7-3 Final Project Prompt II Submission

Nouman Ali

### IT 415 –Advanced Info Systems Design

Southern New Hampshire University

Professor: Gurdeep Basra

**Table of Contents**

**Project Plan**.............................................................................................................................3

Work Breakdown Structure...........................................................................................3

Timeline.........................................................................................................................4

Dependencies.................................................................................................................4

**System Design Document**........................................................................................................6

Introduction...................................................................................................................6

Requirements.................................................................................................................6

Constraints.....................................................................................................................6

Resources.......................................................................................................................7

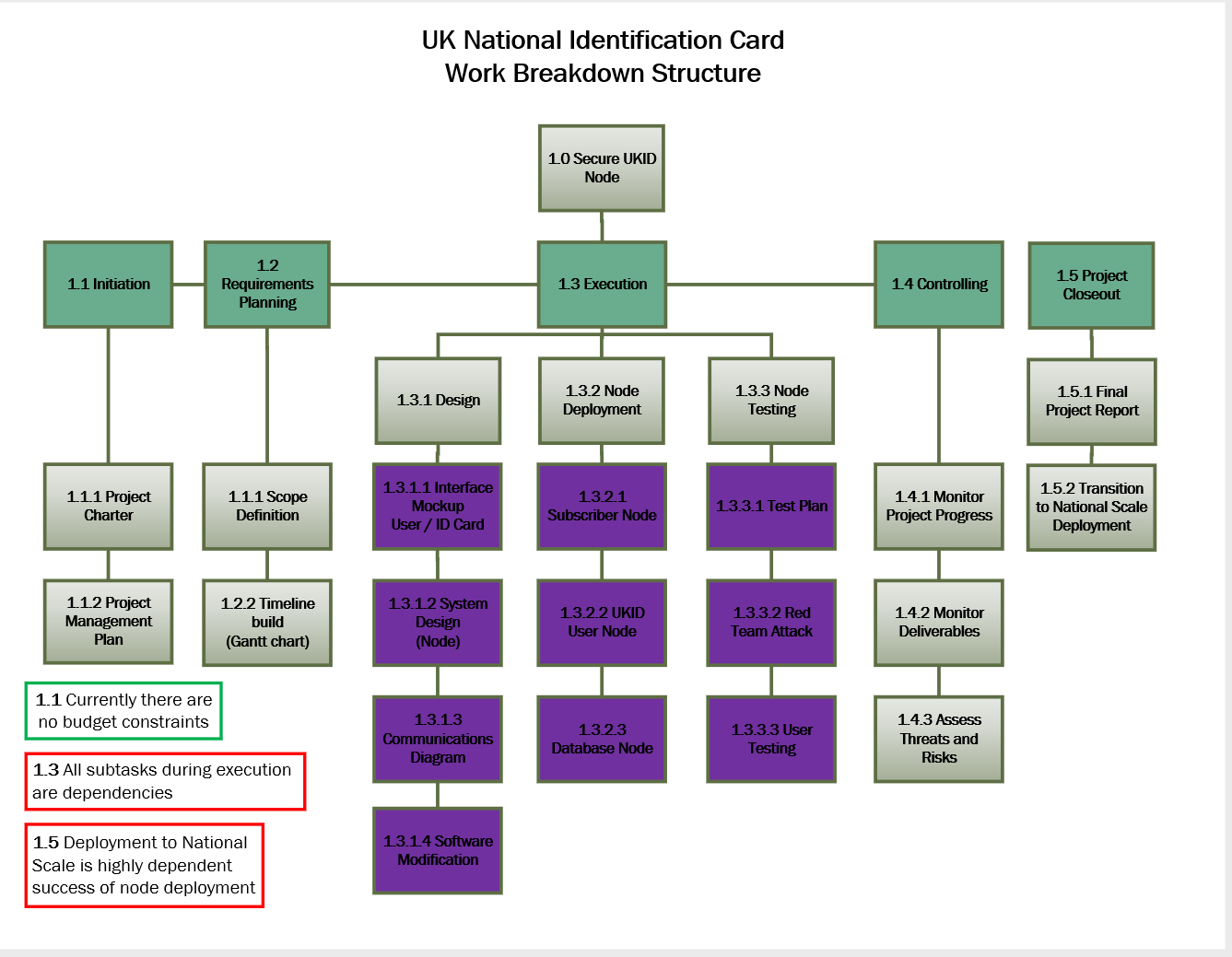
System Overview...........................................................................................................8

