

## ROZHODNUTIE RADY 2008/616/SVV

z 23. júna 2008

**o vykonávaní rozhodnutia 2008/615/SVV o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti**

RADA EURÓPSKEJ ÚNIE,

prostredníctvom jediného vyhľadávania, pričom vhodné riešenia takéhoto postupu sa nájdu na technickej úrovni,

so zreteľom na článok 33 rozhodnutia Rady 2008/615/SVV <sup>(1)</sup>,

ROZHODLA TAKTO:

so zreteľom na podnet Spolkovej republiky Nemecko,

## KAPITOLA I

so zreteľom na stanovisko Európskeho parlamentu <sup>(2)</sup>,

## VŠEOBECNÉ USTANOVENIA

keďže:

## Článok 1

## Cieľ

(1) Rada 23. júna 2008 prijala rozhodnutie 2008/615/SVV o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti.

Cieľom tohto rozhodnutia je ustanoviť administratívne a technické predpisy potrebné na vykonávanie rozhodnutia 2008/615/SVV, najmä na automatizovanú výmenu údajov o DNA, daktyloskopických údajov a údajov z evidencie vozidiel, ako sa uvádzajú v jeho kapitole 2, ako aj na ďalšie formy spolupráce uvedené v jeho kapitole 5.

(2) Prostredníctvom rozhodnutia 2008/615/SVV sa základné prvky Zmluvy z 27. mája 2005 medzi Belgickým kráľovstvom, Spolkovou republikou Nemecko, Španielskym kráľovstvom, Francúzskou republikou, Luxemburským veľkoveľkostvom, Holandským kráľovstvom a Rakúskou republikou o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu, cezhraničnej trestnej činnosti a nelegálnej migrácii (ďalej len „Prümská zmluva“) transponovali do právneho rámca Európskej únie.

## Článok 2

## Vymedzenie pojmov

Na účely tohto rozhodnutia:

(3) V článku 33 rozhodnutia 2008/615/SVV sa ustanovuje, že Rada má prijať opatrenia potrebné na vykonávanie rozhodnutia 2008/615/SVV na úrovni Únie v súlade s postupom ustanoveným v článku 34 ods. 2 písm. c) druhej vete Zmluvy o Európskej únii. Tieto opatrenia sa majú zakladať na vykonávacej dohode z 5. decembra 2006 týkajúcej sa administratívneho a technického vykonávania a uplatňovania Prümskej zmluvy.

a) „vyhľadávanie“ a „porovnávanie“ uvedené v článkoch 3, 4 a 9 rozhodnutia 2008/615/SVV sú postupy, ktorými sa určuje, či existuje zhoda medzi údajmi o DNA, resp. daktyloskopickými údajmi oznámenými jedným členským štátom, a údajmi o DNA, resp. daktyloskopickými údajmi uchovávanými v databázach jedného, niekoľkých alebo všetkých členských štátov;

(4) Týmto rozhodnutím sa zavádzajú tie spoločné normatívne ustanovenia, ktoré sú nevyhnutné na administratívne a technické vykonávanie foriem spolupráce uvedených v rozhodnutí 2008/615/SVV. Príloha k tomuto rozhodnutiu obsahuje vykonávacie ustanovenia technického charakteru. Okrem toho sa vypracuje samostatná príručka obsahujúca výlučne skutkové informácie, ktoré majú poskytnúť členské štáty, pričom jej aktualizáciu bude zabezpečovať Generálny sekretariát Rady.

b) „automatizované vyhľadávanie“ uvedené v článku 12 rozhodnutia 2008/615/SVV je postup umožňujúci prístup online na prehľadávanie databázy jedného, niekoľkých alebo všetkých členských štátov;

(5) Vzhľadom na technické možnosti sa bežné vyhľadávanie nových profilov DNA bude v zásade vykonávať

c) „profil DNA“ je písmenový alebo číselný kód, ktoré predstavujú súbor identifikačných vlastností nekódujúcej časti analyzovanej ľudskej vzorky DNA, t. j. konkrétnej molekulárnej štruktúry na rôznych miestach DNA (loci);

d) „nekódujúca časť DNA“ znamená chromozómové časti, ktoré sa geneticky neprejavujú, t. j. o ktorých nie je známe, že by zabezpečovali akékoľvek funkčné vlastnosti organizmu;

<sup>(1)</sup> Pozri stranu 1 tohto úradného vestníka.

<sup>(2)</sup> Stanovisko z 21. apríla 2008 (zatiaľ neuverejnené v úradnom vestníku).

- e) „referenčné údaje o DNA“ sú profil DNA a referenčné číslo;
- f) „referenčný profil DNA“ je profil DNA identifikovanej osoby;
- g) „neidentifikovaný profil DNA“ je profil DNA získaný zo stôp zozbieraných počas vyšetrovania trestných činov a patriacich zatiaľ neidentifikovanej osobe;
- h) „záznam“ je poznámka, ktorú urobí členský štát v profile DNA vo svojej národnej databáze a v ktorej uvedie, že pri vyhľadávaní alebo porovnávaní iným členským štátom bola v minulosti zistená zhoda tohto profilu DNA;
- i) „daktyloskopické údaje“ sú zobrazenia odtlačkov prstov, zobrazenia skrytých odtlačkov prstov, odtlačkov dlaní, skrytých odtlačkov dlaní, ako aj vzory takýchto zobrazení (kódované podrobnosti), keď sa uchovávajú a spracúvajú v automatizovanej databáze;
- j) „údaje z evidencie vozidla“ znamenajú súbor údajov, ako sa vymedzuje v kapitole 3 prílohy k tomuto rozhodnutiu;
- k) „jednotlivý prípad“ uvedený v článku 3 ods. 1 druhej vete, v článku 9 ods. 1 druhej vete a v článku 12 ods. 1 rozhodnutia 2008/615/SVV je jedno vyšetrovanie alebo jeden vyšetrovací spis. Ak takýto spis obsahuje viac ako jeden profil DNA alebo jeden daktyloskopický údaj alebo údaj z evidencie vozidiel, môžu sa zasielať spolu ako jedna žiadosť.

## KAPITOLA 2

### SPOLOČNÉ USTANOVENIA PRE VÝMENU ÚDAJOV

#### Článok 3

##### Technické špecifikácie

Členské štáty dodržiavajú spoločné technické špecifikácie v súvislosti so všetkými žiadosťami a odpoveďami týkajúcimi sa vyhľadávania a porovnávania profilov DNA, daktyloskopických údajov a údajov z evidencie vozidiel. Tieto technické špecifikácie sa ustanovujú v prílohe k tomuto rozhodnutiu.

#### Článok 4

##### Komunikačná sieť

Elektronická výmena údajov o DNA, daktyloskopických údajov a údajov z evidencie vozidiel medzi členskými štátmi sa uskutočňuje prostredníctvom transeurópskej komunikačnej siete telematických služieb medzi orgánmi štátnej správy (TESTA II) a jej ďalších vylepšení.

#### Článok 5

##### Dostupnosť automatizovanej výmeny údajov

Členské štáty prijímajú všetky opatrenia potrebné na zabezpečenie toho, aby automatizované vyhľadávanie alebo porovnávanie údajov o DNA, daktyloskopických údajov a údajov z evidencie vozidiel bolo možné 24 hodín denne a sedem dní v týždni. V prípade technickej poruchy sa národné kontaktné body členských štátov ihneď navzájom informujú a dohodnú sa na dočasných alternatívnych opatreniach pre výmenu informácií v súlade s uplatniteľnými právnymi ustanoveniami. Automatizovaná výmena údajov sa obnoví čo najskôr.

#### Článok 6

##### Referenčné čísla údajov o DNA a daktyloskopických údajov

Referenčné čísla uvedené v článku 2 a v článku 8 rozhodnutia 2008/615/SVV sa skladajú z kombinácie týchto kódov:

- a) kód umožňujúci členským štátom v prípade zhody vyhľadávať vo svojich databázach osobné údaje a iné informácie s cieľom poskytnúť ich jednému, niekoľkým alebo všetkým členským štátom v súlade s článkom 5 alebo článkom 10 rozhodnutia 2008/615/SVV;
- b) kód uvádzajúci národný pôvod profilu DNA alebo daktyloskopických údajov a
- c) vo vzťahu k údajom o DNA kód označujúci druh profilu DNA.

## KAPITOLA 3

### ÚDAJE O DNA

#### Článok 7

##### Zásady výmeny údajov o DNA

- Členské štáty využívajú pre výmenu údajov o DNA existujúce normy, ako napríklad európsky štandardný súbor (ESS) alebo štandardný súbor miest DNA, ktorý používa Interpol (ISSOL).
- Postup zasielania sa v prípade automatizovaného vyhľadávania alebo porovnávania profilov DNA uskutočňuje v rámci decentralizovanej štruktúry.
- Prijímajú sa primerané opatrenia na zabezpečenie dôvernosti a integrity údajov vrátane ich kódovania pri zasielaní iným členským štátom.
- Členské štáty prijímajú opatrenia potrebné na zabezpečenie integrity profilov DNA poskytnutých alebo zaslaných na porovnávanie iným členským štátom a na zabezpečenie, aby tieto opatrenia spĺňali medzinárodné normy, ako napríklad ISO 17025.

5. Členské štáty používajú kódy členských štátov v súlade s normou ISO 3166-1 alpha-2.

#### Článok 8

##### Pravidlá pre žiadosti a odpovede v súvislosti s údajmi o DNA

1. Žiadosť o automatizované vyhľadávanie alebo porovnávanie, ako sa uvádza v článkoch 3 alebo 4 rozhodnutia 2008/615/SVV, obsahuje len tieto informácie:

- a) kód členského štátu pre žiadajúci členský štát;
- b) dátum, čas a identifikačné číslo žiadosti;
- c) profily DNA a ich referenčné čísla;
- d) druhy zasielaných profilov DNA (neidentifikované profily DNA alebo referenčné profily DNA) a
- e) informácie požadované na kontrolu systémov databáz a kontrolu kvality pre procesy automatizovaného vyhľadávania.

2. Odpoveď (hlásenie o zhode) na žiadosť uvedenú v odseku 1 obsahuje len tieto informácie:

- a) uvedenie o tom, či sa zistila jedna alebo viacero zhôd (pozitívna lustrácia) alebo žiadna zhoda (negatívna lustrácia);
- b) dátum, čas a identifikačné číslo žiadosti;
- c) dátum, čas a identifikačné číslo odpovede;
- d) kódy žiadajúceho a dožiadaného členského štátu;
- e) referenčné čísla žiadajúceho a dožiadaného členského štátu;
- f) druh zasielaných profilov DNA (neidentifikované profily DNA alebo referenčné profily DNA);
- g) dožiadané a zhodné profily DNA a
- h) informácie požadované na kontrolu systémov databáz a kontrolu kvality pre procesy automatizovaného vyhľadávania.

3. Automatizované oznámenie o zhode sa poskytne, iba ak sa automatizovaným vyhľadávaním alebo porovnávaním zistila zhoda v minimálnom počte miest. Tento minimálny počet sa uvádza v kapitole 1 prílohy k tomuto rozhodnutiu.

4. Členské štáty zabezpečia súlad žiadostí s vyhláseniami vydanými podľa článku 2 ods. 3 rozhodnutia 2008/615/SVV. Tieto vyhlásenia budú súčasťou príručky uvedenej v článku 18 ods. 2 tohto rozhodnutia.

#### Článok 9

##### Postup zasielania pre automatizované vyhľadávanie neidentifikovaných profilov DNA v súlade s článkom 3 rozhodnutia 2008/615/SVV

1. Ak sa pri vyhľadávaní podľa neidentifikovaného profilu DNA nezistí v národnej databáze žiadna zhoda alebo sa zistí zhoda podľa neidentifikovaného profilu DNA, neidentifikovaný profil DNA sa môže následne zaslať do databáz všetkých ostatných členských štátov, a ak sa pri vyhľadávaní podľa tohto neidentifikovaného profilu DNA zistia v databázach iných členských štátov zhody s referenčnými profilmi DNA a/alebo neidentifikovanými profilmi DNA, automaticky sa tieto zhody oznámia žiadajúcemu členskému štátu a zašlú sa mu referenčné údaje o DNA. Ak sa v databázach iných členských štátov nezistila žiadna zhoda, táto skutočnosť sa automaticky oznámi žiadajúcemu členskému štátu.

2. Ak sa pri vyhľadávaní podľa neidentifikovaného profilu DNA zistila zhoda v databázach iných členských štátov, môže každý dotknutý členský štát na tento účel vložiť záznam do svojej národnej databázy.

#### Článok 10

##### Postup zasielania pre automatizované vyhľadávanie referenčných profilov DNA v súlade s článkom 3 rozhodnutia 2008/615/SVV

Ak sa pri vyhľadávaní podľa referenčného profilu DNA v národnej databáze nezistila žiadna zhoda s referenčným profilom DNA alebo sa zistila zhoda s neidentifikovaným profilom DNA, tento referenčný profil DNA sa môže následne zaslať do databáz všetkých ostatných členských štátov; ak sa pri vyhľadávaní podľa tohto referenčného profilu DNA zistila zhoda s referenčnými profilmi DNA a/alebo neidentifikovanými profilmi DNA v databázach iných členských štátov, zistené zhody sa automaticky oznámia žiadajúcemu členskému štátu a zašlú sa mu referenčné údaje o DNA; a ak sa v databázach iných členských štátov nezistila žiadna zhoda, automaticky sa to oznámi žiadajúcemu členskému štátu.

#### Článok 11

##### Postup zasielania pre automatizované porovnávanie neidentifikovaných profilov DNA v súlade s článkom 4 rozhodnutia 2008/615/SVV

1. Ak sa pri porovnávaní podľa neidentifikovaných profilov DNA v databázach iných členských štátov zistí zhoda s referenčnými profilmi DNA a/alebo inými neidentifikovanými profilmi DNA, táto zhoda sa automaticky oznámi žiadajúcemu členskému štátu a zašlú sa mu referenčné údaje o DNA.

2. Ak sa pri porovnávaní podľa neidentifikovaných profilov DNA zistí zhoda s neidentifikovanými profilmi DNA v databázach iných členských štátov alebo referenčnými profilmi DNA, každý dotknutý členský štát môže do svojej národnej databázy na tento účel vložiť záznam.

#### KAPITOLA 4

### DAKTYLOSKOPICKÉ ÚDAJE

#### Článok 12

#### Zásady výmeny daktyloskopických údajov

1. Digitalizácia daktyloskopických údajov a ich zasielanie iným členským štátom sa vykonáva v súlade s jednotným formátom údajov uvedeným v kapitole 2 prílohy k tomuto rozhodnutiu.
2. Každý členský štát zabezpečí, aby daktyloskopické údaje, ktoré zasiela, mali dostatočnú kvalitu pre porovnávanie automatizovaným systémom identifikácie odtlačkov prstov (AFIS).
3. Postup zasielania pri výmene daktyloskopických údajov sa uskutočňuje v rámci decentralizovanej štruktúry.
4. Prijmú sa primerané opatrenia na zabezpečenie dôvernosti a integrity daktyloskopických údajov vrátane ich kódovania pri zasielaní iným členským štátom.
5. Členské štáty používajú kódy členských štátov v súlade s normou ISO 3166-1 alpha-2.

#### Článok 13

#### Kapacity na vyhľadávanie daktyloskopických údajov

1. Každý členský štát zabezpečí, aby jeho žiadosti o vyhľadávanie neprekročili vyhľadávacie kapacity vymedzené dožiadaným členským štátom. Členské štáty predložia Generálnemu sekretariátu Rady vyhlásenia uvedené v článku 18 ods. 2, v ktorých stanovujú svoje maximálne denné vyhľadávacie kapacity pre daktyloskopické údaje identifikovaných osôb a pre daktyloskopické údaje osôb ešte neidentifikovaných.
2. Maximálny počet kandidátov prijatých na overenie, ktorý pripadá na jedno zaslanie, sa uvádza v kapitole 2 prílohy k tomuto rozhodnutiu.

#### Článok 14

#### Pravidlá pre žiadosti a odpovede v súvislosti s daktyloskopickými údajmi

1. Dožiadaný členský štát bezodkladne skontroluje kvalitu zasielaných daktyloskopických údajov plne automatizovaným postupom. Ak sú údaje pre automatizované porovnávanie nevhodné, dožiadaný členský štát o tom bezodkladne informuje žiadajúci členský štát.

2. Dožiadaný členský štát vykoná vyhľadávania v poradí, v akom prijal žiadosti. Žiadosti sa musia spracovať do 24 hodín plne automatizovaným postupom. Žiadajúci členský štát môže v prípade, že sa to vyžaduje v jeho vnútroštátnom práve, požiadať o zrýchlené spracovanie svojich žiadostí a dožiadaný členský štát bezodkladne tieto vyhľadávania vykoná. Ak lehoty nemožno splniť z dôvodu vyššej moci, porovnávanie sa vykoná bezodkladne po odstránení prekážok.

#### KAPITOLA 5

### ÚDAJE Z EVIDENCIE VOZIDIEL

#### Článok 15

#### Zásady automatizovaného vyhľadávania údajov z evidencie vozidiel

1. Na automatizované vyhľadávanie údajov z evidencie vozidiel používajú členské štáty verziu softvérovej aplikácie pre európsky informačný systém vozidiel a vodičských preukazov (EUCARIS), ktorá bola vytvorená špeciálne na účely článku 12 rozhodnutia 2008/615/SVV, a upravené verzie tohto softvéru.
2. Automatizované vyhľadávanie údajov z evidencie vozidiel sa uskutočňuje v rámci decentralizovanej štruktúry.
3. Informácie vymieňané prostredníctvom systému EUCARIS sa zasielajú v kódovanej forme.
4. Prvky údajov z evidencie vozidiel, ktoré sa majú vymieňať, sa uvádzajú v kapitole 3 prílohy k tomuto rozhodnutiu.
5. Členské štáty môžu pri vykonávaní článku 12 rozhodnutia 2008/615/SVV uprednostniť vyhľadávania súvisiace s bojom proti závažnej trestnej činnosti.

#### Článok 16

#### Náklady

Každý členský štát znáša náklady vyplývajúce zo správy, používania a údržby softvérovej aplikácie EUCARIS uvedenej v článku 15 ods. 1.

#### KAPITOLA 6

### POLICAJNÁ SPOLUPRÁCA

#### Článok 17

#### Spoločné hliadky a iné spoločné operácie

1. Každý členský štát v súlade s kapitolou 5 rozhodnutia 2008/615/SVV, a najmä s vyhláseniami predkladanými podľa článku 17 ods. 4 a článku 19 ods. 2 a 4 uvedeného rozhodnutia, určí jeden alebo viac kontaktných bodov, aby umožnil iným členským

štátom obracať sa na príslušné orgány, a každý členský štát môže konkretizovať svoje postupy týkajúce sa organizácie spoločných hliadok a iných spoločných operácií, svoje postupy pre podnety z iných členských štátov vo vzťahu k týmto operáciám, ako aj ďalšie praktické aspekty a operatívne metódy týkajúce sa týchto operácií.

2. Generálny sekretariát Rady zostavuje a aktualizuje zoznam týchto kontaktných bodov a o zmenách v zozname informuje príslušné orgány.

3. Príslušné orgány každého členského štátu môžu podať podnet na organizáciu spoločnej operácie. Pred začiatkom konkrétnej operácie príslušné orgány uvedené v odseku 2 písomne alebo ústne formulujú podrobnosti, ktoré sa môžu vzťahovať na:

- a) príslušné orgány členských štátov vo vzťahu k operácii;
- b) konkrétny účel operácie;
- c) hostiteľský členský štát, v ktorom sa operácia uskutočňuje;
- d) geografickú oblasť hostiteľského členského štátu, v ktorom sa operácia uskutočňuje;
- e) obdobie vykonávania operácie;
- f) konkrétnu pomoc, ktorú majú poskytovať vysielajúce členské štáty hostiteľskému členskému štátu, vrátane príslušníkov alebo iných pracovníkov, hmotných a finančných, prostriedkov;
- g) príslušníkov zúčastňujúcich sa na operácii;
- h) príslušníka povereného vedením operácie;
- i) právomoci, ktoré počas operácie môžu príslušníci a iní pracovníci vysielajúcich členských štátov uplatňovať v hostiteľskom členskom štáte;
- j) konkrétne zbrane, strelivo a výzbroj, ktoré vyslaní príslušníci môžu používať počas operácie v súlade s rozhodnutím 2008/615/SVV;
- k) logistické metódy týkajúce sa dopravy, ubytovania a bezpečnosti;
- l) rozdelenie nákladov na spoločnú operáciu, ak sa odchyľuje od rozdelenia uvedeného v prvej vete článku 34 rozhodnutia Rady 2008/615/SVV;
- m) akékoľvek iné možné požadované prvky.

4. Vyhlásenia, postupy a určené kontaktné body ustanovené v tomto článku budú súčasťou príručky uvedenej v článku 18 ods. 2.

## KAPITOLA 7

### ZÁVEREČNÉ USTANOVENIA

#### Článok 18

#### Príloha a príručka

1. Ďalšie podrobnosti týkajúce sa technického a administratívneho vykonávania rozhodnutia 2008/615/SVV sa nachádzajú v prílohe k tomuto rozhodnutiu.

2. Príručku pripraví a aktualizuje Generálny sekretariát Rady tak, aby obsahovala výlučne skutkové informácie poskytnuté členskými štátmi vo vyhláseniach vydaných podľa rozhodnutia 2008/615/SVV alebo tohto rozhodnutia alebo v oznámeniach Generálnemu sekretariátu Rady. Príručka má formu dokumentu Rady.

#### Článok 19

#### Nezávislé orgány na ochranu údajov

Členské štáty v súlade s článkom 18 ods. 2 tohto rozhodnutia informujú Generálny sekretariát Rady o svojich nezávislých orgánoch na ochranu údajov alebo justičných orgánoch uvedených v článku 30 ods. 5 rozhodnutia 2008/615/SVV.

#### Článok 20

#### Príprava rozhodnutí uvedených v článku 25 ods. 2 rozhodnutia 2008/615/SVV

1. Rada prijíma rozhodnutie uvedené v článku 25 ods. 2 rozhodnutia 2008/615/SVV na základe hodnotiacej správy vypracovanej na základe dotazníka.

2. Pokiaľ ide o automatizovanú výmenu údajov v súlade s kapitolou 2 rozhodnutia 2008/615/SVV, hodnotiacia správa sa vypracuje aj na základe hodnotiacej návštevy a skúšobného testu, ktorý sa vykoná, keď príslušný členský štát poskytne generálnemu sekretariátu informácie v súlade s prvou vetou článku 36 ods. 2 rozhodnutia 2008/615/SVV.

