1.pielikums
atklātā konkursa
„Iekšlietu ministrijas Informācijas centra Biometrijas datu apstrādes sistēmas uzturēšana un pilnveidošana četriemgadiem”
(identifikācijas numurs IeM IC 2017/6)
nolikumam

Iekšlietu ministrijas Informācijas centra

ATKLĀTĀ KONKURSA

"Biometrijas datu apstrādes sistēmas uzturēšana uz četriem gadiem”

(iepirkuma identifikācijas numurs – **IeM IC 2017/6**)

Tehniskā specifikācija

EIROPAS SAVIENĪBA

Patvēruma, migrācijas un integrācijas fonds

Rīga, 2017

SATURA RĀDĪTĀJS

I INFORMĀCIJA PAR DOKUMENTU

1. Dokumenta nolūks un mērķauditorija

Dokumenta nolūks ir sniegt informāciju par Iekšlietu ministrijas Informācijas centra (turpmāk – Centrs) uzturētās Biometrijas datu apstrādes sistēmas (turpmāk – BDAS) esošā risinājuma loģisko arhitektūru un pamata funkcijām, kā arī definēt prasības BDAS funkcionalitātes papildināšanai, lai nodrošinātu sistēmas attīstību un nodrošinātu tās atbilstību aktuālajām prasībām.

Dokumenta mērķauditorija ir Centrs, kā BDAS turētājs un Pasūtītājs, un komercsabiedrības vai personas, kuras ir ieinteresētas nodrošināt šajā dokumentā definēto darba uzdevumu, kā potenciālais Izpildītājs.

2. Dokumentā izmantotie apzīmējumi un termini

Dokumentā izmantotie saīsinājumi un termini, kā arī to skaidrojums ir sniegts Tabulā Nr. 1.

Tabula Nr. 1. *Dokumentā izmantotie saīsinājumi un termini*

Saīsinājums / termins	Nozīme
AD, ADFS, ACDS	Aktīvās direktorijas moduļi
AMS, AQS	Rindu mašīnas dažādiem pieprasījumiem
BDAS	Biometrijas datu apstrādes sistēma (turpmāk tekstā arī Sistēma)
CAPS	Programmatūra personu reģistrācijai un meklēšanai CBS
CAPS IDM	Identitātes pārvaldības lietojumprogramma
CAT1	Eurodac datu iegūšanas kategorija – Starptautiskās aizsardzības pieteikuma iesniedzēji
CAT2	Eurodac datu iegūšanas kategorija – Trešo valstu valstspiederīgie vai bezvalstnieki, kas aizturēti sakarā ar nelikumīgu kādas ārējās robežas šķērsošanu
CAT3	Eurodac datu iegūšanas kategorija – Trešo valstu valstspiederīgie vai bezvalstnieki, kas uzturas kādā dalībvalstī
CAT4	Eurodac datu iegūšanas kategorija – Datu salīdzināšana tiesībaizsardzības nolūkos
CAT9	Eurodac datu iegūšanas kategorija – Datu pārbaude pēc datu subjekta pieprasījuma
CBS	Centrālā biometrijas sistēma (ietver DB, SOA, ABIS biometriskās meklēšanas dzini)
CSDD	Ceļu satiksmes un drošības direkcija
DB	Datubāze
DBVS	Datubāzu vadības sistēma
ECRIS	European Criminal Records Information System
Eurodac CU	Eiropas Savienības centrālā Eurodac sistēma
IeM	Iekšlietu ministrija
IIIS	Integrēta Iekšlietu informācijas sistēma (uztur Centrs)
Interpol	Starptautiskās kriminālpoliciju organizācijas informācijas sistēma
IS	Informācijas Sistēma
LR	Latvijas Republika
LVS	Latvijas valsts standarts
NVIS	Eiropas Vīzu informācijas sistēmas nacionālā daļa (uztur PMLP)
PK	Personas kods
PM	Personu meklēšana

Saīsinājums / termins	Nozīme
PMLP	Pilsonības un migrācijas lietu pārvalde
PRUME	Biometrisko datu apmaiņa atbilstoši Eiropas Padomes lēmuma Nr.2008/616/TI nosacījumiem
SIS	Šengenas informācijas sistēma
SOA	Serviss orientēta arhitektūra
US	Uzraudzības saraksts
USS	Universālā starpsistēmu saskarne, BDAS sastāvdaļa
VRS	Valsts robežsardze
WS	Web servisi
Latentie dati	Latenti pirkstu vai delnu nospiedumi jeb pirkstu vai delnu pēdas

3. Pieņēmumi un ierobežojumi.

Dokuments ir sagatavots 2017.gada 17.maijā un raksturo pašreizējo situāciju.

II ESOŠĀS VIDES APRAKSTS

4. Informācija par Centra uzturētajām informācijas sistēmām

Centrs ir Iekšlietu ministrijas pakļautībā esoša tiešās pārvaldes iestāde. Centra darbības mērķis ir veicināt noziedzības novēršanu un apkarošanu, sabiedriskās kārtības un drošības aizsardzību, izmantojot informācijas apstrādes un analīzes līdzekļus, kā arī nodrošināt Iekšlietu ministriju un tās padotībā esošās iestādes ar Eiropas Savienības prasībām atbilstošām operatīvo radiosakaru un privāto elektronisko sakaru tīklu sistēmām.

Centra uzturētās informācijas sistēmas veic automatizēto datu apmaiņu gan ar Latvijas Republikas (Valsts robežsardze, Pilsonības un migrācijas lietu pārvalde, Ceļu satiksmes drošības direkcija, Uzņēmumu reģistrs, Rīgas un citu pašvaldību domes, Zemkopības ministrija u.c.), gan ar ārvalstu (Interpols, Eurodac, Šengenas zonas dalībvalstis, Lietuvas Republikas Iekšlietu ministrija u.c.) institūcijām, kā arī citu organizāciju uzturētajām informācijas sistēmām.

