Biometric Enterprise Architecture

Version 0.1

Prepared by:

Team Biometric Enterprise Architecture

(Team BM-EA)

In partial fulfillment
Of
Requirements for

SYS/OR 798 Fall 2009

Date: October 11, 2009

Revision History

Date	Purpose	Revision Level	Responsible Person
October 11, 2009	Initial Draft	0.1	Luckey

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

1 INTRODUCTION

1.1 BACKGROUND

Biometrics is the science of establishing the identity of a person based on his/or her physical, chemical, or behavioral characteristics. It is a rapidly growing field with many applications that includes various and sundry applications including a means to restrict access to a computer, the use of Automated Teller Machines (ATMs), and passage through airport security checkpoints. Today many commercial and government identity management systems deploy biometric technologies to support their operations. Some use biometrics as support service in their enterprise environment and while others offer biometric services to companies and organizations that require biometric capabilities and cannot bear the biometric enterprise investment. Finally and predominately, the preponderance of biometric applications supports both the legal and security domains allow those stakeholders the ability to assure success within the given domain.

The most common types of biometric applications include the capture, display, search and assessment of fingerprints, facial features, iris scans, and voice traits of individuals for comparison to reference population of scans. The challenge, across an enterprise is to ensure that all biometric applications can interact and be fused into mutually supporting identities across the entire domain and those identities are efficiently compared to ad-hoc, randomly collected data points consisting of a subset of the reference data.

1.2 PROBLEM STATEMENT AND PROJECT PURPOSE

Current biometric systems are generally inflexible and are not optimized for use within an enterprise. Most biometric systems are monolithic, thick-client or standalone applications with very little ability to interface to enterprise management information systems (MISs). While many biometric applications do offer some interoperability and integration points with and for established MISs such as PeopleSoft, SAS, Oracle and the like for personnel and accountability functions, the ability of such enterprise systems to collaborate across a diverse set of biometric systems is limited as a result of the lack of standardization and enterprise architecture support amongst the various biometric systems. Likewise there is a distinct lack of robust architectural support within the security and legal domains when using biometrics in those business contexts evidenced by the significant investment in stovepipe biometric systems.

Thus, the biometric market today is continuing a trend towards monopolistic stovepipe systems risking higher prices and less innovation. Small scale, open-source, initiatives however demonstrate the opportunity for improving biometric system collaboration and performance through higher quality and

modern architectural choices. The purpose of this project is to document and demonstrate the comparison and trade-off of current systems and within their current architecture to like systems supported by a more robust and modern architecture.

1.3 CUSTOMER

Our customer is Noblis, Inc., a nonprofit science, technology and strategy organization that helps clients solve complex systems, process and infrastructure problems in ways that benefit the public. We have partnered with them through Mr. Nat Hall, who works at Noblis and has colleagues interested in engaging our team for architectural analysis of biometric systems.

Some of the relevant areas of interest are to identify architecture for next-generation large-scale government biometric systems identifying effective performance, cost, and flexibility tradeoffs and develop a guidance document for system design, system procurement, and performance testing.

Goals for next-generation systems include:

- Improved system performance such as maximizing "match accuracies" with set throughput and response time requirements.
- Search against very large image/identity repository(ies) –in the millions
- Incentivize vendors to continually invest to improve match algorithm performance
- Incentivize anti-monopoly and open-source algorithms
- Support per search prioritization
- Support flexible system scaling for rapidly changing threat levels
- Identify financially effective tradeoffs among system hardware/software, maintenance, testing, and match review (may assume a fixed sample acquisition process)

The resulting guidance document is to assume that precise weightings of goals will be application specific. Hypothetical examples may help illustrate how the guidance should be followed in practice.

These goals are part of our project this semester; there is no guarantee that we will be able to answer each and every one. We will however, at a minimum, set the stage for answering these requirements and will provide answers at the end where we are able, as we go through the process of documenting processes technology and implementation of enterprise application of biometric capabilities.

1.4 STAKEHOLDERS

Our stakeholders primarily consist of agencies that require biometric capabilities to support their internal business processes and need to expose portions of their business processes to their brother/sister organizations in resolving identity issues.