3. Ďalšie podrobnosti o postupe sa uvádzajú v kapitole 4 prílohy k tomuto rozhodnutiu.

#### Článok 21

#### Hodnotenie výmeny údajov

1. Hodnotenie administratívnej, technickej a finančnej realizácie výmeny údajov podľa kapitoly 2 rozhodnutia 2008/615/SVV, a najmä používania postupu uvedeného v článku 15 ods. 5, sa vykonáva pravidelne. Hodnotenie sa týka tých členských štátov, ktoré už v čase hodnotenia uplatňujú rozhodnutie 2008/615/SVV, a týka sa tých kategórií údajov, ktorých výmena medzi



dotknutými členskými štátmi sa už začala. Hodnotenie sa zakladá na správach príslušných členských štátov.

2. Ďalšie podrobnosti o postupe sa uvádzajú v kapitole 4 prílohy k tomuto rozhodnutiu.

#### Článok 22

#### **Vzťah k vykonávacej dohode Prümskej zmluvy**

Na členské štáty viazané Prümskou zmluvou sa namiesto príslušných ustanovení obsiahnutých vo vykonávacej dohode Prümskej zmluvy uplatňujú príslušné ustanovenia tohto rozhodnutia a jeho prílohy hneď, ako sa v plnej miere začnú vykonávať. Ostatné ustanovenia vykonávacej dohody Prümskej zmluvy zostávajú medzi zmluvnými stranami Prümskej zmluvy v platnosti.

#### Článok 23

#### **Vykonávanie**

Členské štáty prijímú opatrenia potrebné na dosiahnutie súladu s ustanoveniami tohto rozhodnutia v lehotách stanovených v článku 36 ods. 1 rozhodnutia 2008/615/SVV.

#### Článok 24

#### **Uplatňovanie**

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Luxemburgu 23. júna 2008

*Za Radu*

*predseda*

I. JARC

## PRÍLOHA

## OBSAH

## KAPITOLA 1: Výmena údajov o DNA

1. **Súdne otázky týkajúce sa DNA, pravidiel zhodnosti a algoritmy**
  - 1.1. Vlastnosti profilov DNA
  - 1.2. Pravidlá zhodnosti
  - 1.3. Pravidlá oznamovania
2. **Tabuľka kódov členských štátov**
3. **Funkčná analýza**
  - 3.1. Dostupnosť systému
  - 3.2. Druhý krok
4. **Dokument o riadení prepojenia pre DNA**
  - 4.1. Úvod
  - 4.2. Vymedzenie štruktúry XML
5. **Aplikačná, bezpečnostná a komunikačná architektúra**
  - 5.1. Prehľad
  - 5.2. Architektúra vyššieho stupňa
  - 5.3. Bezpečnostné normy a ochrana údajov
  - 5.4. Protokoly a normy na použitie v šifrovacích mechanizmoch: sMIME a súvisiace balíky
  - 5.5. Aplikačná architektúra
  - 5.6. Protokoly a normy na použitie v aplikačnej architektúre
  - 5.7. Komunikačné prostredie

## KAPITOLA 2: Výmena daktyloskopických údajov (dokument o riadení prepojenia)

1. **Prehľad obsahu súboru**
2. **Formát záznamu**
3. **Logický záznam typu 1: Hlavička súboru**
4. **Logický záznam typu 2: Opisný text**
5. **Logický záznam typu 4: Obrázok v odtieňoch šedej s vysokým rozlíšením**
6. **Logický záznam typu 9: Záznam o markantoch**
7. **Logický záznam typu 13: Skrytý obrázok s rôznym rozlíšením**
8. **Logický záznam typu 15: Odtlačok dlane s rôznym rozlíšením**
9. **Dodatky ku kapitole 2 (výmena daktyloskopických údajov)**
  - 9.1. Oddelovacie kódy ASCII
  - 9.2. Výpočet alfanumerických kontrolných znakov

- 9.3. Znakové kódy
- 9.4. Súhrn transakcií
- 9.5. Vymedzenia záznamov typu 1
- 9.6. Vymedzenia záznamov typu 2
- 9.7. Kódy na kompresiu odtieňov šedej
- 9.8. Špecifikácia pošty

### KAPITOLA 3: Výmena údajov z evidencie vozidiel

- 1. **Spoločný súbor údajov na automatizované vyhľadávanie údajov z evidencie vozidiel**
  - 1.1. Vymedzenie pojmov
  - 1.2. Vyhľadávanie podľa vozidla/vlastníka/držiteľa
- 2. **Bezpečnosť údajov**
  - 2.1. Prehľad
  - 2.2. Bezpečnostné prvky výmeny správ
  - 2.3. Bezpečnostné prvky, ktoré sa netýkajú výmeny správ
- 3. **Technické podmienky výmeny údajov**
  - 3.1. Všeobecný opis aplikácie EUCARIS
  - 3.2. Požiadavky na funkčnosť a požiadavky, ktoré sa netýkajú funkčnosti

### KAPITOLA 4: Hodnotenie

- 1. **Hodnotiaci postup podľa článku 20 (príprava rozhodnutí podľa článku 25 ods. 2 rozhodnutia 2008/615/SVV)**
  - 1.1. Dotazník
  - 1.2. Skúšobná prevádzka
  - 1.3. Hodnotiaca návšteva
  - 1.4. Správa Rade
- 2. **Hodnotiaci postup podľa článku 21**
  - 2.1. Štatistika a správa
  - 2.2. Revízia
- 3. **Stretnutia expertov**



Kapitola 1: **Výmena údajov o DNA**1. **Súdne otázky týkajúce sa DNA, pravidiel zhodnosti a algoritmy**1.1. **Vlastnosti profilov DNA**

Profil DNA môže obsahovať 24 párov čísiel, ktoré predstavujú alely na 24 lokusoch a ktoré sa používajú aj v postupoch Interpolu týkajúcich sa DNA. Názvy uvedených lokusov sa nachádzajú v nasledujúcej tabuľke:

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 šedých miest v hornom riadku predstavuje aj súčasný európsky štandardný súbor lokusov (ESS) aj štandardný súbor lokusov DNA Interpolu (ISSOL).

Pravidlá začlenenia:

Profily DNA, ktoré členské štáty sprístupnia na účely vyhľadávania a porovnávania, ako aj profily DNA, ktoré sa odošlú na vyhľadávanie a porovnávania, musia obsahovať aspoň 6 úplných vymedzených<sup>(1)</sup> lokusov a v závislosti od dostupnosti môžu obsahovať dodatočné vymedzené lokusy alebo úseky mimo vymedzeného profilu. Referenčné profily DNA musia obsahovať aspoň 6 zo siedmich lokusov európskeho štandardného súboru. V záujme zvýšenia presnosti zhodných výsledkov sa do indexovanej databázy profilov DNA uložia všetky dostupné alely a budú sa využívať na vyhľadávanie a porovnávanie. Každý členský štát by hneď, ako to bude prakticky možné, mal implementovať všetky nové ESS lokusov, ktoré prijme EÚ.

Nepovoľujú sa zmiešané profily, aby alelová hodnota každého lokusu pozostávala len z dvoch čísiel, ktoré môžu byť v prípade homozygotov na rovnakom lokuse rovnaké.

Pre zástupný znak a mikrosatelity platia tieto pravidlá:

- Každá nečíselná hodnota v profile okrem amelogenínu (napr. „o“, „f“, „r“, „na“, „nr“ alebo „un“) sa automaticky prekonvertuje na zástupný znak (\*) a vyhľadávanie sa uskutoční medzi všetkými inými hodnotami.
- Hodnoty „0“, „1“ a „99“ sa automaticky konvertujú na zástupný znak (\*) a vyhľadávajú medzi všetkými inými hodnotami.
- Ak sa pri jednom mieste poskytnú 3 alely, akceptuje sa len prvá alela a ostávajúce dve sa musia automaticky prekonvertovať na zástupný znak (\*) a vyhľadávať medzi všetkými inými hodnotami.
- Ak sa zástupné znaky použijú pri prvej alebo druhej alele, budú sa vyhľadávať obe permutácie číselnej hodnoty pre daný lokus (napr. „12, \*“ by mohlo hlásiť zhodu s „12,14“ aj „9,12“).
- Pentanukleotidové mikrosatelity (Penta D, Penta E a CD4) sa budú porovnávať takto:

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

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

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

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

- Tetranukleotidové mikrosatelity (zvyšné lokusy sú tetranukleotidy) sa budú porovnávať takto:

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

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

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

<sup>(1)</sup> „Úplný vymedzený“ znamená, že je zahrnuté aj spracovanie zriedkavých alel.

1.2. *Pravidlá zhodnosti*

Porovnávanie dvoch profilov DNA sa uskutoční na základe tých lokusov, pri ktorých je v oboch profiloch dostupný alelový pár. Na oznámenie pozitívnej lustrácie sa v oboch profiloch DNA musí zhodovať aspoň 6 úplných vymedzených lokusov (okrem amelogenínu).

Úplná zhoda (prvá úroveň kvality) sa definuje ako zhoda v prípade, keď sú rovnaké všetky alely porovnávaných spoločných lokusov v oboch porovnávaných profiloch DNA. Čiastočná zhoda sa definuje ako zhoda v prípade, ak sa v oboch profiloch DNA medzi porovnávanými alelami vyskytuje len jedna nerovnaká alela (druhá, tretia a štvrtá úroveň kvality). Čiastočná zhoda sa akceptuje, len ak sa v dvoch porovnávaných profiloch vyskytuje aspoň 6 úplných vymedzených zhodných lokusov.

Dôvodom čiastočnej zhody môže byť:

- preklep pri vkladaní jedného z profilov DNA do vyhľadávачa alebo databázy DNA,
- chyba pri určovaní alely alebo analýze alely počas vytvárania profilu DNA.

1.3. *Pravidlá oznamovania*

Oznamovať sa budú úplné zhody, čiastočné zhody a „negatívna lustrácia“.

Oznámenie o zhode sa zašle žiadajúcemu národnému kontaktnému bodu a sprístupní sa aj dožadovanému národnému kontaktnému bodu (aby mohlo odhadnúť charakter a počet možných následných žiadostí o ďalšie dostupné osobné údaje a iné informácie spojené s profilom DNA, ktorý zodpovedá pozitívnemu výsledku vyhľadávania, v súlade s článkami 5 a 10 rozhodnutia 2008/615/SVV).

2. *Tabuľka kódov členských štátov*

V súlade s rozhodnutím 2008/615/SVV sa na vytvorenie názvov domén a ďalších konfiguračných parametrov, ktoré sa pri uzavretej sieti vyžadujú v průmyskových aplikáciách pri výmene údajov o DNA, používajú dvoj písmenové kódy zo zoznamu ISO 3166-1 alpha-2.

Pri členských štátoch sa používajú tieto dvoj písmenové kódy zo zoznamu ISO 3166-1 alpha-2:

Názov členského štátu	Kód	Názov členského štátu	Kód
Belgicko	BE	Luxembursko	LU
Bulharsko	BG	Maďarsko	HU
Česká republika	CZ	Malta	MT
Dánsko	DK	Holandsko	NL
Nemecko	DE	Rakúsko	AT
Estónsko	EE	Poľsko	PL
Grécko	EL	Portugalsko	PT
Španielsko	ES	Rumunsko	RO
Francúzsko	FR	Slovensko	SK
Írsko	IE	Slovinsko	SI
Taliansko	IT	Fínsko	FI
Cyprus	CY	Švédsko	SE
Lotyšsko	LV	Spojené kráľovstvo	UK
Litva	LT		

### 3. **Funkčná analýza**

#### 3.1. *Dostupnosť systému*

Žiadosti podľa článku 3 rozhodnutia 2008/615/SVV by sa do cieľovej databázy mali dostať v chronologickom poradí podľa odoslania a odpoveď by sa mala žiadajúcemu členskému štátu zaslať tak, aby ju dostal do 15 minút od doručenia žiadosti.

#### 3.2. *Druhý krok*

Keď členský štát dostane oznámenie o zhode, jeho národný kontaktný bod zodpovedá za porovnanie hodnôt predloženého profilu s hodnotami v prijatej odpovedi (profiloch) s cieľom overiť a skontrolovať dôkaznú hodnotu profilu. Národné kontaktné body sa na účely overovania môžu vzájomne kontaktovať priamo.

Postupy právnej pomoci sa začínajú po overení existujúcej zhody medzi dvoma profilmi na základe „úplnej zhody“ alebo „čiastočnej zhody“ získanej počas automatizovanej fázy vyhľadávania.

### 4. **Dokument o riadení prepojenia pre DNA**

#### 4.1. *Úvod*

##### 4.1.1. *Ciele*

V tejto kapitole sa vymedzujú požiadavky na výmenu informácií o profiloch DNA medzi databázovými systémami všetkých členských štátov. Polia v hlavičkách sa definujú špecificky pre prűmskú výmenu informácií o DNA, dátová časť vychádza z dátovej časti DNA profilu vo formáte XML vymedzenom pre bránu Interpolu na výmenu informácií o DNA.

Údaje sa vymieňajú prostredníctvom protokolu SMTP (Simple Mail Transfer Protocol) a iných moderných technológií, pomocou centrálného poštového relay servera od poskytovateľa sieťových služieb. Súbor XML sa prenáša ako telo správy.

##### 4.1.2. *Rozsah*

V tomto dokumente o riadení prepojenia (ICD – Interface Control Document) sa vymedzuje len obsah (poštovej) správy. Všetky témy týkajúce sa špecificky siete alebo pošty sa definujú jednotne, aby sa zabezpečila spoločná technická báza na výmenu údajov o DNA.

Rieši sa:

- formát predmetového poľa správy na umožnenie/zabezpečenie automatizovaného spracovania pošty,
- či je potrebné šifrovanie obsahu a ak áno, aký spôsob by sa mal zvoliť,
- maximálna dĺžka správ.

##### 4.1.3. *Štruktúra a zásady formátu XML*

Správa vo formáte XML sa delí na

- hlavičku (header), ktorá obsahuje informácie o prenose a
- dátovú časť (data), ktorá obsahuje informácie o konkrétnom profile, ako aj samotný profil.

Na žiadosť i odpoveď sa využíva rovnaká schéma XML.

Na účely úplnej kontroly neidentifikovaných profilov DNA (článok 4 rozhodnutia 2008/615/SVV) sa musí dať v jednej správe zaslať súbor profilov. Musí sa vymedziť i maximálny počet profilov v rámci jednej správy. Tento počet závisí od maximálnej povolenej veľkosti správy v elektronickej pošte a vymedzí sa po výbere poštového servera.

Príklad správy vo formáte 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> (...)] v prípade, že sa prostredníctvom jedinej správy SMTP zasiela viacero profilov, štruktúra „datas“ sa opakuje; toto je možné len v prípadoch podľa článku 4

```
</datas>]
```

```
</PRUEMDNA>
```

#### 4.2. Vymedzenie štruktúry XML

Nasledujúce definície sú len na dokumentačné účely a kvôli lepšej čitateľnosti, ozajstné záväzné informácie sa nachádzajú v súbore so schémou vo formáte XML (PRUEM DNA.xsd).

##### 4.2.1. Schéma PRUEMDNAx

Obsahuje tieto polia:

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

##### 4.2.2. Obsah štruktúry hlavičky

###### 4.2.2.1. PRUEM header

Touto štruktúrou sa opisuje hlavička súboru vo formáte XML. Obsahuje tieto polia:

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

Typ údajov obsiahnutých v správe, hodnota môže byť:

Value	Description
R	Request

Value	Description
A	Answer

## 4.2.2.3. PRUEM header info

Štruktúra na opis členského štátu, obsahuje aj dátum/čas správy. Obsahuje tieto polia:

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. Obsah údajov v profile PRUEM

## 4.2.3.1. PRUEM\_datas

Touto štruktúrou sa opisuje dátová časť súboru vo formáte XML. Obsahuje tieto polia:

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

Typ údajov obsiahnutých v správe, hodnota môže byť:

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

## 4.2.3.4. PRUEM\_data\_type

Typ údajov obsiahnutých v správe, hodnota môže byť:

Value	Description
P	Person profile
S	Stain

## 4.2.3.5. PRUEM\_data\_result

Typ údajov obsiahnutých v správe, hodnota môže byť:

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

## 4.2.3.6. IPSPG\_DNA\_profile

Štruktúra, ktorou sa opisuje profil DNA. Obsahuje tieto polia:

Fields	Type	Description
ess_issol	IPSPG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSPG_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. IPSPG\_DNA\_ISSOL

Štruktúra, ktorá obsahuje lokusy ISSOL (štandardná skupina lokusov Interpolu). Obsahuje tieto polia:

Fields	Type	Description
vwa	IPSPG_DNA_locus	Locus vwa
th01	IPSPG_DNA_locus	Locus th01



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

Štruktúra, ktorá obsahuje iné lokusy. Obsahuje tieto polia:

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

Štruktúra, prostredníctvom ktorej sa opisuje lokus. Obsahuje tieto polia:

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

5. **Aplikačná, bezpečnostná a komunikačná architektúra**5.1. *Prehľad*

Pri realizácii žiadostí o výmenu údajov o DNA v rámci rozhodnutia 2008/615/SVV sa používa spoločná komunikačná sieť, ktorá bude medzi členskými štátmi logicky uzavretá. Na účinnejšie využitie tejto spoločnej komunikačnej infraštruktúry, ktorá zahŕňa zasielanie žiadostí a získavanie odpovedí, sa prijal asynchrónny

mechanizmus na prenos žiadostí o údaje DNA a daktyloskopické údaje v správe elektronickej pošty v protokole SMTP. Aby sa vyriešili bezpečnostné obavy a s cieľom vytvoriť ozajstný bezpečný tunel z jedného konca siete na druhý, bude sa používať mechanizmus sMIME ako rozšírenie protokolu SMTP.

Ako komunikačná sieť na výmenu údajov medzi členskými štátmi sa používa funkčná TESTA (Trans European Services for Telematics between Administrations – transeurópska komunikačná sieť telematických služieb medzi orgánmi štátnej správy). Za sieť TESTA v súčasnosti zodpovedá Európska komisia. Vzhľadom na skutočnosť, že vnútroštátne databázy DNA a súčasné vnútroštátne prístupové miesta do siete TESTA sa môžu v členských štátoch nachádzať na iných lokalitách, prístup do siete TESTA sa môže zriadiť buď:

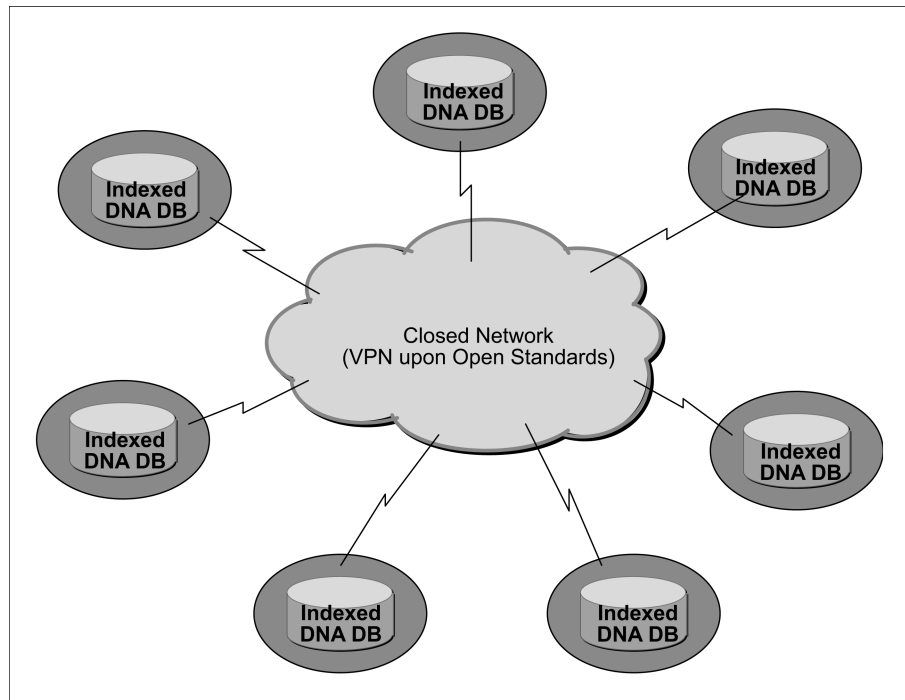
1. prostredníctvom využitia existujúceho vnútroštátneho prístupového miesta alebo vytvorenia nového prístupového miesta do siete TESTA, alebo
2. prostredníctvom vytvorenia bezpečného miestneho pripojenia z lokality, na ktorej je umiestnená databáza DNA a na ktorej ju spravuje príslušná vnútroštátna agentúra, na existujúce vnútroštátne prístupové miesto do siete TESTA.

Protokoly a normy, ktoré sa využívajú pri realizácii žiadostí na základe rozhodnutia 2008/615/SVV, sú v súlade s otvorenými normami a spĺňajú požiadavky uložené tvorcami vnútroštátnych bezpečnostných politík členských štátov.

## 5.2. Architektúra vyššieho stupňa

Každý členský štát sprístupní iným členským štátom svoje údaje DNA na výmenu a vyhľadávanie v súlade so štandardným spoločným formátom údajov v rozsahu pôsobnosti rozhodnutia 2008/615/SVV. Architektúra vychádza z komunikačného modelu „každý s každým“. Na uchovávanie profilov DNA neexistuje ani centrálny počítačový server, ani centralizovaná databáza.

Obrázok 1: Topológia výmeny údajov o DNA



Okrem súladu s vnútroštátnymi právnymi predpismi na lokalitách členských štátov sa každý z týchto štátov môže rozhodnúť, aký hardvér a softvér by mal na svojich lokalitách využiť na konfiguráciu, aby boli splnené požiadavky vyplývajúce z rozhodnutia 2008/615/SVV.

## 5.3. Bezpečnostné normy a ochrana údajov

Posúdili a zaviedli sa tri úrovne bezpečnosti.

#### 5.3.1. Dátová úroveň

Údaje v profile DNA, ktoré poskytnú jednotlivé členské štáty, sa musia pripraviť v súlade so spoločnými normami ochrany údajov tak, aby žiadajúci členský štát dostal odpoveď, v ktorej sa uvádza najmä, či ide o POZITÍVNY alebo NEGATÍVNY výsledok vyhľadávania; ak je výsledok vyhľadávania POZITÍVNY, v odpovedi sa bude nachádzať identifikačné číslo, ale žiadne osobné údaje. Ďalšie vyšetrovanie po oznámení, že výsledok vyhľadávania bol POZITÍVNY, sa vykoná na dvojstrannej úrovni podľa existujúcich vnútroštátnych právnych a organizačných predpisov, ktoré sa vzťahujú na lokality jednotlivých členských štátov.

