FbF® bioServer and AppServer datasheet

FbF® bioServer

The FbF bioServer represents an abstraction of multiple biometric algorithms and server topologies into a single, unified, message-based biometric identification and verification platform. Using the same common messaging architecture that is used by the FbF bioClient, the bioServer is able to greatly simplify the process of submitting biometric identification requests and receiving results. The synchronous Windows Communication Foundation (WCF) interface is designed to provide a rapid response with a biometric result.

The bioServer is designed to support scalable deployments ranging from a single PC-class computer to hundreds of servers distributed across a wide area network. With a common strategy across such a large variance in operating capacity, the bioServer is able to more effectively serve as a universal model for processing biometric requests in both small scale and nation scale solutions. Further, this scalability will allow the bioServer to more effectively be deployed in remote and distributed processing scenarios where 1,000’s of local servers are required in the absence of reliable network connectivity *(e.g. developing nations and military applications)*.

The core of the bioServer architecture is the suite of biometric engines that are developed by Fujitsu. While the bioServer will support engines from other developers, the highly secure and scalable design of Fujitsu is ideally suited to the strategy of the bioServer. Each bioServer will include a minimum of one Fujitsu matching component for Palm Vien and any combination of Cluster Servers and Accelerators to meet the performance requirements of the installation. Further, the data model of the bioServer includes a unique taxonomy that allows for unlimited number of organizations to securely store their biometrics on common servers. This unlimited data segregation means that a single, hosted instance of the bioServer could easily handle thousands of organizations without fear of comprising their data integrity or impacting their individual transaction performance. This ability to host large-scale biometric server farms is particularly suited to FbF’s ability to operate in a true web environment and allow for instantly deployed software-as-a-service business models.

FbF bioServer is comprised of various components which are:

1. **FbFEngine:** Core component of bioServer that analyses, processes, and distributes the incoming requests. It’s also responsible for preparing and answering back to the client applications with an appropriate response.
2. **Database:** MS SQL based database that bioServer use to store biometric information and Unique Id relationships. This database is not used to store any other information.

3. **FbF Matching Server:** This component represents the biometric matching engines responsible for performing 1:1 and 1:N matching. This component can be installed on the same server as bioServer or can be deployed on a dedicated server or servers for large scale deployment.
4. **License Server:** Application to activate and validate server licenses. It can be deployed at any machine that remains accessible to bioServer.
5. **FbF WCF Web Service:** Web service suitable for Windows based client applications. FbF bioServer exposes its web service to receive biometric-transaction calls from various clients. This web service sits on the core component of FbF bioServer which is responsible for all the operations done on FbF bioServer.
6. **FbF Restful Web Service:** HTTP based service suitable for any web\desktop client applications.
7. **FbF SOAP Web Service (Standard Service):** Legacy web service based on XML and SOAP based communication. It is a web service running on HTTP protocol provided by FbF bioServer for quick integration of client applications with FbF bioServer. Best suitable for quick integration with legacy and mobile systems.

Figure 1, shows the different components of FbF bioServer and how they are tied and communicate with each other. Figure 1 also show how the client application can communicate with bioServer as per their requirement on different interfaces exposed to them.

Please note the recommended method used to host licenses for Server as well as clients application of bioServer. License server can also be created on a machine different than the machine where bioServer is deployed.

FbF® AppServer

The FbF AppServer can be thought of as an optional component for the FbF bioServer which provides auditing and security services. FbF AppServer provides a dashboard for FbF bioServer to monitor server health, maintain customer demographics, and provide report and audit logs.

The application integrator can customize what, if any, demographic information is stored on the AppServer.

Each AppServer will include a security layer between the FbF bioServer and the outside network traffic. This layer offers authentication, integrity check and protection against some common web-scenario attacks.

FbF AppServer defines a HMAC-based (Hash-Based Message Authentication Codes) web security protocol to secure communication between bioServer and the outside world.

AppServer is designed to meet Open Web Application Security Project (OWASP) best practices.

FbF AppServer is ideal for rapid and secure integration with FbF bioServer and any client application which requires demographic information, audit logging, and a supplemental security layer.

Figure 2, shows how AppServer can be used in between bioServer and outside network traffic. In the diagram, the word “Ecosystem” is generic term for all processes, servers, and databases managed by an integrator.

