IOM

Terms of Reference

Kosovo Police Biometric Identification System (BIS)

Contents

[1 Background 4](#_Toc168650874)

[2 Objectives 4](#_Toc168650875)

[3 Scope 5](#_Toc168650876)

[4 Legal Basis 5](#_Toc168650877)

[5 Infrastructure Requirements 6](#_Toc168650878)

[5.1 Server Infrastructure 6](#_Toc168650879)

[5.2 Equipment Infrastructure 7](#_Toc168650880)

[6 Functional Requirements 9](#_Toc168650881)

[6.1 Front-End (Website) 9](#_Toc168650882)

[6.2 Back-End 11](#_Toc168650883)

[6.2.1 Data and Database 11](#_Toc168650884)

[6.3 Mobile Application 13](#_Toc168650885)

[7 Business Process 15](#_Toc168650886)

[7.1.1 Incoming Collections 16](#_Toc168650887)

[7.1.2 Outgoing Collections 17](#_Toc168650888)

[7.1.3 Enrolments UI 19](#_Toc168650889)

[7.1.4 Reports and Statistics 20](#_Toc168650890)

[7.1.5 Auditing 22](#_Toc168650891)

[8 Personal and Biometric Data 23](#_Toc168650892)

[8.1 Personal Data 23](#_Toc168650893)

[8.2 Biometric Data 24](#_Toc168650894)

[8.3 Registration process 25](#_Toc168650895)

[8.3.1 NIST Application 25](#_Toc168650896)

[8.3.2 Gateway 26](#_Toc168650897)

[8.3.3 Orchestration 27](#_Toc168650898)

[8.3.4 Store 27](#_Toc168650899)

[9 Integrations 27](#_Toc168650900)

[9.1.1 Integration 28](#_Toc168650901)

[9.1.2 Interconnectivity 28](#_Toc168650902)

[9.1.3 APIs Description 30](#_Toc168650903)

[9.1.4 Integration of other Biometrics (SEEK) 32](#_Toc168650904)

[9.1.5 Checking and Matching 33](#_Toc168650905)

[9.1.6 Alerting and Notification 34](#_Toc168650906)

[10 Backups and Recovery 35](#_Toc168650907)

[11 Security and Access Permissions 35](#_Toc168650908)

[12 Administrative Requirements 37](#_Toc168650909)

[13 Cost 37](#_Toc168650910)

[14 Implementation Plan 38](#_Toc168650911)

**Glossary**

|  |  |
| --- | --- |
| **Term** | **Meaning** |
| AFIS | Automated Fingerprint Identification System. |
| KP | Kosovo Police |
| MIA | Ministry of Internal Affairs |
| DPD | Department for Producing Documents |
| ILECU | International Law Enforcement Cooperation Unit |
| BIS | Biometric Identification System |
| BMS | Border Management System |
| KVIS | Kosovo Visa Information System |
| DCAM | Department for Citizenship Asylum and Migration |
| NIST | National Institute for Standards and Technology |

# Background

The current situation at Kosovo Police's Border Police Department, specifically within the Migration and Foreigner Division, is the lack of a system for the identification and registration of biometric data for foreigners, migrants, asylum seekers and other individuals of interest to the police. Presently, their operations rely on paper documentation. Initially, this was due to the absence of legal provisions for the digitalization and storage of biometric information. However, it has been determined that under the existing legal framework and procedures, detailed in Section 4, the Kosovo Police is authorized and has the full capability to collect and store biometric data, including fingerprints of individuals. This authority is explicitly outlined in Section 4 (Legal Basis).

Several entities are involved with biometric data, including the Kosovo Police as the primary authority, the Ministry of Internal Affairs (MIA), the Agency of Forensics (AFIS), and the Department of Producing Documents (DPD) within the Civil Registration Agency. Within these organizations, there are specific systems that will utilize the biometric data, particularly fingerprints. In terms of IT infrastructure, the Kosovo Police is entirely self-sufficient, owning its infrastructure, data centers, and software applications, all managed by its IT Sector. Therefore, the development of a new biometric identification system should be implemented within the Kosovo Police using the existing infrastructure.

# Objectives

The primary goal of this initiative is to improve migration management in Kosovo by adopting an evidence-driven, comprehensive strategy, thereby leveraging migration to foster sustainable development within the country. Specifically, the initiative aims to bolster the capabilities of Kosovo's authorities in managing migration more effectively. This includes enhancing the skills, knowledge, and operational processes of pertinent institutions, increasing the capacity to admit migrants, offering technical and logistical assistance, improving data gathering across various sectors, raising awareness among Kosovans about the risks of irregular migration, and fostering greater involvement with the diaspora community.

The project sets out specific objectives with well-defined targets. Its foremost aim is to modernize the system for registering migrants through a digitalization process. This process, which is complex by nature, encompasses a series of business workflows designed to capture and store biometric data of individuals. The document outlines the key objectives and goals of the project in detail:

1. To gather/collect digital data evidence of migrants and police actions and interactions related to them.
2. Effective storage of work data and efficient use of work data of the Directorate for Migration and Foreigners.
3. Intelligent check and comparison with the other biometric data enrolled, current data available at Kosovo Police systems for wanted persons those who are in stopwatch lists and additional check AFIS for criminal offences database based on fingerprints.
4. Generate statistical reports which derive from analytical reports conducted by Kosovo Police.
5. Create an easy process of finding information for foreign nationals and quick provision of migration information for foreigners, in Kosovo, based on the competencies of the local and central level and based on the immediate need to be informed, thus complying with the legal provisions on the Law on Foreigners No. 06 L-219, Law on Asylum No. 06/L-026, and the Law on personal data protection No. 06/L-082.
6. Increased efficiency of the return process;
7. Raising the awareness of the return situation (i.e., improving statistical reporting);
8. Adaptability to new circumstance, e.g., new legal implications;
9. Protection of vulnerable groups.

# Scope

To enhance the capabilities of Kosovo's Border Police Department, the Swiss Government has donated biometric equipment, aimed to facilitate the registration and identification of individuals through biometric enrollment system. There is a pressing requirement for the development of software to link and ensure compatibility with this equipment. This software will not only record migrants' biometric information but also maintain and amalgamate this data across all existing systems utilized by the Directorate for Migrants and Foreigners.

The initiative will assist the Border Police in creating novel software designed to archive data, identification papers, and other digital biometric scans securely. The entire process will prioritize data protection. This software will incorporate the Automated Fingerprint Identification Systems (AFIS) to analyze and match fingerprints and photographs. It must also deliver instantaneous updates on verification results and data gathering activities.

Furthermore, the software will integrate with other databases accessed by the Border Police and the Ministry of Internal Affairs, including the Kosovo Police Information System (KPIS), the Border Management System (BMS), DCAM, and the Kosovo Visa Information System (KVIS). The plan is to deploy the software application on all computers operated by personnel tasked with registering and identifying foreign nationals. The software will also be capable of producing statistical reports tailored to the requirements of the Border Department and the Directorate for Migrants and Foreigners, utilizing the data within the database.

# Legal Basis

The Biometric Identification System of the Kosovo Police must adhere to the established legal and procedural standards for handling, processing, and accessing biometric information. To this end, the legal foundation is articulated within the regulatory structure of the Law on Asylum, the Law on Foreigners, and the Law on Data Protection. Additionally, the Kosovo Police sought legal clarification to determine whether the use, processing, and storage of biometric data within its facilities would infringe upon data protection and privacy rights. According to interpretations provided by the legal office of Kosovo Police, the current legal framework of Kosovo Police permits the Kosovo Police to handle, administer, and process the biometric data gathered for investigative or any other purposes. Furthermore, the subsequent text will detail the legal underpinnings and the current legal context concerning the handling, processing, and access to biometric information.