#### 5.3.2. Komunikačná úroveň

Správy, v ktorých sa nachádzajú informácie o profiloch DNA (od žiadajúceho i dožadovaného členského štátu) sa zašifrujú najmodernejším mechanizmom zodpovedajúcim otvoreným normám, ako napríklad sMIME, ešte pred tým, ako sa odošlú na lokality iných členských štátov.

#### 5.3.3. Prenosová úroveň

Všetky zašifrované správy, v ktorých sa nachádzajú informácie o profile DNA, sa budú zasielať do systémov iných členských štátov prostredníctvom privátneho virtuálneho tunelového systému, ktorý spravuje dôveryhodný poskytovateľ siete na medzinárodnej úrovni a prostredníctvom bezpečných liniek k tomuto tunelovému systému pod vnútroštátnou zodpovednosťou. Tento súkromný virtuálny tunelový systém nemá žiadny spoločný bod s verejným internetom.

#### 5.4. Protokoly a normy na použitie v šifrovaných mechanizmoch: sMIME a súvisiace balíky

Na šifrovanie správ obsahujúcich informácie o profiloch DNA sa použije otvorená norma sMIME ako rozšírenie v podstate štandardného protokolu elektronickej pošty SMTP. Protokol sMIME (V3) umožňuje podpísané potvrdenia, bezpečnostné nálepky a bezpečné zoznamy adresátov na základe syntaxe kryptografických správ (CMS – Cryptographic Message Syntax), špecifikácie osobitnej skupiny pre internetové inžinierstvo (IETF – Internet Engineering Task Force) pre kryptograficky chránené správy. Môže sa využiť na digitálne podpisovanie, spracovanie, overovanie alebo šifrovanie akejkoľvek formy digitálnych údajov.

Základný certifikát, ktorý využíva mechanizmus sMIME, musí byť v súlade s normou X.509. S cieľom zabezpečiť súlad spoločných noriem a postupov s inými průmyskými aplikáciami platia pre operácie šifrovania s mechanizmom sMIME alebo na uplatnenie v rámci rôznych aplikačných a užívateľských softvérov (COTS – Commercial Products of the Shelves) tieto pravidlá spracovania:

- Následnosť operácií je: najprv šifrovanie a potom podpis.
- Na symetrické šifrovanie sa použije šifrovací algoritmus AES (Advanced Encryption Standard) s 256-bitovým kľúčom a na nesymetrické algoritmus RSA s 1 024-bitovým kľúčom.
- Využije sa hašovací algoritmus SHA-1.

Funkcia sMIME je zabudovaná do obrovskej väčšiny moderných balíkov softvéru pre elektronickú poštu vrátane aplikácií Outlook, Mozilla Mail a Netscape Communicator 4.x a funguje pri ich prepojení.

Pretože sMIME sa ľahko integruje do vnútroštátnej informačnej infraštruktúry na lokalitách všetkých členských štátov, vybral sa ako životaschopný mechanizmus na realizáciu komunikačnej úrovne bezpečnosti. Na efektívnejšie splnenie cieľa získania „dôkazu vhodnosti koncepcie“ a zníženie nákladov sa však na prvotnú výmenu údajov o DNA vybralo otvorené štandardné rozhranie na programovanie aplikácií (API – Application Programming Interface) JavaMail. Rozhranie JavaMail poskytuje jednoduché šifrovanie a dešifrovanie emailov pomocou mechanizmov s/MIME a/alebo OpenPGP. Zámerom je poskytnúť jediné a jednoduché rozhranie API klientom elektronickej pošty, ktorí si želajú odosielať a prijímať zašifrovanú poštu v jednom z dvoch najrozšírenejších emailových šifrovacích formátov. Preto budú na splnenie požiadaviek ustanovených v rozhodnutí 2008/615/SVV postačovať akékoľvek moderné implementácie rozhrania JavaMail, ako napríklad produkt spoločnosti Bouncy Castle JCE (Java Cryptographic Extension), ktorý sa použije na zavedenie protokolu sMIME na prvotnú výmenu údajov o DNA medzi členskými štátmi.

### 5.5. Aplikačná architektúra

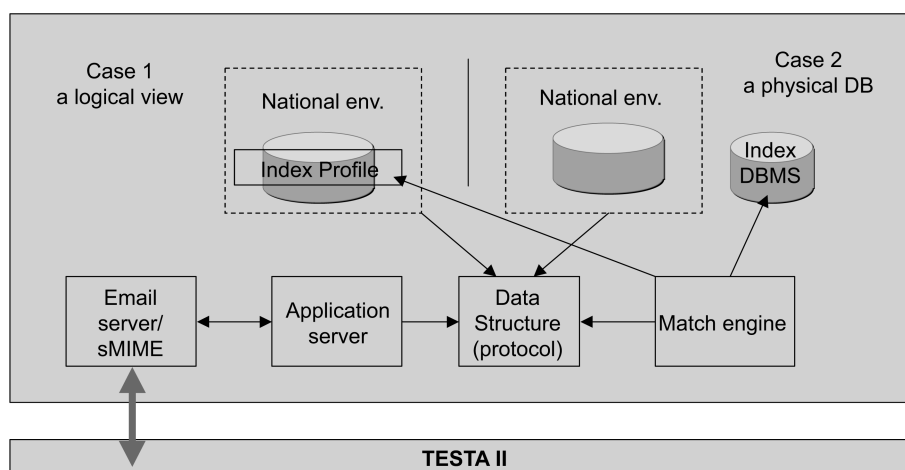
Každý členský štát poskytne ostatným členským štátom súbor standardizovaných údajov o profiloch DNA, ktoré zodpovedajú platnému spoločnému ICD. Môže tak urobiť buď prostredníctvom poskytnutia logického prehľadu jednotlivých vnútroštátnych databáz, alebo vytvorenia fyzicky exportovateľnej databázy (indexovanej databázy).

Pomocou štyroch hlavných zložiek – emailového servera sMIME, aplikačného servera, oblasti štruktúrovania dát na získavanie/vkladanie údajov a evidenciu prichádzajúcich/odchádzajúcich správ a vyhľadávača zhodných profilov – sa celá aplikačná logika realizuje nezávisle od produktu.

Na uľahčenie integrácie uvedených komponentov do príslušných vnútroštátnych lokalít členských štátov sa určené spoločné funkcie implementovali prostredníctvom „open source“ komponentov, ktoré si každý členský štát môže vybrať na základe svojej vnútroštátnej politiky a vnútroštátnych predpisov v oblasti informačných technológií. Pretože na účely získania prístupu do indexovaných databáz, v ktorých sa nachádzajú profily DNA začlenené v rozhodnutí 2008/615/SVV, sa majú zaviesť uvedené nezávislé mechanizmy, každý členský štát má voľný výber hardvérovej a softvérovej platformy vrátane databázy a operačných systémov.

V rámci existujúcej spoločnej siete sa vytvoril a úspešne odskúšal prototyp výmeny údajov o DNA. Vo funkčnom prostredí sa zaviedla verzia 1.0 a používa sa v každodennej prevádzke. Členské štáty môžu využívať uvedený spoločný produkt, ale môžu si vytvoriť aj vlastné. Komponenty spoločného produktu sa budú udržiavať, prispôbovať a naďalej rozvíjať podľa meniacich sa požiadaviek IT, súdneho lekárstva alebo operačných požiadaviek polície.

Obrázok 2: Prehľad aplikačnej topológie



### 5.6. Protokoly a normy na použitie v aplikačnej architektúre

#### 5.6.1. XML

Pri výmene údajov o DNA sa naplno využije schéma XML ako príloha k poštovým správam vo formáte SMTP. Rozšíriteľný značkovací jazyk (XML – eXtensible Markup Language) je všeobecným značkovacím jazykom odporúčaným konzorciom W3C na vytváranie značkovacích jazykov na konkrétne účely, v ktorom je možné opísať mnoho rôznych druhov údajov. Profil DNA, ktorý je vhodný na výmenu medzi členskými štátmi, sa prostredníctvom jazyka XML a schémy XML opísal v dokumente ICD.

#### 5.6.2. ODBC

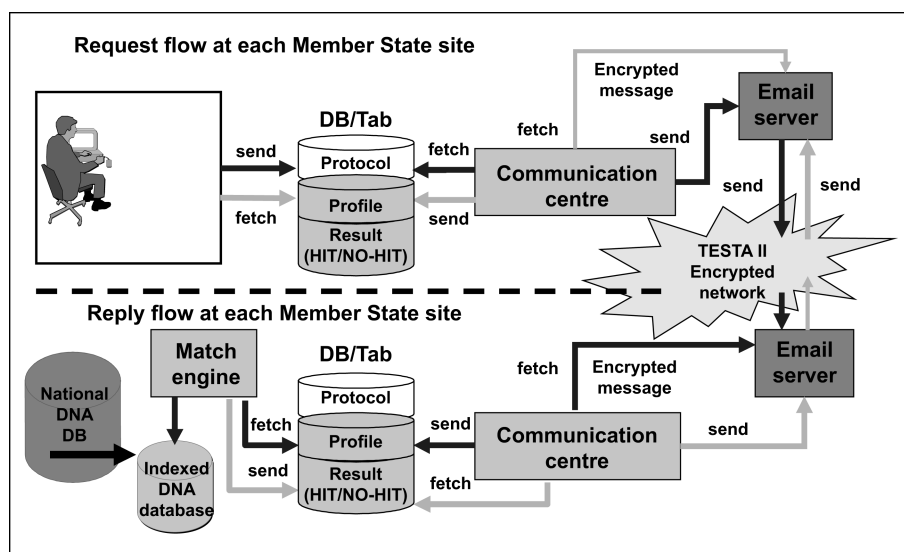
Databázové rozhranie ODBC (Open DataBase Connectivity) poskytuje štandardnú softvérovú API metódu na prístup do riadiacich systémov databáz nezávisle od programovacích jazykov a databázových a operačných systémov. ODBC má však niekoľko nedostatkov. Správa väčšieho počtu klientských zariadení si môže vyžadovať rôzne ovládače a knižnice DLL. Takáto komplexnosť môže zvýšiť réžiu správy systému.

## 5.6.3. JDBC

Rozhranie JDBC (Java DataBase Connectivity) je API pre programovací jazyk Java, v ktorom sa vymedzujú spôsoby prístupu do databázy zo strany klienta. Na rozdiel od ODBC si JDBC nevyžaduje použitie určitého súboru miestnych knižníc DLL na ploche.

Aplikačná logika spracovania žiadostí o profil DNA a odpovedí na lokalite každého členského štátu sa opisuje v nasledujúcom diagrame. Spracovanie žiadostí i odpovedí sa prekrýva s neutrálnou dátovou oblasťou, v ktorej sa nachádzajú rôzne skupiny údajov so spoločnou dátovou štruktúrou.

Obrázok 3: Schéma fungovania aplikácie na lokalite každého členského štátu



## 5.7. Komunikačné prostredie

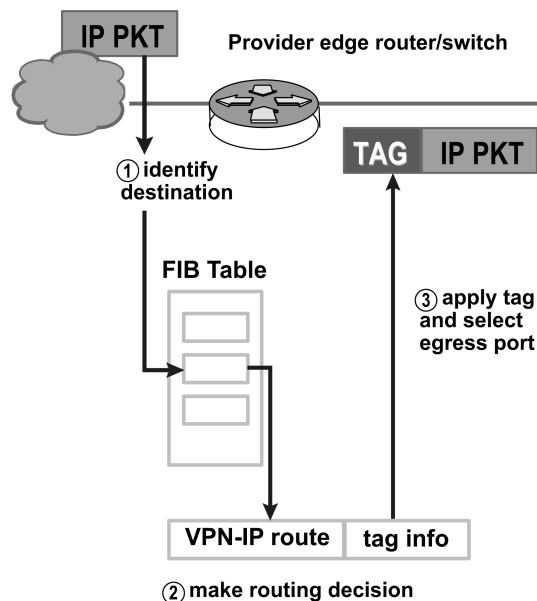
## 5.7.1. Spoločná komunikačná sieť: TESTA a ďalšia infraštruktúra

Aplikácia výmena údajov o DNA bude využívať asynchrónny mechanizmus elektronickej pošty na zasielanie žiadostí a prijímanie odpovedí medzi členskými štátmi. Keďže všetky členské štáty majú aspoň jedno vnútroštátne prístupové miesto do siete TESTA, výmena údajov o DNA bude fungovať v rámci tejto siete. TESTA poskytuje prostredníctvom svojho emailového prenosu niekoľko služieb s pridanou hodnotou. Okrem prevádzkovania a spravovania špecifických emailových schránok pre sieť TESTA sa prostredníctvom uvedenej infraštruktúry realizujú aj zoznamy adresátov pošty a postupy presmerovania. Toto umožňuje, aby sa TESTA využívala ako spracovateľské stredisko pre správy adresované štátnym orgánom prepojeným s celoeurópskymi doménami. Zaviesť sa môže aj mechanizmus antivírusovej kontroly.

Prenos poštových správ v rámci siete TESTA je postavený na vysoko dostupnej hardvérovej platforme umiestnenej v centrálnych aplikačných priestoroch siete TESTA a chránenej bránou firewall. Systém správy doménových mien (DNS – Domain Name Services) v rámci siete TESTA preloží informácie z vyhľadávačov zdroja na IP adresy a skryje informácie o adrese pred používateľom a aplikáciami.

## 5.7.2. Bezpečnostné otázky

V rámci siete TESTA sa realizovala koncepcia virtuálnej privátnej siete (VPN – Virtual Private Network). Štítkovacia technológia použitá na vytvorenie uvedenej VPN sa bude ďalej vyvíjať, aby podporovala štandard MPLS (Multi-Protocol Label Switching), ktorý vytvorila osobitná skupina IETF.



MPLS je štandardnou technológiou, ktorá zvyšuje rýchlosť smerovania dát v sieti tým, že zabráňuje analýze paketov zo strany priebežných smerovačov (vynechávajú sa skoky). Funguje to na základe tzv. značiek, ktoré paketu pridelí okrajový smerovač chrbticovej siete na základe informácií uložených v smerovacej tabuľke FIB (Forwarding Information Base). Značky sa používajú aj na implementáciu virtuálnych súkromných sietí (VPN).

MPLS spája výhody smerovania protokolu tretej vrstvy a prepínania protokolu druhej vrstvy. Pretože počas prechodu cez chrbticovú sieť sa nevyhodnocujú IP adresy, v štandarde MPLS nie sú žiadne obmedzenia týkajúce sa týchto adries.

Okrem toho budú emailové správy v sieti TESTA II chránené šifrovacím mechanizmom na základe sMIME. Bez poznania kľúča a bez správneho certifikátu sa nikomu v sieti nepodari správy dešifrovať.

### 5.7.3. Protokoly a normy, ktoré sa budú využívať v rámci komunikačnej siete

#### 5.7.3.1. SMTP

Protokol SMTP (Simple Mail Transfer Protocol) je vlastne štandardným protokolom na prenos elektronickej pošty cez Internet. SMTP je relatívne jednoduchým textovým protokolom, v ktorom sa špecifikuje jeden alebo viac príjemcov správ a následne sa odošle text správy. SMTP využíva TCP port 25 podľa špecifikácie IETF. Na určenie servera SMTP pre príslušný názov domény sa využíva záznam MX (Mail eXchange) DNS (Domain Name Systems).

Keďže tento protokol bol vytvorený ako čistý textový protokol na základe tabuľky ASCII, prácu s binárnymi súborami nevládal. Na zakódovanie binárnych súborov na účely prenosu prostredníctvom SMTP sa vytvorili normy typu MIME. V súčasnosti väčšina serverov SMTP podporuje rozšírenia 8BITMIME a sMIME, ktoré umožňujú prenos binárnych súborov s ľahkosťou čistého textu. Postupy spracovania pre operácie s/MIME sa opisujú v oddiele s/MIME (pozri kapitolu 5.4).

SMTP je protokolom typu „push“, ktorý neumožňuje používateľovi stiahnuť si správy zo vzdialeného servera na žiadosť. Na to musí klient elektronickej pošty využívať protokoly POP3 alebo IMAP. V rámci realizácie výmeny údajov o DNA sa rozhodlo, že sa bude využívať protokol POP3.

#### 5.7.3.2. POP

Miestni klienti elektronickej pošty využívajú na stiahnutie pošty zo vzdialeného servera cez spojenie TCP/IP tretiu verziu protokolu POP (Post Office Protocol), štandardný internetový protokol aplikačnej vrstvy. Klienti elektronickej pošty posielajú správy cez Internet alebo sieť spoločnosti prostredníctvom profilu SMTP Submit protokolu SMTP. Normou pre prílohy a text, ktorý nie je vytvorený pomocou znakov ASCII, je MIME. Hoci ani POP3, ani SMTP nevyžaduje email formátovaný cez protokol MIME, internetová elektronická pošta prichádza v takomto formáte, a preto klienti služby POP musia MIME chápať a používať. V celom komunikačnom prostredí podľa rozhodnutia 2008/615/SVV sa preto budú nachádzať zložky protokolu POP.



## 5.7.4. Pridelenie sieťovej adresy

## Operačné prostredie

Sieti TESTA prideliť Európsky úrad na registráciu IP adries (RIPE) vymedzený blok podsiete triedy C. V prípade potreby sa v budúcnosti siete TESTA môžu prideliť ďalšie bloky adries. Pridelovanie IP adries členským štátom sa zakladá na geografickej schéme Európy. Výmena údajov medzi členskými štátmi v rámci rozhodnutia 2008/615/SVV sa prevádzkuje cez celoeurópsku, logicky uzavretú sieť IP.

## Testovacie prostredie

Na zabezpečenie hladko fungujúceho prostredia každodennej prevádzky vo všetkých pripojených členských štátoch je potrebné v rámci uzavretej siete vytvoriť testovacie prostredie pre nové členské štáty, ktoré sa pripravujú na pripojenie. Vymedzil sa zoznam parametrov, ktorý obsahuje IP adresy, nastavenia siete, emailové domény a účty používateľa aplikácií, a tieto parametre sa nastavujú na zodpovedajúcej lokalite príslušného členského štátu. Okrem toho sa na skúšobné účely vytvoril súbor pseudoprofilov DNA.

## 5.7.5. Konfiguračné parametre

Vytvoril sa bezpečný systém elektronickej pošty, ktorý využíva doménu eu-admin.net. K tejto doméne a pridruženým adresám nebude existovať prístup z lokalít, ktoré sa nenachádzajú na celoeurópskej doméne TESTA, pretože príslušné mená pozná len centrálny DNS server TESTA, ktorý je chránený pred prístupom z internetu.

Mapovanie uvedených adries lokalít (doménových mien) na ich IP adresy sa vykonáva prostredníctvom služby DNS siete TESTA. Ku každej miestnej doméne sa na uvedenom centrálnom serveri DNS pre sieť TESTA pridá poštová položka, čím sa zabezpečí presmerovanie všetkých emailov odoslaných na miestne domény siete TESTA na centrálny poštový relay server siete TESTA. Tento relay server siete TESTA potom správy presmeruje na špecifický poštový server miestnej domény pomocou emailových adries miestnych domén. Prostredníctvom takéhoto prenosu elektronickej pošty sa zabezpečí, že zásadné informácie obsiahnuté v emailoch sa budú pohybovať len cez celoeurópsku uzavretú sieťovú infraštruktúru, a nie cez málo bezpečný internet.

Na lokalitách všetkých členských štátov je preto potrebné vytvoriť subdomény (**tučná kurzíva**) s takouto syntaxou:

„**typ-aplikácie.pruem.kód-členského štátu.eu-admin.net**“, kde:

„**kód-členského štátu**“ je dvojísmenným kódom členského štátu (napr. AT, BE atď.),

„**typ-aplikácie**“ je buď DNA, alebo FP.

V nasledujúcej tabuľke sa nachádzajú subdomény členských štátov vytvorené na základe uvedenej syntaxe:

MS	Subdomény	Poznámky
BE	<b>dna.pruem.be.eu-admin.net</b>	Vytvára bezpečné miestne pripojenie k existujúcemu vnútroštátnemu prístupovému miestu do siete TESTA II
	<b>fp.pruem.be.eu-admin.net</b>	
BG	<b>dna.pruem.bg.eu-admin.net</b>	
	<b>fp.pruem.bg.eu-admin.net</b>	
CZ	<b>dna.pruem.cz.eu-admin.net</b>	
	<b>fp.pruem.cz.eu-admin.net</b>	
DK	<b>dna.pruem.dk.eu-admin.net</b>	
	<b>fp.pruem.dk.eu-admin.net</b>	
DE	<b>dna.pruem.de.eu-admin.net</b>	Využíva existujúce vnútroštátne prístupové miesta do siete TESTA II
	<b>fp.pruem.de.eu-admin.net</b>	
EE	<b>dna.pruem.ee.eu-admin.net</b>	
	<b>fp.pruem.ee.eu-admin.net</b>	

MS	Subdomény	Poznámky
IE	<b>dna.pruem.ie.eu-admin.net</b>	
	<b>fp.pruem.ie.eu-admin.net</b>	
EL	<b>dna.pruem.el.eu-admin.net</b>	
	<b>fp.pruem.el.eu-admin.net</b>	
ES	<b>dna.pruem.es.eu-admin.net</b>	Využíva existujúce vnútroštátne prístupové miesto do siete TESTA II
	<b>fp.pruem.es.eu-admin.net</b>	
FR	<b>dna.pruem.fr.eu-admin.net</b>	Využíva existujúce vnútroštátne prístupové miesto do siete TESTA II
	<b>fp.pruem.fr.eu-admin.net</b>	
IT	<b>dna.pruem.it.eu-admin.net</b>	
	<b>fp.pruem.it.eu-admin.net</b>	
CY	<b>dna.pruem.cy.eu-admin.net</b>	
	<b>fp.pruem.cy.eu-admin.net</b>	
LV	<b>dna.pruem.lv.eu-admin.net</b>	
	<b>fp.pruem.lv.eu-admin.net</b>	
LT	<b>dna.pruem.lt.eu-admin.net</b>	
	<b>fp.pruem.lt.eu-admin.net</b>	
LU	<b>dna.pruem.lu.eu-admin.net</b>	Využíva existujúce vnútroštátne prístupové miesto do siete TESTA II
	<b>fp.pruem.lu.eu-admin.net</b>	
HU	<b>dna.pruem.hu.eu-admin.net</b>	
	<b>fp.pruem.hu.eu-admin.net</b>	
MT	<b>dna.pruem.mt.eu-admin.net</b>	
	<b>fp.pruem.mt.eu-admin.net</b>	
NL	<b>dna.pruem.nl.eu-admin.net</b>	Plánuje vytvoriť nové prístupové miesto do siete TESTA II pri Holandskom forenznom inštitúte (NFI – Nederlands Forensisch Instituut)
	<b>fp.pruem.nl.eu-admin.net</b>	
AT	<b>dna.pruem.at.eu-admin.net</b>	Využíva existujúce vnútroštátne prístupové miesto do siete TESTA II
	<b>fp.pruem.at.eu-admin.net</b>	
PL	<b>dna.pruem.pl.eu-admin.net</b>	
	<b>fp.pruem.pl.eu-admin.net</b>	
PT	<b>dna.pruem.pt.eu-admin.net</b>	.....
	<b>fp.pruem.pt.eu-admin.net</b>	.....
RO	<b>dna.pruem.ro.eu-admin.net</b>	
	<b>fp.pruem.ro.eu-admin.net</b>	

MS	Subdomény	Poznámky
SI	<b>dna.pruem.si</b> .eu-admin.net	.....
	<b>fp.pruem.si</b> .eu-admin.net	.....
SK	<b>dna.pruem.sk</b> .eu-admin.net	
	<b>fp.pruem.sk</b> .eu-admin.net	
FI	<b>dna.pruem.fi</b> .eu-admin.net	[Vloží sa]
	<b>fp.pruem.fi</b> .eu-admin.net	
SE	<b>dna.pruem.se</b> .eu-admin.net	
	<b>fp.pruem.se</b> .eu-admin.net	
UK	<b>dna.pruem.uk</b> .eu-admin.net	
	<b>fp.pruem.uk</b> .eu-admin.net	

## Kapitola 2: Výmena daktyloskopických údajov (dokument o riadení prepojenia)

Cieľom tohto dokumentu o riadení prepojenia je vymedziť požiadavky na výmenu daktyloskopických informácií medzi automatickými systémami na identifikáciu odtlačkov prstov (AFIS – Automated Fingerprint Identification Systems) v jednotlivých členských štátoch. Vychádza z vykonávania normy ANSI/NIST-ITL 1-2000 (INT-I, verzia 4.22b) zo strany Interpolu.

