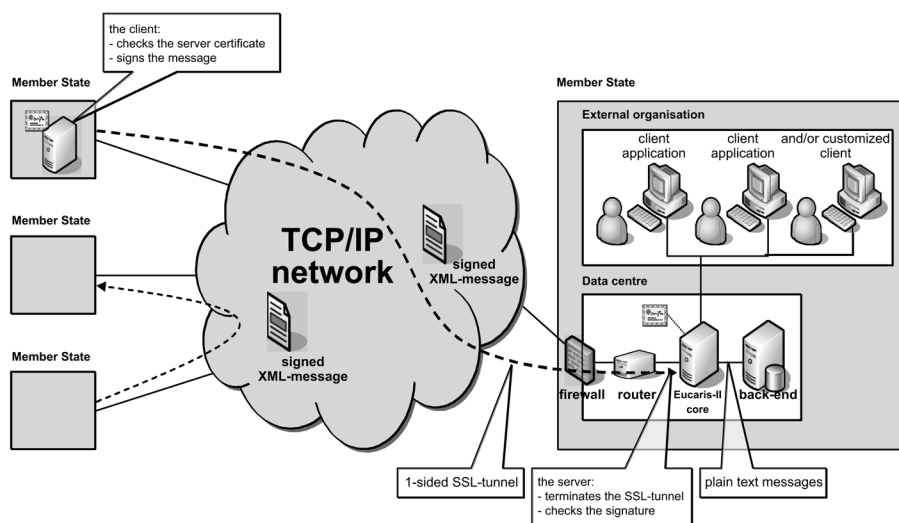
2.3.4 Varnostni modul strojne opreme

Varnostni modul strojne opreme se ne uporablja.

Varnostni modul strojne opreme (HSM) zagotavlja dobro zaščito za ključ, ki se uporablja za podpis sporočil in identifikacijo strežnikov. To dodatno prispeva k splošni ravni varnosti, vendar je HSM drag za nakup/vzdrževanje in ni nobenih zahtev za odločitev za FIPS 140-2 stopnja 2 ali stopnja 3 HSM. Ker se uporablja zaprto omrežje, ki učinkovito ublaži nevarnosti, je bilo odločeno, da se na začetku HSM ne bo uporabljal. Če bo HSM potreben za npr. pridobitev akreditacije, se lahko strukturi doda.

▼ **B**3. **Tehnični pogoji izmenjave podatkov**3.1 *Splošen opis aplikacije EUCARIS*3.1.1 **Pregled**

Aplikacija EUCARIS povezuje vse sodelujoče države članice v zankasto omrežje, v okviru katerega vsaka država članica z drugo državo članico komunicira neposredno. Za vzpostavitev komunikacije ni potrebna osrednja komponenta. Aplikacija Eucaris izvaja varno sporočanje drugim državam članicam in v formatu XML sporoča podpori podedovanim sistemom držav članic. Ta struktura je razvidna na naslednji sliki.



Država članica izmenjuje sporočila, tako da jih neposredno pošlje prejemniku. Podatkovni center države članice je povezan z omrežjem, ki se uporablja za izmenjavo podatkov (TESTA). Za dostop do omrežja TESTA, se države članice priključijo nanj prek nacionalnih portalov. Za povezavo na omrežje se uporablja požarni zid, usmerjevalnik pa povezuje aplikacijo Eucaris s požarnim zidom. Odvisno od možnosti, izbrane za zaščito sporočil, se uporablja certifikat z usmerjevalnikom ali aplikacijo Eucaris.

Zagotovljena je aplikacija odjemalca, ki se lahko uporabi v državi članici za poizvedbo v lastnem registru ali v registrih drugih držav članic. Aplikacija odjemalca se poveže na Eucaris. Odjemalci bodo identificirani s pomočjo uporabniškega imena/gesla ali certifikata stranke. Povezava do uporabnika v zunanji organizaciji (npr. policiji) je lahko šifrirana, vendar je to v pristojnosti vsake posamezne države članice.

