PRJ4M1I - IT Project: Practical Project

Manje Access Control Solution

39197018@mylife.unisa.ac.za | School of Computing | UNISA

Author: Onkgopotse Lenake

Project Proposal: Manje Access Control Solution (MACS)

Project Information

Project Name:	Manje Access Control Solution
Project Time-frame:	2018-03-20 to 2018-07-31
Summary:	The project aims to build a software solution that will be used to simulate the management of access control by events businesses. The software would help by virtually eliminating fraud and corruption with its advanced security processes.
Attached Worksheets:	Project MACS > Project plan
Related Documents:	Resource needs > Requirements document Glossary

Background and Motivation

Setting and history behind the project

Events businesses access control is one of the core events strategic function required to grant valid access to authorized individuals. Different hosted events (e.g.: sports events, music events, seminar events, government events, etc.) require ticket purchasing processes or event registration processes that will grant access to individuals with valid tickets or grant access to individuals with valid event registrations when the event arises. On event day a manual ticket checking process is done or a manual registered event checking process is done for validation and authorization. Tickets are duplicated, event registrations are corrupted, and these manual checking processes can't tell the difference in time to which individuals have valid event access, compared to individuals with invalid event access.

Event organizers and stakeholders lose lots of revenue because of ticket duplication fraud and corrupted invalid event registrations. The high loss of revenue is evident after the event when comparing an event's attendance versus it's sales, in which the results show very low sales. The manual checking processes are inefficient, and they require a great deal of time ahead of the event to be done. Manipulation of the system is easier because of these manual processes and invalid event access entries are gained, which result in a poor event access control management.

Business problem the project addresses

There is a need for events businesses to better manage their access control, and only allow valid authorized individuals to their events. A real-time enhanced security checking process is required for validation and authorization of valid event individuals. This simulated security process for this project would help eliminate ticket duplication fraud and help eliminate corrupted invalid event registrations. With this in-place, efficiency will be archived with the reduced amount of validation time required before the event starts.

By having an innovative simulated biometric fingerprinting technology as a component of the solution, events businesses access control management will be improved. Overall system security will be enhanced to eliminate system manipulations. Validation and authorization processes will be in real-time and this will help improve efficiency. Increases in revenue for the event organizers and stakeholders will be archived.

Some current approaches to the problem

Events businesses can currently do one of the following for access control management:

- Sell their tickets through ticket selling providers (e.g.: Computicket)
- Set up their own private ticket selling premises/sites
- Pay a consultant to set-up a ticket selling website
- Define their in-house event registration processes
- Set up their own event registration sites (Government)

Reasons the problem is worth solving or worth solving better

A managed simulated access-controlled system that eliminates ticket duplication fraud and that eliminates corrupted invalid event registrations will ensure that authorized individuals are permitted to the event. Events will start on their scheduled time with improved efficiency in the validation processes prior to the commencement of the event. Event revenues will increase because of the quality of the system and decreases in costly fraudulent lost sales will be achieved. Fingerprint identification will also save money as no paper will be required to create tickets for selling. Username and password authentication would also help tighten the security.

Some ways the product will be better than previous approaches

By adding new simulation biometric identification system component, we will prevent ticket duplication, prevent event registrations corruption, provide enhanced real-time security verification process and provide a customized solution that is efficient to gain access to an event. A similar biometric system is currently locally used by Capitec Bank to give their clients access to their accounts, and this proves the reliability of the system. This component will give us a unique competitive advantage in the market and is currently not offered by competitors.

Our simulation solution will not have similar ticket purchase processes or event registration processes to gain event access, it will have a fingerprint enrolment process (using an input of images database for simulation purposes) to mimic clients purchasing or registering event access that will be used for verification on event day.

Our simulation solution will not have similar event access acquiring processes and it is uniquely aimed at a specific market segment which is not served by any competing products.

Currently there is no similar product in the same market that will go head-to-head with our product, which gives us full 100% market ownership with no sharing and we are happy about it.

Fingerprint identification and verification, with username and password authentication gives us a unique competitive advantage and our product will leverage those advantages.

Purpose of simulation for this project

For the purpose of this project as a simulation we will have a fingerprint images database that will be used as input instead of using fingerprint reading devices to capture fingerprints. We will develop a customized fingerprint algorithm, with the help from SourceAFIS, that recognizes human fingerprints. It takes fingerprint images on input and produces similarity score on output. With this we can then develop and customize our own algorithm for simulation, instead of using reading devices with their SDKs.

We will also add functionality of username and password authentication as part of the system component. With custom system development, we will also develop a custom database.

Goal

Goal of this project

This project will produce an access control simulation solution, using images databases as input, that would be used by events businesses to grant and manage valid event access for their clients. Our customers would be able to differentiate in real-time to which of their clients have valid access, compared to clients with invalid access. Increased revenue for our customers will be achieved, efficiency, identification and verification processes will also be achieved with our solution's enhanced biometric security features with username and password authentication.

Defining features and benefits of this product

Well managed simulated event access control with advanced real-time security features, including: customized simulation solution for the event, fraud prevention, corruption prevention, efficiency, fingerprint enrolment and linking them to their clients, username and password enrollment, client identification, client verification, client authorization, cost savings because of no paper requirements to create tickets for selling and specialized reports for management and stakeholders.

Scope

We want to focus on a customized simulation solution that uses the capability of biometric fingerprinting technology with the use of an input of images database, capability of registering with username and password. This will be used for client enrolment, client verification, real-time security, efficient performance, and management reports. We will not focus on integration features that connect to the Department of Home Affairs fingerprint database for client verifications.

In Scope	Out of Scope
Building and customizing a biometric algorithm with the help from SourceAFIS, so to have a customized simulation solution.	Building a brand new biometric algorithm.
Fingerprint template creation instructions, for high quality verification results.	Integration features to access Department of Home Affairs fingerprint database.
Username and password registration.	Linking of fingerprint templates and username and passwords. This will be separated.
Real-time security in the form of a biometric image verifications, client-side application and server-side application.	Special security against hackers. Searching for security holes in existing software components.
Database install, server install and data storage that can be handled by one computer.	Managing a cluster of servers.

Deliverables

- Simulation events access control software
- Software installers on each supported platform
- Quick-start guide with sample initial site data
- On-line help for administrators and end users
- Training course materials for administrators
- Utilities to import and/or upgrade database
- Report tool generator

Risks and Rewards

Main risks of this project

1. There are significant technical difficulties in this product. This will be a risk because only one person in our team has much knowledge and experience with software engineering skills and biometric technology. We will address this risk by scoping and scheduling the project to leave enough time for research and reviews.
2. The schedule for this project is very short. We will manage this by planning a conservatively scoped functional core and series of functional enhancements that can be individually slipped to later releases if needed.
3. System performance will be significantly impacted by the decisions made during the database design. To address this, we will frequently review the database design to better optimize the system.
4. There are financial constraints to acquire a biometric fingerprint reader and its SDK to do development work. To address this, we will develop our own biometric fingerprint algorithm that takes fingerprint images as input and produces similarity score on output.

Main rewards of this project if it succeeds

If we successfully simulate this product, we will immediately be able to use it for our own in-house and partner projects. In the 12 months after simulation, we expect to acquire biometric reading devices and their technology, develop a new solution using the devices, sell the new solution and gain significant license and services revenue from customers.

Manje Access Control Solution (MACS) will be the first project of its kind and nature, and there will be no legacy system to phase out for us, but our future competitors. We will be pioneering a new solution that uses biometric identification system to provide increased security for our future customer's event access control and lower their costs by them not needing to buy paper to create tickets for selling.