Táto verzia zahŕňa všetky základné definície logických záznamov typu 1, 2, 4, 9, 13 a 15, ktoré sa vyžadujú na daktyloskopické spracovanie založené na obrázku alebo charakteristických individuálnych znakoch (markantoch).

### 1. Prehľad obsahu súboru

Daktyloskopický súbor pozostáva z viacerých logických záznamov. V pôvodnej norme ANSI/NIST-ITL 1-2000 je vymedzených šesťnásť typov záznamov. Medzi každým záznamom a poliami a subpoliami v rámci záznamov sa používajú príslušné oddeľovacie znaky podľa tabuľky ASCII.

Na výmenu informácií medzi agentúrou pôvodu a určenia sa používa len 6 typov záznamov:

- Typ-1 → Informácie o operácii
- Typ-2 → Alfnumerické údaje o osobách/prípade
- Typ-4 → Daktyloskopické obrázky v odtieňoch šedej s vysokým rozlíšením
- Typ-9 → Záznam o markantoch
- Typ-13 → Záznam latentného obrázku s rôznym rozlíšením
- Typ-15 → Záznam odtlačku dlane s rôznym rozlíšením

#### 1.1. Typ 1 – Hlavička súboru

Tento záznam obsahuje informácie o smerovaní a informácie opisujúce štruktúru zvyšku súboru. V tomto type záznamu sa tiež vymedzujú typy operácií, ktoré patria do nasledujúcich širších kategórií:

#### 1.2. Typ 2 – Opisný text

Tento záznam obsahuje textové informácie, ktoré môžu byť zaujímavé pre odosielajúcu a prijímajúcu agentúru.

#### 1.3. Typ 4 – Obrázok v odtieňoch šedej s vysokým rozlíšením

Tento záznam sa používa na výmenu daktyloskopických obrázkov v odtieňoch šedej (s 8 bitovým kódovaním) s vysokým rozlíšením 500 pixelov na palec. Daktyloskopické obrázky sa komprimujú pomocou algoritmu WSQ (Wavelet/Scalar Quantization) s kompresným pomerom nepresahujúcim 15 : 1. Nesmú sa využívať iné kompresné algoritmy ani nekomprimované obrázky.

#### 1.4. Typ 9 – Záznam o markantoch

Záznamy typu 9 sa používajú na výmenu údajov o papilárnych líniách alebo markantoch. Ich účelom je čiastočne sa vyhnúť nepotrebnému zdvojeniu kódovacích procesov AFIS a čiastočne umožniť prenos kódov AFIS, ktoré obsahujú menej údajov ako zodpovedajúce obrázky.

#### 1.5. Typ 13 – Záznam latentného obrázku s rôznym rozlíšením

Tento záznam sa používa na výmenu skrytých obrázkov odtlačkov prstov a dlaní s rôznym rozlíšením spolu s alfanumerickou informáciou o textúre. Skenovacie rozlíšenie obrázkov je 500 pixelov na palec pri 256 odtieňoch šedej. V prípade dostatočnej kvality sa skrytý obrázok komprimuje pomocou algoritmu WSQ. V prípade potreby sa rozlíšenie obrázkov na základe dvojstrannej dohody môže zvýšiť na viac ako 500 pixelov na palec pri viac než 256 odtieňoch šedej. V tomto prípade sa dôsledne odporúča využiť formát JPEG 2000 (pozri dodatok 7).

#### 1.6. Typ 15 – Záznam odtlačku dlane s rôznym rozlíšením

Záznamy obrázkov s označením polí typu 15 sa používajú na výmenu obrázkov odtlačkov dlane s rôznym rozlíšením spolu s alfanumerickou informáciou o textúre. Skenovacie rozlíšenie obrázkov je 500 pixelov na palec pri 256 odtieňoch šedej. Kvôli minimalizácii objemu údajov sa všetky obrázky odtlačkov dlane komprimujú pomocou algoritmu WSQ. V prípade potreby sa rozlíšenie obrázkov na základe dvojstrannej dohody môže zvýšiť na viac ako 500 pixelov na palec pri viac než 256 odtieňoch šedej. V tomto prípade sa dôsledne odporúča využiť formát JPEG 2000 (pozri dodatok 7).

### 2. Formát záznamu

Prenášaný súbor sa skladá z jedného alebo viacerých logických záznamov. Pri každom logickom zázname v súbore sa nachádza niekoľko informačných polí, ktoré k takémuto záznamu prináležia. Každé informačné pole môže obsahovať jeden alebo viacero základných informačných prvkov s jedinou hodnotou. Tieto prvky sa spoločne používajú na prenos rôznych aspektov údajov, ktoré sa v danom poli nachádzajú. Informačné pole môže pozostávať aj z jedného alebo viacerých zoskupených informačných prvkov, ktoré sa v danom poli niekoľkokrát opakujú. Takéto zoskupenie informačných prvkov sa nazýva podpole. Informačné pole preto pozostáva z jedného alebo viacerých podpolí obsahujúcich informačné prvky.

#### 2.1. Separátory informácií

V logických záznamoch ohraničených tagmi sa mechanizmy na ohraničenie informácií uplatňujú vo forme štyroch separátorov informácií ASCII. Ohraničené informácie môžu byť prvkami v rámci poľa alebo podpoľa, poliami v rámci logických záznamov alebo viackrát sa vyskytujúcimi podpoliami. Uvedené separátory informácií sa vymedzujú v norme ANSI X3.4. Sú to znaky, ktoré sa používajú na oddelenie a zatriedenie informácií v logickom zmysle. V rámci hierarchických vzťahov je najinkluzívnejším znakom separátor súboru „FS“, po ňom separátor skupiny „GS“, separátor záznamu „RS“ a nakoniec separátor jednotky „US“. V tabuľke 1 sa nachádza zoznam týchto separátorov a opis ich použitia v rámci uvedenej normy.

Z funkčného hľadiska by sa mali separátory informácií považovať za označenie typu údajov, ktoré po nich nasledujú. Znak „US“ oddeľuje jednotlivé informácie v poli či podpoli. Signalizuje, že ďalšia informácia bude údaj, ktorý sa týka daného poľa či podpoľa. Viaceré podpolia v poli oddelenom pomocou znaku „RS“ naznačujú začiatok ďalšej skupiny opakovaných informácií. Separátor „GS“ použitý medzi informačnými poliami signalizuje začiatok nového poľa, ktoré predchádza polu identifikovanému zobrazeným číslom. Podobne by aj výskyt separátora „FS“ mal znamenať začiatok nového logického záznamu.

Tieto štyri znaky majú význam len v prípade, ak sa použijú ako separátory jednotlivých údajov v poliach textových záznamov ASCII. V binárnych obrázkoch či v binárnych poliach nemajú tieto znaky žiaden osobitný význam – sú len súčasťou vymieňaných údajov.

Za bežných okolností by sa nemali vyskytovať prázdne polia ani nulové informácie, a preto by sa medzi akýmkoľvek dvoma údajmi mal objavovať len jeden separátor. Výnimkou z tohto pravidla sú prípady, keď nie sú údaje v poliach alebo informáciách v rámci transakcie dostupné, ak chýbajú alebo sú nepovinné, a ak priebeh transakcie nezávisí od prítomnosti takýchto údajov. V takýchto prípadoch sa namiesto vkládania „vaty“ medzi separátory môžu spolu objaviť viaceré príslušné separátory.

Pri definovaní poľa, ktoré sa skladá z troch informácií, platia tieto pravidlá. Ak chýba druhá informácia, medzi prvou a tretou informáciou sa objaví dva znaky „US“ vedľa seba. Ak by chýbala druhá i tretia informácia, mali by sa použiť tri separátory – dva znaky „US“ a separátor uzatvárajúci pole či podpole. Vo všeobecnosti platí, že ak pre pole alebo podpole nie je dostupná jedna povinná alebo nepovinná informácia, alebo viacero takýchto informácií, mal by sa vložiť zodpovedajúci počet separátorov.

Je možné, aby vedľa seba existovali kombinácie dvoch alebo viacerých zo štyroch dostupných separátorov. Ak pri informačných položkách, podpoliach alebo poliach chýbajú údaje alebo ak nie sú dostupné, počet použitých separátorov musí byť o jeden nižší, ako počet vyžadovaných informácií, podpolí alebo polí.

Tabuľka 1: Použité separátory

Kód	Typ	Opis	Hexadecimálna hodnota	Decimálna hodnota
US	separátor jednotky	oddeľuje jednotlivé informácie	1F	31
RS	separátor záznamu	oddeľuje podpolia	1E	30
GS	separátor skupiny	oddeľuje polia	1D	29
FS	separátor súboru	oddeľuje logické záznamy	1C	28

## 2.2. Rozvrhnutie záznamu

V logických záznamoch označených tagmi sa každé použité informačné pole očísľuje v súlade s touto normou. Formát pre každé pole pozostáva z čísla typu logického záznamu, po ktorom nasleduje bodka „.“, a z čísla poľa, po ktorom nasleduje dvojbodka „:“, po nich nasledujú príslušné informácie pre dané pole. Číslo poľa ohraničeného tagmi môže byť akékoľvek číslo pozostávajúce z jednej až deviatich číslic medzi bodkou a dvojbodkou. Vykladá sa ako nezáporný celočíselný kód poľa. Z toho vyplýva, že číslo poľa „2.123:“ je rovnocenné a malo by sa vykladať rovnakým spôsobom ako číslo poľa „2.000000123:“.

Na účely objasnenia sa v tomto dokumente na výpočet polí obsiahnutých v každom z opísaných logických záznamov ohraničených tagmi používa číslo pozostávajúce z troch číslic. Číslo polí budú mať formát „TT.xxx:“, pričom „TT“ bude typ záznamu pozostávajúci z jedného alebo dvoch znakov, po ktorých nasleduje bodka. Ďalšie tri znaky označujú príslušné číslo poľa a nasleduje po nich dvojbodka. Za dvojbodkou sa nachádzajú opisné informácie vo formáte ASCII alebo údaje o obrázku.

V logických záznamoch typu 1 a 2 sa môžu nachádzať len textové dátové polia vo formáte ASCII. V každom type takéhoto záznamu sa ako prvé pole vo formáte ASCII zaznamená úplná dĺžka záznamu (vrátane čísel polí, bodkočiariok a separátorov). Kontrolný znak separátora ASCII poľa „FS“ (ktorý znamená koniec logického záznamu alebo transakcie) nasleduje po poslednom bajte informácie vo formáte ASCII a zahrnie sa do dĺžky záznamu.

Na rozdiel od konceptu poľa ohraničeného tagmi obsahuje záznam typu 4 len binárne údaje zaznamenané ako usporiadané binárne polia s pevnou dĺžkou. Celá dĺžka záznamu sa zaznamená v prvom štvorbajtovom binárnom poli každého záznamu. Pri tomto binárnom zázname sa nezaznamenáva ani číslo záznamu s bodkou, ani číslo identifikátora poľa a nasledujúca dvojbodka. Okrem toho v dôsledku skutočnosti, že všetky polia v tomto zázname majú buď pevnú, alebo vymedzenú dĺžku, sa každý zo štyroch separátorov (US, RS, GS ani FS) môže interpretovať len ako binárny údaj. Znak FS sa pri binárnom zázname nesmie použiť ako separátor ani ako označenie ukončenia transakcie.

## 3. Logický záznam typu 1: Hlavička súboru

Prostredníctvom tohto záznamu sa opisuje štruktúra súboru, jeho typ a iné dôležité informácie. Súbor znakov používaných pre polia typu 1 obsahuje len 7-bitový ANSI kód na výmenu informácií.

### 3.1. Polia pre logický záznam typu 1

#### 3.1.1 Pole 1.001: Dĺžka logického záznamu (LEN – Logical Record Length)

Toto pole obsahuje informáciu o celkovom počte bajtov v celom logickom zázname typu 1. Pole sa začína kódom „1.001:“, po ktorom nasleduje celková dĺžka záznamu vrátane každého znaku každého poľa a separátorov informácií.

### 3.1.2. Pole 1.002: Číslo verzie (VER – Version Number)

Toto štvorbajtové pole konkretizuje číslo verzie normy ANSI/NIST, ktorú použil softvér alebo systém, pomocou ktorého sa vytvoril predmetný súbor, aby sa zabezpečilo, že používatelia vedia, ktorá verzia uvedenej normy sa používa. Prvé dva bajty špecifikujú referenčné číslo hlavnej verzie, druhé dva číslo jej menšej revízie. Napríklad pôvodná norma z roku 1986 sa považuje za prvú verziu a dostane označenie „0100“, zatiaľ čo súčasná norma ANSI/NIST-ITL 1-2000 sa označuje „0300“.

### 3.1.3. Pole 1.003: Obsah poľa (CNT – File Content)

V tomto poli sa nachádza zoznam záznamov v súbore usporiadaný podľa typu a poradia, v ktorom sa tieto záznamy v logickom súbore objavujú. Pozostáva z jedného alebo viacerých podpolí, z ktorých každé naopak obsahuje dve informácie opisujúce jeden logický záznam, ktorý sa nachádza v danom súbore. Takéto podpolia sa vkladajú v rovnakom poradí, v akom sa záznamy zaznamenávajú a prenášajú.

Prvá informácia v prvom podpoli je „1“ a odkazuje na to, že ide o záznam typu 1. Nasleduje za ňou druhá informácia, ktorá pozostáva z počtu ďalších záznamov v danom súbore. Tento počet sa rovná počtu ostávajúcich podpolí poľa 1.003.

Každé z ostávajúcich podpolí sa spája s jedným záznamom v súbore a poradie podpolí zodpovedá poradiu záznamov. Každé podpole obsahuje dve informácie. Prvou je identifikácia typu záznamu, druhou IDC záznamu. Na oddelenie týchto informácií sa používa separátor „US“.

### 3.1.4. Pole 1.004: Typ transakcie (TOT – Type of Transaction)

Toto pole obsahuje trojpísmenovú skratku, ktorou sa označuje typ transakcie. Tieto kódy sa môžu líšiť od kódov, ktoré sa používajú pri inom uplatňovaní normy ANSI/NIST.

CPS: vyhľadávanie odtlačkov súvisiacich s trestnou činnosťou (Criminal Print-to-Print Search). Táto transakcia je žiadosťou o vyhľadanie záznamu, ktorý sa týka trestného činu, v rámci databázy odtlačkov. Odtlačky sa v súbore musia nachádzať ako obrázky komprimované algoritmom WSQ.

V prípade NEGATÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2.

V prípade POZITÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2,
- 1 až 14 záznamov typu 4.

Typ transakcie CPS je zhrnutý v tabuľke A.6.1 (v dodatku 6).

PMS: vyhľadávanie v databáze skrytých obrazcov (Print-to-Latent Search). Táto transakcia sa použije v prípade, ak sa súbor odtlačkov pri vyhľadávaní porovnáva s databázou neidentifikovaných skrytých obrazcov. Odpoveď bude obsahovať pozitívny/negatívny výsledok vyhľadávania v cieľovom automatizovanom systéme identifikácie odtlačkov. Ak sa nájde viac neidentifikovaných skrytých obrazcov, vráti sa niekoľko transakcií SRE, pričom v každej sa bude nachádzať jeden obrázok. Odtlačky sa v súbore musia nachádzať ako obrázky komprimované algoritmom WSQ.

V prípade NEGATÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2.

V prípade POZITÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2,
- 1 záznam typu 13.



Typ transakcie PMS je zhrnutý v tabuľke A.6.1 (v dodatku 6).

MPS: vyhľadávanie skrytých obrazcov v databáze odtlačkov (Latent-to-Print Search). Táto transakcia sa používa pri vyhľadávaní latentného obrazca v databáze odtlačkov prstov. V súbore sa musia nachádzať informácie o markantoch latentného obrazca a obrázok (komprimovaný algoritmom WSQ).

V prípade NEGATÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2.

V prípade POZITÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2,
- 1 záznam typu 4 alebo typu 15

Typ transakcie MPS je zhrnutý v tabuľke A.6.4 (v dodatku 6).

MMS: vyhľadávanie skrytých obrazcov v databáze skrytých obrazcov (Latent-to-Latent Search). Pri tejto transakcii sa v súbore nachádza skrytý obrazec, ktorý sa má porovnávať s databázou neidentifikovaných skrytých obrazcov, aby sa zistila spojitosť medzi rôznymi miestami činu. V súbore sa musia nachádzať informácie o markantoch latentného obrazca a obrázok (komprimovaný algoritmom WSQ).

V prípade NEGATÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2.

V prípade POZITÍVNEHO výsledku vyhľadávania sa vrátia tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2,
- 1 záznam typu 13.

Typ transakcie MMS je zhrnutý v tabuľke A.6.4 (v dodatku 6).

SRE: Túto transakciu vracia agentúra určenia ako reakciu na daktyloskopické informácie. Odpoveď bude obsahovať pozitívny/negatívny výsledok vyhľadávania v cieľovom automatizovanom systéme identifikácie odtlačkov. Ak sa nájde viac kandidátov, vráti sa niekoľko transakcií SRE, pričom v každej sa bude nachádzať jeden kandidát.

Typ transakcie SRE je zhrnutý v tabuľke A.6.2 (v dodatku 6).

ERR: Túto transakciu vracia cieľový AFIS ako označenie chyby v transakcii. Obsahuje pole so správou (ERM), v ktorej sa oznamuje zistená chyba. Vráti sa tieto logické záznamy:

- 1 záznam typu 1,
- 1 záznam typu 2.

Typ transakcie ERR je zhrnutý v tabuľke A.6.3 (v dodatku 6).

Tabuľka 2: Povolené kódy v transakciách

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	—

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Kľúč:

- M = povinné (Mandatory),  
 M\* = môže sa použiť len jeden z dvoch typov záznamov,  
 O = nepovinné (Optional),  
 C = závisí od dostupnosti údajov (Conditional),  
 — = nie je povolené,  
 1\* = závisí od pôvodných systémov.

### 3.1.5. Pole 1.005: Dátum transakcie (DAT – Date of Transaction)

Toto pole označuje dátum začatia transakcie a musí zodpovedať štandardnému tvaru ISO: RRRRMMDD,

v ktorom RRRR je rok, MM je mesiac a DD je deň v mesiaci. Pri dátumoch s jednou číslicou sa používa úvodná nula. Napríklad tvar „19931004“ znamená 4. októbra 1993.

### 3.1.6. Pole 1.006: Priorita (PRY – Priority)

V tomto nepovinnom poli sa určuje priorita žiadosti na stupnici od 1 po 9. Číslo 1 sa označuje najvyššia priorita, číslom 9 najnižšia. Transakcie s prioritou 1 sa spracúvajú bezodkladne.

### 3.1.7. Pole 1.007: Identifikátor agentúry určenia (DAI – Destination Agency Identifier)

V tomto poli sa pre transakciu špecifikuje agentúra určenia.

Pozostáva z dvoch informácií v tomto formáte: CC/agency.

Prvá informácia obsahuje kód krajiny (Country Code) vymedzený v norme ISO 3166, ktorý pozostáva z dvoch alfanumerických znakov. Druhá informácia, agency (agentúra), je voliteľný text na identifikáciu agentúry obsahujúci najviac 32 alfanumerických znakov.

### 3.1.8. Pole 1.008: Identifikátor agentúry pôvodu (ORI – Originating Agency Identifier)

V tomto poli sa špecifikuje pôvodca súboru, a to v rovnakom formáte ako DAI (pole 1.007).

### 3.1.9. Pole 1.009: Kontrolné číslo transakcie (TCN – Transaction Control Number)

Kontrolné číslo na referenčné účely. Mal by ho generovať počítač a malo by mať tento formát: RRSSSSSSSA,

kde RR je rok transakcie, SSSSSSSS je osemmiestne sériové číslo a A je kontrolný znak vytvorený podľa postupu v dodatku 2.

Ak TCN neexistuje, pole RRSSSSSSSS sa vyplní nulami a kontrolný znak sa vytvorí postupom opísaným vyššie.

### 3.1.10. Pole 1.010: Kontrolná odpoveď transakcie (TCR – Transaction Control Response)

Ak je predmetný súbor odpoveďou na žiadosť, toto nepovinné pole bude obsahovať kontrolné číslo transakcie žiadosti. Preto má rovnaký formát ako TCN (pole 1.009).

