Project Plan and System Design Document

Scott Allison

scott.allison1@snhu.edu

Southern New Hampshire University

Project Plan

Work Breakdown Structure

Outlined below is a chart detailing the order of operations in a simplistic manner. Each step is of vital importance to the project. Additions or subtractions are ill-advised and will only compromise the time table and cost given above.

It begins with the initial proposal and assigning the project manager(s) once approved. It moves into the planning stage where meetings are held, assessing risks and reviewing the primary plan of action for step 3's several tasks. A secondary plan is reviewed where-in other non-essential risks are assessed and contingencies are made for changes in work flow. Step 3 is where each system is developed. Divided in several sections for ease of legibility this is where the base database will be constructed, as well as the digital and physical interfaces for this. Additionally further risks not known before will be measured and given due attention if needed. The final step is testing and launch followed by watching for errors arising from public use.

Timeline

Once accepted and the project is under way it will be divided into 4 stages. The first stage is several meetings to ensure the entire team is on the same page. The meetings will go over the 4 stages of development. As well as more in depth looks at the the rest of the first stage. Which will consist of the construction of a first draft of the central database, several mock databases, and ordering the physical and digital hardware. It's expected to take 5 months for this.

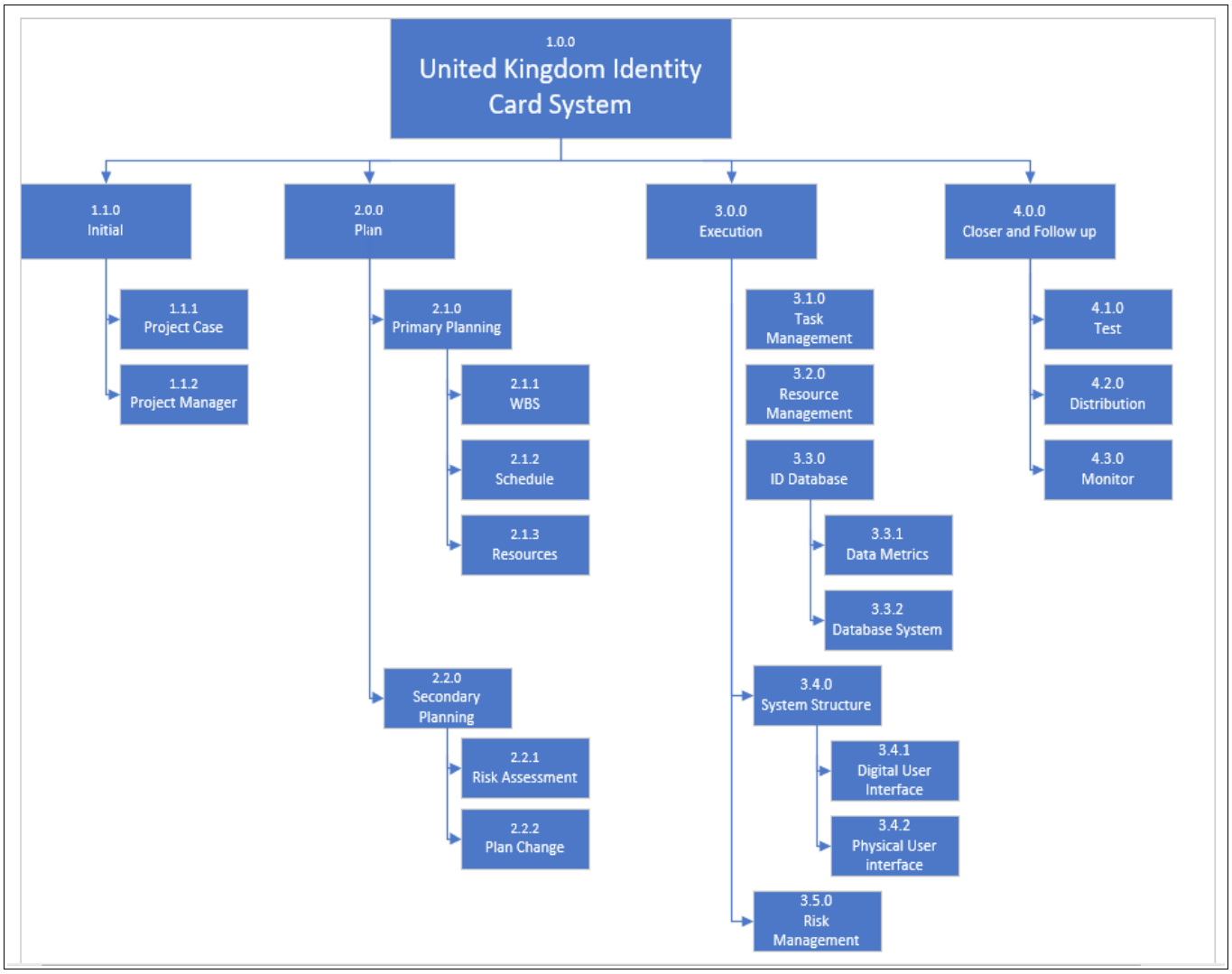
The second stage is connecting the databases to the central and creating the auto-syncing feature. Once completed the security systems will be put in place and stress testing can begin. During this step the central database must be finalized in its development. Again 5 months.