**Law for Asylum**

Article 101, Paragraph 4.3

Article 103, Paragraphs 1 and 2

Article 104, 105,106,107

**Law for Foreigners**

Article 21, Paragraph 1, Paragraph 2

Article 120, Paragraph 3.3

**Law for Data Protection**

Article 3, Paragraph 1.11

If there is necessary for more elaboration of the mentioned Laws, Articles and Paragraphs pointed out in above text, please refer to the annex of this terms of refence document.

# Infrastructure Requirements

The current infrastructure of Kosovo Police will be available to the new developed system “Biometric Identification System”. It means that Kosovo Police will ensure the Server Infrastructure including the adequate Operating Systems Licenses for hosting the developed system with the technical requirements defined in next sessions. In following subsections are defined the Server Infrastructure including licenses and Equipment Infrastructure.

## 5.1 Server Infrastructure

In Table 1 and Table2 are shown the requirements of hardware resources as pre-condition for hosting the BIS (Kosovo Police Biometric Identification System).

**Table 1**. Hardware Resources Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Server Description** | **Minimum Performance** | **Operating System** | **QTY** |
| 1 | Application Server\* | 4 vCpu, 32 GB RAM, 100 GB HDD SSD | Windows Server 2019/2022 Standard Edition | 2 |
| 2 | Database Server | 8 vCPU, 64 GB RAM, 300 GB SSD | Windows Server 2019/2022 Standard Edition | 1 |

\* *If BIS is going to be hosted at BMS application, there is no need to setup new application server (No 1, Table 1). But can be used the existing ones. In case of separate server, the Application Server should be setup.*

As is shown in the Table 1, the total number of servers will be 3 that needs to be allocated for KBIS. Servers can be Virtual Servers hosted in **VMware** or **Hyper-V** or any other Hypervisor that Kosovo Police uses.

\*Note: The Windows and Microsoft SQL Server Licenses must be ensured by Kosovo Police. Regarding the type and no of licenses, please refer to Table 2.

**Table 2**. Licenses Required

|  |  |  |
| --- | --- | --- |
| **No** | **License Type** | **QTY** |
| 1 | Windows Server 2019/2022 Standard Edition (Desktop Experience) \* | 2 |
| 2 | Microsoft SQL Server 2019 Standard Edition | 1 |

*\*Similar as explained in above text.*

## 5.2 Equipment Infrastructure

Besides the server part as crucial part for hosting the BIS, there are some other equipment as integral part that Kosovo Police currently have on use. These equipment’s are in use by Kosovo Border Police – Directorate for Migration and Foreigners to scan the fingerprints of migrants/foreigners and asylum appliers with the aim of checking with the AFIS system. Equipment’s are dislocated and distributed in several locations such: border crossing points, regional border police offices or in green border stations. In Table 3, we have shown the Static Scanners and Tablets distributed in the Central Office of Border Police, Regions and Border Crossing Points, Border Stations and on Field used by Green Border Patrols during the border line patrol tours.

**Table 3**. Fingerprint Scanners and Tablets

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Type** | **Model** | **QTY** |
| 1 | Scanner | Dacty Scan 40i | 30 |
| 2 | Tablets | Chameleon Single Plus 8 | 26 |

 **Figure 1.** Dacty Scan 40i and Chameleon Single Plus Tablet



While, regarding the SDK licenses, Kosovo Police provides the licenses for these equipment’s that ensures the communication with the AFIS system. Please refer to Table 4.

**Table 4.** Licenses for communication with AFIS

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Type** | **License Type** | **QTY** |
| 1 | License | Thales Web ID | 30 |
| 2 | License | Thales Web ID | 26 |

Consider that the existing licenses are in use only for checking (find and match) of the scanned fingerprints by those scanners with the AFIS system.

**NOTE:** The current licenses **DO NOT** support the enrollment/storage of fingerprints! For enrollment/storage of fingerprints, other licenses/SDKs should take place.

These relevant licenses will not be provided by Kosovo Police as beneficiary party. But should be ensured by Economic Operator who will be in charge for installation, configuration and development of BIS. Licenses should be provided by EO life-time.

The developed system BIS must be able to use the existing equipment’s shown in Table 3 with no need to change the equipment’s. In addition, it should support the extension or adding the additional equipment’s or replacing the existing damaged ones by ensuring compatibility and functionality.

# Functional Requirements

In this session are shown the functional requirements for each component of the BIS system. As a system is considered very complex due to the large number of integrations as well as interoperability with other systems. In this regard, BIS system is composed by following components:

-Front-End (UI Interface)

-Backend (Databases, APIs and Services)

-Mobile Application (Tablets)

## Front-End (Website)

The front-end User Interface (UI) should be developed in ASP .NET MVC as other KPs web applications. In this regard, it is recommended to be integrated within the exiting Border Management System (BMS) UI web application but running as independent module named “Biometric Identification”.

This integration as integral part of BMS is due to the need for unification of the KP systems through integration and no need for creating separate interfaces for authentication. Development and hosting separately as Standalone shall be only in case of special request from KP, otherwise it should be integrated within BMS as separate module.

Figure 2. BIS integration in BMS

BMS

BIS

In following shapes are shown the BIS modules and how UI will view nearby:

**Figure 3**. Modules of BIS

Incoming Collections

Outgoing Collections

Enrolments

Reports & Statistics

Audit

In Table 5 are shown the general functional requirements for the Front-End UI interface.

**Table 5**. List of Functional Requirements for UI

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.0 | UI should be designed to use visual colours similar as existing BMS interface (blue with white including state of aim of Kosovo Police, Border Police etc.).  In case of separately hosted, there is no specific colour requested but should be in accordance with KP using similar pattern as other KP applications. |
| 7.1.1 | UI should provide interfaces in three languages, Albanian, Serbian and English. |
| 7.1.2 | User should be authenticated using KP Active Directory (LDAP) with no need for additional accounts but using KP official accounts (email addresses). |
| 7.1.3 | The access permission should be organized using Active Directory groups as KP do with other applications. Please refer to Section 12, Access Permissions organization. |
| 7.1.4 | Due to security risk, UI should be auto-logoff in case of inactivity for 5 mins. |
| 7.1.5 | An SSL Certificate should be used by UI in order to provide secured connection. There can be used the existing SSL or purchasing the new one. |
| 7.1.6 | UI should be accessible from anywhere within network of Kosovo Police |

## 6.2 Back-End

The back-end of a computer system, website, or application refers to the part that is not visible to the user and encompasses the servers, databases, and server-side applications that power the front-end, or user interface. It is responsible for storing and managing data, ensuring that everything on the front-end functions correctly by executing back-end code and applications. The back-end communicates with the front-end by sending and receiving information to be displayed as a web page, app screen, or other interface.

### Data and Database

Database should be developed in Microsoft SQL Server using one of the latest versions of MSSQL at least 2019 or newer. This should be done in accordance with Kosovo Police IT department because of the licenses and compatibility with the existing databases since the BIS will be connected with other databases within Kosovo Police.

**Database Platform: Microsoft SQL Server 2019 Standard Edition**

**Databases:**

* + **OLTP Transactional Database (BIS)**
  + **OLAP Datawarehouse Database (BIS\_DW)**

There should be a standalone server (VM) dedicated only for BIS system because of the expensive queries that might be generated especially for matching and comparing with exiting fingerprints collected.