Documented Detailed Design......................................................................................10

**References**..............................................................................................................................11

“UK National Identity Card Project Plan”

**“Work Breakdown Structure”**

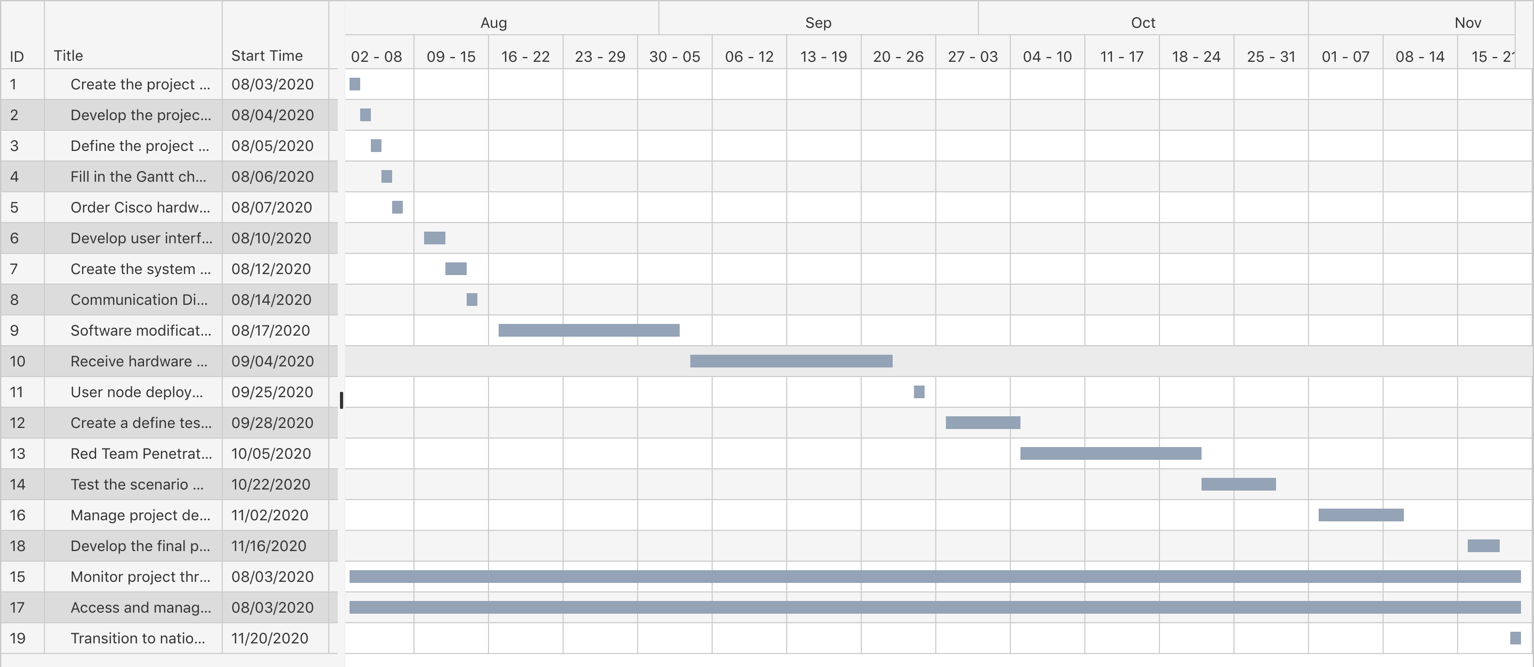
The “work breakdown structure (WBS) for the UKID project (Fig 1.) utilizes the System Development Life Cycle (SDLC) as a framework”. The five phases are shown in green while the critical tasks with high dependency stages are stated in purple.