Stage three is continued stress testing, as well as the construction of more the card reader software for the card syncing technology and connecting it to the central database as well. Additionally a small controlled public test where in non-caustic volunteer databases will be added into the central database in an effort of live testing. After which there will be at trial and error period before wiping it clean in preparation for stage 4. Expected time is 4-6 months.

Stage four is public release. Where in the central database will be wiped clean of internal testing data and populated with external data from real databases. The software modifications developed during stage 2 to connect other databases to the central will be distributed to participating branches, installed by technicians from the team, and monitored. The card readers as well. During this time will be the most crucial task of monitoring for errors and ready to pull the kill switch if necessary. Expected time is 6-12 months. Altogether this project should be completed in 3 years.

Dependencies

Each task in the WBS is vital to the subsequent steps in the order. Risk assessment can not happen without secondary planning. The execution can't occur without the plan. Communication between teams is also of vital significance. The developers of the base database must keep an open dialogue with those linking the database with existing databases. The risk of this is they don't communicate and the wrong data is placed in a metric leading to possibly someone dying. Between each stage outlined above and detailed during the WBS it's important to complete each objective in that stage. Without that the whole process breaks down. Without initial stress testing during stage two, stage three's controlled voluntary test could collapse. Throwing the entire project off schedule.


1.0.0
United Kingdom Identity Card System
1.1.0 Initial
2.0.0 Plan
3.0.0 Execution
4.0.0 Closer and Follow up
1.1.1 Project Case
1.1.2 Project Manager
2.1.0 Primary Planning
2.1.1 WBS
2.1.2 Schedule
2.1.3 Resources
2.2.0 Secondary Planning
2.2.1 Risk Assessment
2.2.2 Plan Change
3.1.0 Task Management
3.2.0 Resource Management
3.3.0 ID Database
3.3.1 Data Metrics
3.3.2 Database System
3.4.0 System Structure
3.4.1 Digital User Interface
3.4.2 Physical User interface
3.5.0 Risk Management
4.1.0 Test
4.2.0 Distribution
4.3.0 Monitor

Use of Tools

Software required for this project is as follows. Other software and hardware has been outlined further below in the “Resources” section.

Microsoft Excel. This will be used largely for record keeping. Using this software allows the large team to keep the goals clear and who is on what project. As well as monitoring the timeline.

MySQL. It will be the server software that will be the basis of each database. It's one of the most commonly used database softwares around and thus perfect for reaching the widest audience with minimal conversion effort needed by the team.

Microsoft Visio, As a chart software it can help give visual guides to the team in what they will be crafting. Using this tool is incredibly helpful for painting a picture and getting everyone on the same page of a project.

System Design

Introduction

The purpose of this project is to create an Identification card for the entire United Kingdom. The purpose of this design document is to introduce, debrief, instruct, and preemptively answer any questions one may have regarding the task ahead. The database will include more than 40 metrics of data including biometrics, photos, and other personal information. It will be usable by every government facility as well private institutions such as universities, hospitals, and police stations. Security is paramount when handling private information must be first and foremost when approaching the project. This document outlines this and the software, hardware, and interface concerns.

Requirements

For the project to be considered a success it must not only function as a database, but must able to collaborate and synchronize with other participating databases. It must also be able to handle the server stress of millions of concurrent users. The GUI must be completed and functional. The hardware card scanners must be delivered, installed, and operational. It must also be successfully populated with its data in their proper categories.