Lai Centra uzturētajās informācijas sistēmās nodrošinātu aktuālas un precīzas informācijas uzglabāšanu un apstrādi, Centra nozīmētie informācijas sistēmu pārziņi veic darbības, lai nodrošinātu informācijas sistēmu atbilstību likumdevēju noteiktajām normām (normatīvo aktu grozījumi, jauni normatīvie akti), lietotāju prasībām, kā arī nodrošina informācijas sistēmu pilnveidošanu, lai novērstu konstatētās datu kvalitātes problēmas un kritiskas datu apstrādes kļūdas. Informācijas centra uzturēto informācijas sistēmu pilnveidošanai un attīstībai ir izmantoti gan ārvalstu fondi, gan valsts budžeta līdzekļi.

Ņemot vērā to, ka iepriekš minēto procesu ietekmē informācijas sistēmu pilnveidošana un attīstība ir nepārtraukts process un to, ka atsevišķu pilnveidojumu īstenošana nepieciešama iespējami īsākā laika periodā, ir nepieciešams pamatojoties uz konkursa rezultātiem noslēgt vispārīgo vienošanos, kuras ietvaros, tiks slēgti atsevišķi Pakalpojumu līgumi par IS pilnveidi. Vispārējā vienošanās tiek paredzēti vispārēji noteikumi attiecībā uz Pakalpojuma līguma priekšmetu, cenu, Pakalpojuma kvalitāti, izpildes termiņiem un citi pamatnoteikumi.

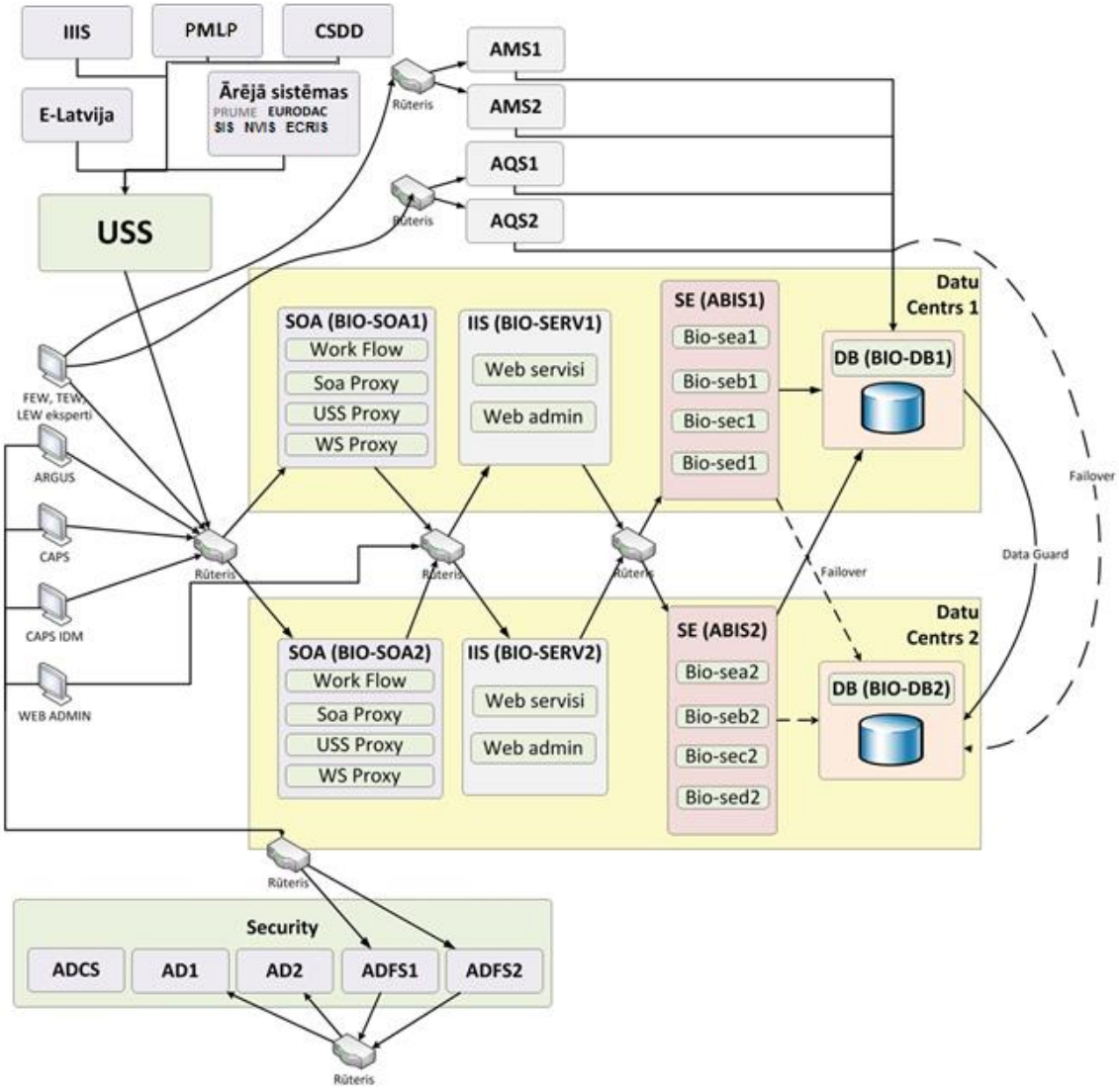
5. Biometrijas datu apstrādes sistēmas esošā risinājuma apraksts

Biometrijas datu apstrādes sistēma (BDAS) ir viena no informācijas sistēmām, kuras uzturēšanu un attīstību nodrošina Centrs. BDAS ir izveidota 2012.gadā un tās izveidošanas mērķis ir fizisko personu identitātes noteikšana un svešas identitātes izmantošanas nepieļaušana. Pamatojoties uz Biometrijas datu apstrādes sistēmas likumu, BDAS uzkrāj un apstrādā personu biometriskos (sejas digitālais attēls, pirkstu (delnu) nospiedumu digitālie attēli) un biogrāfiskos datus.