The success of this project will greatly improve the future ticket purchasing processes used by those hosted event types, greatly improve the future event registration processes used by those hosted event types, with high levels of quality and efficient processes. Ticket duplication fraud and corrupted invalid event registrations will both virtually be eliminated, and this will increase revenue for our future customers, which will generate revenue for our future business.

This project has some clear direct benefits, but it is a journey as much as it is a destination. Significant indirect benefits include our experience with this market segment, product type, development method, development tools, technology, management technique, and partner organization.

Project Overview

Mission and Scope

Business problem the project addresses

There is a need for events businesses to better manage their access control, and only allow valid authorized individuals to their events. A real-time enhanced security checking process is required for validation and authorization of valid event individuals. This simulated security process will help eliminate ticket duplication fraud and help eliminate corrupted invalid event registrations. With this in-place, efficiency will be archived with the reduced amount of validating time required before the event starts.

Goal of this project

This project will produce a simulated access control solution that would be used by events businesses to grant and manage valid event access for their clients. Our customers will be able to differentiate in real-time to which of their clients have valid access, compared to clients with invalid access. Increased revenue for our customers will be achieved, efficiency, identification and verification processes will also be achieved with our simulated solution's enhanced biometric security features, with username and password authentication features.

Scope of this project

We will build an access control simulation solution that uses the capabilities of biometric fingerprinting technology to provide real-time access verification with advanced security features. We will have a fingerprint images database as input for the biometric authentication and have a username and password authentication functionality as part of the simulation for this project. We are not looking into integrate with the fingerprint database of the Department of Home Affairs and this is an opportunity that we can exploit for future projects.

Development methodology of this project

We focus on up-front planning and then iterate during in-house development. We emphasize design documents and use them to tightly manage subcontractors, when they exist.

We will use System Development Life Cycle with Scrum, which is an agile software development method for project management. A few Scrum practices: prioritized work is done, completion of backlog items, progress is explained. That all leads up to a scheduled, major release that must satisfy the initial software requirements specification.

Now that we have a future product insight in the field, we are primarily customer-driven: our process focuses on controlled responses to defects, enhancement requests, and customizations.

Project Plan

Project Information

Project Name:	Manje Access Control Solution
Project Time-frame:	2018-03-20 to 2018-07-31
Attached Worksheets:	Project plan > Resource needs
Related Documents:	Project MACS > Requirements document Glossary

Summary of Project

The project aims to build a software simulation solution that will be used to manage access control by events businesses. The software would help by virtually eliminating fraud and corruption with its advanced security processes, and this in-turn will result in increased revenues for event organizers and resulting in the generation of revenue for our business.

Summary of Methodology

Development approach that will be used

We will use System Development Life Cycle with Scrum, which is an agile software development method for project management. A few Scrum practices: prioritized work is done, completion of backlog items, progress is explained. That all leads up to a scheduled, major release that must satisfy the initial software requirements specifications.

Project team organization

The development team will consist of one lead project manager, whom is also an analyst software engineer and scrum master, one product owner, one qa analyst and one marketing analyst, in which both are also internal software testers.

An independent quality assurance tester will be acquired for beta and release testing.

The management team will be comprised by the project team and potential investor(s).

Development and collaboration tools that will be used

We plan to use the following tools extensively throughout the project:

- Project website
- Project mailing lists
- Issue tracking system
- Version control system
- Automated build system
- Automated test system

Change control management

- Requests for requirements changes will be tracked in the issue tracker.
- The change control board (CCB) will review requested changes and authorize work on them as appropriate.
- After the feature complete milestone, no new features will be added to this release.
- All source code commit log messages must refer to a specific issue ID, after the feature complete milestone.
- Automated build system.

Project plan update process

This project plan will be updated as needed throughout the project. It will be placed under version control and instructions for accessing it will be on the project website. Any change to the plan will cause an automatic notification to be sent to a project mailing list.

Work Breakdown Structure (WBS) and Effort Estimates

Step	Description	Estimate
1.	**Initiation**	**11d**
1.1.	Analyst software engineer research	11d
2.	**Analyses and Planning**	**30d**
2.1.	Requirements gathering	16d
2.2.	Requirements specification	10d
2.3.	Requirements validation	4d
3.	**Design**	**32d**
3.1.	High-level design	5d
3.2.	Low-level design	
3.2.A	Object design	10d
3.2.B	User interface design	10d
3.2.C	Database design	2d
3.3.	Design review and evaluation	5d
4.	**Development and Integration**	**50d**
4.1.A.	System implementation	
4.1.A.1.	Implement object code components	6d
4.1.A.2.	Implement user interface components	6d
4.1.A.3.	Implement database components and configuration	6d
4.1.A.4.	Implement biometric technology components	6d
4.1.A.5.	Integrate components	3d
4.1.B.	Technical documentation	2d
4.1.C.	User documentation	2d
4.1.D.	Testing	
4.1.D.1.	Test planning	2d
4.1.D.2.	Test code implementation	10d
4.1.D.3.	Test execution	2d
4.2.	Implementation review and evaluation	5d
5.	**Implementation and Transition**	**2d**
5.A.	Release packaging	1d
5.B.	Documentation for other groups	1d
6.	**Maintenance and Reflection**	**6d**
6.1.	Postmortem report	6d
	Total	**131 days**

Deliverables in this Release

Deliverable Name	Description	Delivery Date
Software Solution	Simulation events access control software	Implementation Milestone
Software Installs	Software installers on each supported platform	Implementation Milestone
Quick-start Guide	Quick-start guide with sample initial site data	Development Milestone
On-line Support	On-line help for administrators and end users	Implementation Milestone
Training Manuals	Training course materials for administrators	Development Milestone
DB Migration Tool	Utilities to import and/or upgrade database	Development Milestone
Reporting Tool	Report tool generator	Implementation Milestone

Risk Management

The main risks of this project are:

1. There are significant technical difficulties in building an innovative new system using the latest technology trends and standards. This will be a risk because one person on our team has much experience with the relevant tools and technologies. We will address this risk by scoping the project such that we have enough time to research and to review the design and implementation.
2. The schedule for this project is very short. We will manage this by planning a conservatively scoped functional core and series of functional enhancements that can be individually slipped to later releases if needed.
3. The performance of the system will be significantly impacted by the decisions made during the database design task. To address this, we will frequently review the design to better optimize the database.
4. There are financial constraints to acquire a biometric fingerprint reader and its software development kit to conduct development work. To address this and for the purpose of this simulation project, we will develop our own biometric fingerprint algorithm that takes fingerprint images as input and produces similarity score on output. This will be used in conjunction with the development of username and password authentication functionality.

Project Planning Dependencies

Does this project conflict or compete for resources with any other project?

No, this is the only development project that we are working on.

Are the same human or machine resources allocated to maintenance of past versions and/or planning of future versions during this release period?

No, this is the first release and we will not plan the next release anytime soon, but in the future.

Does this project depend on the success of any other project?

No, this project stands alone.

Does any other project depend on this project?

No, the project is not producing any components that will be used in other current projects.

Are there any other important dependencies that will affect this project?

No, everything is covered above.

Yes, we must develop our own biometric algorithm that will simulate the technology capabilities. We must also develop username and password authentication functionality as a part of the simulation for the project.