Design Constraints

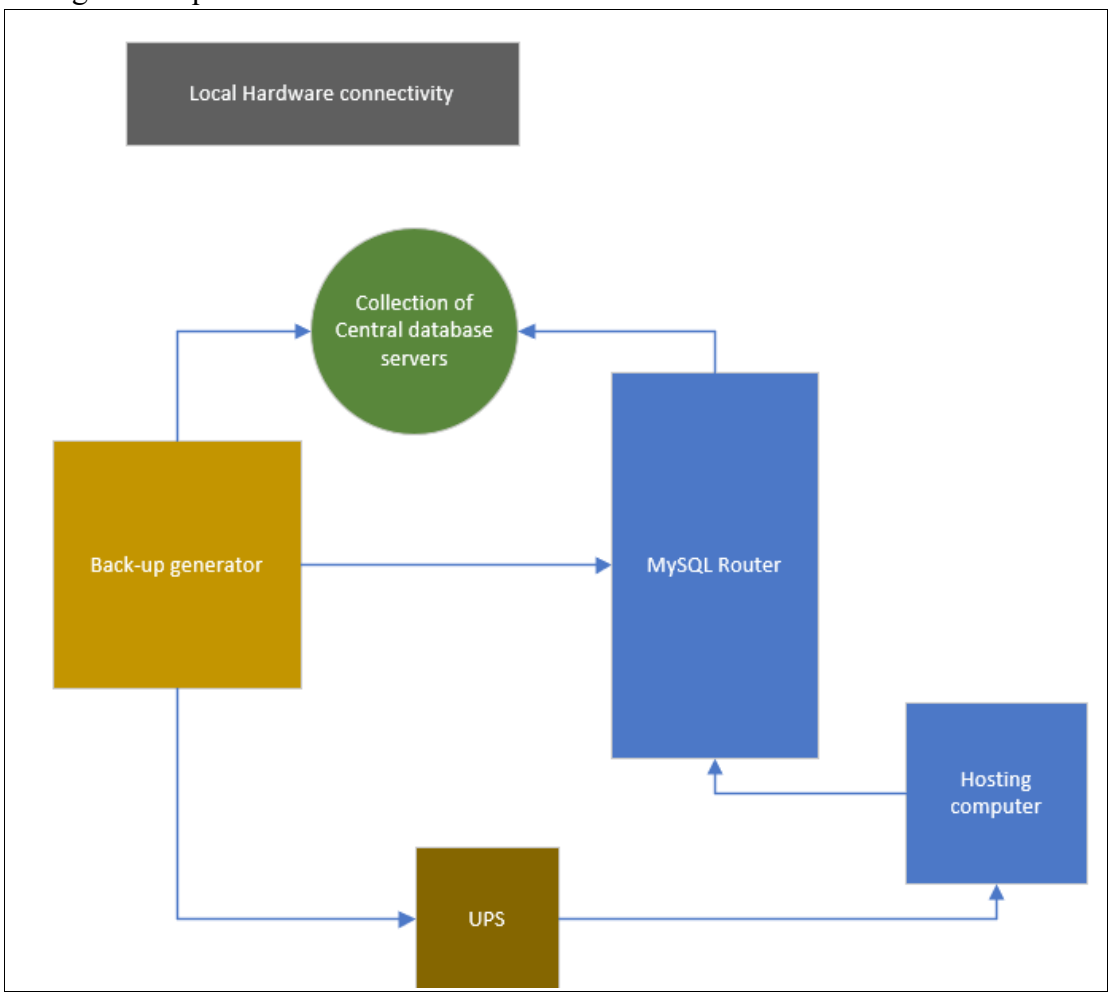
Limiting this endeavor is the structure that the local databases are based on. While the universal database will function on a MySQL server this may not be true. An initial constraint to be managed is acquiring or creating proper drivers to ensure the two databases can 'talk'. While time is amply given during this project it's important to not squander it. The first iteration must be functional by 1 year from initializing the project.

This project will no doubt be highly discussed with many voices trying to get involved. It's important to not get dissuaded or influenced by these outside parties. While the stakeholders hold some influence over the project it's important that these are ironed out immediately. With it made perfectly clear that once design has finished there are no thoughtless changes.

Resources

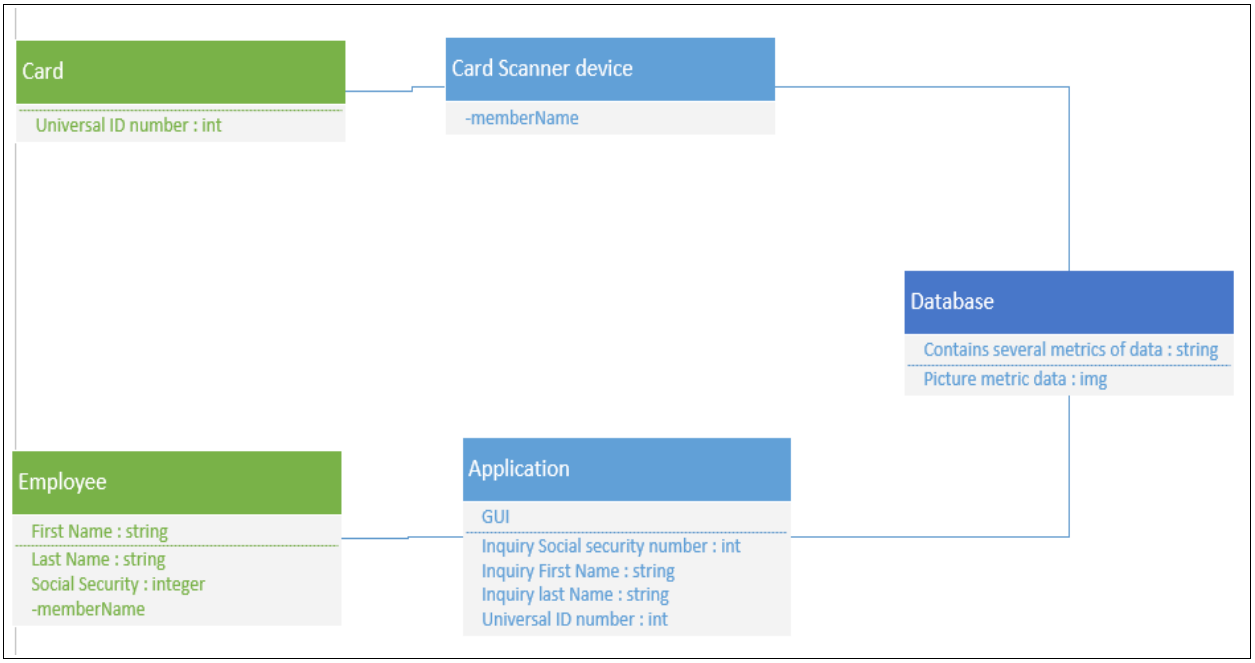
System Hardware Architecture

The hardware necessary for this database is more than just a simple server. The overwhelming and constant load stress that will be put on it requires a proper facility, ventilation, and time tested machinery. This will affect the whole country at all hours of the time so 100% up-time is vital. For the central database itself the hardware required is as follows: a UPS, two dozen servers, a back-up generator, a computer to act as a means of interfacing with the database. Additionally a MySQL router capable of setting up a DMZ, capable of load balancing the servers, having built in firewalls, and is capable of handling the sheer amount of traffic coming in is required.