BDAS sastāv no centralizētas datubāzes, specializētām datu ievades, datu meklēšanas un identitātes pārvaldnieka lietojumprogrammām, kā arī biometrijas ekspertu un dzīvās video plūsmas analīzes lietojumprogrammām.

Uz BDAS tehnoloģiskās platformas ir izveidoti četri loģiski nodalīti reģistri: Civilais datu masīvs, Kriminālais datu masīvs, Patvēruma meklētāju pirkstu nospiedumu informācijas sistēma (turpmāk – Eurodac masīvs) un Automatizētā pirkstu nospiedumu identifikācijas sistēma (turpmāk – Migrācijas masīvs).

BDAS esošā risinājuma augsta līmeņa arhitektūra attēlota 1.attēlā.



1.att. BDAS esošā risinājuma augsta līmeņa arhitektūra.

Zemāk ir sniegta papildus informācija par BDAS esošā risinājuma elementiem.

5.1. Lietojumprogrammas CAPS mērķis un uzdevumi:

5.1.1. Jaunas personas biometrijas lietas izveidošana un biometrijas datu savākšana;

5.1.2. Sejas fotogrāfijas iegūšana un uzglabāšana (iegūst no fotoattēla vai reāla laika režīmā no fotokameras);

5.1.3. Uzspiestie pirkstu nospiedumu iegūšana un uzglabāšana (iegūst no pirkstu nospiedumu skeneriem vai ieskanētām daktiloskopiskām kartēm);

5.1.4. Pārveltie pirkstu nospiedumu iegūšana un uzglabāšana (iegūst no pirkstu nospiedumu skeneriem vai ieskanētām daktiloskopiskām kartēm);

5.1.5. Delnas nospiedumu iegūšana un uzglabāšana (iegūst no delnu nospiedumu skeneriem vai ieskanētām daktiloskopiskām kartēm);

5.1.6. Personas biometriskā verifikācija;

5.1.7. Personas biometriskā identifikācija.

5.2. Lietojumprogrammas CAPS IDM mērķis un uzdevumi:

5.2.1. Personas lietu biogrāfiskā meklēšana;

5.2.2. Personas biometriskā identifikācija;

5.2.3. Personas lietas apskate;

5.2.4. Personas lietas rediģēšana;

5.2.5. Biometrisko datu konfliktsituāciju apstrāde;

5.2.6. Neapstrādātu personas lietu atlase, to nodošana apskatei un apstrādei;

5.2.7. Nepilnīgu biogrāfisko datu apstrāde;

5.2.8. Personas lietu salīdzināšana;

5.2.9. Personas lietas dzēšanas pieprasījuma apstiprinājums;

5.2.10. Personas lietas biometrijas elementa dzēšanas apstiprinājums;

5.2.11. Personas lietas biogrāfijas izmaiņu vēsture;

5.2.12. Personas lietas izmaiņu vēsture (atribūtdatu izmaiņas);

5.2.13. Personas biometriskās identifikācijas pieprasījums un sadarbība ar ārējām sistēmām (Pruem, Eurodac).

5.3. Lietojumprogrammas FEW (sejas ekspertu darbstacija) mērķis un uzdevumi:

5.3.1. Lietas izveide – sistēma nodrošina lietas izveidi, kuras ietvaros ir iegūti digitālie sejas attēli;

5.3.2. Video failu apstrāde – sistēma nodrošina video failu apstrādi, sejas attēlu izgūšanu no video failiem;

5.3.3. Sejas attēlu apstrāde – sistēma nodrošina sejas attēlu apstrādi, digitālu uzlabošanu;

5.3.4. Sejas attēlu meklēšana – sistēma nodrošina sejas attēla meklēšanu centrālajā sistēmā, kā arī lokālajā galerijā;

5.3.5. Sejas attēlu salīdzināšana – sistēma nodrošina divu sejas attēlu salīdzināšanu un līdzīgo punktu izdalīšanu vizuāliem līdzekļiem. Tāpat sistēma nodrošina divu sejas attēlu salīdzināšanu, kas saņemti no CAPS IDM identitātes pārvaldības lietojumprogrammas.

5.4. Lietojumprogrammas TEW (pirkstu nospiedumu ekspertu darbstacija) mērķi un uzdevumi:

5.4.1. Personas pievienošana (enroll) izmantojot daktilokartes – sistēma nodrošina iespēju ieskenēt vai augšupielādēt daktilokarti, norādīt biogrāfisko informāciju par pievienojamo personu un veikt tās pievienošanu sistēmā;

5.4.2. Pirkstu nospiedumu meklēšana – sistēma nodrošina iespēju ieskenēt vai augšupielādēt daktilokarti un veikt daktilokartē norādītas biometrijas identifikāciju sistēmā;

5.4.3. Pirkstu nospiedumu salīdzināšana – sistēma nodrošina pirkstu nospiedumu salīdzināšanu. Tāpat sistēma nodrošina divu pirkstu nospiedumu attēlu salīdzināšanu, kas saņemti no CAPS IDM.

