**System architecture of the biometric identification solution for SHABAS.**

**Main modules.**

The entire solution is splitted into a few modules (microservices). Each one of them is dedicated for one specific task. Such an approach enables to ease the application bug fixes, updates, management and deployment. Another advantage of the microservices architecture is a high scalability. Any particular part of the application functionality may be scaled up just by deploying of additional instances of the corresponding microservice, without a need to duplicate the entire system. The ability to run any number of the instances of a particular microservice greatly increases the application fault tolerance. Properly configured system will launch a new instance of the microservices in case of the failure of the running instance, thus preventing service interruption.

Each of the modules is mostly independent, as it's responsible for a particular functionality, which doesn't intersect the functionality of other modules. If a module requires some services provided by other modules, it communicates to other modules through the standard interface, like HTTP. The examples of the services that are consumed by other services are the security and configuration service.

These are the main modules (microservices) that constitute the application:

**1. Biometric module** is the core application module for the fingerprint authentication (1:1), identification (1:M), duplication checks, fingerprint images segmentation and biometric templates extraction. The

**2. User interface module** is a web application that provides a web pages for the enrollment stations and the desktop and mobile identification stations. UI for all the kinds of the end stations is done as a single page web application (SLA). That enables to unify the development of the user interfaces for various types of devices and provide a high level of the customization by the customer. The consumer of the application may change layout and styling of UI by editing HTML, CSS and image files.

**3. Configuration module** is a module that hosts all the application settings and provides them by demand to other modules. For example, each microservice on its start requests a port number to listen to. Other settings may be more specific for each particular module, depending on its functionality, like the default authentication threshold for the biometric module. Configuration module exposes web user interface for all the system settings. If a specific value has been changed by the administrator, a corresponding microservice gets notified about this change and loads the updated value. That's enables the settings updating without the module restart. The access to the configuration module is allowed for the administrative users only. The administrative users are defined in the organizational Active Directory domain. The permissions for particular action depend on the user's AD group membership.

**4. Security module** handles all the tasks related to the access of the users and end stations to other services of the application. Each request is validated on two levels – the station level and the user level. The station validation is based on mutual SSL authentication by means of the private keys and certificates assigned to each end station. If the station, where the current request is originated from, is registered in the system DB and has a valid status (enabled, unlocked), the user credentials get validated as well. Each user of the application has to authenticate when he opens the application on the end station.

There are two types of the users in the system - administrative users and operative users. The management of the administrative users is based on the Active Directory. Operative users are managed in the system DB. Operative users operate the end stations for the prisoners' enrollment, verification and identification. The authentication protocol used in the application is OAuth2. Security module masks the usage of two different user repositories (Active Directory and the internal DB) and enables to apply various authentication mechanisms without refactoring of the other system modules.

**5. Users and stations management module** is a web application for viewing and editing of the operational users and the stations used for the enrollment and identification of the prisoners. Editing includes adding, removal, status updating and the system rights management. Each operational user is assigned a set of rights and allowed authentication methods. Every action in the system has a set of permissions that define who is allowed to perform this action. For example, the prisoners' enrollment can be done only if a user who runs the enrollment application has been assigned the "prisoners' enrollment" right. The management module applies a similar set of action to the end stations and servers. Each stations has to be enrolled in the system before its first use. Status updates means temporarily disabling of the users or stations and any other statuses that will be found relevant. The management module is available through a browser and doesn't require a dedicated application. The access to the module is allowed only for the administrative users. The user interface provides the ability for the administrative user to search, sort and filter the existing operational users and stations base on various parameters, like IDs, dates, usage statistics and custom queries.

**6. Reports module** is a web application for viewing the statistics of the system functioning. It provides a user friendly presentation of the main activities that have occurred by the current moment. These are a few possible report examples:

* List of the prisoners' biometric authentication actions for the specified period for the specified set of stations including authentication results, an operational user, error message in case of failure.
* List of the identification actions for the particular prisoners with the ordered list of the candidates with their match scores.
* List of all the actions taken in the system by the particular operational user with the stations that have been operated by him for each action.
* Average match score for the entire system or for a particular prisoner or device with the deviation graph.

The reports module enables the user to set the parameters for the report generation, like dates, IDs, IP addresses and other parameters relevant for a particular report type. The report is presented as tables or graphs in the browser and can be exported as Excel or PDF files.

The report results can be used to adjust the system settings based on the statistics available. For example if an average authentication score for a particular prisoner is higher than the default system threshold, the threshold for this user can be increased which improves the system accuracy.

The access to the module is allowed only for the administrative users.

**7. Application Gateway module**

**8. Service discovery module**

**9. Load balancer module**

**DB security.**

**Logging.**

**Station enrollment process.**

**User enrollment process.**

**Prisoner registration process.**

**Management and configuration services access (BioLogin 2FA, multi person auth)**

**System Monitoring.**

**End station applications with API.**

**Containerization.**

**Continuous delivery/deployment**