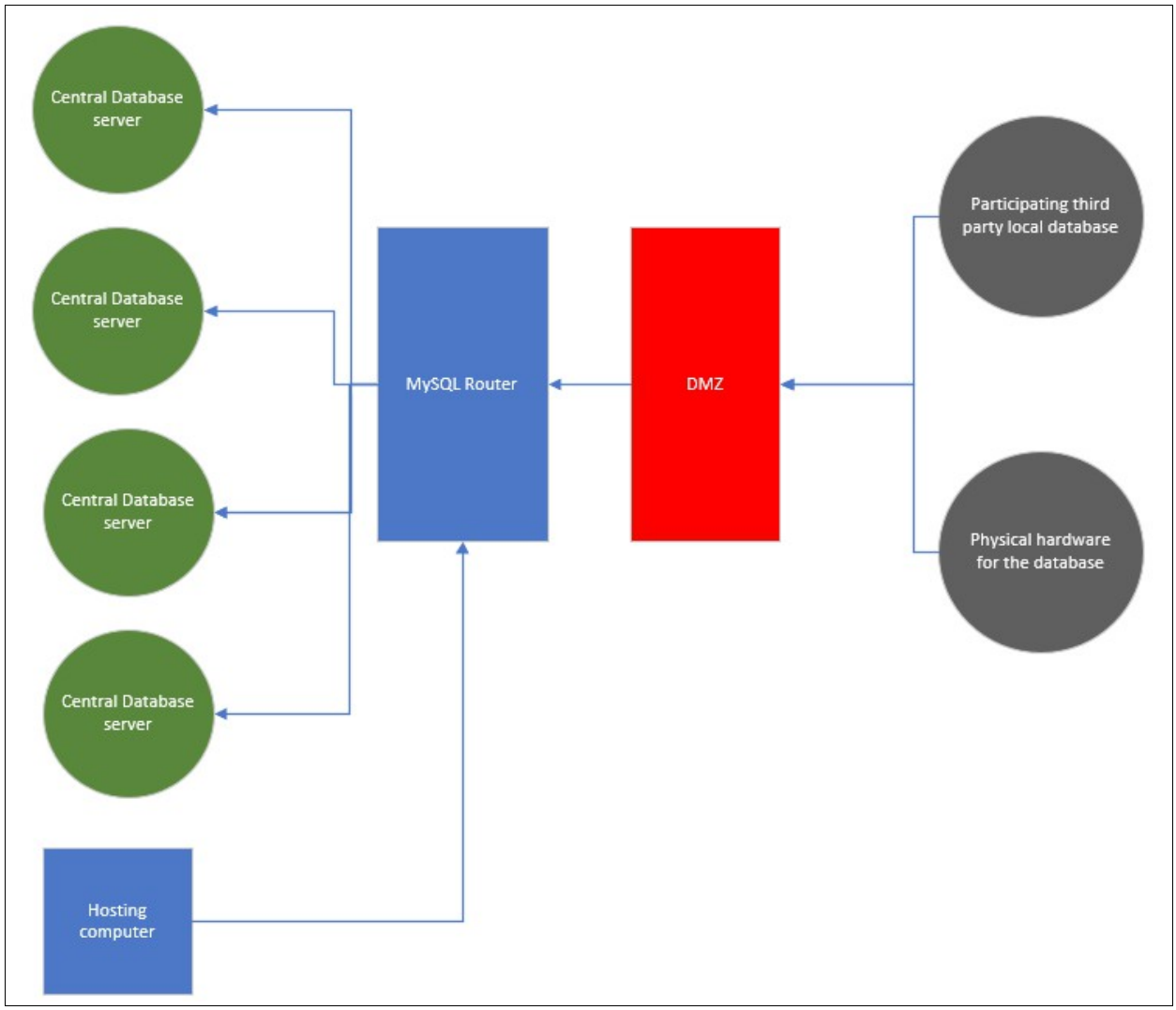
System Software Architecture

Software needs for the central database are central MySQL database to house the information of all users. Functions to access and retrieve data from various local databases throughout the country. A subroutine of that function will be to read each metric of data and add it to the correct user. Subroutines to ensure access to servers is protected from DDoS and similar traffic-related attacks. Within the router a DMZ and several security protections to keep out unwanteds is crucial.