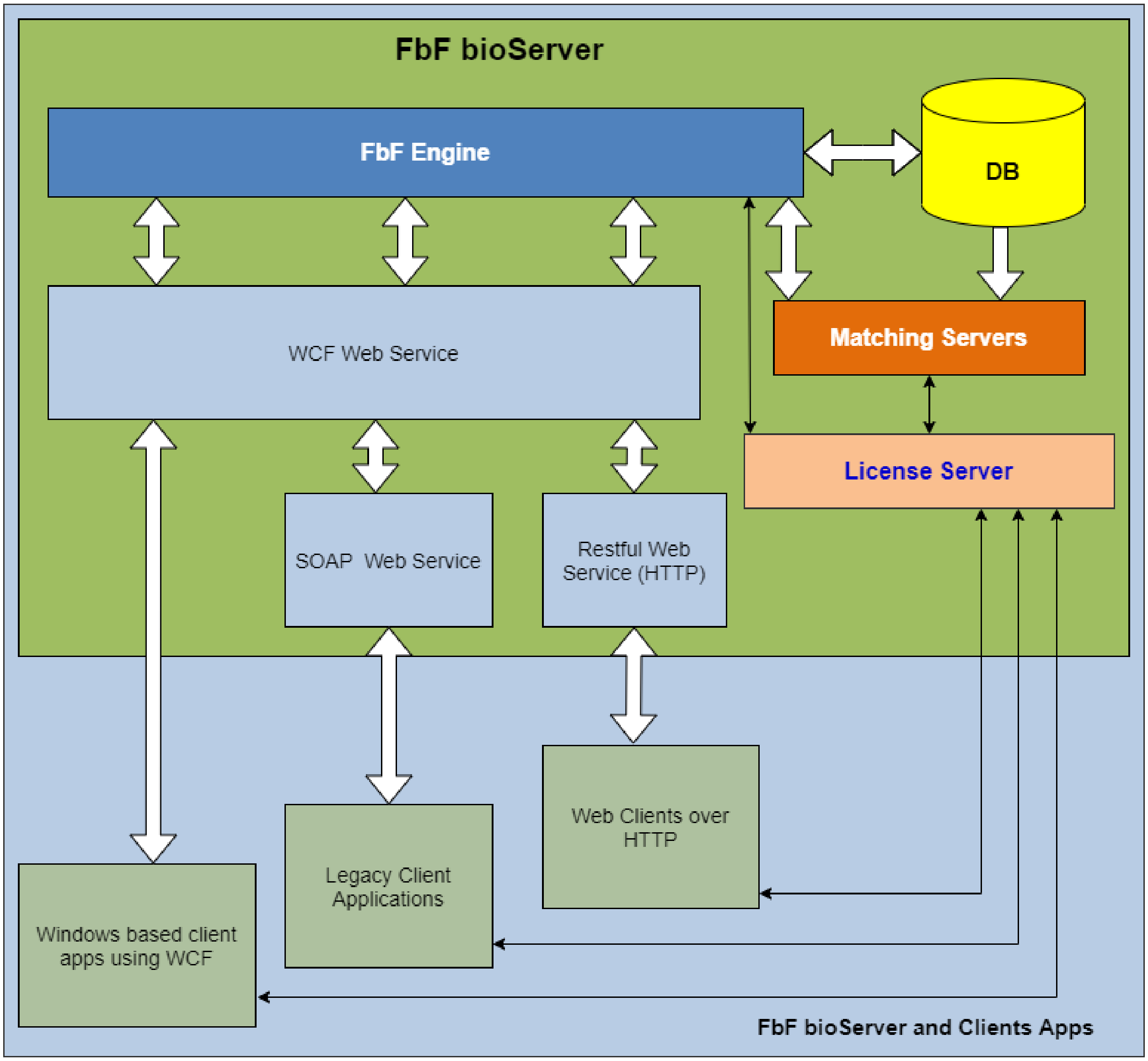
FbF bioServer
FbF Engine
DB
WCF Web Service
Matching Servers
License Server
SOAP Web Service
Restful Web Service (HTTP)
Web Clients over HTTP
Legacy Client Applications
Windows based client apps using WCF
FbF bioServer and Clients Apps

Figure 1

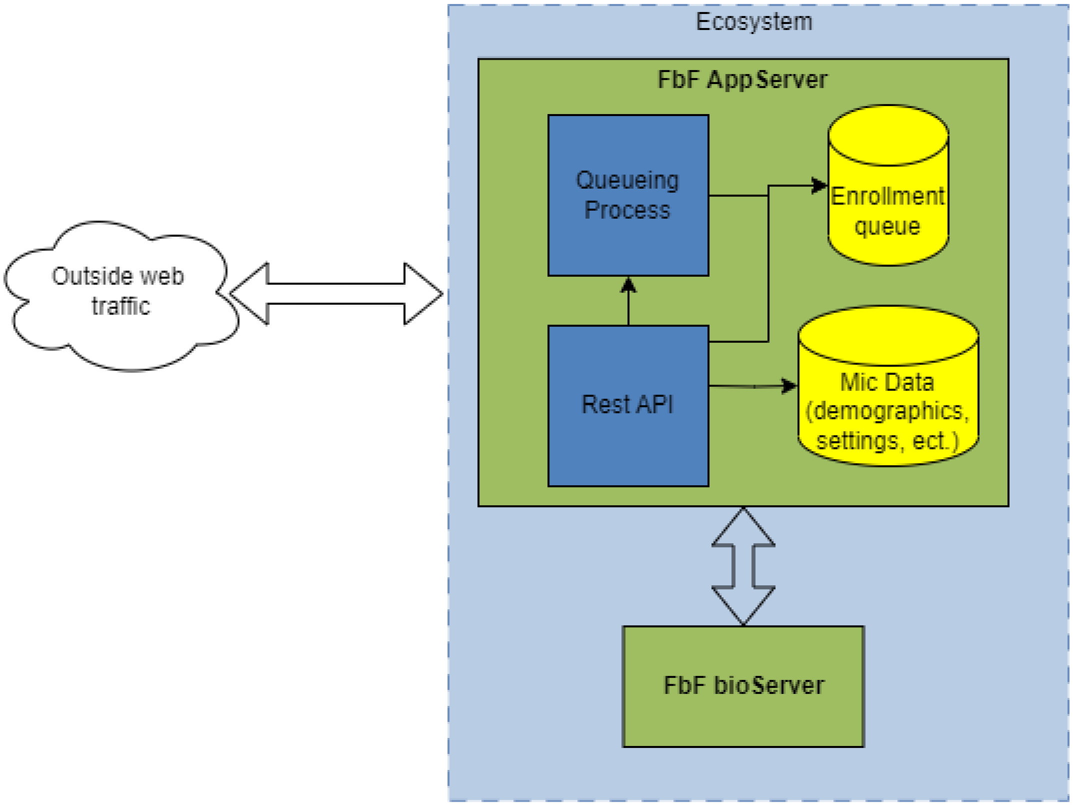
Ecosystem
FbF AppServer
Queueing Process
Enrollment queue
Outside web traffic
Rest API
Mic Data (demographics, settings, ect.)
FbF bioServer

Figure 2