3.1.2 **Področje uporabe sistema**

Področje uporabe sistema Eucaris je omejeno na postopke, vključene v izmenjavo informacij med organi, pristojnimi za registriranje vozil v državah članicah, in osnovno predstavitev teh informacij. Postopki in avtomatizirani procesi, v katerih se bodo informacije uporabljale, ne sodijo v področje uporabe sistema.

Države članice lahko uporabljajo funkcionalnost odjemalca v okviru sistema Eucaris ali pa vzpostavijo svoje prilagojene aplikacije odjemalca. V spodnji tabeli je opisano, kateri vidiki sistema Eucaris so obvezni in/ali predpisani in kateri so neobvezni za uporabo in/ali jih lahko države članice prosto določijo.

▼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 = obvezni za uporabo ali skladnost; O = neobvezni za uporabo ali skladnost.

3.2 *Funkcijske in nefunkcijske zahteve*

3.2.1 *Generična funkcionalnost*

V tem delu so na splošno opisane glavne generične funkcije.

Št.	Opis
1.	Sistem omogoča organom držav članic, pristojnim za registracije, interaktivno izmenjavo sporočil o zaprosilu in odgovoru.
2.	Sistem vsebuje aplikacijo odjemalca, ki omogoča končnemu uporabniku, da pošlje zaprosila in predstavi informacije v odgovoru za ročno obdelavo.
3.	Sistem omogoča „oddajanje“, kar omogoča državam članicam, da pošljejo zaprosilo vsem drugim državam članicam. Glavna aplikacija prihajajoče odgovore uskladi v eno sporočilo o odgovoru aplikaciji odjemalca (ta funkcionalnost se imenuje „poizvedba v več državah“).

▼ B

Št.	Opis
4.	Sistem lahko obravnava različne vrste sporočil. Vloge uporabnikov, pooblastila, usmerjanje, podpis in kontrolno beleženje so opredeljeni glede na posamezno storitev.
5.	Sistem omogoča državam članicam, da izmenjujejo svežnje sporočil ali sporočila, ki vsebujejo veliko število zaprosil ali odgovorov. Ta sporočila se obravnavajo na asinhron način.
6.	Sistem postavi v vrsto asinhrona sporočila, če je država članica prejemnica začasno nedosegljiva in zagotavlja dostavo, kakor hitro prejemnik spet deluje.
7.	Sistem shranjuje prihajajoča asinhrona sporočila, dokler se ne procesirajo.
8.	Sistem omogoča dostop le aplikacijam v okviru sistema Eucaris drugih držav članic, ne pa posameznim organizacijam v teh drugih državah članicah, tj., vsak organ, pristojen za registracijo, deluje kot edini portal med svojimi nacionalnimi končnimi uporabniki in ustreznimi organi v drugih državah članicah.
9.	Možno je opredeliti uporabnike različnih držav članic na enem strežniku Eucaris in jih pooblastiti glede na pravice navedene države članice.
10.	Informacije o državi članici prosilki, organizaciji in končnem uporabniku so vključene v sporočila.
11.	Sistem omogoča kontrolno beleženje izmenjave sporočil med različnimi državami članicami in med osnovno aplikacijo in nacionalnimi registracijskimi sistemi.
12.	Sistem omogoča posebnega sekretarja, ki je organizacija ali država članica, izrecno določena za nalogo, da zbira kontrolno zabeležene informacije o sporočilih, ki so jih vse sodelujoče države članice poslale/prejele, da se pripravijo statistična poročila.
13.	Vsaka država članica sama navede, katere kontrolno zabeležene informacije so dane na voljo sekretarju in katere informacije so „zasebne“.
14.	Sistem omogoča, da nacionalni administratorji vsake države članice pridobijo statistične podatke o uporabi.
15.	Sistem omogoča dodajanje novih držav članic s pomočjo enostavne administrativne naloge.