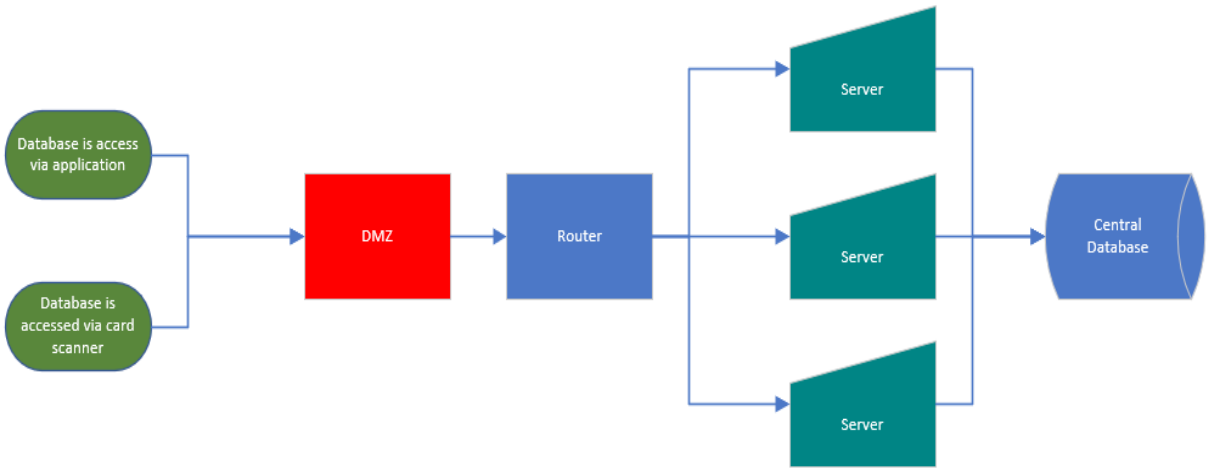
Internal Communications Architecture

The correct MySQL router capable of hosting a DMZ as well as other security measures will be the primary source of entry to the database and its several servers. Linking the servers together through a star topology is slightly faster than other methods so it will be the chosen means.



Interface Architecture

As denoted above the application used is how users interact with the database and system as a whole. Displaying information can be done via a card scanner or by entering information into the application. The displayed information will appear in page and be available for printing if desired. Below is a visual representing the order of operations for the entire process.



System Overview

The system will function simply. Citizens(users) add data into the system in the same way they do already. When applying for driving licenses, at hospitals, or at any other facility where personal data is accumulated. Provided that facility's database is approved by the government and linked to the universal database; the information will be added to both that local database and the universal one. Users will be unable to edit their own data at anytime. To ensure no forgeries are taking place. The following briefs are detailed to greater lengths in the subsequent sections of this document.

Database Management Systems details how the system should pull from each database and populate the central one. As well as the non database managerial documents such as the one operating the UI. Finally it details the expected size requirements for the system as a whole.

Software covers the language(s) to be used, general processes and functions for updating the databases, and security protocols.

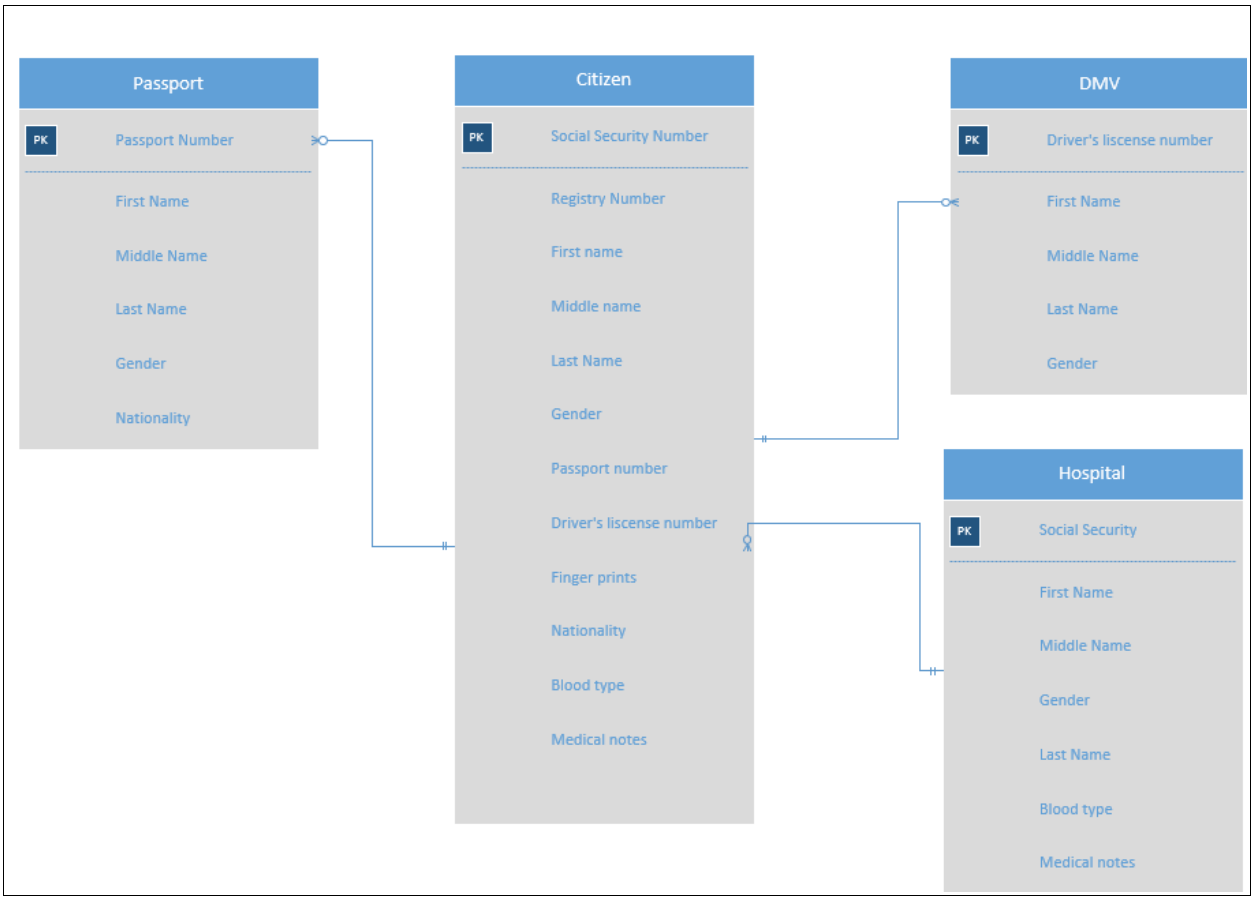
The hardware section outlines what machinery will be required and their parts. Showcasing how to organize them and stating general power needs.