Plan > Resource Needs

Project Information

Project Name:	Manje Access Control Solution
Internal Release Number:	1.0.0
Project Time-frame:	2018-03-20 to 2018-07-31
Related Documents:	Project MACS Project plan QA plan Software development methodology Glossary

Human Resource Needs

Need	Resource	Amount	Status	Comments/Responsibilities
Project Management	Kgupi, Vovi, Nhlakes, Wandile	131 days	Assigned	Manage product development
Research work	Kgupi	11 days	Assigned	
Milestone 1: Preparation	Project team	1 day	Assigned	Status meeting checkpoint
Requirements gathering		16 days		
Requirements validation		4 days		
Software requirements (SRS)		10 days		
Milestone 2: Inception	Project team	1 day	Assigned	Status meeting checkpoint
Overall Design		15 days		
Detailed UI Design		10 days		
Detailed Database Design		7 days		
Milestone 3: Elaboration	Kgupi, project team	1 day	Assigned	Status meeting checkpoint
System implementation		27 days		
Technical and user documentation		4 days		
Software and QA testing	Kgupi, Nhlakes, Wandile	14 days	Assigned	
Implementation evaluation		5 days		
Milestone 4: Construction	Kgupi	1 day		Status meeting checkpoint
Release packaging and other groups documentation		2 days		
Milestone 5: Transition	Kgupi	1 day	Assigned	Status meeting checkpoint
Onsite support and postmortem report		5 days		
Milestone 6: Reflection and handover	Kgupi, project team	1 day	Assigned	Project handover checkpoint

Capital Needs

Need	Resource	Amount	Status	Comments
Development Laptop	Windows 10 i7	1	Satisfied	Used by software engineer
Development DB Server	Windows 10 i7	1	Allocated	
Interactive Testing Workstation	Windows 10 i7	1	Allocated	
Testing DB Server	Windows 10 i7	1	Allocated	Used by software engineer

Possible Status and Resource Values

- **Kgupi**: Onkgopotse Lenake (Lead Project Manager, Scrum Master, Analyst Software Engineer)
- **Vovi**: Sivile Ningiza (Product Owner, Project Team Member)
- **Nhlakes**: Meshack Gumede (QA Analyst, Project Team Member)
- **Wandile**: Wandile Sibeko (Marketing Analyst, Project Team Member)
- **Pending**: request is awaiting management decision
- **Assigned**: task has been assigned to a person in the issue tracker
- **Allocated**: capital request approved by management, but resource has not arrived
- **Satisfied**: request is satisfied, resource has arrived
- **Rejected**: requested resource will not be allocated, plan must be adjusted to work without this resource

I. Project MACS > MACS Requirements document

II. Project Information

Project Name:	Manje Access Control Solution
Internal Release Number:	1.0.0
Related Documents:	Project MACS > MACS Requirements document Glossary

III. Approval

Title: MACS Requirements Document	
Author: Onkgopotse Lenake	**Date:** 2018-04-25
Revision Number: 1.0.0	**Issue Number:** 1.0
Approved by:	**Date:**

IV. Revision history

Revision number	Revision date	Author	Summary of changes
1.0.0	2018-04-25	Onkgopotse Lenake	First Issue

V. Related documents

Document name	Date	Author
MACS Requirements Document	2018-04-25	Onkgopotse Lenake

VI. Distribution

Name / Organizational Unit
UNISA PRJ4M1I Module Department

Table of Contents

1. INTRODUCTION

1.1 Purpose of this document

This document formally describes the user requirements for the conceptual model of Manje Access Control Solution, simulation project. It is intended for review and approval by the UNISA School of Computing, PRJ4M1I module department.

1.2 Scope of this document

This document describes the requirements for the final concept of Manje Access Control Solution, simulation project. User needs identified in the project background and scope will be defined, which will define the user requirements that will define and map the system requirements specifications. The development of each stage of the project is defined in the project plan with the effort estimates and the project resource needs defined in the resource needs document.

Requirements for the system components are marked as “M” (mandatory), “D” (desirable), “O” (optional) and “E” (possible future enhancement) to show their priority and the level of which that they are prioritized. Optional and possible future enhancement does not imply that they are not part of the system, but they will be determined at a later stage.

1.3 Definition of terms

Tag	Description
MACS	Manje Access Control Solution
RD	Requirements Document
Ref.	Reference Document
Rev.	Revision Number
BR	Business Requirements
UR	User Requirements
SRS	System Requirements Specifications
DB	Database
OS	Operating System
SHA	Secure Hash Algorithm
PM	Physical Machine
VM	Virtual Machine
ACS	Access Control System
CAS	Central Authentication System
IDE	Integrated Development Environment
FQDN	Fully-Qualified Domain Name
WLAN	Wireless Local Area Network

1.4 Reference documents

Ref.	Document ID.	Title	Rev.
RD1	MACS RD	MACS Requirements Document (this document)	1.0.0

2. GENERAL DESCRIPTION

There is a need for events businesses to manage access control and only allow authorized individuals to their events. The goal of the project is to build a software solution that will be used to simulate the management of access control by events businesses. The software will help by virtually eliminating fraud and corruption with its advanced security processes.

2.1 Project context

This document lists requirements for the conceptual model of a software solution that will be used to simulate the management of access control. Several ticket purchasing processes or event registration processes exist and are offered by their specific vendors, most notably Computicket, iTickets and Web Tickets, but neither implement the same objectives as desired in this project. The goal of the project is to build a software solution that will be used to simulate the management of access control by events businesses.

The project consists of a number of phases and will produce pre-determined outputs during the course of the development. The outputs of the phases should function as independent components and will be used to assess the progress of the project and to determine the project's course. The core components part of the project "M" (mandatory) are non-negotiable and form part of the final product. Other components "D" (desirable), "O" (optional) and "E" (possible future enhancement) are other components of the project that may or may not be part of the final product and will be determined by how the project progresses. It is recognized that not all user requirements may be met, especially the "O" and "E", at the end of the project.

2.2 General capabilities

Using biometric technology, the software will be capable of producing a solution that will be used for enrollment, identification and verification for access control management. The priorities of this production in order are, client enrolment (input fingerprint images for extraction and creating final biometric fingerprint templates, which will be linked to their specific clients) and client identification for verification and validation.

Some challenges exist in order to provide the full solution and its capabilities. The solution will be developed and made up of four systems, namely: MACS System, Home Affairs System, Bank System and Web Ticket System. MACS System is the main system and because of security and access reasons, the other three systems will also be custom built as I won't be allowed access to the current real-world live systems. For the purpose of the solution, all four systems will be simulation systems.

System Integrations

(a) Integration to the Home Affairs simulation system to request an individual's biometric fingerprints for verification and validation. As the Department of Home Affairs holds all South African's population fingerprint information and personal details, this integration is mainly to request, verify and validate individuals whose fingerprints were not extracted and captured by Manje Access Control Solution (MACS). An individual's ID number will be used in the request query sent to Home Affairs to retrieve the correct individual's information.

(b) Integration to the Bank simulation system to verify and validate individuals that have biometric fingerprints captured by the Bank, so to access individuals bank accounts and transact on them. The bank transactions will be carried out by MACS system users when making account sale purchases (on event day) and when making event ticket orders (Web Ticket system) on behalf of the individuals (clients).

(c) Integration to the Web Ticket simulation system to place event ticket orders for the individuals (clients) by MACS system users. The client's extracted and captured biometric fingerprint features

(which are linked to the extracted final fingerprint template) will be linked with the client's ordered event ticket and order payments will be made with the above Bank simulation system.