### 3.1.11. Pole 1.011: Pôvodné skenovanie rozlíšenie (NSR – Native Scanning Resolution)

V tomto poli sa špecifikuje bežné skenovanie rozlíšenie systému, ktorý podporuje pôvodca transakcie. Rozlíšenie sa vymedzuje vo formáte dve číslice, desatinná čiarka a ďalšie dve číslice.

Pri všetkých transakciách podľa rozhodnutia 2008/615/SVV by mal byť pomer pri rozlíšení vzoriek 500 pixelov/palec alebo 19,68 pixelu/mm.

3.1.12. Pole 1.012: Nominálne rozlíšenie pri prenose (NTR – Nominal Transmitting Resolution)

V tomto päťbajtovom poli sa špecifikuje nominálne rozlíšenie prenášaných obrázkov. Rozlíšenie sa vyjadruje v pixeloch/mm v rovnakom formáte ako pri NSR (pole 1.011).

3.1.13. Pole 1.013: Názov domény (DOM – Domain name)

V tomto povinnom poli sa určuje názov domény na implementáciu logických záznamov typu 2, ktoré definuje používateľ. Obsahuje dve informácie a má formát „INT-I{US}4.22{GS}“.

3.1.14. Pole 1.014: Greenwichský čas (GMT – Greenwich Mean Time)

Toto povinné pole poskytuje mechanizmus na vyjadrenie dátumu a času v univerzálnych jednotkách stredného greenwichského času (GMT). V prípade použitia obsahuje pole GMT univerzálny dátum, ktorý bude doplnkom miestneho dátumu uvedeného v poli 1.005 (DAT). Využitím poľa GMT sa odstráni nezhoda v miestnych časoch, ktoré sa vyskytujú v prípade, ak sa transakcia a odpoveď prenášajú medzi dvoma miestami oddelenými niekoľkými časovými pásmami. Pole GMT poskytuje univerzálny dátum a 24-hodinový svetový čas nezávisle od časových pásiem. Funguje vo formáte „CCRRMMDDHHMMSSZ“, pričom tento 15-znakový reťazec je vytvorený spojením dátumu a GMT a zakončený písmenom Z. Znaky „CCRR“ predstavujú rok transakcie, „MM“ desiatkové a jednotkové hodnoty mesiaca, „DD“ rovnaké hodnoty dňa, „HH“ zastupujú hodinu, „MM“ minútu a „SS“ sekundu. Úplný dátum nesmie byť neskorší, ako je aktuálny dátum.

4. **Logický záznam typu 2: Opisný text**

Štruktúra väčšiny tohto záznamu sa v pôvodnej norme ANSI/NIST nedefinuje. Obsahuje informácie, ktoré môžu byť konkrétne zaujímavé pre odosielačicu a prijímačicu agentúru. Na zabezpečenie kompatibility komunikujúcich daktyloskopických systémov sa vyžaduje, aby sa v záznamoch nachádzali iba polia, ktoré sú uvedené nižšie. V tomto dokumente sa upresňuje, ktoré polia sú povinné a ktoré nepovinné, a vymedzuje sa v ňom štruktúra jednotlivých polí.

4.1. Polia pre logický záznam typu 2

4.1.1. Pole 2.001: Dĺžka logického záznamu (LEN – Logical Record Length)

V tomto povinnom poli sa uvádza dĺžka daného záznamu typu 2 a celkový počet bajtov vrátane každého znaku každého poľa v zázname a separátorov informácií.

4.1.2. Pole 2.002: Znak označenia obrázku (IDC – Image Designation Character)

IDC v tomto povinnom poli je zobrazením IDC definovaného v poli obsah súboru (CNT) záznamu typu 1 (pole 1.003), a to vo formáte ASCII.

4.1.3. Pole 2.003: Systémové informácie (SYS – System Information)

Toto pole je povinné a obsahuje štyri bajty, ktoré označujú verziu INT-I, s ktorou je daný záznam typu 2 v súlade.

Prvé dva bajty špecifikujú číslo hlavnej verzie, druhé dva číslo jej menšej revízie. Napríklad, táto implementácia vychádza z verzie 4 revízie 22 INT-I, a preto bude označená kódom „0422“.

4.1.4. Pole 2.007: Číslo prípadu (CNO – Case Number)

Číslo, ktoré miestny daktyloskopický úrad prideliť zbierke skrytých obrazcov nájdených na mieste činu. Prijal sa tento formát: CC/number,

kde CC je kód krajiny v databáze Interpolu s dĺžkou dvoch alfanumerických znakov a number (číslo) sa riadi podľa príslušných miestnych usmernení, pričom môže mať až 32 alfanumerických znakov.

Toto pole umožňuje systému identifikovať latentné obrazce spojené s konkrétnym trestným činom.

**4.1.5. Pole 2.008: Číslo sekvencie (SQN – Sequence Number)**

Toto číslo špecifikuje každú sekvenciu skrytých obrazcov v rámci prípadu a môže byť až štvormiestne. Sekvencia je skrytý obrazec alebo súbor skrytých obrazcov, ktoré sú spojené na účely archivácie a/alebo vyhľadávania. Z tejto definície vyplýva, že číslo sekvencie treba prideliť každému jednotlivému latentnému obrazcu.

Toto pole sa spolu s MID (pole 2.009) môže využiť na identifikáciu konkrétneho latentného obrazca v rámci sekvencie.

**4.1.6. Pole 2.009: Identifikátor latentného obrazca (MID – Latent Identifier)**

Toto pole špecifikuje jednotlivé latentné obrazce v rámci sekvencie. Jeho hodnota je jedno alebo dve písmená, pričom „A“ sa prideluje prvému latentnému obrazcu, „B“ druhému a tak ďalej až po „ZZ“. Toto pole sa využíva analogicky ako číslo sekvencie pri skrytých obrazcoch uvedených v opise poľa SQN (pole 2.008).

**4.1.7. Pole 2.010: Trestné referenčné číslo (CRN)**

Toto jedinečné referenčné číslo prideluje vnútroštátna agentúra osobe, ktorá je po prvýkrát obvinená zo spáchania trestného činu. V jednej krajine nemôže mať tá istá osoba viac CRN, a taktiež nesmie mať rovnaké CRN ako iná osoba. Rovnaká osoba však môže mať rôzne trestné referenčné čísla v iných krajinách, pričom na ich rozlíšenie slúži kód krajiny.

Pre pole CRN sa prijal tento formát: CC/number,

kde CC je kód krajiny v norme ISO 3166 s dĺžkou dvoch alfanumerických znakov a number (číslo) sa riadi podľa príslušných vnútroštátnych usmernení agentúry pôvodu, pričom môže mať až 32 alfanumerických znakov.

Pri transakciách v súlade s rozhodnutím 2008/615/SVV sa bude toto pole používať na zapísanie vnútroštátneho trestného referenčného čísla agentúry pôvodu, ktoré je spojené s obrázkami v záznamoch typu 4 alebo typu 15.

**4.1.8. Pole 2.012: Neurčené identifikačné číslo (MN1 – Miscellaneous Identification Number)**

Toto pole obsahuje CRN (pole 2.010) prenesené prostredníctvom transakcie CPS alebo PMS bez úvodného kódu krajiny.

**4.1.9. Pole 2.013: Neurčené identifikačné číslo (MN2 – Miscellaneous Identification Number)**

Toto pole obsahuje CNO (pole 2.007) prenesené prostredníctvom transakcie MPS alebo MMS bez úvodného kódu krajiny.

**4.1.10. Pole 2.014: Neurčené identifikačné číslo (MN3 – Miscellaneous Identification Number)**

Toto pole obsahuje SQN (pole 2.008) prenesené prostredníctvom transakcie MPS alebo MMS

**4.1.11. Pole 2.015: Neurčené identifikačné číslo (MN4 – Miscellaneous Identification Number)**

Toto pole obsahuje MID (pole 2.009) prenesené prostredníctvom transakcie MPS alebo MMS

**4.1.12. Pole 2.063: Ďalšie informácie (INF – Additional Information)**

V prípade transakcie SRE na základe žiadosti PMS sa v tomto poli nachádzajú informácie o prste, ktorý znamenal POZITÍVNY výsledok vyhľadávania. Formát poľa je:

NN, kde NN je dvojmiestny numerický kód pozície prsta podľa definície v tabuľke 5.

Vo všetkých ostatných prípadoch je toto pole nepovinné. Pozostáva z 32 alfanumerických znakov a môže poskytovať dodatočné informácie týkajúce sa žiadosti.

**4.1.13. Pole 2.064: Zoznam respondentov (RLS – Respondents List)**

Toto pole obsahuje aspoň dve podpolia. Prvé z nich opisuje typ vykonaného vyhľadávania, a to pomocou trojpísmenovej skratky, ktorou sa špecifikuje typ transakcie v poli TOT (pole 1.004). Druhé podpole obsahuje jeden znak. Znak „I“ sa používa na označenie POZITÍVNEHO výsledku vyhľadávania, zatiaľ čo v opačnom prípade (NEGATÍVNY výsledok vyhľadávania) sa použije znak „N“. Tretie podpole obsahuje identifikátor sekvencie pre výsledky kandidátov a celkový počet kandidátov, pričom tieto dve informácie sú oddelené lomkou. V prípade viacerých kandidátov sa vráti viac správ.

V prípade potenciálneho POZITÍVNEHO výsledku vyhľadávania obsahuje štvrté podpole refazec z najviac šiestich číslic. Ak sa POZITÍVNY výsledok vyhľadávania overil, hodnota tohto poľa sa definuje ako „999999“.

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

Ak vzdialený AFIS neprideľuje skóre, na príslušnom mieste sa zapíše nula.

#### 4.1.14. Pole 2.074: Pole správy o stave/chybe (ERM)

Toto pole obsahuje chybové správy vyplývajúce z transakcií, ktoré sa budú zasielať späť žiadateľovi ako súčasť chybových transakcií.

Tabuľka 3: Chybové správy

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.

Chybové správy od 100 do 199:

Tieto chybové správy sa týkajú overenia záznamov ANSI/NIST a sú definované ako:

<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>...

kde

- „error\_code“ je kód, ktorý sa vzťahuje výlučne na konkrétny dôvod (pozri tabuľku 3),
- „field\_id“ je číslo chybného poľa podľa ANSI/NIST (napr. 1.001, 2.001) vo formáte <record\_type>.field\_id>. <sub\_field\_id>,
- „dynamic text“ je podrobnejší dynamický opis chyby,
- „LF“ je znak posunu o riadok, ktorým sa oddeľujú viaceré chyby,
- pre záznamy typu 1 sa ICD definuje ako „-1“.

Príklad:

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

Toto pole je pre chybové transakcie povinné.

#### 4.1.15. Pole 2.320: Očakávaný počet kandidátov (ENC – Expected Number of Candidates)

Toto pole obsahuje najvyšší počet kandidátov na overenie, ktorý očakáva žiadajúca agentúra. Hodnota ENC nesmie prekročiť hodnoty vymedzené v tabuľke 11.

### 5. **Logický záznam typu 4: Obrázok v odtieňoch šedej s vysokým rozlíšením**

Malo by sa pripomenúť, že záznamy typu 4 sú vo svojej podstate skôr binárne než ASCII. Preto má každé pole v zázname pridelenú konkrétnu pozíciu, z čoho vyplýva, že všetky polia sú povinné.

Norma umožňuje, aby sa v rámci záznamu špecifikovala veľkosť i rozlíšenie obrázku. Vyžaduje si, aby logické záznamy typu 4 obsahovali údaje o daktyloskopických obrázkoch, ktoré sa prenášajú pri nominálnej hustote od 500 do 520 pixelov na palec. Uprednostňovaný pomer pri nových obrázkoch je 500 pixelov na palec alebo 19,68 pixelu na milimeter. Hustota vymedzená v INT-I je 500 pixelov na palec, ale podobné systémy môžu medzi sebou komunikovať pri inom pomere, v rámci rozmedzia od 500 do 520 pixelov na palec.

#### 5.1. Polia pre logický záznam typu 4

##### 5.1.1. Pole 4.001: Dĺžka logického záznamu (LEN – Logical Record Length)

V tomto štvorbajtovom poli sa uvádza dĺžka daného záznamu typu 4 a celkový počet bajtov vrátane každého bajtu každého poľa v zázname.

##### 5.1.2. Pole 4.002: Znak označenia obrázku (IDC – Image Designation Character)

Binárna forma čísla IDC v hlavičke s veľkosťou jedného bajtu.

##### 5.1.3. Pole 4.003: Typ zobrazenia (IMP – Impression Type)

Typ zobrazenia je pole s veľkosťou jedného bajtu, ktoré sa nachádza na šiestom bajte záznamu.

Tabuľka 4: Typ zobrazenia odtlačku

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
4	Latent impression captured directly
5	Latent tracing



Code	Description
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

#### 5.1.4. Pole 4.004: Poloha prsta (FGP – Finger Position)

Toto pole s pevnou dĺžkou šiestich bajtov sa nachádza na siedmom až dvanástom bajte záznamu typu 4. Obsahuje možné polohy prstov začínajúc od bajtu najviac vľavo (siedmy bajt záznamu). Známa alebo najpravdepodobnejšia poloha prsta sa vyberá z tabuľky 5. Vložením polohy ďalších prstov v rovnakom formáte sa v rámci ostávajúcich piatich bajtov môže odkázať až na ďalších päť prstov. Ak sa má použiť odkaz na menej než päť polôh prsta, nevyužívané bajty sa vyplnia binárnym číslom 255. Na neznámu polohu prsta sa pri všetkých prstoch používa kód 0.

Tabuľka 5: Kód polohy prsta a maximálna veľkosť

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

Pre latentné obrázky z miesta činu sa používajú len kódy 0 až 10.

#### 5.1.5. Pole 4.005: Rozlíšenie skenovaného obrázku (ISR – Image Scanning Resolution)

Toto jednobajtové pole sa nachádza na 13. bajte záznamu typu 4. Ak obsahuje nulu („0“), potom sa vzorka skenovala pri uprednostňovanom skenovanom pomere 19,68 pixelu/mm (500 pixelov na palec). Ak obsahuje jednotku („1“), potom sa vzorka skenovala pri alternatívnom skenovanom pomere vymedzenom pri zázname typu 1.

#### 5.1.6. Pole 4.006: Dĺžka horizontálnej línie (HLL – Horizontal Line Length)

Toto pole sa nachádza na 14. a 15. bajte záznamu typu 4. Uvádza počet pixelov na každej skenovacej línii. Najdôležitejší bude prvý bajt.

## 5.1.7. Pole 4.007: Dĺžka vertikálnej línie (VLL – Vertical Line Length)

Toto pole sa nachádza na 16. a 17. bajte a zaznamenáva sa v ňom počet skenovaných línií na obrázku. Najdôležitejší je prvý bajt.

## 5.1.8. Pole 4.008: Algoritmus kompresie odtieňov šedej (GCA – Gray-scale Compression Algorithm)

Toto jednobajtové pole špecifikuje algoritmus kompresie odtieňov šedej, ktorý sa použil na šifrovanie údajov o obrázku. Binárny kód 1 znamená (na účely tejto aplikácie), že sa použila kompresia WSQ (dodatok 7).

## 5.1.9. Pole 4.009: Obrázok

Toto pole obsahuje bajtový tok, ktorý predstavuje obrázok. Jeho štruktúra bude zjavne závisieť od použitého kompresného algoritmu.

6. **Logický záznam typu 9: Záznam o markantoch**

Záznamy typu 9 obsahujú text vo formáte ASCII, ktorým sa opisujú markanty a súvisiace informácie odšifrované zo latentného obrazca. Pri vyhľadávaní medzi skrytými obrázkami je počet takýchto záznamov v súbore neobmedzený, pričom každý záznam sa musí týkať iného pohľadu alebo obrazca.

## 6.1. Výber markantov

## 6.1.1. Identifikácia typu markanta

Touto normou sa definujú tri identifikačné čísla, ktoré sa používajú na opis typu markanta. Uvádzajú sa v tabuľke 6. Koniec papilárnej línie sa označí ako typ 1. Rozdvojenie sa označí ako typ 2. Ak sa markant nedá jasne začleniť medzi tieto dva typy, označí sa ako „iné“, čiže typ 0.

Tabuľka 6: Typy markantov

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

## 6.1.2. Umiestnenie a typ markanta

Kvôli dodržaniu súladu šablón s oddielom 5 normy ANSI INCITS 378-2004 sa na určenie umiestnenia (polohy a smeru uhla) jednotlivých markantov použije nasledujúca metóda, ktorou sa rozširuje platná norma INCITS 378-2004.

Poloha alebo umiestnenie markantu, ktorým je zakončenie papilárnej línie, je miesto rozvetvenia centrálného skeletu priestoru papilárnej brázdy presne pred zakončením danej línie. Ak by sa tri vetvy papilárnej brázdy zúžili na skelet so šírkou jedného pixelu, polohou markantu je bod ich rozvetvenia. Podobne sa aj poloha markantu pri rozdvojení určí ako bod rozvetvenia centrálného skeletu papilárnej línie. Ak by sa tri vetvy papilárnej línie zúžili na skelet so šírkou jedného pixelu, polohou markantu je bod ich rozvetvenia.

Po konverzii všetkých zakončení papilárnych línií na rozdvojenia sú všetky markanty daktyloskopického obrazca zastúpené ako rozdvojenia. Súradnice bodu rozvetvenia troch vetiev každého markantu na osi x a y (v pixeloch) sa dajú priamo formátovať. Z každého rozdvojenia skeletu sa dá priamo určiť smer markantu. Tri vetvy každého rozdvojenia skeletu sa musia preskúmať v bode zakončenia každej určenej vetvy. Na obrázku 6.1.2 sú zobrazené tri použité metódy na určenie konca vetvy pri skenovanom rozlíšení 500 ppi.

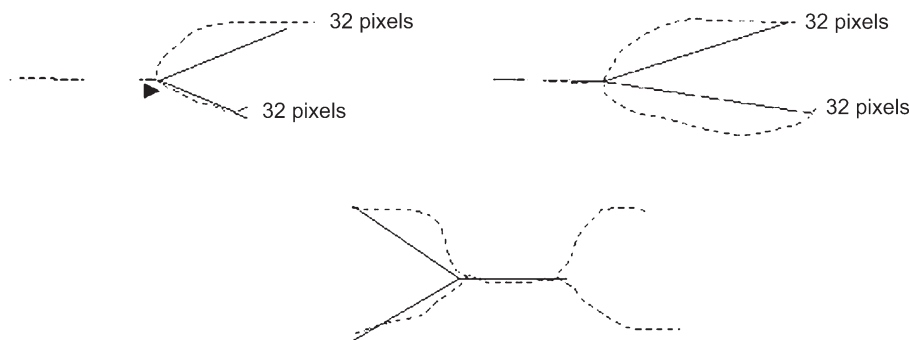
Zakončenie sa určuje podľa následnosti udalostí. Počet pixelov vychádza z rozlíšenia 500 ppi. Z iných rozlíšení bude vyplývať iný počet pixelov.

— Vzdialenosť 0,064" (32. pixel),

— zakončenie vetvy skeletu vo vzdialenosti od 0,02" do 0,064" (od 10. do 32. pixela) kratšie vetvy sa nepoužívajú,

— druhé rozdvojenie sa nachádza vo vzdialenosti do 0,064" (pred 32. pixelom).

Obrázok 6.1.2



Uhol markantu sa určuje na základe vytvorenia troch virtuálnych lúčov vybiehajúcich z bodu rozdvojenia smerom k zakončeniu každej z vetiev. Najmenší z troch uhlov, ktoré tieto lúče vytvoria, sa rozdelia na polovicu, čím sa určí smer markantu.

#### 6.1.3. Súradnicový systém

Na vyjadrenie polohy markanta sa použije karteziánsky súradnicový systém. Polohu markantov zastupujú ich súradnice na osi x a y. Stred súradnicového systému sa nachádza v ľavom hornom rohu pôvodného obrázku, pričom kladná časť osi x smeruje vpravo a osi y nadol. Súradnice markanta na osi x aj y sú vyjadrené vo vzdialenosti od stredu v pixeloch. Malo by sa poznamenať, že poloha stredu a meracie jednotky nie sú v súlade s dohovorom použitým pri definíciách typu 9 v norme ANSI/NIST-ITL 1-2000.

#### 6.1.4. Smer markantov

Uhly sa vyjadrujú v štandardnom matematickom formáte s nulou vpravo a uhlom rastúcim proti smeru hodinových ručičiek. Zaznamenané uhly sú pri zakončení papilárnej línie v smere dozadu od jej konca a popri nej a pri rozdvojení smerom k stredu papilárnej brázdy. Tento dohovor sa od dohovoru o uhloch vo vymedzeniach pre typ 9 normy ANSI/NIST-ITL 1-2000 líši o 180 stupňov.

### 6.2. Polia pre logický záznam typu 9 vo formáte INCITS-378

Všetky polia v záznamoch typu 9 sa zaznamenávajú ako text ASCII. V týchto záznamoch polí označených tagmi nie sú povolené žiadne binárne polia.

#### 6.2.1. Pole 9.001: Dĺžka logického záznamu (LEN – Logical Record Length)

V tomto povinnom poli vo formáte ASCII sa uvádza dĺžka logického záznamu s celkovým počtom bajtov vrátane každého znaku každého poľa v zázname.

#### 6.2.2. Pole 9.002: Znak označenia obrázku (IDC – Image Designation Character)

Toto povinné dvojbajtové pole sa používa na identifikáciu a určenie polohy údajov o markantoch. Znak označenia obrázku v tomto poli je rovnaký ako IDC v poli obsah súboru v zázname typu 1.

#### 6.2.3. Pole 9.003: Typ zobrazenia (IMP – Impression Type)

Týmto povinným jednobajtovým poľom sa opisuje spôsob, akým sa získala informácia vo forme daktyloskopického obrázku. Vloží sa doň hodnota ASCII príslušného kódu z tabuľky 4, ktorá vyjadruje typ zobrazenia.

#### 6.2.4. Pole 9.004: Formát markanta (FMT – Minutiae Format)

Toto pole obsahuje znak „U“, aby sa uviedlo, že markanty sa formátujú podľa normy M1-378. Napriek tomu, že informácie môžu byť zašifrované v súlade s uvedenou normou, všetky dátové polia záznamu typu 9 musia ostať vo formáte textových polí ASCII.