Many of these agencies collect and dismeinate biometric information internally but are reluctant to invest in additional, needed biometric-sourced infmation, primarily because these organization understand that similar (or the same) information is possessed, (but unabvailable) from the other/brother/sister organization. These agencies include:

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation (FBI)
- Department of Justice (DOJ)
- State and Local Law Enforcement Agencies

1.5 TEAM BIOMETRIC ENTERPRISE ARCHITECTURE (TEAM BM-EA)

1.5.1 NAT HALL

1.5.2 MIKE LUCKEY

Mike is enrolled in his last class in the George Mason University MSSE program. He specialized in the Computer Based Systems track, and has over 19 years of program management and systems engineering experience working for the Department of Defense. He has a BS in Business Finance from the University of Florida. As a DOD contractor he is the lead engineer and project manager working with the U. S. Army's Logistics Innovation Agency working to modernize Army Logistics business processes and technologies. A retired U. S. Marine Corps Officer Mike has deployed to Somalia and Okinawa Japan supporting USMC and DOD C4I activities in his role as a Data Communications Officer. Upon retiring, Mike has worked in various levels both with various DOD contractors and with the Defense Information Systems Agency (DISA) working a variety of systems engineering and project management areas. Mike's experiences include requirements planning and analysis, system design and architectures, workflow analysis, scheduling, developmental and operational testing, risk management, configuration management, quality assurance, operations and sustainment, process improvement, and the like. Mike's interest are primarily in engineering and implementation of large-scale and enterprise systems.d by the significant investment in stovepipe biometric systems.

1.5.3 JEREMY WORLEY

2 TECHNICAL APPROACH

Team BM-EA will proceed through literature research, project organization, problem formulation, problem space analysis, problems space requirements definition, solution space definition, solutions space design and development including model design, development, execution and results analysis. The remaining parts of this section describe at a high level our plans for implementing this approach.

2.1 PROBLEM FORMULATION AND ANALYSIS

Team BM-EA will use literature review to analyze key aspects of the problem statement; to uncover existing Biometric System Enterprise Architecture (EA) and how that is applied across the systems that employ it and assess the data processing and communications flow required, how the various data algorithms can be used to improve data flow, and ultimately develop a model that provides an analysis of best case response to chosen Biometric Assessment in our proposed EA.

The following literature will be reviewed as a part of our Biometric Enterprise Architecture research efforts to include published papers, reports, trade journals, books, and other research materials. Research for this project falls mainly into three categories:

- Current Biometric System Architectures,
- Current Biometric Systems Implementation
- Biometric Architecture Modeling and Simulation

Each is discussed briefly below:

Current Biometric System Architectures – Research in this category will include investigating what architecture is in place supporting the various biometric capabilities and includes a look at if various architectures are mutually supporting.

Current Biometric Systems Implementation – Research in this category will include investigating the carious systems implemented within the various architectures and will serve as a catalog for considering architectural trade-offs when assessing alternative architectures. Likewise this catalog is to be used as a basis for documenting the existing and contemplated architecture.

Biometric Architecture Modeling and Simulation - The Biometric Enterprise Architecture project will research modeling and simulation methods and models mining for algorithms and data types that allow for efficient and where possible optimal collection and data exchange of biometric data and information. Where adequate models exist we will take advantage of them, where needed, we will create our own.

With these models, the team will investigate technical and economic performance of existing biometric architecture and determine improvements resulting from proposed architecture.

2.1.1 PRELIMINARY PROBLEM STATEMENT

Biometric practitioners require acquisition of various biometric images from various biometric acquisition systems. These systems are acquired based on thier image acquisition method rather than the purpose or circumstances for which the images are acquired or needed. As a result vendors produce stovepipe systems that include solutions for requirements that do not exist from the perspective of IImage Acquisition.

Biometric practitioners do not have a reliable source for Image Management capabilities beyond purchasing or acquiring image acquisition capabilities (hardware) that happens to have its own, (often proprietary) image management software. As a result Biometric practitioners who have a need to integrate or use multiple biometric capabilities (such as coupling fingerprint, facial and voice recognition into an identity) end up with duplicative but not inter operable image management software. They also end up with a significant interoperability dilemma when integrating operations with other agencies.

2.2 PROJECT ORGANIZATION

This phase includes organizing the project into executable phases and partitioning and allocating work across available project resources. The result is a work breakdown structure (WBS) and associated schedule-to-completion defined within the context of the semester.

2.3 REQUIREMENTS DEFINITION

This phase of the effort will include scoping of system objectives, characteristics and parameters in the form of requirements and derived requirements for the system. From the overarching set of system requirements, the subset to be designed and modeled will be determined.

2.4 SOLUTION

2.4.1 DEFINITION

Our solution is made up of four key components, all of which require significant investment in research, analysis and solution engineering to arrive at what we believe to be a salient point or set of points that represent our solution:

1. Collect requirements and model them in an “as-is” representation of the enterprise biometrics architecture under a stated set of assumptions and conditions.