Human-Machine Interface and Interface Design both outline the graphical interface needs that will be used by users. As well as how they will function and be used.

External Interfaces and System Integrity Controls both detail security needs, accessibility, and other integral functions not debriefed in other systems sections.

Document Detailed Design

Database Management System Files



The DBMS is represented by Microsoft Visio. It details in specifics how the database will be structured, and connected to other participating local databases. The overall storage size of this database will be quite large. The current population of the UK is roughly 66 million. Allowing room for extra non-citizens to acquire a universal ID, and accounting for the number of metrics required for each person. The expected size(at capacity) of this database should be around 50 terabytes of data. The initialized populating of the database will use the extract, transform, load, method.

Update schedules are of course weekly. It will be under constant supervision by a competent crew and evolve as the government's needs do. The recording structure is simple. It's referential and is variable in length to accommodate for unorthodox names. Up to a limit of 20 characters per field. Additionally when entered fields should be safeguarded from malicious pseudo-code entered, in case of attempted hacking. The file access method should be sequential. It's simple and effective.

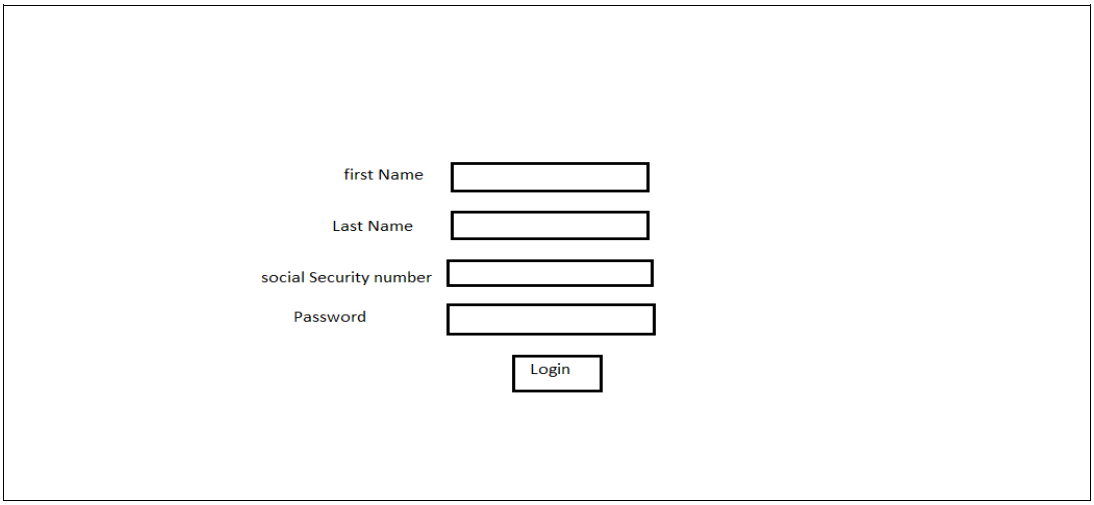
Non-Database Management System Files

There is but only one non-database related file and that's the user interface that's used to access the database. It's access method should sequential, with a maximum variable length of 20, matching the database during query searches. The update frequency will be less than the database given its static nature.

