IT Project Closure Document

IT 420

By: Scott Allison

Introduction

The problem being faced was a rampant miscommunication of varying sources of data within the United Kingdom. A dreadful feeling of unknowns within borders. Finally an inability to communicate medical needs. What way could all of this be managed with one solution? The significance of the National ID database was simple as it addressed the problems outlined above. The severity of which is incomparable to other, unmentioned problems. Objectives that were accomplished were a functioning database that syncs with other participating databases. An interface that allows for the viewing and manipulation of data within the central database, a physical card that displays simple information on a citizen, and finally a hardware interface that allows only the viewing of data by using the aforementioned card.

Verification Plan

Ensuring each artifact and deliverable can be accomplished requires a plan of action. The plan for this project as mentioned in the design document is segregating the project overall into four phases: Completion of the initial database, the modification and linking of participating databases, the construction and implementation of the hardware and software applications, and finally public release and post release management. Testing the phases and more are outlined below in greater detail.

Stage one: Here the initial planning is done, tasks decided upon, teams formed, and tasks delegated. It's here that the initial draft of the first database was made. Verifying its completion is paramount to the project and doing so ensured that it functioned. That data can be entered into it and that the metrics required are all present and accept data accurately. Feedback on whether or not this is satisfactory had been done by an internal team whose job it was to "break" it. Additionally phase one is where the ordering of all physical hardware for later phases was performed. This was a simple task to verify, as records of purchasing and ordering were retained.

Stage two: Crafting the tools to modify participating databases, connecting them to the central database, and creating the auto-sync feature. Additionally basic security features were applied. Criteria to mark these as satisfactory is whether or not they work and are the syncing feature is able to update at the same time for both the third party database and the central.

Stage three: Intense stress testing, placement of the physical hardware, mock up and finalizing of the physical ID card, first foray into controlled public stress test with voluntary data. This phase had many steps. Verification that these artifacts are completed properly was that the physical hardware had been delivered and installed. That it functioned with the central database when accessed via the ID card too. That the controlled public test was done with no security breaches. And finally that the stress testing resulted in a no crashes.

Stage four: Scrubbing of all leftover internal data within database entries and coding comments. Final testing of security features. Distribution and proper installation of software to participating parties. Finally, public release. As well as standby for functionality and troubleshooting. Satisfaction of delivery is measured by the softwares being delivered and installed properly. All unnecessary coding and database entries being deleted, the security features stopping all moderate and high level risks, and finally that the whole system works!

Communicating each phase to the stakeholders and collecting feedback is simple as more than half is internal testing. Feedback was reported after each test, weighted in severity by ease of replication, odds of system failure, causing a data breach, and other factors. Then they were placed in a hierarchy similar to the risk assessment. Those of moderate or above were be acted on until additional time permitted.

Postmortem Summary

Methodologies & Evaluation

For this project the project method employed was the “Hybrid” style. This style calls for breaking down projects into by either discipline or function. With clear goals and a scope that is unwavering. While requiring a strict structure created by a WBS the hybrid style allows for flexibility by incorporating fragments of the agile style. This allowed for minor adjustments based on the market and world at large's changes.

Unexpected changes such as the new coronavirus demanded immediate flexibility. By allowing work from home and equipping staff with the means to do so we were able to stay on schedule with minimal delay and only a modest change to the budget. While working from home it was required for staff to have secure connections and remain in contact for meetings and general communication. Thankfully the business already housed a few employees who worked remotely and this template was followed.

Tools utilized this project were Microsoft Azure, MySQL, Visio, and Excel. These softwares were all quite useful with regard to the project. Excel aided in the cataloging of tasks, minor mock databases. MySQL was crucial as was the basis for the entire database. Microsoft Azure was less useful, but still so. As some members of the team preferred to create and test portions of the project with it for ease of testing while working from home.

Risk Mitigation

Complications and risks that developed during development that hadn't been planned for were the current corona virus, with which a plan needed to be developed immediately. Suggestions for this dilemma required a shift from a large portion of staff working on site and to working remotely. Setting this up entailed equipping said staff with laptops, and establishing a secure connection for them to work on. Expect this to affect project scheduling and budget.