#### 6.2.5. Pole 9.126: Informácie CBEFF (Common Biometric Exchange File Format)

Toto pole obsahuje tri informácie. Prvá položka obsahuje hodnotu „27“ (0x1B). Táto hodnota vyjadruje totožnosť vlastníka formátu CBEFF, ktorú pridelo Medzinárodné združenie biometrických odvetví (IBIA) technickému výboru M1 INCITS. Kódom <US> sa táto položka oddeľuje od typu formátu CBEFF, ktorý má hodnotu „513“ (0x0201) na označenie, že tento záznam obsahuje len údaje o polohe a smere uhla bez informácií v rozšírenom

dátovom bloku. Kódom <US> sa táto informácia oddelí aj od identifikátora produktu CBEFF (PID), ktorým sa určuje „vlastník“ šifrovacieho vybavenia. Túto hodnotu určí predajca. V prípade, že bola zverejnená, sa dá zistiť na webovej stránke IBIA ([www.ibia.org](http://www.ibia.org)).

6.2.6. Pole 9.127: Identifikácia vybavenia na odber vzoriek

Toto pole obsahuje dve informácie oddelené separátorom <US>. Prvé obsahuje kód „APPF“ v prípade, že pôvodne použité vybavenie na získanie obrázku malo osvedčenie zhody potvrdzujúce súlad s dodatkom F (IAFIS Image Quality Specification, 29. januára 1999) špecifikácie FBI na elektronický prenos odtlačkov prstov CJIS-RS-0010. Ak takéto osvedčenie neexistovalo, pole bude obsahovať hodnotu „NONE“. Druhá informácia obsahuje identifikačné číslo vybavenia na odber vzoriek, čo je evidenčné číslo vybavenia, ktoré prideliť predajca. Hodnota „0“ znamená, že identifikačné číslo nebolo nahlásené.

6.2.7. Pole 9.128: Dĺžka horizontálnej línie (HLL – Horizontal Line Length)

Toto povinné pole vo formáte ASCII obsahuje počet pixelov na jednej horizontálnej línii prenášaného obrázku. Maximálna horizontálna veľkosť je obmedzená na 65 534 pixelov.

6.2.8. Pole 9.129: Dĺžka vertikálnej línie (VLL – Vertical Line Length)

Toto povinné pole vo formáte ASCII obsahuje počet horizontálnych línii na prenášanom obrázku. Maximálna vertikálna veľkosť je obmedzená na 65 534 pixelov.

6.2.9. Pole 9.130: Jednotky zobrazenia (SLC – Scale Units)

Toto povinné pole vo formáte ASCII obsahuje jednotky, v ktorých sa opisuje vzorkovacia frekvencia obrázku (hustota pixelov). Jednotka („1“) v tomto poli znamená pixely na palec, zatiaľ čo dvojka („2“) označuje pixely na centimeter. Nula („0“) v tomto poli označuje, že sa nezadala žiadna stupnica. V tomto prípade sa zobrazovací pomer v pixeloch udáva na základe podielu HPS/VPS.

6.2.10. Pole 9.131: Horizontálny rozsah v pixeloch (HPS)

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov v horizontálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje horizontálnu zložku pomeru zobrazenia v pixeloch.

6.2.11. Pole 9.132: Vertikálny rozsah v pixeloch (VPS)

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov vo vertikálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje vertikálnu zložku pomeru zobrazenia v pixeloch.

6.2.12. Pole 9.133: Zobrazenie odtlačku prsta

Toto povinné pole obsahuje číslo zobrazenia odtlačku prsta spojeného s údajmi v tomto zázname. Číslo zobrazenia začína nulou („0“) a rastie po jednej až do „15“.

6.2.13. Pole 9.134: Poloha prsta (FGP – Finger Position)

Toto pole obsahuje kód, ktorým sa označuje poloha prsta, z ktorej vyplynuli informácie v danom zázname typu 9. Na označenie tejto polohy prsta alebo dlane sa zvolí kód medzi 1 a 10 z tabuľky 5 alebo príslušný kód dlane z tabuľky 10.

6.2.14. Pole 9.135: Kvalita odtlačku prsta

Pole uvádza celkovú kvalitu údajov o markantoch a jeho hodnota je od 0 do 100. Toto číslo vyjadruje celkovú kvalitu záznamu odtlačku prsta a spája kvalitu pôvodného obrázku, výberu markantov a všetkých dodatočných operácií, ktoré mohli ovplyvniť záznam o markantoch.

6.2.15. Pole 9.136: Počet markantov

Toto povinné pole obsahuje výpočet markantov v predmetnom logickom zázname.

## 6.2.16. Pole 9.137: Údaje o markantoch odtlačku

Toto povinné pole obsahuje šesť informácií oddelených separátorom <US>. Pozostáva z niekoľkých podpolí, pričom každé z nich obsahuje podrobnosti o jednom markante. Celkový počet podpolí s markantmi musí zodpovedať počtu v poli 136. Prvá informácia je indexový počet markantov, ktorý začína číslom „1“ a rastie o „1“ pri každom ďalšom markante na odtlačku prsta. Druhou a treťou informáciou sú súradnice znaku v pixeloch na osi x a y. Štvrtá informácia vyjadruje uhol markanta v jednotkách s dvojstupňovým rozlíšením. Táto hodnota je nezáporné číslo od 0 do 179. Piatou informáciou je typ markanta. Hodnota „0“ zastupuje markant typu „INÉ“, hodnota „1“ je zakončenie papilárnej línie a hodnota „2“ je rozdvojenie papilárnej línie. Šiestou informáciou je kvalita každého markanta. Táto hodnota je v rozmedzí od 1 (najnižšia kvalita) do 100 (najvyššia kvalita). Hodnota „0“ znamená, že informácia o kvalite nie je dostupná. Každé podpole musí byť od ďalšieho oddelené separátorom <RS>.

## 6.2.17. Pole 9.138: Informácia o počte papilárnych línií

Toto pole je zložené zo súboru podpolí, z ktorých každé obsahuje tri informácie. Prvá informácia prvého podpoľa označuje metódu počítania papilárnych línií. Nula („0“) znamená, že nie je možné zistiť metódu sčítania papilárnych línií ani ich poradie v zázname. Číslcia „1“ znamená že pri každom centrálnom markante sa údaje o počte papilárnych línií zisťovali smerom k susednému markantu v štyroch kvadrantoch a údaje za centrálny markant sa uvádzajú spoločne. Číslcia „2“ znamená že pri každom centrálnom markante sa údaje o počte papilárnych línií zisťovali smerom k susednému markantu v ôsmich oktantoch a údaje za centrálny markant sa uvádzajú spoločne. Zvyšné dve informácie prvého podpoľa obsahujú obe nulu („0“). Informácie sa oddeľujú separátorom <US>. Následné podpolia budú obsahovať indexový počet centrálnych markantov ako prvú informáciu, indexový počet susediacich markantov ako druhú informáciu a počet prekrížených papilárnych línií ako tretiu informáciu. Podpolia sa oddeľujú separátorom <RS>.

## 6.2.18. Pole 9.139: Informácie o jadre

Toto pole pozostáva z jedného podpoľa pre každé jadro, ktoré sa nachádza v pôvodnom obrázku. Každé podpole obsahuje tri informácie. Prvé dve informácie obsahujú súradnice na osi x a y v pixeloch. Tretia informácia obsahuje uhol jadra v dvojstupňových jednotkách. Táto hodnota je nezáporné číslo od 0 do 179. Viaceré jadrá sa oddelia separátorom <RS>.

## 6.2.19. Pole 9.140: Informácie o delte

Toto pole pozostáva z jedného podpoľa pre každú deltu, ktorá sa nachádza v pôvodnom obrázku. Každé podpole obsahuje tri informácie. Prvé dve informácie obsahujú súradnice na osi x a y v pixeloch. Tretia informácia obsahuje uhol delty v dvojstupňových jednotkách. Táto hodnota je nezáporné číslo od 0 do 179. Viaceré jadrá sa oddelia separátorom <RS>.

## 7. Logický záznam typu 13: Skrytý obrázok s rôznym rozlíšením

Logický záznam typu 13 s poliami ohraničenými tagmi obsahuje údaje vo forme obrázkov získané zo skrytých obrázkov. Tieto obrázky sú určené na prenos do agentúr, v ktorých sa z nich automaticky alebo prostredníctvom ľudského zásahu a spracovania získajú potrebné informácie.

Informácie, ktoré sa týkajú použitého skenovacieho rozlíšenia, veľkosti obrázku a iných parametrov vyžadovaných na spracovanie obrázku, sa v rámci záznamu nachádzajú vo forme polí ohraničených tagmi.

Tabuľka 7: Rozvrh záznamu typu 13: skrytý obrázok s rôznym rozlíšením

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

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
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	—	—	—	—	—	—
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	—

Kľúč k typu znakov: N = numerický, A = abecedný, AN = alfanumerický, B = binárny.

#### 7.1. Polia pre logický záznam typu 13

V nasledujúcich odsekoch sa opisujú údaje obsiahnuté v každom poli logického záznamu typu 13.

V rámci logických záznamov typu 13 sa vstupy robia do číslovaných polí. Vyžaduje sa usporiadanie prvých dvoch polí záznamu a pole obsahujúce údaje vo forme obrázku musí byť posledným fyzickým poľom v zázname. V tabuľke 7 sa pre každé pole v zázname typu 13 nachádza „stavový kód“ (buď „M“ označujúce povinné pole, alebo „O“ označujúce pole nepovinné), číslo poľa, typ znaku, veľkosť poľa a obmedzenie výskytu. V poslednom stĺpci sa nachádza maximálna veľkosť v bajtoch, ktorá vychádza z trojmiestneho čísla poľa. Ak sa v čísle poľa nachádza viac číslic, zvýši sa aj maximálny počet bajtov. Dve položky v stĺpci „veľkosť poľa pri každom výskyte“ zahŕňajú všetky separátory, ktoré sú v poli použité. Údaj v stĺpci „maximálny počet bajtov“ zahŕňa číslo poľa, informáciu a všetky separátory vrátane separátora „GS“.

##### 7.1.1. Pole 13.001: Dĺžka logického záznamu (LEN – Logical Record Length)

Toto povinné pole vo formáte ASCII obsahuje informáciu o celkovom počte bajtov v logickom zázname typu 13. Pole 13.001 špecifikuje dĺžku záznamu vrátane každého znaku každého poľa v zázname a separátorov.

##### 7.1.2. Pole 13.002: Znak označenia obrázku (IDC – Image Designation Character)

Toto povinné pole vo formáte ASCII sa používa na identifikáciu údajov vo forme latentného obrázku, ktoré sa nachádzajú v zázname. Tento IDC je rovnaký ako IDC v poli obsah súboru (CNT) v zázname typu 1.

##### 7.1.3. Pole 13.003: Typ zobrazenia (IMP – Impression Type)

Týmto povinným jednobajtovým alebo dvojbajtovým poľom vo formáte ASCII sa opisuje spôsob, akým sa získala informácia vo forme latentného obrázku. Do tohto poľa sa vloží príslušný kód latentného obrázku z tabuľky 4 (pri odtlačkoch prstov) alebo z tabuľky 9 (odtlačok dlane).

**7.1.4. Pole 13.004: Agentúra pôvodu/ORI (SRC – Source Agency)**

Toto povinné pole vo formáte ASCII obsahuje totožnosť správneho orgánu alebo organizácie, ktorá pôvodne získala obrázok v zázname. Za bežných okolností sa v tomto poli uvedie identifikátor agentúry pôvodu (ORI – Originating Agency Identifier) agentúry, ktorá získala obrázok. Pozostáva z dvoch informácií v tomto formáte: CC/agency.

Prvá informácia obsahuje kód krajiny v databáze Interpolu, ktorý pozostáva z dvoch alfanumerických znakov. Druhá informácia, agency (agentúra), je voliteľný text na identifikáciu agentúry obsahujúci najviac 32 alfanumerických znakov.

**7.1.5. Pole 13.005: Dátum získania latentného obrázku (LCD – Latent Capture Date)**

V tomto povinnom poli vo formáte ASCII sa uvádza dátum získania latentného obrázku, ktorý sa nachádza v zázname. Tento dátum sa uvádza ako osem číslíc vo formáte CCRRMMDD. CCRR je rok získania obrázku; znaky MM sú desiatkové a jednotkové hodnoty mesiaca a znaky DD zastupujú rovnaké hodnoty pri dni v danom mesiaci. Napríklad, dátum 20000229 znamená 29. februára 2000. Úplný dátum musí skutočne existovať.

**7.1.6. Pole 13.006: Dĺžka horizontálnej línie (HLL – Horizontal Line Length)**

Toto povinné pole vo formáte ASCII obsahuje počet pixelov na jednej horizontálnej línii prenášaného obrázku.

**7.1.7. Pole 13.007: Dĺžka vertikálnej línie (VLL – Vertical Line Length)**

Toto povinné pole vo formáte ASCII obsahuje počet horizontálnych línii na prenášanom obrázku.

**7.1.8. Pole 13.008: Jednotky zobrazenia (SLC – Scale Units)**

Toto povinné pole vo formáte ASCII obsahuje jednotky, v ktorých sa opisuje vzorkovacia frekvencia obrázku (hustota pixelov). Jednotka („1“) v tomto poli znamená pixely na palec, zatiaľ čo dvojka („2“) označuje pixely na centimeter. Nula („0“) v tomto poli označuje, že sa nezadala žiadna škála. V tomto prípade sa zobrazovací pomer v pixeloch udáva na základe podielu HPS/VPS.

**7.1.9. Pole 13.009: Horizontálny rozsah v pixeloch (HPS)**

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov v horizontálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje horizontálnu zložku pomeru zobrazenia v pixeloch.

**7.1.10. Pole 13.010: Vertikálny rozsah v pixeloch (VPS)**

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov vo vertikálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje vertikálnu zložku pomeru zobrazenia v pixeloch.

**7.1.11. Pole 13.011: Kompresný algoritmus (CGA – Compression Algorithm)**

V tomto povinnom poli ASCII sa špecifikuje algoritmus, ktorý sa používa na kompresiu obrázkov v odtieňoch šedej. Kompresné kódy sa nachádzajú v dodatku 7.

**7.1.12. Pole 13.012: Bity na pixel (BPX)**

Toto povinné pole vo formáte ASCII obsahuje počet bitov, ktoré predstavujú jeden pixel. Pri bežných hodnotách odtieňov šedej v škále od „0“ do „255“ sa v ňom nachádza číslca „8“. Ak sa v tomto poli nachádza číslca vyššia ako „8“, predstavuje pixel v odtieni šedej s vyššou presnosťou.

**7.1.13. Pole 13.013: Poloha prsta/dlane (FGP – Finger/Palm Position)**

V tomto povinnom poli označenom tagmi sa uvádza jedna alebo viac polôh prsta alebo dlane, ktoré sa môžu zhodovať so skrytým obrázkom. Číslo v desiatkovej sústave, ktoré zodpovedá známej alebo najpravdepodobnejšej polohe prsta, sa vyberie z tabuľky 5, alebo ktoré zodpovedá najpravdepodobnejšej polohe dlane, sa vyberie z tabuľky 10 a vloží sa ako jednomiestne alebo dvojmiestne podpole vo formáte ASCII. Na ďalšie polohy prstov alebo dlaní sa môže odkázať vložением alternatívnych kódov polôh vo forme podpolí oddelených separátorom „RS“. Kód „0“ pre „neznámy prst“ sa použije pri odkaze na ktorúkoľvek polohu prsta od 1 do 10. Pri odkaze na všetky polohy dlane v zozname sa použije kód „20“ pre „neznámu dľaň“.

**7.1.14. Polia 13.014 – 13.019: Rezervované na vymedzenie v budúcnosti (RSV – Reserved for future definition)**

Tieto polia sú rezervované na zahrnutie do budúcich revízií tejto normy. Žiadne z nich sa nepoužije na tejto úrovni revízie. Ak sa predsa len vyskytnú, majú sa ignorovať.



**7.1.15. Pole 13.020: Poznámka (COM – Comment)**

Toto nepovinné pole sa môže použiť na vloženie poznámok alebo iných textových informácií vo formáte ASCII s údajmi o skrytom obrázku.

**7.1.16. Polia 13.021 – 13.199: Rezervované na vymedzenie v budúcnosti (RSV – Reserved for future definition)**

Tieto polia sú rezervované na zahrnutie do budúcich revízií tejto normy. Žiadne z nich sa nepoužije na tejto úrovni revízie. Ak sa predsa len vyskytnú, majú sa ignorovať.

**7.1.17. Polia 13.200 – 13.998: Polia vymedzené používateľmi (UDF – User-defined Fields)**

Tieto polia vymedzuje používateľ a využijú sa v budúcnosti. Používateľ definuje aj ich veľkosť a obsah, a to v súlade s požiadavkami agentúry určenia. Ak existujú, musia obsahovať textové informácie vo formáte ASCII.

**7.1.18. Pole 13.999: Údaje z obrázku (DAT – Image Data)**

Toto pole obsahuje všetky údaje zo získaného latentného obrázku. Jeho číslo je vždy 999 a musí byť posledným fyzickým poľom v zázname. Napríklad, po poli „13.999:“ nasleduje údaj vo forme obrázku zastúpený binárnymi znakmi.

Každý pixel nekomprimovaného údaje v odtieňoch šedej je vyjadrený ôsmimi bitmi (pri 256 odtieňoch šedej) obsiahnutými v jednom bajte. Ak je údaj v poli BPX 13.012 vyšší alebo nižší ako „8“, počet bajtov na pixel bude iný. Ak sa použije kompresia, údaje v pixeloch sa skomprimujú v súlade s technikou špecifikovanou v poli CGA.

**7.2. Koniec logického záznamu typu 13: Skrytý obrázok s rôznym rozlíšením**

Kvôli konzistentnosti sa po poslednom bajte údaje z poľa 13.999 použije separátor „FS“ na oddelenie poľa od nasledujúceho logického záznamu. Tento separátor sa musí použiť aj v poli „dĺžka“ logického záznamu typu 13.

**8. Logický záznam typu 15: Odtlačok dlane s rôznym rozlíšením**

Logický záznam typu 15 obsahujúci polia ohraňované tagmi obsahuje údaje z obrázku s odtlačkom dlane spolu so súvisiacimi pevnými textovými poľami a poľami definovanými používateľmi a používa sa na výmenu takýchto údajov. Informácie, ktoré sa týkajú použitého skenovacieho rozlíšenia, veľkosti obrázku a iných parametrov alebo poznámok vyžadovaných na spracovanie obrázku, sa v rámci záznamu nachádzajú vo forme poľí ohraňovaných tagmi. Obrázky odtlačkov dlaní poskytnuté iným agentúram spracujú agentúry určenia tak, aby z nich získali potrebné informácie na účely zistenia zhody.

Údaje vo forme obrázku sa získavajú priamo od dotknutej osoby pomocou zariadenia na biometrické skenovanie alebo z karty z odtlačkom dlane alebo iného média, na ktorom sú uložené odtlačky dlane dotknutej osoby.

Každá metóda použitá na získanie obrázkov odtlačkov dlane by mala umožniť získanie súboru obrázkov z každej ruky. Tento súbor by mal obsahovať dľaň dominantnej ruky vo forme jedného naskenovaného obrázku a oblasť celej dlane od zápästia až po končeky prstov na jednom alebo dvoch naskenovaných obrázkoch. Ak sa na celú dľaň použijú dva obrázky, spodný obrázok by mal zahŕňať oblasť od zápästia až po vrch medziprstovej oblasti (tretí prstový kĺb) vrátane oblasti palcovej a malíčkovkej podušky. Vrchný obrázok by mal zahŕňať priestor od spodku medziprstovej oblasti až po končeky prstov. Takéto rozdelenie poskytuje dostatočné prekrytie oboch obrázkov, keďže oba zahŕňajú medziprstovú oblasť dlane. Porovnaním štruktúry a podrobných znakov papilárnych línií v tejto spoločnej oblasti môže osoba, ktorá obrázok skúma, presvedčivo vyhlásiť, že oba obrázky pochádzajú z rovnakej dlane.

Keďže sa odtlačok dlane môže použiť na rôzne účely, môže obsahovať jednu alebo viac jedinečných zobrazených oblastí získaných z dlane alebo prsta. Úplný súbor záznamov odtlačkov dlane jednotlivca bude za bežných okolností obsahovať dľaň dominantnej ruky a úplný obrázok alebo úplné obrázky odtlačkov dlaní oboch rúk. Keďže logický záznam obrázku vo forme poľí označených tagmi môže obsahovať len jedno binárne pole, pre každú dľaň dominantnej ruky sa bude vyžadovať jeden záznam typu 15, zatiaľ čo pre úplný odtlačok dlane bude potrebný jeden alebo dva takéto záznamy. Preto pri bežnej transakcii s odtlačkami dlaní sa na zobrazenie odtlačkov dlaní dotknutej osoby budú vyžadovať štyri až šesť záznamov typu 15.

**8.1. Polia pre logický záznam typu 15**

V nasledujúcich odsekoch sa opisujú údaje obsiahnuté v každom poli logického záznamu typu 15.



V rámci logických záznamov typu 15 sa vstupy robia do číslovaných polí. Vyžaduje sa usporiadanie prvých dvoch polí záznamu a pole obsahujúce údaje vo forme obrázku musí byť posledným fyzickým poľom v zázname. V tabuľke 8 sa pre každé pole v zázname typu 15 nachádza „stavový kód“ (buď „M“ označujúce povinné pole alebo „O“ označujúce pole nepovinné), číslo poľa, typ znaku, veľkosť poľa a obmedzenie výskytu. V poslednom stĺpci sa nachádza maximálna veľkosť v bajtoch, ktorá vychádza z trojmiestneho čísla poľa. Ak sa v čísle poľa nachádza viac čísiel, zvýši sa aj maximálny počet bajtov. Dve položky v stĺpci „veľkosť poľa pri každom výskyte“ zahŕňajú všetky separátory, ktoré sú v poli použité. Údaj v stĺpci „maximálny počet bajtov“ zahŕňa číslo poľa, informáciu a všetky separátory vrátane separátora „GS“.

8.1.1. Pole 15.001: Dĺžka logického záznamu (LEN – Logical Record Length)

Toto povinné pole vo formáte ASCII obsahuje informáciu o celkovom počte bajtov v logickom zázname typu 15. Pole 15.001 špecifikuje dĺžku záznamu vrátane každého znaku každého poľa v zázname a separátorov.

8.1.2. Pole 15.002: Znak označenia obrázku (IDC – Image Designation Character)

Toto povinné pole vo formáte ASCII sa používa na identifikáciu údajov vo forme obrázku odtlačku dlane, ktoré sa nachádzajú v zázname. Tento IDC je rovnaký ako IDC v poli obsah súboru (CNT) v zázname typu 1.