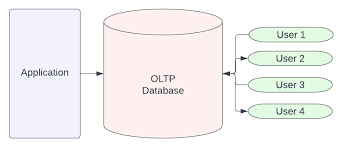
The both databases can be placed on the same MS SQL Instance (within VM) but in case of any suggestion or if Kosovo Police has enough resources and suggests, databases can be deployed as separated in two different VMs that means two different instances.

**NOTE**: Using of two different server instances per database will need two other licenses for Microsoft Windows Server 2019/2022 and Microsoft SQL Server Standard Edition 2019.

**Transactional Database (BIS)**

This database will be used for storing the data of the collected fingerprints and other biometric data enrollments such: images, iris, personal data and other relevant data provided by persons interviewed by Police that will be registered.

**Figure 4**. Transactional Database Illustration



Data should be stored using the traditional ER relationships and the communication of databases with the front-end application, APIs back-end should be done using Microsoft SQL Stored Procedures. Procedures should be designed to be efficient and well optimized using the conventional names based on standards as in following example: (Procedure number, name of procedure based on application who calls it, other number if for specific caller exist more than one procedure) as in example:

*02\_FingerprintCheck\_Call\_01*

*03\_FingerprintInsert\_Call\_01*

*04\_FingerprintMatch\_Call\_01 etc.*

In case of necessary if SQL tables are much loaded (frequent reads/writes) and should be optimized, there should be considered using In-Memory technology provided by Microsoft SQL Server.

Regarding the accessibility, a login user should be used (BIS) as communication interface between application front-end, back-end and other components of kbis application. While interconnectivity in database level with other systems/databases will be done using different users explained at interconnectivity session of this document.

**OLAP Datawarehouse Database (BIS\_DW)**

Datawarehouse should be deployed especially for generating statistics and reports. It would prevent the overloading of the transactional database (OLTP) and will prevent the fails in case of any possible failure or deadlock of the OLTP database. In addition, the Datawarehouse database should not be a copy of the OLTP database but it should content the only data that will be used for statistical reports.

Implementation of Datawarehouse should be based on ETL data transformation using the best models and practices. Since the Datawarehouse database will be placed for analytics, reports and statistics. There are few data sources that will be subject of ETL data transformation and then will be inserted at Datawarehouse. So, the Datawarehouse will serve as data pool that will collect the data not only from BIS system but will be connected with other data-sources such: BMS, KPIS and DCAM. This Datawarehouse that will have the affinity to collect and transform the data from other data sources, will ensure accuracy on the statistics reports and will provide different types of reports and possibility for further analysis.

**Main Data sources:**

BIS (Biometric Enrollment Transactional Database)

DCAM (Database for Citizenship, Asylum and Migration)

**Other Data sources**

BMS (Border Management System)

KPIS (Kosovo Police Information System)

Regarding the data flow from the data sources to the Datawarehouse, there are few models that could be applied such: Replication, Data Collection (Insertion) based on scheduled jobs (every 10’ or every 30 ‘) or using SSIS Package. The preferable version would be SSIS Package data flow.

While regarding the Reports as platform should be used Microsoft SQL Reporting Service. All reports should be designed and developed using this platform included in MSSQL Server 2019/22 Standard Licenses. This is due to the Kosovo Police working stack since all reports are developed and published using SSRS Platform technology. So the same working stack should be followed.

## 6.3 Mobile Application

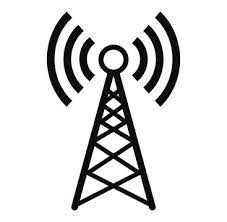
In addition to the web application, the BIS system needs to be accessible via a mobile application to accommodate Chameleon 8 Devices. Therefore, it's suggested either to develop a new mobile application or to integrate it with the existing BMS (Green Border Application). The Kosovo Police emphasize the importance of integrating with the current BMS system on mobile devices (such as tablets) to eliminate the need for multiple devices and applications that have same functionalities. The existing BMS Green Border application is developed in .NET, and it operates as a desktop application. The Kosovo Police is committed to provide the source code for both the BMS Web Application and the Mobile Desktop Application to facilitate these integrations.

The mobile application should be a streamlined version tailored for field operations, focusing on essential functions like biometric enrollment and checks against the Kosovo Police Systems (BMS and KPIS) and biometric systems such as BIS (for existing fingerprints) and AFIS.

For communication, mobile devices should be capable of using SIM cards provided by the Kosovo Police, which will be configured by the Telecommunication Vendor to enable a VPN connection to the APIs designed specifically for mobile equipment. In Figure 5 is shown the mobile registration and check process to Mobile BIS system.

**Figure 5**. BIS Mobile application and communication with BIS Central Database





AFIS

3G/4G

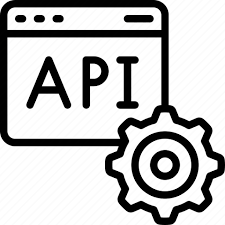
VPN icon PNG transparent image download, size: 810x980pxVPN icon PNG transparent image download, size: 810x980px

insert

BIS

SIM Card

3G/4G



check



Database

Police



BMS Stop Watch

KPIS Warrants

Communication will be via SIM using 3G/4G network of one of the GSM telecommunication operators that Kosovo Police has contract. Communication will be via VPN that would allow communication of end devices (Chameleon 8 plus) with the Mobile API and through mobile API will insert data into BIS Database.

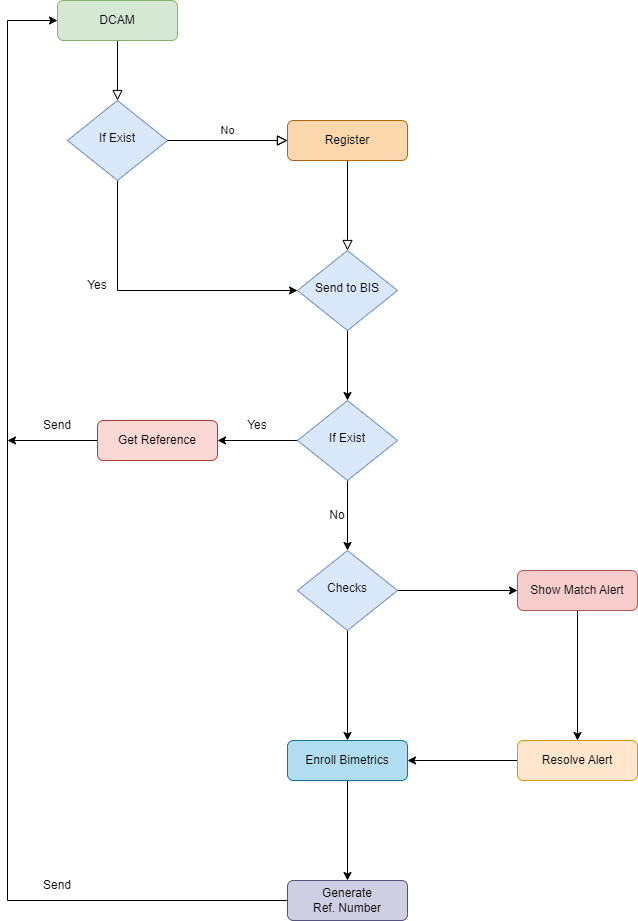
The enrolment collections of Mobile Tablet will be stored and can be found at Enrolment Module.

# Business Process

In following sections are explained the business processes for all modules of BIS system planned to be implemented.