Another risk worth noting for the future of this project is government regulations. As the political sphere is always toxic and full of strife and rapid changes it's important to keep in mind what may be changed for the future. Perhaps cataloging some metric will be deemed unethical or illegal by stakeholders and must be removed or altered to comply. It's important to have a procedure for implementing this, replacing it if necessary, and how to go about this.

Project Status

Objectives

The objectives outlined in the project design document were met. As the scope of this project was narrow with only three large goals to accomplish: A secure and complete working database, a physical ID card with hardware access point, and software established to enter and modify data within the database. The number of metrics called upon by stakeholders after much time and effort were implemented as well.

Issues

Issues, while overcame, still occurred. Some metrics such as biometrics like fingerprints and other image based entries proved to demand more file size than initially though and the servers needed be adjusted to accommodate for that. Additionally the networking required more bandwidth than initially though as even during the tests it was slow. Upgrading the hardware was a simple task and remained within the allotted budget.

Alternatives/Recommendations

While only minor changes to hardware were required the team spoke up about improvements to the software side. Stating that some third party widgets would be used in places to great defectiveness. After testing them for compatibility and probing for security risks most suggestions were actually implemented into the design of the database.

Overall, the projects current status is on task and within the triple constraint of budget schedule and scope.

Communication

Allotted for each phase of the project as denoted in the WBS is time for meetings and reflection. To expound on that in greater detail meetings were held at task leader's discretion but at minimum one a week with the project manager. Upon each tasks completion a report by the task leader was drafted and submitted to the project manager to review and compile with others for a document to present to the stakeholders. Specifically interested politicians who needed information for press conferences. Knowing this the information outlined in the compiled document needed to be non-technical.

Future Enhancements

One future enhancement to this ID database could potentially be added security features. While security is already satisfactory would-be hackers will not rest on their laurels. Constantly improving the security is a necessity in today's society. Another enhancement would be software application. Giving the branch using the database a better tool to modify entries and view them.

Further future additions would be increasing the number of metrics held to create a more extensive database on a citizen. This could aid in saving lives by allowing for more medical information to be stored, and even make it more difficult to forge fake documents. One last potential addition is the implementation of banking information and the ability to use it. Paying for goods using your universal ID tethers all major systems a citizen may need in one secure package. Fraud would be easier to catch and citizens could feel confident knowing that if their information is stolen they and the government will know about it immediately. To accompany this an alert system and several more security features would need to be added.

Implementation Support

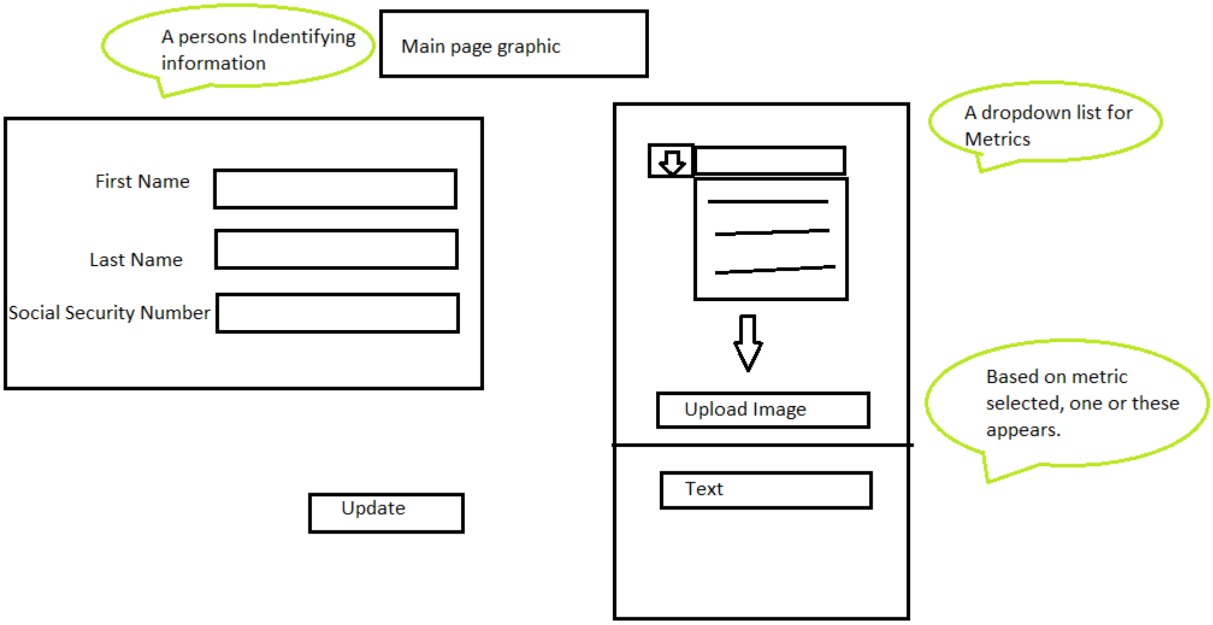
Transitioning from internal to live has been setup already through extensive testing at each phase of the project. As this is not a system modification there is no previous code to worry about disrupting. A simple toggle is all that's required. The physical hardware was distributed prior to going live and has been thoroughly installed at their locations. With each city hall throughout the country being given multiple ID cards. A public hearing should likely decree the systems live status and the allowance of card distribution and usage. The over estimations of bandwidth usage and server space should prevent any further complications with space but on hand should be extra storage units for added server space.