2. Using the same set of assumptions and conditions we will propose an alternative "to-be" architecture
3. We will model the competing architecture's technical and economic/financial performance characteristics.
4. Finally, we will compare the results of the competing models.

2.4.2 PROJECT DESIGN AND DEVELOPMENT

As suggested above we will model the as-is architecture and use that as a basis for developing and designing our technical and economic/financial performance models. After defining the requirements and selecting the scope and domain for the as-is architecture we will use SysML® to develop a context model, the as-is reference architecture and the to-be architecture. Once complete we will design and develop technical and economic/financial models for use in the later comparison of the developed to-be model.

2.4.2.1 MODEL DESIGN AND DEVELOPMENT

Our approach to model design and development is to use the combination of our customer/stakeholder needs (requirements) to understand the distinction between the as-is (the de-facto, ad hoc) architecture and a prospective to-be architecture. We will use Systems Engineering methods and tools to accomplish this by analyzing and documenting user needs, developing a context defining the boundary conditions for our architecture, and modeling both the as-is and to-be architecture using SysML® to document the system's architecture currently and the systems architecture going forward. Finally using this architecture we will develop operationally relevant technical and financial models to assess the effectiveness of the to-be architecture as compared to the as-is architecture.

2.4.2.2 MODEL EXECUTION AND MODEL RESULTS

Our technical models (the technical and the financial) will be used to compare the technical and financial performance of the current (as-is) and prospective (to-be) architecture and support formulating strategy in moving toward the to-be architecture. The goal of our models will be to support answering strategic question such as:

- Improved system performance such as maximizing "match accuracies" with set throughput and response time requirements.
- Search against very large image/identity repository(ies) –in the millions
- Incentivize vendors to continually invest to improve match algorithm performance
- Incentivize anti-monopoly and open-source algorithms
- Support per search prioritization

- Support flexible system scaling for rapidly changing threat levels
- Identify financially effective tradeoffs among system hardware/software, maintenance, testing, and match review (may assume a fixed sample acquisition process)

3 EXPECTED RESULTS

The expected result of this system is proposed alternative architecture for Enterprise scale Biometric systems. Below are the products that will be expected at the end of this study.

1. A technical performance model will be developed to analyze the feasibility of the system as compared to existing implementations for similar capabilities. The artifacts captured in the architecture of the system will be used by our queuing model to simulate the operational concept of this architecture. The result of the model will be an analysis that shows the various performance characteristics for resolving selected, various business requirements.

2. SysML will be used to capture the architecture of the existing biometric architecture. A set of views or artifacts that are defined below will be developed to present the sensor architecture:

- High-Level Operational Concept Description (OV-1): This view will capture the high level operational concept of this sensor system. Describe boundary conditions
- Operational Node Connectivity Description (OV-2): This view will list all operational nodes/stakeholders of the system, and also the information needed to be exchanged among these nodes. In this architecture, all image acquisition nodes image management nodes and image exchange nodes will be captured along with all information exchanged among them.
- Operational Information Exchange Matrix (OV-3): This view will summarize and expand the characteristics of the exchanged information captured in OV-2. The exchanged information's attributes such as information content, classification, periodicity, criticality, and timeliness will be included in this view.
- Activity Model (OV-5): This view will depict a high-level operational activity process of the system. It will display the high-level activities of image acquisition, management and exchanges.
- Event/Trace Description (OV-6c): This view will capture different scenarios/use cases of the operational concept. This view will depict the time-based information flow processes of the activities captured in OV-5.
- Systems Interface Description (SV-1): This view will capture the internal and external interfaces of this system. It will capture system interfaces and boundaries.

- Systems Communication Description (SV-2): This view will capture the communication pathway of the system. All communication nodes that help transmit data among the systems will be captured.
- Systems Functionality Description (SV-4): This view will capture the high-level functionalities of the system. It will capture image acquisition, management and exchange functionalities.
- Operational Activity to System Function Trace ability Matrix (SV-5): This view will map the operational activities captured in OV-5 with functions captured in SV-4 to show how the operational requirements/capabilities can be supported by system's capabilities.
- Systems Data Exchange Matrix (SV-6): This view will capture more details of the data exchanged among systems. Exchanged data's attributes such as data content, format, criticality, periodicity, timeliness, classification, and communication entry point will be captured in this matrix.
- Systems Performance Parameters Matrix (SV-7): This view will capture the performance parameters of the system. All sensors' performance parameters will be captured along with those of C2 systems.