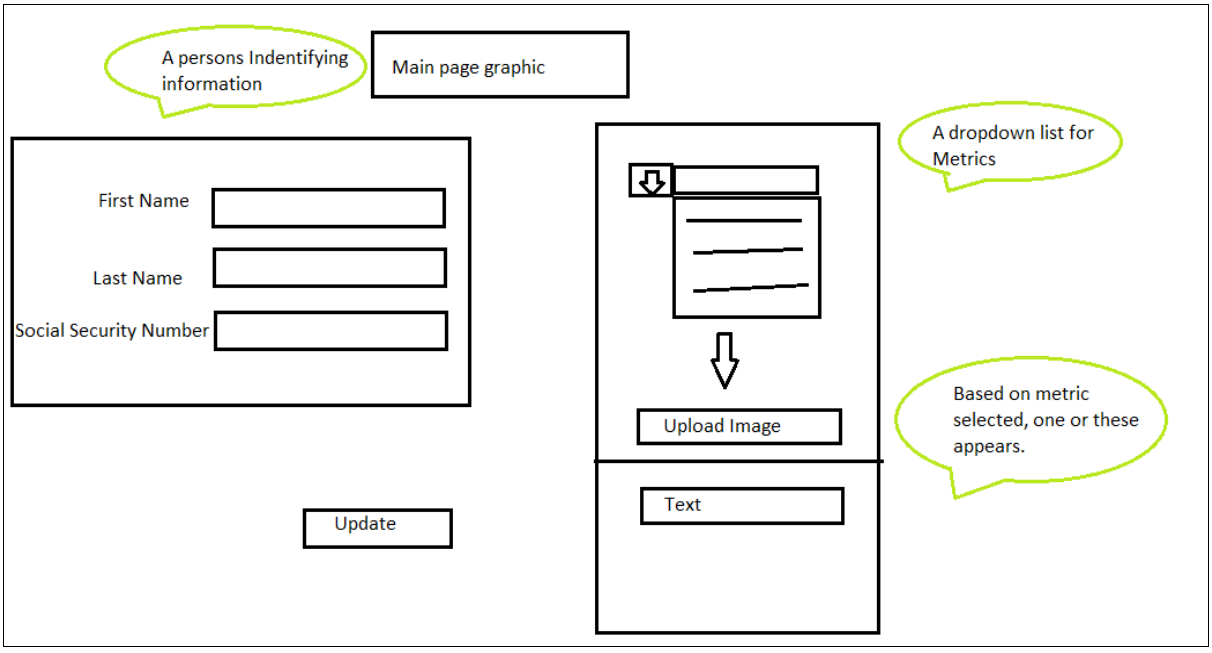
Human-Machine Interface

The central database will be populated automatically with all manually obtained data but also with data from participating local databases. Each of these stations will possess a UI that links either to the central database or their local one. The user selects the metric to update/create and fills in the information. The GUI used transmits the data over a secure https connection to the database. The GUI will possess tools necessary to prevent malicious activity and ensure compatibility. Bio-metrics such as finger prints, facial recognition photos, etc. Can also be stored in the database as blobs with no problems. The GUI itself is minimalist and very small. This allows for most government or medical computers to run it reliably. Security for simple programs like this is of top priority.

The interface is simple. With the login screen requiring dual authentication first with a password and the administrators social security number, and then a follow up text message or email, their choice. It additionally follows an HTTPS connection. It is not browser-based. The main page once entered allows for simple identifying information on the human person that will have their metrics changed. The drop down menu allows for quick selection of the metric in question, and then another menu appears allowing for either upload(if image) or text. Demonstrated below.



(GUI figure 1)



(GUI figure 2)

Hardware Detailed Design

The DAS4E24S SAS JBOD Rackmount allows for housing all of what is required for the server. It allows for 12-384TB of storage via up to 24 different hard drives. It's capable of daisy chaining, has 2400MB/s of bandwidth, and a redundancy back-up power supply. Power usage required for this is roughly 25kWh per day, or 9100kWh a year.

Power usage for the computer(s) necessary to monitor the servers is roughly 20kWh per computer. Central server location computers will require their own tower, and monitor. Quality of monitor is irrelevant. Tower specifications are roughly 100GB of storage, 4GB of RAM, bottom level graphics card, an i5 processor with thermal paste cooling, and a standard 600w power supply. Additionally a keyboard and a mouse.

The router power usage is roughly 5kWh. The router will be CISCO, if budget allows the ASR1002-HX model. It supports 25Gbps of bandwidth, possesses 2 power supplies built in, 1 GE and 10-GE ports. Internally it offers solid WAN coverage.