Maintenance plan

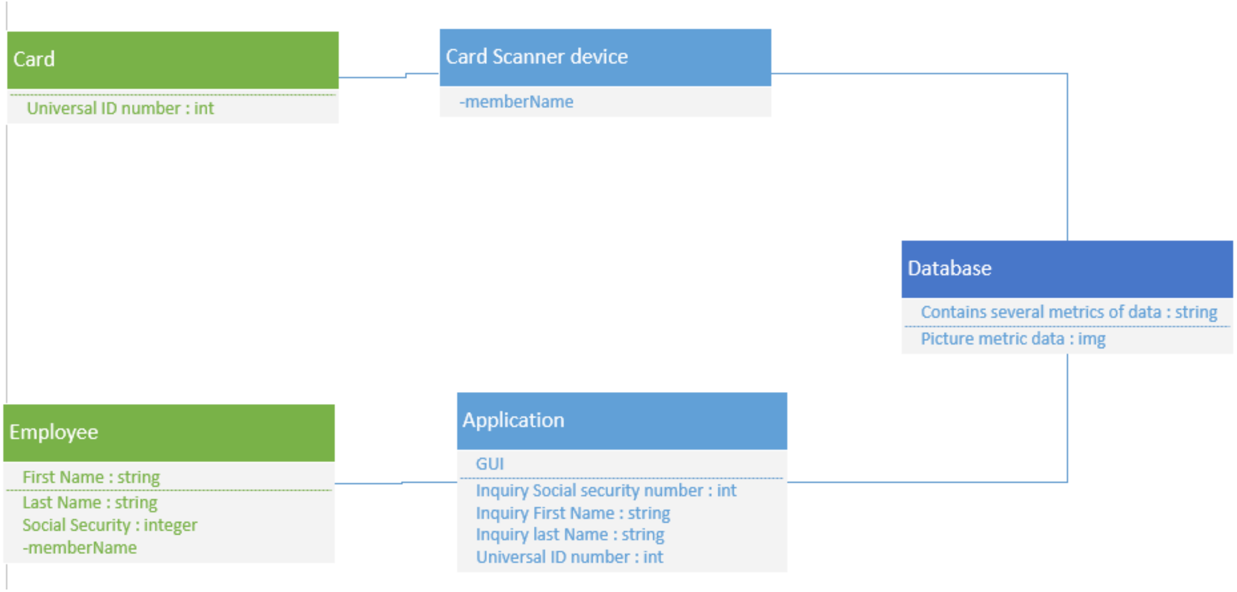
Servers last a long time and so do routers. However as noted above there is a surplus of extra servers. Replacing them is standard practice these days the same as the router. These two factors require minimal extraneous planning for. Software updates however will require some effort as not all participating databases will be using the same base coding as the central database and each other. So communication between the maintenance team and the IT staff at each facility will be required.