3.2.2

Uporabnost

Št.	Opis
16.	Sistem zagotavlja vmesnik za avtomatizirano procesiranje sporočil s strani podpore sistemom/podedovanih programov in omogoča integracijo uporabniškega vmesnika v navedene sisteme (prilagojeni uporabniški vmesnik).
17.	Sistem je lahko obvladljiv, sam po sebi razumljiv in vsebuje besedilo za pomoč.
18.	Sistem je dokumentiran za pomoč državam članicam pri integraciji, operativnih dejavnostih in prihodnjem vzdrževanju (npr. referenčni priročniki, funkcionalna/tehnična dokumentacija, operativne smernice ...).
19.	Uporabniški vmesnik je večjezičen in omogoča končnemu uporabniku, da izbere želen jezik.
20.	Uporabniški vmesnik omogoča, da lokalni administrator prevede točke na ekranu in kodirane informacije v nacionalni jezik.

▼B

3.2.3 Zanesljivost

Št.	Opis
21.	Sistem je oblikovan kot trden in zanesljiv operacijski sistem, ki je odporen na napake operaterja in ki se brez težav ponovno vzpostavi po izpadih elektrike ali drugih nesrečah. Sistem je mogoče ponovno zagnati brez ali z minimalno izgubo podatkov.
22.	Sistem mora dajati stabilne in ponovljive rezultate.
23.	Sistem je oblikovan za zanesljivo delovanje. Sistem je mogoče izvajati v konfiguraciji, ki zagotavlja razpoložljivost 98 % (z redundanco, uporabo sekundarnih strežnikov itd.) v vsaki dvostranski komunikaciji.
24.	Mogoče je uporabiti del sistema, celo med okvaro nekaterih komponent (če je država članica C pokvarjena, državi članici A in B še vedno lahko komunicirata). Čim bolj je treba zmanjšati okvaro posameznih točk sistema v informacijski verigi.
25.	Čas ponovne vzpostavitve sistema po hudi okvari naj bi bil manj kot en dan. Mogoče bi morale biti čim bolj zmanjšati čas pokvarjenosti z uporabo podpore na daljavo, npr. prek osrednjega centra za pomoč uporabnikom.

3.2.4 Delovanje

Št.	Opis
26.	Sistem se lahko uporablja 24 ur na dan, 7 dni na teden. Ta čas delovanja (24x7) se zahteva tudi od podedovanih sistemov držav članic.
27.	Sistem se hitro odziva na zahteve uporabnikov, ne glede na opravila v ozadju. To se zahteva tudi od podedovanih sistemov strank, da se zagotovi sprejemljiv odzivni čas. Sprejemljiv je splošni odzivni čas največ 10 sekund za eno zaprosilo.
28.	Sistem je oblikovan kot večuporabniški, in sicer tako, da se opravila v ozadju lahko nadaljujejo, medtem ko uporabnik opravlja opravila v ospredju.
29.	Sistem je oblikovan tako, da je nadgradljiv zaradi podpore morebitnega povečanja števila sporočil, ko se doda nova funkcionalnost ali nove organizacije ali države članice.

3.2.5 Varnost

Št.	Opis
30.	Sistem je primeren za (npr. glede varnostnih ukrepov) izmenjavo sporočil z občutljivimi zasebnimi podatki (npr. lastniki/imetniki avtomobila), opredeljenimi kot EU interno.
31.	Sistem se vzdržuje na tak način, da se prepreči nepooblaščen dostop do podatkov.
32.	Sistem vsebuje službo za upravljanje pravic in dovoljenj nacionalnih končnih uporabnikov.
33.	Države članice lahko preverijo identiteto pošiljatelja (na ravni države članice) s pomočjo podpisa XML.