5.5. Lietojumprogramma LEW (latento datu ekspertu darbstacija) mērķis un uzdevumi:

5.5.1. Lietas izveide – sistēma nodrošina lietas izveidi, kuras ietvaros ir iegūti latentie dati;

5.5.2. Latentā elementa pievienošana – sistēma nodrošina latentā elementa pievienošanu (enroll) latento elementu datubāzē;

5.5.3. Latentā elementa izņemšana – sistēma nodrošina latentā elementa izņemšanu no latento elementu datubāzes;

5.5.4. Latentā elementa meklēšana – sistēma nodrošina latentā elementa meklēšanu latento elementu datubāzē un centrālajā sistēmā;

5.5.5. Latentā elementa apstrāde – sistēma nodrošina latentā elementa apstrādi.

5.6. Apakšsistēmas AQS (rindu mašīna) mērķi un uzdevumi:

5.6.1. Darba plūsmas pārvaldnieka komponente, kas nodrošina vienmērīgu informācijas apmaiņu starp ekspertu lietojumprogrammām un biometrijas sistēmu.

5.7. Apakšsistēma ASM (ekspertu lietu krātuve)

5.7.1. Seju ekspertu un latento ekspertu lietu krātuve, kurā tiek glabātas izmeklējamās lietas. Sistēma nodrošina lietu administrēšanas funkcionalitāti.

5.8. Apakšsistēma ABIS (biometriskās meklēšanas dzinis)

5.8.1. Biometriskās meklēšanas dzinis, kas nodrošina veidņu veidošanu, kvalitātes novērtēšanu un veidņu salīdzināšanu (meklēšanu pēc biometriskās informācijas).

5.9. Administrēšanas WEB lietojumprogramma (WEBADMIN)

5.9.1. Auditācija pierakstu konfigurēšana pārlūkošana;

5.9.2. Uzraudzības sarakstu darbību apskate;

5.9.3. Uzraudzības sarakstu apskate;

5.9.4. Auditācijas pierakstu apskate;

5.9.5. Administratoru apziņošanas sarakstu konfigurēšana;

5.9.6. Sistēmas kļūdu saraksta apskate;

5.9.7. Nekvalitatīvo datu masīva apskate;

5.9.8. Nekvalitatīvo datu masīva tīrīšana.

5.10. Latvija.lv e-pakalpojums

5.10.1. E-pakalpojums Latvija.lv ir Latvijas valsts portāls (www.latvija.lv), kura mērķis ir nodrošināt Latvijas un ārvalstu iedzīvotājiem pieeju Latvijas valsts institūciju interneta resursiem un centralizētu piekļuvi dažādu institūciju sniegtajiem elektroniskajiem pakalpojumiem. Biometrijas e-pakalpojums „Mani dati Biometrijas datu apstrādes sistēmā" nodrošina iegūt un pārbaudīt informāciju par lietotāja datiem, kas tiek uzturēti Biometrijas datu apstrādes sistēmā.

5.11. Integrācijas slānis

5.11.1. SOA WF – darba plūsmu vadība;

5.11.2. WS – tīmekļa apkalpes darba plūsmām nepieciešamo servisu nodrošināšanai.

6. Izmantotās tehnoloģijas

6.1. BDAS izmantoto tehnoloģiju saraksts.

6.1.1. Datubāzes serveris – Oracle 11GR2;

6.1.2. Lietojumserveris – Oracle SOA Suite 11g;

6.1.3. Lietojumprogramma datu ievadam – MS .NET, Web-Services;

6.1.4. Lietojumprogramma datu meklēšanai – MS .NET, Web-Services;

6.1.5. Tīmekļa saskarnes – Oracle SOA Suite 11g, MS .NET;

6.1.6. Biometriskās meklēšanas dzinis – MorphoTrust ABIS Search Engine 6;

6.1.7. Biometriskās verifikācijas un kvalitātes novērtēšanas bibliotēka – MorphoTrust Foundation SDK 8.7.

6.2. Ārējās programmatūras saskarnes.

6.2.1. Oracle WebLogis Server;

6.2.2. Oracle SOA Suite.

III IZPILDĪTĀJA VEICAMIE DARBI

9. Veicamo darbu izpildes termiņš

9.1. Zemāk minētos darbus jāizpilda ne ilgāk, kā sešu mēnešu laikā no pakalpojuma līguma parakstīšanas dienas. Tehniskajā piedāvājumā ir jānorāda katra uzdevuma plānotais izpildes termiņš.

9.2. Vispārīgās vienošanās darbības laikā var tikt pasūtīti arī citi, šajā tehniskajā specifikācijā nedefinēti izmaiņu pieprasījumi, kuru tehniskā specifikācija un izpildes termiņš tiks definēts uzaicinājumā. Šādu izmaiņu realizācijas kārtība ir atrunāta Vispārīgajā vienošanās.

10. Funkcionālās prasības

10.1. ***Automātiska personas lietu dzēšana no Migrācijas masīva (BDAS/FN_EURODAC_2017_01):***

10.1.1. Jāizveido automātiska Migrācijas masīvā esošo personas lietu dzēšana pēc glabāšanas termiņa beigām. Glabāšanas termiņa beigas = personas lietas pēdējās aktualizācijas datums + glabāšanas termiņš (mēnešos).

10.1.2. Glabāšanas termiņš visu kategoriju Migrācijas masīva personas lietām ir vienāds, tādēļ ir nepieciešams viens konfigurējams parametrs glabāšanas termiņa norādīšanai. Glabāšanas termiņš (mēnešos) konfigurējams Webadmin aplikācijā.

10.1.3. Pēc veiksmīgas personas lietas dzēšanas jānodrošina apziņošanas e-pasta izsūtīšana uz konfigurācijā norādītajiem e-pastiem.