Appendix

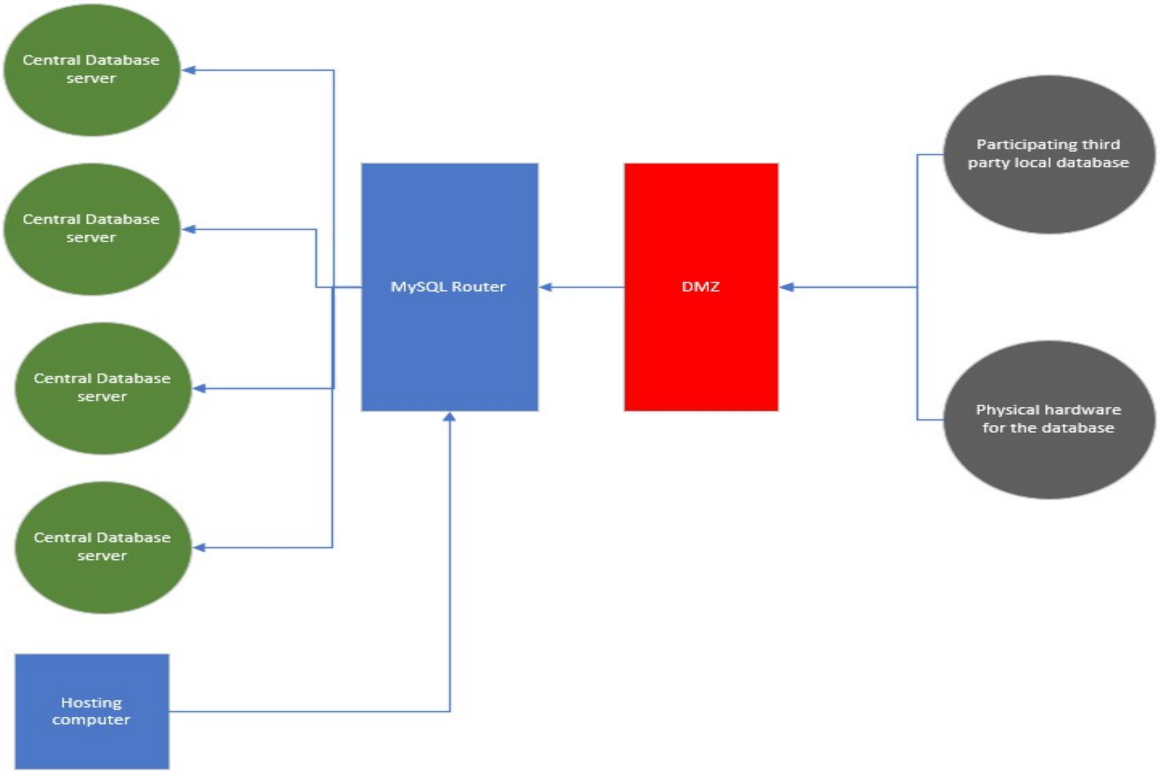
As noted this project is for the creation of a database to house the ID's of every citizen within the United Kingdoms borders. Accomplishing this requires a database, physical hardware, and software. The guidelines noted for these are denoted in charts and graphs below.


A persons Indentifying information
Main page graphic
First Name
Last Name
Social Security Number
Update
A dropdown list for Metrics
Upload Image
Text
Based on metric selected, one or these appears.

(UI for the software access. Note, not final)


Card
Universal ID number : int
Card Scanner device
-memberName
Database
Contains several metrics of data : string
Picture metric data : img
Employee
First Name : string
Last Name : string
Social Security : integer
-memberName
Application
GUI
Inquiry Social security number : int
Inquiry First Name : string
Inquiry last Name : string
Universal ID number : int

(The architecture for the database structure, note: not final)



(Networking path for database access)