The Business process starts from the DCAM as data source from where the case is initiated and sent to BIS for performing biometric enrolment aimed to be send back to DCAM as reference number by completing the case and providing the access to the enrolled biometric data. In following flowchart, we have shown the process:

Figure 6. Flowchart of Business Process



### Incoming Collections

Incoming collection as process is considered crucial for receiving collections initiated and registered in DCAM system at MIA. Through this process, the BIS system will be able to receive the collection of data and to continue further with the enrolling of biometric data and performing of find/match checks.

The term collection represents the collective data collected for individual for different purposes such:

* Asylum Seekers
* Reception Centres
* Detention Centres
* Returns etc.

There can be other collective data purposes that might be integrated in DCAM system, but the BIS system should be able to accept whatever collection come from DCAM.

The elaboration of content of collection purposes is not target of this documentation, so let’s suppose that whatever textual data come from DCAM, it should have a purpose mentioned in above text.

The communication between BIS as Receiver and DCAM as sender should be designed to work based on message queue. In following example, we will show the message queue illustration and how it would be in our scenario.

**Figure 7**. Incoming Queues from DCAM

**Queues Pool**

Receive

Send

Collection 1

Consumer

(BIS)

Collection 2

Producer

(DCAM)

Collection 3

Collection 4

This is the most crucial and the core component of the BIS database that needs to be developed. In following table are shown the functional requirements of the business process for asylum seekers.

Table 6. Functional Requirements for Incoming Collections

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.1.0 | It should be able to list all collections sent by DCAM as row in list table. It can be few not only one at the same time. |
| 7.1.1.1 | It should be able to register collection to BIS database and to provide a referential number in BIS that must be unique for each collection received/registered. |
| 7.1.1.2 | It should be able to perform all needed checks in internal and external databases of Kosovo Police explained in Session of Matching and Finding. |
| 7.1.1.3 | It should be able to should be able to provide the status of collection such:  -Waiting  -In process  -Completed |
| 7.1.1.4 | It should be able to show with colours the statuses above, waiting (green), in process (yellow) and completed (red). |
| 7.1.1.5 | It should be able to show in top new collections received and if the collection has not been opened yet, it should be blinked to understand that nobody is working on. |
| 7.1.1.6 | It should be able to list, show all collections received at least for last 24hrs including their statuses. |
| 7.1.1.7 | It should be able to print / export the collections as list in PDF/Word or Excel sheets. |

### Outgoing Collections

In addition of incoming collection, the outgoing collection is another feature aimed to send to DCAM API the referential number of the collected enrolments such: fingerprints, images, and other details at BIS database. This referential number should be associated to the Incoming collection and should be unique for each one received form DCAM.

In Figure 8is shown the illustration of sending collection’s reference to the DCAM

**Figure 8**. Outgoing References to DCAM

**Queues Pool**

Send

Receive

Reference 1

Consumer

(DCAM)

Sender

(BIS)

Reference 2

Reference 3

Reference 4

The reference number will be sent to DCAM API that will allow the accessibility to the biometric enrolment for collection sent. In addition, only biometric enrolments will be accessible, while the other textual and metadata about the checks / alerts can be send as information and can be registered to DCAM database through Rest API build at DCAM infrastructure.

Table 7. Functional Requirements for outgoing Collections

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.2.0 | It should be able to send the reference number for providing accessibility to the biometric enrolments (fingerprints, images), while the match results will be sent as text or metadata aimed to be stored in DCAM as evidence\* |
| 7.1.2.1 | It should be able to export the collective data in PDF, Word or any other format |
| 7.1.2.2 | It should be able to show the list of collections based on different intervals of time |
| 7.1.2.3 | It should be able to show the matches results for each check performed. In case of match found, the red colour should prevail, while in case of no match found, collection including reference should be marked with green. |
| 7.1.2.4 | It should be able to should be able to provide the status of collection:  -Sent  -Received |
| 7.1.2.5 | It should be able to show collections as list, while for showing more details for specific one, it should be able to open collection individually. |

*\*This feature will need to be discussed with Kosovo Police to be in line with existing laws, procedures and MoU’s in order to be sure if showing of match results should be exposed or NOT to DCAM.*

**Figure 9**. Communication APIs between DCAM and BIS

BMS

KPIS

AFIS



check

check

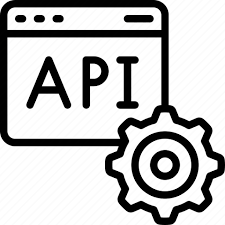
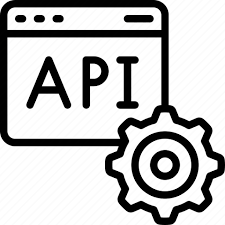
REST

REST

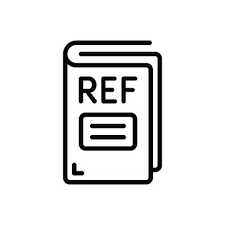
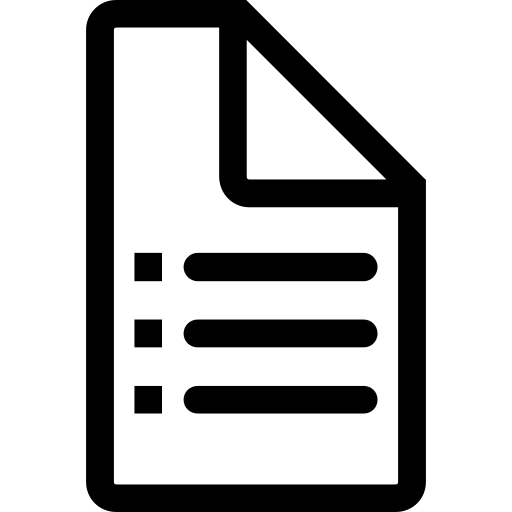
Send

BIS

Send



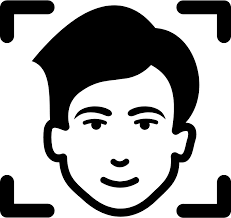
DCAM

VPN icon PNG transparent image download, size: 810x980px

Database

Receive

Receive



Collection

Reference

Database

Generates

Send

Biometric Data Access

Figure 9 illustrates how will be communication between representative APIs of both systems. So, as is shown there is no need for different API for sending and different for receiving, but duplex API based on REST will be used for both operations sending and receiving.

DCAM should be able to send the collection that might be for different purpose, collection is set of textual data about the individuals registered in DCAM. BIS API’s will receive collection and will register in BIS and will proceed with biometric data enrolment.

After competition, BIS will send back the Reference number generated and through this reference number DCAM should be able to show the biometric data.

### Enrolments UI

This module should be designed for performing and storing enrolments that might not come from DCAM but exclusively from Mobile Tablets or DactyScan Scanners.

All the enrolments collected from mobile tablets and DactyScan Scanners should be stored in BIS and should be visible at Enrolments module UI.

Module should be available only for those who have access to work with this module based on access permission hierarchy explained in Session 12.

In Table 8 we have shown some basic requirements that should take place for this module;

Table 8. Functional Requirements for Enrolment module

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.3.0 | It should be able to show all enrolments performed by mobile tablets |
| 7.1.3.1 | It should be able to export the collective data in PDF, Word or any other format |
| 7.1.3.2 | It should be able to show the list of enrolments based on different intervals of time |
| 7.1.3.3 | It should be able to show the matches results for each check performed. In case of match found, the red colour should prevail, while in case of no match found, collection including reference should be marked with green. |
| 7.1.3.4 | It should be able to should be able to register new enrolment even though it didn’t come from DCAM, but Kosovo Police Officer decides to register and to perform needed checks for any purpose. \* |
| 7.1.3.5 | It should be able to provide all needed details for a person including personal data and the purpose of performing fingerprints and other relevant data. |
| 7.1.3.6 | It should be able to show enrolments as list, while for showing more details for specific one, it should be able to open collection individually. |

\*Registration of new enrolments (fingerprints) directly should be done in accordance of existing laws and procedures. BIS as system should provide this feature.