▼B

Št.	Opis
34.	Države članice morajo za zahtevo posebnih informacij izrecno pooblastiti druge države članice.
35.	Sistem na ravni vloge zagotavlja popolno politiko varnosti in šifriranja, združljivo s stopnjo varnosti, ki se zahteva v takih razmerah. Ekskluzivnost in integriteta informacij je zagotovljena z uporabo podpisa XML in šifriranja s pomočjo tuneliranja SSL.
36.	Celotni izmenjavi sporočil se lahko sledi s pomočjo kontrolnega beleženja.
37.	Zagotovljena je zaščita pred izbrisom (tretja oseba izbriše sporočilo) in ponovnim predvajanjem ali vstavljanjem (tretja oseba ponovno predvaja ali vstavi sporočilo).
38.	Sistem uporablja certifikate zaupanja vredne tretje osebe (<i>Trusted Third Party</i> (TTP)).
39.	Sistem lahko obravnava različne certifikate na državo članico, odvisno od tipa sporočila ali storitve.
40.	Varnostni ukrepi na ravni vloge so zadostni, da omogočajo uporabo neakreditiranih omrežij.
41.	Sistem lahko uporablja nove varnostne tehnike, kot je požarni zid XML.

3.2.6 Prilagodljivost

Št.	Opis
42.	Sistem je mogoče razširiti z novimi sporočili in novo funkcionalnostjo. Stroški prilagoditev so minimalni. Zaradi centraliziranega razvoja komponent aplikacije.
43.	Države članice lahko opredelijo nove vrste sporočil za dvostransko uporabo. Ni potrebno, da vse države članice podpirajo vse vrste sporočil.

3.2.7 Podpora in vzdrževanje

Št.	Opis
44.	Sistem zagotavlja možnost spremljanja za osrednji center za pomoč uporabnikom in/ali operaterje za mrežo in strežnike v različnih državah članicah.
45.	Sistem zagotavlja daljinsko podporo osrednjega centra za pomoč uporabnikom.
46.	Sistem zagotavlja možnost analize problemov.
47.	Sistem se lahko razširi na nove države članice.
48.	Aplikacijo zlahka namesti osebje z minimalno usposobljenostjo na področju IT in z minimalnimi izkušnjami. Postopek instalacije je čim bolj avtomatiziran.
49.	Sistem zagotavlja stalno testno in sprejemno okolje.
50.	Letni stroški vzdrževanja in podpore so bili v veliki meri zmanjšani z izpolnjevanjem tržnih standardov in z oblikovanjem aplikacije na tak način, da je potrebno čim manj podpore osrednjega centra za pomoč uporabnikom.

▼B

3.2.8 Oblikovne zahteve

Št.	Opis
51.	Sistem je oblikovan in dokumentiran za operativno dobo več let.
52.	Sistem je oblikovan tako, da je neodvisen od ponudnika dostopa do omrežja.
53.	Sistem je v skladu z obstoječimi HW/SW v državah članicah tako, da vzajemno deluje s tistimi registracijskimi sistemi, ki uporabljajo odprto standardno tehnologijo spletne storitve (XML, XSD, SOAP, WSDL, HTTP(s), spletne storitve, WSS, X.509 itd.).

3.2.9 Veljavni standardi

Št.	Opis
54.	Sistem je skladen z elementi varstva podatkov iz Uredbe (ES) št. 45/2001 (členi 21, 22 in 23) in Direktive 95/46/ES.
55.	Sistem je skladen s standardi IDA.
56.	Sistem podpira UTF8.

POGLAVJE 4: Ocenjevanje

1. *Postopek ocenjevanja v skladu s členom 20 (Priprava sklepov v skladu s členom 25(2) Sklepa 2008/615/PNZ)*1.1 *Vprašalnik*

Ustrezna delovna skupina Sveta pripravi vprašalnik o vsaki avtomatizirani izmenjavi podatkov, kakor je določeno v poglavju 2 Sklepa 2008/615/PNZ.

Takoj ko država članica meni, da izpolnjuje predpogoje za delitev podatkov v ustrezni kategoriji podatkov, izpolni ustrezni vprašalnik.