10.1.4. Nevar dzēst tās personu lietas, kas atrodas neatrisinātā konfliktsituācijā ar citu/ām personu lietām.

10.2. ***Priekšlaicīgi dzēsto Eurodac personas lietu pārvietošana uz Migrācijas masīvu un fiziska dzēšana (BDAS/FN_EURODAC_2017_02):***

10.2.1. Jāpapildina esošo priekšlaicīgo (manuālo) Eurodac masīva personas lietu dzēšanas mehānismu tā, ka, saņemot dzēšanas apstiprinājumu no Eurodac CU, tiktu veikta dzēšamās lietas kopēšana uz Migrācijas masīvu un fiziska dzēšana no Eurodac masīva.

10.2.2. Manuālo dzēšanu iniciē operators, kurš norāda dzēšanas pamatojumu.

10.2.3. Sistēma nosūta dzēšanas pieprasījumu uz Eurodac CU un sagaida atbildi. Ja saņemts dzēšanas apstiprinājums, tad personas lieta tiek kopēta uz Migrācijas masīvu, ievērojot Migrācijas masīva datu kvalitātes un nosacījumu prasības.

10.2.4. Pēc veiksmīgas kopēšanas darbības personas lieta jādzēš no Eurodac masīva un jānodrošina apziņošanas e-pasta izsūtīšana uz konfigurācijā norādītajiem e-pastiem. Ja no Eurodac CU nav saņemts dzēšanas apstiprinājums, tad personas lietā netiek veiktas nekādas izmaiņas.

10.3. ***Eurodac personas lietu vēsturiskās informācijas uzkrāšana (FN_EURODAC_2017_03):***

10.3.1. Jāizstrādā mehānisms Eurodac masīva personas lietu vēsturiskās informācijas uzkrāšanai un attēlošanai CAPS IDM lietojumprogrammā.

10.3.2. Pēc operatora veiktajām izmaiņām personas lietā atļautos datu laukos, piemēram, vārda vai dzimšanas datuma u.c. datu, sākotnēji ievadītie dati jāsaglabā un jāattēlo personas lietas esošajā vēsturisko datu cilnē. Jaunpievienotie dati jāsaglabā pamata datu lauku cilnē. Jānodrošina izmainīto datu kvalitātes kontrole atbilstoši sistēmas nosacījumiem.

10.4. ***INTERPOL NPS NIST sagatavošana un automātiska nosūtīšana uz noteiktām e-pasta adresēm personas īpašai pārbaudei (BDAS/FN_EURODAC_2017_04)***

10.4.1. Jāautomatizē Eurodac un Migrācijas masīvu datu nodošana īpašai pārbaudei ar e-pasta starpniecību, izmantojot konfigurācijā noteiktas e-pasta adreses, gadījumos, kad BDAS tiek reģistrēta jauna Eurodac masīva vai Migrācijas masīva personas lieta. Izpildītājam jāņem vērā, ka e-pasts ir jāizsūta (on behalf of) no noteiktas Pasūtītāja e-pasta adreses, ar nosacījumu, ka e-pasta vēstule tiktu nosūtīta (Reply To) lietotājam, kurš reģistrēja konkrēto personas lietu un uz citām konfigurācijā norādītajām noteiktajām e-pasta adresēm.

10.4.2. Eurodac masīva personas lietām:

- CAT1 kategorijas personas lieta – pēc personas lietas pievienošanas, negaidot atbildi no Eurodac CU, vienmēr automatizēti jānosūta e-pasts uz noteiktām e-pasta adresēm. E-pastam jāsatur INTERPOL NPS NIST datne un papildu informācija. Papildu informācijai jāsatur – personas valstiskā piederība, personas vārds un uzvārds, dzimšanas datums, iesnieguma iesniegšanas / aizturēšanas datums (sūtot e-pastu CAT1 ierakstiem, kā arī ierakstiem pret kuriem bija sakritība ar EURODAC masīvu, e-pasta saturā ir jābūt informācijai – PATVĒRUMA MEKLĒTĀJS, attiecināms uz tiem e-pastiem, kuriem netiek pievienots sejas attēls);
- CAT2 kategorijas personas lieta - pēc personas lietas pievienošanas, negaidot atbildi no Eurodac CU, vienmēr automatizēti jānosūta e-pasts uz noteiktām e-pasta adresēm. E-pastam jāsatur INTERPOL NPS NIST datne, personas sejas attēls (JPEG formātā) un papildu informācija.
- CAT3 kategorijas personas lieta – pēc tam, kad ir saņemta atbilde no Eurodac, automatizēti jānosūta e-pasts uz noteiktām e-pasta adresēm. E-pastam jāsatur:
  - Ja no Eurodac CU ir saņemta No-Hit atbilde, tad INTERPOL NPS NIST datne, personas sejas attēls un papildu informācija;
  - Ja no Eurodac CU ir saņemta Hit atbilde un pēc pirkstu nospiedumu eksperta apstiprinājuma, tad INTERPOL NPS NIST datne un papildu informācija.
- CAT4, CAT9 kategorijas personas lieta - e-pasts uz noteiktām e-pasta adresēm nav jāsūta.