Ideally, the system will consist of distinct modules that function to simulate the components of the system. Once an initial version of the system is produced that fulfils the above capabilities, it will be extended with a library of additional components to enhance the system and extended with other machines to enhance its scalability. The hardware stack properties of the system machine components will be specified in a Hardware Specification Appendix, while the software stack properties of the system software components will be specified in the Software Specification Appendix. Both the hardware and the software specifications will define the system environment and its infrastructure.

The system module components will be defined in the system design and the modules will be re-usable and have the possibility to be enhanced. A custom-built components library will be developed and the idea to build a library was driven by the Model View Controller (MVC) framework because it makes development to be flexible and easy to reuse software components of the system. Using the MVC development strategy to develop the solution, the custom-built library will serve as the *Controller*, the four databases for the four simulation systems that form the solution will serve as the *Model* and the windows forms together with web pages will serve as the *View* in the Model View Controller (MVC) framework.

The ideal final software solution product will be platform independent, able to fulfil the above capabilities on different host configurations.

2.3 Business requirements (BR)

The target group for the software product are end-users that need to simulate the software and end-users that want to simulate the software for the hosted events environment. Their intent is to simulate and allow valid individuals and to simulate not to allow invalid individuals. This raises the need to manage access control and only allow authorized individuals. The group can be classified as users varying from students, small businesses and large businesses.

2.4 User requirements (UR)

Student users will want an environment where they can be able to install the system on their personal Operating System (OS) and be expected to do interactions that uses the capabilities of the system. Interactions expected can be to load sample or load their own fingerprint images, register usernames and passwords and test the system verification processes, mainly the biometric technology functionalities.

Small business users can be expected to install the OSs required for document access, as well as installation of software packages on their own provided environment. Accessing more complex objects, more involved interactions within the system can be expected, resulting in higher loads to the system.

Large business users will want to create their own environments on the fly, tailor-made to their needs. Customizing various modules to create specific settings, along with custom installation of OSs can be expected. The system will be used to the fullest, placing the highest stress on the system. Interchanging modules within one environment to test and compare settings can be expected to lead to various configurations.

2.5 MACS Solution System (Use Case Diagram)

Provided below is a simplified abstraction showing the solution use case. The diagram depicts the solution use context and its system integrations.

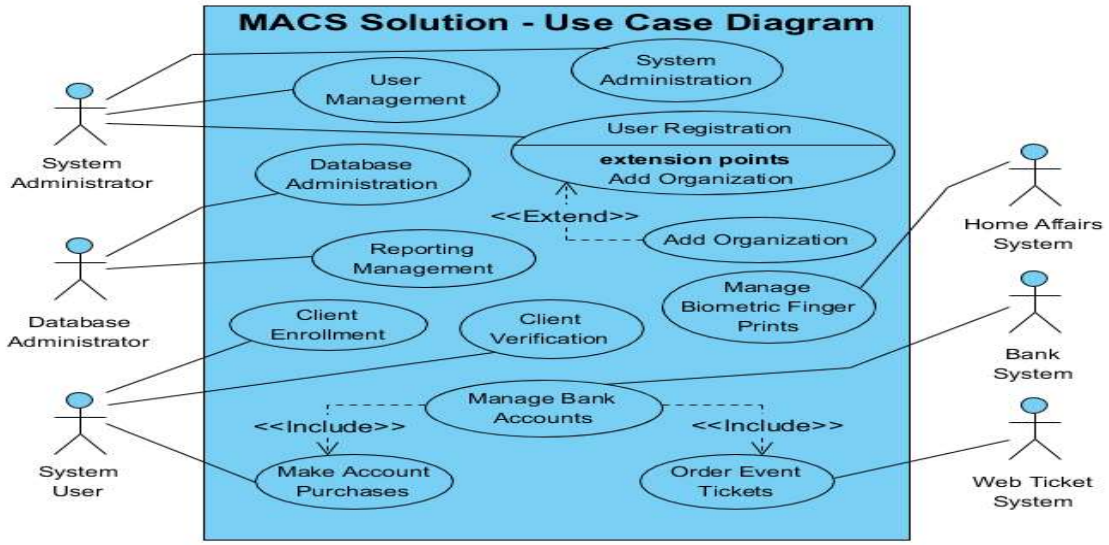


Figure 2.5.1: Simplified diagram of MACS use case

2.6 Assumptions and dependencies

There are several assumptions and dependencies which form the basis for some of the decisions following. These are the following:

2.6.1 Assumptions

- An Access Control System (ACS) can be used to have a Central Authentication System (CAS) that will manage system objects access for security purposes. This functionality would enhance system security on different layers.
- A System Service, services can be used that can provide and manage system communications between the ACS and other system objects. The service can also provide other functionality that can be used to integrate with other third-party systems.
- A File system can be used to manage and save system files. This functionality would enhance the system flexibility and scalability. Another test machine can also be used for this project.
- A Website for on-line client enrollment and registrations can be developed to further enhance the system functionality.

2.6.2 Dependencies

- Direct interaction with ACS depends on the system used which creates a dependency on support from the manufacturer. This functionality is an optional, possible future enhancement and it would be depended on how much time the project has to implement. A separate server can be installed and configured for this functionality.
- System Service, services functionality is an optional, possible future enhancement and it would extend the system functionality. This functionality can provide useful functions that make the system to be easily scalable and it can also provide integration functionality to other systems. It is depended on how much time the project has to implement and can be configured and installed on its own server.
- A File system with a client 2 test machine for this project are optional to have and can be installed and configured on their own (a server for the file system and a test machine for client 2). It is depended on how much time the project has to implement both.
- An on-line client registrations and enrollment Website system functionality is a possible future enhancement and it is depended on how much time the project has to implement.

- Development will be incremental, so later stages depend on previous results. Given the limited timescale, prioritization of tasks will be necessary to ensure the most important items are completed first.

2.7 System network context

Provided below is a system network diagram showing the client-server architecture. The mandatory Physical Machine (PM) or Virtual Machine (VM) show the core non-negotiable hardware components of the system that are to be implemented. Optional and possible future enhancement machine show hardware components that may or may not be implemented depending on how much time the project has to implement.

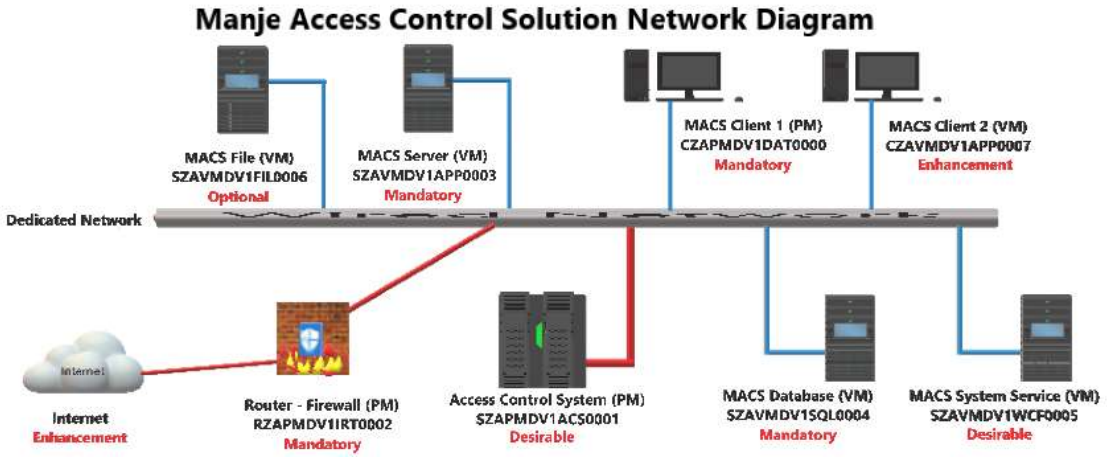


Figure 2.7.1: MACS client-server architecture with Access Control System (ACS)

3. SYSTEM REQUIREMENTS SPECIFICATIONS (SRS)

The SRS is made up of functional requirements that are part of the system and non-functional requirements that are not part of the system. The non-functional requirements are possible future enhancements that may be explored.