### Reports and Statistics

System should be able to generate multiple reports and statistics as is defined on functional requirements of each module. Regarding the technology, as is mentioned in Section 6.2 all reports / statistics should be published in SSRS (SQL Server Reporting Service) and should be called by UI front end for showing repots.

In this regard, reports and statistics should be separate as independent component that will serve for all modules. This pattern is also used by other KP software that uses SSRS as platform technology

**Figure 10.** Databases and SSRS Interaction for generating Reports & Statics

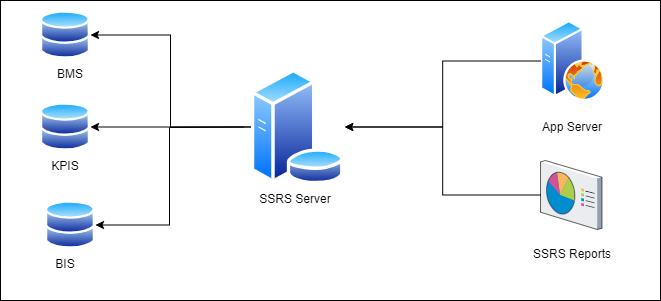


Figure 10 illustrates the potential data sources that SSRS will utilize for the preparation, analysis, and generation of the reports/statistics outlined in Table 11. These reports and statistics will be derived from various search parameters provided. The parameters may vary and can be expanded as required. Below, we list some of the most frequently used parameters, though this list is not exhaustive. The contractual operator will select search parameters that align with the needs of KP. In the subsequent text, we will highlight the most significant and beneficial parameters, including:

**Personal Data Search Parameters:**

Name, Surname, Personal Number, Date of Birth, Country of Birth, Sex, Document Type, Document Number, Father’s Name, Occupation etc.

**Other Search Parameters:**

Report Number (Identification Number Registered), Registered Date/Time, Decision, Decision Purpose, Reason, Report Type etc.

Same parameters should be available for statistical data reports.

Table 9. Functional Requirements for Reports and Statistics

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.4.0 | It should be able to generate reports based on entry parameters provided. |
| 7.1.4.1 | It should be able to generate statistical reports based on entry parameters provided. |
| 7.1.4.2 | It should be able to search, list and print decisions based on the purpose |
| 7.1.4.3 | It should be able to export reports in one of the recognized formats such: PDF or MS Word. |
| 7.1.4.4 | It should be able to export statistical reports in PDF and Excel |
| 7.1.4.5 | It should be able to generate statistical reports using Microsoft Pivot Table. This would allow users to use their own excel sheet connected with BIS Datawarehouse to generate statistical reports. |
| 7.1.4.6 | It should be able to generate analytics reports based on needs. |

**\*NOTE:** Due to the earlier process and not clear picture about the reports/statistics, the Economic Operator (EO) should be able to develop and publish up to 10 other reports and statistics based on needs apart from the existing reports showed in the Table 9. Definition of report/statistic details will be within the contract.

### Auditing

This module is a crucial part of the BIS System, designed to facilitate the investigation and auditing of user actions within the BIS system. Authentication is fully managed through Active Directory, allowing for all audit activities to be monitored and recorded using KP's official accounts in Active Directory.

It is recommended that the audit records be stored in a separate database within the same server instance, eliminating the need for an additional server. Instead, an additional database dedicated to audit activities should be created on the same server. A commonly used name for this audit database is BIS\_Audit.

This database will archive all user-related activities within the system. The subsequent sections will detail the functional requirements for managing audit data.

Table 10. Functional Requirements for Audit Data

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 7.1.5.0 | Audit data should be stored in separate database within the same instance. This is due to performance issues. |
| 7.1.5.1 | Audit data should be accessible by specific permission only to those who have access on it. |
| 7.1.5.2 | Audit data should show the activities and actions performed by specific user in specific date & time. |
| 7.1.8.3 | Audit data retention policy should be implemented and should be allowed to be changed based on needs. Initially, audit data retention policy should be for 1 Year or based on the current log retention policy implemented in KP for other systems. |
| 7.1.8.4 | Audit data should show the activities for specific action performed. |
| 7.1.8.5 | Audit data should be exported in Excel and Pdf to be used as evidence in case of need. |
| 7.1.8.6 | It should be prevented from delete or in case of delete should track who did delete. |

# Personal and Biometric Data

Since the registration process is present in all BIS components, in this section is elaborated in detail how it works.

Registration process covers two different stages:

* Personal Data Registration
* Biometric Data Registration

## 8.1 Personal Data

Personal data, also commonly referred to as personally identifiable information (PII) or personal information, encompasses any information that can be used to identify or directly relate to an individual. The definition of personal data may vary by jurisdiction, but it generally includes the following types of information:

**Name**: Full name, first name, last name, and any nicknames or aliases.

**Contact Information**: This includes postal addresses, email addresses, phone numbers, and fax numbers.

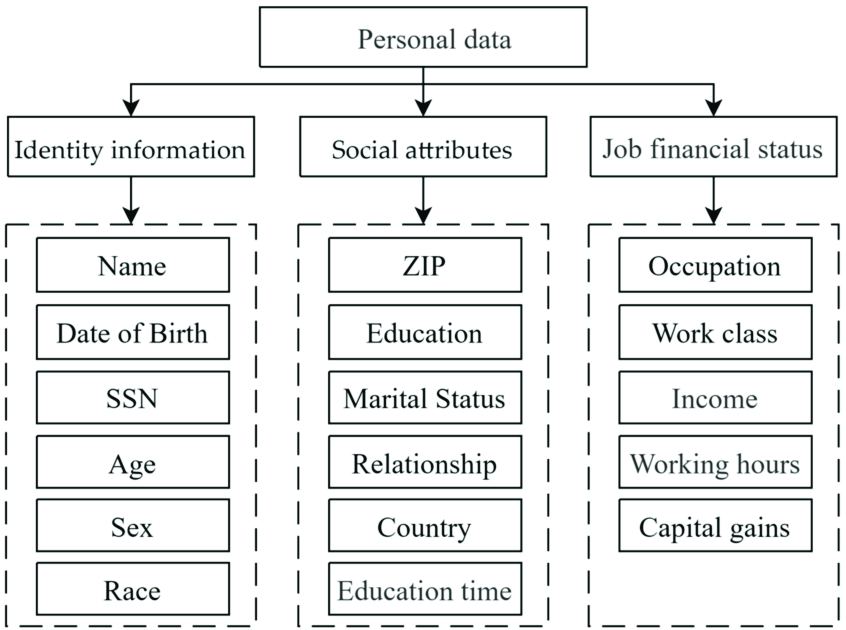
**Identification Numbers**: National identification numbers (e.g., national ID card numbers), passport numbers, driver's license numbers, and taxpayer identification numbers (TIN).

**Date of Birth**: Information about an individual's birthdate is considered personal data.

**Country of Birth**: Information where an individual has born.

**Citizenship**: is a legal status and membership in a particular country or nation that grants an individual certain rights, privileges, and responsibilities within that country

**Figure 11**. Personal Data Types



At BIS modules, personal data will include only some of the personal data types shown in Figure 11, because some of them are irrelevant.