10.4.3. Migrācijas masīva personas lietām:

- Jebkuras kategorijas Migrācijas masīva personas lieta – pēc tam, kad ir veikta pārbaude pret visiem BDAS datu masīviem:
  - Ja pārbaudes rezultātā ir Hit ar Eurodac masīva CAT2, CAT3, CAT9 personas lietu vai ir No-Hit, tad INTERPOL NPS NIST datne, personas sejas attēls un papildu informācija jāsūta uz noteiktām e-pasta adresēm;
  - Ja pārbaudes rezultātā ir Hit ar Eurodac datu masīva CAT1 kategorijas personas lietu, tad jānosūta brīdinājums uz noteiktām e-pasta adresēm.
- Tā kā eksistē situācijas, kad INTERPOL NPS NIST pieprasījuma nosūtīšana uz noteiktām e-pasta adresēm nav iespējama bez lietotāja iesaistes, piem., Migrācijas masīva personas lietām (ja pārbaudes rezultātā ir Hit ar Eurodac datu masīva CAT1 kategorijas personas lietu) tad Migrācijas masīva personas lietām CAPS IDM ir jābūt iespējai no

personas lietas izsaukt e-pasta nosūtīšanu (pēc lietotāja izvēles NPS NIST datnes vai NPS NIST datnes un sejas attēla). Šādā situācijā e-pasta "Reply to" jābūt norādītai personai, kurš izsauca nosūtīšanas procesu.

11. Nefunkcionālās prasības

11.1. *Sistēmas pieejamība (NF_SIST_2017_01):*

11.1.1. Sistēmai jānodrošina 99.96% centrālo mezglu (CBS) darbspēja 1 kalendārā gada mērīšanas periodā.

11.1.2. Izņēmums var būt iepriekš plānoti pārtraukumi, kuri nedrīkst pārsniegt 4 stundas mēnesī. Reglamentētie darbi jāplāno vismaz 3 darba dienas pirms darbu veikšanas. Darbu veikšanas laikā sistēmas darbības pārtraukums nedrīkst pārsniegt 1 stundu.

11.2. *Sistēmas reakcijas laiks (NF_SIST_2017_02):*

11.2.1. Sistēmai jānodrošina šādi reakcijas laiki (gan ievades, gan meklēšanas formās (lietojumprogrammās):

- meklējot pēc indeksētiem laukiem vienas sistēmas ietvaros: 90% gadījumu - ne vairāk kā 4 sekundes, pārējos gadījumos - līdz 30 sekundēm;
- meklējot vienas sistēmas ietvaros pēc neindeksētiem laukiem: 90% gadījumu – ne vairāk kā 30 sekundes, pārējos gadījumos - līdz 60 sekundēm.

11.3. *Datu apmaiņa (NF_SIST_2017_03):*

11.3.1. Datu apmaiņa ar saistītajām sistēmām ir jārealizē, izmantojot esošu datu sistēmas moduli, kur tiek izmantotas SQL, XML, Web Services tehnoloģijas, kā arī SOA Suite darbplūsmas.

11.4. *Servera darbības vide (NF_SIST_2017_04):*

11.4.1. Servera daļai jādarbojas esošajā tehniskajā vidē (MS Windows/RedHatLinux/Sun Solaris platforma).

11.5. *Gala lietotāju interfeiss (NF_SIST_2017_05):*

11.5.1. Gala lietotāju (CAPS, CAPS IDM u.c.) aplikāciju interfeisam ir jābūt latviešu valodā, Sistēmas administrēšanas aplikāciju interfeisi var tikt realizēti gan latviešu, gan angļu valodās.

11.6. *Standartu atbalsts (NF_SIST_2017_06):*

11.6.1. Sistēmā jānodrošina šādu standartu (*vai ekvivalentu standartu*) atbalsts:

- Biometrijas datu apstrāde un sadarbspēja PRĪME – ANSI/NIST-ITL1-2000 standarts;
- Biometrijas datu apstrāde un sadarbspēja PRĪME – ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b) standarta paveids;
- Biometrijas datu apstrāde un sadarbspēja ar ekspertu darbstacijām – EBTS v.9.2.;
- Biometrijas datu apstrāde PRĪME – ANSI X3.4 standarts;
- ANSI INCITS 378-2004 standarts;
- M1-378 standarts;
- Pirksta papillārlīniju detaļu dati - ISO/IEC 19794-2:2005;
- Pirkstu nospiedumu attēli - ISO/IEC 19794-4:2005;
- Sejas attēli - ISO/IEC 19794-5:2005;

- Biometrijas datu apstrāde un sadarbspēja - ANSI/NIST –ITL 1-2007 Data Format for the Interchange Of Fingerprint, Facial & Other Biometric Information – Part 1; ANSI/NIST –ITL 2-2008 Data Format for the Interchange Of Fingerprint, Facial & Other Biometric Information – Part 2;
- Pirkstu nospiedumu attēlu uzglabāšana jānodrošina WSQ formātā, atbilstoši ANSI/NIST-ITL 1-2000. Piedāvātajam WSQ kodēšanas un dekodēšanas risinājumam (encoder/decoder) ir jābūt FIB sertificētam (http://www.fbibiospecs.org/wsq/Implementations/Default.aspx);
- Sejas attēlu uzglabāšanai jāatbalsta looseless JPEG standarts, saskaņā ar ISO/IEC IS 14495-1 | ITU-T Recommendation T.87;
- Biometrijas datu kvalitātes kontroles pasākumi jānodrošina, saskaņā ar standartos ANSI/NIST –ITL 1-2007 un ANSI/NIST –ITL 2-2008 aprakstītiem mehānismiem;
- Datu apritei jānotiek saskaņā ar Starptautiskās biometrijas industrijas asociācijas datu standartu CBEFF, atbilstoši standartam ISO/IEC 19785-1.