3.1 Functional requirements - Processing

This section contains all the users' functional requirements with regards to the processing aspect of the system. Any users' functional requirement shall be defined on the basis of the following rules. In particular, it will be listed in a row of a table as presented in Table 1. Each requirement is prioritized as follows:

M Mandatory requirement. This feature must be built into the final system.

D Desirable requirement. This feature should be built into the final system unless its cost is too high.

O Optional requirement. This feature can be built into the final system at the Project Manager's discretion.

E Possible future enhancement. This feature is recorded here so that the idea is not lost. The decision on whether to include it in the system will depend on progress on the mandatory requirements.

3.1.1 Devices – Table 1

ID	Requirement	Necessity
UR-3.1.1.1	The Server application (server-side) should be configured and installed on its own virtual machine server: MACS Server (VM), Fully-Qualified Domain Name	M

	(FQDN): SZAVMDV1APP0003.macsnetwork.local. The Server to host all four systems. Issues: What if the Server application cannot be installed on its dedicated machine?	
UR-3.1.1.2	The Database application should be configured and installed on its own virtual machine server: MACS Database (VM), FQDN: SZAVMDV1SQL0004.macsnetwork.local. The Server to host all four databases. Issues: What if the Database application cannot be installed on its dedicated machine?	M
UR-3.1.1.3	The Client 1 application (client-side) should be configured and installed on its own physical Laptop machine: MACS Client 1 (PM), FQDN: CZAPMDV1DAT0000.macsnetwork.local. Issues:	M
UR-3.1.1.4	The Wireless Router device should be configured to connect the system dedicated network, FQDN: RZAPMDV1IRT0002.macsnetwork.local. Issues:	M
UR-3.1.1.5	The ACS software should provide code that integrate to its applications and should be configured and installed on its own physical MicroServer machine: Access Control System (PM), FQDN: SZAPMDV1ACS0001.macsnetwork.local. The MicroServer should be able to host the virtualization environment for the virtual machines. Issues: What if support is required from the ACS manufacturer, and what if the MicroServer can't be acquired?	D
UR-3.1.1.6	The System Service, services should be configured and installed on its own virtual machine server: MACS System Service (VM), FQDN: SZAVMDV1WCF0005.macsnetwork.local. Issues: What if the System Service, services cannot be installed on its dedicated machine?	D
UR-3.1.1.7	The File system should be configured and installed on its own virtual machine server: MACS File (VM), FQDN: SZAVMDV1FIL0006.macsnetwork.local. Issues: What if the File system cannot be installed on its dedicated machine?	O
UR-3.1.1.8	The Client 2 application (client-side) should be configured and installed on its own virtual machine for testing purposes: MACS Client 2 (VM), FQDN: CZAVMDV1APP0007.macsnetwork.local. Issues: What if the Client 2 application cannot be installed on its dedicated machine?	E

3.1.2 Database(s) – Table 2

ID	Requirement	Necessity
UR-3.1.2.1	The software main Database(s) should be able to read, write and store system transactional data. See Appendix B for further details. Issues:	M
UR-3.1.2.2	The software integration Database(s) should be able to read, write and store integration systems data. See Appendix B for further details. Issues:	M

3.1.3 External files – Table 3

ID	Requirement	Necessity
UR-3.1.3.1	The software should be able to read and load different image file formats, which contain fingerprint images that identify specific client's fingerprints. The images should be processed to extract and create final biometric fingerprint templates, linked to their specific clients and stored for later verification usage. Issues: What if different image file types cannot be processed and linked?	M
UR-3.1.3.2	The software should be able to import username and password files, which contain specific users' credentials data. This data must be validated. Issues: What if this feature causes system security breaches?	O
UR-3.1.3.3	The software should be able to read a solution configuration file (INI file), which contain a list of configuration data that make up specific configurations, per system. Issues: What if the configuration functionality cannot be implemented?	D

3.1.4 User interface characteristics – Table 4

ID	Requirement	Necessity
UR-3.1.4.1	An image file type can be loaded and processed via a user interface. Issues:	M
UR-3.1.4.2	A username and password can be enrolled/registered via a user interface. Issues:	M
UR-3.1.4.3	A system configuration file can be created via a user interface. Issues:	D

3.1.5 Target software – Table 5

ID	Requirement	Necessity
UR-3.1.5.1	The software should be able to be hosted on operating systems comparable to Microsoft Windows (7, 8, 8.1, 10) Home and Professional. Issues:	M
UR-3.1.5.2	The software should be able to be hosted on operating systems comparable to Microsoft Windows Server (2008 R2, 2012, 2012 R2, 2016) Home and Professional. Issues:	D
UR-3.1.5.3	The software should be able to be hosted on operating systems comparable to Ubuntu Desktop (16.04, 18.04) LTS. Issues:	D
UR-3.1.5.4	The software should be able to be hosted on operating systems comparable to Ubuntu Server (16.04, 18.04) LTS. Issues:	D
UR-3.1.5.5	The hardware and software should be able to be installed, configured and run on the recommended minimum requirements, within the infrastructure environment. See Appendix A for further details. Issues: What if some of the hardware or software can't be acquired?	M
UR-3.1.5.6	The infrastructure environment's Firewall and Anti-Virus software should be able to allow access to the system applications and the system network traffic. Issues:	M

3.2 Functional requirements – Custom Library

This section contains all the users' functional requirements with regards to the library aspect of the system. Any users' functional requirement shall be defined on the basis of the following rules. In particular, it will be listed in a row of table as presented in Table 6. Each requirement is prioritized as follows:

M Mandatory requirement. This feature must be built into the final system.

D Desirable requirement. This feature should be built into the final system unless its cost is too high.

O Optional requirement. This feature can be built into the final system at the Project Manager's discretion.

E Possible future enhancement. This feature is recorded here so that the idea is not lost. The decision on whether to include it in the system will depend on progress on the mandatory requirements.

3.2.1 Module management – Table 6

ID	Requirement	Necessity
UR-3.2.1.1	System modules should be organized in a custom developed library, associating configuration applications and operation applications components code with their modules. Issues:	M
UR-3.2.1.2	The library should maintain a module list consisting of metadata that can be used to identify system modules. Issues:	M
UR-3.2.1.3	The module list should be updateable with newer modules, while maintaining a versioning system of modified modules. Issues:	M
UR-3.2.1.4	The library should be able to provide the system with the module code based on information from the module configuration file. Issues:	M
UR-3.2.1.5	Validation and verification modules should be able to apply customized rules and results, based on the threshold criteria defined and applied. Issues:	M

3.2.2 Module use – Table 7

ID	Requirement	Necessity
UR-3.2.2.1	It should be possible to re-use modules for multiple system configurations. Issues:	M
UR-3.2.2.2	Modules should be in-depended as much as possible from other system components for efficiency, better debugging and better system maintenance. Issues:	M

3.2.3 Events logging – Table 8

ID	Requirement	Necessity
UR-3.2.3.1	It should be possible to log all system events and messages, whether normal or errors, for troubleshooting purposes. Issues:	M
UR-3.2.3.2	Object access matrix with their roles should be enforced and logged for security auditing. Issues:	M
UR-3.2.3.3	The process of logging all system events, messages and security audit logging should be automated.	