## 8.2 Biometric Data

Biometric data refers to unique physical or behavioural characteristics of individuals that can be used for automated recognition or verification of identity. This type of data is often used in security and identification systems. Common types of biometric data include:

**Fingerprint Recognition**: The patterns of ridges and valleys on an individual's fingertips are unique and can be used for identification.

**Facial Recognition**: This involves analysing facial features, such as the shape of the face, distance between eyes, and the contour of the jawline, to identify a person.

There are some other attributes but not related to the business process discussed. While regarding the Biometric Enrolment as terminology is the process of collecting and storing an individual's biometric data for the purpose of identification and verification. This process is a key part of implementing a biometric system, such as those used for security, identification, or access control. The enrolment process typically involves the following steps:

**Data Collection**: The individual's biometric features are captured using specialized sensors or devices. For example, a fingerprint scanner captures the fingerprint, a camera captures facial features, or a microphone records voice pattern.

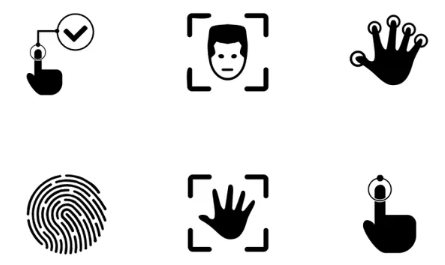
**Data Processing**: The collected raw data is processed to extract unique biometric features. This often involves converting the data into a digital format that can be more easily analysed and compared.

**Template Creation**: The system creates a biometric template based on the processed data. This template is a digital representation of the individual's unique biometric characteristics. It is designed to be easily comparable with new biometric samples taken for verification or identification.

**Storage**: The biometric template is securely stored in a database. The storage method must ensure data security and privacy, as biometric data is sensitive personal information.

**Registration**: The individual's biometric template is linked to their identity in the system. This link is what allows the system to identify or verify the individual when their biometric data is presented in the future.

**Figure 12**. Biometric Data Illustration



## Registration process

The registration process of Biometric Enrolment should be based on file formats standards recognized globally. This is very important because the BIS system will serve as the main registry database for fingerprints and should have the capacity to exchange the biometric data with other local and International Organizations such: Interpol, Europol, Siena etc.

### NIST Application

Here is high level of the component diagram which describe the system components how to manage NIST biometric data management.

**Figure 13**. NIST Application Architecture

Gateway

Orchestration

Database

### Gateway

Gateway acts as a crucial intermediary layer, providing a standardized and secure means for external systems to communicate with the BIS. It employs industry standards such as RESTful Web Services and possibly NIST protocols to ensure interoperability and compliance. The inclusion of business logic indicates that the Gateway is not just a conduit but also plays a role in processing and managing the data exchanged.

**Interface Exposition:**

The interfaces are exposed to external systems, typically using a Service-Oriented Architecture (SOA) approach.

RESTful Web Services are mentioned, suggesting that the communication follows the principles of Representational State Transfer (REST), a popular architectural style for designing networked applications.

**Protocol Support:**

The Gateway supports several protocols for message interchange. The mention of NIST (National Institute of Standards and Technology) indicates adherence to standards, possibly related to biometric data or security.

**Communication with Biometric Application:**

The primary purpose of this Gateway is to facilitate communication between the BIS and other systems. It serves as a bridge, allowing data and requests to flow seamlessly between the BIS and external entities.

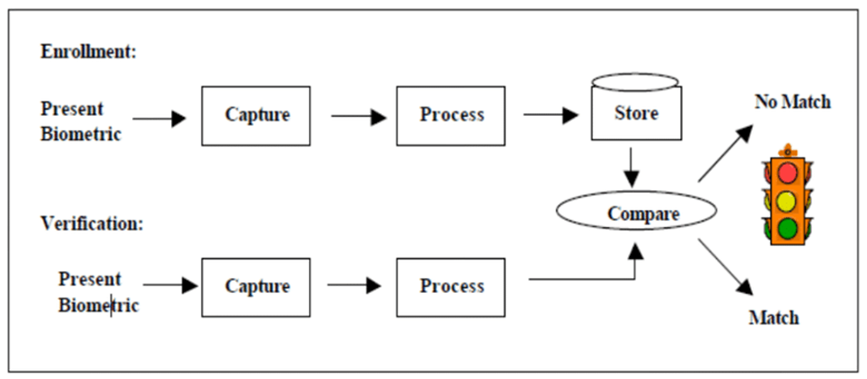
### Orchestration

Orchestration subsystem is a critical component that oversees the business logic and transactional workflows within a system. It excels in managing services that maintain state information, ensuring that the system's processes are executed in a coordinated and correct manner. This orchestration is crucial for maintaining the integrity and consistency of the overall system.

### Store

Described system employs a strategic approach to data storage by placing alphanumeric, audit, and certain biometric data in an RDBMS and storing biometric image data in NIST file containers within a file system. The use of BIS and two-phase commit transactions ensures synchronization between these two main data storage locations. Additionally, the co-location of matcher templates with the matchers suggests an optimized setup for biometric matching operations. This architecture likely balances the need for structured data management and efficient storage of biometric information.

**Figure 14**. Fingerprint Data match and compare process.



# Integrations

Integration in the context of technology and systems refers to the process of combining different software applications, hardware components, or systems to function as a coordinated whole. The main goal of integration at BIS is to create a unified system where each component works seamlessly with others, resulting in improved efficiency, functionality, and user experience. Integration can occur at various levels and in different forms, including:

**System Integration**: Combining different software applications like to work together within and same environment in this case Kosovo Police IT Infrastructure.

**Software Integration**: Merging different software programs, often from different vendors, to operate as a coordinated unit. In this case, integration of BIS with BMS, KPIS, DCAM, KVIS, DPD, etc.

**Data Integration**: Consolidating data from different sources into a single, cohesive dataset. Collection of data from other sources in Datawarehouse (KPIS, BMS, DCAM).

**Hardware Integration**: Connecting different hardware components to work together effectively. Integration of different equipment with BIS software such Dacty Scan Scanners and Chameleon Fingerprint Tablets.

### Integration

The BIS system will be fully integrated and according to the suggestion argued in the project scope, it will serve as integral part of current BMS system integrated in following modules:

* User Interface (website)
* Mobile Application (green border)

The UI interface is elaborated in the above sections that despite the fact that will be integrated will be fully independent in terms of functionality.

In addition, the Mobile Application will be another functionality that should be integrated in BMS Green Border Mobile Application aimed to use the same application for different purposes that is considered as goal in IT strategy plan of Kosovo Police.

### Interconnectivity

The BIS system is considered complex in terms of interconnectivity with other systems internally and externally. In this regard it should be able to send and receive data with following systems:

**Kosovo Police**

BMS (Stop watchlist, entry/exit days 90/180 days calculation)

KPIS (Warrants, Police Quests, Incidents and Citations)

ILECU (Biometric Data verification and exchange with other countries and vice versa)

**Ministry of Internal Affairs:**

DCAM (retrieving collections and sending biometric data access references)

DPD (checking and comparing fingerprints with document produce department)

AFIS (checking and comparing with the existing fingerprints collected from criminal locations)

**Ministry of Foreign Affairs**

KVIS (check and compare fingerprints with the fingerprints issued by KVIS form Kosovo’s embassies around the world or consolations).

**Ministry of Labour and Social Welfare**

Department of Labor and Employment

In Figure 15 is shown an illustration how BIS system will be integrated with other internal and external systems.