8.1.3. Pole 15.003: Typ zobrazenia (IMP – Impression Type)

Týmto povinným jednobajtovým poľom vo formáte ASCII sa uvádza spôsob, akým sa získala informácia vo forme obrázku odtlačku dlane. Do tohto poľa sa vpíše vhodný kód vybraný z tabuľky 9.

8.1.4. Pole 15.004: Agentúra pôvodu/ORI (SRC – Source Agency)

Toto povinné pole vo formáte ASCII obsahuje totožnosť správneho orgánu alebo organizácie, ktorá pôvodne získala obrázok v zázname. Za bežných okolností sa v tomto poli uvedie identifikátor agentúry pôvodu (ORI – Originating Agency Identifier) agentúry, ktorá získala obrázok. Pozostáva z dvoch informácií v tomto formáte: CC/agency.

Prvá informácia obsahuje kód krajiny v databáze Interpolu, ktorý pozostáva z dvoch alfanumerických znakov. Druhá informácia, agency (agentúra), je voliteľný text na identifikáciu agentúry obsahujúci najviac 32 alfanumerických znakov.

8.1.5. Pole 15.005: Dátum získania odtlačku dlane (PCD – Palmprint Capture Date)

Toto povinné pole vo formáte ASCII obsahuje dátum získania obrázku odtlačku dlane. Tento dátum sa uvádza ako osem čísiel vo formáte CCRRMMDD. CCRR je rok získania obrázku; znaky MM sú desiatkové a jednotkové hodnoty mesiaca a znaky DD zastupujú rovnaké hodnoty pri dni v danom mesiaci. Napríklad, dátum 20000229 znamená 29. februára 2000. Úplný dátum musí skutočne existovať.

8.1.6. Pole 15.006: Dĺžka horizontálnej línie (HLL – Horizontal Line Length)

Toto povinné pole vo formáte ASCII obsahuje počet pixelov na jednej horizontálnej línii prenášaného obrázku.

8.1.7. Pole 15.007: Dĺžka vertikálnej línie (VLL – Vertical Line Length)

Toto povinné pole vo formáte ASCII obsahuje počet horizontálnych línii na prenášanom obrázku.

8.1.8. Pole 15.008: Jednotky zobrazenia (SLC – Scale Units)

Toto povinné pole vo formáte ASCII obsahuje jednotky, v ktorých sa opisuje vzorkovacia frekvencia obrázku (hustota pixelov). Jednotka („1“) v tomto poli znamená pixely na palec, zatiaľ čo dvojka („2“) označuje pixely na centimeter. Nula („0“) v tomto poli označuje, že sa nezadala žiadna škála. V tomto prípade sa zobrazovací pomer v pixeloch udáva na základe podielu HPS/VPS.

8.1.9. Pole 15.009: Horizontálny rozsah v pixeloch (HPS)

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov v horizontálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje horizontálnu zložku pomeru zobrazenia v pixeloch.

8.1.10. Pole 15.010: Vertikálny rozsah v pixeloch (VPS)

Toto povinné pole vo formáte ASCII špecifikuje celočíselnú hustotu pixelov vo vertikálnom smere za predpokladu, že pole SLC obsahuje znak „1“ alebo „2“. V iných prípadoch označuje vertikálnu zložku pomeru zobrazenia v pixeloch.

Tabuľka 8: Rozvrh záznamu typu 15: odtlačok dlane s rôznym rozlíšením

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
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	—

Tabuľka 9: Typ zobrazenia dlane

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. Pole 15.011: Kompresný algoritmus (CGA – Compression Algorithm)

V tomto povinnom poli ASCII sa špecifikuje algoritmus, ktorý sa používa na kompresiu obrázkov v odtieňoch šedej. Údaj „NONE“ v tomto poli znamená, že údaje v zázname nie sú komprimované. Pri obrázkoch, ktoré sa majú komprimovať, sa v tomto poli uvedie uprednostňovaná metóda kompresie obrázkov s odtlačkami všetkých desiatich prstov. Platné kompresné kódy sa uvádzajú v dodatku 7.

## 8.1.12. Pole 15.012: Bity na pixel (BPX)

Toto povinné pole vo formáte ASCII obsahuje počet bitov, ktoré predstavujú jeden pixel. Pri bežných hodnotách odtieňov šedej v škále od „0“ do „255“ sa v ňom nachádza číslica „8“. Ak sa v tomto poli nachádza číslica vyššia alebo nižšia ako „8“, predstavuje pixel v odtieni šedej s vyššou alebo nižšou presnosťou.

Tabuľka 10: Kódy, oblasti a veľkosti dlaní

Palm Position	Palm code	Image area (mm <sup>2</sup> )	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
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. Pole 15.013: Poloha odtlačku dlane (PLP – Palmprint Position)

Toto povinné pole vo formáte ASCII obsahuje polohu odtlačku dlane, ktorá zodpovedá obrázku odtlačku dlane. Číselný kód v desiatkovej sústave zodpovedajúci známej alebo najpravdepodobnejšej polohe odtlačku dlane sa vyberie z tabuľky 10 a vloží ako dvojmiestne podpole vo formáte ASCII. V tabuľke 10 sa vymedzujú aj maximálne veľkosti a rozmery pri každej z možných polôh odtlačku dlane.

## 8.1.14. Polia 15.014 – 15.019: Rezervované pre budúce vymedzenie (RSV – Reserved for future definition)

Tieto polia sú rezervované na zahrnutie do budúcich revízií tejto normy. Žiadne z nich sa nepoužije na tejto úrovni revízie. Ak sa predsa len vyskytnú, majú sa ignorovať.

## 8.1.15. Pole 15.020: Poznámka (COM – Comment)

Toto nepovinné pole sa môže použiť na vloženie poznámok alebo iných textových informácií vo formáte ASCII s údajmi o obrázku odtlačku dlane.

## 8.1.16. Polia 15.021 – 15.199: Rezervované pre budúce vymedzenie (RSV – Reserved for future definition)

Tieto polia sú rezervované na zahrnutie do budúcich revízií tejto normy. Žiadne z nich sa nepoužije na tejto úrovni revízie. Ak sa predsa len vyskytnú, majú sa ignorovať.

## 8.1.17. Polia 15.200 – 15.998: Polia vymedzené používateľmi (UDF – User-defined Fields)

Tieto polia vymedzuje používateľ a využijú sa v budúcnosti. Používateľ definuje aj ich veľkosť a obsah, a to v súlade s požiadavkami agentúry určenia. Ak existujú, musia obsahovať textové informácie vo formáte ASCII.

## 8.1.18. Pole 15.999: Údaje z obrázku (DAT – Image Data)

Toto pole obsahuje všetky údaje zo získaného obrázku odtlačku dlane. Jeho číslo je vždy 999 a musí byť posledným fyzickým polom v zázname. Napríklad, po poli „15.999:“ nasleduje údaj vo forme obrázku zastúpený binárnymi znakmi. Každý pixel nekomprimovaného údaje v stupňoch šedej je vyjadrený ôsmimi bitmi (pri 256 odtieňoch šedej) obsiahnutými v jednom bajte. Ak je údaj v poli BPX 15.012 vyšší alebo nižší ako „8“, počet bajtov na pixel bude iný. Ak sa použije kompresia, údaje v pixeloch sa skomprimujú v súlade s technikou špecifikovanou v poli CGA.

8.2. *Koniec logického záznamu typu 15: Odtlačok dlane s rôznym rozlíšením*

Kvôli konzistentnosti sa po poslednom bajte údaju z poľa 15.999 použije separátor „FS“ na oddelenie poľa od nasledujúceho logického záznamu. Tento separátor sa musí použiť aj v poli „dĺžka“ logického záznamu typu 15.

8.3. *Ďalšie logické záznamy typu 15: Odtlačok dlane s rôznym rozlíšením*

Do súboru sa môžu vložiť ďalšie záznamy typu 15. Pre každý ďalší odtlačok dlane sa vyžaduje úplný logický záznam typu 15 spolu so separátorom „FS“.

Tabuľka 11: Maximálny počet kandidátov prijatých na overenie na jeden prenos

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

Typy vyhľadávania:

TP/TP: obrázok s odtlačkami desiatich prstov proti obrázku s odtlačkami desiatich prstov,

LT/TP: skrytý odtlačok prsta proti obrázku s odtlačkami desiatich prstov,

LP/PP: skrytý odtlačok dlane proti odtlačku dlane,

TP/UL: obrázok s odtlačkami desiatich prstov proti nevyriešenému latentnému odtlačku prsta,

LT/UL: skrytý odtlačok prsta proti nevyriešenému latentnému odtlačku prsta,

PP/ULP: odtlačok dlane oproti nevyriešenému latentnému odtlačku dlane,

LP/ULP: skrytý odtlačok dlane oproti nevyriešenému latentnému odtlačku dlane.

9. ***Dodatky ku kapitole 2 (výmena daktyloskopických údajov)***9.1. *Dodatok 1: Oddelovacie kódy ASCII*

ASCII	Position <sup>(1)</sup>	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

<sup>(1)</sup> Ide o pozíciu vymedzenú v norme ASCII.

9.2. *Dodatok 2: Výpočet alfanumerických kontrolných znakov*

Pre TCN a TCR (polia 1.09 a 1.10):

Číslo zodpovedajúce kontrolnému znaku sa vytvorí na základe tohto vzorca:

$(RR * 10^8 + SSSSSSS) \text{ Modulo } 23,$

kde RR sú posledné dve číslice roka a SSSSSSS je sériové číslo.

Kontrolný znak sa potom vytvorí na základe kontrolnej tabuľky, ktorá sa nachádza nižšie.

Pre CRO (pole 2.010)

Číslo zodpovedajúce kontrolnému znaku sa vytvorí na základe tohto vzorca:

$(RR * 10^6 + NNNNNN) \text{ Modulo } 23$ ,

kde RR sú posledné dve číslice roka a NNNNNN je sériové číslo.

Kontrolný znak sa potom vytvorí na základe kontrolnej tabuľky, ktorá sa nachádza nižšie.

Kontrolná tabuľka kontrolných znakov

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. Dodatok 3: Znakové kódy

#### 7-bitové kódy ANSI na výmenu informácií

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	{		}	~			

### 9.4. Dodatok 4: Súhrn transakcií

#### Záznam typu 1 (povinné)

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

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
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 stĺpci s podmienenosťou:

O = nepovinné (optional), M = povinné (mandatory), C = s podmienkou, že transakcia je odpoveďou pre agentúru pôvodu (conditional).

#### Záznam typu 2 (povinné)

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
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 stĺpci s podmienenosťou:

O = nepovinné (optional), M = povinné (mandatory), C = s podmienkou, že sú dostupné údaje (conditional).

\* = ak je prenos údajov v súlade s vnútroštátnymi právnymi predpismi (nepatrí do rozhodnutia 2008/615/SVV).

## 9.5. Dodatok 5: Vymedzenia záznamov typu 1

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

V stĺpci s typom znaku: A = abecedný, N = numerický, B = binárny.

1\* Povolené znaky pre názov agentúry sú [„0..9“, „A..Z“, „a..z“, „\_“, „-“, „.“, „“].

## 9.6. Dodatok 6: Vymedzenia záznamov typu 2

Tabuľka A.6.1: Transakcie CPS a 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}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
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}

Tabuľka A.6.2: Transakcia 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/222222222{GS}
MN1	C	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}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Tabuľka A.6.3: Transakcia 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}



Identifier	Condition	Field Number	Field Name	Character Type	Example Data
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}

Tabuľka A.6.4: Transakcie MPS a 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 stĺpci s podmienenosťou: O = nepovinné (optional), M = povinné (mandatory), C = s podmienkou (conditional).

V stĺpci s typom znaku: A = abecedný, N = numerický, B = binárny.

1\* Povolené znaky sú [„0..9“, „A..Z“, „a..z“, „\_“, „-“, „ “, „-“].

#### 9.7. Dodatok 7: Kódy na kompresiu odtieňov šedej

Kompresné kódy

Compression	Value	Remarks
Wavelet Scalar Quantization Gray-scale 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. Dodatok 8: Špecifikácia pošty

S cieľom zlepšiť vnútorný rozvrh práce sa do predmetu poštovej správy pri transakcii typu PRUEM napíše kód krajiny (CC) členského štátu, ktorý správu odosiela a typ transakcie (TOT, pole 1.004).

Formát: CC/type of transaction

Príklad: „DE/CPS“.

Telo správy môže ostať prázdne.

Kapitola 3: **Výmena údajov z evidencie vozidiel**1. **Spoločný súbor údajov na automatizované vyhľadávanie údajov z evidencie vozidiel**1.1. *Vymedzenie pojmov*

Povinné a nepovinné prvky údajov ustanovené v článku 16 ods. 4 sú vymedzené takto:

## Povinné (M)

Tento prvok sa musí oznámiť v prípade, že sa informácia nachádza vo vnútroštátnom registri členského štátu. Preto v prípade dostupnosti informácie existuje povinnosť jej výmeny.

## Nepovinné (O)

Tento prvok sa môže oznámiť v prípade, že sa informácia nachádza vo vnútroštátnom registri členského štátu. Preto neexistuje povinnosť výmeny informácie ani v prípade, ak je dostupná.

Ak sa prvok v súbore údajov identifikuje ako osobitne dôležitý vzhľadom na rozhodnutie 2008/615/SVV, označí sa (znakom Y).

1.2. *Vyhľadávanie podľa vozidla/vlastníka/držiťela*1.2.1. *Spúšťacie mechanizmy vyhľadávania*

Existujú dva spôsoby vyhľadávania informácií, ktoré sa vymedzujú v ďalšom odseku:

- podľa čísla karosérie (VIN), referenčného dátumu a času (nepovinné),
- podľa čísla poznávacej značky, čísla karosérie (VIN) (nepovinné), referenčného dátumu a času (nepovinné).

Na základe týchto kritérií vyhľadávania sa ako výsledok vrátia informácie týkajúce sa jedného alebo viacerých vozidiel. Ak sa musí vrátiť informácia o len jednom vozidle, všetky jej prvky sa vrátia v rámci jednej odpovede. Ak sa nájde viac než jedno vozidlo, informácie, ktoré sa vrátia, určí samotný dožiadaný členský štát; budú to buď všetky informácie, alebo len informácie potrebné na rozšírenie vyhľadávania (napr. z dôvodu ochrany súkromia alebo z dôvodu výkonu vyhľadávača).

Informácie potrebné na rozšírenie vyhľadávania sa uvádzajú v odseku 1.2.2.1. V odseku 1.2.2.2 sa uvádza kompletný súbor informácií.

Pri vyhľadávaní podľa čísla karosérie a referenčného dátumu a času sa môže vyhľadávať v databázach jedného alebo všetkých zúčastnených členských štátov.

Ak sa vyhľadáva podľa poznávacej značky a referenčného dátumu a času, musí sa vyhľadávať v databáze konkrétneho členského štátu.

Bežne sa vyhľadáva s použitím skutočného času a dátumu, ale je možné použiť aj referenčný dátum a čas v minulosti. Ak sa vyhľadáva s referenčným dátumom a časom v minulosti a informácie z minulosti nie sú v registri členského štátu dostupné, pretože jednoducho vôbec neexistujú, ako odpoveď sa môžu poskytnúť aktuálne informácie, pričom sa táto skutočnosť výslovne uvedie.

1.2.2. *Súbor údajov*1.2.2.1. *Informácie potrebné na rozšírenie vyhľadávania*

Item	M/O <sup>(1)</sup>	Remarks	Prüm Y/N <sup>(2)</sup>
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	[D.1 <sup>(3)</sup> ] e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y

Item	M/O <sup>(1)</sup>	Remarks	Prüm Y/N <sup>(2)</sup>
EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

<sup>(1)</sup> M = mandatory when available in national register, O = optional.

<sup>(2)</sup> All the attributes specifically allocated by the Member States are indicated with Y.

<sup>(3)</sup> Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999.

#### 1.2.2.2. Kompletný súbor údajov

Item	M/O <sup>(1)</sup>	Remarks	Prüm Y/N
Data relating to holders of the vehicle		[C.1 <sup>(2)</sup> ] 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
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

Item	M/O <sup>(1)</sup>	Remarks	Prüm Y/N
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
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 <sup>(3)</sup>	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

Item	M/O <sup>(1)</sup>	Remarks	Prüm Y/N
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

<sup>(1)</sup> M = mandatory when available in national register, O = optional.

<sup>(2)</sup> Harmonised document abbreviation, see Council Directive 1999/37/EC of 27 April 1999.

<sup>(3)</sup> In Luxembourg two separate vehicle registration document ID's are used.

## 2. **Bezpečnosť údajov**

### 2.1. *Prehľad*

Softvérová aplikácia Eucaris umožňuje bezpečnú komunikáciu s inými členskými štátmi a s podpornými (back-end) pôvodnými systémami členských štátov pomocou protokolu XML. Členské štáty si vymieňajú správy prostredníctvom ich priameho odosielania prijímateľovi. Dátové stredisko členského štátu je napojené na sieť Európskej únie TESTA.

Správy vo formáte XML, ktoré sa cez sieť posielajú, sú šifrované. Na šifrovanie sa používa technika SSL. Správy, ktoré sa zasielajú podporným aplikáciám, sú čisto textové správy XML, keďže spojenie medzi klientskou a podpornou aplikáciou by malo byť v chránenom prostredí.

Poskytne sa klientská aplikácia, ktorá sa v rámci členského štátu môže použiť na vyhľadávanie vo vlastnom registri alebo v registri ostatných členských štátov. Títo klienti sa identifikujú prostredníctvom prihlasovacieho mena/hesla alebo klientského certifikátu. Spojenie s používateľom môže byť šifrované, pričom je to v zodpovednosti každého jednotlivého členského štátu.

### 2.2. *Bezpečnostné prvky výmeny správ*

Bezpečnostný dizajn sa zakladá na kombinácii podpisu HTTPS a XML. V tejto alternatíve sa na podpísanie všetkých správ zaslaných na server používa podpis XML, pričom sa prostredníctvom kontroly tohto podpisu dá overiť odosielateľ správy. Na ochranu dôvernosti a celistvosti správy pri prenose sa používa jednostranné zabezpečené spojenie SSL (len s certifikátom servera), ktorým sa poskytuje ochrana proti vymazaniu/opakovaniu a vkladaniu údajov. Namiesto vývoja softvéru na mieru, ktorý by realizoval obojstranné spojenie SSL, sa zaviedol podpis XML. Používanie tohto podpisu je bližšie k plánu webových služieb ako obojstranné spojenie SSL, a preto je aj strategickjšie.

Podpis XML sa môže implementovať rôznymi spôsobmi, pričom zvolený spôsob je v tomto prípade využitie tohto podpisu ako časti špecifikácie Web Services Security (WSS). V tejto špecifikácii sa vymedzuje spôsob použitia podpisu XML. Keďže WSS je postavená na štandarde SOAP, je logické, že SOAP sa bude dodržiavať v čo najväčšej možnej miere.

### 2.3. *Bezpečnostné prvky, ktoré sa netýkajú výmeny správ*

#### 2.3.1. *Autorizácia používateľov*

Používatelia webovej aplikácie sa autorizujú sami pomocou používateľského mena a hesla. Keďže sa pritom využíva štandardná autorizácia systému Windows, členské štáty môžu úroveň autorizácie v prípade potreby zvýšiť prostredníctvom využitia klientských certifikátov.

#### 2.3.2. *Úlohy používateľov*

Softvérová aplikácia Eucaris podporuje rôzne úlohy používateľov. Každý súbor služieb má vlastnú autorizáciu. Napríklad (výhradní) používatelia funkcie „Treaty of Eucaris“ nemôžu používať funkciu „Prüm“. Služby administrátorov sú od bežných úloh koncových používateľov oddelené.

#### 2.3.3. *Zaznamenávanie a vyhľadávanie údajov o výmene správ*

Softvérová aplikácia Eucaris uľahčuje zaznamenávanie všetkých typov informácií. Funkcia správcu umožňuje správcovi vnútroštátneho systému, aby určil, ktoré správy sa zaznamenávajú: žiadosti koncových používateľov, prichádzajúce žiadosti členských štátov, poskytnuté informácie z vnútroštátnych registrov atď.

Aplikácia sa môže nakonfigurovať tak, aby na zaznamenávanie používala vnútornú databázu alebo vonkajšiu databázu (Oracle). Rozhodnutie o tom, ktoré správy sa budú zaznamenávať, jasne závisí od zariadení na zaznamenávanie v pôvodných systémoch a pripojených klientských aplikáciách.

V hlavičke každej správy sa nachádza informácia o žiadajúcom členskom štáte, žiadajúcej organizácii a zúčastnenom používateľovi. Uvádza sa aj dôvod žiadosti.

Prostredníctvom kombinovaného zaznamenávania v žiadajúcom a odpovedajúcom členskom štáte je možné vyhľadať údaje o akejkoľvek výmene správ (napr. na základe žiadosti zúčastneného občana).

Zaznamenávanie sa konfiguruje prostredníctvom webového klienta (menu Administration, Logging configuration). Funkciu zaznamenávania vykonáva Core System. Po umožnení zaznamenávania sa v jednom zázname uloží úplná správa (hlavička aj telo). Úroveň zaznamenávania sa dá nastaviť v súvislosti s definovanou službou a typom správy, ktorá prechádza cez Core System.

Úrovně zaznamenávania

Možné sú tieto úrovne zaznamenávania:

Private (súkromná) – správa sa zaznamenáva: zaznamenávanie NIE je dostupné pre službu „extract logging“, ale je dostupné len na vnútroštátnej úrovni, a to na účely auditu a riešenia problémov.

None (žiadna) – správa sa vôbec nezaznamenáva.

Typy správ

Výmena informácií medzi členskými štátmi pozostáva z niekoľkých správ, ktoré schematicky predstavuje obrázok nachádzajúci sa nižšie.