11.7. ***Vispārējās veiktspējas prasības (NF_SIST_2017_07):***

11.7.1. Sistēmai jānodrošina vismaz šāda apjoma pieprasījumu apstrāde, ievērojot visu šajā tehniskajā specifikācijā norādīto funkcionālo un nefunkcionālo prasību izpildi:

- 2000 datu aktualizācijas pieprasījumi dienā (personas lietu izveide, aktualizācija, izdruka, dzēšana un apskate);
- 30000 verifikācijas meklēšanas pieprasījumi dienā;
- 2000 identifikācijas meklēšanas pieprasījumi dienā.

11.8. ***Lietotāju skaits (NF_SIST_2017_08):***

11.8.1. Sistēmai jānodrošina vismaz šāds lietotāju skaits, ievērojot Sistēmai noteiktos ātrdarbības un veiktspējas kritērijus:

- Datu aktualizētāji, Verifikācijas un Identifikācijas lietotāji – 350 vienlaicīgie / 2500 kopējie lietotāji;
- Latento datu un video plūsmu ierakstu apstrādes izmantotāji – 30 vienlaicīgie / 50 kopējie lietotāji;
- Video plūsmu reāllaika apstrādes izmantotāji – 50 vienlaicīgie / 50 kopējie lietotāji;
- Identitātes pārvaldnieki – 4 vienlaicīgie / 4 kopējie lietotāji;
- EURODAC eksperti – 5 vienlaicīgie / 50 kopējie lietotāji;
- PRĪME eksperti – 5 vienlaicīgie / 50 kopējie lietotāji.

11.9. ***Valodu kodējuma atbalsts (NF_SIST_2017_09):***

11.9.1. Teksta informācijas apstrādei un uzglabāšanai sistēmai jānodrošina UTF-8 kodējuma atbalsts.

11.10. ***Uzglabājamās informācijas apjoms (NF_SIST_2017_10):***

11.10.1. Sistēmai jānodrošina vismaz šāda apjoma datu uzglabāšana, ievērojot visas šajā tehniskajā specifikācijā norādītās funkcionālās un nefunkcionālās prasības:

- Jānodrošina kopumā 3 500 000 civiliedzīvotāju un krimināli sodīto personu lietu apstrāde;
- Vienas personas lietas, kas saistīta ar civiliedzīvotāju, apjoms - 2 uzspiesti nospiedumi, 3 sejas attēli (viens attēls "aktīvs, divi arhīvā);
- No kopējo personas lietu skaita 350 000 lietu jābūt paplašināmām ar papildu biometrisko informāciju, kas attiecas uz krimināli sodītām personām, paplašināšanas apjoms - 10 uzspiesti nospiedumi, 10 pārvelti nospiedumi, 3 sejas attēli, 2 delnu nospiedumi, 4 delnu detaļu nospiedumi; Latentie dati – biometrijas datu elementi kopā 100 000 latento biometrijas datu elementi.

11.11. ***Pieprasījumu atsekojamība (NF_SIST_2017_11):***

11.11.1. Sistēmas administratoram jānodrošina saskarne, kurā viņš varētu apskatīt jebkura izejošā vai ienākošā pieprasījuma stāvokli, katra atsevišķa soļa izpildi, izpildes ilgumu, kā arī rezultātu. Tāpat jānodrošina filtrēšanas iespējas, lai būtu iespējams atlasīt pieprasījumus, kuri izpildi ir beiguši ar sistēmas kļūdu.

11.12. ***Meklēšana – Personas lietas meklēšana pēc biogrāfiskajiem un atribūtdatiem, biometriskā meklēšana (NF_SIST_2017_12):***

11.12.1. Ir jānodrošina šādi personas lietas meklēšanas ātrdarbības minimālie parametri:

- Meklējot pēc unikāla personas identifikatora - 0.5 sekundes (no brīža, kad atbilstošā BDAS centralizēti izvietotā komponente ir saņēmusi meklēšanas pieprasījumu, līdz brīdim, kad tā sagatavo meklēšanas rezultātu sarakstu);
- Meklējot pēc personas vārda, uzvārda, dzimšanas datuma – 10 sekundes (no brīža, kad atbilstošā BDAS centralizēti izvietotā komponente ir saņēmusi meklēšanas pieprasījumu, līdz brīdim, kad tā sagatavo meklēšanas rezultātu sarakstu);
- Verifikācijas meklēšana (1:1 meklēšana) – 2 sekundes (no brīža, kad atbilstošā BDAS centralizēti izvietotā komponente ir saņēmusi meklēšanas pieprasījumu, līdz brīdim, kad tā sagatavo atbilstības sarakstu);
- Identifikācijas meklēšana (1:n meklēšana) – 5 sekundes (no brīža, kad atbilstošā BDAS centralizēti izvietotā komponente ir saņēmusi meklēšanas pieprasījumu, līdz brīdim, kad tā sagatavo atbilstības sarakstu).

11.13. ***Darba plūsmas izpildes stāvokļa saglabāšanas punkti (NF_SIST_2017_13):***

11.13.1. Pieprasījumu apstrādes darba plūsmā pēc jebkura pieprasījuma saglabāt datus biometrijas datu apstrādes sistēmā un pirms nākamā darba plūsmas soļa izpildes jānodrošina stāvokļa saglabāšanas punkts, kurā tiek saglabāts darba plūsmas izpildes stāvoklis un jebkuras kļūdas gadījumā (kas radīsies tālākā procesa izpildē) no šī punkta tiek turpināta procesa izpilde pēc kļūdas novēršanas.