3.3 Integration Systems functional requirements

3.3.1 Integration to Home Affairs System – Table 9

ID	Requirement	Necessity
UR-3.3.1.1	The software will integrate to the Department of Home Affairs simulation system that is custom built so to access the fingerprint database for client's identification and verification. Issues: How will user data privacy be handled with national and international regulators?	M

3.3.2 Integration to Bank System – Table 10

ID	Requirement	Necessity
UR-3.3.2.1	The software will integrate to the Bank simulation system that is custom built so to access client's bank accounts using their biometric fingerprint templates stored at the bank. Issues: How will user data privacy be handled with national and international regulators?	M

3.3.3 Integration to Web Ticket System – Table 11

ID	Requirement	Necessity
UR-3.3.3.1	The software will integrate to the Web Ticket simulation system that is custom built so to place event ticket orders for clients. Issues:	E

3.4 Non-functional requirements

N/A

4. APPENDIX A INFRASTRUCTURE ENVIRONMENT

This section provides information about the simulation system's infrastructure environment, details of the recommended minimum hardware and software requirements and the development tools that will be used to build the system.

The main infrastructure environment's physical devices are: Laptop, Wireless Router and MicroServer. The Laptop will be used for development, testing and/or virtualization host if the MicroServer is not acquired. The Wireless Router will be used to provide a dedicated network. The MicroServer will be used as a host for the virtualization environment and the guest virtual machines to be created and configured in it.

4.1 Infrastructure devices

Name	OS	CPU	RAM	Hard drive	Available?
Lenovo ideadpad 110-15ISK (Laptop)	Windows 10 Home v1803	Intel Core i7-6500U 2.50GHz 2.60GHz	8GB	1TB	Yes
HP ProLiant MicroServer Gen8 (Virtualization Host)	Ubuntu Server 18.04 LTS	Intel Celeron Dual Core 2.3GHz	16GB	500GB	Not yet
Network device name	**WLAN properties**	**Security type**	**Network band**		**Available?**
HUAWEI Mobile WiFi E5573 (Wireless Router)	Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC	WPA2-Personal	2.4GHz		Yes

4.2 System hardware stack

Name	OS	CPU	RAM	Hard drive	Available?
Access Control System (PM) (Server minimal)	Ubuntu Server 18.04 LTS	Intel Celeron Dual Core 2.3GHz	16GB	500GBGB	Not yet
MACS Server (VM) (Server minimal)	Ubuntu Server 16.04 LTS	Dual Core 2GHz	2GB	20GB	Yes
MACS Database (VM) (Server minimal)	Windows Server	Dual Core 2GHz	2GB	50GB	Not yet
MACS System Service (VM) (Server minimal)	Windows Server	Dual Core 1GHz	1GB	20GB	Not yet
MACS File (VM) (Server minimal)	Linux v2.2	Dual Core 1GHz	1GB	15GB	Not yet
MACS Client 1 (PM) (Workstation minimal)	Windows 10 Home v1803	Intel Core i7-6500U 2.50GHz 2.60GHz	8GB	1TB	Yes
MACS Client 2 (VM) (Workstation minimal)	Ubuntu Desktop 16.04 LTS	Dual Core 2GHz	2GB	10GB	Not yet

4.3 System software stack

Application	Version	Files	Available?
Access Control System Application(s)			Not yet

Windows Communication Foundation (WCF) Services			Yes
Configuration			Yes
User Management			Yes
Group Management			Not yet
Launcher			Yes
Enrollment Station			Yes
Load Monitor			Not yet
Reporting Tool			Not yet

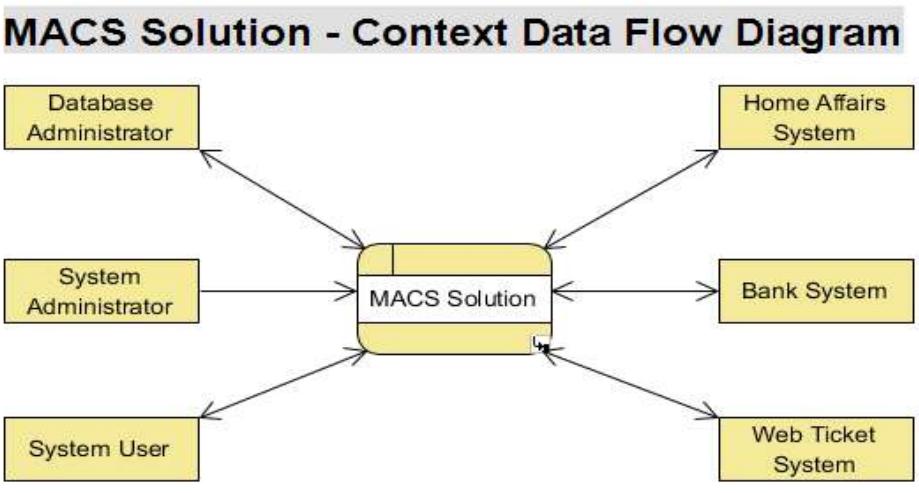
4.4 Development tools

Application	Version	Available?
Microsoft Visual Studio Community (IDE) 2017	v15.6.0	Yes
Microsoft SQL Server Management Studio	v17.6	Yes
C# Programming Language	2017	Yes
Oracle VM VirtualBoxManager for Windows	v5.2.12	Yes
Windows Hyper-V Hypervisor	Windows 10 Home v1803	Yes
Python	V3.5	Yes

5. APPENDIX B INTEGRATION DATA FLOW

This section provides information about the simulation solution and its integrations to other systems. Integration are from the MACS System to the Home Affairs System, the Bank System and the Web Ticket System.

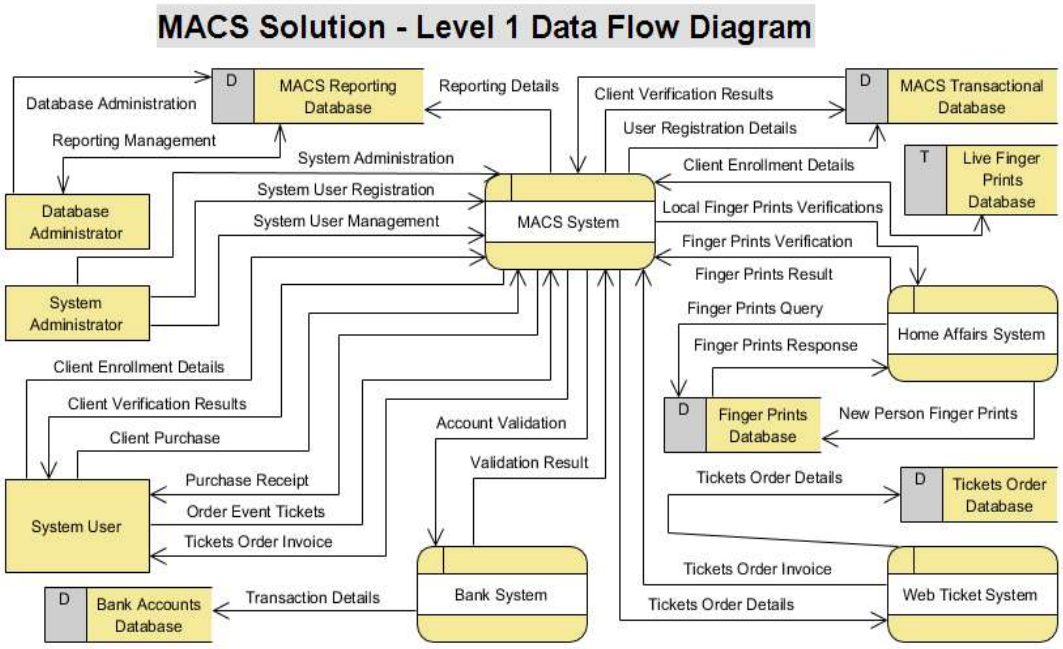
5.1 MACS Solution System (Context DFD)



The data flow diagram here shows a context Data Flow Diagram for MACS Solution System. It contains a process (*MACS Solution* - shape) that represents the system to model. It also shows the participants who will interact with the system, called the external entities.