“Figure 1. Work Breakdown Structure”

**“Timeline”**

The UK ID project 's important dates are between 2nd Aug – 21st Nov timeline (Fig 2.).

* Aug 2nd, 2020 Project kickoff
* Aug 3rdPhase II
* Aug 7th Phase III Receive hardware / Node deployment
* Phase IV runs in parallel with Phase III for project duration
* Nov 20th, 2020 Handoff to national level. End of Phase V



“Figure 2. Project Timeline”

**“Dependencies”**

Many dependencies occur in the project. Those are expected with minimal risk of turning the project off entirely. List of the activities in Figure 3. Contains all of the listed tasks needed to remain on schedule after kickoff. To order to avoid failure, all tasks have previous tasks, however, the following tasks have to be completed:

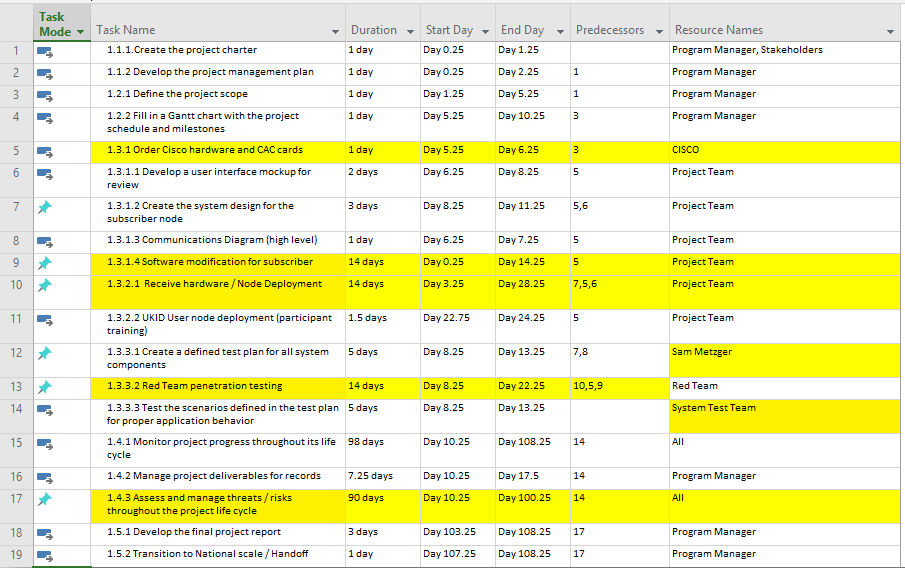
**“1.3.1 Hardware and CAC acquisition.”** – If the "CISCO" supplier does not deliver the necessary equipment, there is a risk of long project timeline delays.

**“1.3.1.4 Software modification for SDK.”** – If you cannot meet UK security requirements, the chosen encryption and security parameters will result in delays.

**“1.3.2.1 Receive hardware, begin node deployment to selected sites.”** - For the company into a network kit and delivery to the sites, the hardware shipping schedule must be met.

“**1.3.3.2 Red Team penetration testing**.” - Specific cyber threat models are used to solve security problems. For national deployment this feedback is important.

“**1.4.3 Assess and manage threats and risks throuout the project lifecycle.”** The success of the project depends on how protected the data is after project execution.



“Figure 3. Task List with Dependencies

System Design Document”

**“Introduction”**

The "UKID card project"   has many functions, including authentication and the prevention of welfare theft and the security of citizens ' personal data to support public service agencies.

**“Requirements”**

* Provide a "secure, scalable node" for transmitting and receiving "national ID card data".
* Transmit and Receive Personally Identifiable Information without compromising the confidentiality, integrity or access to that information.
* Personal identity information shall be transmitted and obtained without regard to privacy, integrity or access.
* Integrate current technologies of biometric authentication to deter and improve the protection of fraud.