12. Prasības nodevumiem

12.1. Izpildītājam Vispārīgās vienošanās darbības laikā ir jānodrošina sekojošu nodevumu sagatavošana un iesniegšana pasūtītājam (katram pakalpojumu līgumam atsevišķi):

12.1.1. sistēmas dokumentācijas (Programmatūras prasību specifikācija, Programmatūras projektējuma apraksts, Lietotāju rokasgrāmatas, Administratora rokasgrāmata) papildināšana atbilstoši veiktajām izmaiņām;

12.1.2. Programmatūras pirmkods un izpildāmais kods;

12.1.3. Piegādes uzstādīšanas apraksts;

12.1.4. Piegādes apraksts, kas satur realizēto prasību sarakstu;

12.1.5. Akceptēšanas kritēriji vai pēc pasūtītāja pieprasījuma testēšanas piemēri/apraksti;

12.1.6. Nodevuma izvērtējuma forma.

13. Atbilstība normatīvajiem aktiem

13.1. Izpildītājam, ņemot vērā visas šajā dokumentā uzskaitītās prasības, ir jāveic darbu realizācija, nodrošinot atbilstību šādiem dokumentiem un normatīvajiem aktiem:

13.1.1. Biometrijas datu apstrādes sistēmas likums;

13.1.2. Ministru kabineta 2014.gada 6.maija noteikumi Nr.234 "Biometrijas datu apstrādes sistēmas noteikumi";

13.1.3. Eiropas Parlamenta un Padomes 2013.gada 26.jūnija regula Nr. 603/2013;

13.1.4. Patvēruma likums (5.panta piektā daļa);

13.1.5. Ministru kabineta 2016.gada 17.miaja noteikumi Nr.296 "Patvēruma meklētāju pirkstu nospiedumu informācijas sistēmas noteikumi";

13.1.6. Imigrācijas likums (3.panta trešā daļa, 51.pants, 60.pants);

13.1.7. Ministru kabineta 2009.gada 3.februāra noteikumi Nr.99 "Noteikumi par automatizētās pirkstu nospiedumu identifikācijas sistēmā (AFIS) iekļaujamās informācijas apjomu un izmantošanas kārtību";

13.1.8. Eiropas Padomes lēmums Nr.2008/616/TI (daktiloskopijas datu apmaiņas noteikumi);

13.1.9. Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām";

13.1.10. Valsts informācijas sistēmu likums;

13.1.11. Informācijas tehnoloģiju drošības likums;

13.1.12. Fizisko personu datu aizsardzības likums.

13.2. Pakalpojumu realizācijas ietvaros Izpildītāja radītais pirmkods ir Pasūtītāja īpašums.

14. Vispārējās drošības prasības

14.1. Veicot informācijas sistēmu pilnveidošanu Vispārējās vienošanās ietvaros, Izpildītājam ir jāievēro šādi drošības politikas nosacījumi:

14.2. Sistēmas lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;

14.3. Sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

14.4. Jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam (ja darbību veic autentificēts lietotājs) un interneta protokola (IP) adresei;

14.5. Sistēmas funkcionalitāte ir īstenojama ar minimāli iespējamām sistēmas līmeņa tiesībām (privilēģijām). Dokumentācijā jāapraksta un jāpamato visas sistēmas darbināšanai nepieciešamās tiesības.

14.6. Sistēmas auditācijas pieraksti tiek veidoti, nodrošinot, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar vienas sekundes precizitāti;

14.7. Sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību

atrisinātu kļūdu. Papildus sistēmas atbalsta personālam jānodrošina detalizētas tehniskās informācijas par kļūdu pieejamība (piem., auditācijas pierakstos);

14.8. Veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmā glabāto datu integritātei;

14.9. Jānodrošina informācijas integritātes saglabāšana (pilnīgas un nemainītas informācijas saglabāšana);

14.10. Jānodrošina informācijas konfidencialitāte (piekļuve informācijai nodrošināma tikai tām personām, kurām ir atbilstošas piekļuves tiesības);

14.11. Veicot sistēmas izstrādi nav pieļaujama tās pirmkoda nodošana nepilnvarotām personām (Pasūtītājs tiek informēts par visām personām kam ir pieeja pirmkodam);

14.12. Sistēmu veido tā, ka to darbinot tiek atslēgtas (atspējotas vai izdzēstas) visas iekļautās, bet neizmantotās komponentes vai to funkcionalitāte (piem., datortīkla pakalpojumus) un attiecīgi dokumentācijā aprakstot veicamās darbības neizmantoto komponenšu atslēgšanai;

14.13. Sistēmu veido tā, lai tiktu nodrošināta datu plūsmas kontrole starp sistēmas komponentēm un dokumentācijā aprakstot realizāciju;

14.14. Sistēmā paredz funkcionalitāti tās automatizētai darbspējas pārbaudei (visu darbībai komponenšu darbspējas uzraudzība). Dokumentācijā apraksta darbspējas pārbaudes funkcionalitāti;

14.15. Dokumentācijā apraksta sistēmā izmantotās aizsardzības metodes (datu ievades kontrole, datu plūsmu kontrole u.c.);

14.16. Dokumentācijā uzskaita potenciālos drošības apdraudējumus, to tuvošanās vai iestāšanās pazīmes un sagatavo ieteikumus sistēmas drošības (pieejamība, integritāte, konfidencialitāte) nodrošināšanai;

14.17. Dokumentācijā uzskaita visas izmantotās šifru metodes, paroles un atslēgas, apraksta to nomaiņas kārtību;

14.18. Dokumentācijā uzskaita visu komponenšu auditācijas pierakstu atrašanās vietu, apraksta to struktūru un nozīmi. Apraksta un nodrošina auditācijas pierakstu lasīšanas iespējamību, kā arī darbības to dzēšanai pārceļot tos glabāšanai uz ārēju datu nesēju;

14.19. Pēc Pasūtītāja pieprasījuma Izpildītājs sadarbojas ar Pasūtītāju sistēmas drošības pārbaudes nodrošināšanai un atklāto trūkumu novēršanai.