**Figure 15.** Interconnection Schema



**Table 11**. APIs types and purposes

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **API Description** | **API Type** | **Qty** |
| 1 | BMS Stop list Check | Rest | 1 |
| 2 | KPIS Warrant Check | Rest | 1 |
| 3 | DCAM Data Send/Receive | Rest | 1 |
| 4 | AFIS Fingerprint Check | Rest | 1 |
| 5 | ILECU Fingerprint Check | Rest | 1 |
| 6 | ILECU Personal Data Check | Rest | 1 |
| 7 | KVIS Persons Check | Rest | 1 |
| 8 | KVIS Fingerprint Check | Rest | 1 |
| 9 | Check Overstaying 90/180 | Rest | 1 |
| 10 | DPD Fingerprint Check | Rest | 1 |
| 11 | Mobile App API | Rest | 1 |
|  |  |  |  |
|  |  | **TOTAL APIs** | **11** |

In Table 12 are shown the total number of APIs that needs to be developed in order to cover interconnectivity functions and to ensure interoperability with other software’s internally and externally.

### APIs Description

API types will be full rest due to the bidirectional way of communication sending/receiving or GET/Post actions. In addition, in follow is provided more details about the APIs:

**BMS Stop list Check** -> This API will get the information from BMS if person registered in BIS have similarity with any person stored in StopWatch List. Regarding parameters, it will use the following parameters:

Post: Name, Surname, Date of Birth, Document Number or any other

Get: Match Status, Percentage of Match, Sex, Comments/Remarks or any other

**KPIS Warrant Check** -> This API will get the information from KPIS if person have any warrant issued or police quest or any other status. Regarding parameters, it will use the following parameters:

Post: Name, Surname, Date of Birth, Sex, Father’s Name, Document Number or any other

Get: Match Status, Percentage of Match, Comments/Remarks or any other

**DCAM Data Send/Receive** -> Through this API will be able to send/receive data from DCAM. Regarding parameters, it will use the following parameters:

Post: Personal Information, Purpose of Registration or any other relevant data specified by actors

Get: Reference Number, Access Number, Fingerprints, Fingerprint Date Captured, Venue etc.

**AFIS Fingerprint Check** - Through this API will be able to send/receive from AFIS Database. Regarding parameters, it will use the following parameters:

Post: Fingerprints

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**ILECU Fingerprint Check** - Through this API will be able to provide information for ILECU if the fingerprint received and stored in ILECU will match with any BIS fingerprint collected. Regarding parameters, it will use the following parameters:

Post: Fingerprints

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**ILECU Personal Data Check** – Similar as with fingerprints, with ILECU is important to exchange also the personal data provided. So, through this API will be able to check if any personal data is located in ILECU database involved in any case or if he/she has been involved in any case earlier.

Post: Personal Data

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**KVIS Persons Check** – This API will serve to check if the collected data have any match with any person that Kosovo’s Embassy in any country have enrolled fingerprints for issuing Visa Entrance. Regarding parameters, it will use the following parameters:

Post: Personal Data

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**KVIS Biometric Check –** Through this API will be able to provide information for Kosovo Visa System KVIS if the fingerprint received and stored in BIS will match with any KVIS fingerprint collected. Regarding parameters, it will use the following parameters:

Post: Fingerprints

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**Check 90/180 Days** – Through this API should be able to provide an API available for Ministry of Labor and Welfare, Department of Employment in order to check the foreigner persons who overstayed more than 90 days / 180

Post: Name, Surname, Date of Birth, Sex, Father’s Name, Document Number or any other

Get: Match Status, Percentage of Match, Comments/Remarks or any other attribute

**DPD Fingerprint Check** – Through this API should be able to check if the fingerprint collected will match with any database record.

Post: Fingerprints

Get: Mach Status, Comments or any other relevant data that both parties agreed.

**Mobile API** – Through this API should be able to send data to BIS

Post: Fingerprint, Name, Surname, Date of Birth, Sex or any other relevant data registered

Get: Status

Table 12. Functional Requirements for Integration

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 8.1.2.0 | It should be able to check in BMS Database – Stoplist using the API for BMS |
| 8.1.2.1 | It should be able to check in KPIS Database Warrants using the API for KPIS |
| 8.1.2.2 | It should be able to send reference number and check results through API to DCAM |
| 8.1.2.3 | It should be able to receive from DCAM the collections |
| 8.1.2.4 | It should be able to check in KVIS Database using APIs for DPD |
| 8.1.2.5 | It should be able to provide biometric info to ILECU module via API |
| 8.1.2.6 | It should be able to check in AFIS database and to receive the status via API |
| 8.1.2.7 | It should be able to provide an API available for Ministry of Labor and Welfare, Department of Employment in order to check the foreigner persons who overstayed more than 90 days / 180. This would avoid the existing communication for sending confirmation via email for each person checked. |
| 8.1.2.8 | It should be able to use Dacty Scan Scanners and Chameleon Tablet device for fingerprint check and enrolment. |
| 8.1.2.9 | It should be able to use API developed for sending/receiving data from mobile device to BIS database and performing checks to BMS, KPIS and AFIS. |

### Integration of other Biometrics (SEEK)

The BIS system should have the flexibility to integrate biometric data from various systems. Currently, Kosovo Police officers at border points, as well as at regional and central levels, utilize devices that capture biometric data and relay this information for enrolment into other systems. Each time a fingerprint is collected, it is checked against their system. Given the intricate nature of the framework and the challenges associated with integrating device SDKs, a versatile approach to importing fingerprint data, particularly in NST file format, is recommended.

Implementing this solution would enhance efficiency and productivity by offering a streamlined operational model that eliminates the need for direct device integration. Therefore, it is essential to establish an automated scheduled task that executes the following procedures:

1. Collecting data from the SEEK equipment (no need for additional development/integration)
2. Send Data to other system (no need for additional development / integration)
3. Deploying an SFTP Server using authentication Username/Password (this server will be ensured/configured by Kosovo Police IT Department)
4. Putting SEEK IP Addresses in Kosovo Police Firewall Whitelist to ensure that only those IP/Ips will have access to SFTP (will be configured by Kosovo Police IT)
5. Development an Automation Tool that will check time by time for e.g every 10 minutes or automatically on trigger when any new data is exported to SFTP Server located at Kosovo Police Datacentre
6. Insert Data to BIS Database (data will be exported in NST format according to agreement of Kosovo Police).
7. Making those data visible as other data collected by BIS devices but should be tagged with a label for e.g SEEK in order to know that those data have been collected by SEEK System.

### Checking and Matching

The core component of the BIS integration will be the find and match process or checking process. In this regard, there are several databases that BIS system should be able to check for each person that will be registered. In following schema is explained how the checking process will work.

**Figure 16.** Find and Match Process

Table 13. Functional Requirements Find and Match

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 9.1.4.0 | It should be able to check in BMS Database during the registration process if person has active status in Stop list in BMS. If yes it should show a Popup. If NO it should continue registering normally. |
| 9.1.4.1 | It should be able to check in KPIS Database during the registration process if person has active warrant or police quest in KPIS database. If yes it should show the Popup. If NO it should continue registering normally. |
| 9.1.4.2 | It should be able to store match result to BIS |
| 9.1.4.3 | It should be able to check in KVIS Database during the registration of process if person has any biometric fingerprint collected from Kosovo’s Embassies. |
| 9.1.2.4 | It should be able to provide information for ILECU office. It should allow ILECU application to check through API if fingerprint exist in KPIS database or vice versa. |
| 9.1.2.5 | It should be able to check in AFIS database if person has criminal record recorded from AFIS. |
| 9.1.2.6 | It should be able to use Dacty Scan Scanners and Chameleon Tablet device for fingerprint check and enrolment. |

### Alerting and Notification

The BIS system should be able to display different alerts and dispatch notifications to the appropriate police officers and their official email addresses. Consequently, after every verification carried out, the system should be capable of presenting popup hints for individuals that have been identified as matches. Figure 17 illustrates the types of alerts, differentiated by colour, where the colour signifies the alert's level of urgency.