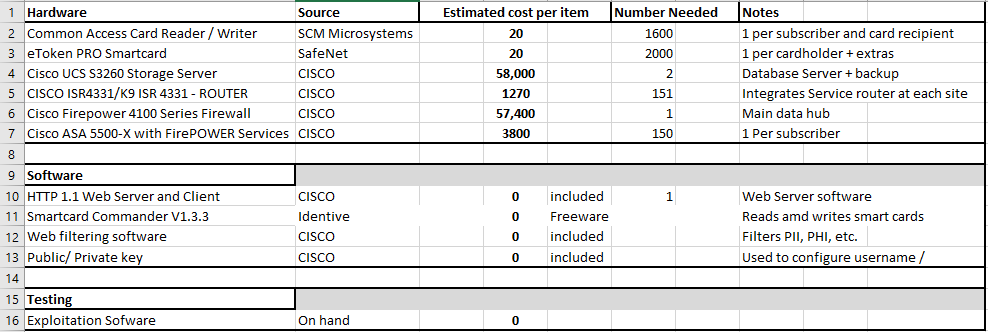
**“Constraints”**

The subscriber type is limited. All subscribers are unable to reach all information.

* “Type 1 Hospitals, Clinics and EMS access PHI, PII and alerts”
* “Type 2 Police, Fire, and public assistance agencies access PII and alerts”
* “Type 3 DMV and Libraries access public information only”
* CAC read / write software that is necessary should be run on existing Subscriber workstations. The system may need to be updated in specific situations, resulting in minor delays.

**“Resources”**

The resources are listed for this project under (Table 1). The ISP is already being funded and the hardware is being developed for "server operating systems / firmware". The key firewall expense to the central data center is notable, which would be the strongest protection against attacks while keeping all data stored secure from attackers. To order to ensure compatibility between "hardware and software", the supplied of equipment is limited to retain a standardized form type throughout installation. This also enables a pace-free installation of most subscriber sites if delivery delays occur.



“Table 1. Resources”