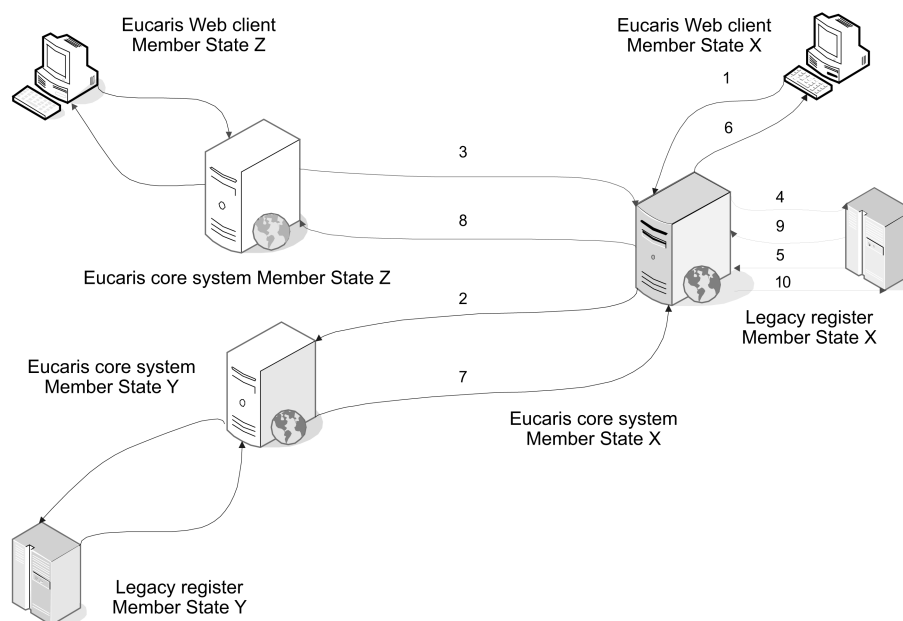
Existujú tieto typy správ (na obrázku sa uvádzajú pre Core System aplikácie Eucaris členského štátu X):

1. Request to Core System\_Request message by Client,
2. Request to Other Member State\_Request message by Core System of this Member State,
3. Request to Core System of this Member State\_Request message by Core System of other Member State,
4. Request to Legacy Register\_Request message by Core System,
5. Request to Core System\_Request message by Legacy Register,
6. Response from Core System\_Request message by Client,
7. Response from Other Member State\_Request message by Core System of this Member State,
8. Response from Core System of this Member State\_Request message by other Member State,
9. Response from Legacy Register\_Request message by Core System,
10. Response from Core System\_Request message by Legacy Register.

Na obrázku sa nachádzajú tieto výmeny informácií:

- Žiadosť o informáciu od členského štátu X členskému štátu Y – modré šípky. Táto žiadosť a odpoveď pozostáva zo správ typu 1, 2, 7 a 6.
- Žiadosť o informáciu od členského štátu Z členskému štátu X – červené šípky. Táto žiadosť a odpoveď pozostáva zo správ typu 3, 4, 9 a 8.
- Žiadosť o informáciu zo strany pôvodného registra na hlavný systém (táto cesta obsahuje aj žiadosť od bežného klienta pred pôvodným registrom) – zelené šípky. Tento druh žiadosti pozostáva zo správ typu 5 a 10.

Obrázok: Typy správ na zaznamenávanie



### 2.3.4. Hardvérový bezpečnostný modul

Hardvérový bezpečnostný modul sa nepoužíva.

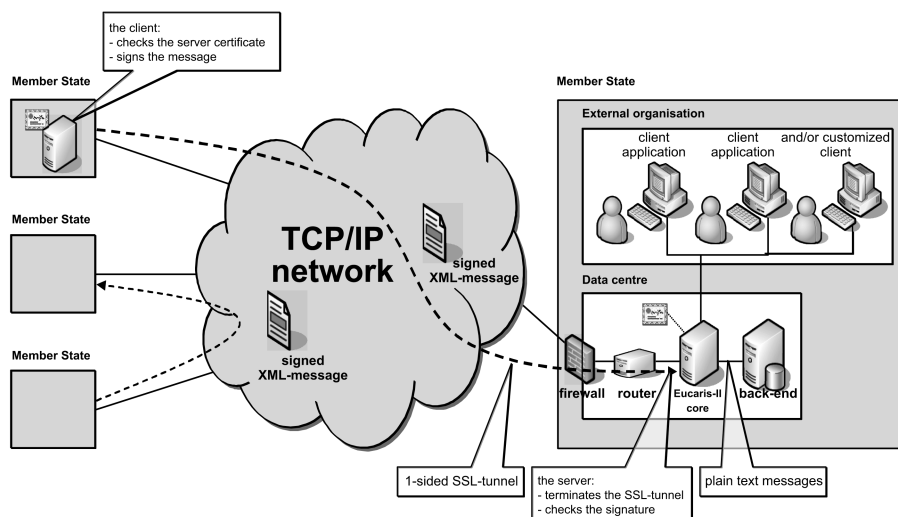
Hardvérový bezpečnostný modul (HSM – Hardware Security Module) poskytuje kvalitnú ochranu pre kľúč, ktorý sa používa na podpisovanie správ a identifikáciu serverov. Hoci prispieva k celkovej úrovni bezpečnosti, jeho kúpa/údržba je nákladnou záležitosťou a neexistujú žiadne požiadavky na rozhodovanie medzi druhou a treťou úrovňou bezpečnosti HSM FIPS 140-2. Keďže sa používa uzavretá sieť, ktorá účinne znižuje ohrozenie, rozhodlo sa, že HSM sa pre začiatok nepoužije. Ak bude HSM nevyhnutný napr. na získanie akreditácie, môže sa do architektúry systému pridať.

## 3. Technické podmienky výmeny údajov

### 3.1. Všeobecný opis aplikácie EUCARIS

#### 3.1.1. Prehľad

Aplikácia Eucaris pripája všetky zúčastnené členské štáty do viaccestnej siete, v ktorej každý členský štát komunikuje priamo s iným členským štátom. Na vytvorenie spojenia nie je potrebný žiadny centrálny komponent. Aplikácia Eucaris umožňuje bezpečnú komunikáciu s inými členskými štátmi a s koncovými pôvodnými systémami členských štátov pomocou protokolu XML. Túto architektúru znázorňuje nasledujúci obrázok.



Členské štáty si vymieňajú správy prostredníctvom ich priameho odosielania prijímateľovi. Dátové stredisko členského štátu je napojené na sieť používanú na výmenu správ (TESTA). Členský štát sa do siete TESTA pripája cez vlastnú vnútroštátnu bránu. Na pripojenie k sieti sa používa brána firewall, ku ktorej je aplikácia Eucaris pripojená pomocou smerovača. V závislosti od alternatív, ktorá sa zvolí na ochranu správ, používa certifikát buď smerovač alebo samotná aplikácia Eucaris.

Poskytne sa klientská aplikácia, ktorá sa v rámci členského štátu môže použiť na vyhľadávanie vo vlastnom registri alebo v registri ostatných členských štátov. Klientská aplikácia sa pripája k aplikácii Eucaris. Títo klienti sa identifikujú prostredníctvom prihlasovacieho mena/hesla alebo klientského certifikátu. Spojenie s používateľom v externej organizácii (napr. polícií) môže byť šifrované, pričom je to v zodpovednosti každého jednotlivého členského štátu.

### 3.1.2. Rozsah funkčnosti systému

Rozsah systému Eucaris je obmedzený na procesy v rámci výmeny informácií medzi orgánmi zodpovednými za evidenciu v členských štátoch a základnou prezentáciou týchto informácií. Postupy a automatizované procesy, pri ktorých sa tieto informácie používajú, sú mimo rozsahu funkčnosti systému.

Členské štáty sa môžu rozhodnúť, či budú využívať klientskú aplikáciu Eucaris alebo si vytvoria vlastnú prispôbenú klientskú aplikáciu. V tabuľke pod týmto textom sa opisuje, ktoré aspekty systému Eucaris sa používajú povinne a/alebo sú predpísané a ktoré sú nepovinné a/alebo na voľnom zvážení zo strany členských štátov.

EUCARIS aspects	M/O <sup>(1)</sup>	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: <ul style="list-style-type: none"> <li>— Encrypting and signing of the messages;</li> <li>— Checking of the identity of the sender;</li> <li>— Authorization of Member States and local users;</li> <li>— Routing of messages;</li> <li>— Queuing of asynchronous messages if the recipient service is temporally unavailable;</li> <li>— Multiple country inquiry functionality;</li> <li>— Logging of the exchange of messages;</li> <li>— Storage of incoming messages</li> </ul>
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.

<sup>(1)</sup> M = mandatory to use or to comply with O = optional to use or to comply with.



## 3.2. Požiadavky na funkčnosť a požiadavky, ktoré sa netýkajú funkčnosti

## 3.2.1. Generické funkcie

V tomto oddiele sa vo všeobecnosti opisujú hlavné generické funkcie.

Číslo	Opis
1.	Systém umožňuje orgánom členských štátov zodpovedným za evidenciu interaktívnu výmenu správ so žiadosťami a odpoveďami.
2.	Systém obsahuje klientskú aplikáciu, ktorá umožňuje koncovým používateľom zasielanie žiadostí a predkladanie informácií v odpovediach na účely manuálneho spracovania.
3.	Systém uľahčuje „vysielanie“, ktorým sa členskému štátu umožňuje zaslať žiadosť všetkým ostatným členským štátom. Centrálna aplikácia konsoliduje prichádzajúce odpovede do jednej správy pre klientskú aplikáciu (táto funkcia sa nazýva „Multiple Country Inquiry“).
4.	Systém dokáže riešiť rôzne typy správ. Úlohy používateľa, autorizácia, smerovanie, podpisovanie i zaznamenávanie sa vymedzujú v závislosti od konkrétnej služby.
5.	Systém umožňuje členským štátom, aby si vymieňali balíky správ alebo správy, ktoré obsahujú veľký počet žiadostí alebo odpovedí. Tieto správy sa spracúvajú asynchrónne.
6.	V prípade, ak je prijímajúci členský štát nedostupný, systém zoradí asynchrónne správy a zabezpečí ich doručenie hneď, ako sa príjemca sprístupní.
7.	Systém ukladá prichádzajúce asynchrónne správy až do ich spracovania.
8.	Systém umožňuje prístup len aplikáciám Eucaris iných členských štátov, a nie jednotlivým organizáciám v týchto členských štátoch, t. j. každý orgán zodpovedný za evidenciu funguje ako jediná brána medzi vnútroštátnymi koncovými používateľmi a zodpovedajúcimi orgánmi v iných členských štátoch.
9.	Na jednom serveri pre Eucaris je možné zadať používateľov z rôznych členských štátov a autorizovať ich v súlade s právami daného členského štátu.
10.	V správach sa nachádzajú informácie o žiadajúcom členskom štáte, organizácii a koncovom používateľovi.
11.	Systém uľahčuje zaznamenávanie údajov o výmene správ medzi rôznymi členskými štátmi a medzi centrálnou aplikáciou a vnútroštátnymi evidenčnými systémami.
12.	Systém umožňuje, aby osobitný tajomník (buď organizácia, alebo členský štát, ktorý je na túto úlohu výslovne vymenovaný) na účely vypracovávania štatistických správ zhromažďoval informácie o správach, ktoré zúčastnené členské štáty odoslali/prijali.
13.	Každý členský štát sám uvedie, ktoré zo zaznamenaných informácií sú pre uvedeného „tajomníka“ dostupné a ktoré sú „súkromné“.
14.	Systém umožňuje správcom vnútroštátnych systémov každého štátu, aby zo systému získali štatistické údaje o používaní.
15.	Systém umožňuje pridanie nových členských štátov prostredníctvom jednoduchých administratívnych postupov.

## 3.2.2. Používanie

Číslo	Opis
16.	Systém poskytuje rozhranie na automatizované spracovanie správ zo strany podporných systémov/pôvodných systémov a umožňuje integráciu používateľského rozhrania do týchto systémov (prispôsobené používateľské rozhranie).
17.	Systém sa ľahko učí, je názorný a obsahuje pomoc v textovom formáte.
18.	Systém preukázateľne pomáha členským štátom pri integrácii, operačných činnostiach a budúcej údržbe (napr. prostredníctvom referenčných pokynov, funkčnej/technickej dokumentácie, operačných pokynov...).
19.	Používateľské rozhranie je viacjazyčné a poskytuje koncovému používateľovi prostriedky na výber uprednostňovaného jazyka.
20.	Používateľské rozhranie poskytuje správcovi miestneho systému prostriedky na preklad položiek na monitore a kódovaných informácií do svojho jazyka.

## 3.2.3. Spôľahlivosť

Číslo	Opis
21.	Systém je vytvorený ako robustný a spoľahlivý operačný systém, tolerantný voči chybám zo strany prevádzkovateľa, pričom sa bez problémov obnovuje po výpadkoch energie alebo iných haváriách. Musí byť možné reštartovať systém bez straty údajov alebo s ich minimálnou stratou.
22.	Systém musí vykazovať stabilné a opakovateľné výsledky.
23.	Systém bol navrhnutý na spoľahlivé fungovanie. Je možné ho implementovať v takej konfigurácii, ktorá zabezpečí 98-percentnú dostupnosť (využitím nadbytočnosti, záložných serverov atď.)
24.	Využitie časti systému je možné dokonca i pri zlyhaní niektorých komponentov (ak „spadol“ členský štát C, členské štáty A a B môžu naďalej komunikovať). Mal by sa minimalizovať počet jednotlivých bodov zlyhania v informačnom reťazci.
25.	Čas obnovenia po vážnom zlyhaní by nemal presiahnuť jeden deň. Malo by byť možné minimalizovať dobu nedostupnosti prostredníctvom podpory na diaľku, napr. zo strany servisného centra.

## 3.2.4. Výkon

Číslo	Opis
26.	Systém sa dá využívať nepretržite, 24 hodín denne a 7 dní v týždni. Tento harmonogram (24 × 7) sa vyžaduje aj od pôvodných systémov členských štátov.
27.	Systém odpovedá na žiadosti používateľov rýchlo bez ohľadu na ďalšie úlohy, ktoré vykonáva. Túto funkčnosť si vyžadujú aj pôvodné systémy zúčastnených strán, aby sa zabezpečil prijateľný reakčný čas. Za prijateľný reakčný čas sa považuje celkový reakčný čas 10 sekúnd na jednu odpoveď.
28.	Systém bol navrhnutý ako systém pre viacerých používateľov a tak, aby zvládol podporné úlohy, zatiaľ čo používateľ vykonáva úlohy základné.
29.	Systém bol navrhnutý ako pružný z hľadiska rozsahu, aby podporoval možný nárast správ v prípade pridania novej funkcie, organizácie alebo nového členského štátu.

## 3.2.5. Bezpečnosť

Číslo	Opis
30.	Systém je vhodný (napr. čo sa týka bezpečnostných opatrení) na výmenu správ, ktoré obsahujú citlivé osobné údaje (napr. vlastníka/užívateľa vozidla) klasifikované ako „EU restricted“.
31.	Údržba systému sa vykonáva spôsobom, pri ktorom sa neumožňuje neoprávnený prístup k údajom.
32.	Systém obsahuje službu pre správu práv a povolení vnútroštátnych koncových používateľov.
33.	Členské štáty môžu skontrolovať totožnosť odosielateľa (na úrovni členského štátu) prostredníctvom podpisu XML.
34.	Členské štáty musia výslovne oprávniť iné členské štáty na žiadanie špecifických informácií.
35.	Na úrovni aplikácie poskytuje systém plnú bezpečnosť a šifrovací postup kompatibilný s úrovňou bezpečnosti, ktorá sa v takýchto situáciách vyžaduje. Výlučnosť a celistvosť informácie sa zaručuje použitím podpisu XML a šifrovania prostredníctvom tunelingu SSL.
36.	Údaje o celej výmene informácií sa dajú vyhľadávať na základe ich zaznamenávania.
37.	Poskytuje sa ochrana proti vymazaniu správ (treťou stranou) a opakovanému prehrávaniu a vkládaniu správ (treťou stranou).
38.	Systém využíva certifikáty TTP (Trusted Third Party) pre dôveryhodné tretie strany.
39.	Systém je schopný zvládať rôzne certifikáty od jedného členského štátu, v závislosti od typu správy alebo služby.

Číslo	Opis
40.	Bezpečnostné opatrenia na úrovni aplikácie postačujú na umožnenie používania neakreditovaných sietí.
41.	Systém dokáže používať najnovšie bezpečnostné technológie, ako napr. bránu XML-firewall.

## 3.2.6. Prispôsobivosť

Číslo	Opis
42.	Systém sa dá rozšíriť o nové správy a nové funkcie. Náklady na prispôbenie sú zanedbateľné z dôvodu centralizovaného vývoja komponentov aplikácie.
43.	Členské štáty môžu definovať nové typy správ na dvojstranné použitie. Podpora všetkých typov správ od všetkých členských štátov sa nevyžaduje.

## 3.2.7. Podpora a údržba

Číslo	Opis
44.	Systém poskytuje servisnému centru a/alebo prevádzkovateľom monitorovacie zariadenia na sledovanie siete a serverov v rôznych členských štátoch.
45.	Systém poskytuje prostriedky na podporu na diaľku zo strany servisného centra.
46.	Systém poskytuje prostriedky na analýzu problémov.
47.	Systém sa dá rozšíriť o nové členské štáty.
48.	Aplikáciu môže jednoducho nainštalovať personál s minimálnou kvalifikáciou a skúsenosťami v oblasti IT. Inštalčný postup je maximálne automatizovaný.
49.	Systém poskytuje stále prostredie pre testovanie a schvaľovanie.
50.	Ročné náklady na údržbu a podporu sa znížili prostredníctvom dodržiavania trhových štandardov a vytvorenia aplikácie spôsobom, ktorý si vyžaduje čo najmenšiu podporu zo strany servisného strediska.

## 3.2.8. Požiadavky na dizajn

Číslo	Opis
51.	Systém bol navrhnutý a overený tak, aby fungoval mnoho rokov.
52.	Systém bol vytvorený tak, aby fungoval nezávisle od poskytovateľa siete.
53.	Systém je v súlade s používaným hardvérom/softvérom v členských štátoch tým, že funguje spolu s evidenčnými systémami, ktoré využívajú voľne dostupné štandardné technológie webových služieb [XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 atď.].

## 3.2.9. Uplatniteľné normy

Číslo	Opis
54.	Systém je v súlade s otázkami ochrany údajov uvedenými v nariadení (ES) č. 45/2001 (články 21, 22 a 23) a so smernicou 95/46/ES.
55.	Systém je v súlade s normami IDA.
56.	Systém podporuje UTF8.

Kapitola 4: **Hodnotenie**1. **Hodnotiaci postup podľa článku 20 (príprava rozhodnutí podľa článku 25 ods. 2 rozhodnutia 2008/615/SVV)**1.1. *Dotazník*

Príslušná pracovná skupina Rady vypracuje dotazník týkajúci sa každej z automatizovaných výmen údajov ustanovených v kapitole 2 rozhodnutia 2008/615/SVV.

Hneď ako bude členský štát presvedčený, že spĺňa predpoklady na výmenu údajov v relevantnej kategórii, vyplní príslušný dotazník.

1.2. *Skúšobná prevádzka*

S cieľom vyhodnotiť výsledky dotazníka uskutoční členský štát, ktorý si želá začať výmenu údajov, skúšobnú prevádzku spolu s jedným alebo viacerými členskými štátmi, ktoré si už vymieňajú údaje podľa predmetného rozhodnutia Rady. Skúšobná prevádzka sa uskutoční krátko pred hodnotiacou návštevou alebo krátko po nej.

Podmienky a pravidlá tejto skúšobnej prevádzky určí príslušná pracovná skupina Rady, pričom budú vychádzať z predchádzajúcej samostatnej dohody s dotknutým členským štátom. O jej praktických podrobnostiach rozhodnú členské štáty, ktoré sa na tejto skúšobnej prevádzke zúčastňujú.

1.3. *Hodnotiacia návšteva*

V členskom štáte, ktorý si želá začať výmenu údajov, sa uskutoční hodnotiacia návšteva s cieľom vyhodnotiť výsledky dotazníka.

Podmienky a pravidlá tejto návštevy určí príslušná pracovná skupina Rady, pričom budú vychádzať z predchádzajúcej samostatnej dohody medzi dotknutým členským štátom a hodnotiacim tímom. Dotknutý členský štát umožní hodnotiacemu tímu, aby skontroloval automatizovanú výmenu údajov v kategórii alebo kategóriách údajov, ktoré sa majú hodnotiť, a to najmä prostredníctvom organizácie programu návštevy, v ktorom sa zohľadnia požiadavky hodnotiaceho tímu.

Hodnotiaci tím pripraví do jedného mesiaca správu o hodnotiacej návšteve, ktorú postúpi dotknutému členskému štátu na pripomienkovanie. V prípade potreby hodnotiaci tím správu na základe pripomienok členského štátu zreviduje.

Hodnotiaci tím pozostáva z najviac troch členov, ktorých vymenujú členské štáty, ktoré sa zúčastňujú na automatizovanej výmene údajov v hodnotených kategóriách; títo členovia musia mať skúsenosti s dotknutou kategóriou údajov, musia mať príslušnú vnútroštátnu bezpečnostnú previerku na tieto záležitosti a musia byť ochotní zúčastniť sa na najmenej jednej hodnotiacej návšteve v inom členskom štáte. Komisia sa vyzve, aby sa k hodnotiacemu tímu pridala ako pozorovateľ.

Členovia hodnotiaceho tímu budú dodržiavať dôverný charakter informácií, ktoré získajú pri výkone svojich úloh.

1.4. *Správa Rade*

Rade sa na rozhodnutie podľa článku 25 ods. 2 rozhodnutia 2008/615/SVV predloží celková hodnotiacia správa, v ktorej sa zhrnú výsledky dotazníkov, hodnotiacej návštevy a skúšobnej prevádzky.

2. **Hodnotiaci postup podľa článku 21**2.1. *Štatistika a správa*

Každý členský štát zostaví štatistiku o výsledkoch automatizovanej výmeny údajov. V záujme zabezpečenia porovnateľnosti, zostaví vzor takejto štatistiky príslušná pracovná skupina Rady.

Štatistika sa každý rok postúpi Komisii a generálnemu sekretariátu, ktorý vypracuje všeobecný prehľad za ukončený rok.

Okrem toho sa členské štáty požiadajú, aby pravidelne, ale nie viac ako raz ročne, zasielali ďalšie informácie o administratívnej, technickej a finančnej realizácii automatizovanej výmeny údajov, ktoré sú potrebné na analýzu a skvalitnenie procesu. Na základe týchto informácií sa pre Radu pripraví správa.

2.2. *Revízia*

Rada v primeranom časovom horizonte preskúma uvedený mechanizmus hodnotenia a v prípade potreby ho zreviduje.

3. *Stretnutia expertov*

Experti sa budú pravidelne stretávať v rámci príslušnej pracovnej skupiny Rady, aby organizovali a realizovali uvedené postupy hodnotenia, vymieňali si skúsenosti a rokovali o možných zlepšeniach. Ak je to možné, výsledky týchto rokovaní sa začlenia do správy uvedenej v bode 2.1.

---