1.2 *Preskus*

Z namenom ocene rezultatov vprašalnika, država članica, ki želi začeti deliti podatke, opravi preskus skupaj z eno ali več drugimi državami članicami, ki si v skladu s Sklepom Sveta podatke že delijo. Preskus se opravi tik pred ali takoj po ocenjevalnem obisku.

Pogoje in ureditev za ta preskus bo opredelila ustrezna delovna skupina Sveta in bodo temeljili na predhodnem posameznem sporazumu z zadevno državo članico. Države članice, ki sodelujejo pri preskusu, bodo določile praktične podrobnosti.

1.3 *Ocenjevalni obisk*

Zaradi ocene rezultatov vprašalnika, se opravi ocenjevalni obisk v državi članici, ki želi začeti deliti podatke.

Pogoje in ureditev za ta obisk bo opredelila ustrezna delovna skupina Sveta in bodo temeljili na predhodnem posameznem sporazumu med zadevno državo članico in ocenjevalno skupino. Zadevna država članica bo omogočila ocenjevalni skupini, da preveri avtomatizirano izmenjavo podatkov v kategoriji ali kategorijah podatkov, ki se ocenjuje, zlasti z organizacijo programa obiska, ki bo upošteval zahteve ocenjevalne skupine.

▼ B

Ocenjevalna skupina bo v roku enega meseca pripravila poročilo o ocenjevalnem obisku in ga bo poslala zadevni državi članici za pripombe. Po potrebi bo ocenjevalna skupina to poročilo revidirala na podlagi pripomb države članice.

Ocenjevalno skupino bodo sestavljali največ trije strokovnjaki, ki jih imenujejo države članice, ki sodelujejo v avtomatizirani izmenjavi podatkov v kategorijah podatkov, ki se ocenjujejo, imajo izkušnje v zvezi z zadevno kategorijo podatkov, so ustrezno nacionalno varnostno preverjeni za obravnavanje takih zadev in so pripravljeni sodelovati pri vsaj enem ocenjevalnem obisku v drugi državi članici. Komisija bo v ocenjevalni skupini sodelovala kot opazovalka.

Člani ocenjevalne skupine bodo spoštovali zaupno naravo informacij, ki jih bodo pridobili pri opravljanju svoje naloge.

1.4 *Poročanje Svetu*

Celovito poročilo o oceni, v katerem bodo povzeti rezultati vprašalnikov, ocenjevalnega obiska in preskusa, bo predloženo Svetu v odločanje na podlagi člena 25(2) Sklepa 2008/615/PNZ.

2. ***Ocenjevalni postopek v skladu s členom 21***2.1 *Statistični podatki in poročilo*

Vsaka država članica zbere statistične podatke o rezultatih avtomatizirane izmenjave podatkov. Da se zagotovi primerljivost, bo zadevna delovna skupina Sveta pripravila vzorec za statistične podatke.

Ti statistični podatki se bodo vsako leto pošiljali generalnemu sekretariatu, ki bo pripravil povzetek pregleda preteklega leta, in Komisiji.

Poleg tega bodo države članice redno zaprosene, da nadaljnjih informacij o administrativnem, tehničnem in finančnem izvajanju avtomatizirane izmenjave podatkov, kakor je potrebno za analizo in izboljšanje procesa, ne pošiljajo več kot enkrat na leto. Na podlagi teh informacij bo za Svet pripravljeno poročilo.

2.2 *Revizija*

Svet bo v razumnem času preučil tu opisani mehanizem ocenjevanja in ga bo po potrebi spremenil.

3. ***Sestanki strokovnjakov***

Strokovnjaki se bodo v okviru ustrezne delovne skupine Sveta redno sestajali za organizacijo in izvajanje navedenih ocenjevalnih postopkov ter si delili izkušnje in razpravljali o morebitnih izboljšavah. Kjer bo ustrezno, se bodo rezultati teh strokovnih razprav vključili v poročilo, navedeno v točki 2.1.