**“System Overview”**

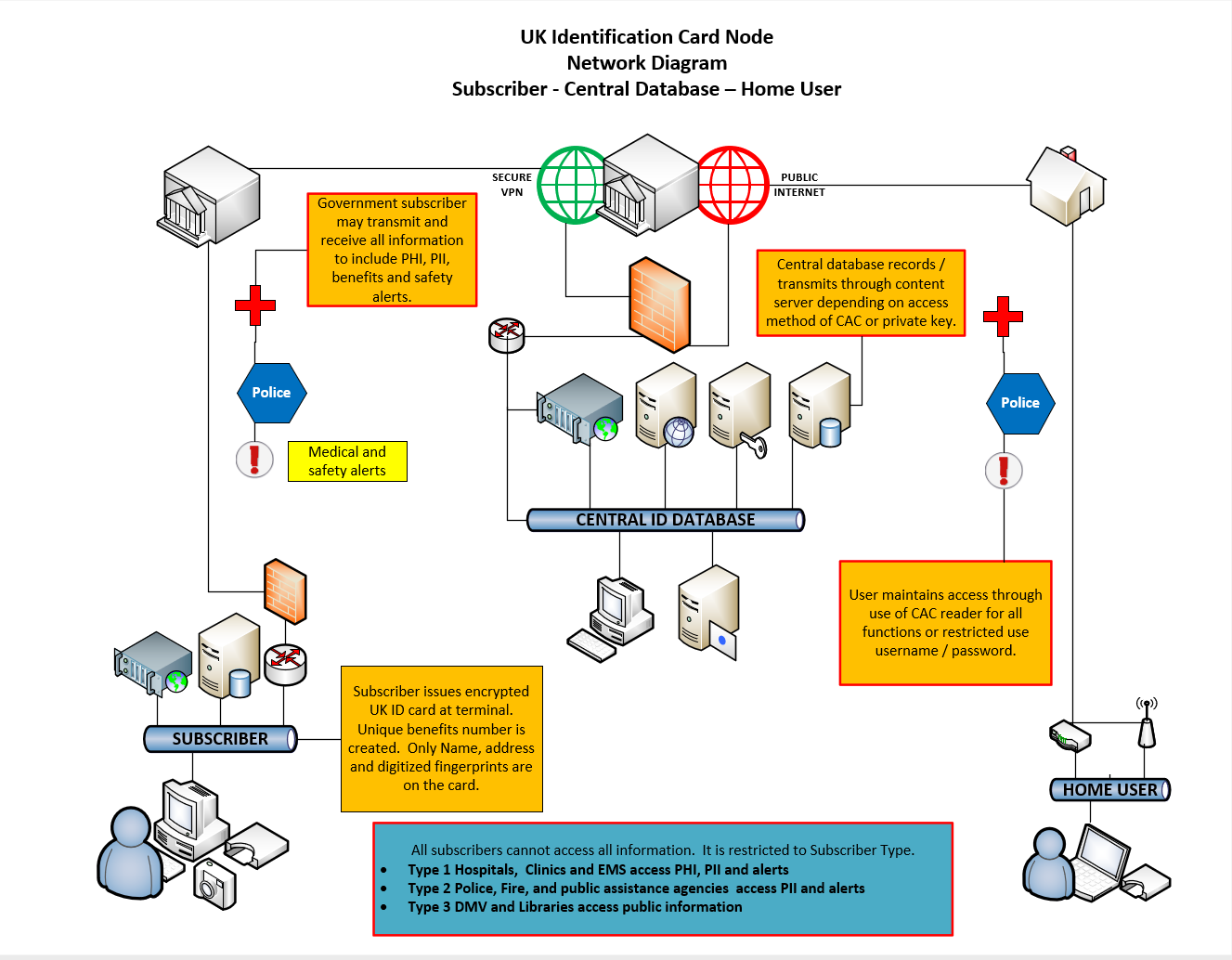
It is not difficult to build the entire "UKID subscriber node". Simplification and protection are the driving forces. The controlled data center firewall from the private internet linked to the data server and on-site router will accomplish these goals. The rack server program generates the Web Host list, the encrypted key list and filters content into the various subscriber forms. The screening program prevents ID card holder medical records from going to a librarian or DMV, maintains a criminal record from hospitals, etc. This program helps you, if appropriate, to send a health warning or a safety warning to all subscribers. Each user node has a smaller data server and firewall router to transmit data via a VPN to the central database. The user will have the option for a username / password to access the majority of medical documents in a limited manner, criminal history, DMV information, with the use of an issued card readers. Considers for preserving the confidentiality, Integrity and Availability to this information (by cardholder) are creating situations where certain data can only be updated on a subscriber page, while cards can simultaneously be linked by the user and data entry specialist for two-party verification. To reduce the costs and delays during deployment, the full use of existing infrastructure, i.e. new equipment adapting to subscriber networks is also necessary.