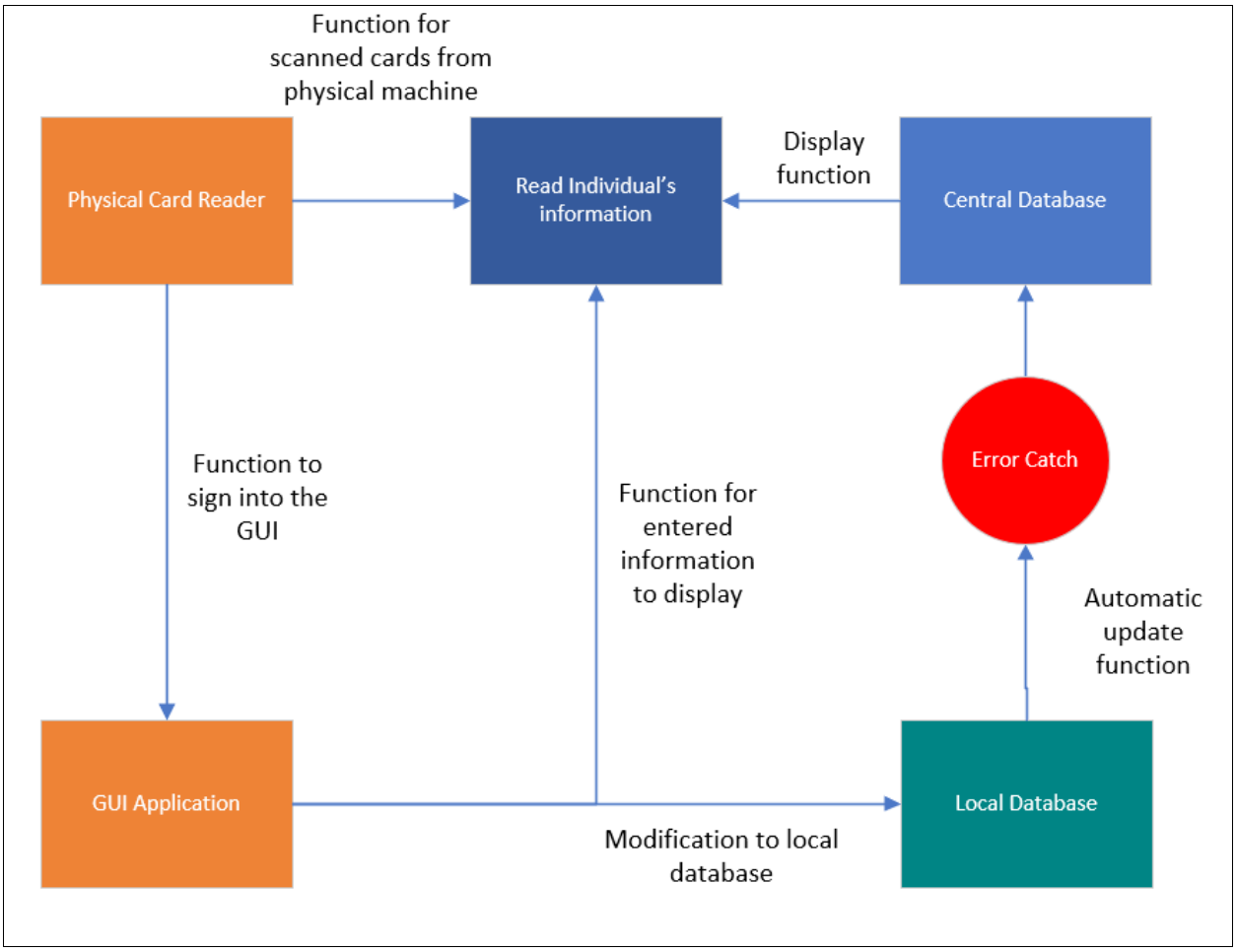
Beyond standard several meter length CAT-5 cables and power cables nothing else is mandatory.

Software Detailed Design

The module for adding or editing data in the central database operates on a simple process. Authorized individuals sign in to their database application and using it update both their local database and the central one at the same time. A secondary process of automatically updating the central database using linked local databases is possible. Using the FEDERATED storage engine in both the local and central databases the two will update each other as changes occur. This will require updates to participating local databases however. Functions to handle errors such as one server being inaccessible will be required.

Interface Detailed Design

There will be a module for physical cards to prompt and read the database. To display information if the GUI application is open but other-wise not.



External Interfaces

As all data is either a basic image or text being stored in a database all information will be dispensed in that simple medium. When accessing the database the source of the call and the router must shake hands and establish that it is a trusted source. It's staffs job to ensure that the router has an up to date trusted white-list excluding all attempts of access that are not included. Each card scanner and participating place of business will have be white-listed. Should an error occur with white-listed connections(such as inputting too much data) a catch is in place to alert the user to this infraction. Additionally catches to prevent malicious code from being inserted into the text fields should be up to date.

System Integrity Controls

As stated throughout the document the database has multiple levels of security. Requiring dual authentication and access to already sensitive data to even gain entry to the application. The database is protected via default denial of access for non-white-listed connecting sources. Before even getting to the router connections must pass through the DMZ where it functions as a second firewall in addition to the one the router possesses innately.

Points of Contact

Name	Role	Contact
Scott Allison	Project Manager	1-800-1234 / scott.allison1@snhu.edu
Chet U'Becha	System Proponent	974-6583 / ChetMXCMstr.yahoo.com
Kenny Blankenship	User Organization	974-3856 / Elimination86@weeb.com
Byleth	QA Manager	001-2019 / 4smash@expected.com
Mario Mario	Security Manager	974-5667 / Turtlebasher@Yahoo.com
Saitama	Configuration Manager	002-5555 / Heroforfun@TownZ.com

Glossary

Terms and abbreviations used in this document. (Updated as project goes on)

Term	Meaning
MySQL	Open source relational database software.
User	The citizens of the United Kingdom who will be in the database.
WBS	Work Breakdown Structure
Load balance	The practice of sharing server stress between an array of local area servers.
UPS	Uninterrupted power supply.
DDoS	Denial of Service attack. A server is overloaded with requests and crashes.
GUI	Graphic User Interface

Cited works (in progress)

https://networkoutlet.com/products/cisco-asr1002-hx-router-with-4x10ge-4x1ge-ports?variant=30323142426704&currency=USD&gclid=EAIaIQobChMI_ajs8vK65wIVuIVaBR2eGwsxEAQYASABEgK46vD_BwE

https://www.digiliant.com/product_info.php?products_id=921&_vsrefdom=adwords&gclid=EAIaIQobChMIs-7eke265wIVEIiGCh1yYAu1EAQYASABEgKPR_D_BwE&action=add_product&osCsid=chu7i9mqf77onodeuk153t7vc7&osCsid=chu7i9mqf77onodeuk153t7vc7