**Figure 17.** Alert Colours Meaning

Match of Personal Data or Fingerprint > 90%

Match of Personal Data or Fingerprint < 90%

Pass

Critical

Waring

Match of Personal Data or Fingerprint < 80%



Table 14. Functional Requirements Alerting and Notification

|  |  |
| --- | --- |
| **No.** | **Requirement Description** |
| 9.1.5.0 | It should be able to show popups / hints if there is a match of personal data of person during registration with the KPIS records (warrants) or BMS records (stop watch list). |
| 9.1.5.1 | It should be able to show popups / hints if there is a matching of fingerprint data in current fingerprint records and AFIS |
| 9.1.5.2 | It should be able to send email notification in case of any match with the any persons that are target of monitoring. In this scenario, matching should be invisible and only persons who receive email should be able to respond. |
| 9.1.5.3 | It should be able to check in KVIS Database during the registration of process if person has any biometric fingerprint collected from Kosovo’s Embassies. |
| 9.1.5.4 | It should be able to provide information for ILECU office. It should allow ILECU application to check through API if fingerprint exist in KPIS database or vice versa. |
| 9.1.5.5 | It should be able to check in AFIS database if person has criminal record recorded from AFIS. |
| 9.1.5.6 | It should be able to use Dacty Scan Scanners and Chameleon Tablet device for fingerprint check and enrolment. |

# Backups and Recovery

The BIS should be designed to operate with high availability and possess the capability to recover from potential failures, whether they arise from hardware malfunctions or human errors. To this end, it is essential that the entire BIS system infrastructure performs regular backups according to a predetermined schedule. Table 18 outlines the frequency and types of backups required to ensure high availability and recovery in case of any failures.

**Table 18**. Backup Types and Components

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Component** | **Backup Type** | **Frequently** |
| **Databases** | | | |
| 1 | Database Backup | Full Backup | Every night at 02:00 AM |
| 2 | Database Backup | Differential | Every 1 hour |
| 3 | Database Log | Log Backup | Every 15 min |
| **Reports in SSRS** | | | |
| 1 | ReportDB Database | Full Backup | Every Sunday at 01:00 AM |
| 2 | SSRS Backup | Full Backup | Every Sunday 02:00 AM |
| **Application Backup** | | | |
| 1 | Web Application Files in IIS | Backup | Every Saturday 08:00 AM |
| 3 | Web Application Log | Backup | Every Saturday 08:00 AM |

# Security and Access Permissions

Security and Access permissions is considered very crucial. Let’s start with the access layers of security. According to the existing Kosovo Police Applications such BMS and KPIS, the security levels are defined as 3 levels: Central, Regional and Local level.

**Figure 19.** Access Levels Organization

Central Level

HQ Department of Border Police  
Division of Migration  
Border Police Central Office



Regional Level

Regional Border Police  
South, West, North, East



Local Level

Border Crossing Points  
Border Police Stations  
Green Border



**Central Level** should be considered the highest level on Police Hierarchy and users from this level can have following access permissions:

* Data Read/ Write / Edit to all data in BIS
* Reports & Statistics all levels
* Improve Data Quality or any issues related to human
* Audit Data if BIS is going to be used correctly

**Regional Level** should be second of Police Hierarchy and users from this level can have following access permissions:

* Data Read for all persons, biometrics and other data
* Data Write only at Regional Leve
* Reports & Statistics only for region where belong
* Improve Data Quality or any issues related to data registration

**Local Level** should be second of Police Hierarchy and users from this level can have following access permissions:

* Data Read for all persons, biometrics and other data
* Data Write only at local Level for eg. Border Crossing Point or Border Station
* Reports & Statistics only for border point or border station where belong
* Improve Data Quality or any issues related to data registration in local level

# Administrative Requirements

See Section Eligibility in the Request for Quotation.

# Cost

Table 19 is presented the cost evaluation estimate for each component of BIS as system and Table 20 represents the maintenance cost.

**Table 19**. Cost for Developments

|  |  |  |
| --- | --- | --- |
| **No.** | **Component** | **Cost (with NO VAT)** |
|  |
| 1 | Server and Services Setup and Configuration |  |  |
| 2 | Front-End UI Interface Development |  |  |
| 3 | Back-End (Database) & Processes Development |  |  |
| 4 | Mobile Application Development |  |  |
| 5 | Integrations |  |  |
| 6 | Backups and Recovery Implementation |  |  |
| 7 | Security and Access Permission Implementation |  |  |
| 8 | Upgrading 56 Licenses (Thales Web ID) |  |  |
| 9 | Testing, Delivery and Training |  |  |
|  | **TOTAL** |  |  |

**Important Notes:**

The above pricing should encompass one year (12 months) of maintenance during the warranty period, which will begin only after the system passes all functional and non-functional tests and receives formal acceptance by the Kosovo Police. Upgrades of licenses (Web ID) are not included in this maintenance as they are managed by Thales, the provider, and delivery and testing are excluded as well since they fall outside of development.

\*Current Web ID Licenses provided by Thales to Kosovo Police that are on use are available only for Find & Match operations with AFIS but NOT for enrolment. There is necessary those licenses to be upgraded to ensure full digitalization of fingerprint enrolment or storing fingerprints in Database as the main request of Kosovo Police.

# Implementation Plan

Implementation of contract should be completed within 24 months from the moment of signing the contract. The implementation of all developments needed including testing, delivery and training phases should be completed within 12 months and other 12 months for maintenance and support. Table 20 shows the contract implementation plan in details.

**Table 20.** Implementation plan based on phases and implementation time

|  |  |  |
| --- | --- | --- |
| **PHASES** | **DETAILS** | **MONTHS** |
|  |
| **Analysis Phase** | Kosovo Police: BMS, KPIS, ILECU | 1 |  |
| Ministry of Internal Affairs: DCAM, AFIS, DPD |  |
| Ministry of Foreign Affairs: KVIS |  |
| **Server Infrastructure** | Database Servers: Transactional Database & Datawarehouse | 1 |  |
| Application Server: Hosting Application at IIS |  |
| Report Server (SSRS) |  |
| **Front – End Development** | Development of UI Design | 3 |  |
| Development of UI Functionalities |  |
| Development of forms and reports |  |
| **Back-End Development** | Development of Databases | 3 |  |
| Development and Design of SSRS Reports |  |
| Development of API and Services for Connectivity and Interoperability |  |
| **Integration** | Interconnectivity within KP Software systems (BMS, KPIS, ILECU) | 2 |  |
| Interconnectivity with other external systems (DCAM, DPD, AFIS, KVIS) |  |
| Connectivity with Hardware Devices (Dacty Scan & Chameleon Tablet) |  |
| **Testing and delivering** | System Testing: End-to-End Testing & Integration Testing | 1 |  |
| Performance Testing: Load Test and Stress Test |  |
| Technical Documentation Providing |  |
| Delivering of Source Code and Documentation |  |
| Training | Training of Trainers how to use BIS System | 1 |  |
| Training of Police Officers and others how to use BIS System |  |
| Training of IT Staf how to administer and maintain BIS System |  |
| **TOTAL:** | | **12** |  |