Figure 4. System Overview

**“Documented Detailed Design”**

|  |  |
| --- | --- |
| **Work Breakdown Structure Item** | **“Design Detail”** |
| **“1.1.1. Create the project charter”** | This is the launch of the project with "stakeholders and the PM". To establish a framework and a timetable, initial guidelines and responsibilities are written up. |
| **“1.1.2 Develop the project management plan”** | How the PM and stakeholders communicate over the SDLC period in management plan. |
| **“1.2.1 Define the project scope”** | Produces the project deliverables |
| **“1.2.2 Fill in a Gantt chart with the project schedule and milestones”** | Project milestones provide all team members with specified and implied tasks. |
| **“1.3.1 Order Cisco hardware and CAC cards”** | Guarantee that equipment can be delivered timely determines how fast subscribers' nodes can be placed. |
| **“1.3.1.1 Develop a user interface mockup for review”** | At the development site the original mock-up is built for actual service and design use. |
| **“1.3.1.2 Create the system design for the subscriber node”** | “Test card readers on multiple operating systems. Most OS have card reader functionality, some need freeware installed” |
| **“1.3.1.3 Communications Diagram (high level)”** | Develops the high-level system-specific architecture between clients, central repositories and home users. |
| **“1.3.1.4 Software modification for subscriber”** | Modification of the laws on data encryption will involve modifications to existing applications, several of them with the SDK (Software Development Kit). |
| **“1.3.2.1 Receive hardware / Node Deployment”** | The computer is grouped into a server, "router and firewall node kit with the card writer". |
| **“1.3.2.2 UKID User node deployment (participant training)”** | Hardware to the main public infrastructure facilities must be transported. |
| **“1.3.3.1 Create a defined test plan for all system components”** | When shipping the devices, the website and data server monitoring program focused on the duration of cyber-attacks and failures. |
| **“1.3.3.2 Red Team penetration testing”** | “This is done with in-house exploitation software not available to the public. The Red team will use every resource to break through the firewalls while finding a solution to seam security gaps or change setting on the hardware.” |
| **“1.3.3.3 Test the scenarios defined in the test plan for proper application behavior”** | Follow up with 1.3.3.2: The device is secured by AGILE sprints. |
| **“1.4.1 Monitor project progress throughout its life cycle”** | Data from all subscribers and house users are retained. |
| **“1.4.2 Manage project deliverables for records”** | Penetration check results with fixes, data and hardware and/or deployment problems. |
| **“1.4.3 Assess and manage threats / risks throughout the project life cycle”** | Red team from external sources continues threat / risk management. Drive counterattacks. |
| **“1.5.1 Develop the final project report”** | The stakeholders and interested parties shall receive all metrics reported during the project in a suitable format. |
| **“1.5.2 Transition to National scale / Handoff”** | Accomplishment itself has benefits. |
|  |  |

# **“References”**

“CISCO. (2019, April 25). *Servers and infrastructure*. Retrieved from CISCO: https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html?CCID=cc000264&DTID=pseggl000015&POSITION=SEM&COUNTRY\_SITE=us&CAMPAIGN=DC-06&CREATIVE=US\_SEM\_DCB\_UCS-Servers\_BMM\_B"-"Servers\_cc000264\_pseggl000015\_0&REFERRING\_SITE=Google&KEYWORD=%2B

Hoffer, J. A. (2013, Janurary 02). *Managing the Information Systems Project.* Retrieved from PrenHall:" "https://web.archive.org/web/20130102214255/http://www.prenhall.com/behindthebook/0132240769/pdf/Hoffer\_CH03.pdf"

"IDENTIVE. (2019, April 25). *Contact Smart Card Readers*. Retrieved from IDENTIVE: https://www.identiv.com/products/smart-card-readers/contact/"

"NextWarehouse. (2019, April 25). *CISCO UCS SP C3260 VALUE*. Retrieved from NextWarehouse:" "http://www.nextwarehouse.com/item/?2656642\_g10e&gclid=Cj0KCQjw2IrmBRCJARIsAJZDdxBWiOqp5o4Sa5LI4d0LbntwxlGOYKtjlvMpnL1qwazTXYYvIGDz8T4aArTCEALw\_wcB"

"SafeNet. (2013, July 03). *eToken PRO Smartcard PRODUCT BRIEF.* Retrieved from dotforce: https://www.dotforce.it/wp-content/uploads/2014/08/eToken-PRO-SmartCard-PB-EN-v5-Jul032013-web.pdf"

"ServerSupply. (2019, April 25). *CISCO ISR4331/K9 ISR 4331 - ROUTER*. Retrieved from Sever Supply:" "https://www.serversupply.com/products/part\_search/pid\_lookup.asp?pid=224285&gclid=Cj0KCQjw2IrmBRCJARIsAJZDdxDb-76P25KHkFs142PdaqWVDuNNYaeEldqRK8MWdCXqvDlB3DKcd\_0aAiUhEALw\_wcB"

"USDOT. (2009, February 1). *Next Generation 9-1-1 (NG9-1-1) System Initiative: Final System Design Document: Version 2.0.* Retrieved from Repository & Open Science Access Portal: https://rosap.ntl.bts.gov/view/dot/4013"