Database Administrator, System Administrator, System User, Home Affairs System, Bank System and the *Web Ticket System* are the entities who will interact with the system. In between the process and the external entities, there are data flow (connectors) that indicate the existence of information exchange between the entities and the system.

5.1.1 MACS Solution System (Level 1 DFD)

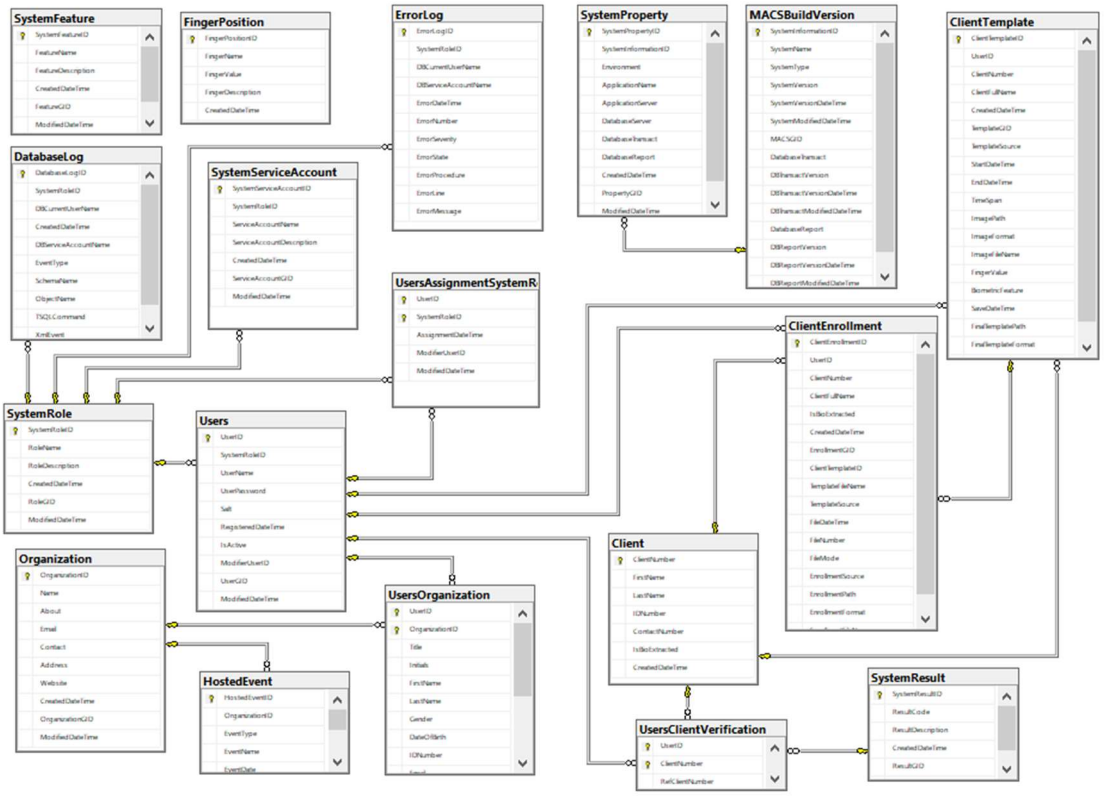


The DFD here shows the level 1 DFD, which is the decomposition (i.e. breakdown) of the MACS Solution process shown in the Context DFD. The MACS Solution Data Flow Diagram contains four processes, three external entities and six data stores.

Based on the diagram, a System User can extract, enroll and verify a client's biometric fingerprint details using the MACS System process, where in the extraction process a final fingerprint template is created and stored for later client verification and validation use, and the related client details (e.g. name, surname etc.) are stored in a local Live Finger Prints Database store. Later during the day, the local database is synced with the main MACS Transactional Database store. While data stored in MACS Transactional Database are persistent data (indicated by the label "D"), data stored in Live Finger Prints Database are transient data that are held for a short time (indicated by the label "T"). A System Administrator can administer the system and manage System Users' registration using the MACS System process. A Database Administrator can administer the database and manage reporting using the MACS Reporting Database. A System User can manage client account purchases using the MACS System process, Bank System process and the Bank Accounts Database store. A System User can manage event tickets ordering for clients using the MACS System process, Web Ticket System process and the Tickets Order Database store. A System User can also request and verify a client's

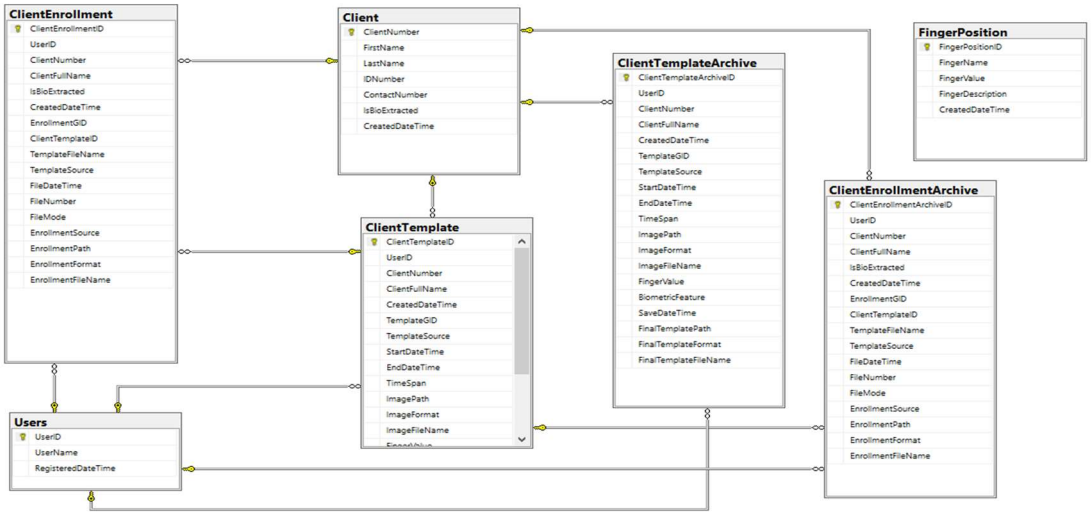
biometric fingerprint template details using the MACS System process, Home Affairs System process and the Finger Prints Database store.

5.2 MACS System – MACS Transactional Database Diagram



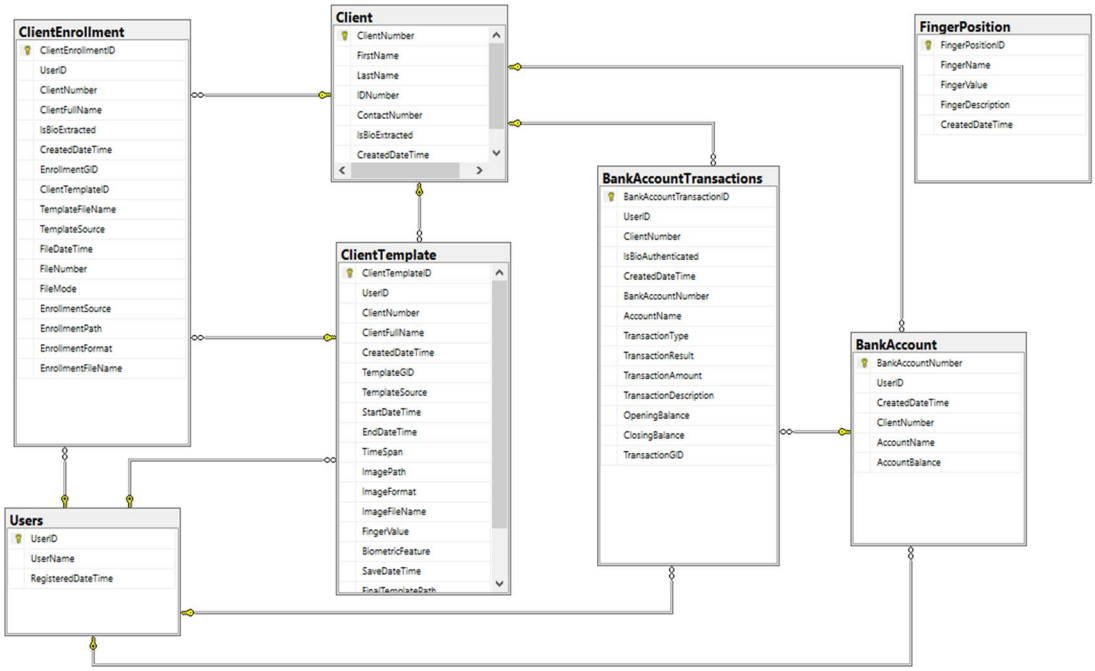
MACS System Process – MACS Transactional Database Diagram store depicted in Level 1 DFD. MACS Reporting Database Diagram store and the Live Finger Prints Database Diagram store, both depicted in the Level 1 DFD are omitted here for brevity.

5.3 Home Affairs System – Finger Prints Database Diagram



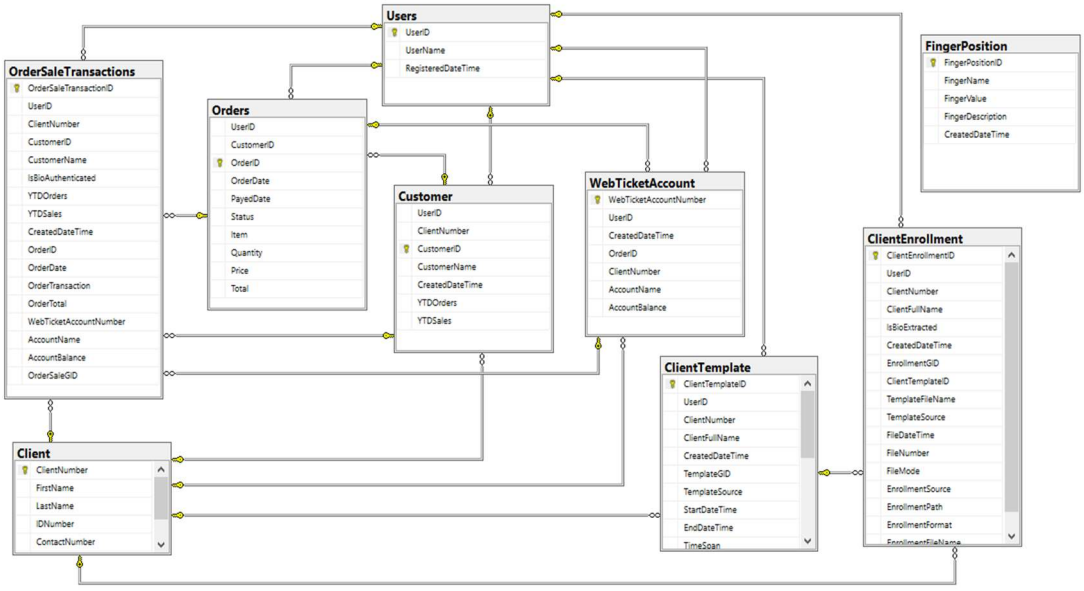
Home Affairs System Process – Finger Prints Database Diagram store depicted in Level 1 DFD.

5.4 Bank System – Bank Accounts Database Diagram



Bank System Process – Bank Accounts Database Diagram store depicted in Level 1 DFD.

5.5 Web Tickets System – Tickets Order Database Diagram



Web Ticket System Process – Tickets Order Database Diagram store depicted in Level 1 DFD.

5.6 Solution Development

Development of the system changed over time with respect to some of the requirements. The system was developed with a custom library, that is compiled into a DLL and mostly composed of the below core class components and WCF services:

SQL Classes	Biometric Classes	General Classes	WCF Services
AddUser	BioClient	AesSymEncryption	HomeAffairsVerify
AddUserOrganization	BioEngine	GetSettings	BankAccountValidate
ChangeUserPassword	BioMatch	VDEventLog	WebTicketOrder
Client	BioTemplate		
ClientEnrollment			
ClientTemplate			
GetClientBioDetails			
GetClientBioTemplates			
GetClientFullDetails			
GetFingerName			
GetLastDBFileNumber			
GetSystemRoles			
GetUserLogin			
UpdateClientBioStatus			

The SQL class components interact with all of the four custom systems databases, mainly to automatically retrieve and record relevant database interactions across all four systems that form the solution.

Biometric classes are used to extract and create final fingerprint templates, match client templates for client verification and validation and link templates to their specific clients in order to identify and authenticate a specific client. As a simulation system, this way I can uniquely link a specific client to their template for matching and verification. Biometric verification is solely done on an extracted and stored template level and "NOT" on a database record level. A template is extracted and created from an input fingerprint image file, where for each client, two fingerprints (right thumb and left thumb) are linked to a specific client, for their two templates. The final template file is stored with the format: "*FirstNameLastName.RightThumb.Date.Time*", where a similar format is followed for the *LeftThumb*. This way, all templates will be unique.

General classes and mainly the GetSettings class automatically retrieve all four systems configurations in terms of database connection strings, event log files, error log files, biometric fingerprint templates storage paths and files, local database storage files and paths, and these settings are configured in one INI file that has all settings per system.

WCF services are used for integration amongst the systems so they interact and exchange data. *HomeAffairsVerify* service to query for a client's biometric fingerprints using the client's ID number to get the correct fingerprints. If they exist, use them for verification, with a result of pass or fail.

BankAccountValidate service to verify a client's fingerprints against the ones stored at the Bank and if a match is valid, validate if the client has funds in their account. If funds are available, then transact on the client's account. Transactions including making sale purchases and paying for web tickets ordered.

WebTicketOrder service to place web ticket orders for clients and paying for the order, with a result of success or failed. The idea to build a library was driven by the Model View Controller (MVC) framework because it makes development to be flexible and easy to reuse components of the system.